Incubed Documentation

Release 1.2

Slock.it GmbH

Feb 03, 2020

Reference

1 Getting Started **1**
- 1.1 TypeScript/JavaScript . . . 1
- 1.2 As Docker Container . . . 2
- 1.3 C Implementation . . . 3
- 1.4 Java . . . 4
- 1.5 Command-line Tool . . . 4
- 1.6 Supported Chains . . . 5
- 1.7 Registering an Incubed Node . . . 6

2 Downloading in3 **9**
- 2.1 in3-node . . . 9
- 2.2 in3-client (ts) . . . 10
- 2.3 in3-client(C) . . . 10

3 Running an in3 node on a VPS **13**
- 3.1 Side notes/ chat summary . . . 17
- 3.2 Recommendations . . . 19

4 IN3-Protocol **21**
- 4.1 Incubed Requests . . . 21
- 4.2 Incubed Responses . . . 22
- 4.3 ChainId . . . 24
- 4.4 Registry . . . 24
- 4.5 Binary Format . . . 28
- 4.6 Communication . . . 30
- 4.7 RPC Specification . . . 31

5 Roadmap **61**
- 5.1 V2.0 Stable: Q3 2019 . . . 61
- 5.2 V2.1 Incentivization: Q4 2019 . . . 62
- 5.3 V2.2 Bitcoin: Q1 2020 . . . 63
- 5.4 V2.3 WASM: Q3 2020 . . . 63
- 5.5 V2.4 Substrate: Q1 2021 . . . 63
- 5.6 V2.5 Services: Q3 2021 . . . 63

6 Benchmarks **65**
- 6.1 Setup and Tools . . . 65

6.2 Considerations . . . 67
6.3 Results/Baseline . . . 67

7 Embedded Devices **69**
7.1 Hardware Requirements . . . 69
7.2 Incubed with ESP-IDF . . . 69
7.3 Incubed with Zephyr . . . 72

8 API Reference C **73**
8.1 Overview . . . 73
8.2 Building . . . 76
8.3 Examples . . . 80
8.4 RPC . . . 96
8.5 Module api/eth1 . . . 100
8.6 Module api/usn . . . 114
8.7 Module core . . . 117
8.8 Module transport/curl . . . 181
8.9 Module transport/http . . . 181
8.10 Module verifier/eth1/basic . . . 182
8.11 Module verifier/eth1/evm . . . 187
8.12 Module verifier/eth1/full . . . 212
8.13 Module verifier/eth1/nano . . . 213

9 API Reference TS **227**
9.1 Examples . . . 227
9.2 Main Module . . . 229
9.3 Package client . . . 232
9.4 Package index.ts . . . 238
9.5 Package modules/eth . . . 263
9.6 Package modules/ipfs . . . 284
9.7 Package util . . . 284
9.8 Common Module . . . 286
9.9 Package index.ts . . . 289
9.10 Package modules/eth . . . 294
9.11 Package types . . . 300
9.12 Package util . . . 309

10 API Reference WASM **315**
10.1 Main Module . . . 315
10.2 Package in3.d.ts . . . 317

11 API Reference Java **345**
11.1 Installing . . . 345
11.2 Examples . . . 345
11.3 Package in3 . . . 350
11.4 Package in3.eth1 . . . 365

12 API Reference CMD **385**
12.1 Usage . . . 385
12.2 Install . . . 386
12.3 Environment Variables . . . 388
12.4 Methods . . . 388
12.5 Running as Server . . . 389
12.6 Cache . . . 389
12.7 Signing . . . 389

12.8 Autocompletion 390
12.9 Function Signatures 390
12.10 Examples 390

13 API Reference Node/Server **393**
13.1 Command-line Arguments 393
13.2 in3-server-setup tool 395
13.3 Registering Your Own Incubed Node 395

14 API Reference Solidity **397**
14.1 NodeRegistryData functions 397
14.2 NodeRegistryLogic functions 402
14.3 BlockHashRegistry functions 406

15 Concept **409**
15.1 Situation 409
15.2 Low-Performance Hardware 410
15.3 Scalability 410
15.4 Use Cases 410
15.5 Architecture 413
15.6 Scaling 421

16 Blockheader Verification **423**
16.1 Ethereum 423
16.2 Bitcoin 425

17 Technical Background **429**
17.1 Ethereum Verification 429

18 Incentivization **437**
18.1 Decentralizing Access 437
18.2 Incentivization for Nodes 437
18.3 Connecting Clients and Server 438
18.4 Ensuring Client Access 438
18.5 Deposit 441
18.6 LoadBalancing 442
18.7 Free Access 442
18.8 Convict 442
18.9 Handling conflicts 443
18.10 Payment 443
18.11 Client Identification 443

19 Decentralizing Central Services **445**
19.1 Incentivization 447
19.2 Verification 447

20 Threat Model for Incubed **449**
20.1 Registry Issues 449
20.2 Network Attacks 452
20.3 Privacy 454
20.4 Risk Calculation 454

Index **457**

CHAPTER 1

Getting Started

Incubed can be used in different ways:

Stack	Size	Code Base	Use Case
TS/JS	2.7 MB (browserified)	TypeScript	Web application (client in the browser) or mobile application
TS/JS/WASM	470 kB	C - (WASM)	Web application (client in the browser) or mobile application
C/C++	200 KB	C	IoT devices can be integrated nicely on many micro controllers (like Zephyr-supported boards (https://docs.zephyrproject.org/latest/boards/index.html)) or any other C/C++ application
Java	705 KB	C	Java implementation of a native wrapper
Docker	2.6 MB	C	For replacing existing clients with this docker and connecting to Incubed via localhost:8545 without needing to change the architecture
Bash	400 KB	C	The command-line tool can be used directly as executable within Bash script or on the shell

Other languages will be supported soon (or simply use the shared library directly).

1.1 TypeScript/JavaScript

Installing Incubed is as easy as installing any other module:

```
npm install --save in3
```

1.1.1 As Provider in Web3

The Incubed client also implements the provider interface used in the Web3 library and can be used directly.

```
// import in3-Module
import In3Client from 'in3'
import * as web3 from 'web3'

// use the In3Client as Http-Provider
const web3 = new Web3(new In3Client({
    proof         : 'standard',
    signatureCount: 1,
    requestCount  : 2,
    chainId       : 'mainnet'
}).createWeb3Provider())

// use the web3
const block = await web.eth.getBlockByNumber('latest')
...
```

1.1.2 Direct API

Incubed includes a light API, allowing the ability to not only use all RPC methods in a type-safe way but also sign transactions and call functions of a contract without the Web3 library.

For more details, see the API doc.

```
// import in3-Module
import In3Client from 'in3'

// use the In3Client
const in3 = new In3Client({
    proof         : 'standard',
    signatureCount: 1,
    requestCount  : 2,
    chainId       : 'mainnet'
})

// use the API to call a function..
const myBalance = await in3.eth.callFn(myTokenContract, 'balanceOf(address):uint',
↪myAccount)

// ot to send a transaction..
const receipt = await in3.eth.sendTransaction({
  to           : myTokenContract,
  method       : 'transfer(address,uint256)',
  args         : [target,amount],
  confirmations: 2,
  pk           : myKey
})

...
```

1.2 As Docker Container

To start Incubed as a standalone client (allowing other non-JS applications to connect to it), you can start the container as the following:

```
docker run -d -p 8545:8545  slockit/in3:latest -port 8545
```

1.3 C Implementation

The C implementation will be released soon!

```
#include <in3/client.h>    // the core client
#include <in3/eth_api.h>   // wrapper for easier use
#include <in3/eth_basic.h> // use the basic module
#include <in3/in3_curl.h>  // transport implementation

#include <inttypes.h>
#include <stdio.h>

int main(int argc, char* argv[]) {

  // register a chain-verifier for basic Ethereum-Support, which is enough to verify␣
↪blocks
  // this needs to be called only once
  in3_register_eth_basic();

  // use curl as the default for sending out requests
  // this needs to be called only once.
  in3_register_curl();

  // create new incubed client
  in3_t* in3 = in3_new();

  // the b lock we want to get
  uint64_t block_number = 8432424;

  // get the latest block without the transaction details
  eth_block_t* block = eth_getBlockByNumber(in3, block_number, false);

  // if the result is null there was an error an we can get the latest error message␣
↪from eth_lat_error()
  if (!block)
    printf("error getting the block : %s\n", eth_last_error());
  else {
    printf("Number of transactions in Block #%llu: %d\n", block->number, block->tx_
↪count);
    free(block);
  }

  // cleanup client after usage
  in3_free(in3);
}
```

More details coming soon. . .

1.4 Java

The Java implementation uses a wrapper of the C implemenation. This is why you need to make sure the libin3.so, in3.dll, or libin3.dylib can be found in the java.library.path. For example:

```
java -cp in3.jar:. HelloIN3.class
```

```
import java.util.*;
import in3.*;
import in3.eth1.*;
import java.math.BigInteger;

public class HelloIN3 {
  //
  public static void main(String[] args) throws Exception {
    // create incubed
    IN3 in3 = new IN3();

    // configure
    in3.setChainId(0x1); // set it to mainnet (which is also dthe default)

    // read the latest Block including all Transactions.
    Block latestBlock = in3.getEth1API().getBlockByNumber(Block.LATEST, true);

    // Use the getters to retrieve all containing data
    System.out.println("current BlockNumber : " + latestBlock.getNumber());
    System.out.println("minded at : " + new Date(latestBlock.getTimeStamp()) + " by "␣
↪+ latestBlock.getAuthor());

    // get all Transaction of the Block
    Transaction[] transactions = latestBlock.getTransactions();

    BigInteger sum = BigInteger.valueOf(0);
    for (int i = 0; i < transactions.length; i++)
      sum = sum.add(transactions[i].getValue());

    System.out.println("total Value transfered in all Transactions : " + sum + " wei
↪");
  }

}
```

1.5 Command-line Tool

Based on the C implementation, a command-line utility is built, which executes a JSON-RPC request and only delivers the result. This can be used within Bash scripts:

```
CURRENT_BLOCK = `in3 -c kovan eth_blockNumber`

#or to send a transaction

in3 -pk my_key_file.json send -to 0x27a37a1210df14f7e058393d026e2fb53b7cf8c1 -value 0.
↪2eth
```

(continues on next page)

(continued from previous page)

```
in3 -pk my_key_file.json send -to 0x27a37a1210df14f7e058393d026e2fb53b7cf8c1 -gas␣
↪1000000  "registerServer(string,uint256)" "https://in3.slock.it/kovan1" 0xFF
```

1.6 Supported Chains

Currently, Incubed is deployed on the following chains:

1.6.1 Mainnet

Registry-legacy: 0x2736D225f85740f42D17987100dc8d58e9e16252

Registry: 0x64abe24afbba64cae47e3dc3ced0fcab95e4edd5

ChainId: 0x1 (alias `mainnet`)

Status: https://in3.slock.it?n=mainnet

NodeList: https://in3.slock.it/mainnet/nd-3

1.6.2 Kovan

Registry-legacy: 0x27a37a1210df14f7e058393d026e2fb53b7cf8c1

Registry: 0x33f55122c21cc87b539e7003f7ab16229bc3af69

ChainId: 0x2a (alias `kovan`)

Status: https://in3.slock.it?n=kovan

NodeList: https://in3.slock.it/kovan/nd-3

1.6.3 Evan

Registry: 0x85613723dB1Bc29f332A37EeF10b61F8a4225c7e

ChainId: 0x4b1 (alias `evan`)

Status: https://in3.slock.it?n=evan

NodeList: https://in3.slock.it/evan/nd-3

1.6.4 Görli

Registry-legacy: 0x85613723dB1Bc29f332A37EeF10b61F8a4225c7e

Registry: 0xfea298b288d232a256ae0ad5941e5c890b1db691

ChainId: 0x5 (alias `goerli`)

Status: https://in3.slock.it?n=goerli

NodeList: https://in3.slock.it/goerli/nd-3

1.6.5 IPFS

Registry: 0xf0fb87f4757c77ea3416afe87f36acaa0496c7e9

ChainId: 0x7d0 (alias `ipfs`)

Status: https://in3.slock.it?n=ipfs

NodeList: https://in3.slock.it/ipfs/nd-3

1.7 Registering an Incubed Node

If you want to participate in this network and also register a node, you need to send a transaction to the registry contract, calling `registerServer(string _url, uint _props)`.

ABI of the registry:


```
[{"constant":true,"inputs":[],"name":"totalServers","outputs":[{"name":"","type":
↪"uint256"}],"payable":false,"stateMutability":"view","type":"function"},{"constant
↪":false,"inputs":[{"name":"_serverIndex","type":"uint256"},{"name":"_props","type":
↪"uint256"}],"name":"updateServer","outputs":[],"payable":true,"stateMutability":
↪"payable","type":"function"},{"constant":false,"inputs":[{"name":"_url","type":
↪"string"},{"name":"_props","type":"uint256"}],"name":"registerServer","outputs":[],
↪"payable":true,"stateMutability":"payable","type":"function"},{"constant":true,
↪"inputs":[{"name":"","type":"uint256"}],"name":"servers","outputs":[{"name":"url",
↪"type":"string"},{"name":"owner","type":"address"},{"name":"deposit","type":"uint256
↪"},{"name":"props","type":"uint256"},{"name":"unregisterTime","type":"uint128"},{
↪"name":"unregisterDeposit","type":"uint128"},{"name":"unregisterCaller","type":
↪"address"}],"payable":false,"stateMutability":"view","type":"function"},{"constant
↪":false,"inputs":[{"name":"_serverIndex","type":"uint256"}],"name":
↪"cancelUnregisteringServer","outputs":[],"payable":false,"stateMutability":
↪"nonpayable","type":"function"},{"constant":false,"inputs":[{"name":"_serverIndex",
↪"type":"uint256"},{"name":"_blockhash","type":"bytes32"},{"name":"_blocknumber",
↪"type":"uint256"},{"name":"_v","type":"uint8"},{"name":"_r","type":"bytes32"},{"name
↪":"_s","type":"bytes32"}],"name":"convict","outputs":[],"payable":false,
↪"stateMutability":"nonpayable","type":"function"},{"constant":true,"inputs":[{"name
↪":"_serverIndex","type":"uint256"}],"name":"calcUnregisterDeposit","outputs":[{"name
↪":"","type":"uint128"}],"payable":false,"stateMutability":"view","type":"function"},
↪{"constant":false,"inputs":[{"name":"_serverIndex","type":"uint256"}],"name":
↪"confirmUnregisteringServer","outputs":[],"payable":false,"stateMutability":
↪"nonpayable","type":"function"},{"constant":false,"inputs":[{"name":"_serverIndex",
↪"type":"uint256"}],"name":"requestUnregisteringServer","outputs":[],"payable":true,
↪"stateMutability":"payable","type":"function"},{"anonymous":false,"inputs":[{
↪"indexed":false,"name":"url","type":"string"},{"indexed":false,"name":"props","type
↪":"uint256"},{"indexed":false,"name":"owner","type":"address"},{"indexed":false,
↪"name":"deposit","type":"uint256"}],"name":"LogServerRegistered","type":"event"},{
↪"anonymous":false,"inputs":[{"indexed":false,"name":"url","type":"string"},{"indexed
↪":false,"name":"owner","type":"address"},{"indexed":false,"name":"caller","type":
↪"address"}],"name":"LogServerUnregisterRequested","type":"event"},{"anonymous
↪":false,"inputs":[{"indexed":false,"name":"url","type":"string"},{"indexed":false,
↪"name":"owner","type":"address"}],"name":"LogServerUnregisterCanceled","type":"event
↪"},{"anonymous":false,"inputs":[{"indexed":false,"name":"url","type":"string"},{
↪"indexed":false,"name":"owner","type":"address"}],"name":"LogServerConvicted","type
↪":"event"},{"anonymous":false,"inputs":[{"indexed":false,"name":"url","type":"string
↪"},{"indexed":false,"name":"owner","type":"address"}],"name":"LogServerRemoved",
↪"type":"event"}]
```


To run an Incubed node, you simply use docker-compose:

```
version: '2'
services:
  incubed-server:
    image: slockit/in3-server:latest
    volumes:
    - $PWD/keys:/secure                                     # directory where the␣
↪private key is stored
    ports:
    - 8500:8500/tcp                                         # open the port 8500 to␣
↪be accessed by the public
    command:
    - --privateKey=/secure/myKey.json                       # internal path to the key
    - --privateKeyPassphrase=dummy                          # passphrase to unlock␣
↪the key
    - --chain=0x1                                           # chain (Kovan)
    - --rpcUrl=http://incubed-parity:8545                   # URL of the Kovan client
    - --registry=0xFdb0eA8AB08212A1fFfDB35aFacf37C3857083ca # URL of the Incubed␣
↪registry
    - --autoRegistry-url=http://in3.server:8500             # check or register this␣
↪node for this URL
    - --autoRegistry-deposit=2                              # deposit to use when␣
↪registering

  incubed-parity:
    image: slockit/parity-in3:v2.2                          # parity-image with the␣
↪getProof-function implemented
    command:
    - --auto-update=none                                    # do not automatically␣
↪update the client
    - --pruning=archive
    - --pruning-memory=30000                                # limit storage
```

CHAPTER 2

Downloading in3

in3 is divided into two distinct components, the in3-node and in3-client. The in3-node is currently written in typescript, whereas the in3-client has a version in typescript as well as a smaller and more feature packed version written in C.

In order to compile from scratch, please use the sources from our github page or the public gitlab page. Instructions for building from scratch can be found in our documentation.

The in3-server and in3-client has been published in multiple package managers and locations, they can be found here:

	Package manager	Link	Use case
in3-node(ts)	Docker Hub	DockerHub	To run the in3-server, which the in3-client can use to connect to the in3 network
in3-client(ts)	NPM	NPM	To use with js applications
in3-client(C)	Ubuntu Launchpad	Ubuntu	It can be quickly integrated on linux systems, IoT devices or any micro controllers
	Docker Hub	DockerHub	Quick and easy way to get in3 client running
	Brew	Homebrew	Easy to install on MacOS or linux/windows subsystems
	Release page	Github	For directly playing with the binaries/deb/jar/wasm files

2.1 in3-node

2.1.1 Docker Hub

1. Pull the image from docker using `docker pull slockit/in3-node`
2. In order to run your own in3-node, you must first register the node. The information for registering a node can be found here

3. Run the in3-node image using a direct docker command or a docker-compose file, the parameters for which are explained here

2.2 in3-client (ts)

2.2.1 npm

1. Install the package by running `npm install --save in3`
2. `import In3Client from "in3"`
3. View our examples for information on how to use the module

2.3 in3-client(C)

2.3.1 Ubuntu Launchpad

There are 2 packages published to Ubuntu Launchpad: `in3` and `in3-dev`. The package `in3` only installs the binary file and allows you to use in3 via command line. The package `in3-dev` would install the binary as well as the library files, allowing you to use in3 not only via command line, but also inside your C programs by including the statically linked files.

Installation instructions for `in3`:

This package will only install the in3 binary in your system.

1. Add the slock.it ppa to your system with `sudo add-apt-repository ppa:devops-slock-it/in3`
2. Update the local sources `sudo apt-get update`
3. Install in3 with `sudo apt-get install in3`

Installation instructions for `in3-dev`:

This package will install the statically linked library files and the include files in your system.

1. Add the slock.it ppa to your system with `sudo add-apt-repository ppa:devops-slock-it/in3`
2. Update the local sources `sudo apt-get update`
3. Install in3 with `sudo apt-get install in3-dev`

2.3.2 Docker Hub

Usage instructions:

1. Pull the image from docker using `docker pull slockit/in3`
2. Run the client using: `docker run -d -p 8545:8545 slockit/in3:latest --chainId=goerli -port 8545`
3. More parameters and their descriptions can be found here.

2.3.3 Release page

Usage instructions:

1. Navigate to the in3-client release page on this github repo
2. Download the binary that matches your target system, or read below for architecture specific information:

For WASM:

1. Download the WASM binding with `npm install --save in3-wasm`
2. More information on how to use the WASM binding can be found here
3. Examples on how to use the WASM binding can be found here

For C library:

1. Download the C library from the release page or by installing the `in3-dev` package from ubuntu launchpad
2. Include the C library in your code, as shown in our examples
3. Build your code with `gcc -std=c99 -o test test.c -lin3 -lcurl`, more information can be found here

For Java:

1. Download the Java file from the release page
2. Use the java binding as show in our example
3. Build your java project with `javac -cp $IN3_JAR_LOCATION/in3.jar *.java`

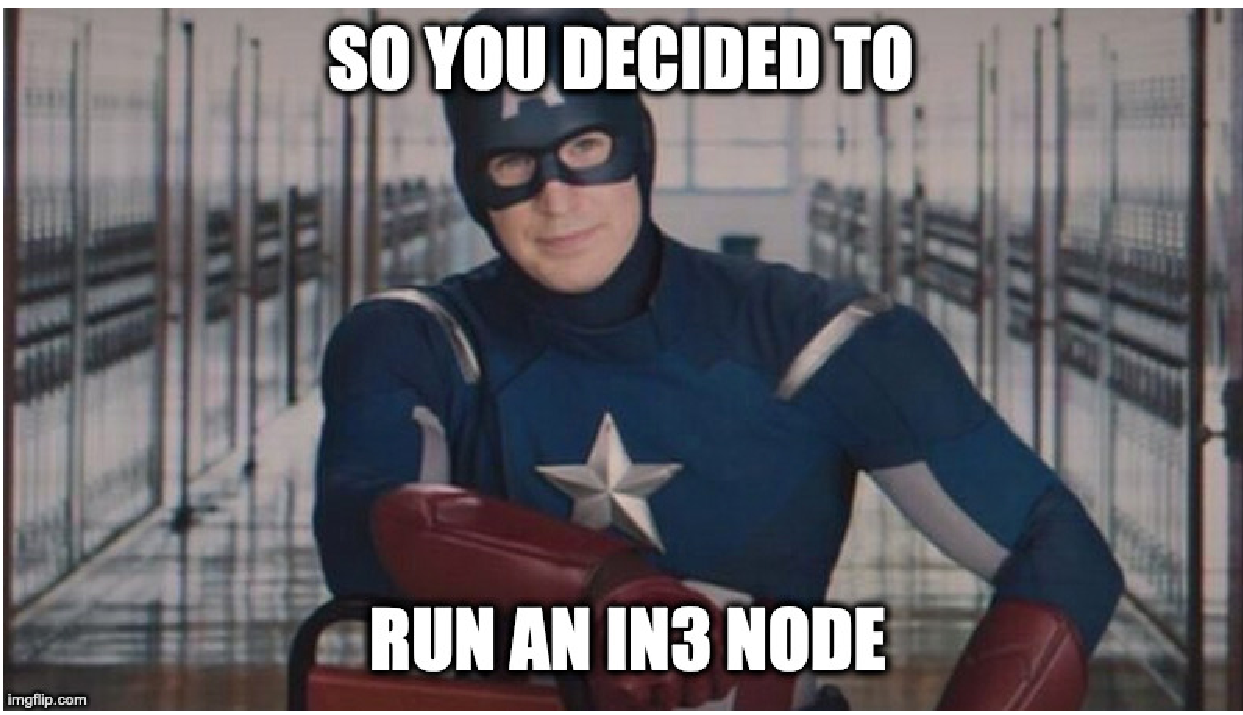
2.3.4 Brew

Usage instructions:

1. Ensure that homebrew is installed on your system
2. Add a brew tap with `brew tap slockit/in3`
3. Install in3 with `brew install in3`
4. You should now be able to use `in3` in the terminal, can be verified with `in3 eth_blockNumber`

CHAPTER 3

Running an in3 node on a VPS



img

Disclaimers: This guide is meant to give you a general idea of the steps needed to run an in3 node on a VPS, please do not take it as a definitive source for all the information. An in3 node is a public facing service that comes with all the associated security implications and complexity. This guide is meant for internal use at this time, once a target audience and depth has been defined, a public version will be made.

That being said, setup of an in3 node requires the following steps:

```
1. Generate a private key and docker-compose file from in3-setup.slock.it
2. Setup a VPS
3. Start the Ethereum RPC node using the docker-compose
```

(continues on next page)

(continued from previous page)

```
4. Assign a DNS domain, static IP (or Dynamic DNS) to the server
5. Run the in3 node docker image with the required flags
6. Register the in3 node with in3-setup.slock.it
```

1. Generate a private key and docker-compose file using in3-setup.slock.it: We will use the in3-setup tool to guide us through the process of starting an incubed node. Begin by filling up the required details, add metadata if you improve our statistics. Choose the required chain and logging level. Choose a secure private key passphrase, it is important to save it in your password manager or somewhere secure, we cannot recover it for you. Click on generate private key, this process takes some time. Download the private key and store it in the secure location.

Once the private key is downloaded, enter your Ethereum node URL in case you already have one. Generate the docker-compose file and save it in the same folder as the private key.

1. Setup a VPS:

A VPS is basically a computer away from home that offers various preselected (usually) Linux distros out of the box. You can then set it up with any service you like - for example Hetzner,Contabo,etc. ServerHunter is a good comparison portal to find a suitable VPS service.The minimum specs required for a server to host both an ethereum RPC node as well as an in3 node would be:

```
4 CPU cores
8GB of Ram
300GB SSD disk space or more
Atleast 5MBit/s up/down
Linux OS, eg: Ubuntu
```

Once the server has been provisioned, look for the IP address,SSH port and username. This information would be used to login,transfer files to the VPS.

Transfer the files to the server using a file browser or an scp command. The target directory for docker-compose.yml and exported-private.key.json file on the incubed server is the /int3 directory The scp command to transfer the files are:

```
scp docker-compose.yml user@ip-address:
scp exported-private-key.json user@ip-address:
```

If you are using windows you should use Winscp. Copy it to your home directory and thean move the files to /int3

Once the files have been transferred, we will SSH into the server with:

```
ssh username@ip-address
```

Now we will install the dependencies required to run in3. This is possible through a one step install script that can be found (here)[https://github.com/slockit/in3-server-setup-tool/blob/master/incubed_dependency_install_script.sh] or by installing each dependency individually.

If you wish to use our dependency install script, please run the following commands in your VPS, then skip to step 4 and setup your domain name:

```
curl -o incubed_dependency_install_script.sh https://raw.githubusercontent.com/
↪slockit/in3-server-setup-tool/master/incubed_dependency_install_script.sh
chmod +x incubed_dependency_install_script.sh
sudo su
./incubed_dependency_install_script.sh
```

If you wish to install each dependency individually, please follow the proceeding steps. Begin by removing older installations of docker:

```
# remove existing docker installations
sudo apt remove docker docker-engine docker.io
```

Make sure you have the necessary packages to allow the use of Docker's repository:

```
# install dependencies
sudo apt install apt-transport-https ca-certificates curl software-properties-common
```

To verify the hashes of the docker images from dockerhub you must add Docker's GPG key:

```
# add the docker gpg key
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
```

Verify the fingerprint of the GPG key, the UID should say "Docker Release":

```
# verify the gpg key
sudo apt-key fingerprint 0EBFCD88
```

Add the stable Docker repository:

```
# add the stable Docker repository
sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu
↪$(lsb_release -cs) stable"
```

Update and install docker-ce:

```
# update the sources
sudo apt update
# install docker-ce
sudo apt install docker-ce
```

Add your limited Linux user account to the docker group:

```
# add your limited Linux user account to the docker group
sudo usermod -aG docker $USER
```

Verify your installation with a hello-world image:

```
docker run hello-world
```

Now we will continue to install docker-compose by downloading it and moving it to the right location:

```
# install docker-compose
sudo curl -L https://github.com/docker/compose/releases/download/1.18.0/docker-
↪compose-`uname -s`-`uname -m` -o /usr/local/bin/docker-compose
```

Set the right permissions:

```
# set the right permissions
sudo chmod +x /usr/local/bin/docker-compose
```

Verify the installation with:

```
docker-compose --version
```

1. Start the Ethereum RPC node using the docker-compose: We will use the downloaded docker-compose file to start the Ethereum RPC node.

Change directory to the created in3 folder, verify that the files exist there and then start parity with:

```
screen
docker-compose up incubed-parity
control+A and control+D to exit from screen
```

The time for the whole sync with parity is nearly 4h. The sync process starts with Block snapshots. After This is ready the block syncing starts. In order to verify the status of the syncing, run:

```
echo $((`curl --data '{"method":"eth_blockNumber","params":[],"id":1,"jsonrpc":"2.0"}
↪' -H "Content-Type: application/json" -X POST 172.15.0.3:8545 | grep -oh "\w*0x\w*
↪"`))
```

That command will return the latest block number, verify that the block number is the latest one by checking on etherscan. We recommend to go forward with Step 4. if sync is completly finished.

1. Run the in3 node docker image with the required flags Once the Ethereum RPC node has been synced, we can proceed with starting the in3-node. This can also be done with the docker-compose file that we used earlier.

```
docker-compose up incubed-server
```

Wait for the in3-server to finish starting, then run the below command to verify the functioning of the in3-server:

```
echo $((`curl --data '{"method":"eth_blockNumber","params":[],"id":1,"jsonrpc":"2.0"}
↪' -H "Content-Type: application/json" -X POST 172.15.0.2:8500 | grep -oh "\w*0x\w*
↪"`))
```

You can now type "exit" to end the SSH session, we should be done with the setup stages in the VPS.

1. Assign a DNS domain, static IP (or Dynamic DNS) to the server You need to register a DNS domain name using cloudflare or some other DNS provider. This Domain name needs to point to your server. A simple way to test it once it is up is with the following command run from your computer:

```
echo $((`curl --data '{"method":"eth_blockNumber","params":[],"id":1,"jsonrpc":"2.0"}
↪' -H "Content-Type: application/json" -X POST Domain-name:80 | grep -oh "\w*0x\w*
↪"`))
```

1. Setup https for your domain

a) Install nginx and certbot and generate certificates.

```
sudo apt-get install certbot nginx
sudo certbot certonly --standalone
# check if automatic renewal of the certificates works as expected
sudo certbot renew --dry-run
```

b) Configure nginx as a reverse proxy using SSL. Replace /etc/nginx/sites/available/default with the following content. (Comment everything else out, also the certbot generated stuff.)

```
server {
        listen 443 default_server;
        server_name Domain-name;
        ssl on;
        ssl_certificate /etc/letsencrypt/live/Domain-name/fullchain.pem;
        ssl_certificate_key /etc/letsencrypt/live/Domain-name/privkey.pem;
        ssl_session_cache shared:SSL:10m;

        location / {
```

(continues on next page)

(continued from previous page)

```
                proxy_pass http://localhost:80;
                proxy_set_header Host $host;

                proxy_redirect http:// https://;
        }
}
```

c) Restart nginx.

```
sudo service nginx restart
```

HTTPS should be working now. Check with:

```
echo $((`curl --data '{"method":"eth_blockNumber","params":[],"id":1,"jsonrpc":"2.0"}
↪' -H "Content-Type: application/json" -X POST Domain-name:443 | grep -oh "\w*0x\w*
↪"`))
```

1. Register the in3 node with in3-setup.slock.it Lastly, we need to head back to in3-setup.slock.it and register our new node. Enter the URL address from which the in3 node can be reached. Add the deposit amount in Ether and click on "Register in3 server" to send the transaction.

3.1 Side notes/ chat summary

1. Redirect HTTP to HTTPS

Using the above config file nginx doesn't listen on port 80, that port is already being listened to by the incubed-server image (see docker-compose file, mapping 80:8500). That way the port is open for normal HTTP requests and when registering the node one can "check" the HTTP capability. If that is unwanted one can append

```
server {
    listen 80;
    return 301 https://$host$request_uri;
}
```

to the nginx config file and change the port mapping for the incubed-server image. One also needs then to adjust the port that nginx redirects to on localhost. For example

```
        ports:
        - 8080:8500/tcp
```

In the incubed-server section in the docker compose file and

```
                proxy_pass http://localhost:8080;
```

in the nginx config. (Port 8080 also has to be closed using the firewall, e.g. `ufw deny 8080`)

1. OOM - Out of memory

If having memory issues while syncing adding some parity flags might help (need to be added in the docker-compose for incubed-parity)

```
    --pruning-history=[NUM]
        Set a minimum number of recent states to keep in memory when pruning is␣
↪active. (default: 64)
```

(continues on next page)

(continued from previous page)

```
    --pruning-memory=[MB]
        The ideal amount of memory in megabytes to use to store recent states. As␣
↪many states as possible will be kept
        within this limit, and at least --pruning-history states will always be kept.␣
↪(default: 32)
```

with appropiate values. Note that inside the docker compose file pruning-memory is set to 30000, which might exceed your RAM!

1. Saving the chaindb on disk using docker volume

To prevent the chaindb data being lost add

```
        volumes:
        - /wherever-you-want-to-store-data/:/home/parity/.local/share/io.parity.
↪ethereum/
```

to the parity section in the docker compose file.

1. Added stability/ speed while syncing

Exposing the port 30303 to the public will prevent parity having to rely on UPnP for node discovery. For this add

```
        ports:
        - 30303:30303
        - 30303:30303/udp
```

to the parity section in the docker compose file.

Increasing the database, state and queuing cache can improve the syncing speed (default is around 200MB). The needed flag for it is:

```
    --cache-size=[MB]
        Set total amount of discretionary memory to use for the entire system,␣
↪overrides other cache and queue options.
```

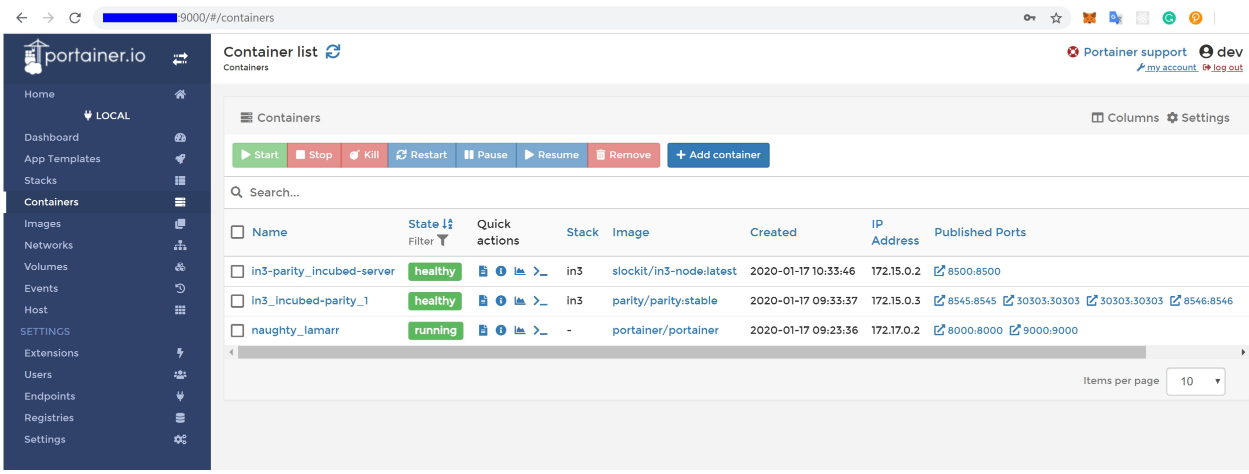
1. If you like a UI to manage and check your docker containers, please have a look at Portainer.io

Installation instructions can be found here: https://www.portainer.io/installation/.

It can be run with docker, using:

```
sudo docker run -d --restart always -p 8000:8000 -p 9000:9000 -v /var/run/docker.
↪sock:/var/run/docker.sock -v portainer_data:/data portainer/portainer
```

After the setup, it will be availabe on port 9000. The enabled WebGUI looks like the below picture:



img

3.2 Recommendations

1. Disable SSH `PasswordAuthentication` & `RootLogin` and install `fail2ban` to protect your VPS from unauthorized access and brute-force attacks. See How To Configure SSH Key-Based Authentication on a Linux Server and How To Protect SSH with Fail2Ban.

CHAPTER 4

IN3-Protocol

This document describes the communication between a Incubed client and a Incubed node. This communication is based on requests that use extended JSON-RPC-Format. Especially for ethereum-based requests, this means each node also accepts all standard requests as defined at Ethereum JSON-RPC, which also includes handling Bulk-requests.

Each request may add an optional `in3` property defining the verification behavior for Incubed.

4.1 Incubed Requests

Requests without an `in3` property will also get a response without `in3`. This allows any Incubed node to also act as a raw ethereum JSON-RPC endpoint. The `in3` property in the request is defined as the following:

- **chainId** `string<hex>` - The requested *chainId*. This property is optional, but should always be specified in case a node may support multiple chains. In this case, the default of the node would be used, which may end up in an undefined behavior since the client cannot know the default.
- **includeCode** `boolean` - Applies only for `eth_call`-requests. If true, the request should include the codes of all accounts. Otherwise only the the codeHash is returned. In this case, the client may ask by calling eth_getCode() afterwards.
- **verifiedHashes** `string<bytes32>[]` - If the client sends an array of blockhashes, the server will not deliver any signatures or blockheaders for these blocks, but only return a string with a number. This allows the client to skip requiring signed blockhashes for blocks already verified.
- **latestBlock** `integer` - If specified, the blocknumber `latest` will be replaced by a blockNumber-specified value. This allows the Incubed client to define finality for PoW-Chains, which is important, since the `latest`-block cannot be considered final and therefore it would be unlikely to find nodes willing to sign a blockhash for such a block.
- **useRef** `boolean` - If true, binary-data (starting with a 0x) will be referred if occurring again. This decreases the payload especially for recurring data such as merkle proofs. If supported, the server (and client) will keep track of each binary value storing them in a temporary array. If the previously used value is used again, the server replaces it with `:<index>`. The client then resolves such refs by lookups in the temporary array.

- **useBinary** `boolean` - If true, binary-data will be used. This format is optimzed for embedded devices and reduces the payload to about 30%. For details see *the Binary-spec*.
- **useFullProof** `boolean` - If true, all data in the response will be proven, which leads to a higher payload. The result depends on the method called and will be specified there.
- **finality** `number` - For PoA-Chains, it will deliver additional proof to reach finality. If given, the server will deliver the blockheaders of the following blocks until at least the number in percent of the validators is reached.
- **verification** `string` - Defines the kind of proof the client is asking for. Must be one of the these values:
  - `'never`' : No proof will be delivered (default). Also no `in3`-property will be added to the response, but only the raw JSON-RPC response will be returned.
  - `'proof`' : The proof will be created including a blockheader, but without any signed blockhashes.
- **whiteList** `address` - If specified, the incubed server will respond with `lastWhiteList`, which will indicate the last block number of whitelist contract event.
- **signers** `string<address>[]` - A list of addresses (as 20bytes in hex) requested to sign the blockhash.

A example of an Incubed request may look like this:

```
{
    "jsonrpc": "2.0",
    "id": 2,
    "method": "eth_getTransactionByHash",
    "params": ["0xf84cfb78971ebd940d7e4375b077244e93db2c3f88443bb93c561812cfed055c"],
    "in3": {
        "chainId": "0x1",
        "verification": "proof",
        "whiteList": "0x08e97ef0a92EB502a1D7574913E2a6636BeC557b",
        "signers":["0x784bfa9eb182C3a02DbeB5285e3dBa92d717E07a"]
  }
}
```

4.2 Incubed Responses

Each Incubed node response is based on JSON-RPC, but also adds the `in3` property. If the request does not contain a `in3` property or does not require proof, the response must also omit the `in3` property.

If the proof is requested, the `in3` property is defined with the following properties:

- **proof** *Proof* - The Proof-data, which depends on the requested method. For more details, see the *Proofs* section.
- **lastNodeList** `number` - The blocknumber for the last block updating the nodeList. This blocknumber should be used to indicate changes in the nodeList. If the client has a smaller blocknumber, it should update the nodeList.
- **lastValidatorChange** `number` - The blocknumber of the last change of the validatorList (only for PoA-chains). If the client has a smaller number, it needs to update the validatorlist first. For details, see *PoA Validations*
- **lastWhiteList** `number` - The blocknumber for the last block updating the whitelist nodes in whitelist contract. This blocknumber could be used to detect if there is any change in whitelist nodes. If the client has a smaller blocknumber, it should update the white list.
- **currentBlock** `number` - The current blocknumber. This number may be stored in the client in order to run sanity checks for `latest` blocks or `eth_blockNumber`, since they cannot be verified directly.

An example of such a response would look like this:

```
{
  "jsonrpc": "2.0",
  "result": {
    "blockHash": "0x2dbbac3abe47a1d0a7843d378fe3b8701ca7892f530fd1d2b13a46b202af4297",
    "blockNumber": "0x79fab6",
    "chainId": "0x1",
    "condition": null,
    "creates": null,
    "from": "0x2c5811cb45ba9387f2e7c227193ad10014960bfc",
    "gas": "0x186a0",
    "gasPrice": "0x4a817c800",
    "hash": "0xf84cfb78971ebd940d7e4375b077244e93db2c3f88443bb93c561812cfed055c",
    "input":
↪"0xa9059cbb000000000000000000000000290648fc6f2cb27a2a81dc35a429090872991b920000000000000000000000000
↪",
    "nonce": "0xa8",
    "publicKey":
↪"0x6b30c392dda89d58866bf2c1bedf8229d12c6ae3589d82d0f52ae588838a475aacda64775b7a1b376935d732bb80226
↪",
    "r": "0x4666976b528fc7802edd9330b935c7d48fce0144ce97ade8236da29878c1aa96",
    "raw":
↪"0xf8ab81a88504a817c800830186a094d3ebdaea9aeac98de723f640bce4aa07e2e4419280b844a9059cbb00000000000
↪",
    "s": "0x5089dca7ecf7b061bec3cca7726aab1fcb4c8beb51517886f91c9b0ca710b09d",
    "standardV": "0x0",
    "to": "0xd3ebdaea9aeac98de723f640bce4aa07e2e44192",
    "transactionIndex": "0x3e",
    "v": "0x25",
    "value": "0x0"
  },
  "id": 2,
  "in3": {
    "proof": {
      "type": "transactionProof",
      "block":
↪"0xf90219a03d050deecd980b16cad9752133333ccdface463cc69e784f32dd981e2e751e34a01dcc4de8dec75d7aab85b5
↪",
      "merkleProof": [

↪"0xf90131a00150ff50e29f3df34b89870f183c85a82a73f21722d7e6c787e663159f165010a0b8c56f207a223067c7ae5c
↪",

↪"0xf90211a0f4a5e4a1197190f910e4a026f50bd6a169716b52be42c99ddb043ad9b4da6117a09ad1def70dd1d991331d01
↪",

↪"0xf8b020b8adf8ab81a88504a817c800830186a094d3ebdaea9aeac98de723f640bce4aa07e2e4419280b844a9059cbb00
↪"
      ],
      "txIndex": 62,
      "signatures": [
        {
          "blockHash":
↪"0x2dbbac3abe47a1d0a7843d378fe3b8701ca7892f530fd1d2b13a46b202af4297",
          "block": 7994038,
          "r": "0xef73a527ae8d38b595437e6436bd4fa037d50550bf3840ad0cd3c6ca641a951e",
          "s": "0x6a5815db16c12b890347d42c014d19b60e1605d2e8e64b729f89e662f9ce706b",
          "v": 27,
```


(continues on next page)

(continued from previous page)


```
          "msgHash":
↪"0xa8fc6e2564e496efc5fd7db8e70f03fd50af53e092f47c98329c84c96026fdff"
        }
      ]
    },
    "currentBlock": 7994124,
    "lastValidatorChange": 0,
    "lastNodeList": 6619795,
    "lastWhiteList": 1546354
  }
}
```


4.3 ChainId

Incubed supports multiple chains and a client may even run requests to different chains in parallel. While, in most cases, a chain refers to a specific running blockchain, chainIds may also refer to abstract networks such as ipfs. So, the definition of a chain in the context of Incubed is simply a distributed data domain offering verifiable api-functions implemented in an in3-node.

Each chain is identified by a `uint64` identifier written as hex-value (without leading zeros). Since incubed started with ethereum, the chainIds for public ethereum-chains are based on the intrinsic chainId of the ethereum-chain. See https://chainid.network.

For each chain, Incubed manages a list of nodes as stored in the *server registry* and a chainspec describing the verification. These chainspecs are held in the client, as they specify the rules about how responses may be validated.

4.4 Registry

As Incubed aims for fully decentralized access to the blockchain, the registry is implemented as an ethereum smart contract.

This contract serves different purposes. Primarily, it manages all the Incubed nodes, both the onboarding and also unregistering process. In order to do so, it must also manage the deposits: reverting when the amount of provided ether is smaller than the current minimum deposit; but also locking and/or sending back deposits after a server leaves the in3-network.

In addition, the contract is also used to secure the in3-network by providing functions to "convict" servers that provided a wrongly signed block, and also having a function to vote out inactive servers.

4.4.1 Register and Unregister of nodes

Register

There are two ways of registering a new node in the registry: either calling `registerNode()` or by calling `registerNodeFor()`. Both functions share some common parameters that have to be provided:

- `url` the url of the to be registered node
- `props` the properties of the node
- `weight` the amount of requests per second the node is capable of handling
- `deposit` the deposit of the node in ERC20 tokens.

Those described parameters are sufficient when calling `registerNode()` and will register a new node in the registry with the sender of the transaction as the owner. However, if the designated signer and the owner should use different keys, `registerNodeFor()` has to be called. In addition to the already described parameters, this function also needs a certain signature (i.e. `v`, `r`, `s`). This signature has to be created by hashing the url, the properties, the weight and the designated owner (i.e. `keccack256(url,properties,weight,owner)`) and signing it with the privateKey of the signer. After this has been done, the owner then can call `registerNodeFor()` and register the node.

However, in order for the register to succeed, at least the correct amount of deposit has to be approved by the designated owner of the node. The supported token can be received by calling `supportedToken()` the registry contract. The same approach also applied to the minimal amount of tokens needed for registering by calling `minDeposit()`.

In addition to that, during the first year after deployment there is also a maximum deposit for each node. This can be received by calling `maxDepositFirstYear()`. Providing a deposit greater then this will result in a failure when trying to register.

Unregister a node

In order to remove a node from the registry, the function `unregisteringNode()` can be used, but is only callable by the owner the node.

While after a successful call the node will be removed from the nodeList immediately, the deposit of the former node will still be locked for the next 40 days after this function had been called. After the timeout is over, the function `returnDeposit()` can be called in order to get the deposit back. The reason for that decision is simple: this approach makes sure that there is enough time to convict a malicious node even after he unregistered his node.

4.4.2 Convicting a node

After a malicious node signed a wrong blockhash, he can be convicted resulting in him loosing the whole deposit while the caller receives 50% of the deposit. There are two steps needed for the process to succeed: calling `convict()` and `revealConvict()`.

calling convict

The first step for convicting a malicious node is calling the `convict()`-function. This function will store a specific hash within the smart contract.

The hash needed for convicting requires some parameters:

- `blockhash` the wrongly blockhash that got signed the by malicious node
- `sender` the account that sends this transaction
- `v` v of the signature of the wrong block
- `r` r of the signature of the wrong block
- `s` s of the signature of the wrong block

All those values are getting hashed (`keccack256(blockhash,sender,v,r,s)` and are stored within the smart contract.

calling revealConvcit

This function requires that at least 2 blocks have passed since `convict()` was called. This mechanic reduces the risks of successful frontrunning attacks.

In addition, there are more requirements for successfully convicting a malicious node:

- the blocknumber of the wrongly signed block has to be either within the latest 256 blocks or be stored within the BlockhashRegistry.
- the malicious node provided a signature for the wong block and it was signed by the node
- the specific hash of the convict-call can be recreated (i.e. the caller provided the very same parameters again)
- the malicious node is either currently active or did not withdraw his deposit yet

If the `revealConvict()`-call passes, the malicious node will be removed immediately from the nodeList. As a reward for finding a malicious node the caller receives 50% of the deposit of the malicious node. The remaining 50% will stay within the nodeRegistry, but nobody will be able to access/transfer them anymore.

recreating blockheaders

When a malicious node returns a block that is not within the latest 256 blocks, the BlockhashRegistry has to be used.

There are different functions to store a blockhash and its number in the registry:

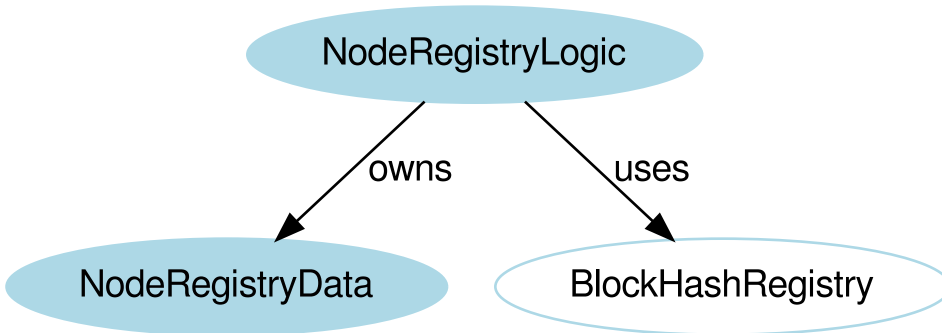
- `snapshot` stores the blockhash and its number of the previous block
- `saveBlockNumber` stores a blockhash and its number from the latest 256 blocks
- `recreateBlockheaders` starts from an already stored block and recreates a chain of blocks. Stores the last block at the end.

In order to reduce the costs of convicting, both `snapshot` and `saveBlockNumber` are the cheapest options, but are limited to the latest 256 blocks.

Recreating a chain of blocks is way more expensive, but is provides the possibility to recreate way older blocks. It requires the blocknumber of an already stored hash in the smart contract as first parameter. As a second parameter an array of serialized blockheaders have to be provided. This array has to start with the blockheader of the stored block and then the previous blockheaders in reverse order (e.g. `100`,`99`,`98`). The smart contract will try to recreate the chain by comparing both the provided (hashed) headers with the calculated parent and also by comparing the extracted blocknumber with the calculated one. After the smart contracts successfully recreates the provided chain, the blockhash of the last element gets stored within the smart contract.

4.4.3 Updating the NodeRegistry

In ethereum the deployed code of an already existing smart contract cannot be changed. This means, that as soon as the Registry smart contract gets updated, the address would change which would result in changing the address of the smart contract containing the nodeList in each client and device.



In order to solve this issue, the registry is divided between two different deployed smart contracts:

- `NodeRegistryData`: a smart contract to store the nodeList
- `NodeRegistryLogic`: a smart contract that has the logic needed to run the registry

There is a special relationship between those two smart contracts: The NodeRegistryLogic "owns" the NodeRegistryData. This means, that only he is allowed to call certain functions of the NodeRegistryData. In our case this means all writing operations, i.e. he is the only entity that is allowed to actually be allowed to store data within the smart contract. We are using this approach to make sure that only the NodeRegistryLogic can call the register, update and remove functions of the NodeRegistryData. In addition, he is the only one allowed to change the ownership to a new contract. Doing so results in the old NodeRegistryLogic to lose write access.

In the NodeRegistryLogic there are 2 special parameters for the update process:

- `updateTimeout`: a timestamp that defines when it's possible to update the registry to the new contract
- `pendingNewLogic`: the address of the already deployed new NodeRegistryLogic contract for the updated registry

When an update of the Registry is needed, the function `adminUpdateLogic` gets called by the owner of the NodeRegistryLogic. This function will set the address of the new pending contract and also set a timeout of 47 days until the new logic can be applied to the NodeRegistryData contract. After 47 days everyone is allowed to call `activateNewLogic` resulting in an update of the registry.

The timeout of accessing the deposit of a node after removing it from the nodeList is only 40 days. In case a node owner dislikes the pending registry, he has 7 days to unregister in order to be able to get his deposit back before the new update can be applied.

4.4.4 Node structure

Each Incubed node must be registered in the NodeRegistry in order to be known to the network. A node or server is defined as:

- **url** `string` - The public url of the node, which must accept JSON-RPC requests.
- **owner** `address` - The owner of the node with the permission to edit or remove the node.
- **signer** `address` - The address used when signing blockhashes. This address must be unique within the nodeList.

- **timeout** `uint64` - Timeout after which the owner is allowed to receive its stored deposit. This information is also important for the client, since an invalid blockhash-signature can only "convict" as long as the server is registered. A long timeout may provide higher security since the node can not lie and unregister right away.
- **deposit** `uint256` - The deposit stored for the node, which the node will lose if it signs a wrong blockhash.
- **props** `uint192` - A bitmask defining the capabilities of the node:
  - **proof** (`0x01`) : The node is able to deliver proof. If not set, it may only serve pure ethereum JSON/RPC. Thus, simple remote nodes may also be registered as Incubed nodes.
  - **multichain** (`0x02`) : The same RPC endpoint may also accept requests for different chains. if this is set the `chainId`-prop in the request in required.
  - **archive** (`0x04`) : If set, the node is able to support archive requests returning older states. If not, only a pruned node is running.
  - **http** (`0x08`) : If set, the node will also serve requests on standard http even if the url specifies https. This is relevant for small embedded devices trying to save resources by not having to run the TLS.
  - **binary** (`0x10`) : If set, the node accepts request with `binary:true`. This reduces the payload to about 30% for embedded devices.
  - **onion** (`0x20`) : If set, the node is reachable through onionrouting and url will be a onion url.
  - **signer** (`0x40`) : If set, the node will sign blockhashes.
  - **data** (`0x80`) : If set, the node will provide rpc responses (at least without proof).
  - **stats** (`0x100`) : If set, the node will provide and endpoint for delivering metrics, which is usually the `/metrics`- endpoint, which can be used by prometheus to fetch statistics.
  - **minBlockHeight** (`0x0100000000` - `0xFF00000000`): : The min number of blocks this node is willing to sign. if this number is low (like <6) the risk of signing unindentially a wrong blockhash because of reorgs is high. The default should be 10)

    ```
    minBlockHeight = props >> 32 & 0xFF
    ```

  More capabilities will be added in future versions.
- **unregisterTime** `uint64` - The earliest timestamp when the node can unregister itself by calling `confirmUnregisteringServer`. This will only be set after the node requests an unregister. The client nodes with an `unregisterTime` set have less trust, since they will not be able to convict after this timestamp.
- **registerTime** `uint64` - The timestamp, when the server was registered.
- **weight** `uint64` - The number of parallel requests this node may accept. A higher number indicates a stronger node, which will be used within the incentivization layer to calculate the score.

4.5 Binary Format

Since Incubed is optimized for embedded devices, a server can not only support JSON, but a special binary-format. You may wonder why we don't want to use any existing binary serialization for JSON like CBOR or others. The reason is simply: because we do not need to support all the features JSON offers. The following features are not supported:

- no escape sequences (this allows use of the string without copying it)
- no float support (at least for now)
- no string literals starting with `0x` since this is always considered as hexcoded bytes

- no propertyNames within the same object with the same key hash

Since we are able to accept these restrictions, we can keep the JSON-parser simple. This binary-format is highly optimized for small devices and will reduce the payload to about 30%. This is achieved with the following optimizations:

- All strings starting with `0x`are interpreted as binary data and stored as such, which reduces the size of the data to 50%.
- Recurring byte-values will use references to previous data, which reduces the payload, especially for merkle proofs.
- All propertyNames of JSON-objects are hashed to a 16bit-value, reducing the size of the data to a signifivant amount (depending on the propertyName).

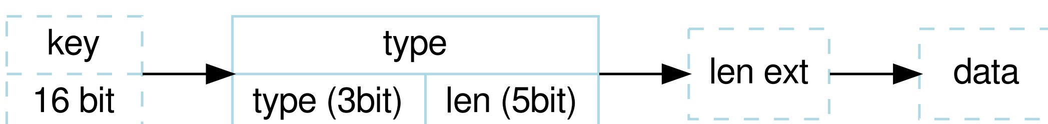
  The hash is calculated very easily like this:

```
static d_key_t key(const char* c) {
  uint16_t val = 0, l = strlen(c);
  for (; l; l--, c++) val ^= *c | val << 7;
  return val;
}
```

Note: A very important limitation is the fact that property names are stored as 16bit hashes, which decreases the payload, but does not allow for the restoration of the full json without knowing all property names!

The binary format is based on JSON-structure, but uses a RLP-encoding approach. Each node or value is represented by these four values:

- **key** `uint16_t` - The key hash of the property. This value will only pass before the property node if the structure is a property of a JSON-object.
- **type** `d_type_t` - 3 bit : defining the type of the element.
- **len** `uint32_t` - 5 bit : the length of the data (for bytes/string/array/object). For (boolean or integer) the length will specify the value.
- **data** `bytes_t` - The bytes or value of the node (only for strings or bytes).



The serialization depends on the type, which is defined in the first 3 bits of the first byte of the element:

```
d_type_t type = *val >> 5;     // first 3 bits define the type
uint8_t  len  = *val & 0x1F;   // the other 5 bits  (0-31) the length
```

The `len` depends on the size of the data. So, the last 5 bit of the first bytes are interpreted as follows:

- `0x00` - `0x1c` : The length is taken as is from the 5 bits.
- `0x1d` - `0x1f` : The length is taken by reading the big-endian value of the next `len - 0x1c` bytes (len ext).

After the type-byte and optional length bytes, the 2 bytes representing the property hash is added, but only if the element is a property of a JSON-object.

Depending on these types, the length will be used to read the next bytes:

- `0x0` : **binary data** - This would be a value or property with binary data. The `len` will be used to read the number of bytes as binary data.
- `0x1` : **string data** - This would be a value or property with string data. The `len` will be used to read the number of bytes (+1) as string. The string will always be null-terminated, since it will allow small devices to use the data directly instead of copying memory in RAM.
- `0x2` : **array** - Represents an array node, where the `len` represents the number of elements in the array. The array elements will be added right after the array-node.
- `0x3` : **object** - A JSON-object with `len` properties coming next. In this case the properties following this element will have a leading `key` specified.
- `0x4` : **boolean** - Boolean value where `len` must be either `0x1`= `true` or `0x0` = `false`. If `len > 1` this element is a copy of a previous node and may reference the same data. The index of the source node will then be `len-2`.
- `0x5` : **integer** - An integer-value with max 29 bit (since the 3 bits are used for the type). If the value is higher than `0x20000000`, it will be stored as binary data.
- `0x6` : **null** - Represents a null-value. If this value has a `len`> 0 it will indicate the beginning of data, where `len` will be used to specify the number of elements to follow. This is optional, but helps small devices to allocate the right amount of memory.

4.6 Communication

Incubed requests follow a simple request/response schema allowing even devices with a small bandwith to retrieve all the required data with one request. But there are exceptions when additional data need to be fetched.

These are:

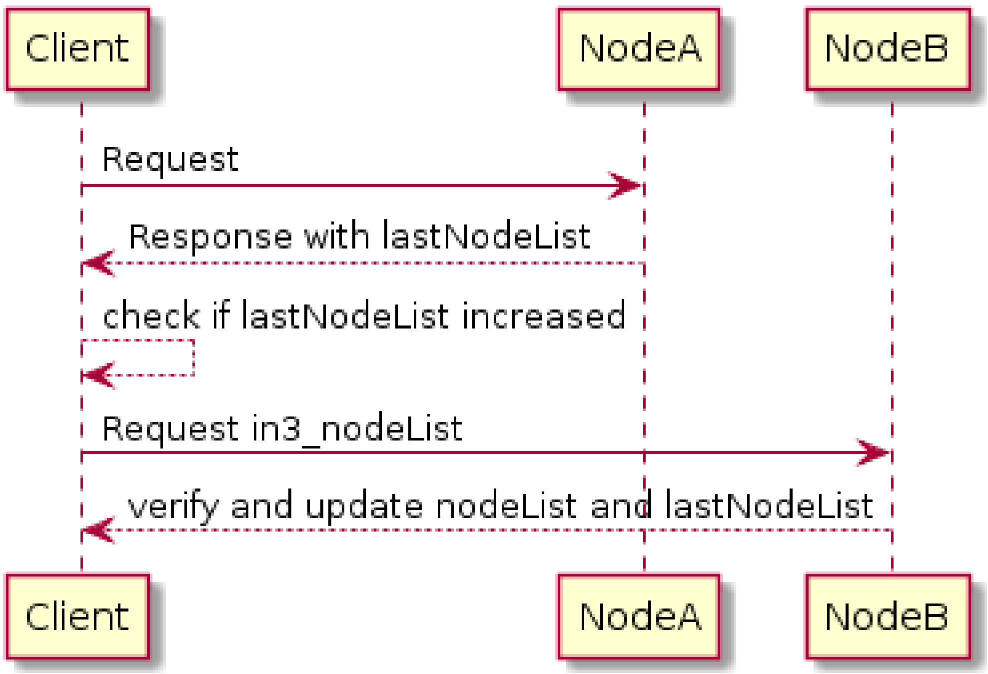
1. **Changes in the NodeRegistry**

   Changes in the NodeRegistry are based on one of the following events:

   - `LogNodeRegistered`
   - `LogNodeRemoved`
   - `LogNodeChanged`

   The server needs to watch for events from the `NodeRegistry` contract, and update the nodeList when needed.

   Changes are detected by the client by comparing the blocknumber of the latest change with the last known blocknumber. Since each response will include the `lastNodeList`, a client may detect this change after receiving the data. The client is then expected to call `in3_nodeList` to update its nodeList before sending out the next request. In the event that the node is not able to proof the new nodeList, the client may blacklist such a node.



1. **Changes in the ValidatorList**

   This only applies to PoA-chains where the client needs a defined and verified validatorList. Depending on the consensus, changes in the validatorList must be detected by the node and indicated with the `lastValidatorChange` on each response. This `lastValidatorChange` holds the last blocknumber of a change in the validatorList.

   Changes are detected by the client by comparing the blocknumber of the latest change with the last known blocknumber. Since each response will include the `lastValidatorChange` a client may detect this change after receiving the data or in case of an unverifiable response. The client is then expected to call `in3_validatorList` to update its list before sending out the next request. In the event that the node is not able to proof the new nodeList, the client may blacklist such a node.

2. **Failover**

   It is also good to have a second request in the event that a valid response is not delivered. This could happen if a node does not respond at all or the response cannot be validated. In both cases, the client may blacklist the node for a while and send the same request to another node.

4.7 RPC Specification

This section describes the behavior for each RPC-method.

4.7.1 Incubed

There are also some Incubed specific rpc-methods, which will help the clients to bootstrap and update the nodeLists.

in3_nodeList

return the list of all registered nodes.

Parameters:

all parameters are optional, but if given a partial NodeList may be returned.

1. `limit`: number - if the number is defined and >0 this method will return a partial nodeList limited to the given number.
2. `seed`: hex - This 32byte hex integer is used to calculate the indexes of the partial nodeList. It is expected to be a random value choosen by the client in order to make the result deterministic.
3. `addresses`: address[] - a optional array of addresses of signers the nodeList must include.

Returns:

an object with the following properties:

- `nodes`: Node[] - a array of node-values. Each Object has the following properties:
  - `url` : string - the url of the node. Currently only http/https is supported, but in the future this may even support onion-routing or any other protocols.
  - `address` : address - the address of the signer
  - `index`: number - the index within the nodeList of the contract
  - `deposit`: string - the stored deposit
  - `props`: string - the bitset of capabilities as described in the *Node Structure*
  - `timeout`: string - the time in seconds describing how long the deposit would be locked when trying to unregister a node.
  - `registerTime` : string - unix timestamp in seconds when the node has registered.
  - `weight` : string - the weight of a node (not used yet) describing the amount of request-points it can handle per second.
  - `proofHash`: hex - a hash value containing the above values. This hash is explicitly stored in the contract, which enables the client to have only one merkle proof per node instead of verifying each property as its own storage value. The proof hash is build :

```
return keccak256(
    abi.encodePacked(
        _node.deposit,
        _node.timeout,
        _node.registerTime,
        _node.props,
        _node.signer,
        _node.url
    )
);
```

- `contract` : address - the address of the Incubed-storage-contract. The client may use this information to verify that we are talking about the same contract or throw an exception otherwise.
- `registryId`: hex - the registryId (32 bytes) of the contract, which is there to verify the correct contract.
- `lastBlockNumber` : number - the blockNumber of the last change of the list (usually the last event).
- `totalServer` : number - the total numbers of nodes.

if proof is requested, the proof will have the type `accountProof`. In the proof-section only the storage-keys of the `proofHash` will be included. The required storage keys are calcualted :

- `0x00` - the length of the nodeList or total numbers of nodes.

- `0x01` - the registryId
- per node : `0x290decd9548b62a8d60345a988386fc84ba6bc95484008f6362f93160ef3e563 + index * 5 + 4`

The blockNumber of the proof must be the latest final block (`latest`- minBlockHeight) and always greater or equal to the `lastBlockNumber`

This proof section contains the following properties:

- `type` : constant : `accountProof`
- `block` : the serialized blockheader of the latest final block
- `signatures` : a array of signatures from the signers (if requested) of the above block.
- `accounts`: a Object with the addresses of the db-contract as key and Proof as value. The Data Structure of the Proof is exactly the same as the result of - `eth_getProof`, but it must containi the above described keys
- `finalityBlocks`: a array of blockHeaders which were mined after the requested block. The number of blocks depends on the request-property `finality`. If this is not specified, this property will not be defined.

Request:

```
{
  "method":"in3_nodeList",
  "params":[2,"0xe9c15c3b26342e3287bb069e433de48ac3fa4ddd32a31b48e426d19d761d7e9b",
↪[]],
  "in3":{
    "verification":"proof"
  }
}
```

Response:

```
{
  "id": 1,
  "result": {
    "totalServers": 5,
    "contract": "0x64abe24afbba64cae47e3dc3ced0fcab95e4edd5",
    "lastBlockNumber": 8669495,
    "nodes": [
      {
        "url": "https://in3-v2.slock.it/mainnet/nd-3",
        "address": "0x945F75c0408C0026a3CD204d36f5e47745182fd4",
        "index": 2,
        "deposit": "10000000000000000",
        "props": "29",
        "chainIds": [
          "0x1"
        ],
        "timeout": "3600",
        "registerTime": "1570109570",
        "weight": "2000",
        "proofHash": "27ffb9b7dc2c5f800c13731e7c1e43fb438928dd5d69aaa8159c21fb13180a4c
↪"
      },
      {
        "url": "https://in3-v2.slock.it/mainnet/nd-5",
        "address": "0xbcdF4E3e90cc7288b578329efd7bcC90655148d2",
        "index": 4,
```

(continues on next page)

(continued from previous page)


```
        "deposit": "10000000000000000",
        "props": "29",
        "chainIds": [
          "0x1"
        ],
        "timeout": "3600",
        "registerTime": "1570109690",
        "weight": "2000",
        "proofHash": "d0dbb6f1e28a8b90761b973e678cf8ecd6b5b3a9d61fb9797d187be011ee9ec7
↪"
      }
    ],
    "registryId": "0x423dd84f33a44f60e5d58090dcdcc1c047f57be895415822f211b8cd1fd692e3"
  },
  "in3": {
    "proof": {
      "type": "accountProof",
      "block": "0xf9021ca01...",
      "accounts": {
        "0x64abe24afbba64cae47e3dc3ced0fcab95e4edd5": {
          "accountProof": [
            "0xf90211a0e822...",
            "0xf90211a0f6d0...",
            "0xf90211a04d7b...",
            "0xf90211a0e749...",
            "0xf90211a059cb...",
            "0xf90211a0568f...",
            "0xf8d1a0ac2433...",
            "0xf86d9d33b981..."
          ],
          "address": "0x64abe24afbba64cae47e3dc3ced0fcab95e4edd5",
          "balance": "0xb1a2bc2ec50000",
          "codeHash":
↪"0x18e64869905158477a607a68e9c0074d78f56a9dd5665a5254f456f89d5be398",
          "nonce": "0x1",
          "storageHash":
↪"0x4386ec93bd665ea07d7ed488e8b495b362a31dc4100cf762b22f4346ee925d1f",
          "storageProof": [
            {
              "key": "0x0",
              "proof": [
                "0xf90211a0ccb6d2d5786...",
                "0xf871808080808080800...",
                "0xe2a0200decd9548b62a...05"
              ],
              "value": "0x5"
            },
            {
              "key": "0x1",
              "proof": [
                "0xf90211a0ccb6d2d5786...",
                "0xf89180a010806a37911...",
                "0xf843a0200e2d5276120...
↪423dd84f33a44f60e5d58090dcdcc1c047f57be895415822f211b8cd1fd692e3"
              ],
              "value":
↪"0x423dd84f33a44f60e5d58090dcdcc1c047f57be895415822f211b8cd1fd692e3"
```


(continues on next page)

(continued from previous page)


```
          },
          {
            "key":
↪"0x290decd9548b62a8d60345a988386fc84ba6bc95484008f6362f93160ef3e571",
            "proof": [
              "0xf90211a0ccb6d2d...",
              "0xf871a08b9ff91d8...",
              "0xf843a0206695c25...
↪27ffb9b7dc2c5f800c13731e7c1e43fb438928dd5d69aaa8159c21fb13180a4c"
            ],
            "value":
↪"0x27ffb9b7dc2c5f800c13731e7c1e43fb438928dd5d69aaa8159c21fb13180a4c"
          },
          {
            "key":
↪"0x290decd9548b62a8d60345a988386fc84ba6bc95484008f6362f93160ef3e57b",
            "proof": [
              "0xf90211a0ccb6d2d1...",
              "0xf851a06807310abd...",
              "0xf843a0204d807394...
↪0d0dbb6f1e28a8b90761b973e678cf8ecd6b5b3a9d61fb9797d187be011ee9ec7"
            ],
            "value":
↪"0xd0dbb6f1e28a8b90761b973e678cf8ecd6b5b3a9d61fb9797d187be011ee9ec7"
          }
        ]
      }
    }
  }
 }
}
```


Partial NodeLists

if the client requests a partial nodeList and the given limit is smaller then the total amount of nodes, the server needs to pick nodes in a deterministic way. This is done by using the given seed.

1. add all required addresses (if any) to the list.
2. iterate over the indexes until the limit is reached:

```
function createIndexes(total: number, limit: number, seed: Buffer): number[] {
  const result: number[] = []              // the result as a list of indexes
  let step = seed.readUIntBE(0, 6)         // first 6 bytes define the step size
  let pos  = seed.readUIntBE(6, 6) % total // next 6 bytes define the offset
  while (result.length < limit) {
    if (result.indexOf(pos) >= 0) {        // if the index is already part of the␣
↪result
      seed = keccak256(seed)               // we create a new seed by hashing the␣
↪seed.
      step = seed.readUIntBE(0, 6)         // and change the step-size
    }
    else
      result.push(pos)
    pos = (pos + step) % total             // use the modulo operator to␣
↪calculate the next position.
```

(continues on next page)

(continued from previous page)

```
  }
  return result
}
```

in3_sign

requests a signed blockhash from the node. In most cases these requests will come from other nodes, because the client simply adds the addresses of the requested signers and the processising nodes will then aquire the signatures with this method from the other nodes.

Since each node has a risk of signing a wrong blockhash and getting convicted and losing its deposit, per default nodes will and should not sign blockHash of the last `minBlockHeight` (default: 6) blocks!

Parameters:

1. `blocks`: Object[] - requested blocks. Each block-object has these 2 properties:
   (a) `blockNumber` : number - the blockNumber to sign.
   (b) `hash` : hex - (optional) the expected hash. This is optional and can be used to check if the expected hash is correct, but as a client you should not rely on it, but only on the hash in the signature.

Returns:

a Object[] with the following properties for each block:

1. `blockHash` : hex - the blockhash signed.
2. `block` : number - the blockNumber
3. `r` : hex - r-value of the signature
4. `s` : hex - s-value of the signature
5. `v` : number- v-value of the signature
6. `msgHash` : the msgHash signed. This Hash is created :

```
keccak256(
    abi.encodePacked(
        _blockhash,
        _blockNumber,
        registryId
    )
)
```

Request:

```
{
  "method":"in3_sign",
  "params":[{"blockNumber":8770580}]
}
```

Response:

```
{
  "id": 1,
  "result": [
    {
```

(continues on next page)

(continued from previous page)

```
      "blockHash": "0xd8189793f64567992eaadefc51834f3d787b03e9a6850b8b9b8003d8d84a76c8
↪",
      "block": 8770580,
      "r": "0x954ed45416e97387a55b2231bff5dd72e822e4a5d60fa43bc9f9e49402019337",
      "s": "0x277163f586585092d146d0d6885095c35c02b360e4125730c52332cf6b99e596",
      "v": 28,
      "msgHash": "0x40c23a32947f40a2560fcb633ab7fa4f3a96e33653096b17ec613fbf41f946ef"
    }
  ],
  "in3": {
    "lastNodeList": 8669495,
    "currentBlock": 8770590
  }
}
```

in3_whitelist

Returns whitelisted in3-nodes addresses. The whitelist addressed are accquired from whitelist contract that user can specify in request params.

Parameters:

1. `address`: address of whitelist contract

Returns:

- `nodes`: address[] - array of whitelisted nodes addresses.
- `lastWhiteList`: number - the blockNumber of the last change of the in3 white list event.
- `contract`: address - whitelist contract address.
- `totalServer` : number - the total numbers of whitelist nodes.
- `lastBlockNumber` : number - the blockNumber of the last change of the in3 nodes list (usually the last event).

If proof requested the proof section contains the following properties:

- `type` : constant : `accountProof`
- `block` : the serialized blockheader of the latest final block
- `signatures` : a array of signatures from the signers (if requested) of the above block.
- `accounts`: a Object with the addresses of the whitelist contract as key and Proof as value. The Data Structure of the Proof is exactly the same as the result of - `eth_getProof` and this proof is for proofHash of byte array at storage location 0 in whitelist contract. This byte array is of whitelisted nodes addresses.
- `finalityBlocks`: a array of blockHeaders which were mined after the requested block. The number of blocks depends on the request-property `finality`. If this is not specified, this property will not be defined.

Request:

```
{
    "jsonrpc": "2.0",
    "method": "in3_whiteList",
    "params": ["0x08e97ef0a92EB502a1D7574913E2a6636BeC557b"],
    "id": 2,
    "in3": {
```

(continues on next page)

(continued from previous page)

```
        "chainId": "0x5",
         "verification": "proofWithSignature",
         "signatures": [
            "0x45d45e6Ff99E6c34A235d263965910298985fcFe"
        ]
    }
}
```

Response:


```
{
    "id": 2,
    "result": {
        "totalServers": 2,
        "contract": "0x08e97ef0a92EB502a1D7574913E2a6636BeC557b",
        "lastBlockNumber": 1546354,
        "nodes": [
            "0x1fe2e9bf29aa1938859af64c413361227d04059a",
            "0x45d45e6ff99e6c34a235d263965910298985fcfe"
        ]
    },
    "jsonrpc": "2.0",
    "in3": {
        "execTime": 285,
        "lastValidatorChange": 0,
        "proof": {
            "type": "accountProof",
            "block":
↪"0xf9025ca0082a4e766b4af76b7be75818f25310cbc684ccfbd747a4ccb6cacfb4f870d06ba01dcc4de8dec75d7aab85b
↪",
            "accounts": {
                "0x08e97ef0a92EB502a1D7574913E2a6636BeC557b": {
                    "accountProof": [

↪"0xf90211a00cb35d3a4253dde597f30682518f94cbac7690d54dc51bb091f67012e606ee1ea065e37ac9eb1773bceb22c
↪",

↪"0xf90211a0d6cce0c7317d26a22e192288b47a5a34ab7aed0b301c249f27a481f5518e4013a05cc0d414a10bdb4a9f1d6
↪",

↪"0xf90211a0432a3bf286f659650359ae590aa340ce2a2a0d1f60fae509ea9d6a8b90215bfea06b2ab1984e6e8d80eac8d
↪",

↪"0xf8d1a06f998e7193562c27933250e1e72c5a2ff0bf2df556fe478b4436e8b8ac7a7900808080a0de5d6d0bab81e7a0d
↪",

↪"0xf851808080808080a03dd3d6e0c95682f178213fd20364be0395c9e94086eb373fd4aa13ebe4ab3ee2808080808080
↪",

↪"0xf8679e39ce2fd3705a1089a91865fc977c0a778d01f4f3ba9a0fd6378abecef87ab846f8440180a0f5e650b7122ddd2
↪"
                    ],
                    "address": "0x08e97ef0a92eb502a1d7574913e2a6636bec557b",
                    "balance": "0x0",
                    "codeHash":
↪"0x640aaa823fe1752d44d83bcfd0081ec6a1dc72bb82223940a621b0ea251b52c4",
                    "nonce": "0x1",
```


(continues on next page)

(continued from previous page)


```
                    "storageHash":
↪"0xf5e650b7122ddd254ecc84d87c04ea99117f12badec917985f5f3335b355cb5e",
                    "storageProof": [
                        {
                            "key": "0x0",
                            "proof": [

↪"0xf90111a05541df1966b288bce9c5b6f93d564e736f3f984cb3aa4b067ba88e4398bdc86da06483c09a5b5f8f4206d30
↪",

↪"0xf851808080808080808080a02b2bb6a045f22c77b07ecf8b1f7655f7ed4ccb826b16681ccf1965d4b72ad6df808080
↪",

↪"0xf843a0200decd9548b62a8d60345a988386fc84ba6bc95484008f6362f93160ef3e563a1a06aa7bbfbb1778efa33da1
↪"
                            ],
                            "value":
↪"0x6aa7bbfbb1778efa33da1ba032cc3a79b9ef57b428441b4de4f1c38c3f258874"
                        }
                    ]
                }
            },
            "signatures": [
                {
                    "blockHash":
↪"0x2d775ab9b1290f487065e612942a84fc2275572e467040eea154fbbae2005c41",
                    "block": 1798342,
                    "r":
↪"0xf6036400705455c1dfb431e1c90b91f3e50815516577f1ebca9a494164b12d17",
                    "s":
↪"0x30e77bc851e02fc79deab63812203b2dfcacd7a83af14a86c8c9d26d95763cc5",
                    "v": 28,
                    "msgHash":
↪"0x7953b8a420bfe9d1c902e2090f533c9b3f73f0f825b7cec247d7d94e548bc5d9"
                }
            ]
        },
        "lastWhiteList": 1546354
    }
}
```


4.7.2 Ethereum 1.x

Standard JSON-RPC calls as described in https://github.com/ethereum/wiki/wiki/JSON-RPC.

Whenever a request is made for a response with `verification`: `proof`, the node must provide the proof needed to validate the response result. The proof itself depends on the chain.

For ethereum, all proofs are based on the correct block hash. That's why verification differentiates between Verifying the blockhash (which depends on the user consensus) the actual result data.

There is another reason why the BlockHash is so important. This is the only value you are able to access from within a SmartContract, because the evm supports a OpCode (`BLOCKHASH`), which allows you to read the last 256 blockhashes, which gives us the chance to verify even the blockhash onchain.

Depending on the method, different proofs are needed, which are described in this document.

Proofs will add a special in3-section to the response containing a `proof`- object. Each `in3`-section of the response containing proofs has a property with a proof-object with the following properties:

- **type** `string` (required) - The type of the proof.Must be one of the these values : `'transactionProof`', `'receiptProof`', `'blockProof`', `'accountProof`', `'callProof`', `'logProof`'
- **block** `string` - The serialized blockheader as hex, required in most proofs.
- **finalityBlocks** `array` - The serialized following blockheaders as hex, required in case of finality asked (only relevant for PoA-chains). The server must deliver enough blockheaders to cover more then 50% of the validators. In order to verify them, they must be linkable (with the parentHash).
- **transactions** `array` - The list of raw transactions of the block if needed to create a merkle trie for the transactions.
- **uncles** `array` - The list of uncle-headers of the block. This will only be set if full verification is required in order to create a merkle tree for the uncles and so prove the uncle_hash.
- **merkleProof** `string[]` - The serialized merkle-nodes beginning with the root-node (depending on the content to prove).
- **merkleProofPrev** `string[]` - The serialized merkle-nodes beginning with the root-node of the previous entry (only for full proof of receipts).
- **txProof** `string[]` - The serialized merkle-nodes beginning with the root-node in order to proof the transactionIndex (only needed for transaction receipts).
- **logProof** *LogProof* - The Log Proof in case of a `eth_getLogs`-request.
- **accounts** `object` - A map of addresses and their AccountProof.
- **txIndex** `integer` - The transactionIndex within the block (for transaactions and receipts).
- **signatures** `Signature[]` - Requested signatures.

web3_clientVersion

Returns the underlying client version.

See web3_clientversion for spec.

No proof or verification possible.

web3_sha3

Returns Keccak-256 (not the standardized SHA3-256) of the given data.

See web3_sha3 for spec.

No proof returned, but the client must verify the result by hashing the request data itself.

net_version

Returns the current network ID.

See net_version for spec.

No proof returned, but the client must verify the result by comparing it to the used chainId.

eth_blockNumber

Returns the number of the most recent block.

See eth_blockNumber for spec.

No proof returned, since there is none, but the client should verify the result by comparing it to the current blocks returned from others. With the `blockTime` from the chainspec, including a tolerance, the current blocknumber may be checked if in the proposed range.

eth_getBlockByNumber

See *block based proof*

eth_getBlockByHash

Return the block data and proof.

See JSON-RPC-Spec

- eth_getBlockByNumber - find block by number.
- eth_getBlockByHash - find block by hash.

The `eth_getBlockBy...` methods return the Block-Data. In this case, all we need is somebody verifying the blockhash, which is done by requiring somebody who stored a deposit and would otherwise lose it, to sign this blockhash.

The verification is then done by simply creating the blockhash and comparing this to the signed one.

The blockhash is calculated by serializing the blockdata with rlp and hashing it:

```
blockHeader = rlp.encode([
  bytes32( parentHash ),
  bytes32( sha3Uncles ),
  address( miner || coinbase ),
  bytes32( stateRoot ),
  bytes32( transactionsRoot ),
  bytes32( receiptsRoot || receiptRoot ),
  bytes256( logsBloom ),
  uint( difficulty ),
  uint( number ),
  uint( gasLimit ),
  uint( gasUsed ),
  uint( timestamp ),
  bytes( extraData ),

  ... sealFields
    ? sealFields.map( rlp.decode )
    : [
      bytes32( b.mixHash ),
      bytes8( b.nonce )
    ]
])
```

For POA-chains, the blockheader will use the `sealFields` (instead of mixHash and nonce) which are already RLP-encoded and should be added as raw data when using rlp.encode.

```
if (keccak256(blockHeader) !== singedBlockHash)
  throw new Error('Invalid Block')
```

In case of the `eth_getBlockTransactionCountBy...`, the proof contains the full blockHeader already serialized plus all transactionHashes. This is needed in order to verify them in a merkle tree and compare them with the `transactionRoot`.

Requests requiring proof for blocks will return a proof of type `blockProof`. Depending on the request, the proof will contain the following properties:

- `type` : constant : `blockProof`
- `signatures` : a array of signatures from the signers (if requested) of the requested block.
- `transactions`: a array of raw transactions of the block. This is only needed the last parameter of the request (includeTransactions) is `false`, In this case the result only contains the transactionHashes, but in order to verify we need to be able to build the complete merkle-trie, where the raw transactions are needed. If the complete transactions are included the raw transactions can be build from those values.
- `finalityBlocks`: a array of blockHeaders which were mined after the requested block. The number of blocks depends on the request-property `finality`. If this is not specified, this property will not be defined.
- `uncles`: only if `fullProof` is requested we add all blockheaders of the uncles to the proof in order to verify the uncleRoot.

Request:

```
{
    "method": "eth_getBlockByNumber",
    "params": [
        "0x967a46",
        false
    ],
    "in3": {
      "verification":"proof"
    }
}
```

Response:

```
{
    "jsonrpc": "2.0",
    "result": {
        "author": "0x00d6cc1ba9cf89bd2e58009741f4f7325badc0ed",
        "difficulty": "0xfffffffffffffffffffffffffffffffe",
        "extraData": "0xde830201088f5061726974792d457468657265756d86312e33302e30827769
↪",
        "gasLimit": "0x7a1200",
        "gasUsed": "0x1ce0f",
        "hash": "0xfeb120ae45f1009e6c2289436d5957c58a15915288ec083658bd044101608f26",
        "logsBloom": "0x0008000...",
        "miner": "0x00d6cc1ba9cf89bd2e58009741f4f7325badc0ed",
        "number": "0x967a46",
        "parentHash":
↪"0xc591335e0cdb6b21dc9af57567a6e075fc6315aff915bd79bf78a2c8815bc657",
        "receiptsRoot":
↪"0xfa2a0b3c0715e798ae41fd4645b0261ae4bf6d2c56f29da6fcc5fbfb7c6f19f8",
        "sealFields": [
            "0x8417098353",
```

(continues on next page)

(continued from previous page)

```
↪"0xb841eb80c1a0be2eb7a1c14fc38759a0f9fe9c33121d72003025160a4b35119d495d34d39a9fd7475d28ba863e35f510
↪"
        ],
        "sha3Uncles":
↪"0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347",
        "size": "0x44e",
        "stateRoot":
↪"0xd618159b6dbd0c6213d90abbf01e06513104f0670cd79503cb2563d7ff116864",
        "timestamp": "0x5c260d4c",
        "totalDifficulty": "0x94373700000000000000000000484b6f390",
        "transactions": [
            "0x16cfadb6a0a823c623788713cb1eb7d399f89f78d599d416f7b91dca44eeb804",
            "0x91458145d2c47527eee34e891879ac2915b3f8ba6f31911c5234928ae32cb191"
        ],
        "transactionsRoot":
↪"0x4f1249c6378282b1f032cc8c2562712f2450a0bed8ce20bdd2d01b6520feb75a",
        "uncles": []
    },
    "id": 77,
    "in3": {
        "proof": {
            "type": "blockProof",
            "signatures": [ ...  ],
            "transactions": [
                "0xf8ac8201158504a817c8....",
                "0xf9014c8301a3d4843b9ac....",
            ]
        },
        "currentBlock": 9866910,
        "lastNodeList": 8057063,
    }
}
```

eth_getBlockTransactionCountByHash

See *transaction count proof*

eth_getBlockTransactionCountByNumber

See *transaction count proof*

eth_getUncleCountByBlockHash

See *count proof*

eth_getUncleCountByBlockNumber

return the number of transactions or uncles.

See JSON-RPC-Spec

- eth_getBlockTransactionCountByHash - number of transaction by block hash.

- eth_getBlockTransactionCountByNumber - number of transaction by block number.
- eth_getUncleCountByBlockHash - number of uncles by block number.
- eth_getUncleCountByBlockNumber - number of uncles by block number.

Requests requiring proof for blocks will return a proof of type `blockProof`. Depending on the request, the proof will contain the following properties:

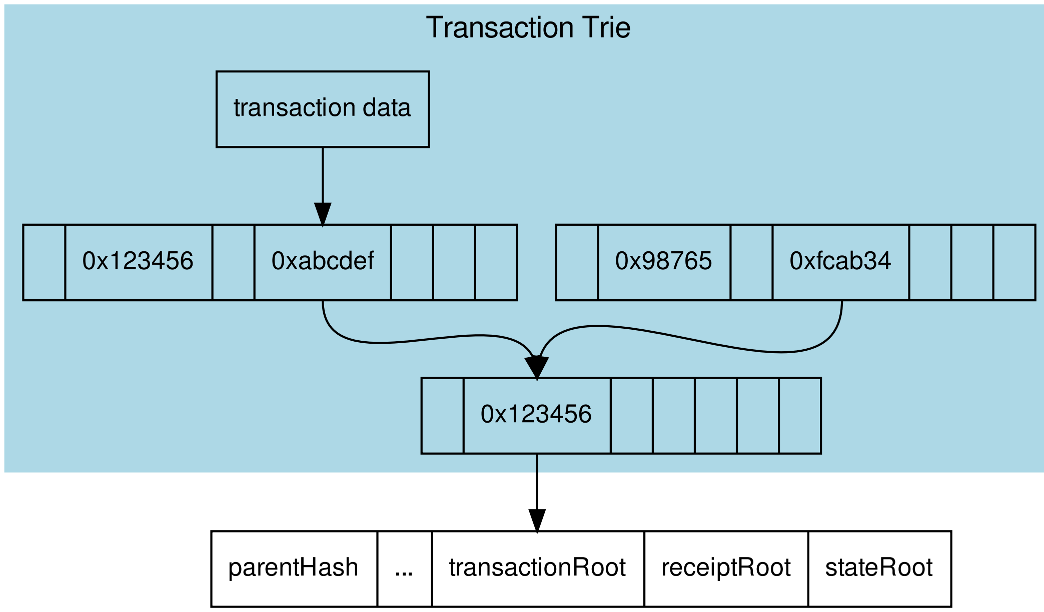
- `type` : constant : `blockProof`
- `signatures` : a array of signatures from the signers (if requested) of the requested block.
- `block` : the serialized blockheader
- `transactions`: a array of raw transactions of the block. This is only needed if the number of transactions are requested.
- `finalityBlocks`: a array of blockHeaders which were mined after the requested block. The number of blocks depends on the request-property `finality`. If this is not specified, this property will not be defined.
- `uncles`: a array of blockheaders of the uncles of the block. This is only needed if the number of uncles are requested.

eth_getTransactionByHash

return the transaction data.

See JSON-RPC-Spec

- eth_getTransactionByHash - transaction data by hash.
- eth_getTransactionByBlockHashAndIndex - transaction data based on blockhash and index
- eth_getTransactionByBlockNumberAndIndex - transaction data based on block number and index



In order to prove the transaction data, each transaction of the containing block must be serialized

```
transaction = rlp.encode([
  uint( tx.nonce ),
  uint( tx.gasPrice ),
  uint( tx.gas || tx.gasLimit ),
  address( tx.to ),
  uint( tx.value ),
  bytes( tx.input || tx.data ),
  uint( tx.v ),
  uint( tx.r ),
  uint( tx.s )
])
```

and stored in a merkle tree with `rlp.encode(transactionIndex)` as key or path, since the blockheader only contains the `transactionRoot`, which is the root-hash of the resulting merkle tree. A merkle-proof with the transactionIndex of the target transaction will then be created from this tree.

If the request requires proof (`verification: proof`) the node will provide an Transaction Proof as part of the in3-section of the response. This proof section contains the following properties:

- `type` : constant : `transactionProof`
- `block` : the serialized blockheader of the requested transaction.
- `signatures` : a array of signatures from the signers (if requested) of the above block.
- `txIndex` : The TransactionIndex as used in the MerkleProof (not needed if the methode was `eth_getTransactionByBlock...`, since already given)
- `merkleProof`: the serialized nodes of the Transaction trie starting with the root node.

- `finalityBlocks`: a array of blockHeaders which were mined after the requested block. The number of blocks depends on the request-property `finality`. If this is not specified, this property will not be defined.

While there is no proof for a non existing transaction, if the request was a `eth_getTransactionByBlock...` the node must deliver a partial merkle-proof to verify that this node does not exist.

Request:

```
{
  "method":"eth_getTransactionByHash",
  "params":["0xe9c15c3b26342e3287bb069e433de48ac3fa4ddd32a31b48e426d19d761d7e9b"],
  "in3":{
    "verification":"proof"
  }
}
```

Response:

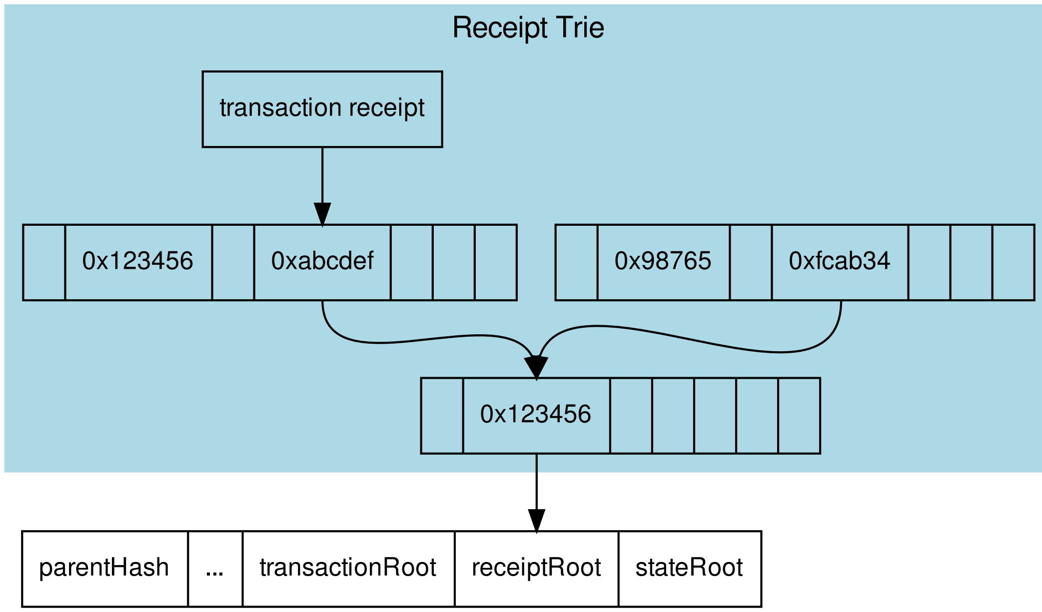
```
{
  "jsonrpc": "2.0",
  "id": 6,
  "result": {
    "blockHash": "0xf1a2fd6a36f27950c78ce559b1dc4e991d46590683cb8cb84804fa672bca395b",
    "blockNumber": "0xca",
    "from": "0x7e5f4552091a69125d5dfcb7b8c2659029395bdf",
    "gas": "0x55f0",
    "gasPrice": "0x0",
    "hash": "0xe9c15c3b26342e3287bb069e433de48ac3fa4ddd32a31b48e426d19d761d7e9b",
    "input": "0x00",
    "value": "0x3e8"
    ...
  },
  "in3": {
    "proof": {
      "type": "transactionProof",
      "block": "0xf901e6a040997a53895b48...", // serialized blockheader
      "merkleProof": [  /* serialized nodes starting with the root-node */
        "0xf868822080b863f86136808255f0942b5ad5c4795c026514f8317c7a215e218dc..."
        "0xcd6cf8203e8001ca0dc967310342af5042bb64c34d3b92799345401b26713b43f..."
      ],
      "txIndex": 0,
      "signatures": [...]
    }
  }
}
```

eth_getTransactionReceipt

The Receipt of a Transaction.

See JSON-RPC-Spec

- eth_getTransactionReceipt - returns the receipt.



The proof works similiar to the transaction proof.

In order to create the proof we need to serialize all transaction receipts

```
transactionReceipt = rlp.encode([
  uint( r.status || r.root ),
  uint( r.cumulativeGasUsed ),
  bytes256( r.logsBloom ),
  r.logs.map(l => [
    address( l.address ),
    l.topics.map( bytes32 ),
    bytes( l.data )
  ])
].slice(r.status === null && r.root === null ? 1 : 0))
```

and store them in a merkle tree with `rlp.encode(transactionIndex)` as key or path, since the blockheader only contains the `receiptRoot`, which is the root-hash of the resulting merkle tree. A merkle proof with the transactionIndex of the target transaction receipt will then be created from this tree.

Since the merkle proof is only proving the value for the given transactionIndex, we also need to prove that the transactionIndex matches the transactionHash requested. This is done by adding another MerkleProof for the transaction itself as described in the *Transaction Proof*.

If the request requires proof (`verification: proof`) the node will provide an Transaction Proof as part of the in3-section of the response. This proof section contains the following properties:

- `type` : constant : `receiptProof`
- `block` : the serialized blockheader of the requested transaction.
- `signatures` : a array of signatures from the signers (if requested) of the above block.
- `txIndex` : The TransactionIndex as used in the MerkleProof

- `txProof` : the serialized nodes of the Transaction trie starting with the root node. This is needed in order to proof that the required transactionHash matches the receipt.
- `merkleProof`: the serialized nodes of the Transaction Receipt trie starting with the root node.
- `merkleProofPrev`: the serialized nodes of the previous Transaction Receipt (if txInxdex>0) trie starting with the root node. This is only needed if full-verification is requested. With a verified previous Receipt we can proof the `usedGas`.
- `finalityBlocks`: a array of blockHeaders which were mined after the requested block. The number of blocks depends on the request-property `finality`. If this is not specified, this property will not be defined.

Request:

```
{
  "method": "eth_getTransactionReceipt",
  "params": [
      "0x5dc2a9ec73abfe0640f27975126bbaf14624967e2b0b7c2b3a0fb6111f0d3c5e"
  ]
  "in3":{
    "verification":"proof"
  }
}
```

Response:

```
{
    "result": {
        "blockHash":
↪"0xea6ee1e20d3408ad7f6981cfcc2625d80b4f4735a75ca5b20baeb328e41f0304",
        "blockNumber": "0x8c1e39",
        "contractAddress": null,
        "cumulativeGasUsed": "0x2466d",
        "gasUsed": "0x2466d",
        "logs": [
            {
                "address": "0x85ec283a3ed4b66df4da23656d4bf8a507383bca",
                "blockHash":
↪"0xea6ee1e20d3408ad7f6981cfcc2625d80b4f4735a75ca5b20baeb328e41f0304",
                "blockNumber": "0x8c1e39",
                "data": "0x00000000000...",
                "logIndex": "0x0",
                "removed": false,
                "topics": [

↪"0x9123e6a7c5d144bd06140643c88de8e01adcbb24350190c02218a4435c7041f8",

↪"0xa2f7689fc12ea917d9029117d32b9fdef2a53462c853462ca86b71b97dd84af6",

↪"0x55a6ef49ec5dcf6cd006d21f151f390692eedd839c813a150000000000000000"
                ],
                "transactionHash":
↪"0x5dc2a9ec73abfe0640f27975126bbaf14624967e2b0b7c2b3a0fb6111f0d3c5e",
                "transactionIndex": "0x0",
                "transactionLogIndex": "0x0",
                "type": "mined"
            }
        ],
        "logsBloom": "0x00000000000000000000200000...",
```

(continues on next page)

(continued from previous page)

```
        "root": null,
        "status": "0x1",
        "transactionHash":
↪"0x5dc2a9ec73abfe0640f27975126bbaf14624967e2b0b7c2b3a0fb6111f0d3c5e",
        "transactionIndex": "0x0"
    },
    "in3": {
        "proof": {
            "type": "receiptProof",
            "block": "0xf9023fa019e9d929ab...",
            "txProof": [
                "0xf851a083c8446ab932130..."
            ],
            "merkleProof": [
                "0xf851a0b0f5b7429a54b10..."
            ],
            "txIndex": 0,
            "signatures": [...],
            "merkleProofPrev": [
                "0xf851a0b0f5b7429a54b10..."
            ]
        },
        "currentBlock": 9182894,
        "lastNodeList": 6194869
    }
}
```

eth_getLogs

Proofs for logs or events.

See JSON-RPC-Spec

- eth_getLogs - returns all event matching the filter.

Since logs or events are based on the TransactionReceipts, the only way to prove them is by proving the TransactionReceipt each event belongs to.

That's why this proof needs to provide:

- all blockheaders where these events occured
- all TransactionReceipts plus their MerkleProof of the logs
- all MerkleProofs for the transactions in order to prove the transactionIndex

The proof data structure will look like this:

```
  Proof {
    type: 'logProof',
    logProof: {
      [blockNr: string]: {  // the blockNumber in hex as key
        block : string  // serialized blockheader
        receipts: {
          [txHash: string]: {  // the transactionHash as key
            txIndex: number // transactionIndex within the block
            txProof: string[] // the merkle Proof-Array for the transaction
            proof: string[] // the merkle Proof-Array for the receipts
```

(continues on next page)

(continued from previous page)

```
          }
        }
      }
    }
  }
```

In order to create the proof, we group all events into their blocks and transactions, so we only need to provide the blockheader once per block. The merkle-proofs for receipts are created as described in the *Receipt Proof*.

If the request requires proof (`verification: proof`) the node will provide an Transaction Proof as part of the in3-section of the response. This proof section contains the following properties:

- `type` : constant : `logProof`
- `logProof` : The proof for all the receipts. This structure contains an object with the blockNumbers as keys. Each block contains the blockheader and the receipt proofs.
- `signatures` : a array of signatures from the signers (if requested) of the above blocks.
- `finalityBlocks`: a array of blockHeaders which were mined after the requested block. The number of blocks depends on the request-property `finality`. If this is not specified, this property will not be defined.

Request:

```
{
  "method": "eth_getLogs",
  "params": [
      {
          "fromBlock": "0x7ae000",
          "toBlock": "0x7af0e4",
          "address": "0x27a37a1210df14f7e058393d026e2fb53b7cf8c1"
      }
  ],
  "in3":{
    "verification":"proof"
  }
}
```

Response:

```
{
    "jsonrpc": "2.0",
    "result": [
        {
            "address": "0x27a37a1210df14f7e058393d026e2fb53b7cf8c1",
            "blockHash":
↪"0x12657acc9dbca74775efcc09bcd55da769e89fff27a0402e02708a6e69caa3bb",
            "blockNumber": "0x7ae16b",
            "data": "0x0000000000000...",
            "logIndex": "0x0",
            "removed": false,
            "topics": [
                "0x690cd1ace756531abc63987913dcfaf18055f3bd6bb27d3def1cc5319ebc1461"
            ],
            "transactionHash":
↪"0xddc81454b0df60fb31dbefd0fd4c5e8fe4f3daa541c879964500d876056e2976",
            "transactionIndex": "0x0",
            "transactionLogIndex": "0x0",
```

(continues on next page)

(continued from previous page)

```
            "type": "mined"
        },
        {
            "address": "0x27a37a1210df14f7e058393d026e2fb53b7cf8c1",
            "blockHash":
↪"0x2410d512d12e18b2451efe195ece85723b7f39c3f5d706ea112bfcc57c0249d2",
            "blockNumber": "0x7af0e4",
            "data": "0x000000000000000...",
            "logIndex": "0x4",
            "removed": false,
            "topics": [
                "0x690cd1ace756531abc63987913dcfaf18055f3bd6bb27d3def1cc5319ebc1461"
            ],
            "transactionHash":
↪"0x30fe995d61a5491a49e8f1283b36f4cb7fa5d370927bd8784c33e702546a9daa",
            "transactionIndex": "0x4",
            "transactionLogIndex": "0x0",
            "type": "mined"
        }
    ],
    "id": 144,
    "in3": {
        "proof": {
            "type": "logProof",
            "logProof": {
                "0x7ae16b": {
                    "number": 8053099,
                    "receipts": {

↪"0xddc81454b0df60fb31dbefd0fd4c5e8fe4f3daa541c879964500d876056e2976": {
                            "txHash":
↪"0xddc81454b0df60fb31dbefd0fd4c5e8fe4f3daa541c879964500d876056e2976",
                            "txIndex": 0,
                            "proof": [
                                "0xf9020e822080b90208f..."
                            ],
                            "txProof": [
                                "0xf8f7822080b8f2f8f080..."
                            ]
                        }
                    },
                    "block": "0xf9023ea002343274..."
                },
                "0x7af0e4": {
                    "number": 8057060,
                    "receipts": {

↪"0x30fe995d61a5491a49e8f1283b36f4cb7fa5d370927bd8784c33e702546a9daa": {
                            "txHash":
↪"0x30fe995d61a5491a49e8f1283b36f4cb7fa5d370927bd8784c33e702546a9daa",
                            "txIndex": 4,
                            "proof": [
                                "0xf851a039faec6276...",
                                "0xf8b180a0ee82c377...",
                                "0xf9020c20b90208f9..."
                            ],
                            "txProof": [
```

(continues on next page)

(continued from previous page)

```
                                        "0xf851a09250840f6b87...",
                                        "0xf8b180a04e5257328b...",
                                        "0xf8f620b8f3f8f18085..."
                                    ]
                                }
                            },
                            "block": "0xf9023ea03837491e4b3b..."
                        }
                    }
                },
                "lastValidatorChange": 0,
                "lastNodeList": 8057063
        }
}
```

eth_getBalance

See *account proof*

eth_getCode

See *account proof*

eth_getTransactionCount

See *account proof*

eth_getStorageAt

Returns account based values and proof.

See JSON-RPC-Spec

- eth_getBalance - returns the balance.
- eth_getCode - the byte code of the contract.
- eth_getTransactionCount - the nonce of the account.
- eth_getStorageAt - the storage value for the given key of the given account.

Each of these account values are stored in the account-object:

```
account = rlp.encode([
  uint( nonce),
  uint( balance),
  bytes32( storageHash || ethUtil.KECCAK256_RLP),
  bytes32( codeHash || ethUtil.KECCAK256_NULL)
])
```

The proof of an account is created by taking the state merkle tree and creating a MerkleProof. Since all of the above RPC-methods only provide a single value, the proof must contain all four values in order to encode them and verify the value of the MerkleProof.

For verification, the `stateRoot` of the blockHeader is used and `keccak(accountProof.address)` as the path or key within the merkle tree.

```
verifyMerkleProof(
 block.stateRoot, // expected merkle root
 keccak(accountProof.address), // path, which is the hashed address
 accountProof.accountProof), // array of Buffer with the merkle-proof-data
 isNotExistend(accountProof) ? null : serializeAccount(accountProof), // the expected␣
↪serialized account
)
```

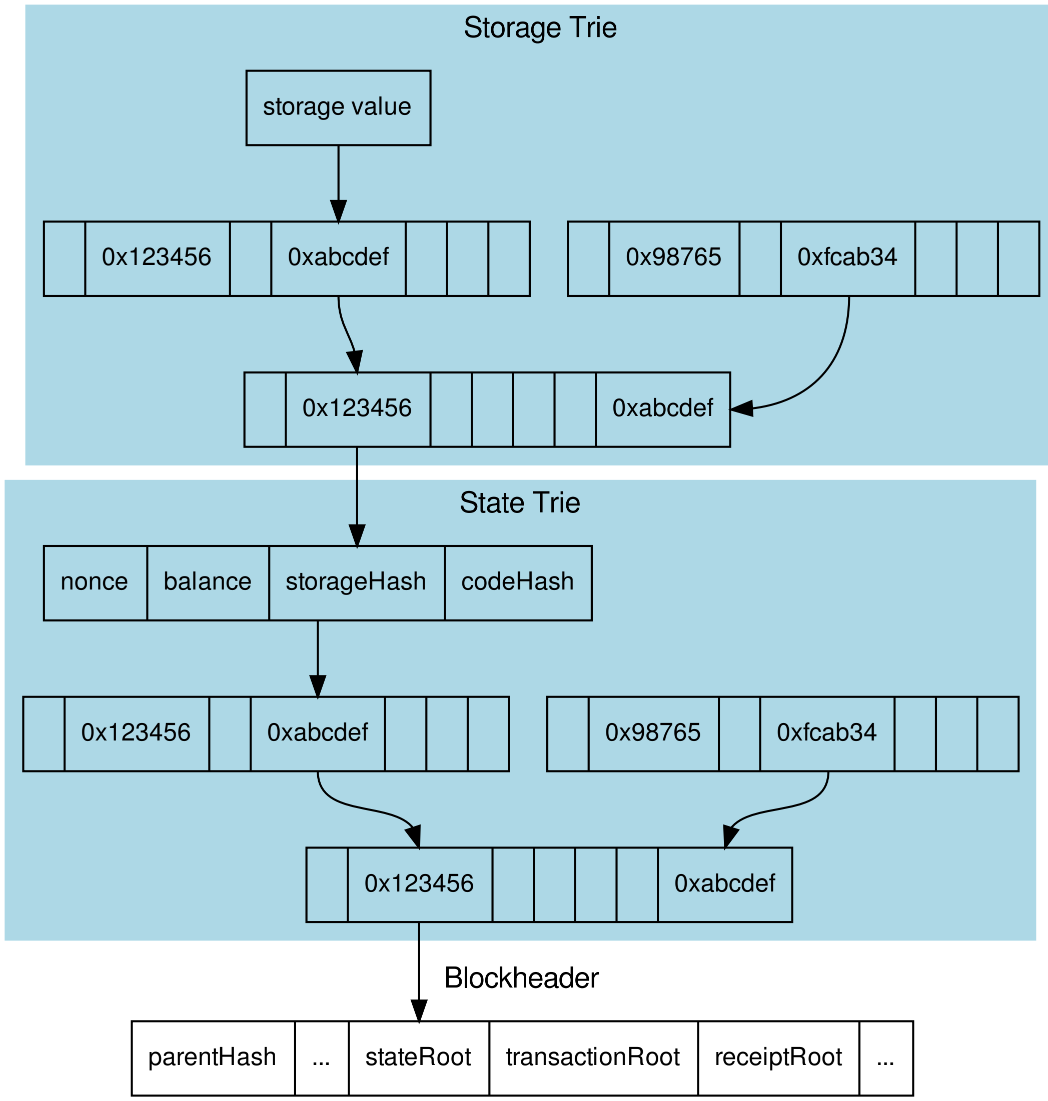
In case the account does not exist yet (which is the case if `none == startNonce` and `codeHash == '0xc5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470'`), the proof may end with one of these nodes:

- The last node is a branch, where the child of the next step does not exist.
- The last node is a leaf with a different relative key.

Both would prove that this key does not exist.

For `eth_getStorageAt`, an additional storage proof is required. This is created by using the `storageHash` of the account and creating a MerkleProof using the hash of the storage key (`keccak(key)`) as path.

```
verifyMerkleProof(
  bytes32( accountProof.storageHash ),   // the storageRoot of the account
  keccak(bytes32(s.key)),  // the path, which is the hash of the key
  s.proof.map(bytes), // array of Buffer with the merkle-proof-data
  s.value === '0x0' ? null : util.rlp.encode(s.value) // the expected value or none␣
↪to proof non-existence
))
```



If the request requires proof (`verification: proof`) the node will provide an Account Proof as part of the in3-section of the response. This proof section contains the following properties:

- `type` : constant : `accountProof`
- `block` : the serialized blockheader of the requested block (the last parameter of the request)
- `signatures` : a array of signatures from the signers (if requested) of the above block.
- `accounts`: a Object with the addresses of all required accounts (in this case it is only one account) as key and Proof as value. The DataStructure of the Proof for each account is exactly the same as the result of - `eth_getProof`.
- `finalityBlocks`: a array of blockHeaders which were mined after the requested block. The number of blocks depends on the request-property `finality`. If this is not specified, this property will not be defined.

Example

Request:

```
{
    "method": "eth_getStorageAt",
    "params": [
        "0x27a37a1210Df14f7E058393d026e2fB53B7cf8c1",
        "0x0",
        "latest"
    ],
    "in3": {
      "verification":"proof"
    }
}
```

Response:

```
{
    "id": 77,
    "jsonrpc": "2.0",
    "result": "0x5",
    "in3": {
        "proof": {
            "type": "accountProof",
            "block": "0xf90246...",
            "signatures": [...],
            "accounts": {
                "0x27a37a1210Df14f7E058393d026e2fB53B7cf8c1": {
                    "accountProof": [
                        "0xf90211a0bf....",
                        "0xf90211a092....",
                        "0xf90211a0d4....",
                        "0xf90211a084....",
                        "0xf9019180a0...."
                    ],
                    "address": "0x27a37a1210df14f7e058393d026e2fb53b7cf8c1",
                    "balance": "0x11c37937e08000",
                    "codeHash":
↪"0x3b4e727399e02beb6c92e8570b4ccdd24b6a3ef447c89579de5975edd861264e",
                    "nonce": "0x1",
                    "storageHash":
↪"0x595b6b8bfaad7a24d0e5725ba86887c81a9d99ece3afcce1faf508184fcbe681",
                    "storageProof": [
                        {
                            "key": "0x0",
                            "proof": [
                                "0xf90191a08e....",
                                "0xf871808080....",

↪"0xe2a0200decd9548b62a8d60345a988386fc84ba6bc95484008f6362f93160ef3e56305"
                            ],
                            "value": "0x5"
                        }
                    ]
                }
            }
        },
```

(continues on next page)

(continued from previous page)

```
        "currentBlock": 9912897,
        "lastNodeList": 8057063
    }
}
```

eth_estimateGas

See *call proof*

eth_call

calls a function of a contract (or simply executes the evm opcodes).

See JSON-RPC-Spec

- eth_call - executes a function and returns the result.
- eth_estimateGas - executes a function and returns the gas used.

Verifying the result of an `eth_call` is a little bit more complex because the response is a result of executing opcodes in the vm. The only way to do so is to reproduce it and execute the same code. That's why a call proof needs to provide all data used within the call. This means:

- All referred accounts including the code (if it is a contract), storageHash, nonce and balance.
- All storage keys that are used (this can be found by tracing the transaction and collecting data based on the `SLOAD`-opcode).
- All blockdata, which are referred at (besides the current one, also the `BLOCKHASH`-opcodes are referring to former blocks).

For verifying, you need to follow these steps:

1. Serialize all used blockheaders and compare the blockhash with the signed hashes. (See *BlockProof*)
2. Verify all used accounts and their storage as showed in *Account Proof*.
3. Create a new VM with a MerkleTree as state and fill in all used value in the state:

```
// create new state for a vm
const state = new Trie()
const vm = new VM({ state })

// fill in values
for (const adr of Object.keys(accounts)) {
  const ac = accounts[adr]

  // create an account-object
  const account = new Account([ac.nonce, ac.balance, ac.stateRoot, ac.codeHash])

  // if we have a code, we will set the code
  if (ac.code) account.setCode( state, bytes( ac.code ))

  // set all storage-values
  for (const s of ac.storageProof)
    account.setStorage( state, bytes32( s.key ), rlp.encode( bytes32( s.value )))

  // set the account data
```

(continues on next page)

(continued from previous page)

```
    state.put( address( adr ), account.serialize())
  }

  // add listener on each step to make sure it uses only values found in the proof
  vm.on('step', ev => {
     if (ev.opcode.name === 'SLOAD') {
        const contract = toHex( ev.address ) // address of the current code
        const storageKey = bytes32( ev.stack[ev.stack.length - 1] ) // last element␣
↪on the stack is the key
        if (!getStorageValue(contract, storageKey))
          throw new Error(`incomplete data: missing key ${storageKey}`)
     }
     /// ... check other opcodes as well
  })

  // create a transaction
  const tx = new Transaction(txData)

  // run it
  const result = await vm.runTx({ tx, block: new Block([block, [], []]) })

  // use the return value
  return result.vm.return
```

In the future, we will be using the same approach to verify calls with ewasm.

If the request requires proof (`verification: proof`) the node will provide an Call Proof as part of the in3-section of the response. Details on how create the proof can be found in the *CallProof-Chapter*. This proof section contains the following properties:

- `type` : constant : `callProof`
- `block` : the serialized blockheader of the requested block (the last parameter of the request)
- `signatures` : a array of signatures from the signers (if requested) of the above block.
- `accounts`: a Object with the addresses of all accounts required to run the call as keys. This includes also all storage values (SLOAD) including proof used. The DataStructure of the Proof for each account is exactly the same as the result of - `eth_getProof`.
- `finalityBlocks`: a array of blockHeaders which were mined after the requested block. The number of blocks depends on the request-property `finality`. If this is not specified, this property will not be defined.

Request:


```
{
    "method": "eth_call",
    "params": [
        {
            "to": "0x2736D225f85740f42D17987100dc8d58e9e16252",
            "data":
↪"0x5cf0f3570000000000000000000000000000000000000000000000000000000000000001"
        },
        "latest"
    ],
    "in3": {
      "verification":"proof"
    }
}
```

Response:

```
{
    "result": "0x0000000000000000000000000...",
    "in3": {
        "proof": {
            "type": "callProof",
            "block": "0xf90215a0c...",
            "signatures": [...],
            "accounts": {
                "0x2736D225f85740f42D17987100dc8d58e9e16252": {
                    "accountProof": [
                        "0xf90211a095...",
                        "0xf90211a010...",
                        "0xf90211a062...",
                        "0xf90211a091...",
                        "0xf90211a03a...",
                        "0xf901f1a0d1...",
                        "0xf8b18080808..."
                    ],
                    "address": "0x2736d225f85740f42d17987100dc8d58e9e16252",
                    "balance": "0x4fffb",
                    "codeHash":
↪"0x2b8bdc59ce78fd8c248da7b5f82709e04f2149c39e899c4cdf4587063da8dc69",
                    "nonce": "0x1",
                    "storageHash":
↪"0xbf904e79d4ebf851b2380d81aab081334d79e231295ae1b87f2dd600558f126e",
                    "storageProof": [
                        {
                            "key": "0x0",
                            "proof": [
                                "0xf901f1a0db74...",
                                "0xf87180808080...",
                                "0xe2a0200decd9....05"
                            ],
                            "value": "0x5"
                        },
                        {
                            "key":
↪"0x290decd9548b62a8d60345a988386fc84ba6bc95484008f6362f93160ef3e569",
                            "proof": [
                                "0xf901f1a0db74...",
                                "0xf891a0795a99...",
                                "0xe2a020ab8540...43"
                            ],
                            "value": "0x43"
                        },
                        {
                            "key":
↪"0xaaab8540682e3a537d17674663ea013e92c83fdd69958f314b4521edb3b76f1a",
                            "proof": [
                                "0xf901f1a0db747...",
                                "0xf891808080808...",
                                "0xf843a0207bd5ee..."
                            ],
                            "value":
↪"0x68747470733a2f2f696e332e736c6f636b2e69742f6d61696e6e65742f6e642d"
                        }
```

(continues on next page)

(continued from previous page)


```
                    ]
                }
            }
        },
        "currentBlock": 8040612,
        "lastNodeList": 6619795
    }
}
```


eth_accounts

eth_sign

eth_sendTransaction

See JSON-RPC-Spec

- eth_accounts - returns the unlocked accounts.
- eth_sign - signs data with an unlocked account.
- eth_sendTransaction - signs and sends a transaction.

Signing is **not supported** since the nodes are serving a public rpc-enpoint. These methods will return a error. The client may still support those methods, but handle those requests internally.

eth_sendRawTransaction

See JSON-RPC-Spec

- eth_sendRawTransaction - sends a prviously signed transaction.

This Method does not require any proof. (even if requested). Clients must at least verify the returned transactionHash by hashing the rawTransaction data. To know whether the transaction was actually broadcasted and mined, the client needs to run a second request `eth_getTransactionByHash` which should contain the blocknumber as soon as this is mined.

CHAPTER 5

Roadmap

Incubed implements two versions:

- **TypeScript / JavaScript**: optimized for dApps, web apps, or mobile apps.
- **C**: optimized for microcontrollers and all other use cases.

In the future we will focus on one codebase, which is C. This will be ported to many platforms (like WASM).

5.1 V2.0 Stable: Q3 2019

This was the first stable release, which was published after Devcon. It contains full verification of all relevant Ethereum RPC calls (except eth_call for eWasm contracts), but there is no payment or incentivization included yet.

- **Fail-safe Connection**: The Incubed client will connect to any Ethereum blockchain (providing Incubed servers) by randomly selecting nodes within the Incubed network and, if the node cannot be reached or does not deliver verifiable responses, automatically retrying with different nodes.
- **Reputation Management**: Nodes that are not available will be temporarily blacklisted and lose reputation. The selection of a node is based on the weight (or performance) of the node and its availability.
- **Automatic NodeList Updates**: All Incubed nodes are registered in smart contracts on chain and will trigger events if the NodeList changes. Each request will always return the blockNumber of the last event so that the client knows when to update its NodeList.
- **Partial NodeList**: To support small devices, the NodeList can be limited and still be fully verified by basing the selection of nodes deterministically on a client-generated seed.
- **Multichain Support**: Incubed is currently supporting any Ethereum-based chain. The client can even run parallel requests to different networks without the need to synchronize first.
- **Preconfigured Boot Nodes**: While you can configure any registry contract, the standard version contains configuration with boot nodes for `mainnet`, `kovan`, `evan`, `tobalaba`, and `ipfs`.
- **Full Verification of JSON-RPC Methods**: Incubed is able to fully verify all important JSON-RPC methods. This even includes calling functions in smart contract and verifying their return value (`eth_call`), which means executing each opcode locally in the client to confirm the result.

- **IPFS Support**: Incubed is able to write and read IPFS content and verify the data by hashing and creating the multihash.
- **Caching Support**: An optional cache enables storage of the results of RPC requests that can automatically be used again within a configurable time span or if the client is offline. This also includes RPC requests, blocks, code, and NodeLists.
- **Custom Configuration**: The client is highly customizable. For each request, a configuration can be explicitly passed or adjusted through events (`client.on('beforeRequest',...)`). This allows the proof level or number of requests to be sent to be optimized depending on the context.
- **Proof Levels**: Incubed supports different proof levels: `none` for no verification, `standard` for verifying only relevant properties, and `full` for complete verification, including uncle blocks or previous transactions (higher payload).
- **Security Levels**: Configurable number of signatures (for PoW) and minimal deposit stored.
- **PoW Support**: For PoW, blocks are verified based on blockhashes signed by Incubed nodes storing a deposit, which they lose if this blockhash is not correct.
- **PoA Support**: (experimental) For PoA chains (using Aura and clique), blockhashes are verified by extracting the signature from the sealed fields of the blockheader and by using the Aura algorithm to determine the signer from the validatorlist (with static validatorlist or contract-based validators).
- **Finality Support**: For PoA chains, the client can require a configurable number of signatures (in percent) to accept them as final.
- **Flexible Transport Layer**: The communication layer between clients and nodes can be overridden, but the layer already supports different transport formats (JSON/CBOR/Incubed).
- **Replace Latest Blocks**: Since most applications per default always ask for the latest block, which cannot be considered final in a PoW chain, a configuration allows applications to automatically use a certain block height to run the request (like six blocks).
- **Light Ethereum API**: Incubed comes with a simple type-safe API, which covers all standard JSON-RPC requests (`in3.eth.getBalance('0x52bc44d5378309EE2abF1539BF71dE1b7d7bE3b5')`). This API also includes support for signing and sending transactions, as well as calling methods in smart contracts without a complete ABI by simply passing the signature of the method as an argument.
- **TypeScript Support**: Because Incubed is written 100% in TypeScript, you get all the advantages of a type-safe toolchain.
- **java**: java version of the Incubed client based on the C sources (using JNI)

5.2 V2.1 Incentivization: Q4 2019

This release will introduce the incentivization layer, which should help provide more nodes to create the decentralized network.

- **PoA Clique**: Supports Clique PoA to verify blockheaders.
- **Signed Requests**: Incubed supports the incentivization layer, which requires signed requests to assign client requests to certain nodes.
- **Network Balancing**: Nodes will balance the network based on load and reputation.
- **python-bindings**: integration in python
- **go-bindings**: bindings for go

5.3 V2.2 Bitcoin: Q1 2020

Multichain Support for BTC

- **Bitcoin**: Supports Verfification for Bitcoin blocks and Transactions
- **WASM**: Typescript client based on a the C-Sources compiled to wasm.

5.4 V2.3 WASM: Q3 2020

For `eth_call` verification, the client and server must be able to execute the code. This release adds the ability to support eWasm contracts.

- **eth 2.0**: Basic Support for Eth 2.0
- **eWasm**: Supports eWasm contracts in eth_call.

5.5 V2.4 Substrate: Q1 2021

Supports Polkadot or any substrate-based chains.

- **Substrate**: Framework support.
- **Runtime Optimization**: Using precompiled runtimes.

5.6 V2.5 Services: Q3 2021

Generic interface enables any deterministic service (such as docker-container) to be decentralized and verified.

CHAPTER 6

Benchmarks

These benchmarks aim to test the Incubed version for stability and performance on the server. As a result, we can gauge the resources needed to serve many clients.

6.1 Setup and Tools

- JMeter is used to send requests parallel to the server
- Custom Python scripts is used to generate lists of transactions as well as randomize them (used to create test plan)
- Link for making JMeter tests online without setting up the server: https://www.blazemeter.com/

JMeter can be downloaded from: https://jmeter.apache.org/download_jmeter.cgi

Install JMeter on Mac OS With HomeBrew

1. Open a Mac Terminal where we will be running all the commands
2. First, check to see if HomeBrew is installed on your Mac by executing this command. You can either run brew help or brew -v
3. If HomeBrew is not installed, run the following command to install HomeBrew on Mac:

```
ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/
↪install/master/install)"
Once HomeBrew is installed, we can continue to install JMeter.
```

4. To install JMeter without the extra plugins, run the following command:

```
brew install jmeter
```

5. To install JMeter with all the extra plugins, run the following command:

```
brew install jmeter --with-plugins
```

6. Finally, verify the installation by executing jmeter -v
7. Run JMeter using 'jmeter' which should load the JMeter GUI

JMeter on EC2 instance CLI only (testing pending):

1. Login to AWS and navigate to the EC2 instance page
2. Create a new instance, choose an Ubuntu AMI]
3. Provision the AWS instance with the needed information, enable CloudWatch monitoring
4. Configure the instance to allow all outgoing traffic, and fine tune Security group rules to suit your need
5. Save the SSH key, use the SSH key to login to the EC2 instance
6. Install Java:

```
sudo add-apt-repository ppa:linuxuprising/java
sudo apt-get update
sudo apt-get install oracle-java11-installer
```

7. Install JMeter using:

```
sudo apt-get install jmeter
```

8. Get the JMeter Plugins:

```
wget http://jmeter-plugins.org/downloads/file/JMeterPlugins-
↪Standard-1.2.0.zip
wget http://jmeter-plugins.org/downloads/file/JMeterPlugins-
↪Extras-1.2.0.zip
wget http://jmeter-plugins.org/downloads/file/JMeterPlugins-
↪ExtrasLibs-1.2.0.zip
```

9. Move the unzipped jar files to the install location:

```
sudo unzip JMeterPlugins-Standard-1.2.0.zip -d /usr/share/jmeter/
sudo unzip JMeterPlugins-Extras-1.2.0.zip -d /usr/share/jmeter/
sudo unzip JMeterPlugins-ExtrasLibs-1.2.0.zip -d /usr/share/
↪jmeter/
```

10. Copy the JML file to the EC2 instance using:

    (On host computer)

```
scp -i <path_to_key> <path_to_local_file> <user>@<server_url>:
↪<path_on_server>
```

11. Run JMeter without the GUI:

```
jmeter -n -t <path_to_jmx> -l <path_to_output_jtl>
```

12. Copy the JTL file back to the host computer and view the file using JMeter with GUI

Python script to create test plan:

1. Navigate to the txGenerator folder in the in3-tests repo.
2. Run the main.py file while referencing the start block (-s), end block (-e) and number of blocks to choose in this range (-n). The script will randomly choose three transactions per block.

3. The transactions chosen are sent through a tumble function, resulting in a randomized list of transactions from random blocks. This should be a realistic scenario to test with, and prevents too many concurrent cache hits.
4. Import the generated CSV file into the loaded test plan on JMeter.
5. Refer to existing test plans for information on how to read transactions from CSV files and to see how it can be integrated into the requests.

6.2 Considerations

- When the Incubed benchmark is run on a new server, create a baseline before applying any changes.
- Run the same benchmark test with the new codebase, test for performance gains.
- The tests can be modified to include the number of users and duration of the test. For a stress test, choose 200 users and a test duration of 500 seconds or more.
- When running in an EC2 instance, up to 500 users can be simulated without issues. Running in GUI mode reduces this number.
- A beneficial method for running the test is to slowly ramp up the user count. Start with a test of 10 users for 120 seconds in order to test basic stability. Work your way up to 200 users and longer durations.
- Parity might often be the bottleneck; you can confirm this by using the get_avg_stddev_in3_response.sh script in the scripts directory of the in3-test repo. This would help show what optimizations are needed.

6.3 Results/Baseline

- The baseline test was done with our existing server running multiple docker containers. It is not indicative of a perfect server setup, but it can be used to benchmark upgrades to our codebase.
- The baseline for our current system is given below. This system has multithreading enabled and has been tested with ethCalls included in the test plan.

Users/duration	Number of requests	tps	getBlockByHash (ms)	getBlockByNumber (ms)	getTransactionHash (ms)	getTransactionReceipt (ms)	EthCall(ms)	eth_getStorage (ms)	Notes
10/120s									
20/120s	4800	40	580	419	521	923	449	206	
40/120s	5705	47	1020	708	902	1508	816	442	
80/120s	7970	66	1105	790	2451	3197	984	452	
100/120s	6911	57	1505	1379	2501	4310	1486	866	
110/120s	6000	50	1789	1646	4204	5662	1811	1007	
120/500s	32000	65	1331	1184	4600	5314	1815	1607	
140/500s	31000	62	1666	1425	5207	6722	1760	941	
160/500s	33000	65	1949	1615	6269	7604	1900	930	In3 -> 400ms, rpc -> 2081ms
200/500s	34000	70	1270	1031	12500	14349	1251	716	At higher loads, the RPC delay adds up. It is the bottlenecking factor. Able to handle 200 users on sustained loads.

- More benchmarks and their results can be found in the in3-tests repo

CHAPTER 7

Embedded Devices

7.1 Hardware Requirements

7.1.1 Memory

For the memory this example requires:

- Dynamic memory(DRAM) : 30 - 50kB
- Flash Memory : 150 - 200kB

7.1.2 Networking

In3 client needs to have a reliable internet connection to work properly, so your hardware must support any network interface or module that could give you access to it. i.e Bluetooth, Wifi, ethernet, etc.

7.2 Incubed with ESP-IDF

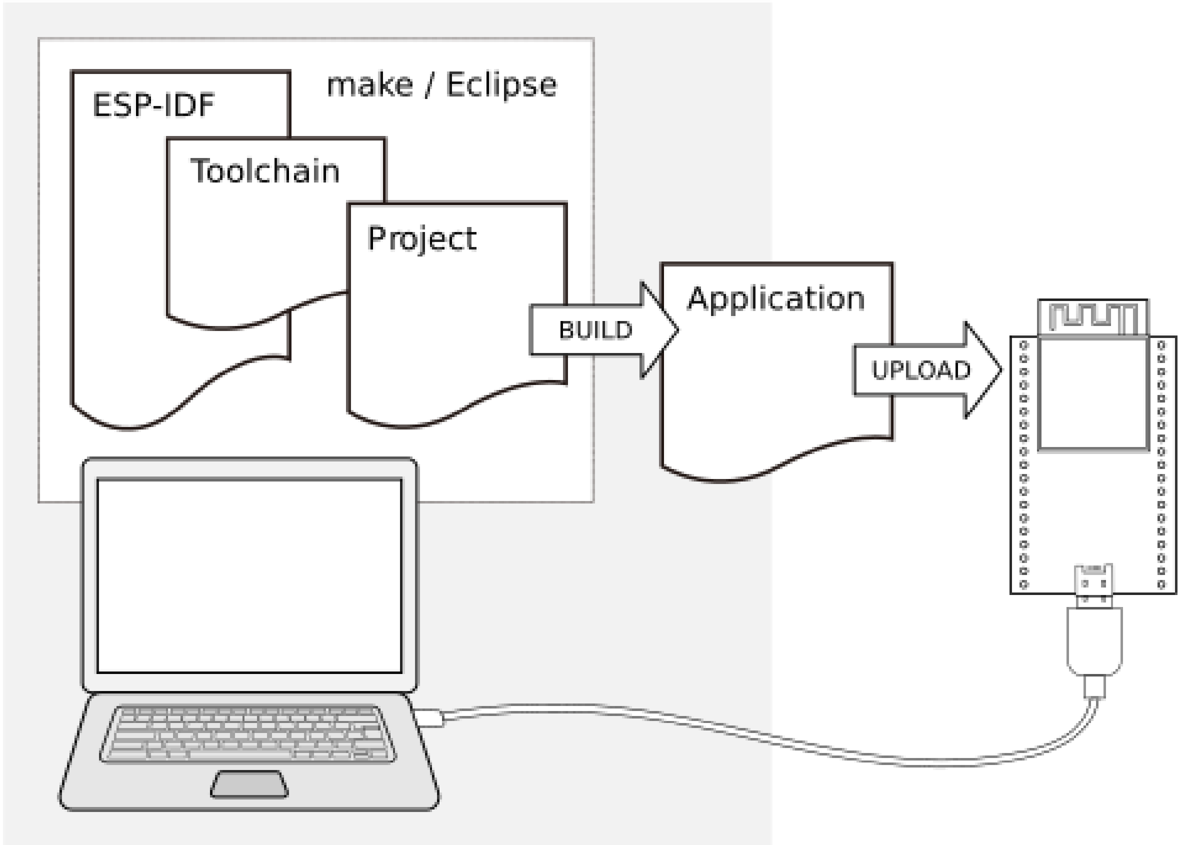
7.2.1 Use case example: Airbnb Property access

A smart door lock that grants access to a rented flat is installed on the property. It is able to connect to the Internet to check if renting is allowed and that the current user is authorized to open the lock.

The computational power of the control unit is restricted to the control of the lock. And it is also needed to maintain a permanent Internet connection.

You want to enable this in your application as an example of how in3 can help you, we will guide through the steps of doing it, from the very basics and the resources you will need

Hardware requirements



from https://docs.espressif.com/projects/esp-idf/en/stable/get-started/

- ESP32-DevKitC V4 or similar dev board
- Android phone
- Laptop MAC, Linux, Windows
- USB Cable

Software requirements

- In3 C client
- Esp-idf toolchain and sdk, (please follow this guide) and be sure on the cloning step to use `release/v4.0` branch

```
git clone -b release/v4.0 --recursive https://github.com/espressif/esp-idf.git
```

- Android Studio
- Solidity smart contract: we will control access to properties using a public smart contract, for this example, we will use the following template
- Silab USB drivers

```
pragma solidity ^0.5.1;

contract Access {
    uint8 access;
```

(continues on next page)

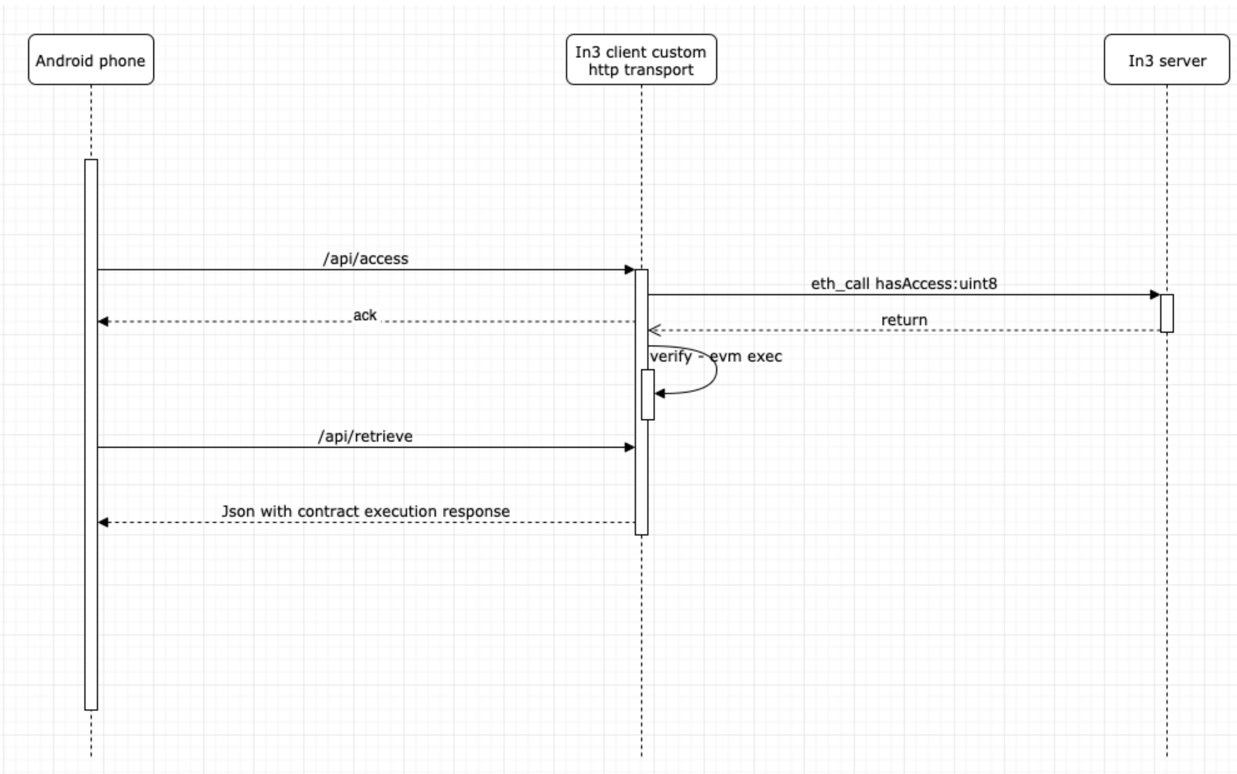
(continued from previous page)

```
    constructor() public  {
        access = 0;
    }

    function hasAccess() public view returns(uint8) {
        return access;
    }

    function setAccess(uint8 accessUpdate) public{
        access = accessUpdate;
    }
}
```

How it works



sequence diagram

In3 will support a wide range of microcontrollers, in this guide we will use well-known esp32 with freertos framework, and an example android app to interact with it via Wifi connection.

Instalation instructions

1. Clone the repo

```
git clone --recursive https://github.com/slockit/in3-devices-esp
```

1. Deploy the contract with your favorite tool (truffle, etc) or use our previously deployed contract on goerli, with address `0x36643F8D17FE745a69A2Fd22188921Fade60a98B`
2. Config your SSID and password inside sdkconfig file `sdkconfig.defaults`

```
CONFIG_WIFI_SSID="YOUR SSID"
CONFIG_WIFI_PASSWORD="YOUR PWD"
```

1. Build the code `idf.py build`
2. Connect the usb cable to flash and monitor the serial output from the application.

```
idf.py flash && idf.py monitor
```

after the build finishes and the serial monitor is running you will see the configuration and init logs.

1. Configure the ip address of the example, to work with: Take a look at the inital output of the serial output of the `idf.py monitor` command, you will the ip address, as follows

```
I (2647) tcpip_adapter: sta ip: 192.168.178.64, mask: 255.255.255.0, gw: 192.168.178.1
I (2647) IN3: got ip:192.168.178.64
```

take note if your ip address which will be used in the android application example.

1. Clone the android repository, compile the android application and install the in3 demo application in your phone.

```
git clone https://github.com/slockit/in3-android-example
```

1. Modify the android source changing ip address variable inside kotlin source file `MainActivity.kt`, with the IP address found on step 6.

```
(L:20) private const val ipaddress = "http://192.168.xx.xx"
```

1. If you want to test directly without using android you can also do it with the following http curl requests:

- `curl -X GET http://slock.local/api/access`
- `curl -X GET http://slock.local/api/retrieve`

we need 2 requests as the verification process needs to be executed in asynchronous manner, first one will trigger the execution and the result could be retrieved with the second one

7.3 Incubed with Zephyr

. . . .(Comming soon)

CHAPTER 8

API Reference C

8.1 Overview

The C implementation of the Incubed client is prepared and optimized to run on small embedded devices. Because each device is different, we prepare different modules that should be combined. This allows us to only generate the code needed and reduce requirements for flash and memory.

8.1.1 Why C?

We have been asked a lot, why we implemented Incubed in C and not in Rust. When we started Incubed we began with a feasibility test and wrote the client in TypeScript. Once we confirmed it was working, we wanted to provide a minimal verifaction client for embedded devices. And yes, we actually wanted to do it in Rust, since Rust offers a lot of safety-features (like the memory-management at compiletime, thread-safety, . . .), but after considering a lot of different aspects we made a pragmatic desicion to use C.

These are the reasons why:

Support for embedded devices.

As of today almost all toolchain used in the embedded world are build for C. Even though Rust may be able to still use some, there are a lot of issues. Quote from rust-embedded.org:

Integrating Rust with an RTOS such as FreeRTOS or ChibiOS is still a work in progress; especially calling RTOS functions from Rust can be tricky.

This may change in the future, but C is so dominant, that chances of Rust taking over the embedded development completly is low.

Portability

C is the most portable programming language. Rust actually has a pretty admirable selection of supported targets for a new language (thanks mostly to LLVM), but it pales in comparison to C, which runs on almost everything. A new

CPU architecture or operating system can barely be considered to exist until it has a C compiler. And once it does, it unlocks access to a vast repository of software written in C. Many other programming languages, such as Ruby and Python, are implemented in C and you get those for free too.

Most programing language have very good support for calling c-function in a shared library (like ctypes in python or cgo in golang) or even support integration of C code directly like android studio does.

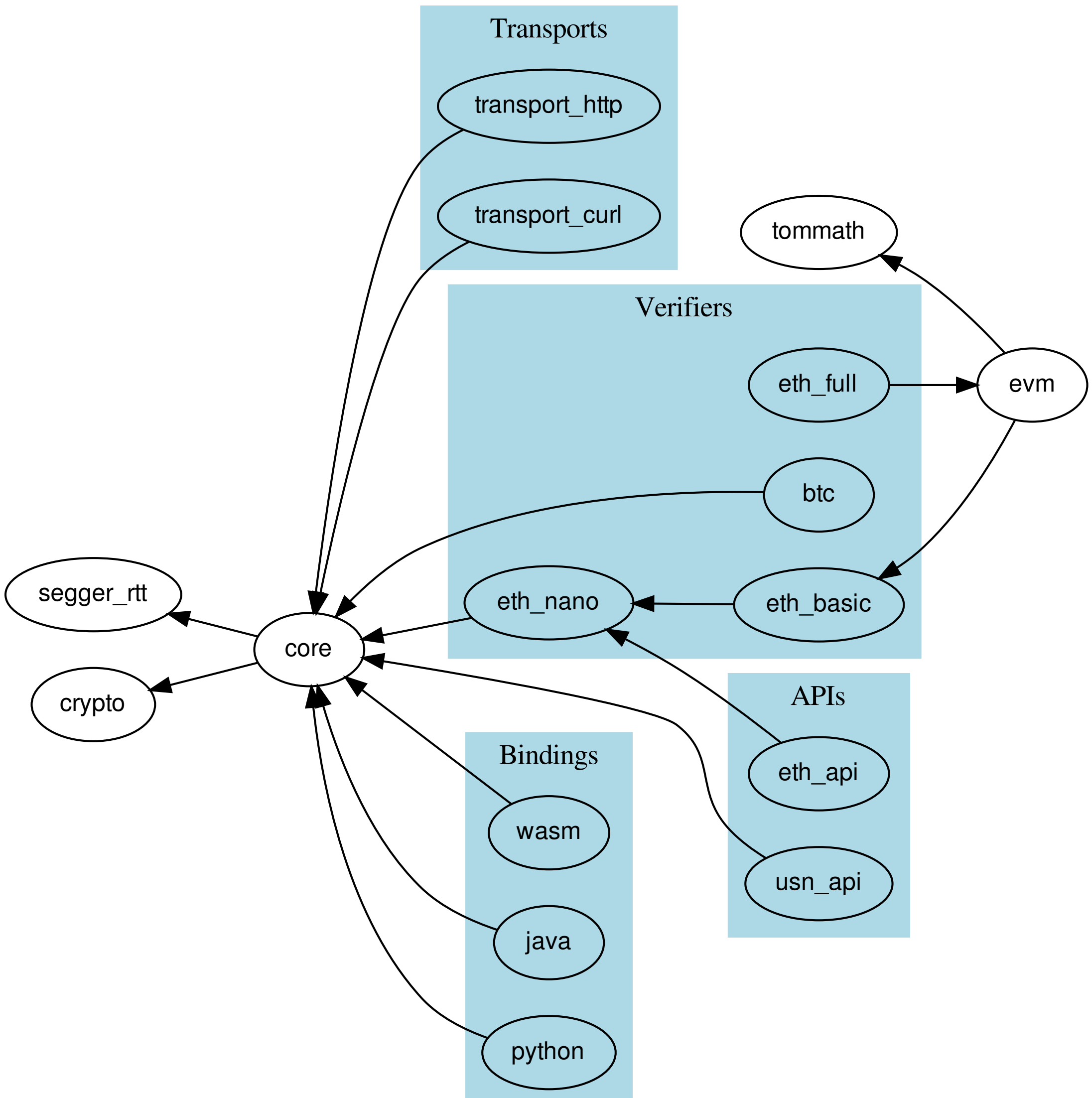
Integration in existing projects

Since especially embedded systems are usually written in C/C++, offering a pure C-Implementation makes it easy for these projects to use Incubed, since they do not have to change their toolchain.

Even though we may not be able to use a lot of great features Rust offers by going with C, it allows to reach the goal to easily integrate with a lot of projects. For the future we might port the incubed to Rust if we see a demand or chance for the same support as C has today.

8.1.2 Modules

Incubed consists of different modules. While the core module is always required, additional functions will be prepared by different modules.



Verifier

Incubed is a minimal verification client, which means that each response needs to be verifiable. Depending on the expected requests and responses, you need to carefully choose which verifier you may need to register. For Ethereum, we have developed three modules:

1. *eth_nano*: a minimal module only able to verify transaction receipts (`eth_getTransactionReceipt`).
2. *eth_basic*: module able to verify almost all other standard RPC functions (except `eth_call`).
3. *eth_full*: module able to verify standard RPC functions. It also implements a full EVM to handle `eth_call`.
4. *btc*: module able to verify bitcoin or bitcoin based chains.

Depending on the module, you need to register the verifier before using it. This is done by calling the `in3_register...` function like *in3_register_eth_full()*.

Transport

To verify responses, you need to be able to send requests. The way to handle them depends heavily on your hardware capabilities. For example, if your device only supports Bluetooth, you may use this connection to deliver the request to a device with an existing internet connection and get the response in the same way, but if your device is able to use a direct internet connection, you may use a curl-library to execute them. This is why the core client only defines function pointer *in3_transport_send*, which must handle the requests.

At the moment we offer these modules; other implementations are supported by different hardware modules.

1. *transport_curl*: module with a dependency on curl, which executes these requests and supports HTTPS. This module runs a standard OS with curl installed.
2. *transport_http*: module with no dependency, but a very basic http-implementation (no https-support)

API

While Incubed operates on JSON-RPC level, as a developer, you might want to use a better-structured API to prepare these requests for you. These APIs are optional but make life easier:

1. ***eth***: This module offers all standard RPC functions as described in the Ethereum JSON-RPC Specification. In addition, it allows you to sign and encode/decode calls and transactions.
2. ***usn***: This module offers basic USN functions like renting, event handling, and message verification.

8.2 Building

While we provide binaries, you can also build from source:

8.2.1 requirements

- cmake
- curl : curl is used as transport for command-line tools.
- optional: libsycrypt, which would be used for unlocking keystore files using `scrypt` as kdf method. if it does not exist you can still build, but not decrypt such keys.

for osx `brew install libscrypt` and for debian `sudo apt-get install libscrypt-dev`

Incubed uses cmake for configuring:

```
mkdir build && cd build
cmake -DCMAKE_BUILD_TYPE=Release .. && make
make install
```

8.2.2 CMake options

When configuring cmake, you can set a lot of different incubed specific like `cmake -DEVM_GAS=false ..`.

ASMJS

compiles the code as asm.js.

Default-Value: `-DASMJS=OFF`

BUILD_DOC

generates the documenation with doxygen.

Default-Value: `-DBUILD_DOC=OFF`

CMD

build the comandline utils

Default-Value: `-DCMD=ON`

ERR_MSG

if set human readable error messages will be inculded in th executable, otherwise only the error code is used. (saves about 19kB)

Default-Value: `-DERR_MSG=ON`

ETH_BASIC

build basic eth verification.(all rpc-calls except eth_call)

Default-Value: `-DETH_BASIC=ON`

ETH_FULL

build full eth verification.(including eth_call)

Default-Value: `-DETH_FULL=ON`

ETH_NANO

build minimal eth verification.(eth_getTransactionReceipt)

Default-Value: `-DETH_NANO=ON`

EVM_GAS

if true the gas costs are verified when validating a eth_call. This is a optimization since most calls are only interessted in the result. EVM_GAS would be required if the contract uses gas-dependend op-codes.

Default-Value: `-DEVM_GAS=ON`

FAST_MATH

Math optimizations used in the EVM. This will also increase the filesize.

Default-Value: `-DFAST_MATH=OFF`

FILTER_NODES

if true the nodelist is filtered against config node properties

Default-Value: `-DFILTER_NODES=OFF`

IN3API

build the USN-API which offer better interfaces and additional functions on top of the pure verification

Default-Value: `-DIN3API=ON`

IN3_LIB

if true a shared anmd static library with all in3-modules will be build.

Default-Value: `-DIN3_LIB=ON`

IN3_SERVER

support for proxy server as part of the cmd-tool, which allows to start the cmd-tool with the -p option and listens to the given port for rpc-requests

Default-Value: `-DIN3_SERVER=OFF`

IN3_STAGING

if true, the client will use the staging-network instead of the live ones

Default-Value: `-DIN3_STAGING=OFF`

JAVA

build the java-binding (shared-lib and jar-file)

Default-Value: `-DJAVA=OFF`

PKG_CONFIG_EXECUTABLE

pkg-config executable

Default-Value: `-DPKG_CONFIG_EXECUTABLE=/usr/local/bin/pkg-config`

POA

support POA verification including validatorlist updates

Default-Value: `-DPOA=OFF`

SEGGER_RTT

Use the segger real time transfer terminal as the logging mechanism

Default-Value: `-DSEGGER_RTT=OFF`

TAG_VERSION

the tagged version, which should be used

Default-Value: `-DTAG_VERSION=OFF`

TEST

builds the tests and also adds special memory-management, which detects memory leaks, but will cause slower performance

Default-Value: `-DTEST=OFF`

TRANSPORTS

builds transports, which may require extra libraries.

Default-Value: `-DTRANSPORTS=ON`

USE_CURL

if true the curl transport will be build (with a dependency to libcurl)

Default-Value: `-DUSE_CURL=ON`

USE_PRECOMPUTED_EC

if true the secp256k1 curve uses precompiled tables to boost performance. turning this off makes ecrecover slower, but saves about 37kb.

Default-Value: `-DUSE_PRECOMPUTED_EC=ON`

USE_SCRYPT

if scrypt is installed, it will link dynamicly to the shared scrypt lib.

Default-Value: `-DUSE_SCRYPT=OFF`

WASM

Includes the WASM-Build. In order to build it you need emscripten as toolchain. Usually you also want to turn off other builds in this case.

Default-Value: `-DWASM=OFF`

WASM_EMBED

embedds the wasm as base64-encoded into the js-file

Default-Value: `-DWASM_EMBED=ON`

WASM_EMMALLOC

use ther smaller EMSCRIPTEN Malloc, which reduces the size about 10k, but may be a bit slower

Default-Value: `-DWASM_EMMALLOC=ON`

WASM_SYNC

intiaializes the WASM synchronisly, which allows to require and use it the same function, but this will not be supported by chrome (4k limit)

Default-Value: `-DWASM_SYNC=OFF`

8.3 Examples

8.3.1 call_a_function

source : in3-c/examples/c/call_a_function.c

This example shows how to call functions on a smart contract eiither directly or using the api to encode the arguments

```
#include <in3/client.h>   // the core client
#include <in3/eth_api.h>  // wrapper for easier use
#include <in3/eth_full.h> // the full ethereum verifier containing the EVM
#include <in3/in3_curl.h> // transport implementation
#include <in3/log.h>
#include <inttypes.h>
#include <stdio.h>

static in3_ret_t call_func_rpc(in3_t* c);
static in3_ret_t call_func_api(in3_t* c, address_t contract);

int main() {
  in3_ret_t ret = IN3_OK;

  // register a chain-verifier for full Ethereum-Support in order to verify eth_call
  // this needs to be called only once.
  in3_register_eth_full();
```

(continues on next page)

(continued from previous page)

```
  // use curl as the default for sending out requests
  // this needs to be called only once.
  in3_register_curl();

  // Remove log prefix for readability
  in3_log_set_prefix("");

  // create new incubed client
  in3_t* c = in3_for_chain(ETH_CHAIN_ID_MAINNET);

  // define a address (20byte)
  address_t contract;

  // copy the hexcoded string into this address
  hex_to_bytes("0x2736D225f85740f42D17987100dc8d58e9e16252", -1, contract, 20);

  // call function using RPC
  ret = call_func_rpc(c);
  if (ret != IN3_OK) goto END;

  // call function using API
  ret = call_func_api(c, contract);
  if (ret != IN3_OK) goto END;

END:
  // clean up
  in3_free(c);
  return 0;
}

in3_ret_t call_func_rpc(in3_t* c) {
  // prepare 2 pointers for the result.
  char *result, *error;

  // send raw rpc-request, which is then verified
  in3_ret_t res = in3_client_rpc(
      c,                                                                          ␣
↪                 //  the configured client
      "eth_call",                                                                 ␣
↪                 // the rpc-method you want to call.
      "[{\"to\":\"0x2736d225f85740f42d17987100dc8d58e9e16252\", \"data\":\"0x15625c5e\
↪"}, \"latest\"]", // the signed raw txn, same as the one used in the API example
      &result,                                                                    ␣
↪                 // the reference to a pointer which will hold the result
      &error);                                                                    ␣
↪                 // the pointer which may hold a error message

  // check and print the result or error
  if (res == IN3_OK) {
    printf("Result: \n%s\n", result);
    free(result);
    return 0;
  } else {
    printf("Error sending tx: \n%s\n", error);
    free(error);
    return IN3_EUNKNOWN;
  }
```

(continues on next page)

(continued from previous page)

```
}

in3_ret_t call_func_api(in3_t* c, address_t contract) {
  // ask for the number of servers registered
  json_ctx_t* response = eth_call_fn(c, contract, BLKNUM_LATEST(),
↪"totalServers():uint256");
  if (!response) {
    printf("Could not get the response: %s", eth_last_error());
    return IN3_EUNKNOWN;
  }

  // convert the response to a uint32_t,
  uint32_t number_of_servers = d_int(response->result);

  // clean up resources
  json_free(response);

  // output
  printf("Found %u servers registered : \n", number_of_servers);

  // read all structs ...
  for (uint32_t i = 0; i < number_of_servers; i++) {
    response = eth_call_fn(c, contract, BLKNUM_LATEST(), "servers(uint256):(string,
↪address,uint,uint,uint,address)", to_uint256(i));
    if (!response) {
      printf("Could not get the response: %s", eth_last_error());
      return IN3_EUNKNOWN;
    }

    char*     url     = d_get_string_at(response->result, 0); // get the first item of␣
↪the result (the url)
    bytes_t* owner   = d_get_bytes_at(response->result, 1);  // get the second item␣
↪of the result (the owner)
    uint64_t deposit = d_get_long_at(response->result, 2);   // get the third item of␣
↪the result (the deposit)

    printf("Server %i : %s owner = %02x%02x...", i, url, owner->data[0], owner->
↪data[1]);
    printf(", deposit = %" PRIu64 "\n", deposit);

    // free memory
    json_free(response);
  }
  return 0;
}
```

8.3.2 get_balance

source : in3-c/examples/c/get_balance.c

get the Balance with the API and also as direct RPC-call

```

#include <in3/client.h>    // the core client
#include <in3/eth_api.h>   // wrapper for easier use
```

(continues on next page)

(continued from previous page)

```
#include <in3/eth_basic.h> // use the basic module
#include <in3/in3_curl.h>  // transport implementation

#include <stdio.h>

static void get_balance_rpc(in3_t* in3);
static void get_balance_api(in3_t* in3);

int main() {

  // register a chain-verifier for basic Ethereum-Support, which is enough to verify␣
↪accounts
  // this needs to be called only once
  in3_register_eth_basic();

  // use curl as the default for sending out requests
  // this needs to be called only once.
  in3_register_curl();

  // create new incubed client
  in3_t* in3 = in3_for_chain(ETH_CHAIN_ID_MAINNET);

  // get balance using raw RPC call
  get_balance_rpc(in3);

  // get balance using API
  get_balance_api(in3);

  // cleanup client after usage
  in3_free(in3);
}

void get_balance_rpc(in3_t* in3) {
  // prepare 2 pointers for the result.
  char *result, *error;

  // send raw rpc-request, which is then verified
  in3_ret_t res = in3_client_rpc(
      in3,                                                          //  the␣
↪configured client
      "eth_getBalance",                                             // the rpc-
↪method you want to call.
      "[\"0xc94770007dda54cF92009BFF0dE90c06F603a09f\", \"latest\"]", // the␣
↪arguments as json-string
      &result,                                                      // the␣
↪reference to a pointer whill hold the result
      &error);                                                      // the pointer␣
↪which may hold a error message

  // check and print the result or error
  if (res == IN3_OK) {
    printf("Balance: \n%s\n", result);
    free(result);
  } else {
    printf("Error getting balance: \n%s\n", error);
    free(error);
  }
```

(continues on next page)

(continued from previous page)

```
}

void get_balance_api(in3_t* in3) {
  // the address of account whose balance we want to get
  address_t account;
  hex_to_bytes("0xc94770007dda54cF92009BFF0dE90c06F603a09f", -1, account, 20);

  // get balance of account
  long double balance = as_double(eth_getBalance(in3, account, BLKNUM_EARLIEST()));

  // if the result is null there was an error an we can get the latest error message␣
↪from eth_lat_error()
  balance ? printf("Balance: %Lf\n", balance) : printf("error getting the balance :
↪%s\n", eth_last_error());
}
```

8.3.3 get_block

source : in3-c/examples/c/get_block.c

using the basic-module to get and verify a Block with the API and also as direct RPC-call

```

#include <in3/client.h>    // the core client
#include <in3/eth_api.h>   // wrapper for easier use
#include <in3/eth_basic.h> // use the basic module
#include <in3/in3_curl.h>  // transport implementation

#include <inttypes.h>
#include <stdio.h>

static void get_block_rpc(in3_t* in3);
static void get_block_api(in3_t* in3);

int main() {

  // register a chain-verifier for basic Ethereum-Support, which is enough to verify␣
↪blocks
  // this needs to be called only once
  in3_register_eth_basic();

  // use curl as the default for sending out requests
  // this needs to be called only once.
  in3_register_curl();

  // create new incubed client
  in3_t* in3 = in3_for_chain(ETH_CHAIN_ID_MAINNET);

  // get block using raw RPC call
  get_block_rpc(in3);

  // get block using API
  get_block_api(in3);

  // cleanup client after usage
```

(continues on next page)

(continued from previous page)

```
  in3_free(in3);
}

void get_block_rpc(in3_t* in3) {
  // prepare 2 pointers for the result.
  char *result, *error;

  // send raw rpc-request, which is then verified
  in3_ret_t res = in3_client_rpc(
      in3,                    //  the configured client
      "eth_getBlockByNumber", // the rpc-method you want to call.
      "[\"latest\",true]",    // the arguments as json-string
      &result,                // the reference to a pointer whill hold the result
      &error);                // the pointer which may hold a error message

  // check and print the result or error
  if (res == IN3_OK) {
    printf("Latest block : \n%s\n", result);
    free(result);
  } else {
    printf("Error verifing the Latest block : \n%s\n", error);
    free(error);
  }
}

void get_block_api(in3_t* in3) {
  // get the block without the transaction details
  eth_block_t* block = eth_getBlockByNumber(in3, BLKNUM(8432424), false);

  // if the result is null there was an error an we can get the latest error message␣
↪from eth_lat_error()
  if (!block)
    printf("error getting the block : %s\n", eth_last_error());
  else {
    printf("Number of transactions in Block #%llu: %d\n", block->number, block->tx_
↪count);
    free(block);
  }
}
```

8.3.4 get_logs

source : in3-c/examples/c/get_logs.c

fetching events and verify them with eth_getLogs

```

#include <in3/client.h>    // the core client
#include <in3/eth_api.h>   // wrapper for easier use
#include <in3/eth_basic.h> // use the basic module
#include <in3/in3_curl.h>  // transport implementation

#include <inttypes.h>
#include <stdio.h>

```

(continues on next page)

(continued from previous page)

```
static void get_logs_rpc(in3_t* in3);
static void get_logs_api(in3_t* in3);

int main() {

  // register a chain-verifier for basic Ethereum-Support, which is enough to verify␣
↪logs
  // this needs to be called only once
  in3_register_eth_basic();

  // use curl as the default for sending out requests
  // this needs to be called only once.
  in3_register_curl();

  // create new incubed client
  in3_t* in3     = in3_for_chain(ETH_CHAIN_ID_MAINNET);
  in3->chain_id = ETH_CHAIN_ID_KOVAN;

  // get logs using raw RPC call
  get_logs_rpc(in3);

  // get logs using API
  get_logs_api(in3);

  // cleanup client after usage
  in3_free(in3);
}

void get_logs_rpc(in3_t* in3) {
  // prepare 2 pointers for the result.
  char *result, *error;

  // send raw rpc-request, which is then verified
  in3_ret_t res = in3_client_rpc(
      in3,           //  the configured client
      "eth_getLogs", // the rpc-method you want to call.
      "[{}]",        // the arguments as json-string
      &result,       // the reference to a pointer whill hold the result
      &error);       // the pointer which may hold a error message

  // check and print the result or error
  if (res == IN3_OK) {
    printf("Logs : \n%s\n", result);
    free(result);
  } else {
    printf("Error getting logs : \n%s\n", error);
    free(error);
  }
}

void get_logs_api(in3_t* in3) {
  // Create filter options
  char b[30];
  sprintf(b, "{\"fromBlock\":\"0x%" PRIx64 "\"}", eth_blockNumber(in3) - 2);
  json_ctx_t* jopt = parse_json(b);

  // Create new filter with options
```

(continues on next page)

(continued from previous page)

```
  size_t fid = eth_newFilter(in3, jopt);

  // Get logs
  eth_log_t* logs = NULL;
  in3_ret_t  ret  = eth_getFilterLogs(in3, fid, &logs);
  if (ret != IN3_OK) {
    printf("eth_getFilterLogs() failed [%d]\n", ret);
    return;
  }

  // print result
  while (logs) {
    eth_log_t* l = logs;
    printf("--------------------------------------------------------------------------------
↪------\n");
    printf("\tremoved: %s\n", l->removed ? "true" : "false");
    printf("\tlogId: %lu\n", l->log_index);
    printf("\tTxId: %lu\n", l->transaction_index);
    printf("\thash: ");
    ba_print(l->block_hash, 32);
    printf("\n\tnum: %" PRIu64 "\n", l->block_number);
    printf("\taddress: ");
    ba_print(l->address, 20);
    printf("\n\tdata: ");
    b_print(&l->data);
    printf("\ttopics[%lu]: ", l->topic_count);
    for (size_t i = 0; i < l->topic_count; i++) {
      printf("\n\t");
      ba_print(l->topics[i], 32);
    }
    printf("\n");
    logs = logs->next;
    free(l->data.data);
    free(l->topics);
    free(l);
  }
  eth_uninstallFilter(in3, fid);
  json_free(jopt);
}
```

8.3.5 get_transaction

source : in3-c/examples/c/get_transaction.c

checking the transaction data

```

#include <in3/client.h>    // the core client
#include <in3/eth_api.h>   // wrapper for easier use
#include <in3/eth_basic.h> // use the basic module
#include <in3/in3_curl.h>  // transport implementation

#include <stdio.h>

static void get_tx_rpc(in3_t* in3);
```

(continues on next page)

(continued from previous page)

```
static void get_tx_api(in3_t* in3);

int main() {

  // register a chain-verifier for basic Ethereum-Support, which is enough to verify␣
↪txs
  // this needs to be called only once
  in3_register_eth_basic();

  // use curl as the default for sending out requests
  // this needs to be called only once.
  in3_register_curl();

  // create new incubed client
  in3_t* in3 = in3_for_chain(ETH_CHAIN_ID_MAINNET);

  // get tx using raw RPC call
  get_tx_rpc(in3);

  // get tx using API
  get_tx_api(in3);

  // cleanup client after usage
  in3_free(in3);
}

void get_tx_rpc(in3_t* in3) {
  // prepare 2 pointers for the result.
  char *result, *error;

  // send raw rpc-request, which is then verified
  in3_ret_t res = in3_client_rpc(
      in3,                                                                      // ␣
↪the configured client
      "eth_getTransactionByHash",                                               //␣
↪the rpc-method you want to call.
      "[\"0xdd80249a0631cf0f1593c7a9c9f9b8545e6c88ab5252287c34bc5d12457eab0e\"]", //␣
↪the arguments as json-string
      &result,                                                                  //␣
↪the reference to a pointer which will hold the result
      &error);                                                                  //␣
↪the pointer which may hold a error message

  // check and print the result or error
  if (res == IN3_OK) {
    printf("Latest tx : \n%s\n", result);
    free(result);
  } else {
    printf("Error verifing the Latest tx : \n%s\n", error);
    free(error);
  }
}

void get_tx_api(in3_t* in3) {
  // the hash of transaction that we want to get
  bytes32_t tx_hash;
  hex_to_bytes("0xdd80249a0631cf0f1593c7a9c9f9b8545e6c88ab5252287c34bc5d12457eab0e", -
↪1, tx_hash, 32);
```

(continues on next page)

(continued from previous page)

```
  // get the tx by hash
  eth_tx_t* tx = eth_getTransactionByHash(in3, tx_hash);

  // if the result is null there was an error an we can get the latest error message␣
↪from eth_last_error()
  if (!tx)
    printf("error getting the tx : %s\n", eth_last_error());
  else {
    printf("Transaction #%d of block #%llx", tx->transaction_index, tx->block_number);
    free(tx);
  }
}
```

8.3.6 get_transaction_receipt

source : in3-c/examples/c/get_transaction_receipt.c

validating the result or receipt of an transaction

```
#include <in3/client.h>    // the core client
#include <in3/eth_api.h>   // wrapper for easier use
#include <in3/eth_basic.h> // use the basic module
#include <in3/in3_curl.h>  // transport implementation

#include <inttypes.h>
#include <stdio.h>

static void get_tx_receipt_rpc(in3_t* in3);
static void get_tx_receipt_api(in3_t* in3);

int main() {

  // register a chain-verifier for basic Ethereum-Support, which is enough to verify␣
↪tx receipts
  // this needs to be called only once
  in3_register_eth_basic();

  // use curl as the default for sending out requests
  // this needs to be called only once.
  in3_register_curl();

  // create new incubed client
  in3_t* in3 = in3_for_chain(ETH_CHAIN_ID_MAINNET);

  // get tx receipt using raw RPC call
  get_tx_receipt_rpc(in3);

  // get tx receipt using API
  get_tx_receipt_api(in3);

  // cleanup client after usage
  in3_free(in3);
}
```

(continues on next page)

(continued from previous page)

```
void get_tx_receipt_rpc(in3_t* in3) {
  // prepare 2 pointers for the result.
  char *result, *error;

  // send raw rpc-request, which is then verified
  in3_ret_t res = in3_client_rpc(
      in3,                                                                         // ␣
↪the configured client
      "eth_getTransactionReceipt",                                                 //␣
↪the rpc-method you want to call.
      "[\"0xdd80249a0631cf0f1593c7a9c9f9b8545e6c88ab5252287c34bc5d12457eab0e\"]", //␣
↪the arguments as json-string
      &result,                                                                     //␣
↪the reference to a pointer which will hold the result
      &error);                                                                     //␣
↪the pointer which may hold a error message

  // check and print the result or error
  if (res == IN3_OK) {
    printf("Transaction receipt: \n%s\n", result);
    free(result);
  } else {
    printf("Error verifing the tx receipt: \n%s\n", error);
    free(error);
  }
}

void get_tx_receipt_api(in3_t* in3) {
  // the hash of transaction whose receipt we want to get
  bytes32_t tx_hash;
  hex_to_bytes("0xdd80249a0631cf0f1593c7a9c9f9b8545e6c88ab5252287c34bc5d12457eab0e", -
↪1, tx_hash, 32);

  // get the tx receipt by hash
  eth_tx_receipt_t* txr = eth_getTransactionReceipt(in3, tx_hash);

  // if the result is null there was an error an we can get the latest error message␣
↪from eth_last_error()
  if (!txr)
    printf("error getting the tx : %s\n", eth_last_error());
  else {
    printf("Transaction #%d of block #%llx, gas used = %" PRIu64 ", status = %s\n",␣
↪txr->transaction_index, txr->block_number, txr->gas_used, txr->status ? "success" :
↪"failed");
    eth_tx_receipt_free(txr);
  }
}
```

8.3.7 send_transaction

source : in3-c/examples/c/send_transaction.c

sending a transaction including signing it with a private key

```
#include <in3/client.h>    // the core client
#include <in3/eth_api.h>   // wrapper for easier use
#include <in3/eth_basic.h> // use the basic module
#include <in3/in3_curl.h>  // transport implementation
#include <in3/signer.h>    // default signer implementation

#include <stdio.h>

// fixme: This is only for the sake of demo. Do NOT store private keys as plaintext.
#define ETH_PRIVATE_KEY
↪"0x8da4ef21b864d2cc526dbdb2a120bd2874c36c9d0a1fb7f8c63d7f7a8b41de8f"

static void send_tx_rpc(in3_t* in3);
static void send_tx_api(in3_t* in3);

int main() {

  // register a chain-verifier for basic Ethereum-Support, which is enough to verify␣
↪txs
  // this needs to be called only once
  in3_register_eth_basic();

  // use curl as the default for sending out requests
  // this needs to be called only once.
  in3_register_curl();

  // create new incubed client
  in3_t* in3 = in3_for_chain(ETH_CHAIN_ID_MAINNET);

  // convert the hexstring to bytes
  bytes32_t pk;
  hex_to_bytes(ETH_PRIVATE_KEY, -1, pk, 32);

  // create a simple signer with this key
  eth_set_pk_signer(in3, pk);

  // send tx using raw RPC call
  send_tx_rpc(in3);

  // send tx using API
  send_tx_api(in3);

  // cleanup client after usage
  in3_free(in3);
}

void send_tx_rpc(in3_t* in3) {
  // prepare 2 pointers for the result.
  char *result, *error;

  // send raw rpc-request, which is then verified
  in3_ret_t res = in3_client_rpc(
      in3,                      //  the configured client
      "eth_sendRawTransaction", // the rpc-method you want to call.
      "[\"0xf892808609184e72a0008296c094d46e8dd67c5d32be8058bb8eb970870f0724456"

↪"7849184e72aa9d46e8dd67c5d32be8d46e8dd67c5d32be8058bb8eb970870f072445675058bb8eb9"
```

(continues on next page)

(continued from previous page)

```
↪"70870f07244567526a06f0103fccdcae0d6b265f8c38ee42f4a722c1cb36230fe8da40315acc3051"
        "9a8a06252a68b26a5575f76a65ac08a7f684bc37b0c98d9e715d73ddce696b58f2c72\"]", //␣
↪the signed raw txn, same as the one used in the API example
        &result,                                                              //␣
↪the reference to a pointer which will hold the result
        &error);                                                              //␣
↪the pointer which may hold a error message

  // check and print the result or error
  if (res == IN3_OK) {
    printf("Result: \n%s\n", result);
    free(result);
  } else {
    printf("Error sending tx: \n%s\n", error);
    free(error);
  }
}

void send_tx_api(in3_t* in3) {
  // prepare parameters
  address_t to, from;
  hex_to_bytes("0x63FaC9201494f0bd17B9892B9fae4d52fe3BD377", -1, from, 20);
  hex_to_bytes("0xd46e8dd67c5d32be8058bb8eb970870f07244567", -1, to, 20);

  bytes_t* data = hex_to_new_bytes(
↪"d46e8dd67c5d32be8d46e8dd67c5d32be8058bb8eb970870f072445675058bb8eb970870f072445675
↪", 82);

  // send the tx
  bytes_t* tx_hash = eth_sendTransaction(in3, from, to, OPTIONAL_T_VALUE(uint64_t,␣
↪0x96c0), OPTIONAL_T_VALUE(uint64_t, 0x9184e72a000), OPTIONAL_T_VALUE(uint256_t, to_
↪uint256(0x9184e72a)), OPTIONAL_T_VALUE(bytes_t, *data), OPTIONAL_T_UNDEFINED(uint64_
↪t));

  // if the result is null there was an error and we can get the latest error message␣
↪from eth_last_error()
  if (!tx_hash)
    printf("error sending the tx : %s\n", eth_last_error());
  else {
    printf("Transaction hash: ");
    b_print(tx_hash);
    b_free(tx_hash);
  }
  b_free(data);
}
```

8.3.8 usn_device

source : in3-c/examples/c/usn_device.c

a example how to watch usn events and act upon it.

```
#include <in3/client.h>   // the core client
```

(continues on next page)

(continued from previous page)

```
#include <in3/eth_api.h>  // wrapper for easier use
#include <in3/eth_full.h> // the full ethereum verifier containing the EVM
#include <in3/in3_curl.h> // transport implementation
#include <in3/signer.h>   // signer-api
#include <in3/usn_api.h>  // api for renting
#include <inttypes.h>
#include <stdio.h>
#include <time.h>
#if defined(_WIN32) || defined(WIN32)
#include <windows.h>
#else
#include <unistd.h>
#endif

static int handle_booking(usn_event_t* ev) {
  printf("\n%s Booking timestamp=%" PRIu64 "\n", ev->type == BOOKING_START ? "START"␣
↪: "STOP", ev->ts);
  return 0;
}

int main(int argc, char* argv[]) {

  // register a chain-verifier for full Ethereum-Support in order to verify eth_call
  // this needs to be called only once.
  in3_register_eth_full();

  // use curl as the default for sending out requests
  // this needs to be called only once.
  in3_register_curl();

  // create new incubed client
  in3_t* c = in3_for_chain(ETH_CHAIN_ID_MAINNET);

  // switch to goerli
  c->chain_id = 0x5;

  // setting up a usn-device-config
  usn_device_conf_t usn;
  usn.booking_handler    = handle_booking;                                           //
↪ this is the handler, which is called for each rent/return or start/stop
  usn.c                  = c;                                                        //
↪ the incubed client
  usn.chain_id           = c->chain_id;                                              //
↪ the chain_id
  usn.devices            = NULL;                                                     //
↪ this will contain the list of devices supported
  usn.len_devices        = 0;                                                        //
↪ and length of this list
  usn.now                = 0;                                                        //
↪ the current timestamp
  unsigned int wait_time = 5;                                                        //
↪ the time to wait between the internval
  hex_to_bytes("0x85Ec283a3Ed4b66dF4da23656d4BF8A507383bca", -1, usn.contract, 20); //
↪ address of the usn-contract, which we copy from hex

  // register a usn-device
  usn_register_device(&usn, "office@slockit");
```

(continues on next page)

(continued from previous page)

```
  // now we run en endless loop which simply wait for events on the chain.
  printf("\n start watching...\n");
  while (true) {
    usn.now                = time(NULL);                               // update the
↪timestamp, since this is running on embedded devices, this may be depend on the
↪hardware.
    unsigned int timeout = usn_update_state(&usn, wait_time) * 1000; // this will now
↪check for new events and trigger the handle_booking if so.

    // sleep
#if defined(_WIN32) || defined(WIN32)
    Sleep(timeout);
#else
    nanosleep((const struct timespec[]){{0, timeout * 1000000L}}, NULL);
#endif
  }

  // clean up
  in3_free(c);
  return 0;
}
```

8.3.9 usn_rent

source : in3-c/examples/c/usn_rent.c

how to send a rent transaction to a usn contract usinig the usn-api.

```
#include <in3/client.h>   // the core client
#include <in3/eth_api.h>  // wrapper for easier use
#include <in3/eth_full.h> // the full ethereum verifier containing the EVM
#include <in3/in3_curl.h> // transport implementation
#include <in3/signer.h>   // signer-api
#include <in3/usn_api.h>  // api for renting
#include <inttypes.h>
#include <stdio.h>

void unlock_key(in3_t* c, char* json_data, char* passwd) {
  // parse the json
  json_ctx_t* key_data = parse_json(json_data);
  if (!key_data) {
    perror("key is not parseable!\n");
    exit(EXIT_FAILURE);
  }

  // decrypt the key
  uint8_t* pk = malloc(32);
  if (decrypt_key(key_data->result, passwd, pk) != IN3_OK) {
    perror("wrong password!\n");
    exit(EXIT_FAILURE);
  }

  // free json
```

(continues on next page)

(continued from previous page)

```
  json_free(key_data);

  // create a signer with this key
  eth_set_pk_signer(c, pk);
}

int main(int argc, char* argv[]) {

  // register a chain-verifier for full Ethereum-Support in order to verify eth_call
  // this needs to be called only once.
  in3_register_eth_full();

  // use curl as the default for sending out requests
  // this needs to be called only once.
  in3_register_curl();

  // create new incubed client
  in3_t* c = in3_for_chain(ETH_CHAIN_ID_GOERLI);

  // address of the usn-contract, which we copy from hex
  address_t contract;
  hex_to_bytes("0x85Ec283a3Ed4b66dF4da23656d4BF8A507383bca", -1, contract, 20);

  // read the key from args - I know this is not safe, but this is just a example.
  if (argc < 3) {
    perror("you need to provide a json-key and password to rent it");
    exit(EXIT_FAILURE);
  }
  char* key_data = argv[1];
  char* passwd   = argv[2];
  unlock_key(c, key_data, passwd);

  // rent it for one hour.
  uint32_t renting_seconds = 3600;

  // allocate 32 bytes for the resulting tx hash
  bytes32_t tx_hash;

  // start charging
  if (usn_rent(c, contract, NULL, "office@slockit", renting_seconds, tx_hash))
    printf("Could not start charging\n");
  else {
    printf("Charging tx successfully sent... tx_hash=0x");
    for (int i = 0; i < 32; i++) printf("%02x", tx_hash[i]);
    printf("\n");

    if (argc == 4) // just to include it : if you want to stop earlier, you can call
      usn_return(c, contract, "office@slockit", tx_hash);
  }

  // clean up
  in3_free(c);
  return 0;
}
```

8.3.10 Building

In order to run those examples, you only need a c-compiler (gcc or clang) and curl installed.

```
./build.sh
```

will build all examples in this directory. You can build them individually by executing:

```
gcc -o get_block_api get_block_api.c -lin3 -lcurl
```

8.4 RPC

The core of incubed is to execute rpc-requests which will be send to the incubed nodes and verified. This means the available RPC-Requests are defined by the clients itself.

- For Ethereum : https://github.com/ethereum/wiki/wiki/JSON-RPC
- For Bitcoin : https://bitcoincore.org/en/doc/0.18.0/

The Incbed nodes already add a few special RPC-methods, which are specified in the RPC-Specification Section of the Protocol.

In addition the incubed client itself offers special RPC-Methods, which are mostly handled directly inside the client:

8.4.1 in3_config

changes the configuration of a client. The configuration is passed as the first param and may contain only the values to change.

Parameters:

1. `config`: config-object - a Object with config-params.

The config params support the following properties :

- **autoUpdateList** :`boolean` *(optional)* - if true the nodelist will be automaticly updated if the lastBlock is newer example: true
- **chainId** :`string` - servers to filter for the given chain. The chain-id based on EIP-155. example: 0x1
- **finality** :`number` *(optional)* - the number in percent needed in order reach finality (% of signature of the validators) example: 50
- **includeCode** :`boolean` *(optional)* - if true, the request should include the codes of all accounts. otherwise only the the codeHash is returned. In this case the client may ask by calling eth_getCode() afterwards example: true
- **keepIn3** :`boolean` *(optional)* - if true, requests sent to the input sream of the comandline util will be send theor responses in the same form as the server did. example: false
- **key** :`any` *(optional)* - the client key to sign requests example: 0x387a8233c96e1fc0ad5e284353276177af2186e7afa85296f106336e
- **maxAttempts** :`number` *(optional)* - max number of attempts in case a response is rejected example: 10
- **maxBlockCache** :`number` *(optional)* - number of number of blocks cached in memory example: 100
- **maxCodeCache** :`number` *(optional)* - number of max bytes used to cache the code in memory example: 100000
- **minDeposit** :`number` - min stake of the server. Only nodes owning at least this amount will be chosen.

- **nodeLimit** :`number` *(optional)* - the limit of nodes to store in the client. example: 150
- **proof** :,'none, | 'standard' | 'full'' *(optional)* - if true the nodes should send a proof of the response example: true
- **replaceLatestBlock** :`number` *(optional)* - if specified, the blocknumber *latest* will be replaced by blockNumber- specified value example: 6
- **requestCount** :`number` - the number of request send when getting a first answer example: 3
- **rpc** :`string` *(optional)* - url of one or more rpc-endpoints to use. (list can be comma seperated)
- **servers** *(optional)* - the nodelist per chain
- **signatureCount** :`number` *(optional)* - number of signatures requested example: 2
- **verifiedHashes** :`string`[] *(optional)* - if the client sends a array of blockhashes the server will not deliver any signatures or blockheaders for these blocks, but only return a string with a number. This is automaticly updated by the cache, but can be overriden per request.

Returns:

an boolean confirming that the config has changed.

Example:

Request:

```
{
  "method":"in3_config",
  "params":[{
      "chainId":"0x5",
      "maxAttempts":4,
      "nodeLimit":10
      "servers":{
          "0x1": [
              "nodeList": [
                  {
                    "address":"0x1234567890123456789012345678901234567890",
                    "url":"https://mybootnode-A.com",
                    "props":"0xFFFF",
                  },
                  {
                    "address":"0x1234567890123456789012345678901234567890",
                    "url":"https://mybootnode-B.com",
                    "props":"0xFFFF",
                  }
              ]
          ]
      }

   }]
}
```

Response:

```
{
  "id": 1,
  "result": true,
}
```

8.4.2 in3_abiEncode

based on the ABI-encoding used by solidity, this function encodes the values and returns it as hex-string.

Parameters:

1. `signature`: string - the signature of the function. e.g. `getBalance(uint256)`. The format is the same as used by solidity to create the functionhash. optional you can also add the return type, which in this case is ignored.
2. `params`: array - a array of arguments. the number of arguments must match the arguments in the signature.

Returns:

the ABI-encoded data as hex including the 4 byte function-signature. These data can be used for `eth_call` or to send a transaction.

Request:

```
{
    "method":"in3_abiEncode",
    "params":[
        "getBalance(address)",
        ["0x1234567890123456789012345678901234567890"]
    ]
}
```

Response:

```
{
  "id": 1,
  "result":
↪"0xf8b2cb4f0000000000000000000000001234567890123456789012345678901234567890",
}
```

8.4.3 in3_abiDecode

based on the ABI-encoding used by solidity, this function decodes the bytes given and returns it as array of values.

Parameters:

1. `signature`: string - the signature of the function. e.g. `uint256`, `(address,string,uint256)` or `getBalance(address):uint256`. If the complete functionhash is given, only the return-part will be used.
2. `data`: hex - the data to decode (usually the result of a eth_call)

Returns:

a array (if more then one arguments in the result-type) or the the value after decodeing.

Request:

```
{
    "method":"in3_abiDecode",
    "params":[
        "(address,uint256)",

↪"0x0000000000000000000000001234567890123456789012345678901234567890000000000000000000000000000000000
↪"
```

(continues on next page)

(continued from previous page)

```
    ]
}
```

Response:

```
{
  "id": 1,
  "result": ["0x123456789012345678901234567890","0x05"],
}
```

8.4.4 in3_checksumAddress

Will convert an upper or lowercase Ethereum address to a checksum address. (See EIP55)

Parameters:

1. `address`: address - the address to convert.
2. `useChainId`: boolean - if true, the chainId is integrated as well (See EIP1191)

Returns:

the address-string using the upper/lowercase hex characters.

Request:

```
{
    "method":"in3_checksumAddress",
    "params":[
        "0x1fe2e9bf29aa1938859af64c413361227d04059a",
        false
    ]
}
```

Response:

```
{
  "id": 1,
  "result": "0x1Fe2E9bf29aa1938859Af64C413361227d04059a"
}
```

8.4.5 in3_ens

resolves a ens-name. the domain names consist of a series of dot-separated labels. Each label must be a valid normalised label as described in UTS46 with the options `transitional=false` and `useSTD3AsciiRules=true`. For Javascript implementations, a library is available that normalises and checks names.

Parameters:

1. `name`: string - the domain name UTS46 compliant string.
2. `field`: string - the required data, which could be

- `addr` - the address (default)
- `resolver` - the address of the resolver

- `hash` - the namehash
- `owner` - the owner of the domain

Returns:

the address-string using the upper/lowercase hex characters.

Request:

```
{
    "method":"in3_ens",
    "params":[
        "cryptokitties.eth",
        "addr"
    ]
}
```

Response:

```
{
  "id": 1,
  "result": "0x06012c8cf97bead5deae237070f9587f8e7a266d"
}
```

8.5 Module api/eth1

8.5.1 eth_api.h

Ethereum API.

This header-file defines easy to use function, which are preparing the JSON-RPC-Request, which is then executed and verified by the incubed-client.

File: src/api/eth1/eth_api.h

BLKNUM (blk)

Initializer macros for eth_blknum_t.

```
#define BLKNUM (blk) ((eth_blknum_t){.u64 = blk, .is_u64 = true})
```

BLKNUM_LATEST ()

```
#define BLKNUM_LATEST () ((eth_blknum_t){.def = BLK_LATEST, .is_u64 = false})
```

BLKNUM_EARLIEST ()

```
#define BLKNUM_EARLIEST () ((eth_blknum_t){.def = BLK_EARLIEST, .is_u64 = false})
```

BLKNUM_PENDING ()

```
#define BLKNUM_PENDING () ((eth_blknum_t){.def = BLK_PENDING, .is_u64 = false})
```

eth_tx_t

A transaction.

The stuct contains following fields:

bytes32_t	**hash**	the blockhash
bytes32_t	**block_hash**	hash of ther containnig block
`uint64_t`	**block_number**	number of the containing block
address_t	**from**	sender of the tx
`uint64_t`	**gas**	gas send along
`uint64_t`	**gas_price**	gas price used
bytes_t	**data**	data send along with the transaction
`uint64_t`	**nonce**	nonce of the transaction
address_t	**to**	receiver of the address 0x0000. . -Address is used for contract creation.
uint256_t	**value**	the value in wei send
`int`	**transaction_index**	the transaction index
`uint8_t`	**signature**	signature of the transaction

eth_block_t

An Ethereum Block.

The stuct contains following fields:

`uint64_t`	**number**	the blockNumber
bytes32_t	**hash**	the blockhash
`uint64_t`	**gasUsed**	gas used by all the transactions
`uint64_t`	**gasLimit**	gasLimit
address_t	**author**	the author of the block.
uint256_t	**difficulty**	the difficulty of the block.
bytes_t	**extra_data**	the extra_data of the block.
`uint8_t`	**logsBloom**	the logsBloom-data
bytes32_t	**parent_hash**	the hash of the parent-block
bytes32_t	**sha3_uncles**	root hash of the uncle-trie
bytes32_t	**state_root**	root hash of the state-trie
bytes32_t	**receipts_root**	root of the receipts trie
bytes32_t	**transaction_root**	root of the transaction trie
`int`	**tx_count**	number of transactions in the block
eth_tx_t *	**tx_data**	array of transaction data or NULL if not requested
bytes32_t *	**tx_hashes**	array of transaction hashes or NULL if not requested
`uint64_t`	**timestamp**	the unix timestamp of the block
bytes_t *	**seal_fields**	sealed fields
`int`	**seal_fields_count**	number of seal fields

eth_log_t

A linked list of Ethereum Logs

The stuct contains following fields:

`bool`	**removed**	true when the log was removed, due to a chain reorganization. false if its a valid log
`size_t`	**log_index**	log index position in the block
`size_t`	**transaction_index**	transactions index position log was created from
bytes32_t	**transaction_hash**	hash of the transactions this log was created from
bytes32_t	**block_hash**	hash of the block where this log was in
`uint64_t`	**block_number**	the block number where this log was in
address_t	**address**	address from which this log originated
bytes_t	**data**	non-indexed arguments of the log
*bytes32_t **	**topics**	array of 0 to 4 32 Bytes DATA of indexed log arguments
`size_t`	**topic_count**	counter for topics
*eth_logstruct , **	**next**	pointer to next log in list or NULL

eth_tx_receipt_t

A transaction receipt.

The stuct contains following fields:

bytes32_t	**transaction_hash**	the transaction hash
`int`	**transaction_index**	the transaction index
bytes32_t	**block_hash**	hash of ther containnig block
`uint64_t`	**block_number**	number of the containing block
`uint64_t`	**cumulative_gas_used**	total amount of gas used by block
`uint64_t`	**gas_used**	amount of gas used by this specific transaction
*bytes_t **	**contract_address**	contract address created (if the transaction was a contract creation) or NULL
`bool`	**status**	1 if transaction succeeded, 0 otherwise.
*eth_log_t **	**logs**	array of log objects, which this transaction generated

DEFINE_OPTIONAL_T

```
DEFINE_OPTIONAL_T(uint64_t);
```

Optional types.

arguments:

`uint64_t`

returns: ‘‘

DEFINE_OPTIONAL_T

```
DEFINE_OPTIONAL_T(bytes_t);
```

arguments:

bytes_t

returns: ‘‘

DEFINE_OPTIONAL_T

```
DEFINE_OPTIONAL_T(address_t);
```

arguments:

address_t

returns: ‘‘

DEFINE_OPTIONAL_T

```
DEFINE_OPTIONAL_T(uint256_t);
```

arguments:

uint256_t

returns: ‘‘

eth_getStorageAt

```
uint256_t eth_getStorageAt(in3_t *in3, address_t account, bytes32_t key, eth_blknum_t␣
↪block);
```

Returns the storage value of a given address.

arguments:

*in3_t **	**in3**
address_t	**account**
bytes32_t	**key**
eth_blknum_t	**block**

returns: `uint256_t`

eth_getCode

```
bytes_t eth_getCode(in3_t *in3, address_t account, eth_blknum_t block);
```

Returns the code of the account of given address.

(Make sure you free the data-point of the result after use.)

arguments:

*in3_t **	**in3**
address_t	**account**
eth_blknum_t	**block**

returns: `bytes_t`

eth_getBalance

```
uint256_t eth_getBalance(in3_t *in3, address_t account, eth_blknum_t block);
```

Returns the balance of the account of given address.

arguments:

*in3_t **	**in3**
address_t	**account**
eth_blknum_t	**block**

returns: `uint256_t`

eth_blockNumber

```
uint64_t eth_blockNumber(in3_t *in3);
```

Returns the current price per gas in wei.

arguments:

*in3_t **	**in3**

returns: `uint64_t`

eth_gasPrice

```
uint64_t eth_gasPrice(in3_t *in3);
```

Returns the current blockNumber, if bn==0 an error occured and you should check eth_last_error()

arguments:

*in3_t **	**in3**

returns: `uint64_t`

eth_getBlockByNumber

```
eth_block_t* eth_getBlockByNumber(in3_t *in3, eth_blknum_t number, bool include_tx);
```

Returns the block for the given number (if number==0, the latest will be returned).

If result is null, check eth_last_error()! otherwise make sure to free the result after using it!

arguments:

*in3_t **	**in3**
eth_blknum_t	**number**
`bool`	**include_tx**

returns: *eth_block_t **

eth_getBlockByHash

```
eth_block_t* eth_getBlockByHash(in3_t *in3, bytes32_t hash, bool include_tx);
```

Returns the block for the given hash.

If result is null, check eth_last_error()! otherwise make sure to free the result after using it!

arguments:

*in3_t **	**in3**
bytes32_t	**hash**
`bool`	**include_tx**

returns: *eth_block_t **

eth_getLogs

```
eth_log_t* eth_getLogs(in3_t *in3, char *fopt);
```

Returns a linked list of logs.

If result is null, check eth_last_error()! otherwise make sure to free the log, its topics and data after using it!

arguments:

*in3_t **	**in3**
`char *`	**fopt**

returns: *eth_log_t **

eth_newFilter

```
in3_ret_t eth_newFilter(in3_t *in3, json_ctx_t *options);
```

Creates a new event filter with specified options and returns its id (>0) on success or 0 on failure.

arguments:

*in3_t **	**in3**
*json_ctx_t **	**options**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==`IN3_OK`)

eth_newBlockFilter

```
in3_ret_t eth_newBlockFilter(in3_t *in3);
```

Creates a new block filter with specified options and returns its id (>0) on success or 0 on failure.

arguments:

*in3_t **	**in3**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==`IN3_OK`)

eth_newPendingTransactionFilter

```
in3_ret_t eth_newPendingTransactionFilter(in3_t *in3);
```

Creates a new pending txn filter with specified options and returns its id on success or 0 on failure.

arguments:

*in3_t **	**in3**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==`IN3_OK`)

eth_uninstallFilter

```
bool eth_uninstallFilter(in3_t *in3, size_t id);
```

Uninstalls a filter and returns true on success or false on failure.

arguments:

*in3_t **	**in3**
`size_t`	**id**

returns: `bool`

eth_getFilterChanges

```
in3_ret_t eth_getFilterChanges(in3_t *in3, size_t id, bytes32_t **block_hashes, eth_
↪log_t **logs);
```

Sets the logs (for event filter) or blockhashes (for block filter) that match a filter; returns <0 on error, otherwise no.

of block hashes matched (for block filter) or 0 (for log filter)

arguments:

*in3_t **	**in3**
`size_t`	**id**
*bytes32_t ***	**block_hashes**
*eth_log_t ***	**logs**

returns: *`in3_ret_t`* the *result-status* of the function.

Please make sure you check if it was successfull (`==IN3_OK`)

eth_getFilterLogs

```
in3_ret_t eth_getFilterLogs(in3_t *in3, size_t id, eth_log_t **logs);
```

Sets the logs (for event filter) or blockhashes (for block filter) that match a filter; returns <0 on error, otherwise no.

of block hashes matched (for block filter) or 0 (for log filter)

arguments:

*in3_t **	**in3**
`size_t`	**id**
*eth_log_t ***	**logs**

returns: *`in3_ret_t`* the *result-status* of the function.

Please make sure you check if it was successfull (`==IN3_OK`)

eth_chainId

```
uint64_t eth_chainId(in3_t *in3);
```

Returns the currently configured chain id.

arguments:

*in3_t **	**in3**

returns: `uint64_t`

eth_getBlockTransactionCountByHash

```
uint64_t eth_getBlockTransactionCountByHash(in3_t *in3, bytes32_t hash);
```

Returns the number of transactions in a block from a block matching the given block hash.

arguments:

*in3_t **	**in3**
bytes32_t	**hash**

returns: `uint64_t`

eth_getBlockTransactionCountByNumber

```
uint64_t eth_getBlockTransactionCountByNumber(in3_t *in3, eth_blknum_t block);
```

Returns the number of transactions in a block from a block matching the given block number.

arguments:

*in3_t **	**in3**
eth_blknum_t	**block**

returns: `uint64_t`

eth_call_fn

```
json_ctx_t* eth_call_fn(in3_t *in3, address_t contract, eth_blknum_t block, char *fn_
↪sig,...);
```

Returns the result of a function_call.

If result is null, check eth_last_error()! otherwise make sure to free the result after using it with json_free()!

arguments:

*in3_t **	**in3**
address_t	**contract**
eth_blknum_t	**block**
`char *`	**fn_sig**
`...`	

returns: `json_ctx_t *`

eth_estimate_fn

```
uint64_t eth_estimate_fn(in3_t *in3, address_t contract, eth_blknum_t block, char *fn_
↪sig,...);
```

Returns the result of a function_call.

If result is null, check eth_last_error()! otherwise make sure to free the result after using it with json_free()!

arguments:

*in3_t **	**in3**
address_t	**contract**
eth_blknum_t	**block**
`char *`	**fn_sig**
`...`	

returns: `uint64_t`

eth_getTransactionByHash

```
eth_tx_t* eth_getTransactionByHash(in3_t *in3, bytes32_t tx_hash);
```

Returns the information about a transaction requested by transaction hash.

If result is null, check eth_last_error()! otherwise make sure to free the result after using it!

arguments:

*in3_t **	**in3**
bytes32_t	**tx_hash**

returns: *eth_tx_t **

eth_getTransactionByBlockHashAndIndex

```
eth_tx_t* eth_getTransactionByBlockHashAndIndex(in3_t *in3, bytes32_t block_hash,␣
↪size_t index);
```

Returns the information about a transaction by block hash and transaction index position.

If result is null, check eth_last_error()! otherwise make sure to free the result after using it!

arguments:

*in3_t **	**in3**
bytes32_t	**block_hash**
`size_t`	**index**

returns: *eth_tx_t **

eth_getTransactionByBlockNumberAndIndex

```
eth_tx_t* eth_getTransactionByBlockNumberAndIndex(in3_t *in3, eth_blknum_t block,␣
↪size_t index);
```

Returns the information about a transaction by block number and transaction index position.

If result is null, check eth_last_error()! otherwise make sure to free the result after using it!

arguments:

*in3_t **	**in3**
eth_blknum_t	**block**
`size_t`	**index**

returns: *eth_tx_t **

eth_getTransactionCount

```
uint64_t eth_getTransactionCount(in3_t *in3, address_t address, eth_blknum_t block);
```

Returns the number of transactions sent from an address.

arguments:

*in3_t **	**in3**
address_t	**address**
eth_blknum_t	**block**

returns: `uint64_t`

eth_getUncleByBlockNumberAndIndex

```
eth_block_t* eth_getUncleByBlockNumberAndIndex(in3_t *in3, eth_blknum_t block, size_t␣
↪index);
```

Returns information about a uncle of a block by number and uncle index position.

If result is null, check eth_last_error()! otherwise make sure to free the result after using it!

arguments:

*in3_t **	**in3**
eth_blknum_t	**block**
`size_t`	**index**

returns: *eth_block_t **

eth_getUncleCountByBlockHash

```
uint64_t eth_getUncleCountByBlockHash(in3_t *in3, bytes32_t hash);
```

Returns the number of uncles in a block from a block matching the given block hash.

arguments:

*in3_t **	**in3**
bytes32_t	**hash**

returns: `uint64_t`

eth_getUncleCountByBlockNumber

```
uint64_t eth_getUncleCountByBlockNumber(in3_t *in3, eth_blknum_t block);
```

Returns the number of uncles in a block from a block matching the given block number.

arguments:

*in3_t **	**in3**
eth_blknum_t	**block**

returns: `uint64_t`

eth_sendTransaction

```
bytes_t* eth_sendTransaction(in3_t *in3, address_t from, address_t to, OPTIONAL_
→T(uint64_t) gas, OPTIONAL_T(uint64_t) gas_price, OPTIONAL_T(uint256_t) value,␣
→OPTIONAL_T(bytes_t) data, OPTIONAL_T(uint64_t) nonce);
```

Creates new message call transaction or a contract creation.

Returns (32 Bytes) - the transaction hash, or the zero hash if the transaction is not yet available. Free result after use with b_free().

arguments:

*in3_t **	**in3**
address_t	**from**
address_t	**to**
OPTIONAL_T(uint64_t)	**gas**
OPTIONAL_T(uint64_t)	**gas_price**
`(,)`	**value**
`(,)`	**data**
OPTIONAL_T(uint64_t)	**nonce**

returns: `bytes_t *`

eth_sendRawTransaction

```
bytes_t* eth_sendRawTransaction(in3_t *in3, bytes_t data);
```

Creates new message call transaction or a contract creation for signed transactions.

Returns (32 Bytes) - the transaction hash, or the zero hash if the transaction is not yet available. Free after use with b_free().

arguments:

*in3_t **	**in3**
bytes_t	**data**

returns: `bytes_t *`

eth_getTransactionReceipt

```
eth_tx_receipt_t* eth_getTransactionReceipt(in3_t *in3, bytes32_t tx_hash);
```

Returns the receipt of a transaction by transaction hash.

Free result after use with eth_tx_receipt_free()

arguments:

*in3_t **	**in3**
bytes32_t	**tx_hash**

returns: `eth_tx_receipt_t *`

eth_wait_for_receipt

```
char* eth_wait_for_receipt(in3_t *in3, bytes32_t tx_hash);
```

Waits for receipt of a transaction requested by transaction hash.

arguments:

*in3_t **	**in3**
bytes32_t	**tx_hash**

returns: `char *`

eth_last_error

```
char* eth_last_error();
```

The current error or null if all is ok.

returns: `char *`

as_double

```
long double as_double(uint256_t d);
```

Converts a uint256_t in a long double.

Important: since a long double stores max 16 byte, there is no guarantee to have the full precision.

Converts a uint256_t in a long double.

arguments:

uint256_t	**d**

returns: `long double`

as_long

```
uint64_t as_long(uint256_t d);
```

Converts a uint256_t in a long .

Important: since a long double stores 8 byte, this will only use the last 8 byte of the value.

Converts a uint256_t in a long .

arguments:

uint256_t	**d**

returns: `uint64_t`

to_uint256

```
uint256_t to_uint256(uint64_t value);
```

Converts a uint64_t into its uint256_t representation.

arguments:

`uint64_t`	**value**

returns: *uint256_t*

decrypt_key

```
in3_ret_t decrypt_key(d_token_t *key_data, char *password, bytes32_t dst);
```

Decrypts the private key from a json keystore file using PBKDF2 or SCRYPT (if enabled)

arguments:

*d_token_t **	**key_data**
`char *`	**password**
bytes32_t	**dst**

returns: *in3_ret_t* the *result-status* of the function.

Please make sure you check if it was successfull (==IN3_OK)

log_free

```
void log_free(eth_log_t *log);
```

Frees a eth_log_t object.

arguments:

*eth_log_t **	**log**

eth_tx_receipt_free

```
void eth_tx_receipt_free(eth_tx_receipt_t *txr);
```

Frees a eth_tx_receipt_t object.

arguments:

*eth_tx_receipt_t **	**txr**

to_checksum

```
in3_ret_t to_checksum(address_t adr, chain_id_t chain_id, char out[43]);
```

converts the given address to a checksum address.

If chain_id is passed, it will use the EIP1191 to include it as well.

arguments:

address_t	**adr**
chain_id_t	**chain_id**
`char`	**out**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (`==IN3_OK`)

in3_register_eth_api

```
void in3_register_eth_api();
```

8.6 Module api/usn

8.6.1 usn_api.h

USN API.

This header-file defines easy to use function, which are verifying USN-Messages.

File: src/api/usn/usn_api.h

usn_booking_handler

```
typedef int(* usn_booking_handler) (usn_event_t *)
```

returns: `int(*`

usn_verify_message

```
usn_msg_result_t usn_verify_message(usn_device_conf_t *conf, char *message);
```

arguments:

*usn_device_conf_t **	**conf**
`char *`	**message**

returns: *usn_msg_result_t*

usn_register_device

```
in3_ret_t usn_register_device(usn_device_conf_t *conf, char *url);
```

arguments:

*usn_device_conf_t **	**conf**
`char *`	**url**

returns: *in3_ret_t* the *result-status* of the function.

Please make sure you check if it was successfull (==IN3_OK)

usn_parse_url

```
usn_url_t usn_parse_url(char *url);
```

arguments:

`char *`	**url**

returns: *usn_url_t*

usn_update_state

```
unsigned int usn_update_state(usn_device_conf_t *conf, unsigned int wait_time);
```

arguments:

*usn_device_conf_t **	**conf**
`unsigned int`	**wait_time**

returns: `unsigned int`

usn_update_bookings

```
in3_ret_t usn_update_bookings(usn_device_conf_t *conf);
```

arguments:

*usn_device_conf_t **	**conf**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==`IN3_OK`)

usn_remove_old_bookings

```
void usn_remove_old_bookings(usn_device_conf_t *conf);
```

arguments:

*usn_device_conf_t **	**conf**

usn_get_next_event

```
usn_event_t usn_get_next_event(usn_device_conf_t *conf);
```

arguments:

*usn_device_conf_t **	**conf**

returns: `usn_event_t`

usn_rent

```
in3_ret_t usn_rent(in3_t *c, address_t contract, address_t token, char *url, uint32_t␣
↪seconds, bytes32_t tx_hash);
```

arguments:

*in3_t **	**c**
address_t	**contract**
address_t	**token**
`char *`	**url**
`uint32_t`	**seconds**
bytes32_t	**tx_hash**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==`IN3_OK`)

usn_return

```
in3_ret_t usn_return(in3_t *c, address_t contract, char *url, bytes32_t tx_hash);
```

arguments:

*in3_t **	**c**
address_t	**contract**
`char *`	**url**
bytes32_t	**tx_hash**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==IN3_OK)

usn_price

```
in3_ret_t usn_price(in3_t *c, address_t contract, address_t token, char *url, uint32_
↪t seconds, address_t controller, bytes32_t price);
```

arguments:

*in3_t **	**c**
address_t	**contract**
address_t	**token**
`char *`	**url**
`uint32_t`	**seconds**
address_t	**controller**
bytes32_t	**price**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==IN3_OK)

8.7 Module core

8.7.1 client.h

this file defines the incubed configuration struct and it registration.

File: src/core/client/client.h

IN3_PROTO_VER

the protocol version used when sending requests from the this client

```
#define IN3_PROTO_VER "2.1.0"
```

ETH_CHAIN_ID_MULTICHAIN

chain_id working with all known chains

```
#define ETH_CHAIN_ID_MULTICHAIN 0x0
```

ETH_CHAIN_ID_MAINNET

chain_id for mainnet

```
#define ETH_CHAIN_ID_MAINNET 0x01
```

ETH_CHAIN_ID_KOVAN

chain_id for kovan

```
#define ETH_CHAIN_ID_KOVAN 0x2a
```

ETH_CHAIN_ID_TOBALABA

chain_id for tobalaba

```
#define ETH_CHAIN_ID_TOBALABA 0x44d
```

ETH_CHAIN_ID_GOERLI

chain_id for goerlii

```
#define ETH_CHAIN_ID_GOERLI 0x5
```

ETH_CHAIN_ID_EVAN

chain_id for evan

```
#define ETH_CHAIN_ID_EVAN 0x4b1
```

ETH_CHAIN_ID_IPFS

chain_id for ipfs

```
#define ETH_CHAIN_ID_IPFS 0x7d0
```

ETH_CHAIN_ID_VOLTA

chain_id for volta

```
#define ETH_CHAIN_ID_VOLTA 0x12046
```

ETH_CHAIN_ID_LOCAL

chain_id for local chain

```
#define ETH_CHAIN_ID_LOCAL 0xFFFF
```

in3_node_props_init (np)

Initializer for in3_node_props_t.

```
#define in3_node_props_init (np) *(np) = 0
```

IN3_SIGN_ERR_REJECTED

return value used by the signer if the the signature-request was rejected.

```
#define IN3_SIGN_ERR_REJECTED -1
```

IN3_SIGN_ERR_ACCOUNT_NOT_FOUND

return value used by the signer if the requested account was not found.

```
#define IN3_SIGN_ERR_ACCOUNT_NOT_FOUND -2
```

IN3_SIGN_ERR_INVALID_MESSAGE

return value used by the signer if the message was invalid.

```
#define IN3_SIGN_ERR_INVALID_MESSAGE -3
```

IN3_SIGN_ERR_GENERAL_ERROR

return value used by the signer for unspecified errors.

```
#define IN3_SIGN_ERR_GENERAL_ERROR -4
```

chain_id_t

type for a chain_id.

```
typedef uint32_t chain_id_t
```

in3_request_config_t

the configuration as part of each incubed request.

This will be generated for each request based on the client-configuration. the verifier may access this during verification in order to check against the request.

The stuct contains following fields:

chain_id_t	**chain_id**	the chain to be used. this is holding the integer-value of the hexstring.
`uint8_t`	**include_code**	if true the code needed will always be devlivered.
`uint8_t`	**use_full_proof**	this flaqg is set, if the proof is set to "PROOF_FULL"
`uint8_t`	**use_binary**	this flaqg is set, the client should use binary-format
*bytes_t **	**verified_hashes**	a list of blockhashes already verified. The Server will not send any proof for them again .
`uint16_t`	**verified_hashes_length**	number of verified blockhashes
`uint16_t`	**latest_block**	the last blocknumber the nodelistz changed
`uint16_t`	**finality**	number of signatures(in percent) needed in order to reach finality.
in3_verification_t	**verification**	Verification-type.
*bytes_t **	**client_signature**	the signature of the client with the client key
*bytes_t **	**signers**	the addresses of servers requested to sign the blockhash
`uint8_t`	**signers_length**	number or addresses
`uint32_t`	**time**	meassured time in ms for the request

in3_node_props_t

Node capabilities.

```
typedef uint64_t in3_node_props_t
```

in3_node_t

incubed node-configuration.

These information are read from the Registry contract and stored in this struct representing a server or node.

The stuct contains following fields:

*bytes_t **	**address**	address of the server
`uint64_t`	**deposit**	the deposit stored in the registry contract, which this would lose if it sends a wrong blockhash
`uint32_t`	**index**	index within the nodelist, also used in the contract as key
`uint32_t`	**capacity**	the maximal capacity able to handle
in3_node_props_t	**props**	used to identify the capabilities of the node. See in3_node_props_type_t in nodelist.h
`char *`	**url**	the url of the node
`bool`	**whitelisted**	boolean indicating if node exists in whiteList

in3_node_weight_t

Weight or reputation of a node.

Based on the past performance of the node a weight is calculated given faster nodes a higher weight and chance when selecting the next node from the nodelist. These weights will also be stored in the cache (if available)

The stuct contains following fields:

`uint32_t`	**response_count**	counter for responses
`uint32_t`	**total_response_time**	total of all response times
`uint64_t`	**blacklisted_until**	if >0 this node is blacklisted until k. k is a unix timestamp

in3_whitelist_t

defines a whitelist structure used for the nodelist.

The stuct contains following fields:

address_t	**contract**	address of whiteList contract. If specified, whiteList is always auto-updated and manual whiteList is overridden
bytes_t	**addresses**	serialized list of node addresses that constitute the whiteList
`uint64_t`	**last_block**	last blocknumber the whiteList was updated, which is used to detect changed in the whitelist
`bool`	**needs_update**	if true the nodelist should be updated and will trigger a *in3_nodeList*-request before the next request is send.

in3_verified_hash_t

represents a blockhash which was previously verified

The stuct contains following fields:

`uint64_t`	**block_number**	the number of the block
bytes32_t	**hash**	the blockhash

in3_chain_t

Chain definition inside incubed.

for incubed a chain can be any distributed network or database with incubed support.

The stuct contains following fields:

chain_id_t	**chain_id**	chain_id, which could be a free or based on the public ethereum networkId
in3_chain_type_t	**type**	chaintype
`uint64_t`	**last_block**	last blocknumber the nodeList was updated, which is used to detect changed in the nodelist
`int`	**nodelist_length**	number of nodes in the nodeList
*in3_node_t **	**nodelist**	array of nodes
*in3_node_weight_t **	**weights**	stats and weights recorded for each node
*bytes_t ***	**init_addresses**	array of addresses of nodes that should always part of the nodeList
*bytes_t **	**contract**	the address of the registry contract
bytes32_t	**registry_id**	the identifier of the registry
`uint8_t`	**version**	version of the chain
*in3_verified_hash_t **	**verified_hashes**	contains the list of already verified blockhashes
*in3_whitelist_t **	**whitelist**	if set the whitelist of the addresses.
address_t	**node**	node that reported the last_block which necessitated a nodeList update
`uint64_t`	**exp_last_block**	the last_block when the nodelist last changed reported by this node
`struct in3_chain::@2 *`	**nodelist_upd8_params**	

in3_storage_get_item

storage handler function for reading from cache.

```
typedef bytes_t*(* in3_storage_get_item) (void *cptr, char *key)
```

returns: `bytes_t *(*` : the found result. if the key is found this function should return the values as bytes otherwise `NULL`.

in3_storage_set_item

storage handler function for writing to the cache.

```
typedef void(* in3_storage_set_item) (void *cptr, char *key, bytes_t *value)
```

in3_storage_clear

storage handler function for clearing the cache.

```
typedef void(* in3_storage_clear) (void *cptr)
```

in3_storage_handler_t

storage handler to handle cache.

The stuct contains following fields:

in3_storage_get_item	**get_item**	function pointer returning a stored value for the given key.
in3_storage_set_item	**set_item**	function pointer setting a stored value for the given key.
in3_storage_clear	**clear**	function pointer clearing all contents of cache.
`void *`	**cptr**	custom pointer which will be passed to functions

in3_sign

signing function.

signs the given data and write the signature to dst. the return value must be the number of bytes written to dst. In case of an error a negativ value must be returned. It should be one of the IN3_SIGN_ERR... values.

```
typedef in3_ret_t(* in3_sign) (void *ctx, d_signature_type_t type, bytes_t message,␣
↪bytes_t account, uint8_t *dst)
```

returns: `in3_ret_t (*` the *result-status* of the function.

Please make sure you check if it was successfull (`==IN3_OK`)

in3_prepare_tx

transform transaction function.

for multisigs, we need to change the transaction to gro through the ms. if the new_tx is not set within the function, it will use the old_tx.

```
typedef in3_ret_t(* in3_prepare_tx) (void *ctx, d_token_t *old_tx, json_ctx_t **new_
↪tx)
```

returns: `in3_ret_t (*` the *result-status* of the function.

Please make sure you check if it was successfull (`==IN3_OK`)

in3_signer_t

The stuct contains following fields:

in3_sign	**sign**
in3_prepare_tx	**prepare_tx**
`void *`	**wallet**

in3_response_t

response-object.

if the error has a length>0 the response will be rejected

The stuct contains following fields:

sb_t	**error**	a stringbuilder to add any errors!
sb_t	**result**	a stringbuilder to add the result

in3_request_t

request-object.

represents a RPC-request

The stuct contains following fields:

`char *`	**payload**	the payload to send
`char **`	**urls**	array of urls
`int`	**urls_len**	number of urls
*in3_response_t **	**results**	the responses
`uint32_t`	**timeout**	the timeout 0= no timeout
`uint32_t *`	**times**	measured times (in ms) which will be used for ajusting the weights

in3_transport_send

the transport function to be implemented by the transport provider.

```
typedef in3_ret_t(* in3_transport_send) (in3_request_t *request)
```

returns: `in3_ret_t (*` the *result-status* of the function.

Please make sure you check if it was successfull (`==IN3_OK`)

in3_filter_t

The stuct contains following fields:

in3_filter_type_t	**type**	filter type: (event, block or pending)
`char *`	**options**	associated filter options
`uint64_t`	**last_block**	block no. when filter was created OR eth_getFilterChanges was called
`bool`	**is_first_usage**	if true the filter was not used previously
`void(*`	**release**	method to release owned resources

in3_filter_handler_t

Handler which is added to client config in order to handle filter.

The stuct contains following fields:

*in3_filter_t ***	**array**	
`size_t`	**count**	array of filters

in3_t

Incubed Configuration.

This struct holds the configuration and also point to internal resources such as filters or chain configs.

The stuct contains following fields:

`uint32_t`	**cache_timeout**	number of seconds requests can be cached.
`uint16_t`	**node_limit**	the limit of nodes to store in the client.
*bytes_t **	**key**	the client key to sign requests
`uint32_t`	**max_code_cache**	number of max bytes used to cache the code in memory
`uint32_t`	**max_block_cache**	number of number of blocks cached in memory
in3_proof_t	**proof**	the type of proof used
`uint8_t`	**request_count**	the number of request send when getting a first answer
`uint8_t`	**signature_count**	the number of signatures used to proof the blockhash.
`uint64_t`	**min_deposit**	min stake of the server. Only nodes owning at least this amount will be chosen.
`uint16_t`	**replace_latest_block**	if specified, the blocknumber *latest* will be replaced by blockNumber- specified value
`uint16_t`	**finality**	the number of signatures in percent required for the request
`uint_fast16_t`	**max_attempts**	the max number of attempts before giving up
`uint_fast16_t`	**max_verified_hashes**	max number of verified hashes to cache
`uint32_t`	**timeout**	specifies the number of milliseconds before the request times out. increasing may be helpful if the device uses a slow connection.
chain_id_t	**chain_id**	servers to filter for the given chain. The chain-id based on EIP-155.
`uint8_t`	**auto_update_list**	if true the nodelist will be automaticly updated if the last_block is newer
*in3_storage_handler_t **	**cache**	a cache handler offering 2 functions (setItem(string,string), getItem(string))
*in3_signer_t **	**signer**	signer-struct managing a wallet
in3_transport_send	**transport**	the transporthandler sending requests
`uint8_t`	**include_code**	includes the code when sending eth_call-requests
`uint8_t`	**use_binary**	if true the client will use binary format
`uint8_t`	**use_http**	if true the client will try to use http instead of https
`uint8_t`	**keep_in3**	if true the in3-section with the proof will also returned
*in3_chain_t **	**chains**	chain spec and nodeList definitions
`uint16_t`	**chains_length**	number of configured chains
*in3_filter_handler_t **	**filters**	filter handler
in3_node_props_t	**node_props**	used to identify the capabilities of the node.

in3_node_props_set

```
void in3_node_props_set(in3_node_props_t *node_props, in3_node_props_type_t type,␣
↪uint8_t value);
```

setter method for interacting with in3_node_props_t.

arguments:

*in3_node_props_t **	**node_props**
`in3_node_props_type_t`	**type**
`uint8_t`	**value**

in3_node_props_get

```
static uint32_t in3_node_props_get(in3_node_props_t np, in3_node_props_type_t t);
```

returns the value of the specified propertytype.

arguments:

in3_node_props_t	**np**
`in3_node_props_type_t`	**t**

returns: `uint32_t` : value as a number

in3_node_props_matches

```
static bool in3_node_props_matches(in3_node_props_t np, in3_node_props_type_t t);
```

checkes if the given type is set in the properties

arguments:

in3_node_props_t	**np**
`in3_node_props_type_t`	**t**

returns: `bool` : true if set

in3_new

```
in3_t* in3_new() __attribute__((deprecated("use in3_for_chain(ETH_CHAIN_ID_MULTICHAIN)
↪")));
```

creates a new Incubes configuration and returns the pointer.

This Method is depricated. you should use `in3_for_chain(ETH_CHAIN_ID_MULTICHAIN)` instead.

you need to free this instance with `in3_free` after use!

Before using the client you still need to set the tramsport and optional the storage handlers:

- example of initialization:

```
// register verifiers
in3_register_eth_full();

// create new client
in3_t* client = in3_new();

// configure storage...
in3_storage_handler_t storage_handler;
storage_handler.get_item = storage_get_item;
storage_handler.set_item = storage_set_item;
storage_handler.clear = storage_clear;

// configure transport
```

(continues on next page)

(continued from previous page)

```
client->transport    = send_curl;

// configure storage
client->cache = &storage_handler;

// init cache
in3_cache_init(client);

// ready to use ...
```

returns: *in3_t* *: the incubed instance.

in3_for_chain

```
in3_t* in3_for_chain(chain_id_t chain_id);
```

creates a new Incubes configuration for a specified chain and returns the pointer.

when creating the client only the one chain will be configured. (saves memory). but if you pass `ETH_CHAIN_ID_MULTICHAIN` as argument all known chains will be configured allowing you to switch between chains within the same client or configuring your own chain.

you need to free this instance with `in3_free` after use!

Before using the client you still need to set the tramsport and optional the storage handlers:

- example of initialization: , ** This Method is depricated. you should use `in3_for_chain` instead.**

```
// register verifiers
in3_register_eth_full();

// create new client
in3_t* client = in3_for_chain(ETH_CHAIN_ID_MAINNET);

// configure storage...
in3_storage_handler_t storage_handler;
storage_handler.get_item = storage_get_item;
storage_handler.set_item = storage_set_item;
storage_handler.clear = storage_clear;

// configure transport
client->transport    = send_curl;

// configure storage
client->cache = &storage_handler;

// init cache
in3_cache_init(client);

// ready to use ...
```

arguments:

chain_id_t	**chain_id**	the chain_id (see **ETH_CHAIN_ID_**... constants).

returns: *in3_t* *: the incubed instance.

in3_client_rpc

```
in3_ret_t in3_client_rpc(in3_t *c, char *method, char *params, char **result, char␣
↪**error);
```

sends a request and stores the result in the provided buffer

arguments:

*in3_t **	**c**	the pointer to the incubed client config.
`char *`	**method**	the name of the rpc-funcgtion to call.
`char *`	**params**	docs for input parameter v.
`char **`	**result**	pointer to string which will be set if the request was successfull. This will hold the result as json-rpc-string. (make sure you free this after use!)
`char **`	**error**	pointer to a string containg the error-message. (make sure you free it after use!)

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (`==IN3_OK`)

in3_client_exec_req

```
char* in3_client_exec_req(in3_t *c, char *req);
```

executes a request and returns result as string.

in case of an error, the error-property of the result will be set. The resulting string must be free by the the caller of this function!

arguments:

*in3_t **	**c**	the pointer to the incubed client config.
`char *`	**req**	the request as rpc.

returns: `char *`

in3_req_add_response

```
void in3_req_add_response(in3_response_t *res, int index, bool is_error, void *data,␣
↪int data_len);
```

adds a response for a request-object.

This function should be used in the transport-function to set the response.

arguments:

*in3_response_t **	**res**	the response-pointer
`int`	**index**	the index of the url, since this request could go out to many urls
`bool`	**is_error**	if true this will be reported as error. the message should then be the error-message
`void *`	**data**	the data or the the string
`int`	**data_len**	the length of the data or the the string (use -1 if data is a null terminated string)

in3_client_register_chain

```
in3_ret_t in3_client_register_chain(in3_t *client, chain_id_t chain_id, in3_chain_
↪type_t type, address_t contract, bytes32_t registry_id, uint8_t version, address_t␣
↪wl_contract);
```

registers a new chain or replaces a existing (but keeps the nodelist)

arguments:

*in3_t **	**client**	the pointer to the incubed client config.
chain_id_t	**chain_id**	the chain id.
in3_chain_type_t	**type**	the verification type of the chain.
address_t	**contract**	contract of the registry.
bytes32_t	**registry_id**	the identifier of the registry.
`uint8_t`	**version**	the chain version.
address_t	**wl_contract**	contract of whiteList.

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==`IN3_OK`)

in3_client_add_node

```
in3_ret_t in3_client_add_node(in3_t *client, chain_id_t chain_id, char *url, in3_node_
↪props_t props, address_t address);
```

adds a node to a chain ore updates a existing node

[in] public address of the signer.

arguments:

*in3_t **	**client**	the pointer to the incubed client config.
chain_id_t	**chain_id**	the chain id.
`char *`	**url**	url of the nodes.
in3_node_props_t	**props**	properties of the node.
address_t	**address**	

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==`IN3_OK`)

in3_client_remove_node

```
in3_ret_t in3_client_remove_node(in3_t *client, chain_id_t chain_id, address_t␣
↪address);
```

removes a node from a nodelist

[in] public address of the signer.

arguments:

*in3_t **	**client**	the pointer to the incubed client config.
chain_id_t	**chain_id**	the chain id.
address_t	**address**	

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (`==IN3_OK`)

in3_client_clear_nodes

```
in3_ret_t in3_client_clear_nodes(in3_t *client, chain_id_t chain_id);
```

removes all nodes from the nodelist

[in] the chain id.

arguments:

*in3_t **	**client**	the pointer to the incubed client config.
chain_id_t	**chain_id**	

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (`==IN3_OK`)

in3_free

```
void in3_free(in3_t *a);
```

frees the references of the client

arguments:

*in3_t **	**a**	the pointer to the incubed client config to free.

in3_cache_init

```
in3_ret_t in3_cache_init(in3_t *c);
```

inits the cache.

this will try to read the nodelist from cache.

arguments:

*in3_t **	**c**	the incubed client

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==`IN3_OK`)

in3_find_chain

```
in3_chain_t* in3_find_chain(in3_t *c, chain_id_t chain_id);
```

finds the chain-config for the given chain_id.

My return NULL if not found.

arguments:

*in3_t **	**c**	the incubed client
chain_id_t	**chain_id**	chain_id

returns: `in3_chain_t *`

in3_configure

```
char* in3_configure(in3_t *c, const char *config);
```

configures the clent based on a json-config.

For details about the structure of ther config see https://in3.readthedocs.io/en/develop/api-ts.html#type-in3config

arguments:

*in3_t **	**c**	the incubed client
`const char *`	**config**	JSON-string with the configuration to set.

returns: `char *`

in3_set_default_transport

```
void in3_set_default_transport(in3_transport_send transport);
```

defines a default transport which is used when creating a new client.

arguments:

in3_transport_send	**transport**	the default transport-function.

in3_set_default_storage

```
void in3_set_default_storage(in3_storage_handler_t *cacheStorage);
```

defines a default storage handler which is used when creating a new client.

arguments:

*in3_storage_handler_t **	**cacheStorage**	pointer to the handler-struct

in3_set_default_signer

```
void in3_set_default_signer(in3_signer_t *signer);
```

defines a default signer which is used when creating a new client.

arguments:

*in3_signer_t **	**signer**	default signer-function.

in3_create_signer

```
in3_signer_t* in3_create_signer(in3_sign sign, in3_prepare_tx prepare_tx, void␣
↪*wallet);
```

create a new signer-object to be set on the client.

the caller will need to free this pointer after usage.

arguments:

in3_sign	**sign**	function pointer returning a stored value for the given key.
in3_prepare_tx	**prepare_tx**	function pointer returning capable of manipulating the transaction before signing it. This is needed in order to support multisigs.
`void *`	**wallet**	custom object whill will be passed to functions

returns: `in3_signer_t *`

in3_create_storage_handler

```
in3_storage_handler_t* in3_create_storage_handler(in3_storage_get_item get_item, in3_
↪storage_set_item set_item, in3_storage_clear clear, void *cptr);
```

create a new storage handler-object to be set on the client.

the caller will need to free this pointer after usage.

arguments:

in3_storage_get_item	**get_item**	function pointer returning a stored value for the given key.
in3_storage_set_item	**set_item**	function pointer setting a stored value for the given key.
in3_storage_clear	**clear**	function pointer clearing all contents of cache.
`void *`	**cptr**	custom pointer which will will be passed to functions

returns: *in3_storage_handler_t **

8.7.2 context.h

Request Context. This is used for each request holding request and response-pointers but also controls the execution process.

File: src/core/client/context.h

ctx_set_error (c,msg,err)

```
#define ctx_set_error (c,msg,err) ctx_set_error_intern(c, NULL, err)
```

ctx_type_t

type of the request context,

The enum type contains the following values:

CT_RPC	0	a json-rpc request, which needs to be send to a incubed node
CT_SIGN	1	a sign request

node_match_t

the weight of a certain node as linked list.

This will be used when picking the nodes to send the request to. A linked list of these structs desribe the result.

The stuct contains following fields:

*in3_node_t **	**node**	the node definition including the url
*in3_node_weight_t **	**weight**	the current weight and blacklisting-stats
`float`	**s**	The starting value.
`float`	**w**	weight value
*weightstruct , **	**next**	next in the linkedlist or NULL if this is the last element

in3_ctx_t

The Request config.

This is generated for each request and represents the current state. it holds the state until the request is finished and must be freed afterwards.

The stuct contains following fields:

ctx_type_t	**type**	the type of the request
*in3_t **	**client**	reference to the client
*json_ctx_t **	**request_context**	the result of the json-parser for the request.
*json_ctx_t **	**response_context**	the result of the json-parser for the response.
`char *`	**error**	in case of an error this will hold the message, if not it points to *NULL*
`int`	**len**	the number of requests
`unsigned int`	**attempt**	the number of attempts
*d_token_t ***	**responses**	references to the tokens representring the parsed responses
*d_token_t ***	**requests**	references to the tokens representring the requests
*in3_request_config_t **	**requests_configs**	array of configs adjusted for each request.
*node_match_t **	**nodes**	
*cache_entry_t **	**cache**	optional cache-entries. These entries will be freed when cleaning up the context.
*in3_response_t **	**raw_response**	the raw response-data, which should be verified.
*in3_ctxstruct , **	**required**	pointer to the next required context. if not NULL the data from this context need get finished first, before being able to resume this context.
in3_ret_t	**verification_state**	state of the verification

in3_ctx_state_t

The current state of the context.

you can check this state after each execute-call.

The enum type contains the following values:

CTX_SUCCESS	0	The ctx has a verified result.
CTX_WAITING_FOR_REQUIRED_CTX	1	there are required contexts, which need to be resolved first
CTX_WAITING_FOR_RESPONSE	2	the response is not set yet
CTX_ERROR	-1	the request has a error

ctx_new

```
in3_ctx_t* ctx_new(in3_t *client, char *req_data);
```

creates a new context.

the request data will be parsed and represented in the context. calling this function will only parse the request data, but not send anything yet.

Important: the req_data will not be cloned but used during the execution. The caller of the this function is also responsible for freeing this string afterwards.

arguments:

in3_t *	**client**	the client-config.
`char *`	**req_data**	the rpc-request as json string.

returns: *in3_ctx_t **

in3_send_ctx

```
in3_ret_t in3_send_ctx(in3_ctx_t *ctx);
```

sends a previously created context to nodes and verifies it.

The execution happens within the same thread, thich mean it will be blocked until the response ha beedn received and verified. In order to handle calls asynchronously, you need to call the `in3_ctx_execute` function and provide the data as needed.

arguments:

in3_ctx_t *	**ctx**	the request context.

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==`IN3_OK`)

in3_ctx_execute

```
in3_ret_t in3_ctx_execute(in3_ctx_t *ctx);
```

tries to execute the context, but stops whenever data are required.

This function should be used in order to call data in a asyncronous way, since this function will not use the transport-function to actually send it.

The caller is responsible for delivering the required responses. After calling you need to check the return-value:

- IN3_WAITING : provide the required data and then call in3_ctx_execute again.
- IN3_OK : success, we have a result.
- any other status = error

Here is a example how to use this function:

```
in3_ret_t in3_send_ctx(in3_ctx_t* ctx) {
 in3_ret_t ret;
 // execute the context and store the return value.
 // if the return value is 0 == IN3_OK, it was successful and we return,
 // if not, we keep on executing
 while ((ret = in3_ctx_execute(ctx))) {
   // error we stop here, because this means we got an error
   if (ret != IN3_WAITING) return ret;

   // handle subcontexts first, if they have not been finished
   while (ctx->required && in3_ctx_state(ctx->required) != CTX_SUCCESS) {
     // exxecute them, and return the status if still waiting or error
     if ((ret = in3_send_ctx(ctx->required))) return ret;
```

(continues on next page)

(continued from previous page)

```
      // recheck in order to prepare the request.
      // if it is not waiting, then it we cannot do much, becaus it will an error or␣
↪successfull.
      if ((ret = in3_ctx_execute(ctx)) != IN3_WAITING) return ret;
    }

    // only if there is no response yet...
    if (!ctx->raw_response) {

      // what kind of request do we need to provide?
      switch (ctx->type) {

        // RPC-request to send to the nodes
        case CT_RPC: {

            // build the request
            in3_request_t* request = in3_create_request(ctx);

            // here we use the transport, but you can also try to fetch the data in␣
↪any other way.
            ctx->client->transport(request);

            // clean up
            request_free(request, ctx, false);
            break;
        }

        // this is a request to sign a transaction
        case CT_SIGN: {
            // read the data to sign from the request
            d_token_t* params = d_get(ctx->requests[0], K_PARAMS);
            // the data to sign
            bytes_t    data   = d_to_bytes(d_get_at(params, 0));
            // the account to sign with
            bytes_t    from   = d_to_bytes(d_get_at(params, 1));

            // prepare the response
            ctx->raw_response = _malloc(sizeof(in3_response_t));
            sb_init(&ctx->raw_response[0].error);
            sb_init(&ctx->raw_response[0].result);

            // data for the signature
            uint8_t sig[65];
            // use the signer to create the signature
            ret = ctx->client->signer->sign(ctx, SIGN_EC_HASH, data, from, sig);
            // if it fails we report this as error
            if (ret < 0) return ctx_set_error(ctx, ctx->raw_response->error.data,␣
↪ret);
            // otherwise we simply add the raw 65 bytes to the response.
            sb_add_range(&ctx->raw_response->result, (char*) sig, 0, 65);
        }
      }
    }
  }
  // done...
  return ret;
}
```

arguments:

*in3_ctx_t **	**ctx**	the request context.

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==`IN3_OK`)

in3_ctx_state

```
in3_ctx_state_t in3_ctx_state(in3_ctx_t *ctx);
```

returns the current state of the context.

arguments:

*in3_ctx_t **	**ctx**	the request context.

returns: `in3_ctx_state_t`

in3_create_request

```
in3_request_t* in3_create_request(in3_ctx_t *ctx);
```

creates a request-object, which then need to be filled with the responses.

each request object contains a array of reponse-objects. In order to set the response, you need to call

```
// set a succesfull response
sb_add_chars(&request->results[0].result, my_response);
// set a error response
sb_add_chars(&request->results[0].error, my_error);
```

arguments:

*in3_ctx_t **	**ctx**	the request context.

returns: `in3_request_t *`

request_free

```
void request_free(in3_request_t *req, const in3_ctx_t *ctx, bool response_free);
```

frees a previuosly allocated request.

arguments:

*in3_request_t **	**req**	the request.
*in3_ctx_tconst , **	**ctx**	the request context.
`bool`	**response_free**	if true the responses will freed also, but usually this is done when the ctx is freed.

ctx_free

```
void ctx_free(in3_ctx_t *ctx);
```

frees all resources allocated during the request.

But this will not free the request string passed when creating the context!

arguments:

*in3_ctx_t **	**ctx**	the request context.

ctx_add_required

```
in3_ret_t ctx_add_required(in3_ctx_t *parent, in3_ctx_t *ctx);
```

adds a new context as a requirment.

Whenever a verifier needs more data and wants to send a request, we should create the request and add it as dependency and stop.

If the function is called again, we need to search and see if the required status is now useable.

Here is an example of how to use it:

```
in3_ret_t get_from_nodes(in3_ctx_t* parent, char* method, char* params, bytes_t* dst)
↪{
  // check if the method is already existing
  in3_ctx_t* ctx = ctx_find_required(parent, method);
  if (ctx) {
    // found one - so we check if it is useable.
    switch (in3_ctx_state(ctx)) {
      // in case of an error, we report it back to the parent context
      case CTX_ERROR:
        return ctx_set_error(parent, ctx->error, IN3_EUNKNOWN);
      // if we are still waiting, we stop here and report it.
      case CTX_WAITING_FOR_REQUIRED_CTX:
      case CTX_WAITING_FOR_RESPONSE:
        return IN3_WAITING;

      // if it is useable, we can now handle the result.
      case CTX_SUCCESS: {
        d_token_t* r = d_get(ctx->responses[0], K_RESULT);
        if (r) {
          // we have a result, so write it back to the dst
          *dst = d_to_bytes(r);
          return IN3_OK;
        } else
          // or check the error and report it
          return ctx_check_response_error(parent, 0);
      }
    }
  }

  // no required context found yet, so we create one:

  // since this is a subrequest it will be freed when the parent is freed.
```

(continues on next page)

(continued from previous page)

```
  // allocate memory for the request-string
  char* req = _malloc(strlen(method) + strlen(params) + 200);
  // create it
  sprintf(req, "{\"method\":\"%s\",\"jsonrpc\":\"2.0\",\"id\":1,\"params\":%s}",
→method, params);
  // and add the request context to the parent.
  return ctx_add_required(parent, ctx_new(parent->client, req));
}
```

arguments:

in3_ctx_t *	**parent**	the current request context.
in3_ctx_t *	**ctx**	the new request context to add.

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==IN3_OK)

ctx_find_required

```
in3_ctx_t* ctx_find_required(const in3_ctx_t *parent, const char *method);
```

searches within the required request contextes for one with the given method.

This method is used internaly to find a previously added context.

arguments:

in3_ctx_tconst , *	**parent**	the current request context.
`const char *`	**method**	the method of the rpc-request.

returns: `in3_ctx_t *`

ctx_remove_required

```
in3_ret_t ctx_remove_required(in3_ctx_t *parent, in3_ctx_t *ctx);
```

removes a required context after usage.

removing will also call free_ctx to free resources.

arguments:

in3_ctx_t *	**parent**	the current request context.
in3_ctx_t *	**ctx**	the request context to remove.

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==IN3_OK)

ctx_check_response_error

```
in3_ret_t ctx_check_response_error(in3_ctx_t *c, int i);
```

check if the response contains a error-property and reports this as error in the context.

arguments:

*in3_ctx_t **	**c**	the current request context.
`int`	**i**	the index of the request to check (if this is a batch-request, otherwise 0).

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==`IN3_OK`)

ctx_set_error_intern

```
in3_ret_t ctx_set_error_intern(in3_ctx_t *c, char *msg, in3_ret_t errnumber);
```

sets the error message in the context.

If there is a previous error it will append it. the return value will simply be passed so you can use it like

```
return ctx_set_error(ctx, "wrong number of arguments", IN3_EINVAL)
```

arguments:

*in3_ctx_t **	**c**	the current request context.
`char *`	**msg**	the error message. (This string will be copied)
in3_ret_t	**errnumber**	the error code to return

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==`IN3_OK`)

ctx_get_error

```
in3_ret_t ctx_get_error(in3_ctx_t *ctx, int id);
```

determins the errorcode for the given request.

arguments:

*in3_ctx_t **	**ctx**	the current request context.
`int`	**id**	the index of the request to check (if this is a batch-request, otherwise 0).

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==`IN3_OK`)

in3_client_rpc_ctx

```
in3_ctx_t* in3_client_rpc_ctx(in3_t *c, char *method, char *params);
```

sends a request and returns a context used to access the result or errors.

This context *MUST* be freed with ctx_free(ctx) after usage to release the resources.

arguments:

*in3_t **	**c**	the clientt config.
`char *`	**method**	rpc method.
`char *`	**params**	params as string.

returns: *`in3_ctx_t *`*

8.7.3 verifier.h

Verification Context. This context is passed to the verifier.

File: src/core/client/verifier.h

vc_err (vc,msg)

```
#define vc_err (vc,msg) vc_set_error(vc, NULL)
```

in3_verify

function to verify the result.

```
typedef in3_ret_t(* in3_verify) (in3_vctx_t *c)
```

returns: `in3_ret_t (*` the *result-status* of the function.

Please make sure you check if it was successfull (==`IN3_OK`)

in3_pre_handle

function which is called to fill the response before a request is triggered.

This can be used to handle requests which don't need a node to response.

```
typedef in3_ret_t(* in3_pre_handle) (in3_ctx_t *ctx, in3_response_t **response)
```

returns: `in3_ret_t (*` the *result-status* of the function.

Please make sure you check if it was successfull (==`IN3_OK`)

in3_verifier_t

The stuct contains following fields:

in3_verify	**verify**
in3_pre_handle	**pre_handle**
in3_chain_type_t	**type**
*verifierstruct , **	**next**

in3_get_verifier

```
in3_verifier_t* in3_get_verifier(in3_chain_type_t type);
```

returns the verifier for the given chainType

arguments:

in3_chain_type_t	**type**

returns: `in3_verifier_t *`

in3_register_verifier

```
void in3_register_verifier(in3_verifier_t *verifier);
```

arguments:

*in3_verifier_t **	**verifier**

vc_set_error

```
in3_ret_t vc_set_error(in3_vctx_t *vc, char *msg);
```

arguments:

*in3_vctx_t **	**vc**
`char *`	**msg**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==IN3_OK)

8.7.4 bytes.h

util helper on byte arrays.

File: src/core/util/bytes.h

bb_new ()

creates a new bytes_builder with a initial size of 32 bytes

```
#define bb_new () bb_newl(32)
```

bb_read (*bb*,*i*,*vptr*)

```
#define bb_read (_bb_,_i_,_vptr_) bb_readl((_bb_), (_i_), (_vptr_), sizeof(*_vptr_))
```

bb_read_next (*bb*,*iptr*,*vptr*)

```
#define bb_read_next (_bb_,_iptr_,_vptr_) do {
↪   \
    size_t _l_ = sizeof(*_vptr_);               \
    bb_readl((_bb_), *(_iptr_), (_vptr_), _l_); \
    *(_iptr_) += _l_;                           \
  } while (0)
```

bb_readl (*bb*,*i*,*vptr*,*l*)

```
#define bb_readl (_bb_,_i_,_vptr_,_l_) memcpy((_vptr_), (_bb_)->b.data + (_i_), _l_)
```

b_read (*b*,*i*,*vptr*)

```
#define b_read (_b_,_i_,_vptr_) b_readl((_b_), (_i_), _vptr_, sizeof(*_vptr_))
```

b_readl (*b*,*i*,*vptr*,*l*)

```
#define b_readl (_b_,_i_,_vptr_,_l_) memcpy(_vptr_, (_b_)->data + (_i_), (_l_))
```

address_t

pointer to a 20byte address

```
typedef uint8_t address_t[20]
```

bytes32_t

pointer to a 32byte word

```
typedef uint8_t bytes32_t[32]
```

wlen_t

number of bytes within a word (min 1byte but usually a uint)

```
typedef uint_fast8_t wlen_t
```

bytes_t

a byte array

The stuct contains following fields:

uint8_t *	**data**	the byte-data
uint32_t	**len**	the length of the array ion bytes

b_new

```
bytes_t* b_new(const char *data, int len);
```

allocates a new byte array with 0 filled

arguments:

const char *	**data**
int	**len**

returns: *bytes_t **

b_print

```
void b_print(const bytes_t *a);
```

prints a the bytes as hex to stdout

arguments:

*bytes_tconst , **	**a**

ba_print

```
void ba_print(const uint8_t *a, size_t l);
```

prints a the bytes as hex to stdout

arguments:

const uint8_t *	**a**
size_t	**l**

b_cmp

```
int b_cmp(const bytes_t *a, const bytes_t *b);
```

compares 2 byte arrays and returns 1 for equal and 0 for not equal

arguments:

*bytes_tconst , **	**a**
*bytes_tconst , **	**b**

returns: `int`

bytes_cmp

```
int bytes_cmp(const bytes_t a, const bytes_t b);
```

compares 2 byte arrays and returns 1 for equal and 0 for not equal

arguments:

bytes_tconst	**a**
bytes_tconst	**b**

returns: `int`

b_free

```
void b_free(bytes_t *a);
```

frees the data

arguments:

*bytes_t **	**a**

b_dup

```
bytes_t* b_dup(const bytes_t *a);
```

clones a byte array

arguments:

*bytes_tconst , **	**a**

returns: `bytes_t *`

b_read_byte

```
uint8_t b_read_byte(bytes_t *b, size_t *pos);
```

reads a byte on the current position and updates the pos afterwards.

arguments:

*bytes_t **	**b**
`size_t *`	**pos**

returns: `uint8_t`

b_read_int

```
uint32_t b_read_int(bytes_t *b, size_t *pos);
```

reads a integer on the current position and updates the pos afterwards.

arguments:

*bytes_t **	**b**
`size_t *`	**pos**

returns: `uint32_t`

b_read_long

```
uint64_t b_read_long(bytes_t *b, size_t *pos);
```

reads a long on the current position and updates the pos afterwards.

arguments:

*bytes_t **	**b**
`size_t *`	**pos**

returns: `uint64_t`

b_new_chars

```
char* b_new_chars(bytes_t *b, size_t *pos);
```

creates a new string (needs to be freed) on the current position and updates the pos afterwards.

arguments:

*bytes_t **	**b**
`size_t *`	**pos**

returns: `char *`

b_new_fixed_bytes

```
bytes_t* b_new_fixed_bytes(bytes_t *b, size_t *pos, int len);
```

reads bytes with a fixed length on the current position and updates the pos afterwards.

arguments:

*bytes_t **	**b**
`size_t *`	**pos**
`int`	**len**

returns: *bytes_t **

bb_newl

```
bytes_builder_t* bb_newl(size_t l);
```

creates a new bytes_builder

arguments:

`size_t`	**l**

returns: *bytes_builder_t **

bb_free

```
void bb_free(bytes_builder_t *bb);
```

frees a bytebuilder and its content.

arguments:

*bytes_builder_t **	**bb**

bb_check_size

```
int bb_check_size(bytes_builder_t *bb, size_t len);
```

internal helper to increase the buffer if needed

arguments:

*bytes_builder_t **	**bb**
`size_t`	**len**

returns: `int`

bb_write_chars

```c
void bb_write_chars(bytes_builder_t *bb, char *c, int len);
```

writes a string to the builder.

arguments:

*bytes_builder_t **	**bb**
`char *`	**c**
`int`	**len**

bb_write_dyn_bytes

```c
void bb_write_dyn_bytes(bytes_builder_t *bb, const bytes_t *src);
```

writes bytes to the builder with a prefixed length.

arguments:

*bytes_builder_t **	**bb**
*bytes_tconst , **	**src**

bb_write_fixed_bytes

```c
void bb_write_fixed_bytes(bytes_builder_t *bb, const bytes_t *src);
```

writes fixed bytes to the builder.

arguments:

*bytes_builder_t **	**bb**
*bytes_tconst , **	**src**

bb_write_int

```c
void bb_write_int(bytes_builder_t *bb, uint32_t val);
```

writes a ineteger to the builder.

arguments:

*bytes_builder_t **	**bb**
`uint32_t`	**val**

bb_write_long

```c
void bb_write_long(bytes_builder_t *bb, uint64_t val);
```

writes s long to the builder.

arguments:

*bytes_builder_t **	**bb**
`uint64_t`	**val**

bb_write_long_be

```
void bb_write_long_be(bytes_builder_t *bb, uint64_t val, int len);
```

writes any integer value with the given length of bytes

arguments:

*bytes_builder_t **	**bb**
`uint64_t`	**val**
`int`	**len**

bb_write_byte

```
void bb_write_byte(bytes_builder_t *bb, uint8_t val);
```

writes a single byte to the builder.

arguments:

*bytes_builder_t **	**bb**
`uint8_t`	**val**

bb_write_raw_bytes

```
void bb_write_raw_bytes(bytes_builder_t *bb, void *ptr, size_t len);
```

writes the bytes to the builder.

arguments:

*bytes_builder_t **	**bb**
`void *`	**ptr**
`size_t`	**len**

bb_clear

```
void bb_clear(bytes_builder_t *bb);
```

resets the content of the builder.

arguments:

*bytes_builder_t **	**bb**

bb_replace

```
void bb_replace(bytes_builder_t *bb, int offset, int delete_len, uint8_t *data, int␣
↪data_len);
```

replaces or deletes a part of the content.

arguments:

*bytes_builder_t **	**bb**
`int`	**offset**
`int`	**delete_len**
`uint8_t *`	**data**
`int`	**data_len**

bb_move_to_bytes

```
bytes_t* bb_move_to_bytes(bytes_builder_t *bb);
```

frees the builder and moves the content in a newly created bytes struct (which needs to be freed later).

arguments:

*bytes_builder_t **	**bb**

returns: *`bytes_t *`*

bb_read_long

```
uint64_t bb_read_long(bytes_builder_t *bb, size_t *i);
```

reads a long from the builder

arguments:

*bytes_builder_t **	**bb**
`size_t *`	**i**

returns: `uint64_t`

bb_read_int

```
uint32_t bb_read_int(bytes_builder_t *bb, size_t *i);
```

reads a int from the builder

arguments:

*bytes_builder_t **	**bb**
`size_t *`	**i**

returns: `uint32_t`

bytes

```
static bytes_t bytes(uint8_t *a, uint32_t len);
```

converts the given bytes to a bytes struct

arguments:

`uint8_t *`	**a**
`uint32_t`	**len**

returns: *bytes_t*

cloned_bytes

```
bytes_t cloned_bytes(bytes_t data);
```

cloned the passed data

arguments:

bytes_t	**data**

returns: *bytes_t*

b_optimize_len

```
static void b_optimize_len(bytes_t *b);
```

< changed the data and len to remove leading 0-bytes

arguments:

*bytes_t **	**b**

8.7.5 data.h

json-parser.

The parser can read from :

- json

- bin

When reading from json all '0x'... values will be stored as bytes_t. If the value is lower than 0xFFFFFFF, it is converted as integer.

File: src/core/util/data.h

DATA_DEPTH_MAX

the max DEPTH of the JSON-data allowed.

It will throw an error if reached.

```
#define DATA_DEPTH_MAX 11
```

printX

```
#define printX printf
```

fprintX

```
#define fprintX fprintf
```

snprintX

```
#define snprintX snprintf
```

vprintX

```
#define vprintX vprintf
```

d_key_t

```
typedef uint16_t d_key_t
```

d_token_t

a token holding any kind of value.

use d_type, d_len or the cast-function to get the value.

The stuct contains following fields:

`uint8_t *`	**data**	the byte or string-data
`uint32_t`	**len**	the length of the content (or number of properties) depending + type.
`d_key_t`	**key**	the key of the property.

str_range_t

internal type used to represent the a range within a string.

The stuct contains following fields:

`char *`	**data**	pointer to the start of the string
`size_t`	**len**	len of the characters

json_ctx_t

parser for json or binary-data.

it needs to freed after usage.

The stuct contains following fields:

*d_token_t **	**result**	the list of all tokens. the first token is the main-token as returned by the parser.
`char *`	**c**	
`size_t`	**allocated**	pointer to the src-data
`size_t`	**len**	amount of tokens allocated result
`size_t`	**depth**	number of tokens in result

d_iterator_t

iterator over elements of a array opf object.

usage:

```
for (d_iterator_t iter = d_iter( parent ); iter.left ; d_iter_next(&iter)) {
  uint32_t val = d_int(iter.token);
}
```

The stuct contains following fields:

*d_token_t **	**token**	current token
`int`	**left**	number of result left

d_to_bytes

```
bytes_t d_to_bytes(d_token_t *item);
```

returns the byte-representation of token.

In case of a number it is returned as bigendian. booleans as 0x01 or 0x00 and NULL as 0x. Objects or arrays will return 0x.

arguments:

*d_token_t **	**item**

returns: `bytes_t`

d_bytes_to

```
int d_bytes_to(d_token_t *item, uint8_t *dst, const int max);
```

writes the byte-representation to the dst.

details see d_to_bytes.

arguments:

*d_token_t **	**item**
`uint8_t *`	**dst**
`const int`	**max**

returns: `int`

d_bytes

```
bytes_t* d_bytes(const d_token_t *item);
```

returns the value as bytes (Carefully, make sure that the token is a bytes-type!)

arguments:

*d_token_tconst , **	**item**

returns: *bytes_t **

d_bytesl

```
bytes_t* d_bytesl(d_token_t *item, size_t l);
```

returns the value as bytes with length l (may reallocates)

arguments:

*d_token_t **	**item**
`size_t`	**l**

returns: *bytes_t **

d_string

```
char* d_string(const d_token_t *item);
```

converts the value as string.

Make sure the type is string!

arguments:

*d_token_tconst , **	**item**

returns: `char *`

d_int

```
int32_t d_int(const d_token_t *item);
```

returns the value as integer.

only if type is integer

arguments:

*d_token_tconst , **	**item**

returns: `int32_t`

d_intd

```
int32_t d_intd(const d_token_t *item, const uint32_t def_val);
```

returns the value as integer or if NULL the default.

only if type is integer

arguments:

*d_token_tconst , **	**item**
`const uint32_t`	**def_val**

returns: `int32_t`

d_long

```
uint64_t d_long(const d_token_t *item);
```

returns the value as long.

only if type is integer or bytes, but short enough

arguments:

*d_token_tconst , **	**item**

returns: `uint64_t`

d_longd

```
uint64_t d_longd(const d_token_t *item, const uint64_t def_val);
```

returns the value as long or if NULL the default.

only if type is integer or bytes, but short enough

arguments:

*d_token_tconst , **	**item**
`const uint64_t`	**def_val**

returns: `uint64_t`

d_create_bytes_vec

```
bytes_t** d_create_bytes_vec(const d_token_t *arr);
```

arguments:

*d_token_tconst , **	**arr**

returns: *`bytes_t **`*

d_type

```
static d_type_t d_type(const d_token_t *item);
```

creates a array of bytes from JOSN-array

type of the token

arguments:

*d_token_tconst , **	**item**

returns: *`d_type_t`*

d_len

```
static int d_len(const d_token_t *item);
```

number of elements in the token (only for object or array, other will return 0)

arguments:

*d_token_tconst , **	**item**

returns: `int`

d_eq

```
bool d_eq(const d_token_t *a, const d_token_t *b);
```

compares 2 token and if the value is equal

arguments:

*d_token_tconst , **	**a**
*d_token_tconst , **	**b**

returns: `bool`

keyn

```
d_key_t keyn(const char *c, const size_t len);
```

generates the keyhash for the given stringrange as defined by len

arguments:

`const char *`	**c**
`const size_t`	**len**

returns: `d_key_t`

d_get

```
d_token_t* d_get(d_token_t *item, const uint16_t key);
```

returns the token with the given propertyname (only if item is a object)

arguments:

*d_token_t **	**item**
`const uint16_t`	**key**

returns: `d_token_t *`

d_get_or

```
d_token_t* d_get_or(d_token_t *item, const uint16_t key1, const uint16_t key2);
```

returns the token with the given propertyname or if not found, tries the other.

(only if item is a object)

arguments:

*d_token_t **	**item**
`const uint16_t`	**key1**
`const uint16_t`	**key2**

returns: `d_token_t *`

d_get_at

```
d_token_t* d_get_at(d_token_t *item, const uint32_t index);
```

returns the token of an array with the given index

arguments:

*d_token_t **	**item**
`const uint32_t`	**index**

returns: `d_token_t *`

d_next

```
d_token_t* d_next(d_token_t *item);
```

returns the next sibling of an array or object

arguments:

*d_token_t **	**item**

returns: `d_token_t *`

d_serialize_binary

```
void d_serialize_binary(bytes_builder_t *bb, d_token_t *t);
```

write the token as binary data into the builder

arguments:

*bytes_builder_t **	**bb**
*d_token_t **	**t**

parse_binary

```
json_ctx_t* parse_binary(const bytes_t *data);
```

parses the data and returns the context with the token, which needs to be freed after usage!

arguments:

*bytes_tconst , **	**data**

returns: `json_ctx_t *`

parse_binary_str

```
json_ctx_t* parse_binary_str(const char *data, int len);
```

parses the data and returns the context with the token, which needs to be freed after usage!

arguments:

const char *	**data**
int	**len**

returns: *json_ctx_t **

parse_json

```
json_ctx_t* parse_json(char *js);
```

parses json-data, which needs to be freed after usage!

arguments:

char *	**js**

returns: *json_ctx_t **

json_free

```
void json_free(json_ctx_t *parser_ctx);
```

frees the parse-context after usage

arguments:

*json_ctx_t **	**parser_ctx**

d_to_json

```
str_range_t d_to_json(const d_token_t *item);
```

returns the string for a object or array.

This only works for json as string. For binary it will not work!

arguments:

*d_token_tconst , **	**item**

returns: *str_range_t*

d_create_json

```
char* d_create_json(d_token_t *item);
```

creates a json-string.

It does not work for objects if the parsed data were binary!

arguments:

d_token_t *	**item**

returns: `char *`

json_create

```
json_ctx_t* json_create();
```

returns: *`json_ctx_t *`*

json_create_null

```
d_token_t* json_create_null(json_ctx_t *jp);
```

arguments:

json_ctx_t *	**jp**

returns: *`d_token_t *`*

json_create_bool

```
d_token_t* json_create_bool(json_ctx_t *jp, bool value);
```

arguments:

json_ctx_t *	**jp**
`bool`	**value**

returns: *`d_token_t *`*

json_create_int

```
d_token_t* json_create_int(json_ctx_t *jp, uint64_t value);
```

arguments:

json_ctx_t *	**jp**
`uint64_t`	**value**

returns: *d_token_t **

json_create_string

```
d_token_t* json_create_string(json_ctx_t *jp, char *value);
```

arguments:

*json_ctx_t **	**jp**
`char *`	**value**

returns: *d_token_t **

json_create_bytes

```
d_token_t* json_create_bytes(json_ctx_t *jp, bytes_t value);
```

arguments:

*json_ctx_t **	**jp**
bytes_t	**value**

returns: *d_token_t **

json_create_object

```
d_token_t* json_create_object(json_ctx_t *jp);
```

arguments:

*json_ctx_t **	**jp**

returns: *d_token_t **

json_create_array

```
d_token_t* json_create_array(json_ctx_t *jp);
```

arguments:

*json_ctx_t **	**jp**

returns: *d_token_t **

json_object_add_prop

```
d_token_t* json_object_add_prop(d_token_t *object, d_key_t key, d_token_t *value);
```

arguments:

d_token_t *	**object**
d_key_t	**key**
d_token_t *	**value**

returns: *d_token_t **

json_array_add_value

```
d_token_t* json_array_add_value(d_token_t *object, d_token_t *value);
```

arguments:

d_token_t *	**object**
d_token_t *	**value**

returns: *d_token_t **

d_get_keystr

```
char* d_get_keystr(d_key_t k);
```

returns the string for a key.

This only works track_keynames was activated before!

arguments:

d_key_t	**k**

returns: `char *`

d_track_keynames

```
void d_track_keynames(uint8_t v);
```

activates the keyname-cache, which stores the string for the keys when parsing.

arguments:

uint8_t	**v**

d_clear_keynames

```
void d_clear_keynames();
```

delete the cached keynames

key

```
static d_key_t key(const char *c);
```

arguments:

const char *	**c**

returns: d_key_t

d_get_stringk

```
static char* d_get_stringk(d_token_t *r, d_key_t k);
```

reads token of a property as string.

arguments:

*d_token_t **	**r**
d_key_t	**k**

returns: char *

d_get_string

```
static char* d_get_string(d_token_t *r, char *k);
```

reads token of a property as string.

arguments:

*d_token_t **	**r**
char *	**k**

returns: char *

d_get_string_at

```
static char* d_get_string_at(d_token_t *r, uint32_t pos);
```

reads string at given pos of an array.

arguments:

*d_token_t **	**r**
uint32_t	**pos**

returns: char *

d_get_intk

```
static int32_t d_get_intk(d_token_t *r, d_key_t k);
```

reads token of a property as int.

arguments:

*d_token_t **	**r**
d_key_t	**k**

returns: int32_t

d_get_intkd

```
static int32_t d_get_intkd(d_token_t *r, d_key_t k, uint32_t d);
```

reads token of a property as int.

arguments:

*d_token_t **	**r**
d_key_t	**k**
uint32_t	**d**

returns: int32_t

d_get_int

```
static int32_t d_get_int(d_token_t *r, char *k);
```

reads token of a property as int.

arguments:

*d_token_t **	**r**
char *	**k**

returns: int32_t

d_get_int_at

```
static int32_t d_get_int_at(d_token_t *r, uint32_t pos);
```

reads a int at given pos of an array.

arguments:

*d_token_t **	**r**
uint32_t	**pos**

returns: int32_t

d_get_longk

```
static uint64_t d_get_longk(d_token_t *r, d_key_t k);
```

reads token of a property as long.

arguments:

*d_token_t **	**r**
`d_key_t`	**k**

returns: `uint64_t`

d_get_longkd

```
static uint64_t d_get_longkd(d_token_t *r, d_key_t k, uint64_t d);
```

reads token of a property as long.

arguments:

*d_token_t **	**r**
`d_key_t`	**k**
`uint64_t`	**d**

returns: `uint64_t`

d_get_long

```
static uint64_t d_get_long(d_token_t *r, char *k);
```

reads token of a property as long.

arguments:

*d_token_t **	**r**
`char *`	**k**

returns: `uint64_t`

d_get_long_at

```
static uint64_t d_get_long_at(d_token_t *r, uint32_t pos);
```

reads long at given pos of an array.

arguments:

*d_token_t **	**r**
`uint32_t`	**pos**

returns: `uint64_t`

d_get_bytesk

```
static bytes_t* d_get_bytesk(d_token_t *r, d_key_t k);
```

reads token of a property as bytes.

arguments:

d_token_t *	**r**
d_key_t	**k**

returns: `bytes_t *`

d_get_bytes

```
static bytes_t* d_get_bytes(d_token_t *r, char *k);
```

reads token of a property as bytes.

arguments:

d_token_t *	**r**
char *	**k**

returns: `bytes_t *`

d_get_bytes_at

```
static bytes_t* d_get_bytes_at(d_token_t *r, uint32_t pos);
```

reads bytes at given pos of an array.

arguments:

d_token_t *	**r**
uint32_t	**pos**

returns: `bytes_t *`

d_is_binary_ctx

```
static bool d_is_binary_ctx(json_ctx_t *ctx);
```

check if the parser context was created from binary data.

arguments:

json_ctx_t *	**ctx**

returns: `bool`

d_get_byteskl

```
bytes_t* d_get_byteskl(d_token_t *r, d_key_t k, uint32_t minl);
```

arguments:

*d_token_t **	**r**
d_key_t	**k**
uint32_t	**minl**

returns: *bytes_t **

d_getl

```
d_token_t* d_getl(d_token_t *item, uint16_t k, uint32_t minl);
```

arguments:

*d_token_t **	**item**
uint16_t	**k**
uint32_t	**minl**

returns: *d_token_t **

d_iter

```
static d_iterator_t d_iter(d_token_t *parent);
```

creates a iterator for a object or array

arguments:

*d_token_t **	**parent**

returns: *d_iterator_t*

d_iter_next

```
static bool d_iter_next(d_iterator_t *const iter);
```

fetched the next token an returns a boolean indicating whther there is a next or not.

arguments:

*d_iterator_t *const*	**iter**

returns: bool

8.7.6 debug.h

logs debug data only if the DEBUG-flag is set.

File: src/core/util/debug.h

IN3_EXPORT_TEST

```
#define IN3_EXPORT_TEST static
```

dbg_log (msg,. . .)

logs a debug-message including file and linenumber

dbg_log_raw (msg,. . .)

logs a debug-message without the filename

msg_dump

```
void msg_dump(const char *s, const unsigned char *data, unsigned len);
```

dumps the given data as hex coded bytes to stdout

arguments:

`const char *`	**s**
`const unsigned char *`	**data**
`unsigned`	**len**

8.7.7 error.h

defines the return-values of a function call.

File: src/core/util/error.h

DEPRECATED

depreacted-attribute

```
#define DEPRECATED __attribute__((deprecated))
```

OPTIONAL_T (t)

Optional type similar to C++ std::optional Optional types must be defined prior to usage (e.g.

DEFINE_OPTIONAL_T(int)) Use OPTIONAL_T_UNDEFINED(t) & OPTIONAL_T_VALUE(t, v) for easy initialization (rvalues) Note: Defining optional types for pointers is ill-formed by definition. This is because redundant

```
#define OPTIONAL_T (t) opt_##t
```

DEFINE_OPTIONAL_T (t)

Optional types must be defined prior to usage (e.g.

DEFINE_OPTIONAL_T(int)) Use OPTIONAL_T_UNDEFINED(t) & OPTIONAL_T_VALUE(t, v) for easy initialization (rvalues)

```
#define DEFINE_OPTIONAL_T (t) typedef struct {            \
    t    value;               \
    bool defined;             \
  } OPTIONAL_T(t)
```

OPTIONAL_T_UNDEFINED (t)

marks a used value as undefined.

```
#define OPTIONAL_T_UNDEFINED (t) ((OPTIONAL_T(t)){.defined = false})
```

OPTIONAL_T_VALUE (t,v)

sets the value of an optional type.

```
#define OPTIONAL_T_VALUE (t,v) ((OPTIONAL_T(t)){.value = v, .defined = true})
```

in3_errmsg

```
char* in3_errmsg(in3_ret_t err);
```

converts a error code into a string.

These strings are constants and do not need to be freed.

arguments:

in3_ret_t	**err**	the error code

returns: `char *`

8.7.8 scache.h

util helper on byte arrays.

File: src/core/util/scache.h

cache_entry_t

represents a single cache entry in a linked list.

These are used within a request context to cache values and automaticly free them.

The stuct contains following fields:

bytes_t	**key**	an optional key of the entry
bytes_t	**value**	the value
`uint8_t`	**buffer**	the buffer is used to store extra data, which will be cleaned when freed.
`bool`	**must_free**	if true, the cache-entry will be freed when the request context is cleaned up.
cache_entrystruct , *	**next**	pointer to the next entry.

in3_cache_get_entry

```
bytes_t* in3_cache_get_entry(cache_entry_t *cache, bytes_t *key);
```

get the entry for a given key.

arguments:

cache_entry_t *	**cache**	the root entry of the linked list.
bytes_t *	**key**	the key to compare with

returns: `bytes_t *`

in3_cache_add_entry

```
cache_entry_t* in3_cache_add_entry(cache_entry_t **cache, bytes_t key, bytes_t value);
```

adds an entry to the linked list.

arguments:

cache_entry_t **	**cache**	the root entry of the linked list.
bytes_t	**key**	an optional key
bytes_t	**value**	the value of the entry

returns: `cache_entry_t *`

in3_cache_free

```
void in3_cache_free(cache_entry_t *cache);
```

clears all entries in the linked list.

arguments:

cache_entry_t *	**cache**	the root entry of the linked list.

in3_cache_add_ptr

```
static cache_entry_t* in3_cache_add_ptr(cache_entry_t **cache, void *ptr);
```

adds a pointer, which should be freed when the context is freed.

arguments:

cache_entry_t **	**cache**	the root entry of the linked list.
`void *`	**ptr**	pointer to memory which shold be freed.

returns: `cache_entry_t *`

8.7.9 stringbuilder.h

simple string buffer used to dynamicly add content.

File: src/core/util/stringbuilder.h

sb_add_hexuint (sb,i)

shortcut macro for adding a uint to the stringbuilder using sizeof(i) to automaticly determine the size

```
#define sb_add_hexuint (sb,i) sb_add_hexuint_l(sb, i, sizeof(i))
```

sb_t

string build struct, which is able to hold and modify a growing string.

The stuct contains following fields:

`char *`	**data**	the current string (null terminated)
`size_t`	**allocted**	number of bytes currently allocated
`size_t`	**len**	the current length of the string

sb_new

```
sb_t* sb_new(const char *chars);
```

creates a new stringbuilder and copies the inital characters into it.

arguments:

`const char *`	**chars**

returns: `sb_t *`

sb_init

```
sb_t* sb_init(sb_t *sb);
```

initializes a stringbuilder by allocating memory.

arguments:

*sb_t **	**sb**

returns: *sb_t **

sb_free

```
void sb_free(sb_t *sb);
```

frees all resources of the stringbuilder

arguments:

*sb_t **	**sb**

sb_add_char

```
sb_t* sb_add_char(sb_t *sb, char c);
```

add a single character

arguments:

*sb_t **	**sb**
`char`	**c**

returns: *sb_t **

sb_add_chars

```
sb_t* sb_add_chars(sb_t *sb, const char *chars);
```

adds a string

arguments:

*sb_t **	**sb**
`const char *`	**chars**

returns: *sb_t **

sb_add_range

```
sb_t* sb_add_range(sb_t *sb, const char *chars, int start, int len);
```

add a string range

arguments:

*sb_t **	**sb**
const char *	**chars**
int	**start**
int	**len**

returns: *sb_t **

sb_add_key_value

```
sb_t* sb_add_key_value(sb_t *sb, const char *key, const char *value, int value_len,␣
↪bool as_string);
```

adds a value with an optional key.

if as_string is true the value will be quoted.

arguments:

*sb_t **	**sb**
const char *	**key**
const char *	**value**
int	**value_len**
bool	**as_string**

returns: *sb_t **

sb_add_bytes

```
sb_t* sb_add_bytes(sb_t *sb, const char *prefix, const bytes_t *bytes, int len, bool␣
↪as_array);
```

add bytes as 0x-prefixed hexcoded string (including an optional prefix), if len>1 is passed bytes maybe an array (if as_array==true)

arguments:

*sb_t **	**sb**
const char *	**prefix**
*bytes_tconst , **	**bytes**
int	**len**
bool	**as_array**

returns: *sb_t **

sb_add_hexuint_l

```
sb_t* sb_add_hexuint_l(sb_t *sb, uintmax_t uint, size_t l);
```

add a integer value as hexcoded, 0x-prefixed string

Other types not supported

arguments:

*sb_t **	**sb**
`uintmax_t`	**uint**
`size_t`	**l**

returns: `sb_t *`

8.7.10 utils.h

utility functions.

File: src/core/util/utils.h

SWAP (a,b)

simple swap macro for integral types

```
#define SWAP (a,b) {                   \
    void* p = a;    \
    a       = b;    \
    b       = p;    \
  }
```

min (a,b)

simple min macro for interagl types

```
#define min (a,b) ((a) < (b) ? (a) : (b))
```

max (a,b)

simple max macro for interagl types

```
#define max (a,b) ((a) > (b) ? (a) : (b))
```

IS_APPROX (n1,n2,err)

Check if n1 & n2 are at max err apart Expects n1 & n2 to be integral types.

```
#define IS_APPROX (n1,n2,err) ((n1 > n2) ? ((n1 - n2) <= err) : ((n2 - n1) <= err))
```

optimize_len (a,l)

changes to pointer (a) and it length (l) to remove leading 0 bytes.

```
#define optimize_len (a,l) while (l > 1 && *a == 0) { \
    l--;                  \
    a++;                  \
  }
```

TRY (exp)

executes the expression and expects the return value to be a int indicating the error.

if the return value is negative it will stop and return this value otherwise continue.

```
#define TRY (exp) {                           \
    int _r = (exp);          \
    if (_r < 0) return _r; \
  }
```

TRY_SET (var,exp)

executes the expression and expects the return value to be a int indicating the error.

the return value will be set to a existing variable (var). if the return value is negative it will stop and return this value otherwise continue.

```
#define TRY_SET (var,exp) {                              \
    var = (exp);              \
    if (var < 0) return var; \
  }
```

TRY_GOTO (exp)

executes the expression and expects the return value to be a int indicating the error.

if the return value is negative it will stop and jump (goto) to a marked position "clean". it also expects a previously declared variable "in3_ret_t res".

```
#define TRY_GOTO (exp) {                            \
    res = (exp);              \
    if (res < 0) goto clean; \
  }
```

bytes_to_long

```
uint64_t bytes_to_long(const uint8_t *data, int len);
```

converts the bytes to a unsigned long (at least the last max len bytes)

arguments:

`const uint8_t *`	**data**
`int`	**len**

returns: `uint64_t`

bytes_to_int

```
static uint32_t bytes_to_int(const uint8_t *data, int len);
```

converts the bytes to a unsigned int (at least the last max len bytes)

arguments:

`const uint8_t *`	**data**
`int`	**len**

returns: `uint32_t`

char_to_long

```
uint64_t char_to_long(const char *a, int l);
```

converts a character into a uint64_t

arguments:

`const char *`	**a**
`int`	**l**

returns: `uint64_t`

hexchar_to_int

```
uint8_t hexchar_to_int(char c);
```

converts a hexchar to byte (4bit)

arguments:

`char`	**c**

returns: `uint8_t`

u64_to_str

```
const unsigned char* u64_to_str(uint64_t value, char *pBuf, int szBuf);
```

converts a uint64_t to string (char*); buffer-size min.

21 bytes

arguments:

`uint64_t`	**value**
`char *`	**pBuf**
`int`	**szBuf**

returns: `const unsigned char *`

hex_to_bytes

```
int hex_to_bytes(const char *hexdata, int hexlen, uint8_t *out, int outlen);
```

convert a c hex string to a byte array storing it into an existing buffer.

arguments:

`const char *`	**hexdata**
`int`	**hexlen**
`uint8_t *`	**out**
`int`	**outlen**

returns: `int`

hex_to_new_bytes

```
bytes_t* hex_to_new_bytes(const char *buf, int len);
```

convert a c string to a byte array creating a new buffer

arguments:

`const char *`	**buf**
`int`	**len**

returns: *`bytes_t *`*

bytes_to_hex

```
int bytes_to_hex(const uint8_t *buffer, int len, char *out);
```

convefrts a bytes into hex

arguments:

`const uint8_t *`	**buffer**
`int`	**len**
`char *`	**out**

returns: `int`

sha3

```
bytes_t* sha3(const bytes_t *data);
```

hashes the bytes and creates a new bytes_t

arguments:

*bytes_tconst , **	**data**

returns: *`bytes_t *`*

sha3_to

```
int sha3_to(bytes_t *data, void *dst);
```

writes 32 bytes to the pointer.

arguments:

*bytes_t **	**data**
`void *`	**dst**

returns: `int`

long_to_bytes

```
void long_to_bytes(uint64_t val, uint8_t *dst);
```

converts a long to 8 bytes

arguments:

`uint64_t`	**val**
`uint8_t *`	**dst**

int_to_bytes

```
void int_to_bytes(uint32_t val, uint8_t *dst);
```

converts a int to 4 bytes

arguments:

`uint32_t`	**val**
`uint8_t *`	**dst**

_strdupn

```c
char* _strdupn(const char *src, int len);
```

duplicate the string

arguments:

`const char *`	**src**
`int`	**len**

returns: `char *`

min_bytes_len

```c
int min_bytes_len(uint64_t val);
```

calculate the min number of byte to represents the len

arguments:

`uint64_t`	**val**

returns: `int`

uint256_set

```c
void uint256_set(const uint8_t *src, wlen_t src_len, bytes32_t dst);
```

sets a variable value to 32byte word.

arguments:

`const uint8_t *`	**src**
wlen_t	**src_len**
bytes32_t	**dst**

str_replace

```c
char* str_replace(const char *orig, const char *rep, const char *with);
```

replaces a string and returns a copy.

arguments:

`const char *`	**orig**
`const char *`	**rep**
`const char *`	**with**

returns: `char *`

str_replace_pos

```
char* str_replace_pos(const char *orig, size_t pos, size_t len, const char *rep);
```

replaces a string at the given position.

arguments:

const char *	**orig**
size_t	**pos**
size_t	**len**
const char *	**rep**

returns: `char *`

str_find

```
char* str_find(const char *haystack, const char *needle);
```

lightweight strstr() replacements

arguments:

const char *	**haystack**
const char *	**needle**

returns: `char *`

current_ms

```
uint64_t current_ms();
```

current timestamp in ms.

returns: `uint64_t`

memiszero

```
static bool memiszero(uint8_t *ptr, size_t l);
```

arguments:

uint8_t *	**ptr**
size_t	**l**

returns: `bool`

8.8 Module transport/curl

8.8.1 in3_curl.h

transport-handler using libcurl.

File: src/transport/curl/in3_curl.h

send_curl

```
in3_ret_t send_curl(in3_request_t *req);
```

a transport function using curl.

You can use it by setting the transport-function-pointer in the in3_t->transport to this function:

```
#include <in3/in3_curl.h>
...
c->transport = send_curl;
```

arguments:

*in3_request_t **	**req**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (`==IN3_OK`)

in3_register_curl

```
void in3_register_curl();
```

registers curl as a default transport.

8.9 Module transport/http

8.9.1 in3_http.h

transport-handler using simple http.

File: src/transport/http/in3_http.h

send_http

```
in3_ret_t send_http(in3_request_t *req);
```

a very simple transport function, which allows to send http-requests without a dependency to curl.

Here each request will be transformed to http instead of https.

You can use it by setting the transport-function-pointer in the in3_t->transport to this function:

```
#include <in3/in3_http.h>
...
c->transport = send_http;
```

arguments:

*in3_request_t **	**req**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==IN3_OK)

8.10 Module verifier/eth1/basic

8.10.1 eth_basic.h

Ethereum Nanon verification.

File: src/verifier/eth1/basic/eth_basic.h

in3_verify_eth_basic

```
in3_ret_t in3_verify_eth_basic(in3_vctx_t *v);
```

entry-function to execute the verification context.

arguments:

*in3_vctx_t **	**v**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==IN3_OK)

eth_verify_tx_values

```
in3_ret_t eth_verify_tx_values(in3_vctx_t *vc, d_token_t *tx, bytes_t *raw);
```

verifies internal tx-values.

arguments:

*in3_vctx_t **	**vc**
*d_token_t **	**tx**
*bytes_t **	**raw**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==IN3_OK)

eth_verify_eth_getTransaction

```
in3_ret_t eth_verify_eth_getTransaction(in3_vctx_t *vc, bytes_t *tx_hash);
```

verifies a transaction.

arguments:

*in3_vctx_t **	**vc**
*bytes_t **	**tx_hash**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (`==IN3_OK`)

eth_verify_eth_getTransactionByBlock

```
in3_ret_t eth_verify_eth_getTransactionByBlock(in3_vctx_t *vc, d_token_t *blk, uint32_
↪t tx_idx);
```

verifies a transaction by block hash/number and id.

arguments:

*in3_vctx_t **	**vc**
*d_token_t **	**blk**
`uint32_t`	**tx_idx**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (`==IN3_OK`)

eth_verify_account_proof

```
in3_ret_t eth_verify_account_proof(in3_vctx_t *vc);
```

verify account-proofs

arguments:

*in3_vctx_t **	**vc**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (`==IN3_OK`)

eth_verify_eth_getBlock

```
in3_ret_t eth_verify_eth_getBlock(in3_vctx_t *vc, bytes_t *block_hash, uint64_t␣
↪blockNumber);
```

verifies a block

arguments:

in3_vctx_t *	**vc**
bytes_t *	**block_hash**
uint64_t	**blockNumber**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==IN3_OK)

in3_register_eth_basic

```
void in3_register_eth_basic();
```

this function should only be called once and will register the eth-nano verifier.

eth_verify_eth_getLog

```
in3_ret_t eth_verify_eth_getLog(in3_vctx_t *vc, int l_logs);
```

verify logs

arguments:

in3_vctx_t *	**vc**
int	**l_logs**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==IN3_OK)

eth_handle_intern

```
in3_ret_t eth_handle_intern(in3_ctx_t *ctx, in3_response_t **response);
```

this is called before a request is send

arguments:

in3_ctx_t *	**ctx**
in3_response_t **	**response**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==IN3_OK)

8.10.2 signer.h

Ethereum Nano verification.

File: src/verifier/eth1/basic/signer.h

eth_set_pk_signer

```
in3_ret_t eth_set_pk_signer(in3_t *in3, bytes32_t pk);
```

simply signer with one private key.

since the pk pointting to the 32 byte private key is not cloned, please make sure, you manage memory allocation correctly!

simply signer with one private key.

arguments:

*in3_t **	**in3**
bytes32_t	**pk**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==IN3_OK)

8.10.3 trie.h

Patricia Merkle Tree Imnpl

File: src/verifier/eth1/basic/trie.h

in3_hasher_t

hash-function

```
typedef void(* in3_hasher_t) (bytes_t *src, uint8_t *dst)
```

in3_codec_add_t

codec to organize the encoding of the nodes

```
typedef void(* in3_codec_add_t) (bytes_builder_t *bb, bytes_t *val)
```

in3_codec_finish_t

```
typedef void(* in3_codec_finish_t) (bytes_builder_t *bb, bytes_t *dst)
```

in3_codec_decode_size_t

```
typedef int(* in3_codec_decode_size_t) (bytes_t *src)
```

returns: `int(*`

in3_codec_decode_index_t

```
typedef int(* in3_codec_decode_index_t) (bytes_t *src, int index, bytes_t *dst)
```

returns: `int(*`

trie_node_t

single node in the merkle trie.

The stuct contains following fields:

`uint8_t`	**hash**	the hash of the node
bytes_t	**data**	the raw data
bytes_t	**items**	the data as list
`uint8_t`	**own_memory**	if true this is a embedded node with own memory
trie_node_type_t	**type**	type of the node
trie_nodestruct , *	**next**	used as linked list

trie_codec_t

the codec used to encode nodes.

The stuct contains following fields:

in3_codec_add_t	**encode_add**
`in3_codec_finish_t`	**encode_finish**
`in3_codec_decode_size_t`	**decode_size**
`in3_codec_decode_index_t`	**decode_item**

trie_t

a merkle trie implementation.

This is a Patricia Merkle Tree.

The stuct contains following fields:

in3_hasher_t	**hasher**	hash-function.
trie_codec_t *	**codec**	encoding of the nocds.
bytes32_t	**root**	The root-hash.
trie_node_t *	**nodes**	linked list of containes nodes

trie_new

```
trie_t* trie_new();
```

creates a new Merkle Trie.

returns: `trie_t *`

trie_free

```
void trie_free(trie_t *val);
```

frees all resources of the trie.

arguments:

*trie_t **	**val**

trie_set_value

```
void trie_set_value(trie_t *t, bytes_t *key, bytes_t *value);
```

sets a value in the trie.

The root-hash will be updated automaticly.

arguments:

*trie_t **	**t**
*bytes_t **	**key**
*bytes_t **	**value**

8.11 Module verifier/eth1/evm

8.11.1 big.h

Ethereum Nanon verification.

File: src/verifier/eth1/evm/big.h

big_is_zero

```
uint8_t big_is_zero(uint8_t *data, wlen_t l);
```

arguments:

`uint8_t *`	**data**
wlen_t	**l**

returns: `uint8_t`

big_shift_left

```
void big_shift_left(uint8_t *a, wlen_t len, int bits);
```

arguments:

uint8_t *	**a**
wlen_t	**len**
int	**bits**

big_shift_right

```
void big_shift_right(uint8_t *a, wlen_t len, int bits);
```

arguments:

uint8_t *	**a**
wlen_t	**len**
int	**bits**

big_cmp

```
int big_cmp(const uint8_t *a, const wlen_t len_a, const uint8_t *b, const wlen_t len_
↪b);
```

arguments:

const uint8_t *	**a**
wlen_tconst	**len_a**
const uint8_t *	**b**
wlen_tconst	**len_b**

returns: `int`

big_signed

```
int big_signed(uint8_t *val, wlen_t len, uint8_t *dst);
```

returns 0 if the value is positive or 1 if negavtive.

in this case the absolute value is copied to dst.

arguments:

uint8_t *	**val**
wlen_t	**len**
uint8_t *	**dst**

returns: `int`

big_int

```
int32_t big_int(uint8_t *val, wlen_t len);
```

arguments:

`uint8_t *`	**val**
wlen_t	**len**

returns: `int32_t`

big_add

```
int big_add(uint8_t *a, wlen_t len_a, uint8_t *b, wlen_t len_b, uint8_t *out, wlen_t␣
↪max);
```

arguments:

`uint8_t *`	**a**
wlen_t	**len_a**
`uint8_t *`	**b**
wlen_t	**len_b**
`uint8_t *`	**out**
wlen_t	**max**

returns: `int`

big_sub

```
int big_sub(uint8_t *a, wlen_t len_a, uint8_t *b, wlen_t len_b, uint8_t *out);
```

arguments:

`uint8_t *`	**a**
wlen_t	**len_a**
`uint8_t *`	**b**
wlen_t	**len_b**
`uint8_t *`	**out**

returns: `int`

big_mul

```
int big_mul(uint8_t *a, wlen_t la, uint8_t *b, wlen_t lb, uint8_t *res, wlen_t max);
```

arguments:

uint8_t *	**a**
wlen_t	**la**
uint8_t *	**b**
wlen_t	**lb**
uint8_t *	**res**
wlen_t	**max**

returns: `int`

big_div

```
int big_div(uint8_t *a, wlen_t la, uint8_t *b, wlen_t lb, wlen_t sig, uint8_t *res);
```

arguments:

uint8_t *	**a**
wlen_t	**la**
uint8_t *	**b**
wlen_t	**lb**
wlen_t	**sig**
uint8_t *	**res**

returns: `int`

big_mod

```
int big_mod(uint8_t *a, wlen_t la, uint8_t *b, wlen_t lb, wlen_t sig, uint8_t *res);
```

arguments:

uint8_t *	**a**
wlen_t	**la**
uint8_t *	**b**
wlen_t	**lb**
wlen_t	**sig**
uint8_t *	**res**

returns: `int`

big_exp

```
int big_exp(uint8_t *a, wlen_t la, uint8_t *b, wlen_t lb, uint8_t *res);
```

arguments:

uint8_t *	**a**
wlen_t	**la**
uint8_t *	**b**
wlen_t	**lb**
uint8_t *	**res**

returns: `int`

big_log256

```
int big_log256(uint8_t *a, wlen_t len);
```

arguments:

uint8_t *	**a**
wlen_t	**len**

returns: `int`

8.11.2 code.h

code cache.

File: src/verifier/eth1/evm/code.h

in3_get_code

```
in3_ret_t in3_get_code(in3_vctx_t *vc, address_t address, cache_entry_t **target);
```

fetches the code and adds it to the context-cache as cache_entry.

So calling this function a second time will take the result from cache.

arguments:

*in3_vctx_t **	**vc**
address_t	**address**
*cache_entry_t ***	**target**

returns: *`in3_ret_t`* the *result-status* of the function.

Please make sure you check if it was successfull (`==IN3_OK`)

8.11.3 evm.h

main evm-file.

File: src/verifier/eth1/evm/evm.h

gas_options

EVM_ERROR_EMPTY_STACK

the no more elements on the stack

```
#define EVM_ERROR_EMPTY_STACK -20
```

EVM_ERROR_INVALID_OPCODE

the opcode is not supported

```
#define EVM_ERROR_INVALID_OPCODE -21
```

EVM_ERROR_BUFFER_TOO_SMALL

reading data from a position, which is not initialized

```
#define EVM_ERROR_BUFFER_TOO_SMALL -22
```

EVM_ERROR_ILLEGAL_MEMORY_ACCESS

the memory-offset does not exist

```
#define EVM_ERROR_ILLEGAL_MEMORY_ACCESS -23
```

EVM_ERROR_INVALID_JUMPDEST

the jump destination is not marked as valid destination

```
#define EVM_ERROR_INVALID_JUMPDEST -24
```

EVM_ERROR_INVALID_PUSH

the push data is empy

```
#define EVM_ERROR_INVALID_PUSH -25
```

EVM_ERROR_UNSUPPORTED_CALL_OPCODE

error handling the call, usually because static-calls are not allowed to change state

```
#define EVM_ERROR_UNSUPPORTED_CALL_OPCODE -26
```

EVM_ERROR_TIMEOUT

the evm ran into a loop

```
#define EVM_ERROR_TIMEOUT -27
```

EVM_ERROR_INVALID_ENV

the enviroment could not deliver the data

```
#define EVM_ERROR_INVALID_ENV -28
```

EVM_ERROR_OUT_OF_GAS

not enough gas to exewcute the opcode

```
#define EVM_ERROR_OUT_OF_GAS -29
```

EVM_ERROR_BALANCE_TOO_LOW

not enough funds to transfer the requested value.

```
#define EVM_ERROR_BALANCE_TOO_LOW -30
```

EVM_ERROR_STACK_LIMIT

stack limit reached

```
#define EVM_ERROR_STACK_LIMIT -31
```

EVM_ERROR_SUCCESS_CONSUME_GAS

write success but consume all gas

```
#define EVM_ERROR_SUCCESS_CONSUME_GAS -32
```

EVM_PROP_FRONTIER

```
#define EVM_PROP_FRONTIER 1
```

EVM_PROP_EIP150

```
#define EVM_PROP_EIP150 2
```

EVM_PROP_EIP158

```
#define EVM_PROP_EIP158 4
```

EVM_PROP_CONSTANTINOPL

```
#define EVM_PROP_CONSTANTINOPL 16
```

EVM_PROP_ISTANBUL

```
#define EVM_PROP_ISTANBUL 32
```

EVM_PROP_NO_FINALIZE

```
#define EVM_PROP_NO_FINALIZE 32768
```

EVM_PROP_STATIC

```
#define EVM_PROP_STATIC 256
```

EVM_ENV_BALANCE

```
#define EVM_ENV_BALANCE 1
```

EVM_ENV_CODE_SIZE

```
#define EVM_ENV_CODE_SIZE 2
```

EVM_ENV_CODE_COPY

```
#define EVM_ENV_CODE_COPY 3
```

EVM_ENV_BLOCKHASH

```
#define EVM_ENV_BLOCKHASH 4
```

EVM_ENV_STORAGE

```
#define EVM_ENV_STORAGE 5
```

EVM_ENV_BLOCKHEADER

```
#define EVM_ENV_BLOCKHEADER 6
```

EVM_ENV_CODE_HASH

```
#define EVM_ENV_CODE_HASH 7
```

EVM_ENV_NONCE

```
#define EVM_ENV_NONCE 8
```

MATH_ADD

```
#define MATH_ADD 1
```

MATH_SUB

```
#define MATH_SUB 2
```

MATH_MUL

```
#define MATH_MUL 3
```

MATH_DIV

```
#define MATH_DIV 4
```

MATH_SDIV

```
#define MATH_SDIV 5
```

MATH_MOD

```
#define MATH_MOD 6
```

MATH_SMOD

```
#define MATH_SMOD 7
```

MATH_EXP

```
#define MATH_EXP 8
```

MATH_SIGNEXP

```
#define MATH_SIGNEXP 9
```

CALL_CALL

```
#define CALL_CALL 0
```

CALL_CODE

```
#define CALL_CODE 1
```

CALL_DELEGATE

```
#define CALL_DELEGATE 2
```

CALL_STATIC

```
#define CALL_STATIC 3
```

OP_AND

```
#define OP_AND 0
```

OP_OR

```
#define OP_OR 1
```

OP_XOR

```
#define OP_XOR 2
```

EVM_DEBUG_BLOCK (. . .)

OP_LOG (. . .)

```
#define OP_LOG (...) EVM_ERROR_UNSUPPORTED_CALL_OPCODE
```

OP_SLOAD_GAS (...)

OP_CREATE (...)

```
#define OP_CREATE (...) EVM_ERROR_UNSUPPORTED_CALL_OPCODE
```

OP_ACCOUNT_GAS (...)

```
#define OP_ACCOUNT_GAS (...) 0
```

OP_SELFDESTRUCT (...)

```
#define OP_SELFDESTRUCT (...) EVM_ERROR_UNSUPPORTED_CALL_OPCODE
```

OP_EXTCODECOPY_GAS (evm)

OP_SSTORE (...)

```
#define OP_SSTORE (...) EVM_ERROR_UNSUPPORTED_CALL_OPCODE
```

EVM_CALL_MODE_STATIC

```
#define EVM_CALL_MODE_STATIC 1
```

EVM_CALL_MODE_DELEGATE

```
#define EVM_CALL_MODE_DELEGATE 2
```

EVM_CALL_MODE_CALLCODE

```
#define EVM_CALL_MODE_CALLCODE 3
```

EVM_CALL_MODE_CALL

```
#define EVM_CALL_MODE_CALL 4
```

evm_state_t

the current state of the evm

The enum type contains the following values:

EVM_STATE_INIT	0	just initialised, but not yet started
EVM_STATE_RUNNING	1	started and still running
EVM_STATE_STOPPED	2	successfully stopped
EVM_STATE_REVERTED	3	stopped, but results must be reverted

evm_get_env

This function provides data from the enviroment.

depending on the key the function will set the out_data-pointer to the result. This means the enviroment is responsible for memory management and also to clean up resources afterwards.

```
typedef int(* evm_get_env) (void *evm, uint16_t evm_key, uint8_t *in_data, int in_len,
↪ uint8_t **out_data, int offset, int len)
```

returns: `int(*`

storage_t

The stuct contains following fields:

bytes32_t	**key**
bytes32_t	**value**
*account_storagestruct , **	**next**

logs_t

The stuct contains following fields:

bytes_t	**topics**
bytes_t	**data**
*logsstruct , **	**next**

account_t

The stuct contains following fields:

address_t	**address**
bytes32_t	**balance**
bytes32_t	**nonce**
bytes_t	**code**
*storage_t **	**storage**
*accountstruct , **	**next**

evm_t

The stuct contains following fields:

bytes_builder_t	**stack**	
bytes_builder_t	**memory**	
`int`	**stack_size**	
bytes_t	**code**	
`uint32_t`	**pos**	
evm_state_t	**state**	
bytes_t	**last_returned**	
bytes_t	**return_data**	
`uint32_t *`	**invalid_jumpdest**	
`uint32_t`	**properties**	
evm_get_env	**env**	
`void *`	**env_ptr**	
`uint64_t`	**chain_id**	the chain_id as returned by the opcode
`uint8_t *`	**address**	the address of the current storage
`uint8_t *`	**account**	the address of the code
`uint8_t *`	**origin**	the address of original sender of the root-transaction
`uint8_t *`	**caller**	the address of the parent sender
bytes_t	**call_value**	value send
bytes_t	**call_data**	data send in the tx
bytes_t	**gas_price**	current gasprice
`uint64_t`	**gas**	
	gas_options	

evm_stack_push

```
int evm_stack_push(evm_t *evm, uint8_t *data, uint8_t len);
```

arguments:

*evm_t **	**evm**
`uint8_t *`	**data**
`uint8_t`	**len**

returns: `int`

evm_stack_push_ref

```
int evm_stack_push_ref(evm_t *evm, uint8_t **dst, uint8_t len);
```

arguments:

*evm_t **	**evm**
`uint8_t **`	**dst**
`uint8_t`	**len**

returns: `int`

evm_stack_push_int

```
int evm_stack_push_int(evm_t *evm, uint32_t val);
```

arguments:

*evm_t **	**evm**
uint32_t	**val**

returns: int

evm_stack_push_long

```
int evm_stack_push_long(evm_t *evm, uint64_t val);
```

arguments:

*evm_t **	**evm**
uint64_t	**val**

returns: int

evm_stack_get_ref

```
int evm_stack_get_ref(evm_t *evm, uint8_t pos, uint8_t **dst);
```

arguments:

*evm_t **	**evm**
uint8_t	**pos**
uint8_t **	**dst**

returns: int

evm_stack_pop

```
int evm_stack_pop(evm_t *evm, uint8_t *dst, uint8_t len);
```

arguments:

*evm_t **	**evm**
uint8_t *	**dst**
uint8_t	**len**

returns: int

evm_stack_pop_ref

```
int evm_stack_pop_ref(evm_t *evm, uint8_t **dst);
```

arguments:

*evm_t **	**evm**
`uint8_t **`	**dst**

returns: `int`

evm_stack_pop_byte

```
int evm_stack_pop_byte(evm_t *evm, uint8_t *dst);
```

arguments:

*evm_t **	**evm**
`uint8_t *`	**dst**

returns: `int`

evm_stack_pop_int

```
int32_t evm_stack_pop_int(evm_t *evm);
```

arguments:

*evm_t **	**evm**

returns: `int32_t`

evm_stack_peek_len

```
int evm_stack_peek_len(evm_t *evm);
```

arguments:

*evm_t **	**evm**

returns: `int`

evm_run

```
int evm_run(evm_t *evm, address_t code_address);
```

arguments:

*evm_t **	**evm**
address_t	**code_address**

returns: int

evm_sub_call

```
int evm_sub_call(evm_t *parent, uint8_t address[20], uint8_t account[20], uint8_t␣
↪*value, wlen_t l_value, uint8_t *data, uint32_t l_data, uint8_t caller[20], uint8_t␣
↪origin[20], uint64_t gas, wlen_t mode, uint32_t out_offset, uint32_t out_len);
```

handle internal calls.

arguments:

*evm_t **	**parent**
uint8_t	**address**
uint8_t	**account**
uint8_t *	**value**
wlen_t	**l_value**
uint8_t *	**data**
uint32_t	**l_data**
uint8_t	**caller**
uint8_t	**origin**
uint64_t	**gas**
wlen_t	**mode**
uint32_t	**out_offset**
uint32_t	**out_len**

returns: int

evm_ensure_memory

```
int evm_ensure_memory(evm_t *evm, uint32_t max_pos);
```

arguments:

*evm_t **	**evm**
uint32_t	**max_pos**

returns: int

in3_get_env

```
int in3_get_env(void *evm_ptr, uint16_t evm_key, uint8_t *in_data, int in_len, uint8_
↪t **out_data, int offset, int len);
```

arguments:

void *	**evm_ptr**
uint16_t	**evm_key**
uint8_t *	**in_data**
int	**in_len**
uint8_t **	**out_data**
int	**offset**
int	**len**

returns: int

evm_call

```
int evm_call(void *vc, uint8_t address[20], uint8_t *value, wlen_t l_value, uint8_t *data, uint32_t l_data, uint8_t caller[20], uint64_t gas, uint64_t chain_id, bytes_t **result);
```

run a evm-call

arguments:

void *	**vc**
uint8_t	**address**
uint8_t *	**value**
wlen_t	**l_value**
uint8_t *	**data**
uint32_t	**l_data**
uint8_t	**caller**
uint64_t	**gas**
uint64_t	**chain_id**
bytes_t **	**result**

returns: int

evm_print_stack

```
void evm_print_stack(evm_t *evm, uint64_t last_gas, uint32_t pos);
```

arguments:

evm_t *	**evm**
uint64_t	**last_gas**
uint32_t	**pos**

evm_free

```
void evm_free(evm_t *evm);
```

arguments:

*evm_t **	**evm**

evm_execute

```
int evm_execute(evm_t *evm);
```

arguments:

*evm_t **	**evm**

returns: `int`

8.11.4 gas.h

evm gas defines.

File: src/verifier/eth1/evm/gas.h

op_exec (m,gas)

```
#define op_exec (m,gas) return m;
```

subgas (g)

GAS_CC_NET_SSTORE_NOOP_GAS

Once per SSTORE operation if the value doesn't change.

```
#define GAS_CC_NET_SSTORE_NOOP_GAS 200
```

GAS_CC_NET_SSTORE_INIT_GAS

Once per SSTORE operation from clean zero.

```
#define GAS_CC_NET_SSTORE_INIT_GAS 20000
```

GAS_CC_NET_SSTORE_CLEAN_GAS

Once per SSTORE operation from clean non-zero.

```
#define GAS_CC_NET_SSTORE_CLEAN_GAS 5000
```

GAS_CC_NET_SSTORE_DIRTY_GAS

Once per SSTORE operation from dirty.

```
#define GAS_CC_NET_SSTORE_DIRTY_GAS 200
```

GAS_CC_NET_SSTORE_CLEAR_REFUND

Once per SSTORE operation for clearing an originally existing storage slot.

```
#define GAS_CC_NET_SSTORE_CLEAR_REFUND 15000
```

GAS_CC_NET_SSTORE_RESET_REFUND

Once per SSTORE operation for resetting to the original non-zero value.

```
#define GAS_CC_NET_SSTORE_RESET_REFUND 4800
```

GAS_CC_NET_SSTORE_RESET_CLEAR_REFUND

Once per SSTORE operation for resetting to the original zero valuev.

```
#define GAS_CC_NET_SSTORE_RESET_CLEAR_REFUND 19800
```

G_ZERO

Nothing is paid for operations of the set Wzero.

```
#define G_ZERO 0
```

G_JUMPDEST

JUMP DEST.

```
#define G_JUMPDEST 1
```

G_BASE

This is the amount of gas to pay for operations of the set Wbase.

```
#define G_BASE 2
```

G_VERY_LOW

This is the amount of gas to pay for operations of the set Wverylow.

```
#define G_VERY_LOW 3
```

G_LOW

This is the amount of gas to pay for operations of the set Wlow.

```
#define G_LOW 5
```

G_MID

This is the amount of gas to pay for operations of the set Wmid.

```
#define G_MID 8
```

G_HIGH

This is the amount of gas to pay for operations of the set Whigh.

```
#define G_HIGH 10
```

G_EXTCODE

This is the amount of gas to pay for operations of the set Wextcode.

```
#define G_EXTCODE 700
```

G_BALANCE

This is the amount of gas to pay for a BALANCE operation.

```
#define G_BALANCE 400
```

G_SLOAD

This is paid for an SLOAD operation.

```
#define G_SLOAD 200
```

G_SSET

This is paid for an SSTORE operation when the storage value is set to non-zero from zero.

```
#define G_SSET 20000
```

G_SRESET

This is the amount for an SSTORE operation when the storage value’s zeroness remains unchanged or is set to zero.

```
#define G_SRESET 5000
```

R_SCLEAR

This is the refund given (added into the refund counter) when the storage value is set to zero from non-zero.

```
#define R_SCLEAR 15000
```

R_SELFDESTRUCT

This is the refund given (added into the refund counter) for self-destructing an account.

```
#define R_SELFDESTRUCT 24000
```

G_SELFDESTRUCT

This is the amount of gas to pay for a SELFDESTRUCT operation.

```
#define G_SELFDESTRUCT 5000
```

G_CREATE

This is paid for a CREATE operation.

```
#define G_CREATE 32000
```

G_CODEDEPOSIT

This is paid per byte for a CREATE operation to succeed in placing code into the state.

```
#define G_CODEDEPOSIT 200
```

G_CALL

This is paid for a CALL operation.

```
#define G_CALL 700
```

G_CALLVALUE

This is paid for a non-zero value transfer as part of the CALL operation.

```
#define G_CALLVALUE 9000
```

G_CALLSTIPEND

This is a stipend for the called contract subtracted from Gcallvalue for a non-zero value transfer.

```
#define G_CALLSTIPEND 2300
```

G_NEWACCOUNT

This is paid for a CALL or for a SELFDESTRUCT operation which creates an account.

```
#define G_NEWACCOUNT 25000
```

G_EXP

This is a partial payment for an EXP operation.

```
#define G_EXP 10
```

G_EXPBYTE

This is a partial payment when multiplied by dlog256(exponent)e for the EXP operation.

```
#define G_EXPBYTE 50
```

G_MEMORY

This is paid for every additional word when expanding memory.

```
#define G_MEMORY 3
```

G_TXCREATE

This is paid by all contract-creating transactions after the Homestead transition.

```
#define G_TXCREATE 32000
```

G_TXDATA_ZERO

This is paid for every zero byte of data or code for a transaction.

```
#define G_TXDATA_ZERO 4
```

G_TXDATA_NONZERO

This is paid for every non-zero byte of data or code for a transaction.

```
#define G_TXDATA_NONZERO 68
```

G_TRANSACTION

This is paid for every transaction.

```
#define G_TRANSACTION 21000
```

G_LOG

This is a partial payment for a LOG operation.

```
#define G_LOG 375
```

G_LOGDATA

This is paid for each byte in a LOG operation's data.

```
#define G_LOGDATA 8
```

G_LOGTOPIC

This is paid for each topic of a LOG operation.

```
#define G_LOGTOPIC 375
```

G_SHA3

This is paid for each SHA3 operation.

```
#define G_SHA3 30
```

G_SHA3WORD

This is paid for each word (rounded up) for input data to a SHA3 operation.

```
#define G_SHA3WORD 6
```

G_COPY

This is a partial payment for *COPY operations, multiplied by the number of words copied, rounded up.

```
#define G_COPY 3
```

G_BLOCKHASH

This is a payment for a BLOCKHASH operation.

```
#define G_BLOCKHASH 20
```

G_PRE_EC_RECOVER

Precompile EC RECOVER.

```
#define G_PRE_EC_RECOVER 3000
```

G_PRE_SHA256

Precompile SHA256.

```
#define G_PRE_SHA256 60
```

G_PRE_SHA256_WORD

Precompile SHA256 per word.

```
#define G_PRE_SHA256_WORD 12
```

G_PRE_RIPEMD160

Precompile RIPEMD160.

```
#define G_PRE_RIPEMD160 600
```

G_PRE_RIPEMD160_WORD

Precompile RIPEMD160 per word.

```
#define G_PRE_RIPEMD160_WORD 120
```

G_PRE_IDENTITY

Precompile IDENTIY (copyies data)

```
#define G_PRE_IDENTITY 15
```

G_PRE_IDENTITY_WORD

Precompile IDENTIY per word.

```
#define G_PRE_IDENTITY_WORD 3
```

G_PRE_MODEXP_GQUAD_DIVISOR

Gquaddivisor from modexp precompile for gas calculation.

```
#define G_PRE_MODEXP_GQUAD_DIVISOR 20
```

G_PRE_ECADD

Gas costs for curve addition precompile.

```
#define G_PRE_ECADD 500
```

G_PRE_ECMUL

Gas costs for curve multiplication precompile.

```
#define G_PRE_ECMUL 40000
```

G_PRE_ECPAIRING

Base gas costs for curve pairing precompile.

```
#define G_PRE_ECPAIRING 100000
```

G_PRE_ECPAIRING_WORD

Gas costs regarding curve pairing precompile input length.

```
#define G_PRE_ECPAIRING_WORD 80000
```

EVM_STACK_LIMIT

max elements of the stack

```
#define EVM_STACK_LIMIT 1024
```

EVM_MAX_CODE_SIZE

max size of the code

```
#define EVM_MAX_CODE_SIZE 24576
```

FRONTIER_G_EXPBYTE

fork values

This is a partial payment when multiplied by dlog256(exponent)e for the EXP operation.

```
#define FRONTIER_G_EXPBYTE 10
```

FRONTIER_G_SLOAD

This is a partial payment when multiplied by dlog256(exponent)e for the EXP operation.

```
#define FRONTIER_G_SLOAD 50
```

FREE_EVM (. . .)

INIT_EVM (. . .)

INIT_GAS (. . .)

SUBGAS (. . .)

FINALIZE_SUBCALL_GAS (. . .)

UPDATE_SUBCALL_GAS (. . .)

FINALIZE_AND_REFUND_GAS (. . .)

KEEP_TRACK_GAS (evm)

```
#define KEEP_TRACK_GAS (evm) 0
```

SELFDESTRUCT_GAS (evm,g)

```
#define SELFDESTRUCT_GAS (evm,g) EVM_ERROR_UNSUPPORTED_CALL_OPCODE
```

UPDATE_ACCOUNT_CODE (. . .)

8.12 Module verifier/eth1/full

8.12.1 eth_full.h

Ethereum Nanon verification.

File: src/verifier/eth1/full/eth_full.h

in3_verify_eth_full

```
int in3_verify_eth_full(in3_vctx_t *v);
```

entry-function to execute the verification context.

arguments:

*in3_vctx_t **	**v**

returns: `int`

in3_register_eth_full

```
void in3_register_eth_full();
```

this function should only be called once and will register the eth-full verifier.

8.13 Module verifier/eth1/nano

8.13.1 chainspec.h

Ethereum chain specification

File: src/verifier/eth1/nano/chainspec.h

BLOCK_LATEST

```
#define BLOCK_LATEST 0xFFFFFFFFFFFFFFFF
```

eip_transition_t

The stuct contains following fields:

uint64_t	**transition_block**
eip_t	**eips**

consensus_transition_t

The stuct contains following fields:

uint64_t	**transition_block**
eth_consensus_type_t	**type**
bytes_t	**validators**
uint8_t *	**contract**

chainspec_t

The stuct contains following fields:

uint64_t	**network_id**
uint64_t	**account_start_nonce**
uint32_t	**eip_transitions_len**
eip_transition_t *	**eip_transitions**
uint32_t	**consensus_transitions_len**
consensus_transition_t *	**consensus_transitions**

attribute

```
struct __attribute__((__packed__)) eip_;
```

defines the flags for the current activated EIPs.

Since it does not make sense to support a evm defined before Homestead, homestead EIP is always turned on!

< REVERT instruction

< Bitwise shifting instructions in EVM

< Gas cost changes for IO-heavy operations

< Simple replay attack protection

< EXP cost increase

< Contract code size limit

< Precompiled contracts for addition and scalar multiplication on the elliptic curve alt_bn128

< Precompiled contracts for optimal ate pairing check on the elliptic curve alt_bn128

< Big integer modular exponentiation

< New opcodes: RETURNDATASIZE and RETURNDATACOPY

< New opcode STATICCALL

< Embedding transaction status code in receipts

< Skinny CREATE2

< EXTCODEHASH opcode

< Net gas metering for SSTORE without dirty maps

arguments:

(__packed__)

returns: `struct`

chainspec_create_from_json

```
chainspec_t* chainspec_create_from_json(d_token_t *data);
```

arguments:

*d_token_t **	**data**

returns: *`chainspec_t *`*

chainspec_get_eip

```
eip_t chainspec_get_eip(chainspec_t *spec, uint64_t block_number);
```

arguments:

*chainspec_t **	**spec**
`uint64_t`	**block_number**

returns: `eip_t`

chainspec_get_consensus

```
consensus_transition_t* chainspec_get_consensus(chainspec_t *spec, uint64_t block_
↪number);
```

arguments:

*chainspec_t **	**spec**
`uint64_t`	**block_number**

returns: `consensus_transition_t *`

chainspec_to_bin

```
in3_ret_t chainspec_to_bin(chainspec_t *spec, bytes_builder_t *bb);
```

arguments:

*chainspec_t **	**spec**
*bytes_builder_t **	**bb**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==`IN3_OK`)

chainspec_from_bin

```
chainspec_t* chainspec_from_bin(void *raw);
```

arguments:

`void *`	**raw**

returns: `chainspec_t *`

chainspec_get

```
chainspec_t* chainspec_get(chain_id_t chain_id);
```

arguments:

chain_id_t	**chain_id**

returns: `chainspec_t *`

chainspec_put

```
void chainspec_put(chain_id_t chain_id, chainspec_t *spec);
```

arguments:

chain_id_t	**chain_id**
*chainspec_t **	**spec**

8.13.2 eth_nano.h

Ethereum Nanon verification.

File: src/verifier/eth1/nano/eth_nano.h

in3_verify_eth_nano

```
in3_ret_t in3_verify_eth_nano(in3_vctx_t *v);
```

entry-function to execute the verification context.

arguments:

*in3_vctx_t **	**v**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==IN3_OK)

eth_verify_blockheader

```
in3_ret_t eth_verify_blockheader(in3_vctx_t *vc, bytes_t *header, bytes_t *expected_
↪blockhash);
```

verifies a blockheader.

verifies a blockheader.

arguments:

*in3_vctx_t **	**vc**
*bytes_t **	**header**
*bytes_t **	**expected_blockhash**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==IN3_OK)

eth_verify_signature

```
int eth_verify_signature(in3_vctx_t *vc, bytes_t *msg_hash, d_token_t *sig);
```

verifies a single signature blockheader.

This function will return a positive integer with a bitmask holding the bit set according to the address that signed it. This is based on the signatiures in the request-config.

arguments:

*in3_vctx_t **	**vc**
*bytes_t **	**msg_hash**
*d_token_t **	**sig**

returns: `int`

ecrecover_signature

```
bytes_t* ecrecover_signature(bytes_t *msg_hash, d_token_t *sig);
```

returns the address of the signature if the msg_hash is correct

arguments:

*bytes_t **	**msg_hash**
*d_token_t **	**sig**

returns: `bytes_t *`

eth_verify_eth_getTransactionReceipt

```
in3_ret_t eth_verify_eth_getTransactionReceipt(in3_vctx_t *vc, bytes_t *tx_hash);
```

verifies a transaction receipt.

arguments:

*in3_vctx_t **	**vc**
*bytes_t **	**tx_hash**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==`IN3_OK`)

eth_verify_in3_nodelist

```
in3_ret_t eth_verify_in3_nodelist(in3_vctx_t *vc, uint32_t node_limit, bytes_t *seed,
↪d_token_t *required_addresses);
```

verifies the nodelist.

arguments:

*in3_vctx_t **	**vc**
`uint32_t`	**node_limit**
*bytes_t **	**seed**
*d_token_t **	**required_addresses**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==IN3_OK)

eth_verify_in3_whitelist

```
in3_ret_t eth_verify_in3_whitelist(in3_vctx_t *vc);
```

verifies the nodelist.

arguments:

*in3_vctx_t **	**vc**

returns: `in3_ret_t` the *result-status* of the function.

Please make sure you check if it was successfull (==IN3_OK)

in3_register_eth_nano

```
void in3_register_eth_nano();
```

this function should only be called once and will register the eth-nano verifier.

create_tx_path

```
bytes_t* create_tx_path(uint32_t index);
```

helper function to rlp-encode the transaction_index.

The result must be freed after use!

arguments:

`uint32_t`	**index**

returns: `bytes_t *`

8.13.3 merkle.h

Merkle Proof Verification.

File: src/verifier/eth1/nano/merkle.h

MERKLE_DEPTH_MAX

```
#define MERKLE_DEPTH_MAX 64
```

trie_verify_proof

```
int trie_verify_proof(bytes_t *rootHash, bytes_t *path, bytes_t **proof, bytes_t *expectedValue);
```

verifies a merkle proof.

expectedValue == NULL : value must not exist expectedValue.data ==NULL : please copy the data I want to evaluate it afterwards. expectedValue.data !=NULL : the value must match the data.

arguments:

bytes_t *	**rootHash**
bytes_t *	**path**
bytes_t **	**proof**
bytes_t *	**expectedValue**

returns: `int`

trie_path_to_nibbles

```
uint8_t* trie_path_to_nibbles(bytes_t path, int use_prefix);
```

helper function split a path into 4-bit nibbles.

The result must be freed after use!

arguments:

bytes_t	**path**
`int`	**use_prefix**

returns: `uint8_t *` : the resulting bytes represent a 4bit-number each and are terminated with a 0xFF.

trie_matching_nibbles

```
int trie_matching_nibbles(uint8_t *a, uint8_t *b);
```

helper function to find the number of nibbles matching both paths.

arguments:

`uint8_t *`	**a**
`uint8_t *`	**b**

returns: `int`

trie_free_proof

```
void trie_free_proof(bytes_t **proof);
```

used to free the NULL-terminated proof-array.

arguments:

bytes_t **	**proof**

8.13.4 rlp.h

RLP-En/Decoding as described in the Ethereum RLP-Spec.

This decoding works without allocating new memory.

File: src/verifier/eth1/nano/rlp.h

rlp_decode

```
int rlp_decode(bytes_t *b, int index, bytes_t *dst);
```

this function decodes the given bytes and returns the element with the given index by updating the reference of dst.

the bytes will only hold references and do **not** need to be freed!

```
bytes_t* tx_raw = serialize_tx(tx);

bytes_t item;

// decodes the tx_raw by letting the item point to range of the first element, which␣
↪should be the body of a list.
if (rlp_decode(tx_raw, 0, &item) !=2) return -1 ;

// now decode the 4th element (which is the value) and let item point to that range.
if (rlp_decode(&item, 4, &item) !=1) return -1 ;
```

arguments:

bytes_t *	**b**
`int`	**index**
bytes_t *	**dst**

returns: `int` : - 0 : means item out of range

- 1 : item found
- 2 : list found (you can then decode the same bytes again)

rlp_decode_in_list

```
int rlp_decode_in_list(bytes_t *b, int index, bytes_t *dst);
```

this function expects a list item (like the blockheader as first item and will then find the item within this list).

It is a shortcut for

```
// decode the list
if (rlp_decode(b,0,dst)!=2) return 0;
// and the decode the item
return rlp_decode(dst,index,dst);
```

arguments:

*bytes_t **	**b**
`int`	**index**
*bytes_t **	**dst**

returns: `int` : - 0 : means item out of range

- 1 : item found
- 2 : list found (you can then decode the same bytes again)

rlp_decode_len

```
int rlp_decode_len(bytes_t *b);
```

returns the number of elements found in the data.

arguments:

*bytes_t **	**b**

returns: `int`

rlp_encode_item

```
void rlp_encode_item(bytes_builder_t *bb, bytes_t *val);
```

encode a item as single string and add it to the bytes_builder.

arguments:

*bytes_builder_t **	**bb**
*bytes_t **	**val**

rlp_encode_list

```
void rlp_encode_list(bytes_builder_t *bb, bytes_t *val);
```

encode a the value as list of already encoded items.

arguments:

*bytes_builder_t **	**bb**
*bytes_t **	**val**

rlp_encode_to_list

```
bytes_builder_t* rlp_encode_to_list(bytes_builder_t *bb);
```

converts the data in the builder to a list.

This function is optimized to not increase the memory more than needed and is fastet than creating a second builder to encode the data.

arguments:

*bytes_builder_t **	**bb**

returns: `bytes_builder_t *` : the same builder.

rlp_encode_to_item

```
bytes_builder_t* rlp_encode_to_item(bytes_builder_t *bb);
```

converts the data in the builder to a rlp-encoded item.

This function is optimized to not increase the memory more than needed and is fastet than creating a second builder to encode the data.

arguments:

*bytes_builder_t **	**bb**

returns: `bytes_builder_t *` : the same builder.

rlp_add_length

```
void rlp_add_length(bytes_builder_t *bb, uint32_t len, uint8_t offset);
```

helper to encode the prefix for a value

arguments:

*bytes_builder_t **	**bb**
`uint32_t`	**len**
`uint8_t`	**offset**

8.13.5 serialize.h

serialization of ETH-Objects.

This incoming tokens will represent their values as properties based on JSON-RPC.

File: src/verifier/eth1/nano/serialize.h

BLOCKHEADER_PARENT_HASH

```
#define BLOCKHEADER_PARENT_HASH 0
```

BLOCKHEADER_SHA3_UNCLES

```
#define BLOCKHEADER_SHA3_UNCLES 1
```

BLOCKHEADER_MINER

```
#define BLOCKHEADER_MINER 2
```

BLOCKHEADER_STATE_ROOT

```
#define BLOCKHEADER_STATE_ROOT 3
```

BLOCKHEADER_TRANSACTIONS_ROOT

```
#define BLOCKHEADER_TRANSACTIONS_ROOT 4
```

BLOCKHEADER_RECEIPT_ROOT

```
#define BLOCKHEADER_RECEIPT_ROOT 5
```

BLOCKHEADER_LOGS_BLOOM

```
#define BLOCKHEADER_LOGS_BLOOM 6
```

BLOCKHEADER_DIFFICULTY

```
#define BLOCKHEADER_DIFFICULTY 7
```

BLOCKHEADER_NUMBER

```
#define BLOCKHEADER_NUMBER 8
```

BLOCKHEADER_GAS_LIMIT

```
#define BLOCKHEADER_GAS_LIMIT 9
```

BLOCKHEADER_GAS_USED

```
#define BLOCKHEADER_GAS_USED 10
```

BLOCKHEADER_TIMESTAMP

```
#define BLOCKHEADER_TIMESTAMP 11
```

BLOCKHEADER_EXTRA_DATA

```
#define BLOCKHEADER_EXTRA_DATA 12
```

BLOCKHEADER_SEALED_FIELD1

```
#define BLOCKHEADER_SEALED_FIELD1 13
```

BLOCKHEADER_SEALED_FIELD2

```
#define BLOCKHEADER_SEALED_FIELD2 14
```

BLOCKHEADER_SEALED_FIELD3

```
#define BLOCKHEADER_SEALED_FIELD3 15
```

serialize_tx_receipt

```
bytes_t* serialize_tx_receipt(d_token_t *receipt);
```

creates rlp-encoded raw bytes for a receipt.

The bytes must be freed with b_free after use!

arguments:

*d_token_t **	**receipt**

returns: `bytes_t *`

serialize_tx

```
bytes_t* serialize_tx(d_token_t *tx);
```

creates rlp-encoded raw bytes for a transaction.

The bytes must be freed with b_free after use!

arguments:

*d_token_t **	**tx**

returns: `bytes_t *`

serialize_tx_raw

```
bytes_t* serialize_tx_raw(bytes_t nonce, bytes_t gas_price, bytes_t gas_limit, bytes_
↪t to, bytes_t value, bytes_t data, uint64_t v, bytes_t r, bytes_t s);
```

creates rlp-encoded raw bytes for a transaction from direct values.

The bytes must be freed with b_free after use!

arguments:

bytes_t	**nonce**
bytes_t	**gas_price**
bytes_t	**gas_limit**
bytes_t	**to**
bytes_t	**value**
bytes_t	**data**
`uint64_t`	**v**
bytes_t	**r**
bytes_t	**s**

returns: `bytes_t *`

serialize_account

```
bytes_t* serialize_account(d_token_t *a);
```

creates rlp-encoded raw bytes for a account.

The bytes must be freed with b_free after use!

arguments:

*d_token_t **	**a**

returns: `bytes_t *`

serialize_block_header

```
bytes_t* serialize_block_header(d_token_t *block);
```

creates rlp-encoded raw bytes for a blockheader.

The bytes must be freed with b_free after use!

arguments:

*d_token_t **	**block**

returns: `bytes_t *`

rlp_add

```
int rlp_add(bytes_builder_t *rlp, d_token_t *t, int ml);
```

adds the value represented by the token rlp-encoded to the byte_builder.

arguments:

*bytes_builder_t **	**rlp**
*d_token_t **	**t**
`int`	**ml**

returns: `int` : 0 if added -1 if the value could not be handled.

CHAPTER 9

API Reference TS

This page contains a list of all Datastructures and Classes used within the TypeScript IN3 Client.

9.1 Examples

This is a collection of different incubed-examples.

9.1.1 using Web3

Since incubed works with on a JSON-RPC-Level it can easily be used as Provider for Web3:

```
// import in3-Module
import In3Client from 'in3'
import * as web3 from 'web3'

// use the In3Client as Http-Provider
const web3 = new Web3(new In3Client({
    proof         : 'standard',
    signatureCount: 1,
    requestCount  : 2,
    chainId       : 'mainnet'
}).createWeb3Provider())

// use the web3
const block = await web.eth.getBlockByNumber('latest')
...
```

9.1.2 using Incubed API

Incubed includes a light API, allowinng not only to use all RPC-Methods in a typesafe way, but also to sign transactions and call funnctions of a contract without the web3-library.

For more details see the API-Doc

```
// import in3-Module
import In3Client from 'in3'

// use the In3Client
const in3 = new In3Client({
    proof         : 'standard',
    signatureCount: 1,
    requestCount  : 2,
    chainId       : 'mainnet'
})

// use the api to call a funnction..
const myBalance = await in3.eth.callFn(myTokenContract, 'balanceOf(address):uint',␣
↪myAccount)

// ot to send a transaction..
const receipt = await in3.eth.sendTransaction({
  to           : myTokenContract,
  method       : 'transfer(address,uint256)',
  args         : [target,amount],
  confirmations: 2,
  pk           : myKey
})

...
```

9.1.3 Reading event with incubed

```
// import in3-Module
import In3Client from 'in3'

// use the In3Client
const in3 = new In3Client({
    proof         : 'standard',
    signatureCount: 1,
    requestCount  : 2,
    chainId       : 'mainnet'
})

// use the ABI-String of the smart contract
abi = [{"anonymous":false,"inputs":[{"indexed":false,"name":"name","type":"string"},{
↪"indexed":true,"name":"label","type":"bytes32"},{"indexed":true,"name":"owner","type
↪":"address"},{"indexed":false,"name":"cost","type":"uint256"},{"indexed":false,"name
↪":"expires","type":"uint256"}],"name":"NameRegistered","type":"event"}]

// create a contract-object for a given address
const contract = in3.eth.contractAt(abi, '0xF0AD5cAd05e10572EfcEB849f6Ff0c68f9700455
↪') // ENS contract.

// read all events starting from a specified block until the latest
const logs = await c.events.NameRegistered.getLogs({fromBlock:8022948}))

// print out the properties of the event.
for (const ev of logs)
```

(continues on next page)

(continued from previous page)

```
  console.log(`${ev.owner} registered ${ev.name} for ${ev.cost} wei until ${new Date(ev.expires.toNumber()*1000).toString()}`)

...
```

9.2 Main Module

Importing incubed is as easy as

```
import Client,{util} from "in3"
```

While the In3Client-class is the default import, the following imports can be used:

Type	*ABI*	the ABI
Interface	*AccountProof*	the AccountProof
Interface	*AuraValidatoryProof*	the AuraValidatoryProof
Type	*BlockData*	the BlockData
Type	*BlockType*	the BlockType
Interface	*ChainSpec*	the ChainSpec
Class	*IN3Client*	the IN3Client
Interface	*IN3Config*	the IN3Config
Interface	*IN3NodeConfig*	the IN3NodeConfig
Interface	*IN3NodeWeight*	the IN3NodeWeight
Interface	*IN3RPCConfig*	the IN3RPCConfig
Interface	*IN3RPCHandlerConfig*	the IN3RPCHandlerConfig

Continued on next page

Table 1 – continued from previous page

Interface	*IN3RPCRequestConfig*	the IN3RPCRequestConfig
Interface	*IN3ResponseConfig*	the IN3ResponseConfig
Type	*Log*	the Log
Type	*LogData*	the LogData
Interface	*LogProof*	the LogProof
Interface	*Proof*	the Proof
Interface	*RPCRequest*	the RPCRequest
Interface	*RPCResponse*	the RPCResponse
Type	*ReceiptData*	the ReceiptData
Interface	*ServerList*	the ServerList
Interface	*Signature*	the Signature
Type	*Transaction*	the Transaction
Type	*TransactionData*	the TransactionData
Type	*TransactionReceipt*	the TransactionReceipt
Type	*Transport*	the Transport
`any`	AxiosTransport	the AxiosTransport value= `transport.AxiosTransport`

Continued on next page

Table 1 – continued from previous page

EthAPI	EthAPI	the EthAPI value= `_ethapi.default`
`any`	cbor	the cbor value= `_cbor`
	chainAliases	the chainAliases value= `aliases`
chainData	chainData	the chainData value= `_chainData`
`number` []	createRandomIndexes (len:`number`, limit:`number`, seed:*Buffer* , result:`number` [])	helper function creating deterministic random indexes used for limited nodelists
header	header	the header value= `_header`
serialize	serialize	the serialize value= `_serialize`
`any`	storage	the storage value= `_storage`
`any`	transport	the transport value= `_transport`
	typeDefs	the typeDefs value= `types.validationDef`
`any`	util	the util value= `_util`

Continued on next page

Table 1 – continued from previous page

`any`	validate	the validate value= `validateOb.validate`

9.3 Package client

9.3.1 Type Client

Source: client/Client.ts

Client for N3.

`number`	defaultMaxListeners	the defaultMaxListeners
`number`	listenerCount (emitter:*EventEmitter* , event:`string` | `symbol`)	listener count
Client	constructor (config:*Partial<IN3Config>* , transport:*Transport*)	creates a new Client.
IN3Config	defConfig	the defConfig
EthAPI	eth	the eth
IpfsAPI	ipfs	the ipfs
IN3Config	config	config
`this`	addListener (event:`string` | `symbol`, listener:)	add listener

Continued on next page

Table 2 – continued from previous page

`Promise<any>`	call (method:`string`, params:`any`, chain:`string`, config:*Partial<IN3Config>*)	sends a simply RPC-Request
`void`	clearStats ()	clears all stats and weights, like blocklisted nodes
`any`	createWeb3Provider ()	create web3 provider
`boolean`	emit (event:`string` | `symbol`, args:`any` [])	emit
Array<>	eventNames ()	event names
ChainContext	getChainContext (chainId:`string`)	Context for a specific chain including cache and chainSpecs.
`number`	getMaxListeners ()	get max listeners
`number`	listenerCount (type:`string` | `symbol`)	listener count
Function []	listeners (event:`string` | `symbol`)	listeners
`this`	off (event:`string` | `symbol`, listener:)	off

Continued on next page

Table 2 – continued from previous page

`this`	on (event:`string` | `symbol`, listener:)	on
`this`	once (event:`string` | `symbol`, listener:)	once
`this`	prependListener (event:`string` | `symbol`, listener:)	prepend listener
`this`	prependOnceListener (event:`string` | `symbol`, listener:)	prepend once listener
Function []	rawListeners (event:`string` | `symbol`)	raw listeners
`this`	removeAllListeners (event:`string` | `symbol`)	remove all listeners
`this`	removeListener (event:`string` | `symbol`, listener:)	remove listener

Continued on next page

Table 2 – continued from previous page

`Promise<>`	send (request:*RPCRequest* [] | *RPCRequest* , callback:, config:*Partial<IN3Config>*)	sends one or a multiple requests. if the request is a array the response will be a array as well. If the callback is given it will be called with the response, if not a Promise will be returned. This function supports callback so it can be used as a Provider for the web3.
Promise<RPCResponse>	sendRPC (method:`string`, params:`any` [], chain:`string`, config:*Partial<IN3Config>*)	sends a simply RPC-Request
`this`	setMaxListeners (n:`number`)	set max listeners
`Promise<void>`	updateNodeList (chainId:`string`, conf:*Partial<IN3Config>* , retryCount:`number`)	fetches the nodeList from the servers.
`Promise<void>`	updateWhiteListNodes (config:*IN3Config*)	update white list nodes

Continued on next page

Table 2 – continued from previous page

`Promise<boolean>`	verifyResponse (request:*RPCRequest* , response:*RPCResponse* , chain:`string`, config:*Partial<IN3Config>*)	Verify the response of a request without any effect on the state of the client. Note: The node-list will not be updated. The method will either return *true* if its inputs could be verified. Or else, it will throw an exception with a helpful message.

9.3.2 Type ChainContext

Source: client/ChainContext.ts

Context for a specific chain including cache and chainSpecs.

ChainContext	constructor (client:*Client* , chainId:string, chainSpec:*ChainSpec* [])	Context for a specific chain including cache and chainSpecs.
string	chainId	the chainId
ChainSpec []	chainSpec	the chainSpec
Client	client	the client
	genericCache	the genericCache
number	lastValidatorChange	the lastValidatorChange
Module	module	the module
string	registryId	the registryId *(optional)*
void	clearCache (prefix:string)	clear cache
ChainSpec	getChainSpec (block:number)	returns the chainspec for th given block number
string	getFromCache (key:string)	get from cache
Promise<RPCResponse>	handleIntern (request:*RPCRequest*)	this function is calleds before the server is asked. If it returns a promise than the request is handled internally otherwise the server will handle the response. this function should be overriden by modules that want to handle calls internally

9.3.3 Type Module

Source: client/modules.ts

`string`	name	the name
ChainContext	createChainContext (client:*Client* , chainId:`string`, spec:*ChainSpec* [])	Context for a specific chain including cache and chainSpecs.
`Promise<boolean>`	verifyProof (request:*RPCRequest* , response:*RPCResponse* , allowWithoutProof:`boolean`, ctx:*ChainContext*)	general verification-function which handles it according to its given type.

9.4 Package index.ts

9.4.1 Type AccountProof

Source: index.ts

the Proof-for a single Account the Proof-for a single Account

`string` []	accountProof	the serialized merle-noodes beginning with the root-node
`string`	address	the address of this account
`string`	balance	the balance of this account as hex
`string`	code	the code of this account as hex (if required) *(optional)*
`string`	codeHash	the codeHash of this account as hex
`string`	nonce	the nonce of this account as hex
`string`	storageHash	the storageHash of this account as hex
[]	storageProof	proof for requested storage-data

9.4.2 Type AuraValidatoryProof

Source: index.ts

a Object holding proofs for validator logs. The key is the blockNumber as hex a Object holding proofs for validator logs. The key is the blockNumber as hex

`string`	block	the serialized blockheader example: 0x72804cfa0179d648ccbe6a65b01a6463a8f1ebb14f3aff6
`any` []	finalityBlocks	the serialized blockheader as hex, required in case of finality asked example: 0x72804cfa0179d648ccbe6a65b01a6463a8f1ebb14f3aff6 *(optional)*
`number`	logIndex	the transaction log index
`string` []	proof	the merkleProof
`number`	txIndex	the transactionIndex within the block

9.4.3 Type ChainSpec

Source: index.ts

describes the chainspecific consensus params describes the chainspecific consensus params

`number`	block	the blocknumnber when this configuration should apply *(optional)*
`number`	bypassFinality	Bypass finality check for transition to contract based Aura Engines example: bypassFinality = 10960502 -> will skip the finality check and add the list at block 10960502 *(optional)*
`string`	contract	The validator contract at the block *(optional)*
`'ethHash' |'authorityRound' |'clique'`	engine	the engine type (like Ethhash, authorityRound, ...) *(optional)*
`string` []	list	The list of validators at the particular block *(optional)*
`boolean`	requiresFinality	indicates whether the transition requires a finality check example: true *(optional)*

9.4.4 Type IN3Client

Source: index.ts

Client for N3. Client for N3.

`number`	defaultMaxListeners	the defaultMaxListeners

Continued on next page

Table 3 – continued from previous page

number	listenerCount (emitter:*EventEmitter* , event:string | symbol)	listener count
Client	constructor (config:*Partial<IN3Config>* , transport:*Transport*)	creates a new Client.
IN3Config	defConfig	the defConfig
EthAPI	eth	the eth
IpfsAPI	ipfs	the ipfs
IN3Config	config	config
this	addListener (event:string | symbol, listener:)	add listener
Promise<any>	call (method:string, params:any, chain:string, config:*Partial<IN3Config>*)	sends a simply RPC-Request
void	clearStats ()	clears all stats and weights, like blocklisted nodes
any	createWeb3Provider ()	create web3 provider

Continued on next page

Table 3 – continued from previous page

`boolean`	emit (event:`string` | `symbol`, args:`any` [])	emit
Array<>	eventNames ()	event names
ChainContext	getChainContext (chainId:`string`)	Context for a specific chain including cache and chainSpecs.
`number`	getMaxListeners ()	get max listeners
`number`	listenerCount (type:`string` | `symbol`)	listener count
Function []	listeners (event:`string` | `symbol`)	listeners
`this`	off (event:`string` | `symbol`, listener:)	off
`this`	on (event:`string` | `symbol`, listener:)	on
`this`	once (event:`string` | `symbol`, listener:)	once

Continued on next page

Table 3 – continued from previous page

this	prependListener (event:string | symbol, listener:)	prepend listener
this	prependOnceListener (event:string | symbol, listener:)	prepend once listener
Function []	rawListeners (event:string | symbol)	raw listeners
this	removeAllListeners (event:string | symbol)	remove all listeners
this	removeListener (event:string | symbol, listener:)	remove listener
Promise<>	send (request:*RPCRequest* [] | *RPCRequest* , callback:, config:*Partial<IN3Config>*)	sends one or a multiple requests. if the request is a array the response will be a array as well. If the callback is given it will be called with the response, if not a Promise will be returned. This function supports callback so it can be used as a Provider for the web3.
Promise<RPCResponse>	sendRPC (method:string, params:any [], chain:string, config:*Partial<IN3Config>*)	sends a simply RPC-Request

Continued on next page

Table 3 – continued from previous page

`this`	setMaxListeners (n:`number`)	set max listeners
`Promise<void>`	updateNodeList (chainId:`string`, conf:*Partial<IN3Config>* , retryCount:`number`)	fetches the nodeList from the servers.
`Promise<void>`	updateWhiteListNodes (config:*IN3Config*)	update white list nodes
`Promise<boolean>`	verifyResponse (request:*RPCRequest* , response:*RPCResponse* , chain:`string`, config:*Partial<IN3Config>*)	Verify the response of a request without any effect on the state of the client. Note: The node-list will not be updated. The method will either return *true* if its inputs could be verified. Or else, it will throw an exception with a helpful message.

9.4.5 Type IN3Config

Source: index.ts

the iguration of the IN3-Client. This can be paritally overriden for every request. the iguration of the IN3-Client. This can be paritally overriden for every request.

`boolean`	archiveNodes	if true the in3 client will filter out non archive supporting nodes example: true *(optional)*
`boolean`	autoConfig	if true the config will be adjusted depending on the request *(optional)*

Continued on next page

Table 4 – continued from previous page

`boolean`	autoUpdateList	if true the nodelist will be automaticly updated if the lastBlock is newer example: true *(optional)*
`boolean`	binaryNodes	if true the in3 client will only include nodes that support binary encording example: true *(optional)*
`any`	cacheStorage	a cache handler offering 2 functions (setItem(string,string), getItem(string)) *(optional)*
`number`	cacheTimeout	number of seconds requests can be cached. *(optional)*
`string`	chainId	servers to filter for the given chain. The chain-id based on EIP-155. example: 0x1
`string`	chainRegistry	main chain-registry contract example: 0xe36179e2286ef405e929C90ad3E70E649B22a945 *(optional)*
`number`	depositTimeout	timeout after which the owner is allowed to receive its stored deposit. This information is also important for the client example: 3000 *(optional)*
`number`	finality	the number in percent needed in order reach finality (% of signature of the validators) example: 50 *(optional)*

Continued on next page

Table 4 – continued from previous page

`'json'|'jsonRef'|'cbor'`	format	the format for sending the data to the client. Default is json, but using cbor means using only 30-40% of the payload since it is using binary encoding example: json *(optional)*
`boolean`	httpNodes	if true the in3 client will include http nodes example: true *(optional)*
`boolean`	includeCode	if true, the request should include the codes of all accounts. otherwise only the the codeHash is returned. In this case the client may ask by calling eth_getCode() afterwards example: true *(optional)*
`boolean`	keepIn3	if true, the in3-section of thr response will be kept. Otherwise it will be removed after validating the data. This is useful for debugging or if the proof should be used afterwards. *(optional)*
`any`	key	the client key to sign requests example: 0x387a8233c96e1fc0ad5e284353276177af2186e7afa8529 *(optional)*
`string`	loggerUrl	a url of RES-Endpoint, the client will log all errors to. The client will post to this endpoint JSON like { id?, level, message, meta? } *(optional)*
`string`	mainChain	main chain-id, where the chain registry is running. example: 0x1 *(optional)*

Continued on next page

Table 4 – continued from previous page

number	maxAttempts	max number of attempts in case a response is rejected example: 10 *(optional)*
number	maxBlockCache	number of number of blocks cached in memory example: 100 *(optional)*
number	maxCodeCache	number of max bytes used to cache the code in memory example: 100000 *(optional)*
number	minDeposit	min stake of the server. Only nodes owning at least this amount will be chosen.
boolean	multichainNodes	if true the in3 client will filter out nodes other then which have capability of the same RPC endpoint may also accept requests for different chains example: true *(optional)*
number	nodeLimit	the limit of nodes to store in the client. example: 150 *(optional)*
'none'|'standard'|'full'	proof	if true the nodes should send a proof of the response example: true *(optional)*
boolean	proofNodes	if true the in3 client will filter out nodes which are providing no proof example: true *(optional)*
number	replaceLatestBlock	if specified, the blocknumber *latest* will be replaced by blockNumber- specified value example: 6 *(optional)*

Continued on next page

Table 4 – continued from previous page

`number`	requestCount	the number of request send when getting a first answer example: 3
`boolean`	retryWithoutProof	if true the the request may be handled without proof in case of an error. (use with care!) *(optional)*
`string`	rpc	url of one or more rpc-endpoints to use. (list can be comma seperated) *(optional)*
	servers	the nodelist per chain *(optional)*
`number`	signatureCount	number of signatures requested example: 2 *(optional)*
`number`	timeout	specifies the number of milliseconds before the request times out. increasing may be helpful if the device uses a slow connection. example: 3000 *(optional)*
`boolean`	torNodes	if true the in3 client will filter out non tor nodes example: true *(optional)*
`string` []	verifiedHashes	if the client sends a array of blockhashes the server will not deliver any signatures or blockheaders for these blocks, but only return a string with a number. This is automaticly updated by the cache, but can be overriden per request. *(optional)*

Continued on next page

Table 4 – continued from previous page

`string` []	whiteList	a list of in3 server addresses which are whitelisted manually by client example: 0xe36179e2286ef405e929C90ad3E70E649B22a945,0x6d *(optional)*
`string`	whiteListContract	White list contract address *(optional)*

9.4.6 Type IN3NodeConfig

Source: index.ts

a configuration of a in3-server. a configuration of a in3-server.

string	address	the address of the node, which is the public address it iis signing with. example: 0x6C1a01C2aB554930A937B0a2E8105fB47946c679
number	capacity	the capacity of the node. example: 100 *(optional)*
string []	chainIds	the list of supported chains example: 0x1
number	deposit	the deposit of the node in wei example: 12350000
number	index	the index within the contract example: 13 *(optional)*
number	props	the properties of the node. example: 3 *(optional)*
number	registerTime	the UNIX-timestamp when the node was registered example: 1563279168 *(optional)*
number	timeout	the time (in seconds) until an owner is able to receive his deposit back after he unregisters himself example: 3600 *(optional)*
number	unregisterTime	the UNIX-timestamp when the node is allowed to be deregister example: 1563279168 *(optional)*
string	url	the endpoint to post to example: https://in3.slock.it

9.4.7 Type IN3NodeWeight

Source: index.ts

a local weight of a n3-node. (This is used internally to weight the requests) a local weight of a n3-node. (This is used internally to weight the requests)

`number`	avgResponseTime	average time of a response in ms example: 240 *(optional)*
`number`	blacklistedUntil	blacklisted because of failed requests until the timestamp example: 1529074639623 *(optional)*
`number`	lastRequest	timestamp of the last request in ms example: 1529074632623 *(optional)*
`number`	pricePerRequest	last price *(optional)*
`number`	responseCount	number of uses. example: 147 *(optional)*
`number`	weight	factor the weight this noe (default 1.0) example: 0.5 *(optional)*

9.4.8 Type IN3RPCConfig

Source: index.ts

the configuration for the rpc-handler the configuration for the rpc-handler

	chains	a definition of the Handler per chain *(optional)*
	db	the db *(optional)*
string	defaultChain	the default chainId in case the request does not contain one. *(optional)*
string	id	a identifier used in logfiles as also for reading the config from the database *(optional)*
	logging	logger config *(optional)*
number	port	the listeneing port for the server *(optional)*
	profile	the profile *(optional)*

9.4.9 Type IN3RPCHandlerConfig

Source: index.ts

the configuration for the rpc-handler the configuration for the rpc-handler

	autoRegistry	the autoRegistry *(optional)*
`string`	clientKeys	a comma sepearted list of client keys to use for simulating clients for the watchdog *(optional)*
`number`	freeScore	the score for requests without a valid signature *(optional)*
`'eth'|'ipfs'|'btc'`	handler	the impl used to handle the calls *(optional)*
`string`	ipfsUrl	the url of the ipfs-client *(optional)*
`number`	maxThreads	the maximal number of threads ofr running parallel processes *(optional)*
`number`	minBlockHeight	the minimal blockheight in order to sign *(optional)*
`string`	persistentFile	the filename of the file keeping track of the last handled blocknumber *(optional)*
`string`	privateKey	the private key used to sign blockhashes. this can be either a 0x-prefixed string with the raw private key or the path to a key-file.
`string`	privateKeyPassphrase	the password used to decrpyt the private key *(optional)*
`string`	registry	the address of the server registry used in order to update the nodeList

9.4.10 Type IN3RPCRequestConfig

Source: index.ts

additional config for a IN3 RPC-Request additional config for a IN3 RPC-Request

`string`	chainId	the requested chainId example: 0x1
`any`	clientSignature	the signature of the client *(optional)*
`number`	finality	if given the server will deliver the blockheaders of the following blocks until at least the number in percent of the validators is reached. *(optional)*
`boolean`	includeCode	if true, the request should include the codes of all accounts. otherwise only the the codeHash is returned. In this case the client may ask by calling eth_getCode() afterwards example: true *(optional)*
`number`	latestBlock	if specified, the blocknumber *latest* will be replaced by blockNumber- specified value example: 6 *(optional)*
`string` []	signatures	a list of addresses requested to sign the blockhash example: 0x6C1a01C2aB554930A937B0a2E8105fB47946c679 *(optional)*
`boolean`	useBinary	if true binary-data will be used. *(optional)*
`boolean`	useFullProof	if true all data in the response will be proven, which leads to a higher payload. *(optional)*
`boolean`	useRef	if true binary-data (starting with a 0x) will be refered if occuring again. *(optional)*

9.4.11 Type IN3ResponseConfig

Source: index.ts

additional data returned from a IN3 Server additional data returned from a IN3 Server

`number`	currentBlock	the current blocknumber. example: 320126478 *(optional)*
`number`	lastNodeList	the blocknumber for the last block updating the nodelist. If the client has a smaller blocknumber he should update the nodeList. example: 326478 *(optional)*
`number`	lastValidatorChange	the blocknumber of the last change of the validatorList *(optional)*
`number`	lastWhiteList	The blocknumber of the last white list event *(optional)*
Proof	proof	the Proof-data *(optional)*
`string`	version	IN3 protocol version example: 1.0.0 *(optional)*

9.4.12 Type LogProof

Source: index.ts

a Object holding proofs for event logs. The key is the blockNumber as hex a Object holding proofs for event logs. The key is the blockNumber as hex

9.4.13 Type Proof

Source: index.ts

the Proof-data as part of the in3-section the Proof-data as part of the in3-section

	accounts	a map of addresses and their AccountProof *(optional)*
`string`	block	the serialized blockheader as hex, required in most proofs example: 0x72804cfa0179d648ccbe6a65b01a6463a8f1ebb14f3aff6 *(optional)*
`any` []	finalityBlocks	the serialized blockheader as hex, required in case of finality asked example: 0x72804cfa0179d648ccbe6a65b01a6463a8f1ebb14f3aff6 *(optional)*
LogProof	logProof	the Log Proof in case of a Log-Request *(optional)*
`string` []	merkleProof	the serialized merle-noodes beginning with the root-node *(optional)*
`string` []	merkleProofPrev	the serialized merkle-noodes beginning with the root-node of the previous entry (only for full proof of receipts) *(optional)*
Signature []	signatures	requested signatures *(optional)*
`any` []	transactions	the list of transactions of the block example: *(optional)*
`number`	txIndex	the transactionIndex within the block example: 4 *(optional)*
`string` []	txProof	the serialized merkle-nodes beginning with the root-node in order to prrof the transactionIndex *(optional)*

9.4.14 Type RPCRequest

Source: index.ts

a JSONRPC-Request with N3-Extension a JSONRPC-Request with N3-Extension

`number` | `string`	id	the identifier of the request example: 2 *(optional)*
IN3RPCRequestConfig	in3	the IN3-Config *(optional)*
`'2.0'`	jsonrpc	the version
`string`	method	the method to call example: eth_getBalance
`any` []	params	the params example: 0xe36179e2286ef405e929C90ad3E70E649B22a945,lates *(optional)*

9.4.15 Type RPCResponse

Source: index.ts

a JSONRPC-Responset with N3-Extension a JSONRPC-Responset with N3-Extension

`string`	error	in case of an error this needs to be set *(optional)*
`string|number`	id	the id matching the request example: 2
IN3ResponseConfig	in3	the IN3-Result *(optional)*
IN3NodeConfig	in3Node	the node handling this response (internal only) *(optional)*
`'2.0'`	jsonrpc	the version
`any`	result	the params example: 0xa35bc *(optional)*

9.4.16 Type ServerList

Source: index.ts

a List of nodes a List of nodes

`string`	contract	IN3 Registry *(optional)*
`number`	lastBlockNumber	last Block number *(optional)*
IN3NodeConfig []	nodes	the list of nodes
Proof	proof	the proof *(optional)*
`string`	registryId	registry id of the contract *(optional)*
`number`	totalServers	number of servers *(optional)*

9.4.17 Type Signature

Source: index.ts

Verified ECDSA Signature. Signatures are a pair (r, s). Where r is computed as the X coordinate of a point R, modulo the curve order n. Verified ECDSA Signature. Signatures are a pair (r, s). Where r is computed as the X coordinate of a point R, modulo the curve order n.

`string`	address	the address of the signing node example: 0x6C1a01C2aB554930A937B0a2E8105fB47946c679 *(optional)*
`number`	block	the blocknumber example: 3123874
`string`	blockHash	the hash of the block example: 0x6C1a01C2aB554930A937B0a212346037E8105fB4794
`string`	msgHash	hash of the message example: 0x9C1a01C2aB554930A937B0a212346037E8105fB4794
`string`	r	Positive non-zero Integer signature.r example: 0x72804cfa0179d648ccbe6a65b01a6463a8f1ebb14f3aff6
`string`	s	Positive non-zero Integer signature.s example: 0x6d17b34aeaf95fee98c0437b4ac839d8a2ece1b18166da
`number`	v	Calculated curve point, or identity element O. example: 28

9.4.18 Type Transport

Source: index.ts

= *_transporttype*

9.5 Package modules/eth

9.5.1 Type EthAPI

Source: modules/eth/api.ts

EthAPI	constructor (client:*Client*)	constructor
Client	client	the client
Signer	signer	the signer *(optional)*
`Promise<number>`	blockNumber ()	Returns the number of most recent block. (as number)
`Promise<string>`	call (tx:*Transaction* , block:*BlockType*)	Executes a new message call immediately without creating a transaction on the block chain.
`Promise<any>`	callFn (to:*Address* , method:`string`, args:`any` [])	Executes a function of a contract, by passing a [method-signature](https://github.com/ethereumjs/ethereumjs-abi/blob/master/README.md#simple-encoding-and-decoding) and the arguments, which will then be ABI-encoded and send as eth_call.
`Promise<string>`	chainId ()	Returns the EIP155 chain ID used for transaction signing at the current best block. Null is returned if not available.
	contractAt (abi:*ABI* [], address:*Address*)	contract at

Continued on next page

Table 5 – continued from previous page

any	decodeEventData (log:*Log* , d:*ABI*)	decode event data
Promise<number>	estimateGas (tx:*Transaction*)	Makes a call or transaction, which won't be added to the blockchain and returns the used gas, which can be used for estimating the used gas.
Promise<number>	gasPrice ()	Returns the current price per gas in wei. (as number)
Promise<BN>	getBalance (address:*Address* , block:*BlockType*)	Returns the balance of the account of given address in wei (as hex).
Promise<Block>	getBlockByHash (hash:*Hash* , includeTransactions:boolean)	Returns information about a block by hash.
Promise<Block>	getBlockByNumber (block:*BlockType* , includeTransactions:boolean)	Returns information about a block by block number.
Promise<number>	getBlockTransactionCountByHash (block:*Hash*)	Returns the number of transactions in a block from a block matching the given block hash.
Promise<number>	getBlockTransactionCountByNumber (block:*Hash*)	Returns the number of transactions in a block from a block matching the given block number.
Promise<string>	getCode (address:*Address* , block:*BlockType*)	Returns code at a given address.

Continued on next page

Table 5 – continued from previous page

`Promise<>`	getFilterChanges (id:*Quantity*)	Polling method for a filter, which returns an array of logs which occurred since last poll.
`Promise<>`	getFilterLogs (id:*Quantity*)	Returns an array of all logs matching filter with given id.
`Promise<>`	getLogs (filter:*LogFilter*)	Returns an array of all logs matching a given filter object.
`Promise<string>`	getStorageAt (address:*Address* , pos:*Quantity* , block:*BlockType*)	Returns the value from a storage position at a given address.
Promise<TransactionDetail>	getTransactionByBlockHashAndIndex (hash:*Hash* , pos:*Quantity*)	Returns information about a transaction by block hash and transaction index position.
Promise<TransactionDetail>	getTransactionByBlockNumberAndIndex (block:*BlockType* , pos:*Quantity*)	Returns information about a transaction by block number and transaction index position.
Promise<TransactionDetail>	getTransactionByHash (hash:*Hash*)	Returns the information about a transaction requested by transaction hash.
`Promise<number>`	getTransactionCount (address:*Address* , block:*BlockType*)	Returns the number of transactions sent from an address. (as number)
Promise<TransactionReceipt>	getTransactionReceipt (hash:*Hash*)	Returns the receipt of a transaction by transaction hash. Note That the receipt is available even for pending transactions.

Continued on next page

Table 5 – continued from previous page

Promise<Block>	getUncleByBlockHashAndIndex (hash:*Hash* , pos:*Quantity*)	Returns information about a uncle of a block by hash and uncle index position. Note: An uncle doesn't contain individual transactions.
Promise<Block>	getUncleByBlockNumberAndIndex (block:*BlockType* , pos:*Quantity*)	Returns information about a uncle of a block number and uncle index position. Note: An uncle doesn't contain individual transactions.
`Promise<number>`	getUncleCountByBlockHash (hash:*Hash*)	Returns the number of uncles in a block from a block matching the given block hash.
`Promise<number>`	getUncleCountByBlockNumber (block:*BlockType*)	Returns the number of uncles in a block from a block matching the given block hash.
Buffer	hashMessage (data:*Data* | *Buffer*)	hash message
`Promise<string>`	newBlockFilter ()	Creates a filter in the node, to notify when a new block arrives. To check if the state has changed, call eth_getFilterChanges.
`Promise<string>`	newFilter (filter:*LogFilter*)	Creates a filter object, based on filter options, to notify when the state changes (logs). To check if the state has changed, call eth_getFilterChanges.
`Promise<string>`	newPendingTransactionFilter ()	Creates a filter in the node, to notify when new pending transactions arrive.

Continued on next page

Table 5 – continued from previous page

`Promise<string>`	protocolVersion ()	Returns the current ethereum protocol version.
`Promise<string>`	sendRawTransaction (data:*Data*)	Creates new message call transaction or a contract creation for signed transactions.
`Promise<>`	sendTransaction (args:*TxRequest*)	sends a Transaction
Promise<Signature>	sign (account:*Address* , data:*Data*)	signs any kind of message using the *x19Ethereum Signed Message:n*-prefix
`Promise<>`	syncing ()	Returns the current ethereum protocol version.
Promise<Quantity>	uninstallFilter (id:*Quantity*)	Uninstalls a filter with given id. Should always be called when watch is no longer needed. Additonally Filters timeout when they aren't requested with eth_getFilterChanges for a period of time.

9.5.2 Type chainData

Source: modules/eth/chainData.ts

`Promise<any>`	callContract (client:*Client* , contract:`string`, chainId:`string`, signature:`string`, args:`any` [], config:*IN3Config*)	call contract
`Promise<>`	getChainData (client:*Client* , chainId:`string`, config:*IN3Config*)	get chain data

9.5.3 Type header

Source: modules/eth/header.ts

Interface	*AuthSpec*	Authority specification for proof of authority chains
Interface	*HistoryEntry*	the HistoryEntry
`Promise<void>`	addAuraValidators (history:*DeltaHistory<string>* , ctx:*ChainContext* , states:*HistoryEntry* [], contract:`string`)	add aura validators
`void`	addCliqueValidators (history:*DeltaHistory<string>* , ctx:*ChainContext* , states:*HistoryEntry* [])	add clique validators
`Promise<number>`	checkBlockSignatures (blockHeaders:`any` [], getChainSpec:)	verify a Blockheader and returns the percentage of finality
`void`	checkForFinality (stateBlockNumber:`number`, proof:*AuraValidatoryProof* , current:*Buffer* [], _finality:`number`)	check for finality
`Promise<void>`	checkForValidators (ctx:*ChainContext* , validators:*DeltaHistory<string>*)	check for validators
Promise<AuthSpec>	getChainSpec (b:*Block* , ctx:*ChainContext*)	get chain spec

9.5.4 Type Signer

Source: modules/eth/api.ts

Promise<Transaction>	prepareTransaction (client:*Client* , tx:*Transaction*)	optiional method which allows to change the transaction-data before sending it. This can be used for redirecting it through a multisig.
Promise<Signature>	sign (data:*Buffer* , account:*Address*)	signing of any data.
`Promise<boolean>`	hasAccount (account:*Address*)	returns true if the account is supported (or unlocked)

9.5.5 Type Transaction

Source: modules/eth/api.ts

`any`	chainId	optional chain id *(optional)*
`string`	data	4 byte hash of the method signature followed by encoded parameters. For details see Ethereum Contract ABI.
Address	from	20 Bytes - The address the transaction is send from.
Quantity	gas	Integer of the gas provided for the transaction execution. eth_call consumes zero gas, but this parameter may be needed by some executions.
Quantity	gasPrice	Integer of the gas price used for each paid gas.
Quantity	nonce	nonce
Address	to	(optional when creating new contract) 20 Bytes - The address the transaction is directed to.
Quantity	value	Integer of the value sent with this transaction.

9.5.6 Type BlockType

Source: modules/eth/api.ts

= `number | 'latest' | 'earliest' | 'pending'`

9.5.7 Type Address

Source: modules/eth/api.ts

= `string`

9.5.8 Type ABI

Source: modules/eth/api.ts

`boolean`	anonymous	the anonymous *(optional)*
`boolean`	constant	the constant *(optional)*
ABIField []	inputs	the inputs *(optional)*
`string`	name	the name *(optional)*
ABIField []	outputs	the outputs *(optional)*
`boolean`	payable	the payable *(optional)*
`'nonpayable'` | `'payable'` | `'view'` | `'pure'`	stateMutability	the stateMutability *(optional)*
`'event'` | `'function'` | `'constructor'` | `'fallback'`	type	the type

9.5.9 Type Log

Source: modules/eth/api.ts

Address	address	20 Bytes - address from which this log originated.
Hash	blockHash	Hash, 32 Bytes - hash of the block where this log was in. null when its pending. null when its pending log.
Quantity	blockNumber	the block number where this log was in. null when its pending. null when its pending log.
Data	data	contains the non-indexed arguments of the log.
Quantity	logIndex	integer of the log index position in the block. null when its pending log.
`boolean`	removed	true when the log was removed, due to a chain reorganization. false if its a valid log.
Data []	topics	- Array of 0 to 4 32 Bytes DATA of indexed log arguments. (In solidity: The first topic is the hash of the signature of the event (e.g. Deposit(address,bytes32,uint256)), except you declared the event with the anonymous specifier.)
Hash	transactionHash	Hash, 32 Bytes - hash of the transactions this log was created from. null when its pending log.
Quantity	transactionIndex	integer of the transactions index position log was created from. null when its pending log.

9.5.10 Type Block

Source: modules/eth/api.ts

Address	author	20 Bytes - the address of the author of the block (the beneficiary to whom the mining rewards were given)
Quantity	difficulty	integer of the difficulty for this block
Data	extraData	the 'extra data' field of this block
Quantity	gasLimit	the maximum gas allowed in this block
Quantity	gasUsed	the total used gas by all transactions in this block
Hash	hash	hash of the block. null when its pending block
Data	logsBloom	256 Bytes - the bloom filter for the logs of the block. null when its pending block
Address	miner	20 Bytes - alias of 'author'
Data	nonce	8 bytes hash of the generated proof-of-work. null when its pending block. Missing in case of PoA.
Quantity	number	The block number. null when its pending block
Hash	parentHash	hash of the parent block
Data	receiptsRoot	32 Bytes - the root of the receipts trie of the block

9.5.11 Type Hash

Source: modules/eth/api.ts

= `string`

9.5.12 Type Quantity

Source: modules/eth/api.ts

= `number` | *Hex*

9.5.13 Type LogFilter

Source: modules/eth/api.ts

Address	address	(optional) 20 Bytes - Contract address or a list of addresses from which logs should originate.
BlockType	fromBlock	Quantity or Tag - (optional) (default: latest) Integer block number, or 'latest' for the last mined block or 'pending', 'earliest' for not yet mined transactions.
Quantity	limit	å(optional) The maximum number of entries to retrieve (latest first).
BlockType	toBlock	Quantity or Tag - (optional) (default: latest) Integer block number, or 'latest' for the last mined block or 'pending', 'earliest' for not yet mined transactions.
`string` | `string` [] []	topics	(optional) Array of 32 Bytes Data topics. Topics are order-dependent. It's possible to pass in null to match any topic, or a subarray of multiple topics of which one should be matching.

9.5.14 Type TransactionDetail

Source: modules/eth/api.ts

Hash	blockHash	32 Bytes - hash of the block where this transaction was in. null when its pending.
BlockType	blockNumber	block number where this transaction was in. null when its pending.
Quantity	chainId	the chain id of the transaction, if any.
`any`	condition	(optional) conditional submission, Block number in block or timestamp in time or null. (parity-feature)
Address	creates	creates contract address
Address	from	20 Bytes - address of the sender.
Quantity	gas	gas provided by the sender.
Quantity	gasPrice	gas price provided by the sender in Wei.
Hash	hash	32 Bytes - hash of the transaction.
Data	input	the data send along with the transaction.
Quantity	nonce	the number of transactions made by the sender prior to this one.
`any`	pk	optional private key for signing *(optional)*

9.5.15 Type TransactionReceipt

Source: modules/eth/api.ts

Hash	blockHash	32 Bytes - hash of the block where this transaction was in.
BlockType	blockNumber	block number where this transaction was in.
Address	contractAddress	20 Bytes - The contract address created, if the transaction was a contract creation, otherwise null.
Quantity	cumulativeGasUsed	The total amount of gas used when this transaction was executed in the block.
Address	from	20 Bytes - The address of the sender.
Quantity	gasUsed	The amount of gas used by this specific transaction alone.
Log []	logs	Array of log objects, which this transaction generated.
Data	logsBloom	256 Bytes - A bloom filter of logs/events generated by contracts during transaction execution. Used to efficiently rule out transactions without expected logs.
Hash	root	32 Bytes - Merkle root of the state trie after the transaction has been executed (optional after Byzantium hard fork EIP609)
Quantity	status	0x0 indicates transaction failure , 0x1 indicates transaction success. Set for blocks mined after Byzantium hard fork EIP609, null before.

9.5.16 Type Data

Source: modules/eth/api.ts

= `string`

9.5.17 Type TxRequest

Source: modules/eth/api.ts

`any` []	args	the argument to pass to the method *(optional)*
`number`	confirmations	number of block to wait before confirming *(optional)*
Data	data	the data to send *(optional)*
Address	from	address of the account to use *(optional)*
`number`	gas	the gas needed *(optional)*
`number`	gasPrice	the gasPrice used *(optional)*
`string`	method	the ABI of the method to be used *(optional)*
`number`	nonce	the nonce *(optional)*
Hash	pk	raw private key in order to sign *(optional)*
Address	to	contract *(optional)*
Quantity	value	the value in wei *(optional)*

9.5.18 Type AuthSpec

Source: modules/eth/header.ts

Authority specification for proof of authority chains

Buffer []	authorities	List of validator addresses storead as an buffer array
Buffer	proposer	proposer of the block this authspec belongs
ChainSpec	spec	chain specification

9.5.19 Type HistoryEntry

Source: modules/eth/header.ts

`number`	block	the block
AuraValidatoryProof | `string` []	proof	the proof
`string` []	validators	the validators

9.5.20 Type ABIField

Source: modules/eth/api.ts

`boolean`	indexed	the indexed *(optional)*
`string`	name	the name
`string`	type	the type

9.5.21 Type Hex

Source: modules/eth/api.ts

= `string`

9.6 Package modules/ipfs

9.6.1 Type IpfsAPI

Source: modules/ipfs/api.ts

simple API for IPFS

IpfsAPI	constructor (_client:*Client*)	simple API for IPFS
Client	client	the client
Promise<Buffer>	get (hash:`string`, resultEncoding:`string`)	retrieves the conent for a hash from IPFS.
`Promise<string>`	put (data:*Buffer* , dataEncoding:`string`)	stores the data on ipfs and returns the IPFS-Hash.

9.7 Package util

a collection of util classes inside incubed. They can be get directly through `require('in3/js/srrc/util/util')`

9.7.1 Type DeltaHistory

Source: util/DeltaHistory.ts

DeltaHistory	constructor (init:*T* [], deltaStrings:`boolean`)	constructor
Delta<T> []	data	the data
`void`	addState (start:`number`, data:*T* [])	add state
T []	getData (index:`number`)	get data
`number`	getLastIndex ()	get last index
`void`	loadDeltaStrings (deltas:`string` [])	load delta strings
`string` []	toDeltaStrings ()	to delta strings

9.7.2 Type Delta

Source: util/DeltaHistory.ts

This file is part of the Incubed project. Sources: https://github.com/slockit/in3

`number`	block	the block
T []	data	the data
`number`	len	the len
`number`	start	the start

9.8 Common Module

The common module (in3-common) contains all the typedefs used in the node and server.

Interface	*BlockData*	the BlockData
Interface	*LogData*	the LogData
Type	*Receipt*	the Receipt
Interface	*ReceiptData*	the ReceiptData
Type	*Transaction*	the Transaction
Interface	*TransactionData*	the TransactionData
Interface	*Transport*	the Transport
AxiosTransport	AxiosTransport	the AxiosTransport value= `_transport.AxiosTransport`

Continued on next page

Table 6 – continued from previous page

Block	Block	the Block value= `_serialize.Block`
`any`	address (val:`any`)	converts it to a Buffer with 20 bytes length
Block	blockFromHex (hex:`string`)	converts a hexstring to a block-object
`any`	bytes (val:`any`)	converts it to a Buffer
`any`	bytes32 (val:`any`)	converts it to a Buffer with 32 bytes length
`any`	bytes8 (val:`any`)	converts it to a Buffer with 8 bytes length
cbor	cbor	the cbor value= `_cbor`
	chainAliases	the chainAliases value= `_util.aliases`
`number` []	createRandomIndexes (len:`number`, limit:`number`, seed:*Buffer* , result:`number` [])	create random indexes
`any`	createTx (transaction:`any`)	creates a Transaction-object from the rpc-transaction-data
Buffer	getSigner (data:*Block*)	get signer

Continued on next page

Table 6 – continued from previous page

Buffer	hash (val:*Block* | *Transaction* | *Receipt* | *Account* | *Buffer*)	returns the hash of the object
index	rlp	the rlp value= `_serialize.rlp`
serialize	serialize	the serialize value= `_serialize`
storage	storage	the storage value= `_storage`
Buffer []	toAccount (account:*AccountData*)	to account
Buffer []	toBlockHeader (block:*BlockData*)	create a Buffer[] from RPC-Response
`Object`	toReceipt (r:*ReceiptData*)	create a Buffer[] from RPC-Response
Buffer []	toTransaction (tx:*TransactionData*)	create a Buffer[] from RPC-Response
transport	transport	the transport value= `_transport`
`any`	uint (val:`any`)	converts it to a Buffer with a variable length. 0 = length 0
`any`	uint128 (val:`any`)	uint128

Continued on next page

Table 6 – continued from previous page

any	uint64 (val:any)	uint64
util	util	the util value= _util
validate	validate	the validate value= _validate

9.9 Package index.ts

9.9.1 Type BlockData

Source: index.ts

Block as returned by eth_getBlockByNumber Block as returned by eth_getBlockByNumber

`string`	coinbase	the coinbase *(optional)*
`string|number`	difficulty	the difficulty
`string`	extraData	the extraData
`string|number`	gasLimit	the gasLimit
`string|number`	gasUsed	the gasUsed
`string`	hash	the hash
`string`	logsBloom	the logsBloom
`string`	miner	the miner
`string`	mixHash	the mixHash *(optional)*
`string|number`	nonce	the nonce *(optional)*
`string|number`	number	the number
`string`	parentHash	the parentHash
`string`	receiptRoot	the receiptRoot *(optional)*
`string`	receiptsRoot	the receiptsRoot
`string []`	sealFields	the sealFields *(optional)*
`string`	sha3Uncles	the sha3Uncles

9.9.2 Type LogData

Source: index.ts

LogData as part of the TransactionReceipt LogData as part of the TransactionReceipt

`string`	address	the address
`string`	blockHash	the blockHash
`string`	blockNumber	the blockNumber
`string`	data	the data
`string`	logIndex	the logIndex
`boolean`	removed	the removed
`string` []	topics	the topics
`string`	transactionHash	the transactionHash
`string`	transactionIndex	the transactionIndex
`string`	transactionLogIndex	the transactionLogIndex

9.9.3 Type ReceiptData

Source: index.ts

TransactionReceipt as returned by eth_getTransactionReceipt TransactionReceipt as returned by eth_getTransactionReceipt

string	blockHash	the blockHash *(optional)*
string|number	blockNumber	the blockNumber *(optional)*
string|number	cumulativeGasUsed	the cumulativeGasUsed *(optional)*
string|number	gasUsed	the gasUsed *(optional)*
LogData []	logs	the logs
string	logsBloom	the logsBloom *(optional)*
string	root	the root *(optional)*
string|boolean	status	the status *(optional)*
string	transactionHash	the transactionHash *(optional)*
number	transactionIndex	the transactionIndex *(optional)*

9.9.4 Type TransactionData

Source: index.ts

Transaction as returned by eth_getTransactionByHash Transaction as returned by eth_getTransactionByHash

`string`	blockHash	the blockHash *(optional)*
`number|string`	blockNumber	the blockNumber *(optional)*
`number|string`	chainId	the chainId *(optional)*
`string`	condition	the condition *(optional)*
`string`	creates	the creates *(optional)*
`string`	data	the data *(optional)*
`string`	from	the from *(optional)*
`number|string`	gas	the gas *(optional)*
`number|string`	gasLimit	the gasLimit *(optional)*
`number|string`	gasPrice	the gasPrice *(optional)*
`string`	hash	the hash
`string`	input	the input
`number|string`	nonce	the nonce
`string`	publicKey	the publicKey *(optional)*
`string`	r	the r *(optional)*
`string`	raw	the raw *(optional)*
`string`	s	the s *(optional)*

9.9.5 Type Transport

Source: index.ts

A Transport-object responsible to transport the message to the handler. A Transport-object responsible to transport the message to the handler.

`Promise<>`	handle (url:`string`, data:*RPCRequest* | *RPCRequest* [], timeout:`number`)	handles a request by passing the data to the handler
`Promise<boolean>`	isOnline ()	check whether the handler is onlne.
`number` []	random (count:`number`)	generates random numbers (between 0-1)

9.10 Package modules/eth

9.10.1 Type Block

Source: modules/eth/serialize.ts

encodes and decodes the blockheader

Block	constructor (data:*Buffer* | `string` | *BlockData*)	creates a Block-Oject from either the block-data as returned from rpc, a buffer or a hex-string of the encoded blockheader
BlockHeader	raw	the raw Buffer fields of the BlockHeader
Tx []	transactions	the transaction-Object (if given)
Buffer	bloom	bloom
Buffer	coinbase	coinbase
Buffer	difficulty	difficulty
Buffer	extra	extra
Buffer	gasLimit	gas limit
Buffer	gasUsed	gas used
Buffer	number	number
Buffer	parentHash	parent hash
Buffer	receiptTrie	receipt trie
Buffer []	sealedFields	sealed fields
Buffer	stateRoot	state root
Buffer	timestamp	timestamp

9.10.2 Type Transaction

Source: modules/eth/serialize.ts

Buffer[] of the transaction = *Buffer* []

9.10.3 Type Receipt

Source: modules/eth/serialize.ts

Buffer[] of the Receipt = [*Buffer* ,*Buffer* ,*Buffer* ,*Buffer* , *Buffer* [] , *Buffer* []]

9.10.4 Type Account

Source: modules/eth/serialize.ts

Buffer[] of the Account = *Buffer* []

9.10.5 Type serialize

Source: modules/eth/serialize.ts

Class	*Block*	encodes and decodes the blockheader
Interface	*AccountData*	Account-Object
Interface	*BlockData*	Block as returned by eth_getBlockByNumber
Interface	*LogData*	LogData as part of the TransactionReceipt
Interface	*ReceiptData*	TransactionReceipt as returned by eth_getTransactionReceipt
Interface	*TransactionData*	Transaction as returned by eth_getTransactionByHash
Type	*Account*	Buffer[] of the Account
Type	*BlockHeader*	Buffer[] of the header
Type	*Receipt*	Buffer[] of the Receipt
Type	*Transaction*	Buffer[] of the transaction
index	rlp	RLP-functions value= `ethUtil.rlp`
`any`	address (val:`any`)	converts it to a Buffer with 20 bytes length
Block	blockFromHex (hex:`string`)	converts a hexstring to a block-object
`string`	blockToHex (block:`any`)	converts blockdata to a hexstring

9.10.6 Type storage

Source: modules/eth/storage.ts

`any`	getStorageArrayKey (pos:`number`, arrayIndex:`number`, structSize:`number`, structPos:`number`)	calc the storrage array key
`any`	getStorageMapKey (pos:`number`, key:`string`, structPos:`number`)	calcs the storage Map key.
`Promise<>`	getStorageValue (rpc:`string`, contract:`string`, pos:`number`, type:`'address'` | `'bytes32'` | `'bytes16'` | `'bytes4'` | `'int'` | `'string'`, keyOrIndex:`number` | `string`, structSize:`number`, structPos:`number`)	get a storage value from the server
`string` |	getStringValue (data:*Buffer* , storageKey:*Buffer*)	creates a string from storage.
`string`	getStringValueFromList (values:*Buffer* [], len:`number`)	concats the storage values to a string.
BN	toBN (val:`any`)	converts any value to BN

9.10.7 Type AccountData

Source: modules/eth/serialize.ts

Account-Object

`string`	balance	the balance
`string`	code	the code *(optional)*
`string`	codeHash	the codeHash
`string`	nonce	the nonce
`string`	storageHash	the storageHash

9.10.8 Type BlockHeader

Source: modules/eth/serialize.ts

Buffer[] of the header = *Buffer* []

9.11 Package types

9.11.1 Type RPCRequest

Source: types/types.ts

a JSONRPC-Request with N3-Extension

`number|string`	id	the identifier of the request example: 2 *(optional)*
IN3RPCRequestConfig	in3	the IN3-Config *(optional)*
`'2.0'`	jsonrpc	the version
`string`	method	the method to call example: eth_getBalance
`any` []	params	the params example: 0xe36179e2286ef405e929C90ad3E70E649B22a945,lates *(optional)*

9.11.2 Type RPCResponse

Source: types/types.ts

a JSONRPC-Responset with N3-Extension

`string`	error	in case of an error this needs to be set *(optional)*
`string|number`	id	the id matching the request example: 2
IN3ResponseConfig	in3	the IN3-Result *(optional)*
IN3NodeConfig	in3Node	the node handling this response (internal only) *(optional)*
`'2.0'`	jsonrpc	the version
`any`	result	the params example: 0xa35bc *(optional)*

9.11.3 Type IN3RPCRequestConfig

Source: types/types.ts

additional config for a IN3 RPC-Request

`string`	chainId	the requested chainId example: 0x1
`any`	clientSignature	the signature of the client *(optional)*
`number`	finality	if given the server will deliver the blockheaders of the following blocks until at least the number in percent of the validators is reached. *(optional)*
`boolean`	includeCode	if true, the request should include the codes of all accounts. otherwise only the the codeHash is returned. In this case the client may ask by calling eth_getCode() afterwards example: true *(optional)*
`number`	latestBlock	if specified, the blocknumber *latest* will be replaced by blockNumber- specified value example: 6 *(optional)*
`string` []	signatures	a list of addresses requested to sign the blockhash example: 0x6C1a01C2aB554930A937B0a2E8105fB47946c679 *(optional)*
`boolean`	useBinary	if true binary-data will be used. *(optional)*
`boolean`	useFullProof	if true all data in the response will be proven, which leads to a higher payload. *(optional)*
`boolean`	useRef	if true binary-data (starting with a 0x) will be refered if occuring again. *(optional)*

9.11.4 Type IN3ResponseConfig

Source: types/types.ts

additional data returned from a IN3 Server

`number`	currentBlock	the current blocknumber. example: 320126478 *(optional)*
`number`	lastNodeList	the blocknumber for the last block updating the nodelist. If the client has a smaller blocknumber he should update the nodeList. example: 326478 *(optional)*
`number`	lastValidatorChange	the blocknumber of gthe last change of the validatorList *(optional)*
Proof	proof	the Proof-data *(optional)*
`string`	version	the in3 protocol version. example: 1.0.0 *(optional)*

9.11.5 Type IN3NodeConfig

Source: types/types.ts

a configuration of a in3-server.

`string`	address	the address of the node, which is the public address it iis signing with. example: 0x6C1a01C2aB554930A937B0a2E8105fB47946c679
`number`	capacity	the capacity of the node. example: 100 *(optional)*
`string` []	chainIds	the list of supported chains example: 0x1
`number`	deposit	the deposit of the node in wei example: 12350000
`number`	index	the index within the contract example: 13 *(optional)*
`number`	props	the properties of the node. example: 3 *(optional)*
`number`	registerTime	the UNIX-timestamp when the node was registered example: 1563279168 *(optional)*
`number`	timeout	the time (in seconds) until an owner is able to receive his deposit back after he unregisters himself example: 3600 *(optional)*
`number`	unregisterTime	the UNIX-timestamp when the node is allowed to be deregister example: 1563279168 *(optional)*
`string`	url	the endpoint to post to example: https://in3.slock.it

9.11.6 Type Proof

Source: types/types.ts

the Proof-data as part of the in3-section

	accounts	a map of addresses and their AccountProof *(optional)*
`string`	block	the serialized blockheader as hex, required in most proofs example: 0x72804cfa0179d648ccbe6a65b01a6463a8f1ebb14f3aff6 *(optional)*
`any` []	finalityBlocks	the serialized blockheader as hex, required in case of finality asked example: 0x72804cfa0179d648ccbe6a65b01a6463a8f1ebb14f3aff6 *(optional)*
LogProof	logProof	the Log Proof in case of a Log-Request *(optional)*
`string` []	merkleProof	the serialized merle-noodes beginning with the root-node *(optional)*
`string` []	merkleProofPrev	the serialized merkle-noodes beginning with the root-node of the previous entry (only for full proof of receipts) *(optional)*
Signature []	signatures	requested signatures *(optional)*
`any` []	transactions	the list of transactions of the block example: *(optional)*
`number`	txIndex	the transactionIndex within the block example: 4 *(optional)*
`string` []	txProof	the serialized merkle-nodes beginning with the root-node in order to prrof the transactionIndex *(optional)*

9.11.7 Type LogProof

Source: types/types.ts

a Object holding proofs for event logs. The key is the blockNumber as hex

9.11.8 Type Signature

Source: types/types.ts

Verified ECDSA Signature. Signatures are a pair (r, s). Where r is computed as the X coordinate of a point R, modulo the curve order n.

`string`	address	the address of the signing node example: 0x6C1a01C2aB554930A937B0a2E8105fB47946c679 *(optional)*
`number`	block	the blocknumber example: 3123874
`string`	blockHash	the hash of the block example: 0x6C1a01C2aB554930A937B0a212346037E8105fB4794
`string`	msgHash	hash of the message example: 0x9C1a01C2aB554930A937B0a212346037E8105fB4794
`string`	r	Positive non-zero Integer signature.r example: 0x72804cfa0179d648ccbe6a65b01a6463a8f1ebb14f3aff6
`string`	s	Positive non-zero Integer signature.s example: 0x6d17b34aeaf95fee98c0437b4ac839d8a2ece1b18166da
`number`	v	Calculated curve point, or identity element O. example: 28

9.12 Package util

9.12.1 Type AxiosTransport

Source: util/transport.ts

Default Transport impl sending http-requests.

<table>
<tr><td>AxiosTransport</td><td>constructor (
format:'json'
| 'cbor'
| 'jsonRef')</td><td>Default Transport impl sending http-requests.</td></tr>
<tr><td>'json' | 'cbor' | 'jsonRef'</td><td>format</td><td>the format</td></tr>
<tr><td>Promise<></td><td>handle (
url:string,
data:RPCRequest
| RPCRequest [],
timeout:number)</td><td>handle</td></tr>
<tr><td>Promise<boolean></td><td>isOnline ()</td><td>is online</td></tr>
<tr><td>number []</td><td>random (
count:number)</td><td>random</td></tr>
</table>

9.12.2 Type cbor

Source: util/cbor.ts

`any`	convertToBuffer (val:`any`)	convert to buffer
`any`	convertToHex (val:`any`)	convert to hex
T	createRefs (val:*T* , cache:`string` [])	create refs
RPCRequest []	decodeRequests (request:*Buffer*)	decode requests
RPCResponse []	decodeResponses (responses:*Buffer*)	decode responses
Buffer	encodeRequests (requests:*RPCRequest* [])	turn
Buffer	encodeResponses (responses:*RPCResponse* [])	encode responses
T	resolveRefs (val:*T* , cache:`string` [])	resolve refs

9.12.3 Type transport

Source: util/transport.ts

Class	*AxiosTransport*	Default Transport impl sending http-requests.
Interface	*Transport*	A Transport-object responsible to transport the message to the handler.

9.12.4 Type util

Source: util/util.ts

BN	BN	the BN value= `ethUtil.BN`
`any`	Buffer	This file is part of the Incubed project. Sources: https://github.com/slockit/in3-common value= `require('buffer').Buffer`
T	checkForError (res:*T*)	check a RPC-Response for errors and rejects the promise if found
`number` []	createRandomIndexes (len:`number`, limit:`number`, seed:*Buffer* , result:`number` [])	create random indexes
`string`	fixLength (hex:`string`)	fix length
`string`	getAddress (pk:`string`)	returns a address from a private key
Buffer	getSigner (data:*Block*)	get signer
`string`	padEnd (val:`string`, minLength:`number`, fill:`string`)	padEnd for legacy
`string`	padStart (val:`string`, minLength:`number`, fill:`string`)	padStart for legacy
`Promise<any>`	promisify (	simple promisy-function

9.12.5 Type validate

Source: util/validate.ts

Ajv	ajv	the ajv instance with custom formatters and keywords value= `new Ajv()`
`void`	validate (ob:`any`, def:`any`)	validate
`void`	validateAndThrow (fn:*Ajv.ValidateFunction* , ob:`any`)	validates the data and throws an error in case they are not valid.

CHAPTER 10

API Reference WASM

This page contains a list of all Datastructures and Classes used within the IN3 WASM-Client.

10.1 Main Module

Importing incubed is as easy as

```
import Client from "in3-wasm"
```

While the In3Client-class is the default import, the following imports can be used:

This file is part of the Incubed project. Sources: https://github.com/slockit/in3-c

Class	*IN3*	the IN3
Class	*SimpleSigner*	the SimpleSigner
Interface	*EthAPI*	the EthAPI
Interface	*IN3Config*	the iguration of the IN3-Client. This can be paritally overriden for every request.
Interface	*IN3NodeConfig*	a configuration of a in3-server.
Interface	*IN3NodeWeight*	a local weight of a n3-node. (This is used internally to weight the requests)
Interface	*RPCRequest*	a JSONRPC-Request with N3-Extension
Interface	*RPCResponse*	a JSONRPC-Responset with N3-Extension
Interface	*Signer*	the Signer
Interface	*Utils*	Collection of different util-functions.
Type literal	*ABI*	the ABI
Type literal	*ABIField*	the ABIField
Type alias	*Address*	a 20 byte Address encoded as Hex (starting with 0x)
Type literal	*Block*	the Block

10.2 Package in3.d.ts

10.2.1 Type IN3

Source: in3.d.ts

IN3	default	supporting both ES6 and UMD usage
Utils	util	collection of util-functions.
`void`	freeAll ()	frees all Incubed instances.
Promise<T>	onInit (fn:)	registers a function to be called as soon as the wasm is ready. If it is already initialized it will call it right away.
`void`	setStorage (handler:)	changes the storage handler, which is called to read and write to the cache.
`void`	setTransport (fn:)	changes the transport-function.
IN3	constructor (config:*Partial<IN3Config>*)	creates a new client.
EthAPI	eth	eth1 API.
Signer	signer	the signer, if specified this interface will be used to sign transactions, if not, sending transaction will not be possible.
Utils	util	collection of util-functions.
`any`	free ()	disposes the Client. This must be called in order to free allocated memory!
Promise<RPCResponse>	send (request:*RPCRequest* , callback:)	sends a raw request. if the request is a array the response will be a array as well.

10.2.2 Type SimpleSigner

Source: in3.d.ts

SimpleSigner	constructor (pks:`any` [])	constructor
	accounts	the accounts
Promise<Transaction>	prepareTransaction (client:*IN3* , tx:*Transaction*)	optiional method which allows to change the transaction-data before sending it. This can be used for redirecting it through a multisig.
Promise<Uint8Array>	sign (data:*Hex* , account:*Address* , hashFirst:`boolean`, ethV:`boolean`)	signing of any data. if hashFirst is true the data should be hashed first, otherwise the data is the hash.
`string`	addAccount (pk:*Hash*)	add account
`Promise<boolean>`	hasAccount (account:*Address*)	returns true if the account is supported (or unlocked)

10.2.3 Type EthAPI

Source: in3.d.ts

IN3	client	the client
Signer	signer	the signer *(optional)*

Continued on next page

Table 1 – continued from previous page

Promise<number>	blockNumber ()	Returns the number of most recent block. (as number)
Promise<string>	call (tx:*Transaction* , block:*BlockType*)	Executes a new message call immediately without creating a transaction on the block chain.
Promise<any>	callFn (to:*Address* , method:string, args:any [])	Executes a function of a contract, by passing a [method-signature](https://github.com/ethereumjs/ethereumjs-abi/blob/master/README.md#simple-encoding-and-decoding) and the arguments, which will then be ABI-encoded and send as eth_call.
Promise<string>	chainId ()	Returns the EIP155 chain ID used for transaction signing at the current best block. Null is returned if not available.
any	constructor (client:*IN3*)	constructor
	contractAt (abi:*ABI* [], address:*Address*)	contract at
any	decodeEventData (log:*Log* , d:*ABI*)	decode event data
Promise<number>	estimateGas (tx:*Transaction*)	Makes a call or transaction, which won't be added to the blockchain and returns the used gas, which can be used for estimating the used gas.
Promise<number>	gasPrice ()	Returns the current price per gas in wei. (as number)

Continued on next page

Table 1 – continued from previous page

`Promise<bigint>`	getBalance (address:*Address* , block:*BlockType*)	Returns the balance of the account of given address in wei (as hex).
Promise<Block>	getBlockByHash (hash:*Hash* , includeTransactions:`boolean`)	Returns information about a block by hash.
Promise<Block>	getBlockByNumber (block:*BlockType* , includeTransactions:`boolean`)	Returns information about a block by block number.
`Promise<number>`	getBlockTransactionCountByHash (block:*Hash*)	Returns the number of transactions in a block from a block matching the given block hash.
`Promise<number>`	getBlockTransactionCountByNumber (block:*Hash*)	Returns the number of transactions in a block from a block matching the given block number.
`Promise<string>`	getCode (address:*Address* , block:*BlockType*)	Returns code at a given address.
`Promise<>`	getFilterChanges (id:*Quantity*)	Polling method for a filter, which returns an array of logs which occurred since last poll.
`Promise<>`	getFilterLogs (id:*Quantity*)	Returns an array of all logs matching filter with given id.
`Promise<>`	getLogs (filter:*LogFilter*)	Returns an array of all logs matching a given filter object.

Continued on next page

Table 1 – continued from previous page

`Promise<string>`	getStorageAt (address:*Address* , pos:*Quantity* , block:*BlockType*)	Returns the value from a storage position at a given address.
Promise<TransactionDetail>	getTransactionByBlockHashAndIndex (hash:*Hash* , pos:*Quantity*)	Returns information about a transaction by block hash and transaction index position.
Promise<TransactionDetail>	getTransactionByBlockNumberAndIndex (block:*BlockType* , pos:*Quantity*)	Returns information about a transaction by block number and transaction index position.
Promise<TransactionDetail>	getTransactionByHash (hash:*Hash*)	Returns the information about a transaction requested by transaction hash.
`Promise<number>`	getTransactionCount (address:*Address* , block:*BlockType*)	Returns the number of transactions sent from an address. (as number)
Promise<TransactionReceipt>	getTransactionReceipt (hash:*Hash*)	Returns the receipt of a transaction by transaction hash. Note That the receipt is available even for pending transactions.
Promise<Block>	getUncleByBlockHashAndIndex (hash:*Hash* , pos:*Quantity*)	Returns information about a uncle of a block by hash and uncle index position. Note: An uncle doesn't contain individual transactions.

Continued on next page

Table 1 – continued from previous page

Promise<Block>	getUncleByBlockNumberAndIndex (block:*BlockType* , pos:*Quantity*)	Returns information about a uncle of a block number and uncle index position. Note: An uncle doesn't contain individual transactions.
`Promise<number>`	getUncleCountByBlockHash (hash:*Hash*)	Returns the number of uncles in a block from a block matching the given block hash.
`Promise<number>`	getUncleCountByBlockNumber (block:*BlockType*)	Returns the number of uncles in a block from a block matching the given block hash.
Hex	hashMessage (data:*Data*)	a Hexcoded String (starting with 0x)
`Promise<string>`	newBlockFilter ()	Creates a filter in the node, to notify when a new block arrives. To check if the state has changed, call eth_getFilterChanges.
`Promise<string>`	newFilter (filter:*LogFilter*)	Creates a filter object, based on filter options, to notify when the state changes (logs). To check if the state has changed, call eth_getFilterChanges.
`Promise<string>`	newPendingTransactionFilter ()	Creates a filter in the node, to notify when new pending transactions arrive.
`Promise<string>`	protocolVersion ()	Returns the current ethereum protocol version.
`Promise<string>`	sendRawTransaction (data:*Data*)	Creates new message call transaction or a contract creation for signed transactions.

Continued on next page

Table 1 – continued from previous page

`Promise<>`	sendTransaction (args:*TxRequest*)	sends a Transaction
Promise<Signature>	sign (account:*Address* , data:*Data*)	signs any kind of message using the *x19Ethereum Signed Message:n*-prefix
`Promise<>`	syncing ()	Returns the current ethereum protocol version.
Promise<Quantity>	uninstallFilter (id:*Quantity*)	Uninstalls a filter with given id. Should always be called when watch is no longer needed. Additonally Filters timeout when they aren't requested with eth_getFilterChanges for a period of time.

10.2.4 Type IN3Config

Source: in3.d.ts

the iguration of the IN3-Client. This can be paritally overriden for every request.

`boolean`	autoConfig	if true the config will be adjusted depending on the request *(optional)*
`boolean`	autoUpdateList	if true the nodelist will be automaticly updated if the lastBlock is newer example: true *(optional)*
`number`	cacheTimeout	number of seconds requests can be cached. *(optional)*
`string`	chainId	servers to filter for the given chain. The chain-id based on EIP-155. example: 0x1
`string`	chainRegistry	main chain-registry contract example: 0xe36179e2286ef405e929C90ad3E70E649B22a945 *(optional)*
`number`	finality	the number in percent needed in order reach finality (% of signature of the validators) example: 50 *(optional)*
`'json'|'jsonRef'|'cbor'`	format	the format for sending the data to the client. Default is json, but using cbor means using only 30-40% of the payload since it is using binary encoding example: json *(optional)*
`boolean`	includeCode	if true, the request should include the codes of all accounts. otherwise only the the codeHash is returned. In this case the client may ask by calling eth_getCode() afterwards example: true *(optional)*

10.2.5 Type IN3NodeConfig

Source: in3.d.ts

a configuration of a in3-server.

`string`	address	the address of the node, which is the public address it iis signing with. example: 0x6C1a01C2aB554930A937B0a2E8105fB47946c679
`number`	capacity	the capacity of the node. example: 100 *(optional)*
`string` []	chainIds	the list of supported chains example: 0x1
`number`	deposit	the deposit of the node in wei example: 12350000
`number`	index	the index within the contract example: 13 *(optional)*
`number`	props	the properties of the node. example: 3 *(optional)*
`number`	registerTime	the UNIX-timestamp when the node was registered example: 1563279168 *(optional)*
`number`	timeout	the time (in seconds) until an owner is able to receive his deposit back after he unregisters himself example: 3600 *(optional)*
`number`	unregisterTime	the UNIX-timestamp when the node is allowed to be deregister example: 1563279168 *(optional)*
`string`	url	the endpoint to post to example: https://in3.slock.it

10.2.6 Type IN3NodeWeight

Source: in3.d.ts

a local weight of a n3-node. (This is used internally to weight the requests)

`number`	avgResponseTime	average time of a response in ms example: 240 *(optional)*
`number`	blacklistedUntil	blacklisted because of failed requests until the timestamp example: 1529074639623 *(optional)*
`number`	lastRequest	timestamp of the last request in ms example: 1529074632623 *(optional)*
`number`	pricePerRequest	last price *(optional)*
`number`	responseCount	number of uses. example: 147 *(optional)*
`number`	weight	factor the weight this noe (default 1.0) example: 0.5 *(optional)*

10.2.7 Type RPCRequest

Source: in3.d.ts

a JSONRPC-Request with N3-Extension

`number	string`	id	the identifier of the request example: 2 *(optional)*
`'2.0'`	jsonrpc	the version
`string`	method	the method to call example: eth_getBalance
`any []`	params	the params example: 0xe36179e2286ef405e929C90ad3E70E649B22a945,lates *(optional)*

10.2.8 Type RPCResponse

Source: in3.d.ts

a JSONRPC-Responset with N3-Extension

`string`	error	in case of an error this needs to be set *(optional)*
`string	number`	id	the id matching the request example: 2
`'2.0'`	jsonrpc	the version
`any`	result	the params example: 0xa35bc *(optional)*

10.2.9 Type Signer

Source: in3.d.ts

Promise<Transaction>	prepareTransaction (client:*IN3* , tx:*Transaction*)	optiional method which allows to change the transaction-data before sending it. This can be used for redirecting it through a multisig.
Promise<Uint8Array>	sign (data:*Hex* , account:*Address* , hashFirst:`boolean`, ethV:`boolean`)	signing of any data. if hashFirst is true the data should be hashed first, otherwise the data is the hash.
`Promise<boolean>`	hasAccount (account:*Address*)	returns true if the account is supported (or unlocked)

10.2.10 Type Utils

Source: in3.d.ts

Collection of different util-functions.

any []	abiDecode (signature:string, data:*Data*)	decodes the given data as ABI-encoded (without the methodHash)
Hex	abiEncode (signature:string, args:any [])	encodes the given arguments as ABI-encoded (including the methodHash)
string	createSignature (fields:*ABIField* [])	create signature
Hex	createSignatureHash (def:*ABI*)	a Hexcoded String (starting with 0x)
any	decodeEvent (log:*Log* , d:*ABI*)	decode event
Uint8Array	ecSign (pk:*Uint8Array* | *Hex* , msg:*Uint8Array* | *Hex* , hashFirst:boolean, adjustV:boolean)	create a signature (65 bytes) for the given message and kexy
Uint8Array	keccak (data:*Uint8Array* | *Data*)	calculates the keccack hash for the given data.
Address	private2address (pk:*Hex* | *Uint8Array*)	generates the public address from the private key.
string	soliditySha3 (args:any [])	solidity sha3
Signature	splitSignature (signature:*Uint8Array* | *Hex* ,	takes raw signature (65 bytes) and splits it into a signature object.

10.2.11 Type ABI

Source: in3.d.ts

`boolean`	anonymous	the anonymous *(optional)*
`boolean`	constant	the constant *(optional)*
ABIField []	inputs	the inputs *(optional)*
`string`	name	the name *(optional)*
ABIField []	outputs	the outputs *(optional)*
`boolean`	payable	the payable *(optional)*

`'nonpayable'`
`|'payable'`
`|'view'`
`|'pure'`
	stateMutability	the stateMutability *(optional)*

`'event'`
`|'function'`
`|'constructor'`
`|'fallback'`
	type	the type

10.2.12 Type ABIField

Source: in3.d.ts

`boolean`	indexed	the indexed *(optional)*
`string`	name	the name
`string`	type	the type

10.2.13 Type Address

Source: in3.d.ts

a 20 byte Address encoded as Hex (starting with 0x) a Hexcoded String (starting with 0x) = `string`

10.2.14 Type Block

Source: in3.d.ts

Address	author	20 Bytes - the address of the author of the block (the beneficiary to whom the mining rewards were given)
Quantity	difficulty	integer of the difficulty for this block
Data	extraData	the 'extra data' field of this block
Quantity	gasLimit	the maximum gas allowed in this block
Quantity	gasUsed	the total used gas by all transactions in this block
Hash	hash	hash of the block. null when its pending block
Data	logsBloom	256 Bytes - the bloom filter for the logs of the block. null when its pending block
Address	miner	20 Bytes - alias of 'author'
Data	nonce	8 bytes hash of the generated proof-of-work. null when its pending block. Missing in case of PoA.
Quantity	number	The block number. null when its pending block
Hash	parentHash	hash of the parent block
Data	receiptsRoot	32 Bytes - the root of the receipts trie of the block

10.2.15 Type Data

Source: in3.d.ts

data encoded as Hex (starting with 0x) a Hexcoded String (starting with 0x) = `string`

10.2.16 Type Hash

Source: in3.d.ts

a 32 byte Hash encoded as Hex (starting with 0x) a Hexcoded String (starting with 0x) = `string`

10.2.17 Type Log

Source: in3.d.ts

Address	address	20 Bytes - address from which this log originated.
Hash	blockHash	Hash, 32 Bytes - hash of the block where this log was in. null when its pending. null when its pending log.
Quantity	blockNumber	the block number where this log was in. null when its pending. null when its pending log.
Data	data	contains the non-indexed arguments of the log.
Quantity	logIndex	integer of the log index position in the block. null when its pending log.
`boolean`	removed	true when the log was removed, due to a chain reorganization. false if its a valid log.
Data []	topics	- Array of 0 to 4 32 Bytes DATA of indexed log arguments. (In solidity: The first topic is the hash of the signature of the event (e.g. Deposit(address,bytes32,uint256)), except you declared the event with the anonymous specifier.)
Hash	transactionHash	Hash, 32 Bytes - hash of the transactions this log was created from. null when its pending log.
Quantity	transactionIndex	integer of the transactions index position log was created from. null when its pending log.

10.2.18 Type LogFilter

Source: in3.d.ts

Address	address	(optional) 20 Bytes - Contract address or a list of addresses from which logs should originate.
BlockType	fromBlock	Quantity or Tag - (optional) (default: latest) Integer block number, or 'latest' for the last mined block or 'pending', 'earliest' for not yet mined transactions.
Quantity	limit	å(optional) The maximum number of entries to retrieve (latest first).
BlockType	toBlock	Quantity or Tag - (optional) (default: latest) Integer block number, or 'latest' for the last mined block or 'pending', 'earliest' for not yet mined transactions.
`string` | `string` [] []	topics	(optional) Array of 32 Bytes Data topics. Topics are order-dependent. It's possible to pass in null to match any topic, or a subarray of multiple topics of which one should be matching.

10.2.19 Type Signature

Source: in3.d.ts

Signature

Data	message	the message
Hash	messageHash	the messageHash
Hash	r	the r
Hash	s	the s
Data	signature	the signature *(optional)*
Hex	v	the v

10.2.20 Type Transaction

Source: in3.d.ts

`any`	chainId	optional chain id *(optional)*
`string`	data	4 byte hash of the method signature followed by encoded parameters. For details see Ethereum Contract ABI.
Address	from	20 Bytes - The address the transaction is send from.
Quantity	gas	Integer of the gas provided for the transaction execution. eth_call consumes zero gas, but this parameter may be needed by some executions.
Quantity	gasPrice	Integer of the gas price used for each paid gas.
Quantity	nonce	nonce
Address	to	(optional when creating new contract) 20 Bytes - The address the transaction is directed to.
Quantity	value	Integer of the value sent with this transaction.

10.2.21 Type TransactionDetail

Source: in3.d.ts

Hash	blockHash	32 Bytes - hash of the block where this transaction was in. null when its pending.
BlockType	blockNumber	block number where this transaction was in. null when its pending.
Quantity	chainId	the chain id of the transaction, if any.
`any`	condition	(optional) conditional submission, Block number in block or timestamp in time or null. (parity-feature)
Address	creates	creates contract address
Address	from	20 Bytes - address of the sender.
Quantity	gas	gas provided by the sender.
Quantity	gasPrice	gas price provided by the sender in Wei.
Hash	hash	32 Bytes - hash of the transaction.
Data	input	the data send along with the transaction.
Quantity	nonce	the number of transactions made by the sender prior to this one.
`any`	pk	optional: the private key to use for signing *(optional)*

10.2.22 Type TransactionReceipt

Source: in3.d.ts

Hash	blockHash	32 Bytes - hash of the block where this transaction was in.
BlockType	blockNumber	block number where this transaction was in.
Address	contractAddress	20 Bytes - The contract address created, if the transaction was a contract creation, otherwise null.
Quantity	cumulativeGasUsed	The total amount of gas used when this transaction was executed in the block.
Address	from	20 Bytes - The address of the sender.
Quantity	gasUsed	The amount of gas used by this specific transaction alone.
Log []	logs	Array of log objects, which this transaction generated.
Data	logsBloom	256 Bytes - A bloom filter of logs/events generated by contracts during transaction execution. Used to efficiently rule out transactions without expected logs.
Hash	root	32 Bytes - Merkle root of the state trie after the transaction has been executed (optional after Byzantium hard fork EIP609)
Quantity	status	0x0 indicates transaction failure , 0x1 indicates transaction success. Set for blocks mined after Byzantium hard fork EIP609, null before.

10.2.23 Type TxRequest

Source: in3.d.ts

`any` []	args	the argument to pass to the method *(optional)*
`number`	confirmations	number of block to wait before confirming *(optional)*
Data	data	the data to send *(optional)*
Address	from	address of the account to use *(optional)*
`number`	gas	the gas needed *(optional)*
`number`	gasPrice	the gasPrice used *(optional)*
`string`	method	the ABI of the method to be used *(optional)*
`number`	nonce	the nonce *(optional)*
Hash	pk	raw private key in order to sign *(optional)*
Address	to	contract *(optional)*
Quantity	value	the value in wei *(optional)*

10.2.24 Type Hex

Source: in3.d.ts

a Hexcoded String (starting with 0x) = `string`

10.2.25 Type BlockType

Source: in3.d.ts

BlockNumber or predefined Block = `number` | `'latest'` | `'earliest'` | `'pending'`

10.2.26 Type Quantity

Source: in3.d.ts

a BigInteger encoded as hex. = `number` | *Hex*

CHAPTER 11

API Reference Java

11.1 Installing

The Incubed Java client uses JNI in order to call native functions. But all the native-libraries are bundled inside the jar-file. This jar file ha **no** dependencies and can even be used standalone:

like

```
java -cp in3.jar in3.IN3 eth_getBlockByNumber latest false
```

11.2 Examples

11.2.1 Using in3 directly

```
import in3.IN3;

public class HelloIN3 {
   //
   public static void main(String[] args) {
       String blockNumber = args[0];

       // create incubed
       IN3 in3 = new IN3();

       // configure
       in3.setChainId(0x1);  // set it to mainnet (which is also dthe default)

       // execute the request
       String jsonResult = in3.sendRPC("eth_getBlockByNumber",new Object[]{
↪blockNumber ,true});
```

(continues on next page)

(continued from previous page)

```
        ....
    }
}
```

11.2.2 Using the API

in3 also offers a API for getting Information directly in a structured way.

Reading Blocks

```
import java.util.*;
import in3.*;
import in3.eth1.*;

public class HelloIN3 {
    //
     public static void main(String[] args) throws Exception {
         // create incubed
         IN3 in3 = new IN3();

         // configure
         in3.setChainId(0x1); // set it to mainnet (which is also dthe default)

         // read the latest Block including all Transactions.
         Block latestBlock = in3.getEth1API().getBlockByNumber(Block.LATEST, true);

         // Use the getters to retrieve all containing data
         System.out.println("current BlockNumber : " + latestBlock.getNumber());
         System.out.println("minded at : " + new Date(latestBlock.getTimeStamp()) + "␣
↪by " + latestBlock.getAuthor());

         // get all Transaction of the Block
         Transaction[] transactions = latestBlock.getTransactions();

         BigInteger sum = BigInteger.valueOf(0);
         for (int i = 0; i < transactions.length; i++)
             sum = sum.add(transactions[i].getValue());

         System.out.println("total Value transfered in all Transactions : " + sum + "␣
↪wei");
     }

}
```

Calling Functions of Contracts

This Example shows how to call functions and use the decoded results. Here we get the struct from the registry.

```
import in3.*;
import in3.eth1.*;

public class HelloIN3 {
```

(continues on next page)

(continued from previous page)

```
    //
    public static void main(String[] args) {
        // create incubed
        IN3 in3 = new IN3();

        // configure
        in3.setChainId(0x1);  // set it to mainnet (which is also dthe default)

        // call a contract, which uses eth_call to get the result.
        Object[] result = (Object[]) in3.getEth1API().call(                                    ␣
↪        // call a function of a contract
            "0x2736D225f85740f42D17987100dc8d58e9e16252",                         //␣
↪address of the contract
            "servers(uint256):(string,address,uint256,uint256,uint256,address)",//␣
↪function signature
            1);                                                                   //␣
↪first argument, which is the index of the node we are looking for.

         System.out.println("url     : " + result[0]);
         System.out.println("owner   : " + result[1]);
         System.out.println("deposit : " + result[2]);
         System.out.println("props   : " + result[3]);


        ....
    }
}
```

Sending Transactions

In order to send, you need a Signer. The SimpleWallet class is a basic implementation which can be used.

```
package in3;

import java.io.IOException;
import java.math.BigInteger;
import java.nio.charset.StandardCharsets;
import java.nio.file.Files;
import java.nio.file.Paths;

import in3.*;
import in3.eth1.*;

public class Example {
    //
    public static void main(String[] args) throws IOException{
        // create incubed
        IN3 in3 = new IN3();

        // configure
        in3.setChainId(0x1); // set it to mainnet (which is also dthe default)

        // create a wallet managing the private keys
        SimpleWallet wallet = new SimpleWallet();
```

(continues on next page)

(continued from previous page)

```
        // add accounts by adding the private keys
        String keyFile = "myKey.json";
        String myPassphrase = "<secrect>";

        // read the keyfile and decoded the private key
        String account = wallet.addKeyStore(
                Files.readString(Paths.get(keyFile)),
                myPassphrase);

        // use the wallet as signer
        in3.setSigner(wallet);

        String receipient = "0x1234567890123456789012345678901234567890";
        BigInteger value = BigInteger.valueOf(100000);

        // create a Transaction
        TransactionRequest tx = new TransactionRequest();
        tx.from = account;
        tx.to = "0x1234567890123456789012345678901234567890";
        tx.function = "transfer(address,uint256)";
        tx.params = new Object[] { receipient, value };

        String txHash = in3.getEth1API().sendTransaction(tx);

        System.out.println("Transaction sent with hash = " + txHash);

    }
}
```

11.2.3 Downloading

The jar file can be downloaded from the latest release. here.

Alternatively, If you wish to download Incubed using the maven package manager, add this to your pom.xml

```
<dependency>
  <groupId>it.slock</groupId>
  <artifactId>in3</artifactId>
  <version>2.21</version>
</dependency>
```

After which, install in3 with `mvn install`.

11.2.4 Building

For building the shared library you need to enable java by using the `-DJAVA=true` flag:

```
git clone git@github.com:slockit/in3-c.git
mkdir -p in3-c/build
cd in3-c/build
cmake -DJAVA=true .. && make
```

You will find the `in3.jar` in the build/lib - folder.

11.2.5 Android

In order to use Incubed in android simply follow these steps:

Step 1: Create a top-level CMakeLists.txt in android project inside app folder and link this to gradle. Follow the steps using this guide on howto link.

The Content of the `CMakeLists.txt` should look like this:

```
cmake_minimum_required(VERSION 3.4.1)

# turn off FAST_MATH in the evm.
ADD_DEFINITIONS(-DIN3_MATH_LITE)

# loop through the required module and cretae the build-folders
foreach(module
  core
  verifier/eth1/nano
  verifier/eth1/evm
  verifier/eth1/basic
  verifier/eth1/full
  bindings/java
  third-party/crypto
  third-party/tommath
  api/eth1)
        file(MAKE_DIRECTORY in3-c/src/${module}/outputs)
        add_subdirectory( in3-c/src/${module} in3-c/src/${module}/outputs )
endforeach()
```

Step 2: clone in3-c into the `app`-folder or use this script to clone and update in3:

```
#!/usr/bin/env sh

#github-url for in3-c
IN3_SRC=https://github.com/slockit/in3-c.git

cd app

# if it exists we only call git pull
if [ -d in3-c ]; then
    cd in3-c
    git pull
    cd ..
else
# if not we clone it
    git clone $IN3_SRC
fi


# copy the java-sources to the main java path
cp -r in3-c/src/bindings/java/in3 src/main/java/
# but not the native libs, since these will be build
rm -rf src/main/java/in3/native
```

Step 3: Use methods available in app/src/main/java/in3/IN3.java from android activity to access IN3 functions.

Here is example how to use it:

https://github.com/slockit/in3-example-android

11.3 Package in3

11.3.1 class Chain

Constants for Chain-specs.

MULTICHAIN

support for multiple chains, a client can then switch between different chains (but consumes more memory)

Type: static `final long`

MAINNET

use mainnet

Type: static `final long`

KOVAN

use kovan testnet

Type: static `final long`

TOBALABA

use tobalaba testnet

Type: static `final long`

GOERLI

use goerli testnet

Type: static `final long`

EVAN

use evan testnet

Type: static `final long`

IPFS

use ipfs

Type: static `final long`

VOLTA

use volta test net

Type: static `final long`

LOCAL

use local client

Type: static `final long`

11.3.2 class IN3

This is the main class creating the incubed client.

The client can then be configured.

getCacheTimeout

number of seconds requests can be cached.

public `native int` getCacheTimeout();

setCacheTimeout

sets number of seconds requests can be cached.

public `native void` setCacheTimeout(*int* val);

arguments:

`int`	**val**

setConfig

sets config object in the client

public `native void` setConfig(*String* val);

arguments:

`String`	**val**

getNodeLimit

the limit of nodes to store in the client.

public `native int` getNodeLimit();

setNodeLimit

sets the limit of nodes to store in the client.

public `native void` setNodeLimit(*int* val);

arguments:

`int`	**val**

getKey

the client key to sign requests

public `native byte[]` getKey();

setKey

sets the client key to sign requests

public `native void` setKey(*byte[]* val);

arguments:

`byte[]`	**val**

setKey

sets the client key as hexstring to sign requests

public `void` setKey(*String* val);

arguments:

`String`	**val**

getMaxCodeCache

number of max bytes used to cache the code in memory

public `native int` getMaxCodeCache();

setMaxCodeCache

sets number of max bytes used to cache the code in memory

public `native void` setMaxCodeCache(*int* val);

arguments:

`int`	**val**

getMaxBlockCache

number of blocks cached in memory

public `native int` getMaxBlockCache();

setMaxBlockCache

sets the number of blocks cached in memory

public `native void` setMaxBlockCache(*int* val);

arguments:

`int`	**val**

getProof

the type of proof used

public *Proofnative* getProof();

setProof

sets the type of proof used

public `native void` setProof(*Proof* val);

arguments:

Proof	**val**

getRequestCount

the number of request send when getting a first answer

public `native int` getRequestCount();

setRequestCount

sets the number of requests send when getting a first answer

public `native void` setRequestCount(*int* val);

arguments:

`int`	**val**

getSignatureCount

the number of signatures used to proof the blockhash.

public `native int` getSignatureCount();

setSignatureCount

sets the number of signatures used to proof the blockhash.

public `native void` setSignatureCount(*int* val);

arguments:

`int`	**val**

getMinDeposit

min stake of the server.

Only nodes owning at least this amount will be chosen.

public `native long` getMinDeposit();

setMinDeposit

sets min stake of the server.

Only nodes owning at least this amount will be chosen.

public `native void` setMinDeposit(*long* val);

arguments:

`long`	**val**

getReplaceLatestBlock

if specified, the blocknumber *latest* will be replaced by blockNumber- specified value

public `native int` getReplaceLatestBlock();

setReplaceLatestBlock

replaces the *latest* with blockNumber- specified value

public `native void` setReplaceLatestBlock(*int* val);

arguments:

`int`	**val**

getFinality

the number of signatures in percent required for the request

public `native int` getFinality();

setFinality

sets the number of signatures in percent required for the request

public `native void` setFinality(*`int`* val);

arguments:

`int`	**val**

getMaxAttempts

the max number of attempts before giving up

public `native int` getMaxAttempts();

setMaxAttempts

sets the max number of attempts before giving up

public `native void` setMaxAttempts(*`int`* val);

arguments:

`int`	**val**

getSigner

returns the signer or wallet.

public *`Signer`* getSigner();

getEth1API

gets the ethereum-api

public *`in3.eth1.API`* getEth1API();

setSigner

sets the signer or wallet.

public `void` setSigner(*`Signer`* signer);

arguments:

Signer	**signer**

getTimeout

specifies the number of milliseconds before the request times out.

increasing may be helpful if the device uses a slow connection.

public `native int` getTimeout();

setTimeout

specifies the number of milliseconds before the request times out.

increasing may be helpful if the device uses a slow connection.

public `native void` setTimeout(*int* val);

arguments:

`int`	**val**

getChainId

servers to filter for the given chain.

The chain-id based on EIP-155.

public `native long` getChainId();

setChainId

sets the chain to be used.

The chain-id based on EIP-155.

public `native void` setChainId(*long* val);

arguments:

`long`	**val**

isAutoUpdateList

if true the nodelist will be automaticly updated if the lastBlock is newer

public `native boolean` isAutoUpdateList();

setAutoUpdateList

activates the auto update.if true the nodelist will be automaticly updated if the lastBlock is newer

public `native void` setAutoUpdateList(*boolean* val);

arguments:

`boolean`	**val**

getStorageProvider

provides the ability to cache content

public *StorageProvider* getStorageProvider();

setStorageProvider

provides the ability to cache content like nodelists, contract codes and validatorlists

public `void` setStorageProvider(*StorageProvider* val);

arguments:

StorageProvider	**val**

send

send a request.

The request must a valid json-string with method and params

public `native String` send(*String* request);

arguments:

`String`	**request**

sendobject

send a request but returns a object like array or map with the parsed response.

The request must a valid json-string with method and params

public `native Object` sendobject(*String* request);

arguments:

`String`	**request**

sendRPC

send a RPC request by only passing the method and params.

It will create the raw request from it and return the result.

public `String` sendRPC(*String* method, *Object[]* params);

arguments:

`String`	**method**
`Object[]`	**params**

sendRPCasObject

send a RPC request by only passing the method and params.

It will create the raw request from it and return the result.

public `Object` sendRPCasObject(*`String`* method, *`Object[]`* params);

arguments:

`String`	**method**
`Object[]`	**params**

IN3

public IN3();

setTransport

sets The transport interface.

This allows to fetch the result of the incubed in a different way.

public `void` setTransport(*`IN3Transport`* newTransport);

arguments:

`IN3Transport`	**newTransport**

getTransport

returns the current transport implementation.

public `IN3Transport` getTransport();

forChain

create a Incubed client using the chain-config.

if chainId is Chain.MULTICHAIN, the client can later be switched between different chains, for all other chains, it will be initialized only with the chainspec for this one chain (safes memory)

public static *`IN3`* forChain(*`long`* chainId);

arguments:

`long`	**chainId**

main

public static `void` main(*`String[]`* args);

arguments:

`String[]`	**args**

11.3.3 class IN3DefaultTransport

handle

public `byte[][]` handle(*String[]* urls, *byte[]* payload);

arguments:

`String[]`	**urls**
`byte[]`	**payload**

11.3.4 class JSON

internal helper tool to represent a JSON-Object.

Since the internal representation of JSON in incubed uses hashes instead of name, the getter will creates these hashes.

get

gets the property

public `Object` get(*String* prop);

arguments:

`String`	**prop**	the name of the property.

returns: `Object` : the raw object.

put

adds values.

This function will be called from the JNI-Iterface.

Internal use only!

public `void` put(*int* key, *Object* val);

arguments:

`int`	**key**	the hash of the key
`Object`	**val**	the value object

getLong

returns the property as long

public `long` getLong(*String* key);

arguments:

`String`	**key**	the propertyName

returns: `long` : the long value

getBigInteger

returns the property as BigInteger

public `BigInteger` getBigInteger(*String* key);

arguments:

`String`	**key**	the propertyName

returns: `BigInteger` : the BigInteger value

getStringArray

returns the property as StringArray

public `String[]` getStringArray(*String* key);

arguments:

`String`	**key**	the propertyName

returns: `String[]` : the array or null

getString

returns the property as String or in case of a number as hexstring.

public `String` getString(*String* key);

arguments:

`String`	**key**	the propertyName

returns: `String` : the hexstring

toString

public `String` toString();

hashCode

public `int` hashCode();

equals

public `boolean` equals(*Object* obj);

arguments:

`Object`	**obj**

asStringArray

casts the object to a String[]

public static `String[]` asStringArray(*Object* o);

arguments:

`Object`	**o**

asBigInteger

public static `BigInteger` asBigInteger(*Object* o);

arguments:

`Object`	**o**

asLong

public static `long` asLong(*Object* o);

arguments:

`Object`	**o**

asInt

public static `int` asInt(*Object* o);

arguments:

`Object`	**o**

asString

public static `String` asString(*`Object`* o);

arguments:

`Object`	**o**

toJson

public static `String` toJson(*`Object`* ob);

arguments:

`Object`	**ob**

appendKey

public static `void` appendKey(*`StringBuilder`* sb, *`String`* key, *`Object`* value);

arguments:

`StringBuilder`	**sb**
`String`	**key**
`Object`	**value**

11.3.5 class Loader

loadLibrary

public static `void` loadLibrary();

11.3.6 class TempStorageProvider

a simple Storage Provider storing the cache in the temp-folder.

getItem

returns a item from cache ()

public `byte[]` getItem(*`String`* key);

arguments:

`String`	**key**	the key for the item

returns: `byte[]` : the bytes or null if not found.

setItem

stores a item in the cache.

public `void` setItem(*String* key, *byte[]* content);

arguments:

`String`	**key**	the key for the item
`byte[]`	**content**	the value to store

11.3.7 enum Proof

The Proof type indicating how much proof is required.

The enum type contains the following values:

none	0	No Verification.
standard	1	Standard Verification of the important properties.
full	2	Full Verification including even uncles wich leads to higher payload.

11.3.8 interface IN3Transport

handle

public `byte[][]` handle(*String[]* urls, *byte[]* payload);

arguments:

`String[]`	**urls**
`byte[]`	**payload**

11.3.9 interface Signer

a Interface responsible for signing data or transactions.

prepareTransaction

optiional method which allows to change the transaction-data before sending it.

This can be used for redirecting it through a multisig.

public *TransactionRequest* prepareTransaction(*IN3* in3, *TransactionRequest* tx);

arguments:

IN3	**in3**
TransactionRequest	**tx**

hasAccount

returns true if the account is supported (or unlocked)

> public `boolean` hasAccount(*`String`* address);

arguments:

`String`	**address**

sign

signing of the raw data.

> public `String` sign(*`String`* data, *`String`* address);

arguments:

`String`	**data**
`String`	**address**

11.3.10 interface StorageProvider

Provider methods to cache data.

These data could be nodelists, contract codes or validator changes.

getItem

returns a item from cache ()

> public `byte[]` getItem(*`String`* key);

arguments:

`String`	**key**	the key for the item

returns: `byte[]` : the bytes or null if not found.

setItem

stores a item in the cache.

> public `void` setItem(*`String`* key, *`byte[]`* content);

arguments:

`String`	**key**	the key for the item
`byte[]`	**content**	the value to store

11.4 Package in3.eth1

11.4.1 class API

a Wrapper for the incubed client offering Type-safe Access and additional helper functions.

API

creates a API using the given incubed instance.

public API(*IN3* in3);

arguments:

IN3	**in3**

getBlockByNumber

finds the Block as specified by the number.

use `Block.LATEST` for getting the lastest block.

public *Block* getBlockByNumber(*long* block, *boolean* includeTransactions);

arguments:

`long`	**block**	
`boolean`	**includeTransactions**	< the Blocknumber < if true all Transactions will be includes, if not only the transactionhashes

getBlockByHash

Returns information about a block by hash.

public *Block* getBlockByHash(*String* blockHash, *boolean* includeTransactions);

arguments:

`String`	**blockHash**	
`boolean`	**includeTransactions**	< the Blocknumber < if true all Transactions will be includes, if not only the transactionhashes

getBlockNumber

the current BlockNumber.

public `long` getBlockNumber();

getGasPrice

the current Gas Price.

public `long` getGasPrice();

getChainId

Returns the EIP155 chain ID used for transaction signing at the current best block.

Null is returned if not available.

public `String` getChainId();

call

calls a function of a smart contract and returns the result.

public `Object` call(*TransactionRequest* request, *long* block);

arguments:

TransactionRequest	**request**	
`long`	**block**	< the transaction to call. < the Block used to for the state.

returns: `Object` : the decoded result. if only one return value is expected the Object will be returned, if not an array of objects will be the result.

estimateGas

Makes a call or transaction, which won't be added to the blockchain and returns the used gas, which can be used for estimating the used gas.

public `long` estimateGas(*TransactionRequest* request, *long* block);

arguments:

TransactionRequest	**request**	
`long`	**block**	< the transaction to call. < the Block used to for the state.

returns: `long` : the gas required to call the function.

getBalance

Returns the balance of the account of given address in wei.

public `BigInteger` getBalance(*String* address, *long* block);

arguments:

`String`	**address**
`long`	**block**

getCode

Returns code at a given address.

public `String` getCode(*String* address, *long* block);

arguments:

`String`	**address**
`long`	**block**

getStorageAt

Returns the value from a storage position at a given address.

public `String` getStorageAt(*String* address, *BigInteger* position, *long* block);

arguments:

`String`	**address**
`BigInteger`	**position**
`long`	**block**

getBlockTransactionCountByHash

Returns the number of transactions in a block from a block matching the given block hash.

public `long` getBlockTransactionCountByHash(*String* blockHash);

arguments:

`String`	**blockHash**

getBlockTransactionCountByNumber

Returns the number of transactions in a block from a block matching the given block number.

public `long` getBlockTransactionCountByNumber(*long* block);

arguments:

`long`	**block**

getFilterChangesFromLogs

Polling method for a filter, which returns an array of logs which occurred since last poll.

public *Log[]* getFilterChangesFromLogs(*long* id);

arguments:

`long`	**id**

getFilterChangesFromBlocks

Polling method for a filter, which returns an array of logs which occurred since last poll.

public `String[]` getFilterChangesFromBlocks(*`long`* id);

arguments:

`long`	**id**

getFilterLogs

Polling method for a filter, which returns an array of logs which occurred since last poll.

public *`Log[]`* getFilterLogs(*`long`* id);

arguments:

`long`	**id**

getLogs

Polling method for a filter, which returns an array of logs which occurred since last poll.

public *`Log[]`* getLogs(*`LogFilter`* filter);

arguments:

LogFilter	**filter**

getTransactionByBlockHashAndIndex

Returns information about a transaction by block hash and transaction index position.

public *`Transaction`* getTransactionByBlockHashAndIndex(*`String`* blockHash, *`int`* index);

arguments:

`String`	**blockHash**
`int`	**index**

getTransactionByBlockNumberAndIndex

Returns information about a transaction by block number and transaction index position.

public *`Transaction`* getTransactionByBlockNumberAndIndex(*`long`* block, *`int`* index);

arguments:

`long`	**block**
`int`	**index**

getTransactionByHash

Returns the information about a transaction requested by transaction hash.

public *Transaction* getTransactionByHash(*String* transactionHash);

arguments:

`String`	**transactionHash**

getTransactionCount

Returns the number of transactions sent from an address.

public `BigInteger` getTransactionCount(*String* address, *long* block);

arguments:

`String`	**address**
`long`	**block**

getTransactionReceipt

Returns the number of transactions sent from an address.

public *TransactionReceipt* getTransactionReceipt(*String* transactionHash);

arguments:

`String`	**transactionHash**

getUncleByBlockNumberAndIndex

Returns information about a uncle of a block number and uncle index position.

Note: An uncle doesn't contain individual transactions.

public *Block* getUncleByBlockNumberAndIndex(*long* block, *int* pos);

arguments:

`long`	**block**
`int`	**pos**

getUncleCountByBlockHash

Returns the number of uncles in a block from a block matching the given block hash.

public `long` getUncleCountByBlockHash(*String* block);

arguments:

`String`	**block**

getUncleCountByBlockNumber

Returns the number of uncles in a block from a block matching the given block hash.

public `long` getUncleCountByBlockNumber(*`long`* block);

arguments:

`long`	**block**

newBlockFilter

Creates a filter in the node, to notify when a new block arrives.

To check if the state has changed, call eth_getFilterChanges.

public `long` newBlockFilter();

newLogFilter

Creates a filter object, based on filter options, to notify when the state changes (logs).

To check if the state has changed, call eth_getFilterChanges.

A note on specifying topic filters: Topics are order-dependent. A transaction with a log with topics [A, B] will be matched by the following topic filters:

[] "anything" [A] "A in first position (and anything after)" [null, B] "anything in first position AND B in second position (and anything after)" [A, B] "A in first position AND B in second position (and anything after)" [[A, B], [A, B]] "(A OR B) in first position AND (A OR B) in second position (and anything after)"

public `long` newLogFilter(*`LogFilter`* filter);

arguments:

LogFilter	**filter**

uninstallFilter

uninstall filter.

public `boolean` uninstallFilter(*`long`* filter);

arguments:

`long`	**filter**

sendRawTransaction

Creates new message call transaction or a contract creation for signed transactions.

public `String` sendRawTransaction(*`String`* data);

arguments:

`String`	**data**

returns: `String` : transactionHash

sendTransaction

sends a Transaction as desribed by the TransactionRequest.

This will require a signer to be set in order to sign the transaction.

public `String` sendTransaction(*`TransactionRequest`* tx);

arguments:

TransactionRequest	**tx**

call

the current Gas Price.

public `Object` call(*`String`* to, *`String`* function, *`Object...`* params);

arguments:

`String`	**to**
`String`	**function**
`Object...`	**params**

returns: `Object` : the decoded result. if only one return value is expected the Object will be returned, if not an array of objects will be the result.

11.4.2 class Block

represents a Block in ethereum.

LATEST

The latest Block Number.

Type: static `long`

EARLIEST

The Genesis Block.

Type: static `long`

getTotalDifficulty

returns the total Difficulty as a sum of all difficulties starting from genesis.

public `BigInteger` getTotalDifficulty();

getGasLimit

the gas limit of the block.

public `BigInteger` getGasLimit();

getExtraData

the extra data of the block.

public `String` getExtraData();

getDifficulty

the difficulty of the block.

public `BigInteger` getDifficulty();

getAuthor

the author or miner of the block.

public `String` getAuthor();

getTransactionsRoot

the roothash of the merkletree containing all transaction of the block.

public `String` getTransactionsRoot();

getTransactionReceiptsRoot

the roothash of the merkletree containing all transaction receipts of the block.

public `String` getTransactionReceiptsRoot();

getStateRoot

the roothash of the merkletree containing the complete state.

public `String` getStateRoot();

getTransactionHashes

the transaction hashes of the transactions in the block.

public `String[]` getTransactionHashes();

getTransactions

the transactions of the block.

public `Transaction[]` getTransactions();

getTimeStamp

the unix timestamp in seconds since 1970.

public `long` getTimeStamp();

getSha3Uncles

the roothash of the merkletree containing all uncles of the block.

public `String` getSha3Uncles();

getSize

the size of the block.

public `long` getSize();

getSealFields

the seal fields used for proof of authority.

public `String[]` getSealFields();

getHash

the block hash of the of the header.

public `String` getHash();

getLogsBloom

the bloom filter of the block.

public `String` getLogsBloom();

getMixHash

the mix hash of the block.

(only valid of proof of work)

public `String` getMixHash();

getNonce

the mix hash of the block.

(only valid of proof of work)

public `String` getNonce();

getNumber

the block number

public `long` getNumber();

getParentHash

the hash of the parent-block.

public `String` getParentHash();

getUncles

returns the blockhashes of all uncles-blocks.

public `String[]` getUncles();

hashCode

public `int` hashCode();

equals

public `boolean` equals(*`Object`* obj);

arguments:

`Object`	**obj**

11.4.3 class Log

a log entry of a transaction receipt.

isRemoved

true when the log was removed, due to a chain reorganization.

false if its a valid log.

public `boolean` isRemoved();

getLogIndex

integer of the log index position in the block.

null when its pending log.

public `int` getLogIndex();

gettTansactionIndex

integer of the transactions index position log was created from.

null when its pending log.

public `int` gettTansactionIndex();

getTransactionHash

Hash, 32 Bytes - hash of the transactions this log was created from.

null when its pending log.

public `String` getTransactionHash();

getBlockHash

Hash, 32 Bytes - hash of the block where this log was in.

null when its pending. null when its pending log.

public `String` getBlockHash();

getBlockNumber

the block number where this log was in.

null when its pending. null when its pending log.

public `long` getBlockNumber();

getAddress

20 Bytes - address from which this log originated.

public `String` getAddress();

getTopics

Array of 0 to 4 32 Bytes DATA of indexed log arguments.

(In solidity: The first topic is the hash of the signature of the event (e.g. Deposit(address,bytes32,uint256)), except you declared the event with the anonymous specifier.)

public `String[]` getTopics();

11.4.4 class LogFilter

Log configuration for search logs.

getFromBlock

public `long` getFromBlock();

setFromBlock

public `void` setFromBlock(*`long`* fromBlock);

arguments:

`long`	**fromBlock**

getToBlock

public `long` getToBlock();

setToBlock

public `void` setToBlock(*`long`* toBlock);

arguments:

`long`	**toBlock**

getAddress

public `String` getAddress();

setAddress

public `void` setAddress(*`String`* address);

arguments:

`String`	**address**

getTopics

public `Object[]` getTopics();

setTopics

public `void` setTopics(*Object[]* topics);

arguments:

`Object[]`	**topics**

getLimit

public `int` getLimit();

setLimit

public `void` setLimit(*int* limit);

arguments:

`int`	**limit**

toString

creates a JSON-String.

public `String` toString();

11.4.5 class SimpleWallet

a simple Implementation for holding private keys to sing data or transactions.

addRawKey

adds a key to the wallet and returns its public address.

public `String` addRawKey(*String* data);

arguments:

`String`	**data**

addKeyStore

adds a key to the wallet and returns its public address.

public `String` addKeyStore(*String* jsonData, *String* passphrase);

arguments:

`String`	**jsonData**
`String`	**passphrase**

prepareTransaction

optiional method which allows to change the transaction-data before sending it.

This can be used for redirecting it through a multisig.

public *TransactionRequest* prepareTransaction(*IN3* in3, *TransactionRequest* tx);

arguments:

IN3	**in3**
TransactionRequest	**tx**

hasAccount

returns true if the account is supported (or unlocked)

public `boolean` hasAccount(*String* address);

arguments:

`String`	**address**

sign

signing of the raw data.

public `String` sign(*String* data, *String* address);

arguments:

`String`	**data**
`String`	**address**

11.4.6 class Transaction

represents a Transaction in ethereum.

getBlockHash

the blockhash of the block containing this transaction.

public `String` getBlockHash();

getBlockNumber

the block number of the block containing this transaction.

public `long` getBlockNumber();

getChainId

the chainId of this transaction.

public `String` getChainId();

getCreatedContractAddress

the address of the deployed contract (if successfull)

public `String` getCreatedContractAddress();

getFrom

the address of the sender.

public `String` getFrom();

getHash

the Transaction hash.

public `String` getHash();

getData

the Transaction data or input data.

public `String` getData();

getNonce

the nonce used in the transaction.

public `long` getNonce();

getPublicKey

the public key of the sender.

public `String` getPublicKey();

getValue

the value send in wei.

public `BigInteger` getValue();

getRaw

the raw transaction as rlp encoded data.

public `String` getRaw();

getTo

the address of the receipient or contract.

public `String` getTo();

getSignature

the signature of the sender - a array of the [r, s, v]

public `String[]` getSignature();

getGasPrice

the gas price provided by the sender.

public `long` getGasPrice();

getGas

the gas provided by the sender.

public `long` getGas();

11.4.7 class TransactionReceipt

represents a Transaction receipt in ethereum.

getBlockHash

the blockhash of the block containing this transaction.

public `String` getBlockHash();

getBlockNumber

the block number of the block containing this transaction.

public `long` getBlockNumber();

getCreatedContractAddress

the address of the deployed contract (if successfull)

public `String` getCreatedContractAddress();

getFrom

the address of the sender.

public `String` getFrom();

getTransactionHash

the Transaction hash.

public `String` getTransactionHash();

getTransactionIndex

the Transaction index.

public `int` getTransactionIndex();

getTo

20 Bytes - The address of the receiver.

null when it's a contract creation transaction.

public `String` getTo();

getGasUsed

The amount of gas used by this specific transaction alone.

public `long` getGasUsed();

getLogs

Array of log objects, which this transaction generated.

public `Log[]` getLogs();

getLogsBloom

256 Bytes - A bloom filter of logs/events generated by contracts during transaction execution.

Used to efficiently rule out transactions without expected logs

public `String` getLogsBloom();

getRoot

32 Bytes - Merkle root of the state trie after the transaction has been executed (optional after Byzantium hard fork EIP609).

public `String` getRoot();

getStatus

success of a Transaction.

true indicates transaction failure , false indicates transaction success. Set for blocks mined after Byzantium hard fork EIP609, null before.

public `boolean` getStatus();

11.4.8 class TransactionRequest

represents a Transaction Request which should be send or called.

getFrom

public `String` getFrom();

setFrom

public `void` setFrom(*`String`* from);

arguments:

`String`	**from**

getTo

public `String` getTo();

setTo

public `void` setTo(*`String`* to);

arguments:

`String`	**to**

getValue

public `BigInteger` getValue();

setValue

public `void` setValue(*`BigInteger`* value);

arguments:

`BigInteger`	**value**

getNonce

public `long` getNonce();

setNonce

public `void` setNonce(*`long`* nonce);

arguments:

`long`	**nonce**

getGas

public `long` getGas();

setGas

public `void` setGas(*`long`* gas);

arguments:

`long`	**gas**

getGasPrice

public `long` getGasPrice();

setGasPrice

public `void` setGasPrice(*`long`* gasPrice);

arguments:

`long`	**gasPrice**

getFunction

public `String` getFunction();

setFunction

public `void` setFunction(*`String`* function);

arguments:

`String`	**function**

getParams

public `Object[]` getParams();

setParams

public void setParams(*Object[]* params);

arguments:

Object[]	**params**

setData

public void setData(*String* data);

arguments:

String	**data**

getData

creates the data based on the function/params values.

public String getData();

getTransactionJson

public String getTransactionJson();

getResult

public Object getResult(*String* data);

arguments:

String	**data**

CHAPTER 12

API Reference CMD

Incubed can be used as a command-line utility or as a tool in Bash scripts. This tool will execute a JSON-RPC request and write the result to standard output.

12.1 Usage

```
in3 [options] method [arguments]
```

-c, -chain The chain to use currently:

- **mainnet** Mainnet
- **kovan** Kovan testnet
- **tobalaba** EWF testchain
- **goerli** Goerli testchain using Clique
- **btc** Bitcoin (still experimental)
- **local** Use the local client on http://localhost:8545
- **RPCURL** If any other RPC-URL is passed as chain name, this is used but without verification

-p, -proof Specifies the verification level:

- **none** No proof
- **standard** Standard verification (default)
- **full** Full verification

-np Short for `-p none`.

-s, -signs Number of signatures to use when verifying.

-b, -block The block number to use when making calls. Could be either `latest` (default), `earliest`, or a hex number.

-l, -latest replaces `latest` with latest BlockNumber - the number of blocks given.

-pk The path to the private key as keystore file.

-pwd Password to unlock the key. (Warning: since the passphrase must be kept private, make sure that this key may not appear in the bash_history)

-to The target address of the call.

-st, -sigtype the type of the signature data : `eth_sign` (use the prefix and hash it), `raw` (hash the raw data), `hash` (use the already hashed data). Default: raw

-port specifies the port to run incubed as a server. Opening port 8545 may replace a local parity or geth client.

-d, -data The data for a transaction.

This can be a file path, a 0x-hexvalue, or `-` to read it from standard input. If a method signature is given with the data, they will be combined and used as constructor arguments when deploying.

-gas The gas limit to use when sending transactions (default: 100000).

-value The value to send when conducting a transaction. Can be a hex value or a float/integer with the suffix `eth` or `wei` like `1.8eth` (default: 0).

-w, -wait If given, `eth_sendTransaction` or `eth_sendRawTransaction` will not only return the transaction hash after sending but also wait until the transaction is mined and returned to the transaction receipt.

-json If given, the result will be returned as JSON, which is especially important for `eth_call`, which results in complex structres.

-hex If given, the result will be returned as hex.

-debug If given, Incubed will output debug information when executing.

-q quiet. no warnings or log to stderr.

-ri Reads the response from standard input instead of sending the request, allowing for offline use cases.

-ro Writes the raw response from the node to standard output.

12.2 Install

12.2.1 From Binaries

You can download the from the latest release-page:

https://github.com/slockit/in3-c/releases

These release files contain the sources, precompiled libraries and executables, headerfiles and documentation.

12.2.2 From Package Managers

We currently support

Ubuntu Launchpad (Linux)

Installs libs and binaries on IoT devices or Linux-Systems

```
# Add the slock.it ppa to your system
sudo add-apt-repository ppa:devops-slock-it/in3

# install the commandline tool in3
apt-get install in3

# install shared and static libs and header files
apt-get install in3-dev
```

Brew (MacOS)

This is the easiest way to install it on your mac using brew

```
# Add a brew tap
brew tap slockit/in3

# install all binaries and libraries
brew install in3
```

12.2.3 From Sources

Before building, make sure you have these components installed:

- CMake (should be installed as part of the build-essential: `apt-get install build-essential`)
- libcurl (for Ubuntu, use either `sudo apt-get install libcurl4-gnutls-dev` or `apt-get install libcurl4-openssl-dev`)
- If libcurl cannot be found, Conan is used to fetch and build curl

```
# clone the sources
git clone https://github.com/slockit/in3-c.git

# create build-folder
cd in3-c
mkdir build && cd build

# configure and build
cmake -DCMAKE_BUILD_TYPE=Release .. && make in3

# install
sudo make install
```

When building from source, CMake accepts the flags which help to optimize. For more details just look at the CMake-Options .

12.2.4 From Docker

Incubed can be run as docker container. For this pull the container:

```
# run a simple statement
docker run slockit/in3:latest eth_blockNumber

# to start it as a server
docker run -p 8545:8545 slockit/in3:latest -port 8545

# mount the cache in order to cache nodelists, validatorlists and contract code.
docker run -v $(pwd)/cache:/root/.in3 -p 8545:8545 slockit/in3:latest -port 8545
```

12.3 Environment Variables

The following environment variables may be used to define defaults:

IN3_PK The raw private key used for signing. This should be used with caution, since all subprocesses have access to it!

IN3_CHAIN The chain to use (default: mainnet) (same as -c). If a URL is passed, this server will be used instead.

12.4 Methods

As methods, the following can be used:

<JSON-RPC>-method All officially supported JSON-RPC methods may be used.

send <signature> ...args Based on the `-to`, `-value`, and `-pk`, a transaction is built, signed, and sent. If there is another argument after *send*, this would be taken as a function signature of the smart contract followed by optional arguments of the function.

```
# Send some ETH (requires setting the IN3_PK-variable before).
in3 send -to 0x1234556 -value 0.5eth
# Send a text to a function.
in3 -to 0x5a0b54d5dc17e0aadc383d2db43b0a0d3e029c4c  -gas 1000000 send
↪"registerServer(string,uint256)" "https://in3.slock.it/kovan1" 0xFF
```

sign <data> signs the data and returns the signature (65byte as hex). Use the -sigtype to specify the creation of the hash.

call <signature> ...args `eth_call` to call a function. After the `call` argument, the function signature and its arguments must follow.

in3_nodeList Returns the NodeList of the Incubed NodeRegistry as JSON.

in3_sign <blocknumber> Requests a node to sign. To specify the signer, you need to pass the URL like this:

```
# Send a text to a function.
in3 in3_sign -c https://in3.slock.it/mainnet/nd-1 6000000
```

in3_stats Returns the stats of a node. Unless you specify the node with `-c <rpcurl>`, it will pick a random node.

abi_encode <signature> ...args Encodes the arguments as described in the method signature using ABI encoding.

abi_decode <signature> data Decodes the data based on the signature.

pk2address <privatekey> Extracts the public address from a private key.

pk2public <privatekey> Extracts the public key from a private key.

ecrecover <msg> <signature> Extracts the address and public key from a signature.

createkey Generates a random raw private key.

key <keyfile> Reads the private key from JSON keystore file from the first argument and returns the private key. This may ask the user to enter the passphrase (unless provided with -pwd). To unlock the key to reuse it within the shell, you can set the environment variable like this:

```
export IN3_PK=`in3 keystore mykeyfile.json`
```

if no method is passed, this tool will read json-rpc-requests from stdin and response on stdout until stdin is closed.

```
echo '{"method":"eth_blockNumber","params":[]}' | in3 -q -c goerli
```

This can also be used process to communicate with by startiing a in3-process and send rpc-comands through stdin and read the responses from stout. if multiple requests are passed in the input stream, they will executed in the same order. The result will be terminated by a newline-character.

12.5 Running as Server

While you can use in3 to execute a request, return a result and quit, you can also start it as a server using the specified port (-port 8545) to serve RPC-requests. Thiss way you can replace your local parity or geth with a incubed client. All Dapps can then connect to http://localhost:8545.

```
# starts a server at the standard port for kovan.
in3 -c kovan -port 8545
```

12.6 Cache

Even though Incubed does not need a configuration or setup and runs completely statelessly, caching already verified data can boost the performance. That's why in3 uses a cache to store.

NodeLists List of all nodes as verified from the registry.

Reputations Holding the score for each node to improve weights for honest nodes.

Code For eth_call, Incubed needs the code of the contract, but this can be taken from a cache if possible.

Validators For PoA changes, the validators and their changes over time will be stored.

By default, Incubed will use ~/.in3 as a folder to cache data.

If you run the docker container, you need to mount /root/.in3 in to persist the cache.

12.7 Signing

While Incubed itself uses an abstract definition for signing, at the moment, the command-line utility only supports raw private keys. There are two ways you can specify the private keys that Incubed should use to sign transactions:

1. Use the environment variable IN3_PK. This makes it easier to run multiple transaction.

> **Warning:** Since the key is stored in an envirmoent variable all subpoccess have access to this. That's why this method is potentially unsafe.

```
#!/bin/sh

# reads the key from the keyfile and asks the user for the passphrase.
IN3_PK = `in3 key my_keyfile.json`

# you can can now use this private keys since it is stored in a enviroment-
↪variable
in3 -to 0x27a37a1210df14f7e058393d026e2fb53b7cf8c1 -value 3.5eth -wait send
in3 -to 0x5a0b54d5dc17e0aadc383d2db43b0a0d3e029c4c  -gas 1000000 send
↪"registerServer(string,uint256)" "https://in3.slock.it/kovan1" 0xFF
```

2. Use the -pk option

   This option takes the path to the keystore-file and will ask the user to unlock as needed. It will not store the unlocked key anywhere.

```
in3 -pk my_keyfile.json -to 0x27a37a1210df14f7e058393d026e2fb53b7cf8c1 -value␣
↪200eth -wait send
```

12.8 Autocompletion

If you want autocompletion, simply add these lines to your *.bashrc* or *.bash_profile*:

```
_IN3_WORDS=`in3 autocompletelist`
complete -W "$_IN3_WORDS" in3
```

12.9 Function Signatures

When using send or call, the next optional parameter is the function signature. This signature describes not only the name of the function to call but also the types of arguments and return values.

In general, the signature is built by simply removing all names and only holding onto the types:

```
<FUNCTION_NAME>(<ARGUMENT_TYPES>):(<RETURN_TYPES>)
```

It is important to mention that the type names must always be the full Solidity names. Most Solidity functions use aliases. They would need to be replaced with the full type name.

e.g., uint -> uint256

12.10 Examples

12.10.1 Getting the Current Block

```
# On a command line:
in3 eth_blockNumber
> 8035324

# For a different chain:
in3 -c kovan eth_blockNumber
```

(continues on next page)

(continued from previous page)

```
> 11834906

# Getting it as hex:
in3 -c kovan -hex eth_blockNumber
> 0xb49625

# As part of shell script:
BLOCK_NUMBER=`in3 eth_blockNumber`
```

12.10.2 Using jq to Filter JSON

```
# Get the timestamp of the latest block:
in3 eth_getBlockByNumber latest false | jq -r .timestamp
> 0x5d162a47

# Get the first transaction of the last block:
in3 eth_getBlockByNumber latest true | jq  '.transactions[0]'
> {
   "blockHash": "0xe4edd75bf43cd8e334ca756c4df1605d8056974e2575f5ea835038c6d724ab14",
   "blockNumber": "0x7ac96d",
   "chainId": "0x1",
   "condition": null,
   "creates": null,
   "from": "0x91fdebe2e1b68da999cb7d634fe693359659d967",
   "gas": "0x5208",
   "gasPrice": "0xba43b7400",
   "hash": "0x4b0fe62b30780d089a3318f0e5e71f2b905d62111a4effe48992fcfda36b197f",
   "input": "0x",
   "nonce": "0x8b7",
   "publicKey":
↪"0x17f6413717c12dab2f0d4f4a033b77b4252204bfe4ae229a608ed724292d7172a19758e84110a2a926842457c351f803
↪",
   "r": "0x1d04ee9e31727824a19a4fcd0c29c0ba5dd74a2f25c701bd5fdabbf5542c014c",
   "raw":
↪"0xf86e8208b7850ba43b7400825208947fb38d6a092bbdd476e80f00800b03c3f1b2d332883aefa89df48ed4008026a01c
↪",
   "s": "0x43f8df6c171e51bf05036c8fe8d978e182316785d0aace8ecc56d2add157a635",
   "standardV": "0x1",
   "to": "0x7fb38d6a092bbdd476e80f00800b03c3f1b2d332",
   "transactionIndex": "0x0",
   "v": "0x26",
   "value": "0x3aefa89df48ed400"
  }
```

12.10.3 Calling a Function of a Smart Contract

```
# Without arguments:
in3 -to 0x2736D225f85740f42D17987100dc8d58e9e16252 call "totalServers():uint256"
> 5

# With arguments returning an array of values:
in3 -to 0x2736D225f85740f42D17987100dc8d58e9e16252 call "servers(uint256):(string,
↪address,uint256,uint256,uint256,address)" 1
```

(continues on next page)

(continued from previous page)

```
> https://in3.slock.it/mainnet/nd-1
> 0x784bfa9eb182c3a02dbeb5285e3dba92d717e07a
> 65535
> 65535
> 0
> 0x0000000000000000000000000000000000000000

# With arguments returning an array of values as JSON:
 in3 -to 0x2736D225f85740f42D17987100dc8d58e9e16252 -json call
↪"servers(uint256):(string,address,uint256,uint256,uint256,address)" 1
 > ["https://in3.slock.it/mainnet/nd-4","0xbc0ea09c1651a3d5d40bacb4356fb59159a99564",
↪"0xffff","0xffff","0x00","0x0000000000000000000000000000000000000000"]
```

12.10.4 Sending a Transaction

```
# Sends a transaction to a register server function and signs it with the private key␣
↪given :
in3 -pk mykeyfile.json -to 0x27a37a1210df14f7e058393d026e2fb53b7cf8c1  -gas 1000000 ␣
↪send "registerServer(string,uint256)" "https://in3.slock.it/kovan1" 0xFF
```

12.10.5 Deploying a Contract

```
# Compiling the Solidity code, filtering the binary, and sending it as a transaction␣
↪returning the txhash:
solc --bin ServerRegistry.sol | in3 -gas 5000000 -pk my_private_key.json -d - send

# If you want the address, you would need to wait until the text is mined before␣
↪obtaining the receipt:
solc --bin ServerRegistry.sol | in3 -gas 5000000 -pk my_private_key.json -d - -wait␣
↪send | jq -r .contractAddress
```

CHAPTER 13

API Reference Node/Server

The term in3-server and in3-node are used interchangeably.

Nodes are the backend of Incubed. Each node serves RPC requests to Incubed clients. The node itself runs like a proxy for an Ethereum client (Geth, Parity, etc.), but instead of simply passing the raw response, it will add the required proof needed by the client to verify the response.

To run such a node, you need to have an Ethereum client running where you want to forward the request to. At the moment, the minimum requirement is that this client needs to support `eth_getProof` (see http://eips.ethereum.org/EIPS/eip-1186).

You can create your own docker compose file/docker command using our command line descriptions below. But you can also use our tool in3-server-setup to help you through the process.

13.1 Command-line Arguments

--autoRegistry-capabilities-multiChain If true, this node is able to deliver multiple chains.

--autoRegistry-capabilities-proof If true, this node is able to deliver proofs.

--autoRegistry-capacity Max number of parallel requests.

--autoRegistry-deposit The deposit you want to store.

--autoRegistry-depositUnit Unit of the deposit value.

--autoRegistry-url The public URL to reach this node.

--cache Cache Merkle tries.

--chain ChainId.

--clientKeys A comma-separated list of client keys to use for simulating clients for the watchdog.

--db-database Name of the database.

--db-host Db-host (default: local host).

--db-password Password for db-access.

--db-user Username for the db.

--defaultChain The default chainId in case the request does not contain one.

--freeScore The score for requests without a valid signature.

--handler The implementation used to handle the calls.

--help Output usage information.

--id An identifier used in log files for reading the configuration from the database.

--ipfsUrl The URL of the IPFS client.

--logging-colors If true, colors will be used.

--logging-file The path to the log file.

--logging-host The host for custom logging.

--logging-level Log level.

--logging-name The name of the provider.

--logging-type The module of the provider.

--maxThreads The maximal number of threads running parallel to the processes.

--maxPointsPerMinute The Score for one client able to use within one minute, which is used as DOS-Protection.

--maxBlocksSigned The max number of blocks signed per in3_sign-request

--maxSignatures The max number of signatures to sign per request

--minBlockHeight The minimal block height needed to sign.

--persistentFile The file name of the file keeping track of the last handled blockNumber.

--privateKey The path to the keystore-file for the signer key used to sign blockhashes.

--privateKeyPassphrase The password used to decrypt the private key.

--profile-comment Comments for the node.

--profile-icon URL to an icon or logo of a company offering this node.

--profile-name Name of the node or company.

--profile-noStats If active, the stats will not be shown (default: false).

--profile-url URL of the website of the company.

--profile-prometheus URL of the prometheus gateway to report stats

--registry The address of the server registry used to update the NodeList.

--registryRPC The URL of the client in case the registry is not on the same chain.

--rpcUrl The URL of the client.

--startBlock BlockNumber to start watching the registry.

--timeout Number of milliseconds needed to wait before a request times out.

--version Output of the version number.

--watchInterval The number of seconds before a new event.

--watchdogInterval Average time between sending requests to the same node. 0 turns it off (default).

13.2 in3-server-setup tool

The in3-server-setup tool can be found both [online](https://in3-setup.slock.it) and on [DockerHub](https://hub.docker.com/r/slockit/in3-server-setup). The DockerHub version can be used to avoid relying on our online service, a full source will be released soon.

The tool can be used to generate the private key as well as the docker-compose file for use on the server.

Note: The below guide is a basic example of how to setup and in3 node, no assurances are made as to the security of the setup. Please take measures to protect your private key and server.

Setting up a server on AWS:

1. Create an account on AWS and create a new EC2 instance
2. Save the key and SSH into the machine with `` `ssh -i "SSH_KEY.pem" user@IP` ``
3. Install docker and docker-compose on the EC2 instance `` `apt-get install docker docker-compose` ``
4. Use scp to transfer the docker-compose file and private key, `` `scp -i "SSH_KEY" FILE user@IP:.` ``
5. Run the Ethereum client, for example parity and allow it to sync
6. Once the client is synced, run the docker-compose file with `` `docker-compose up` ``
7. **Test the in3 node by making a request to the address**

```
curl -X POST -H 'Content-Type:application/json' \
--data '{"id":1,"jsonrpc":"2.0","method":"in3_nodeList", \
"params":[],"in3":{"version": "0x2","chainId":"0x1","verification":"proof
↪"}}' \
    <MY_NODE_URL>
```

8. Consider using tools such as AWS Shield to protect your server from DOS attacks

13.3 Registering Your Own Incubed Node

If you want to participate in this network and register a node, you need to send a transaction to the registry contract, calling *registerServer(string _url, uint _props)*.

To run an Incubed node, you simply use docker-compose:

First run partiy, and allow the client to sync:

```
version: '2'
services:
incubed-parity:
    image: parity:latest                                    # Parity image with␣
↪the proof function implemented.
    command:
    - --auto-update=none                                    # Do not␣
↪automatically update the client.
    - --pruning=archive
```

(continues on next page)

(continued from previous page)

```
    - --pruning-memory=30000                                        # Limit storage.
    - --jsonrpc-experimental                                        # Currently still␣
↪needed until EIP 1186 is finalized.
```

Then run in3 with the below docker-compose file:

```
version: '2'
      services:
      incubed-server:
          image: slockit/in3-server:latest
          volumes:
          - $PWD/keys:/secure                                             # Directory␣
↪where the private key is stored.
          ports:
          - 8500:8500/tcp                                                 # Open the port␣
↪8500 to be accessed by the public.
          command:
          - --privateKey=/secure/myKey.json                               # Internal path␣
↪to the key.
          - --privateKeyPassphrase=dummy                                  # Passphrase to␣
↪unlock the key.
          - --chain=0x1                                                   # Chain (Kovan).
          - --rpcUrl=http://incubed-parity:8545                           # URL of the␣
↪Kovan client.
          - --registry=0xFdb0eA8AB08212A1fFfDB35aFacf37C3857083ca # URL of the␣
↪Incubed registry.
          - --autoRegistry-url=http://in3.server:8500                     # Check or␣
↪register this node for this URL.
          - --autoRegistry-deposit=2                                      # Deposit to␣
↪use when registering.
```

CHAPTER 14

API Reference Solidity

This page contains a list of function for the registry contracts.

14.1 NodeRegistryData functions

14.1.1 adminRemoveNodeFromRegistry

Removes an in3-node from the nodeList

Development notice:

- only callable by the NodeRegistryLogic-contract

Parameters:

- _signer `address`: the signer

14.1.2 adminSetLogic

Sets the new Logic-contract as owner of the contract.

Development notice:

- only callable by the current Logic-contract / owner
- the `0x00`-address as owner is not supported

Return Parameters:

- true when successful

14.1.3 adminSetNodeDeposit

Sets the deposit of an existing in3-node

Development notice:

- only callable by the NodeRegistryLogic-contract
- used to remove the deposit of a node after he had been convicted

Parameters:

- _signer `address`: the signer of the in3-node
- _newDeposit `uint`: the new deposit

Return Parameters:

- true when successful

14.1.4 adminSetStage

Sets the stage of a signer

Development notice:

- only callable by the current Logic-contract / owner

Parameters:

- _signer `address`: the signer of the in3-node
- *stage* `uint`: the new stage

Return Parameters:

- true when successful

14.1.5 adminSetSupportedToken

Sets a new erc20-token as supported token for the in3-nodes.

Development notice:

- only callable by the NodeRegistryLogic-contract

Parameters:

- _newToken `address`: the address of the new supported token

Return Parameters:

- true when successful

14.1.6 adminSetTimeout

Sets the new timeout until the deposit of a node can be accessed after he was unregistered.

Development notice:

- only callable by the NodeRegistryLogic-contract

Parameters:

- _newTimeout `uint`: the new timeout

Return Parameters:

- true when successful

14.1.7 adminTransferDeposit

Transfers a certain amount of ERC20-tokens to the provided address

Development notice:

- only callable by the NodeRegistryLogic-contract
- reverts when the transfer failed

Parameters:

- _to `address`: the address to receive the tokens
- _amount: `uint`: the amount of tokens to be transferred

Return Parameters:

- true when successful

14.1.8 setConvict

Writes a value to te convictMapping to be used later for revealConvict in the logic contract.

Development notice:

- only callable by the NodeRegistryLogic-contract

Parameters:

- _hash `bytes32`: the data to be written
- _caller `address`: the address for that called convict in the logic-contract

Development notice:

- only callable by the NodeRegistryLogic-contract

14.1.9 registerNodeFor

Registers a new node in the nodeList

Development notice:

- only callable by the NodeRegistryLogic-contract

Parameters:

- _url `string`: the url of the in3-node
- _props `uint192`: the properties of the in3-node
- _signer `address`: the signer address
- _weight `uit64`: the weight
- _owner `address`: the address of the owner

- _deposit `uint`: the deposit in erc20 tokens
- _stage `uint`: the stage the in3-node should have

Return Parameters:

- true when successful

14.1.10 transferOwnership

Transfers the ownership of an active in3-node

Development notice:

- only callable by the NodeRegistryLogic-contract

Parameters:

- _signer `address`: the signer of the in3-node
- _newOwner `address`: the address of the new owner

Return Parameters:

- true when successful

14.1.11 unregisteringNode

Removes a node from the nodeList

Development notice:

- only callable by the NodeRegistryLogic-contract
- calls `_unregisterNodeInternal()`

Parameters:

- _signer `address`: the signer of the in3-node

Return Parameters:

- true when successful

14.1.12 updateNode

Updates an existing in3-node

Development notice:

- only callable by the NodeRegistryLogic-contract
- reverts when the an updated url already exists

Parameters:

- _signer `address`: the signer of the in3-node
- _url `string`: the new url
- _props `uint192` the new properties
- _weight `uint64` the new weight

- _deposit `uint` the new deposit

Return Parameters:

- true when successful

14.1.13 getIn3NodeInformation

Returns the In3Node-struct of a certain index

Parameters:

- index `uint`: the index-position in the nodes-array

Return Parameters:

- the In3Node-struct

14.1.14 getSignerInformation

Returns the SignerInformation of a signer

Parameters:

- _signer `address`: the signer

Return Parameters: the SignerInformation of a signer

14.1.15 totalNodes

Returns the length of the nodeList

Return Parameters: The length of the nodeList

14.1.16 adminSetSignerInfo

Sets the SignerInformation-struct for a signer

Development notice:

- only callable by the NodeRegistryLogic-contract
- gets used for updating the information after returning the deposit

Parameters:

- _signer `address`: the signer
- _si: `SignerInformation` the struct to be set

Return Parameters:

- true when successful

14.2 NodeRegistryLogic functions

14.2.1 activateNewLogic

Applies a new update to the logic-contract by setting the pending NodeRegistryLogic-contract as owner to the NodeRegistryData-conract

Development notice:

- Only callable after 47 days have passed since the latest update has been proposed

14.2.2 adminRemoveNodeFromRegistry

Removes an malicious in3-node from the nodeList

Development notice:

- only callable by the admin of the smart contract
- only callable in the 1st year after deployment
- ony usable on registered in3-nodes

Parameters:

- _signer `address`: the malicious signer

14.2.3 adminUpdateLogic

Proposes an update to the logic contract which can only be applied after 47 days. This will allow all nodes that don't approve the update to unregister from the registry

Development notice:

- only callable by the admin of the smart contract
- does not allow for the 0x0-address to be set as new logic

Parameters:

- _newLogic `address`: the malicious signer

14.2.4 convict

Must be called before revealConvict and commits a blocknumber and a hash.

Development notice:

- The `v`,`r`,`s` parameters are from the signature of the wrong blockhash that the node provided

Parameters:

- _hash `bytes32`: `keccak256(wrong blockhash, msg.sender, v, r, s)`; used to prevent frontrunning.

14.2.5 registerNode

Registers a new node with the sender as owner

Development notice:

- will call the registerNodeInteral function
- the amount of `_deposit` token have be approved by the signer in order for them to be transferred by the logic contract

Parameters:

- _url `string`: the url of the node, has to be unique
- _props `uint64`: properties of the node
- _weight `uint64`: how many requests per second the node is able to handle
- _deposit `uint`: amount of supported ERC20 tokens as deposit

14.2.6 registerNodeFor

Registers a new node as a owner using a different signer address*

Development notice:

- will revert when a wrong signature has been provided which is calculated by the hash of the url, properties, weight and the owner in order to prove that the owner has control over the signer-address he has to sign a message
- will call the registerNodeInteral function
- the amount of `_deposit` token have be approved by the in3-node-owner in order for them to be transferred by the logic contract

Parameters:

- _url `string`: the url of the node, has to be unique
- _props `uint64`: properties of the node
- _signer `address`: the signer of the in3-node
- _weight `uint64`: how many requests per second the node is able to handle
- _depositAmount `uint`: the amount of supported ERC20 tokens as deposit
- _v `uint8`: v of the signed message
- _r `bytes32`: r of the signed message
- _s `bytes32`: s of the signed message

14.2.7 returnDeposit

Returns the deposit after a node has been removed and it's timeout is over.

Development notice:

- reverts if the deposit is still locked
- reverts when there is nothing to transfer
- reverts when not the owner of the former in3-node

Parameters:

- _signer `address`: the signer-address of a former in3-node

14.2.8 revealConvict

Reveals the wrongly provided blockhash, so that the node-owner will lose its deposit while the sender will get half of the deposit

Development notice:

- reverts when the wrong convict hash (see convict-function) is used
- reverts when the _signer did not sign the block
- reverts when trying to reveal immediately after calling convict
- reverts when trying to convict someone with a correct blockhash
- reverts if a block with that number cannot be found in either the latest 256 blocks or the blockhash registry

Parameters:

- _signer `address`: the address that signed the wrong blockhash
- _blockhash `bytes32`: the wrongly provided blockhash
- _blockNumber `uint`: number of the wrongly provided blockhash
- _v `uint8`: v of the signature
- _r `bytes32`: r of the signature
- _s `bytes32`: s of the signature

14.2.9 transferOwnership

Changes the ownership of an in3-node.

Development notice:

- reverts when the sender is not the current owner
- reverts when trying to pass ownership to `0x0`
- reverts when trying to change ownership of an inactive node

Parameters:

- _signer `address`: the signer-address of the in3-node, used as an identifier
- _newOwner `address`: the new owner

14.2.10 unregisteringNode

A node owner can unregister a node, removing it from the nodeList. Doing so will also lock his deposit for the timeout of the node.

Development notice:

- reverts when not called by the owner of the node
- reverts when the provided address is not an in3-signer

- reverts when node is not active

Parameters:

- _signer `address`: the signer of the in3-node

14.2.11 updateNode

Updates a node by changing its props

Development notice:

- if there is an additional deposit the owner has to approve the tokenTransfer before
- reverts when trying to change the url to an already existing one
- reverts when the signer does not own a node
- reverts when the sender is not the owner of the node

Parameters:

- _signer `address`: the signer-address of the in3-node, used as an identifier
- _url `string`: the url, will be changed if different from the current one
- _props `uint64`: the new properties, will be changed if different from the current one
- _weight `uint64`: the amount of requests per second the node is able to handle
- _additionalDeposit `uint`: additional deposit in supported erc20 tokens

14.2.12 maxDepositFirstYear

Returns the current maximum amount of deposit allowed for registering or updating a node

Return Parameters:

- `uint` the maximum amount of tokens

14.2.13 minDeposit

Returns the current minimal amount of deposit required for registering a new node

Return Parameters:

- `uint` the minimal amount of tokens needed for registering a new node

14.2.14 supportedToken

Returns the current supported ERC20 token-address

Return Parameters:

- `address` the address of the currently supported erc20 token

14.3 BlockHashRegistry functions

14.3.1 searchForAvailableBlock

Searches for an already existing snapshot

Parameters:

- _startNumber `uint`: the blocknumber to start searching
- _numBlocks `uint`: the number of blocks to search for

Return Parameters:

- `uint` returns a blocknumber when a snapshot had been found. It will return 0 if no blocknumber was found.

14.3.2 recreateBlockheaders

Starts with a given blocknumber and its header and tries to recreate a (reverse) chain of blocks. If this has been successful the last blockhash of the header will be added to the smart. contract. It will be checked whether the provided chain is correct by using the reCalculateBlockheaders function.

Development notice:

- only usable when the given blocknumber is already in the smart contract
- function is public due to the usage of a dynamic bytes array (not yet supported for external functions)
- reverts when the chain of headers is incorrect
- reverts when there is not parent block already stored in the contract

Parameters:

- _blockNumber `uint`: the block number to start recreation from
- _blockheaders `bytes[]`: array with serialized blockheaders in reverse order (youngest -> oldest) => (e.g. 100, 99, 98)

14.3.3 saveBlockNumber

Stores a certain blockhash to the state

Development notice:

- reverts if the block can't be found inside the evm

Parameters:

- _blockNumber `uint`: the blocknumber to be stored

14.3.4 snapshot

Stores the currentBlock-1 in the smart contract

14.3.5 getRlpUint

Returns the value from the rlp encoded data

Development notice: *This function is limited to only value up to 32 bytes length!

Parameters:

- _data `bytes`: the rlp encoded data
- _offset `uint`: the offset

Return Parameters:

- value `uint` the value

14.3.6 getParentAndBlockhash

Returns the blockhash and the parent blockhash from the provided blockheader

Parameters:

- _blockheader `bytes`: a serialized (rlp-encoded) blockheader

Return Parameters:

- parentHash `bytes32`
- bhash `bytes32`

14.3.7 reCalculateBlockheaders

Starts with a given blockhash and its header and tries to recreate a (reverse) chain of blocks. The array of the blockheaders have to be in reverse order (e.g. [100,99,98,97]).

Parameters:

- _blockheaders `bytes[]`: array with serialized blockheaders in reverse order, i.e. from youngest to oldest
- _bHash `bytes32`: blockhash of the 1st element of the _blockheaders-array

CHAPTER 15

Concept

To enable smart devices of the internet of things to be connected to the Ethereum blockchain, an Ethereum client needs to run on this hardware. The same applies to other blockchains, whether based on Ethereum or not. While current notebooks or desktop computers with a broadband Internet connection are able to run a full node without any problems, smaller devices such as tablets and smartphones with less powerful hardware or more restricted Internet connection are capable of running a light node. However, many IoT devices are severely limited in terms of computing capacity, connectivity and often also power supply. Connecting an IoT device to a remote node enables even low-performance devices to be connected to blockchain. By using distinct remote nodes, the advantages of a decentralized network are undermined without being forced to trust single players or there is a risk of malfunction or attack because there is a single point of failure.

With the presented Trustless Incentivized Remote Node Network, in short INCUBED, it will be possible to establish a decentralized and secure network of remote nodes, which enables trustworthy and fast access to blockchain for a large number of low-performance IoT devices.

15.1 Situation

The number of IoT devices is increasing rapidly. This opens up many new possibilities for equipping these devices with payment or sharing functionality. While desktop computers can run an Ethereum full client without any problems, small devices are limited in terms of computing power, available memory, Internet connectivity and bandwidth. The development of Ethereum light clients has significantly contributed to the connection of smaller devices with the blockchain. Devices like smartphones or computers like Raspberry PI or Samsung Artik 5/7/10 are able to run light clients. However, the requirements regarding the mentioned resources and the available power supply are not met by a large number of IoT devices.

One option is to run the client on an external server, which is then used by the device as a remote client. However, central advantages of the blockchain technology - decentralization rather than having to trust individual players - are lost this way. There is also a risk that the service will fail due to the failure of individual nodes.

A possible solution for this may be a decentralized network of remote-nodes (netservice nodes) combined with a protocol to secure access.

15.2 Low-Performance Hardware

There are several classes of IoT devices, for which running a full or light client is somehow problematic and a INNN can be a real benefit or even a job enabler:

- **Devices with insufficient calculation power or memory space**

  Today, the majority of IoT devices do not have processors capable of running a full client or a light client. To run such a client, the computer needs to be able to synchronize the blockchain and calculate the state (or at least the needed part thereof).

- **Devices with insufficient power supply**

  If devices are mobile (for instance a bike lock or an environment sensor) and rely on a battery for power supply, running a full or a light light, which needs to be constantly synchronized, is not possible.

- **Devices which are not permanently connected to the Internet**

  Devices which are not permantently connected to the Internet, also have trouble running a full or a light client as these clients need to be in sync before they can be used.

15.3 Scalability

One of the most important topics discussed regarding blockchain technology is scalability. Of course, a working INCUBED does not solve the scaling problems that more transactions can be executed per second. However, it does contribute to providing access to the Ethereum network for devices that could not be integrated into existing clients (full client, light client) due to their lack of performance or availability of a continuous Internet connection with sufficient bandwidth.

15.4 Use Cases

With the following use cases, some realistic scenarios should be designed in which the use of INCUBED will be at least useful. These use cases are intended as real-life relevant examples only to envision the potential of this technology but are by no means a somehow complete list of possible applications.

15.4.1 Publicly Accessible Environment Sensor

Description

An environment sensor, which measures some air quality characteristics, is installed in the city of Stuttgart. All measuring data is stored locally and can be accessed via the Internet by paying a small fee. Also a hash of the current data set is published to the public Ethereum blockchain to validate the integrity of the data.

The computational power of the control unit is restricted to collecting the measuring data from the sensors and storing these data to the local storage. It is able to encrypt or cryptographically sign messages. As this sensor is one of thousands throughout Europe, the energy consumption must be as low as possible. A special low-performance hardware is installed. An Internet connection is provided, but the available bandwidth is not sufficient to synchrone a blockchain client.

Blockchain Integration

The connection to the blockchain is only needed if someone requests the data and sends the validation hash code to the smart contract.

The installed hardware (available computational power) and the requirement to minimize energy consumption disable the installation and operation of a light client without installing addition hardware (like a Samsung Artik 7) as PBCD (Physical Blockchain Connection Device/Ethereum computer). Also, the available Internet bandwidth would need to be enhanced to be able to synchronize properly with the blockchain.

Using a netservice-client connected to the INCUBED can be realized using the existing hardware and Internet connection. No additional hardware or Internet bandwidth is needed. The netservice-client connects to the INCUBED only to send signed messages, to trigger transactions or to request information from the blockchain.

15.4.2 Smart Bike Lock

Description

A smart bike lock which enables sharing is installed on an e-bike. It is able to connect to the Internet to check if renting is allowed and the current user is authorized to open the lock.

The computational power of the control unit is restricted to the control of the lock. Because the energy is provided by the e-bike's battery, the controller runs only when needed in order to save energy. For this reason, it is also not possible to maintain a permanent Internet connection.

Blockchain Integration

Running a light-client on such a platform would consume far too much energy, but even synchronizing the client only when needed would take too much time and require an Internet connection with the corresponding bandwidth, which is not always the case. With a netservice-client running on the lock, a secure connection to the blockchain can be established at the required times, even if the Internet connection only allows limited bandwidth. In times when there is no rental process in action, neither computing power is needed nor data is transferred.

15.4.3 Smart Home - Smart Thermostat

Description

With smart home devices it is possible to realize new business models, e. g. for the energy supply. With smart thermostats it is possible to bill heating energy pay-per-use. During operation, the thermostat must only be connected to the blockchain if there is a heating requirement and a demand exists. Then the thermostat must check whether the user is authorized and then also perform the transactions for payment.

Blockchain Integration

Similar to the cycle lock application, a thermostat does not need to be permanently connected to the blockchain to keep a client in sync. Furthermore, its hardware is not able to run a full or light client. Here, too, it makes sense to use a netservice-client. Such a client can be developed especially for this hardware.

15.4.4 Smartphone App

Description

The range of smartphone apps that can or should be connected to the blockchain is widely diversified. These can be any apps with payment functions, apps that use blockchain as a notary service, apps that control or lend IoT devices, apps that visualize data from the blockchain, and much more.

Often these apps only need sporadic access to the blockchain. Due to the limited battery power and limited data volume, neither a full client nor a light client is really suitable for such applications, as these clients require a permanent connection to keep the blockchain up-to-date.

Blockchain Integration

In order to minimize energy consumption and the amount of data to be transferred, it makes sense to implement smartphone applications that do not necessarily require a permanent connection to the Internet and thus also to the blockchain with a netservice-client. This makes it possible to dispense with a centralized remote server solution, but only have access to the blockchain when it is needed without having to wait long before the client is synchronized.

15.4.5 Advantages

As has already been pointed out in the use cases, there are various advantages that speak in favor of using INCUBED:

- Devices with low computing power can communicate with the blockchain.
- Devices with a poor Internet connection or limited bandwidth can communicate with the blockchain.
- Devices with a limited power supply can be integrated.
- It is a decentralized solution that does not require a central service provider for remote nodes.
- A remote node does not need to be trusted, as there is a verification facility.
- Existing centralized remote services can be easily integrated.
- Net service clients for special and proprietary hardware can be implemented independently of current Ethereum developments.

15.4.6 Challenges

Of course, there are several challenges that need to be solved in order to implement a working INCUBED.

Security

The biggest challenge for a decentralized and trust-free system is to ensure that one can make sure that the information supplied is actually correct. If a full client runs on a device and is synchronized with the network, it can check the correctness itself. A light client can also check if the block headers match, but does not have the transactions available and requires a connection to a full client for this information. A remote client that communicates with a full client via the REST API has no direct way to verify that the answer is correct. In a decentralized network of netservice-nodes whose trustworthiness is not known, a way to be certain with a high probability that the answer is correct is required. The INCUBED system provides the nodes that supply the information with additional nodes that serve as validators.

Business models

In order to provide an incentive to provide nodes for a decentralized solution, any transaction or query that passes through such a node would have to be remunerated with an additional fee for the operator of the node. However, this would further increase the transaction costs, which are already a real problem for micro-payments. However, there are also numerous non-monetary incentives that encourage participation in this infrastructure.

15.5 Architecture

15.5.1 Overview

An INCUBED network consists of several components:

1. The INCUBED registry (later called registry). This is a Smart Contract deployed on the Ethereum Main-Net where all nodes that want to participate in the network must register and, if desired, store a security deposit.
2. The INCUBED or Netservice node (later called node), which are also full nodes for the blockchain. The nodes act as information providers and validators.
3. The INCUBED or Netservice clients (later called client), which are installed e.g. in the IoT devices.
4. Watchdogs who as autonomous authorities (bots) ensure that misbehavior of nodes is uncovered and punished.

Initialization of a Client

Each client gets an initial list of boot nodes by default. Before its first "real" communication with the network, the current list of nodes must be queried as they are registered in the registry (see section [subsec:IN3-Registry-Smart-Contract]). Initially, this can only be done using an invalidated query (see figure [fig:unvalidated request]). In order to have the maximum possible security, this query can and should be made to several or even all boot nodes in order to obtain a valid list with great certainty.

This list must be updated at regular intervals to ensure that the current network is always available.

Unvalidated Requests / Transactions

Unvalidated queries and transactions are performed by the client by selecting one or more nodes from the registry and sending them the request (see figure [fig:unvalidated request]). Although the responses cannot be verified directly, the option to send the request to multiple nodes in parallel remains. The returned results can then be checked for consistency by the client. Assuming that the majority will deliver the correct result (or execute the transaction correctly), this will at least increase the likelihood of receiving the correct response (Proof of Majority).

There are other requests too that can only be returned as an unverified response. This could be the case, for example:

- Current block number (the node may not have synchronized the latest block yet or may be in a micro fork,. . .)
- Information from a block that has not yet been finalized
- Gas price

The multiple parallel query of several nodes and the verification of the results according to the majority principle is a standard functionality of the client. With the number of nodes requested in parallel, a suitable compromise must be made between increased data traffic, effort for processing the data (comparison) and higher security.

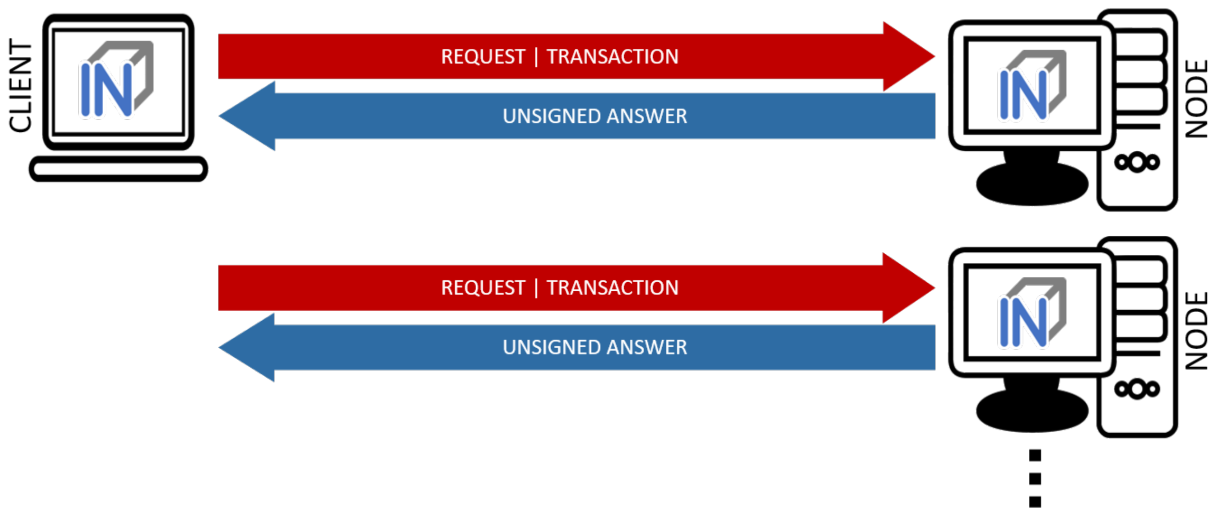
The selection of the nodes to be queried must be made at random. In particular, successive queries should always be sent to different nodes. This way it is not possible, or at least only very difficult, for a possibly misbehaving node to send specific incorrect answers to a certain client, since it cannot be foreseen at any time that the same client will also send a follow-up query to the same node, for example, and thus the danger is high that the misbehavior will be uncovered.

In the case of a misbehavior, the client can blacklist this node or at least reduce the internal rating of this node. However, inconsistent responses can also be provided unintentionally by a node, i.e. without the intention of spreading false information. This can happen, for example, if the node has not yet synchronized the current block or is running on a micro fork. These possibilities must therefore always be taken into consideration when the client "reacts" to such a response.

An unvalidated answer will be returned unsigned. Thus, it is not possible to punish the sender in case of an incorrect response, except that the client can blacklist or downgrade the sender in the above-mentioned form.

Validated Requests

The second form of queries are validated requests. The nodes must be able to provide various verification options and proofs in addition to the result of the request. With validated requests, it is possible to achieve a similar level of security with an INCUBED client as with a light or even full client, without having to blindly trust a centralized middleman (as is the case with a remote client). Depending on the security requirements and the available resources (e.g. computing power), different validations and proofs are possible.



As with an invalidated query, the node to be queried should be selected randomly. However, there are various criteria, such as the deposited security deposit, reliability and performance from previous requests, etc., which can or must also be included in the selection.

Call Parameter

A validated request consists of the parts:

- Actual request
- List of validators
- Proof request
- List of already known validations and proofs (optional).

Return values

The return depends on the request:

- The requested information (signed by the node)
- The signed answers of the validators (block hash) - 1 or more

- The Merkle Proof
- Request for a payment.

Validation

Validation refers to the checking of a block hash by one or more additional nodes. A client cannot perform this check on its own. To check the credibility of a node (information provider), the block hash it returns is checked by one or more independent nodes (validators). If a validator node can detect the malfunction of the originally requested node (delivery of an incorrect block), it can receive its security deposit and the compromised node is removed from the registry. The same applies to a validator node.

Since the network connection and bandwidth of a node is often better than that of a client, and the number of client requests should be as small as possible, the validation requests are sent from the requested node (information provider) to the validators. These return the signed answer, so that there is no possibility for the information provider to manipulate the answer. Since the selection of nodes to act as validators is made only by the client, a potentially malfunctioning node cannot influence it or select a validator to participate in a conspiracy with it.

If the selected validator is not available or does not respond, the client can specify several validators in the request, which are then contacted instead of the failed node. For example, if multiple nodes are involved in a conspiracy, the requested misbehaving node could only send the validation requests to the nodes that support the wrong response.

Proof

The validators only confirm that the block hash of the block from which the requested information originates is correct. The consistency of the returned response cannot be checked in this way.

Optionally, this information can be checked directly by the client. However, this is obligatory, but considerably increases safety. On the other hand, more information has to be transferred and a computationally complex check has to be performed by the client.

When a proof is requested, the node provides the Merkle Tree of the response so that the client can calculate and check the Merkle Root for the result itself.

Payment and Incentives

As an incentive system for the return of verified responses, the node can request a payment. For this, however, the node must guarantee with its security deposit that the answer is correct.

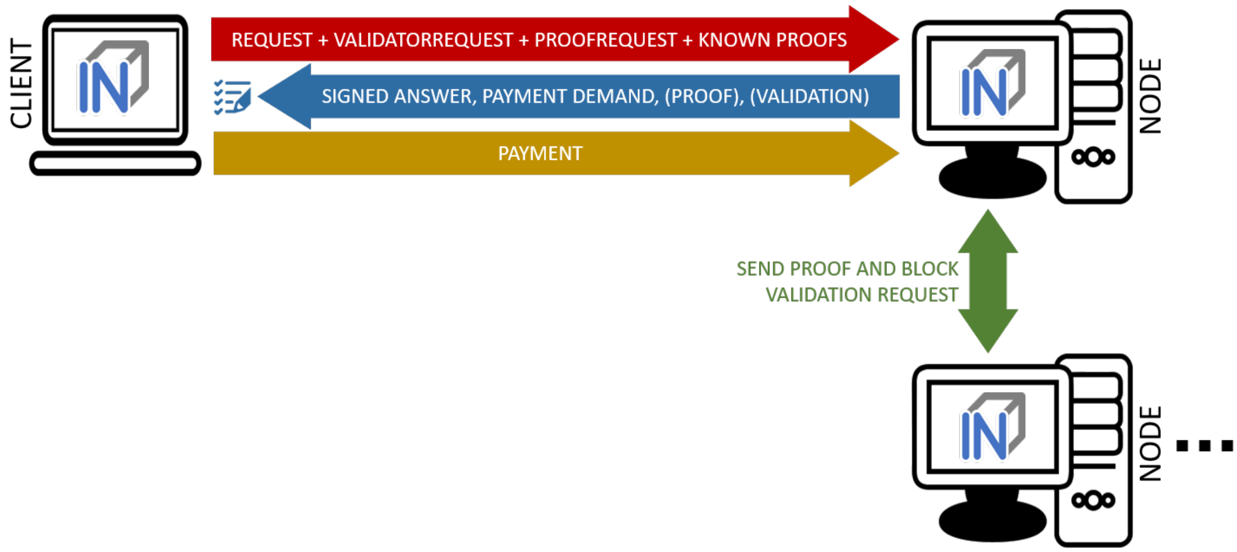
There are two strong incentives for the node to provide the correct response with high performance since it loses its deposit when a validator (wrong block hash) detects misbehavior and is eliminated from the registry, and receives a reward for this if it provides a correct response.

If a client refuses payment after receiving the correctly validated information which it requested, it can be blacklisted or downgraded by the node so that it will no longer receive responses to its requests.

If a node refuses to provide the information for no reason, it is blacklisted by the client in return or is at least downgraded in rating, which means that it may no longer receive any requests and therefore no remuneration in the future.

If the client detects that the Merkle Proof is not correct (although the validated block hash is correct), it cannot attack the node's deposit but has the option to blacklist or downgrade the node to no longer ask it. A node caught this way of misbehavior does not receive any more requests and therefore cannot make any profits.

The security deposit of the node has a decisive influence on how much trust is placed in it. When selecting the node, a client chooses those nodes that have a corresponding deposit (stake), depending on the security requirements (e.g. high value of a transaction). Conversely, nodes with a high deposit will also charge higher fees, so that a market with supply and demand for different security requirements will develop.



15.5.2 IN3-Registry Smart Contract

Each client is able to fetch the complete list including the deposit and other information from the contract, which is required in order to operate. The client must update the list of nodes logged into the registry during initialization and regularly during operation to notice changes (e.g. if a node is removed from the registry intentionally or due to misbehavior detected).

In order to maintain a list of network nodes offering INCUBED-services a smart contract IN3Registry in the Ethereum Main-Net is deployed. This contract is used to manage ownership and deposit for each node.

```
contract ServerRegistry {

    /// server has been registered or updated its registry props or deposit
    event LogServerRegistered(string url, uint props, address owner, uint deposit);

    ///  a caller requested to unregister a server.
    event LogServerUnregisterRequested(string url, address owner, address caller);

    /// the owner canceled the unregister-proccess
    event LogServerUnregisterCanceled(string url, address owner);

    /// a Server was convicted
    event LogServerConvicted(string url, address owner);

    /// a Server is removed
    event LogServerRemoved(string url, address owner);

    struct In3Server {
        string url;  // the url of the server
        address owner; // the owner, which is also the key to sign blockhashes
        uint deposit; // stored deposit
        uint props; // a list of properties-flags representing the capabilities of␣
↪the server

        // unregister state
        uint128 unregisterTime; // earliest timestamp in to to call unregister
        uint128 unregisterDeposit; // Deposit for unregistering
```

(continues on next page)

(continued from previous page)

```
        address unregisterCaller; // address of the caller requesting the unregister
    }

    /// server list of incubed nodes
    In3Server[] public servers;

    /// length of the serverlist
    function totalServers() public view returns (uint) ;

    /// register a new Server with the sender as owner
    function registerServer(string _url, uint _props) public payable;

    /// updates a Server by adding the msg.value to the deposit and setting the props␣
↪
    function updateServer(uint _serverIndex, uint _props) public payable;

    /// this should be called before unregistering a server.
    /// there are 2 use cases:
    /// a) the owner wants to stop offering the service and remove the server.
    ///    in this case he has to wait for one hour before actually removing the␣
↪server.
    ///    This is needed in order to give others a chance to convict it in case this␣
↪server signs wrong hashes
    /// b) anybody can request to remove a server because it has been inactive.
    ///    in this case he needs to pay a small deposit, which he will lose
    //       if the owner become active again
    //       or the caller will receive 20% of the deposit in case the owner does not␣
↪react.
    function requestUnregisteringServer(uint _serverIndex) payable public;

    /// this function must be called by the caller of the requestUnregisteringServer-
↪function after 28 days
    /// if the owner did not cancel, the caller will receive 20% of the server␣
↪deposit + his own deposit.
    /// the owner will receive 80% of the server deposit before the server will be␣
↪removed.
    function confirmUnregisteringServer(uint _serverIndex) public ;

    /// this function must be called by the owner to cancel the unregister-process.
    /// if the caller is not the owner, then he will also get the deposit paid by the␣
↪caller.
    function cancelUnregisteringServer(uint _serverIndex) public;


    /// convicts a server that signed a wrong blockhash
    function convict(uint _serverIndex, bytes32 _blockhash, uint _blocknumber, uint8 _
↪v, bytes32 _r, bytes32 _s) public ;

}
```

To register, the owner of the node needs to provide the following data:

- **props** : a bitmask holding properties like.
- **url** : the public url of the server.
- **msg.value** : the value sent during this transaction is stored as deposit in the contract.
- **msg.sender** : the sender of the transaction is set as owner of the node and therefore able to manage it at any

given time.

Deposit

The deposit is an important incentive for the secure operation of the INCUBED network. The risk of losing the deposit if misconduct is detected motivates the nodes to provide correct and verifiable answers.

The amount of the deposit can be part of the decision criterion for the clients when selecting the node for a request. The "value" of the request can therefore influence the selection of the node (as information provider). For example, a request that is associated with a high value may not be sent to a node that has a very low deposit. On the other hand, for a request for a dashboard, which only provides an overview of some information, the size of the deposit may play a subordinate role.

15.5.3 Netservice-Node

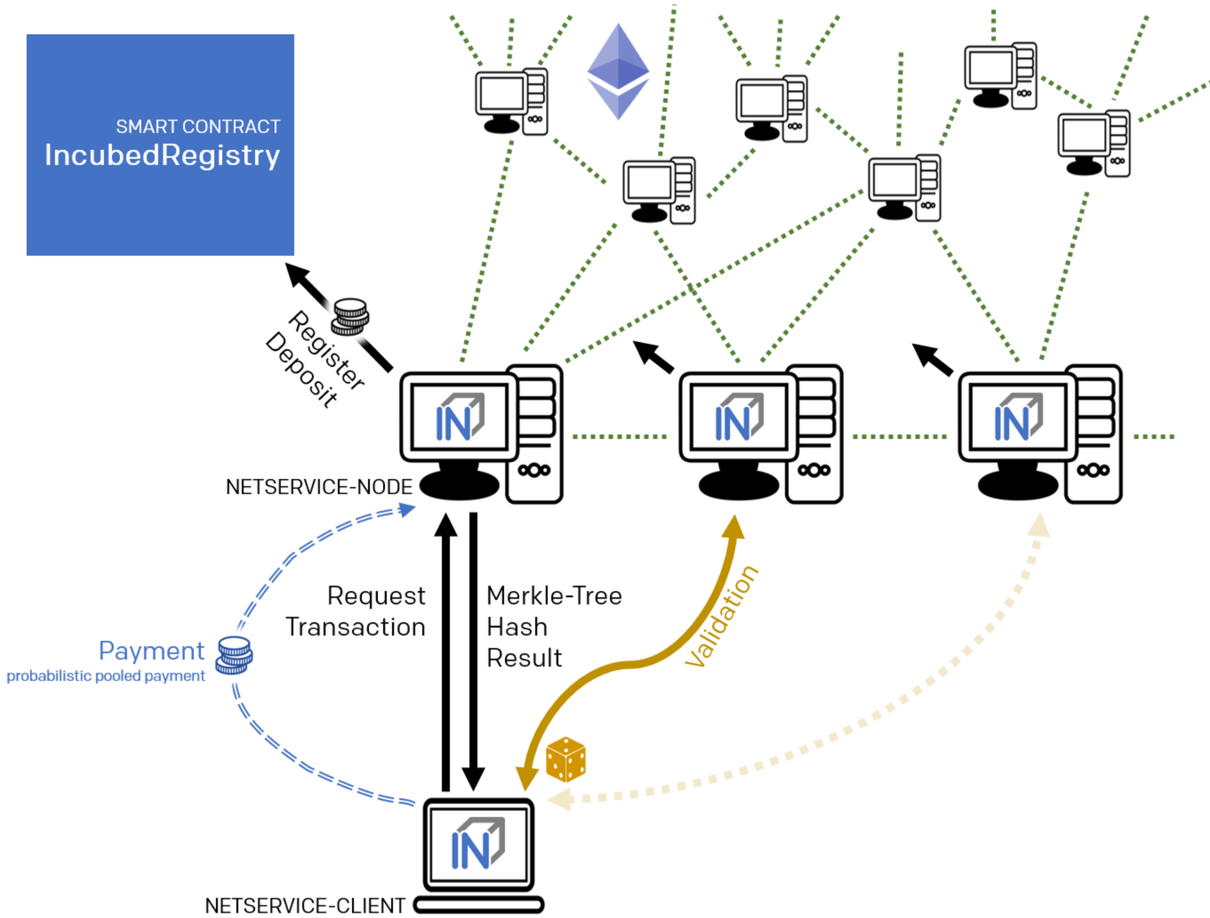
The net service node (short: node) is the communication interface for the client to the blockchain client. It can be implemented as a separate application or as an integrated module of a blockchain client (such as Geth or Parity).

Nodes must provide two different services:

- Information Provider
- Validator.

Information Provider

A client directly addresses a node (information provider) to retrieve the desired information. Similar to a remote client, the node interacts with the blockchain via its blockchain client and returns the information to the requesting client. Furthermore, the node (information provider) provides the information the client needs to verify the result of the query (validation and proof). For the service, it can request payment when it returns a validated response.



If an information provider is found to return incorrect information as a validated response, it loses its deposit and is removed from the registry. It can be transferred by a validator or watchdog.

Validator

The second service that a node has to provide is validation. When a client submits a validated request to the information provider, it also specifies the node(s) that are designated as validators. Each node that is logged on to the registry must also accept the task as validator.

If a validator is found to return false information as validation, it loses its deposit and is removed from the registry. It can be transferred by another validator or a watchdog.

Watchdog

Watchdogs are independent bots whose random validators logged in to the registry are checked by specific queries to detect misbehavior. In order to provide an incentive for validator activity, watchdogs can also deliberately pretend misbehavior and thus give the validator the opportunity to claim the security deposit.

15.5.4 Netservice-Client

The netservice client (short client) is the instance running on the device that needs the connection to the blockchain. It communicates with the nodes of the INCUBED network via a REST API.

The client can decide autonomously whether it wants to request an unvalidated or a validated answer (see section. . .). In addition to communicating with the nodes, the client has the ability to verify the responses by evaluating the majority (unvalidated request) or validations and proofs (validated requests).

The client receives the list of available nodes of the INCUBED network from the registry and ensures that this list is always kept up-to-date. Based on the list, the client also manages a local reputation system of nodes to take into account performance, reliability, trustworthiness and security when selecting a node.

A client can communicate with different blockchains at the same time. In the registry, nodes of different blockchains (identified by their ID) are registered so that the client can and must filter the list to identify the nodes that can process (and validate, if necessary) its request.

Local Reputation System

The local reputations system aims to support the selection of a node.

The reputation system is also the only way for a client to blacklist nodes that are unreliable or classified as fraudulent. This can happen, for example, in the case of an unvalidated query if the results of a node do not match those of the majority, or in the case of validated queries, if the validation is correct but the proof is incorrect.

Performance-Weighting

In order to balance the network, each client may weight each node by:

$$weight = \frac{\max(\lg(deposit),1)}{\max(avgResponseTime,100)}$$

Based on the weight of each node a random node is chosen for each request. While the deposit is read by the contract, the avgResponseTime is managed by the client himself. The does so by measuring the time between request and response and calculate the average (in ms) within the last 24 hours. This way the load is balanced and faster servers will get more traffic.

15.5.5 Payment / Incentives

To build an incentive-based network, it is necessary to have appropriate technologies to process payments. The payments to be made in INCUBED (e.g. as a fee for a validated answer) are, without exception micro payments (other than the deposit of the deposit, which is part of the registration of a node and which is not mentioned here, however). When designing a suitable payment solution, it must therefore be ensured that a reasonable balance is always found between the actual fee, transaction costs and transaction times.

Direct Transaction Payment

Direct payment by transaction is of course possible, but this is not possible due to the high transaction costs. Exceptions to this could be transactions with a high value, so that corresponding transaction costs would be acceptable.

However, such payments are not practical for general use.

State Channels

State channels are well-suited for the processing of micropayments. A decisive point of the protocol is that the node must always be selected randomly (albeit weighted according to further criteria). However, it is not practical for a client to open a separate state channel (including deposit) with each potential node that it wants to use for a request. To establish a suitable micropayment system based on state channels, a state channel network such as Raiden is required. If enough partners are interconnected in such a network and a path can be found between two partners, payments can also be exchanged between these participants.

Probabilistic Payment

Another way of making small payments is probabilistic micropayments. The idea is based on issuing probabilistic lottery tickets instead of very small direct payments, which, with a certain probability, promise to pay out a higher amount. The probability distribution is adjusted so that the expected value corresponds to the payment to be made.

For a probabilistic payment, an amount corresponding to the value of the lottery ticket is deposited. Instead of direct payment, tickets are now issued that have a high likelihood of winning. If a ticket is not a winning ticket, it expires and does not entitle the recipient to receive a payment. Winning tickets, on the other hand, entitle the recipient to receive the full value of the ticket.

Since this value is so high that a transaction is worthwhile, the ticket can be redeemed in exchange for a payment.

Probabilistic payments are particularly suitable for combining a continuous, preferably evenly distributed flow of small payments into individual larger payments (e.g. for streaming data).

Similar to state channels, a type of payment channel is created between two partners (with an appropriate deposit).

For the application in the INCUBED protocol, it is not practical to establish individual probabilistic payment channels between each client and requested node, since on the one hand the prerequisite of a continuous and evenly distributed payment stream is not given and, on the other hand, payments may be very irregularly required (e.g. if a client only rarely sends queries).

The analog to a state channel network is pooled probabilistic payments. Payers can be pooled and recipients can also be connected in a pool, or both.

15.6 Scaling

The interface between client and node is independent of the blockchain with which the node communicates. This allows a client to communicate with multiple blockchains / networks simultaneously as long as suitable nodes are registered in the registry.

For example, a payment transaction can take place on the Ethereum Mainnet and access authorization can be triggered in a special application chain.

15.6.1 Multi Chain Support

Each node may support one or more network or chains. The supported list can be read by filtering the list of all servers in the contract.

The ChainId refers to a list based on EIP-155. The ChainIds defined there will be extended by enabling even custom chains to register a new chainId.

15.6.2 Conclusion

INCUBED establishes a decentralized network of validatable remote nodes, which enables IoT devices in particular to gain secure and reliable access to the blockchain. The demands on the client's computing and storage capacity can be reduced to a minimum, as can the requirements on connectivity and network traffic.

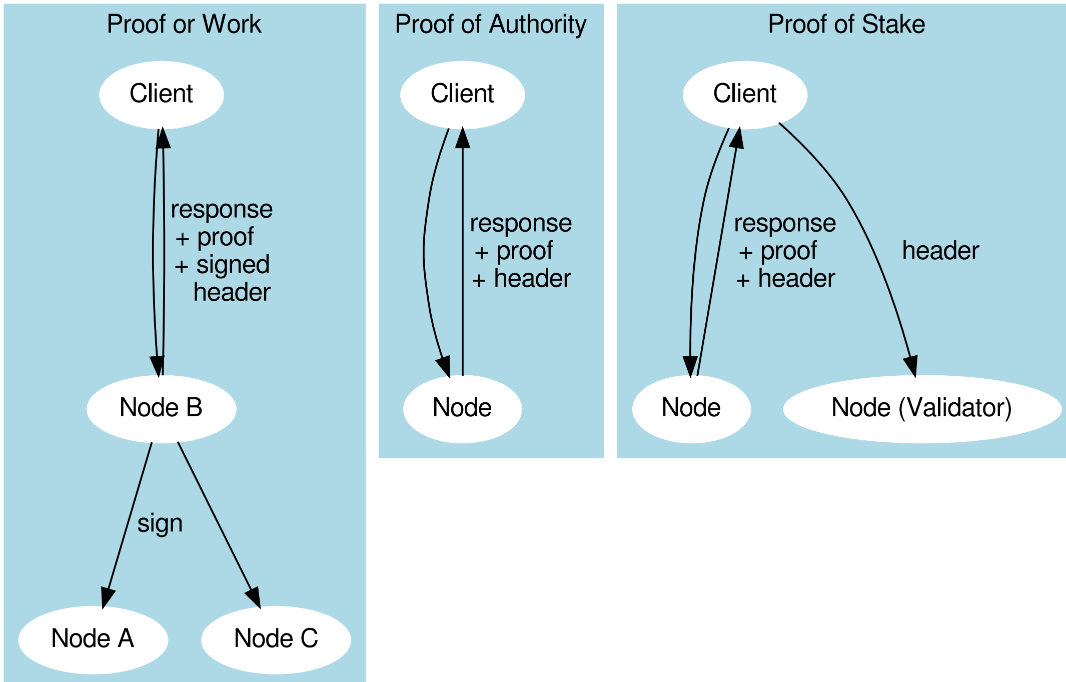
INCUBED also provides a platform for scaling by allowing multiple blockchains to be accessed in parallel from the same client. Although INCUBED is designed in the first instance for the Ethereum network (and other chains using the Ethereum protocol), in principle other networks and blockchains can also be integrated, as long as it is possible to realize a node that can work as information provider (incl. proof) and validator.

CHAPTER 16

Blockheader Verification

16.1 Ethereum

Since all proofs always include the blockheader, it is crucial to verify the correctness of these data as well. But verification depends on the consensus of the underlying blockchain. (For details, see *Ethereum Verification and MerkleProof*.)



16.1.1 Proof of Work

Currently, the public chain uses proof of work. This makes it very hard to verify the header since anybody can produce such a header. So the only way to verify that the block in question is an accepted block is to let registered nodes sign the blockhash. If they are wrong, they lose their previously stored deposit. For the client, this means that the required security depends on the deposit stored by the nodes.

This is why a client may be configured to require multiple signatures and even a minimal deposit:

```
client.sendRPC('eth_getBalance', [account, 'latest'], chain, {
  minDeposit: web3.utils.toWei(10,'ether'),
  signatureCount: 3
})
```

The `minDeposit` lets the client preselect only nodes with at least that much deposit. The `signatureCount` asks for multiple signatures and so increases the security.

Since most clients are small devices with limited bandwith, the client is not asking for the signatures directly from the nodes but, rather, chooses one node and lets this node run a subrequest to get the signatures. This means not only fewer requests for the clients but also that at least one node checks the signatures and "convicts" another if it lied.

16.1.2 Proof of Authority

The good thing about proof of authority is that there is already a signature included in the blockheader. So if we know who is allowed to sign a block, we do not need an additional blockhash signed. The only critical information we rely on is the list of validators.

Currently, there are two consensus algorithms:

Aura

Aura is only used by Parity, and there are two ways to configure it:

- **static list of nodes** (like the Kovan network): in this case, the validatorlist is included in the chain-spec and cannot change, which makes it very easy for a client to verify blockheaders.
- **validator contract**: a contract that offers the function `getValidators()`. Depending on the chain, this contract may contain rules that define how validators may change. But this flexibility comes with a price. It makes it harder for a client to find a secure way to detect validator changes. This is why the proof for such a contract depends on the rules laid out in the contract and is chain-specific.

Clique

Clique is a protocol developed by the Geth team and is now also supported by Parity (see Görli testnet).

Instead of relying on a contract, Clique defines a protocol of how validator nodes may change. All votes are done directly in the blockheader. This makes it easier to prove since it does not rely on any contract.

The Incubed nodes will check all the blocks for votes and create a `validatorlist` that defines the validatorset for any given blockNumber. This also includes the proof in form of all blockheaders that either voted the new node in or out. This way, the client can ask for the list and automatically update the internal list after it has verified each blockheader and vote. Even though malicious nodes cannot forge the signatures of a validator, they may skip votes in the validatorlist. This is why a validatorlist update should always be done by running multiple requests and merging them together.

16.2 Bitcoin

Bitcoin may be a complete different chain, but there are ways to verify a Bitcoin Blockheader within a Ethereum Smart Contract. This requires a little bit more effort but you can use all the features of Incubed.

16.2.1 Block Proof

The data we want to verify are mainly Blocks and Transactions. Usually, if we want to get the BlockHeader or the complete block we already know the blockhash. And if we know that this hash is correct, verifying the rest of the block is easy.

1. We take the first 80 Bytes of the Blockdata, which is the blockHeader and hash it twice with sha256. Since Bitcoin stores the hashes in little endian, we then have to reverse the byteorder.

```
// btc hash = sha256(sha256(data))
const hash(data: Buffer)  => crypto.createHash('sha256').update(crypto.createHash(
↪'sha256').update(data).digest()).digest()

const blockData:Buffer = ....
// take the first 80 bytes, hash them and reverse the order
const blockHash = hash( blockData.slice(0,80)).reverse()
```

2. In order to check the Proof of work in the BlockHeader, we compare the target with the hash:

```
const target = Buffer.alloc(32)
// we take the first 3 bytes from the bits-field and use the 4th byte as exponent:
blockData.copy(target, blockData[75]-3,72,75);
// the hash must be lower than the target
if ( target.reverse().compare( blockHash )<0)
   throw new Error('blockHash must be smaller than the target')
```

Note : In order to verify that the target is correct, we can :

- take the target from a different blockheader in the same 2016 blocks epoch
- if we don't have one, we should ask for multiple nodes to make sure we have a correct target.

3. If we want to know if this is final, the Node needs to provide us with additional BlockHeaders on top of the current Block (FinalityHeaders).

   These header need to be verified the same way. But additionaly we need to check the parentHash:

```
if (!parentHash.reverse().equals( blockData.slice(4,36) ))
  throw new Error('wrong parentHash!')
```

4. In order to verify the Transactions (only if we have the complete Block, not only the BlockHeader), we need to read them, hash each one and put them in a merkle tree. If the root of the tree matches the merkleRoot, the transactions are correct.

```
// we take each Transactiondata, hash them and put the transactionhashes into a␣
↪merkle tree
const merkleRoot = createMerkleRoot ( readTransactions(blockData).map(_=>hash(_).
↪reverse()) )

// compare the root with merkleRoot of the header starting at offset 36
if (!merkleRoot.equals(blockData.slice(36,68).reverse()))
  throw new Error('Invalid MerkleRoot!')
```

16.2.2 Transaction Proof

In order to Verify a Transaction, we need a Merkle Proof. So the Incubed Server will have create a complete Merkle-Tree and then pass the other part of the pair as Proof.

Verifying means we start by hashing the transaction and then keep on hashing this result with the next hash from the proof. The last hash must match the merkleRoot.

16.2.3 Convicting For wrong Blockhashes in the NodeRegistry

Just as the Incubed Client can ask for signed blockhashes in Ethereum, he can do this in Bitcoin as well. The signed payload from the node will have to contain these data:

```
bytes32 blockhash;
uint256 timestamp;
bytes32 registryId;
```

Client requires a Signed Blockhash

and the Data Provider Node will ask the chosen node to sign.

The Data Provider Node (or Watchdog) will then check the signature

If the signed blockhash is wrong it will start the conviting process:

Convict with BlockHeaders

In order to convict, the Node needs to provide proof, which is the correct blockheader.

But since the BlockHeader does not contain the BlockNumber, we have to use the timestamp. So the correct block as proof must have either the same timestamp or a the last block before the timestamp. Additionally the Node may provide FinalityBlockHeaders. As many as possible, but at least one in order to prove, that the timestamp of the correct block is the closest one.

The Registry Contract will then verify

- the Signature of the convited Node.
- the BlockHeaders gives as Proof

The Verification of the BlockHeader can be done directly in Solitidy, because the EVM offers a precompiled Contract at address `0x2` : sha256, which is needed to calculate the Blockhash. With this in mind we can follow the steps 1-3 as described in *Block Proof* implemented in Solidity.

While doing so we need to add the difficulties of each block and store the last blockHash and the `totalDifficulty` for later.

Challenge the longest chain

Now the convited Server has the chance to also deliver blockheaders to proof that he has signed the correct one.

The simple rule is:

> If the other node (convited or convitor) is not able to add enough verified BlockHeaders with a higher `totalDifficulty` within 1 hour, the other party can get the deposit and kick the malicious node out.

Even though this game could go for a while, if the convicted Node signed a hash, which is not part of the longest chain, it will not be possible to create enough mining power to continue mining enough blocks to keep up with the longest chain in the mainnet. Therefore he will most likely give up right after the first transaction.

CHAPTER 17

Technical Background

17.1 Ethereum Verification

The Incubed is also often called Minimal Verifying Client because it may not sync, but still is able to verify all incoming data. This is possible since ethereum is based on a technology allowing to verify almost any value.

Our goal was to verify at least all standard `eth_...` rpc methods as described in the Specification.

In order to prove something, you always need a starting value. In our case this is the BlockHash. Why do we use the BlockHash? If you know the BlockHash of a block, you can easily verify the full BlockHeader. And since the BlockHeader contains the stateRoot, transationRoot and receiptRoot, these can be verified as well. And the rest will simply depend on them.

There is also another reason why the BlockHash is so important. This is the only value you are able to access from within a SmartContract, because the evm supports a OpCode (`BLOCKHASH`), which allows you to read the last 256 Blockhashes, which gives us the chance to even verify the blockhash onchain.

Depending on the method, different proofs are needed, which are described in this document.

- ***Block Proof*** - verifies the content of the BlockHeader
- ***Transaction Proof*** - verifies the input data of a transaction
- ***Receipt Proof*** - verifies the outcome of a transaction
- ***Log Proof*** - verifies the response of `eth_getPastLogs`
- ***Account Proof*** - verifies the state of an account
- ***Call Proof*** - verifies the result of a `eth_call` - response

17.1.1 BlockProof

BlockProofs are used whenever you want to read data of a Block and verify them. This would be:

- eth_getBlockTransactionCountByHash

- eth_getBlockTransactionCountByNumber
- eth_getBlockByHash
- eth_getBlockByNumber

The `eth_getBlockBy...` methods return the Block-Data. In this case all we need is somebody verifying the blockhash, which is don by requiring somebody who stored a deposit and would lose it, to sign this blockhash.

The Verification is then simply by creating the blockhash and comparing this to the signed one.

The Blockhash is calculated by serializing the blockdata with rlp and hashing it:

```
blockHeader = rlp.encode([
  bytes32( parentHash ),
  bytes32( sha3Uncles ),
  address( miner || coinbase ),
  bytes32( stateRoot ),
  bytes32( transactionsRoot ),
  bytes32( receiptsRoot || receiptRoot ),
  bytes256( logsBloom ),
  uint( difficulty ),
  uint( number ),
  uint( gasLimit ),
  uint( gasUsed ),
  uint( timestamp ),
  bytes( extraData ),

  ... sealFields
    ? sealFields.map( rlp.decode )
    : [
      bytes32( b.mixHash ),
      bytes8( b.nonce )
    ]
])
```

For POA-Chains the blockheader will use the `sealFields` (instead of mixHash and nonce) which are already rlp-encoded and should be added as raw data when using rlp.encode.

```
if (keccak256(blockHeader) !== singedBlockHash)
  throw new Error('Invalid Block')
```

In case of the `eth_getBlockTransactionCountBy...` the proof contains the full blockHeader already serialized + all transactionHashes. This is needed in order to verify them in a merkleTree and compare them with the `transactionRoot`

17.1.2 Transaction Proof

TransactionProofs are used for the following transaction-methods:

- eth_getTransactionByHash
- eth_getTransactionByBlockHashAndIndex
- eth_getTransactionByBlockNumberAndIndex

In order to verify we need :

1. serialize the blockheader and compare the blockhash with the signed hash as well as with the blockHash and number of the transaction. (See *BlockProof*)

2. serialize the transaction-data

```
transaction = rlp.encode([
  uint( tx.nonce ),
  uint( tx.gasPrice ),
  uint( tx.gas || tx.gasLimit ),
  address( tx.to ),
  uint( tx.value ),
  bytes( tx.input || tx.data ),
  uint( tx.v ),
  uint( tx.r ),
  uint( tx.s )
])
```

1. verify the merkleProof of the transaction with

```
verifyMerkleProof(
  blockHeader.transactionRoot, /* root */,
  keccak256(proof.txIndex), /* key or path */
  proof.merkleProof, /* serialized nodes starting with the root-node */
  transaction /* expected value */
)
```

The Proof-Data will look like these:

```
{
  "jsonrpc": "2.0",
  "id": 6,
  "result": {
    "blockHash": "0xf1a2fd6a36f27950c78ce559b1dc4e991d46590683cb8cb84804fa672bca395b",
    "blockNumber": "0xca",
    "from": "0x7e5f4552091a69125d5dfcb7b8c2659029395bdf",
    "gas": "0x55f0",
    "gasPrice": "0x0",
    "hash": "0xe9c15c3b26342e3287bb069e433de48ac3fa4ddd32a31b48e426d19d761d7e9b",
    "input": "0x00",
    "value": "0x3e8"
    ...
  },
  "in3": {
    "proof": {
      "type": "transactionProof",
      "block": "0xf901e6a040997a53895b48...", // serialized blockheader
      "merkleProof": [  /* serialized nodes starting with the root-node */

↪"f868822080b863f86136808255f0942b5ad5c4795c026514f8317c7a215e218dccd6cf8203e8001ca0dc967310342af50
↪"
      ],
      "txIndex": 0,
      "signatures": [...]
    }
  }
}
```

17.1.3 Receipt Proof

Proofs for the transactionReceipt are used for the following transaction-method:

- eth_getTransactionReceipt

In order to verify we need :

1. serialize the blockheader and compare the blockhash with the signed hash as well as with the blockHash and number of the transaction. (See *BlockProof*)
2. serialize the transaction receipt

```
transactionReceipt = rlp.encode([
  uint( r.status || r.root ),
  uint( r.cumulativeGasUsed ),
  bytes256( r.logsBloom ),
  r.logs.map(l => [
    address( l.address ),
    l.topics.map( bytes32 ),
    bytes( l.data )
  ])
].slice(r.status === null && r.root === null ? 1 : 0))
```

1. verify the merkleProof of the transaction receipt with

```
verifyMerkleProof(
  blockHeader.transactionReceiptRoot, /* root */,
  keccak256(proof.txIndex), /* key or path */
  proof.merkleProof, /* serialized nodes starting with the root-node */
  transactionReceipt /* expected value */
)
```

1. Since the merkle-Proof is only proving the value for the given transactionIndex, we also need to prove that the transactionIndex matches the transactionHash requested. This is done by adding another MerkleProof for the Transaction itself as described in the *Transaction Proof*

17.1.4 Log Proof

Proofs for logs are only for the one rpc-method:

- eth_getLogs

Since logs or events are based on the TransactionReceipts, the only way to prove them is by proving the TransactionReceipt each event belongs to.

That's why this proof needs to provide

- all blockheaders where these events occured
- all TransactionReceipts + their MerkleProof of the logs
- all MerkleProofs for the transactions in order to prove the transactionIndex

The Proof data structure will look like this:

```
  Proof {
    type: 'logProof',
    logProof: {
      [blockNr: string]: {  // the blockNumber in hex as key
        block : string  // serialized blockheader
        receipts: {
          [txHash: string]: {  // the transactionHash as key
            txIndex: number // transactionIndex within the block
```

(continues on next page)

(continued from previous page)

```
            txProof: string[] // the merkle Proof-Array for the transaction
            proof: string[] // the merkle Proof-Array for the receipts
          }
        }
      }
    }
  }
```

In order to verify we need :

1. deserialize each blockheader and compare the blockhash with the signed hashes. (See *BlockProof*)
2. for each blockheader we verify all receipts by using

```
verifyMerkleProof(
  blockHeader.transactionReceiptRoot, /* root */,
  keccak256(proof.txIndex), /* key or path */
  proof.merkleProof, /* serialized nodes starting with the root-node */
  transactionReceipt /* expected value */
)
```

1. The resulting values are the receipts. For each log-entry, we are comparing the verified values of the receipt with the returned logs to ensure that they are correct.

17.1.5 Account Proof

Prooving an account-value applies to these functions:

- eth_getBalance
- eth_getCode
- eth_getTransactionCount
- eth_getStorageAt

eth_getProof

For the Transaction or Block Proofs all needed data can be found in the block itself and retrieved through standard rpc calls, but if we want to approve the values of an account, we need the MerkleTree of the state, which is not accessable through the standard rpc. That's why we have created a EIP to add this function and also implemented this in geth and parity:

- parity (Status: pending pull request) - Docker
- geth (Status: pending pull request) - Docker

This function accepts 3 parameter :

1. `account` - the address of the account to proof
2. `storage` - a array of storage-keys to include in the proof.
3. `block` - integer block number, or the string "latest", "earliest" or "pending"

```
{
  "jsonrpc": "2.0",
  "id": 1,
```

(continues on next page)

(continued from previous page)

```
  "method": "eth_getProof",
  "params": [
    "0x7F0d15C7FAae65896648C8273B6d7E43f58Fa842",
    [  "0x56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421" ],
    "latest"
  ]
}
```

The result will look like this:

```
{
  "jsonrpc": "2.0",
  "result": {
    "accountProof": [
      "0xf90211a...0701bc80",
      "0xf90211a...0d832380",
      "0xf90211a...5fb20c80",
      "0xf90211a...0675b80",
      "0xf90151a0...ca08080"
    ],
    "address": "0x7f0d15c7faae65896648c8273b6d7e43f58fa842",
    "balance": "0x0",
    "codeHash": "0xc5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470",
    "nonce": "0x0",
    "storageHash": "0x56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421
↪",
    "storageProof": [
      {
        "key": "0x56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421",
        "proof": [
          "0xf90211a...0701bc80",
          "0xf90211a...0d832380"
        ],
        "value": "0x1"
      }
    ]
  },
  "id": 1
}
```

In order to run the verification the blockheader is needed as well.

The Verification of such a proof is done in the following steps:

1. serialize the blockheader and compare the blockhash with the signed hash as well as with the blockHash and number of the transaction. (See *BlockProof*)
2. Serialize the account, which holds the 4 values:

```
account = rlp.encode([
  uint( nonce),
  uint( balance),
  bytes32( storageHash || ethUtil.KECCAK256_RLP),
  bytes32( codeHash || ethUtil.KECCAK256_NULL)
])
```

1. verify the merkle Proof for the account using the stateRoot of the blockHeader:

```
verifyMerkleProof(
 block.stateRoot, // expected merkle root
 util.keccak(accountProof.address), // path, which is the hashed address
 accountProof.accountProof.map(bytes), // array of Buffer with the merkle-proof-data
 isNotExistend(accountProof) ? null : serializeAccount(accountProof), // the expected␣
↪serialized account
)
```

In case the account does exist yet, (which is the case if `none == startNonce` and `codeHash == '0xc5d2460186f7233c927e7db2dcc703c0e500b653ca82273b7bfad8045d85a470'`), the proof may end with one of these nodes:

- the last node is a branch, where the child of the next step does not exist.
- the last node is a leaf with different relative key

Both would prove, that this key does not exist.

1. Verify each merkle Proof for the storage using the storageHash of the account:

```
verifyMerkleProof(
  bytes32( accountProof.storageHash ),   // the storageRoot of the account
  util.keccak(bytes32(s.key)),  // the path, which is the hash of the key
  s.proof.map(bytes), // array of Buffer with the merkle-proof-data
  s.value === '0x0' ? null : util.rlp.encode(s.value) // the expected value or none␣
↪to proof non-existence
))
```

17.1.6 Call Proof

Call Proofs are used whenever you are calling a read-only function of smart contract:

- eth_call

Verifying the result of a `eth_call` is a little bit more complex. Because the response is a result of executing opcodes in the vm. The only way to do so, is to reproduce it and execute the same code. That's why a Call Proof needs to provide all data used within the call. This means :

- all referred accounts including the code (if it is a contract), storageHash, nonce and balance.
- all storage keys, which are used (This can be found by tracing the transaction and collecting data based on th `SLOAD`-opcode)
- all blockdata, which are referred at (besides the current one, also the `BLOCKHASH`-opcodes are referring to former blocks)

For Verifying you need to follow these steps:

1. serialize all used blockheaders and compare the blockhash with the signed hashes. (See *BlockProof*)
2. Verify all used accounts and their storage as showed in *Account Proof*
3. create a new VM with a MerkleTree as state and fill in all used value in the state:

```
  // create new state for a vm
  const state = new Trie()
  const vm = new VM({ state })

  // fill in values
  for (const adr of Object.keys(accounts)) {
```

(continues on next page)

(continued from previous page)

```
    const ac = accounts[adr]

    // create an account-object
    const account = new Account([ac.nonce, ac.balance, ac.stateRoot, ac.codeHash])

    // if we have a code, we will set the code
    if (ac.code) account.setCode( state, bytes( ac.code ))

    // set all storage-values
    for (const s of ac.storageProof)
      account.setStorage( state, bytes32( s.key ), rlp.encode( bytes32( s.value )))

    // set the account data
    state.put( address( adr ), account.serialize())
  }

  // add listener on each step to make sure it uses only values found in the proof
  vm.on('step', ev => {
     if (ev.opcode.name === 'SLOAD') {
        const contract = toHex( ev.address ) // address of the current code
        const storageKey = bytes32( ev.stack[ev.stack.length - 1] ) // last element␣
↪on the stack is the key
        if (!getStorageValue(contract, storageKey))
          throw new Error(`incomplete data: missing key ${storageKey}`)
     }
     /// ... check other opcodes as well
  })

  // create a transaction
  const tx = new Transaction(txData)

  // run it
  const result = await vm.runTx({ tx, block: new Block([block, [], []]) })

  // use the return value
  return result.vm.return
```

In the future we will be using the same approach to verify calls with ewasm.

CHAPTER 18

Incentivization

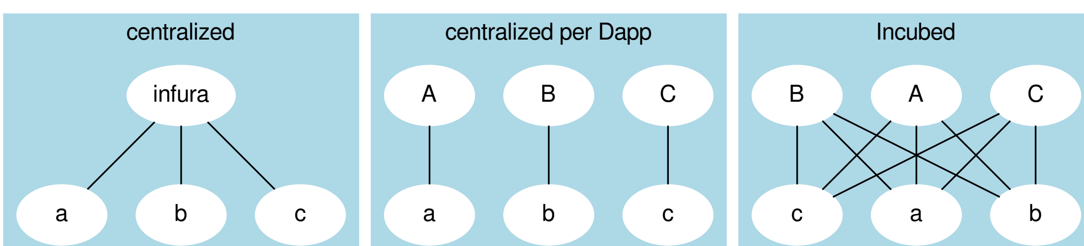
Important: This concept is still in development and discussion and is not yet fully implemented.

The original idea of blockchain is a permissionless peer-to-peer network in which anybody can participate if they run a node and sync with other peers. Since this is still true, we know that such a node won't run on a small IoT-device.

18.1 Decentralizing Access

This is why a lot of users try remote-nodes to serve their devices. However, this introduces a new single point of failure and the risk of man-in-the-middle attacks.

So the first step is to decentralize remote nodes by sharing rpc-nodes with other apps.



18.2 Incentivization for Nodes

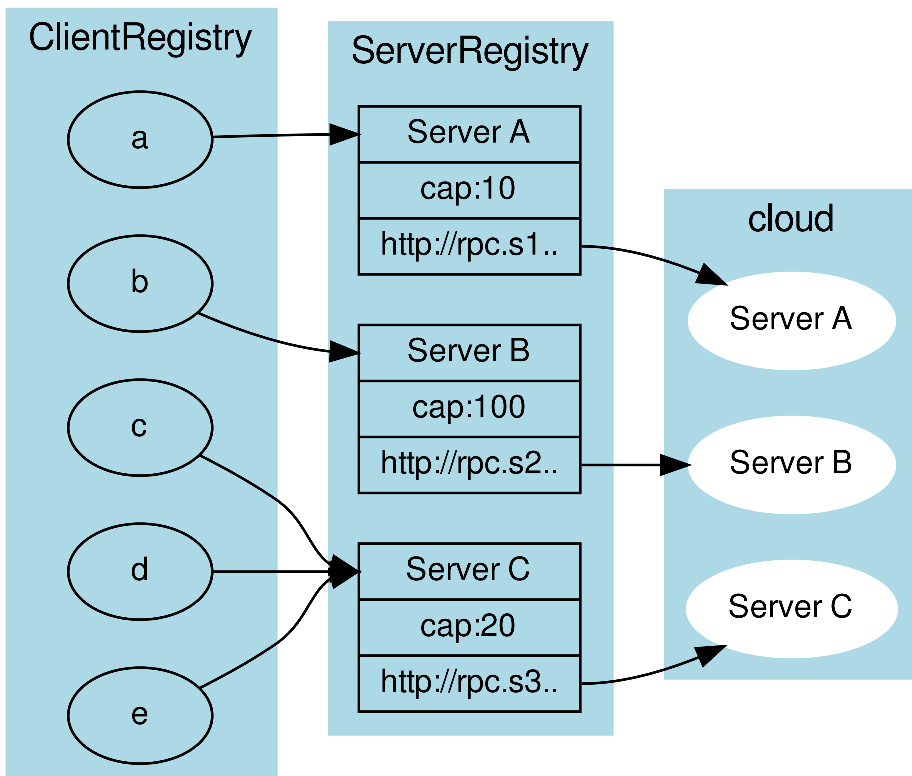
In order to incentivize a node to serve requests to clients, there must be something to gain (payment) or to lose (access to other nodes for its clients).

18.3 Connecting Clients and Server

As a simple rule, we can define this as:

> **The Incubed network will serve your client requests if you also run an honest node.**

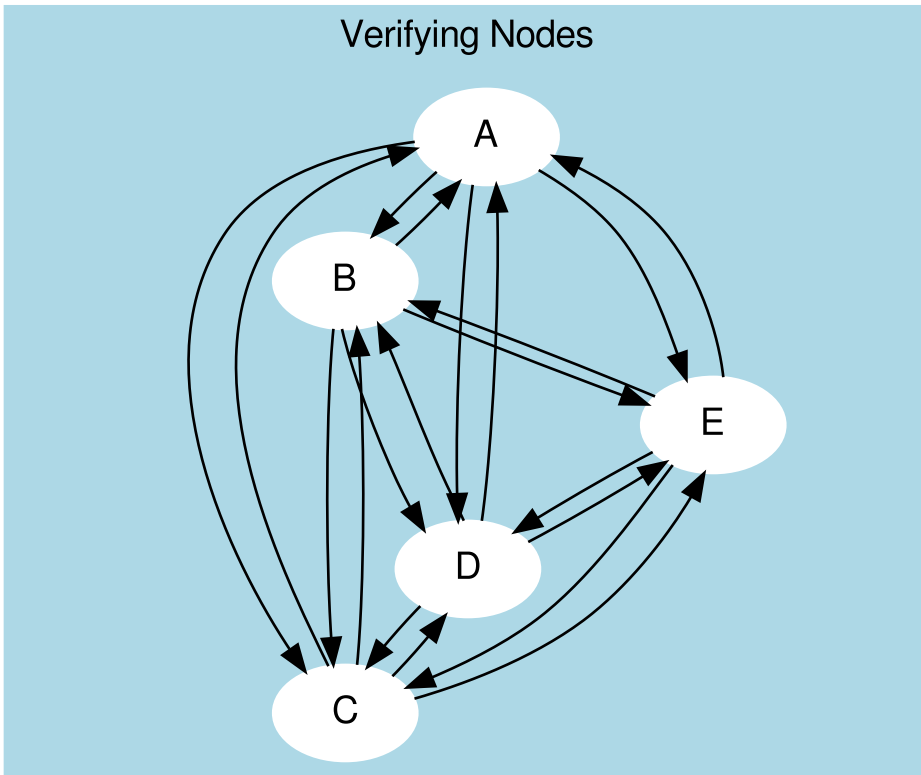
This requires a user to connect a client key (used to sign their requests) with a registered server. Clients are able to share keys as long as the owner of the node is able to ensure their security. This makes it possible to use one key for the same mobile app or device. The owner may also register as many keys as they want for their server or even change them from time to time (as long as only one client key points to one server). The key is registered in a client-contract, holding a mapping of the key to the server address.



18.4 Ensuring Client Access

Connecting a client key to a server does not mean the key relies on that server. Instead, the requests are simply served in the same quality as the connected node serves other clients. This creates a very strong incentive to deliver to all clients, because if a server node were offline or refused to deliver, eventually other nodes would deliver less or even stop responding to requests coming from the connected clients.

To actually find out which node delivers to clients, each server node uses one of the client keys to send test requests and measure the availability based on verified responses.



The servers measure the $A_{availability}$ by checking periodically (about every hour in order to make sure a malicious server is not only responding to test requests). These requests may be sent through an anonymous network like tor.

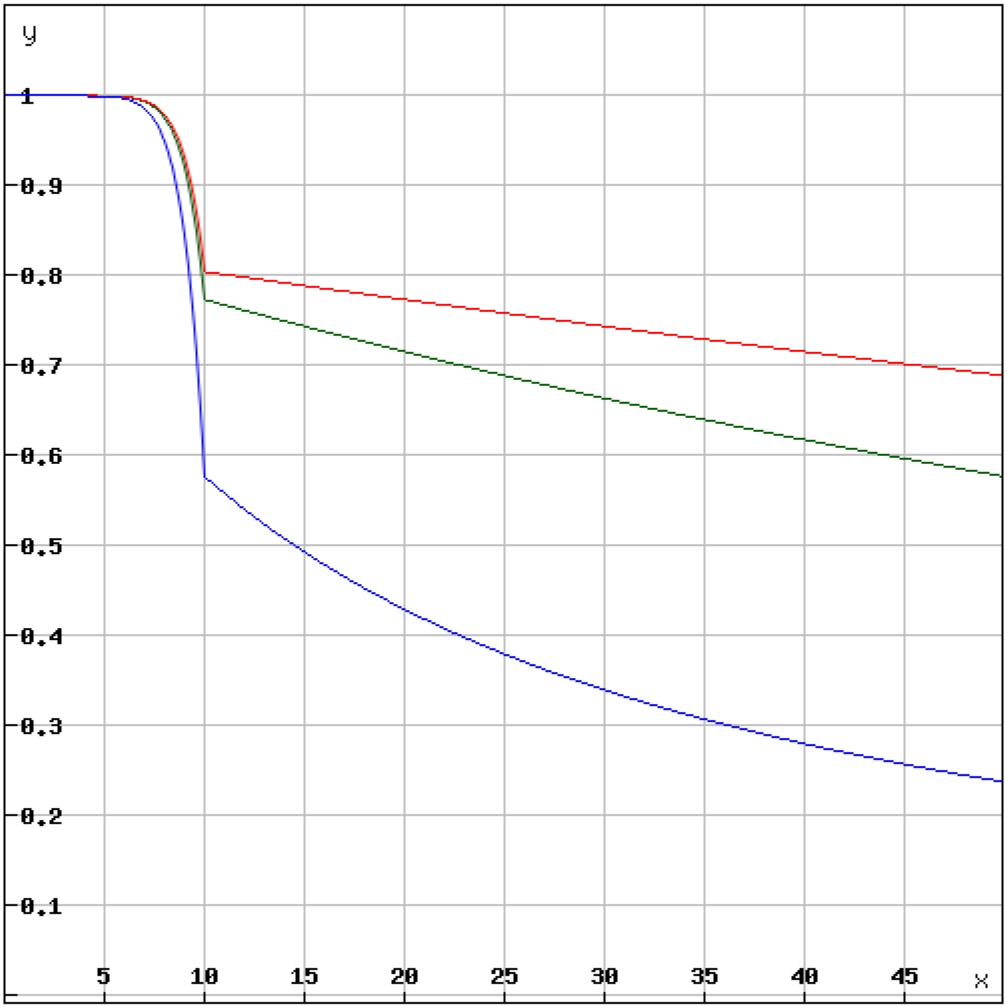
Based on the long-term (>1 day) and short-term (<1 day) availibility, the score is calculated as:

$$A = \frac{R_{received}}{R_{sent}}$$

In order to balance long-term and short-term availability, each node measures both and calculates a factor for the score. This factor should ensure that short-term avilability will not drop the score immediately, but keep it up for a while before dropping. Long-term availibility will be rewarded by dropping the score slowly.

$$A = 1 - (1 - \frac{A_{long} + 5 \cdot A_{short}}{6})^{10}$$

- A_{long} - The ratio between valid requests received and sent within the last month.
- A_{short} - The ratio between valid requests received and sent within the last 24 hours.



Depending on the long-term availibility the disconnected node will lose its score over time.

The final score is then calulated:

$$score = \frac{A \cdot D_{weight} \cdot C_{max}}{weight}$$

- A - The availibility of the node.
- $weight$ - The weight of the incoming request from that server's clients (see LoadBalancing).
- C_{max} - The maximal number of open or parallel requests the server can handle (will be taken from the registry).
- D_{weight} - The weight of the deposit of the node.

This score is then used as the priority for incoming requests. This is done by keeping track of the number of currently open or serving requests. Whenever a new request comes in, the node does the following:

1. Checks the signature.
2. Calculates the score based on the score of the node it is connected to.
3. Accepts or rejects the request.

```
if ( score < openRequests ) reject()
```

This way, nodes reject requests with a lower score when the load increases. For a client, this means if you have a low score and the load in the network is high, your clients may get rejected often and will have to wait longer for responses. If the node has a score of 0, they are blacklisted.

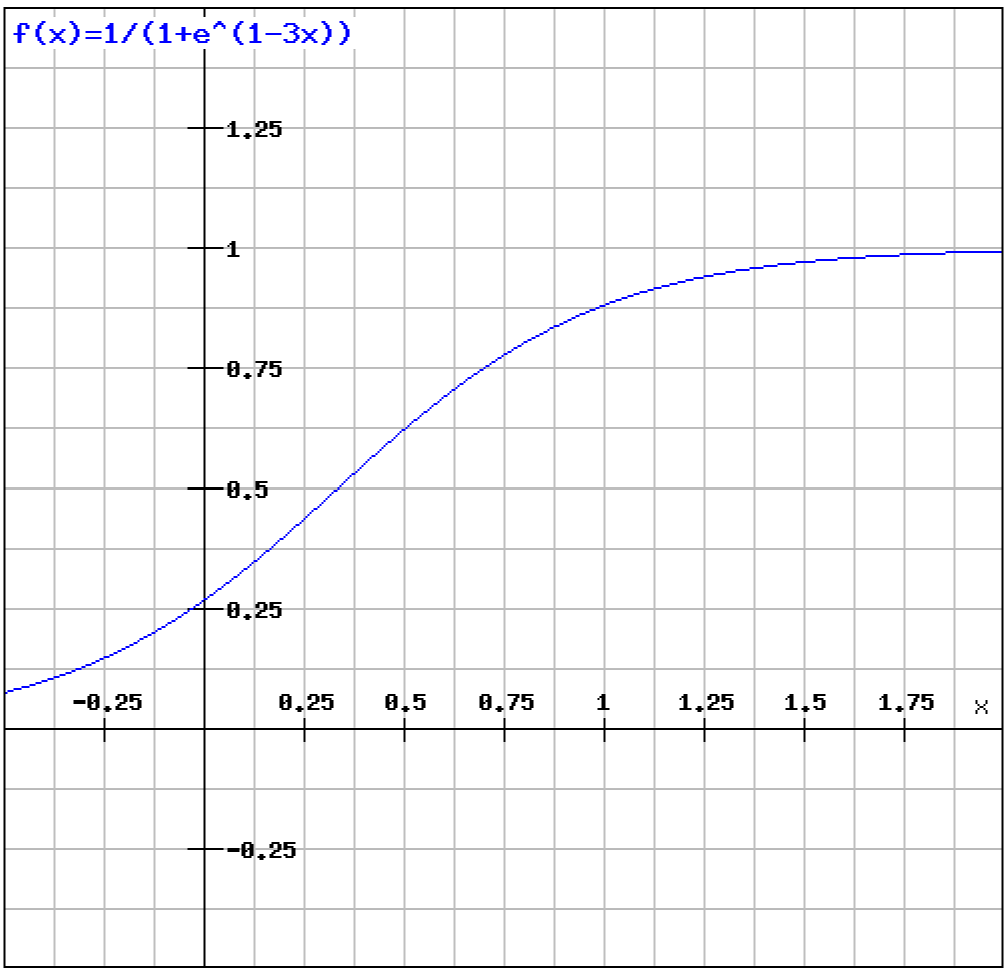
18.5 Deposit

Storing a high deposit brings more security to the network. This is important for proof-of-work chains. In order to reflect the benefit in the score, the client multiplies it with the D_{weight} (the deposit weight).

$$D_{weight} = \frac{1}{1 + e^{1 - \frac{3D}{D_{avg}}}}$$

- D - The stored deposit of the node.
- D_{avg} - The average deposit of all nodes.

A node without any deposit will only receive 26.8% of the max cap, while any node with an average deposit gets 88% and above and quickly reaches 99%.



18.6 LoadBalancing

In an optimal network, each server would handle an equal amount and all clients would have an equal share. In order to prevent situations where 80% of the requests come from clients belonging to the same node, we need to decrease the score for clients sending more requests than their shares. Thus, for each node the weight can be calculated by:

$$weight_n = \frac{\sum_{i=0}^{n} C_i \cdot R_n}{\sum_{i=0}^{n} R_i \cdot C_n}$$

- R_n - The number of requests served to one of the clients connected to the node.
- $\sum_{i=0}^{n} R_i$ - The total number of requests served.
- $\sum_{i=0}^{n} C_i$ - The total number of capacities of the registered servers.
- C_n - The capacity of the registered node.

Each node will update the $score$ and the $weight$ for the other nodes after each check in order to prioritize incoming requests.

The capacity of a node is the maximal number of parallel requests it can handle and is stored in the ServerRegistry. This way, all clients know the cap and will weigh the nodes accordingly, which leads to stronger servers. A node declaring a high capacity will gain a higher score, and its clients will receive more reliable responses. On the other hand, if a node cannot deliver the load, it may lose its availability as well as its score.

18.7 Free Access

Each node may allow free access for clients without any signature. A special option `--freeScore=2` is used when starting the server. For any client requests without a signature, this $score$ is used. Setting this value to 0 would not allow any free clients.

```
if (!signature) score = conf.freeScore
```

A low value for freeScore would serve requests only if the current load or the open requests are less than this number, which would mean that getting a response from the network without signing may take longer as the client would have to send a lot of requests until they are lucky enough to get a response if the load is high. Chances are higher if the load is very low.

18.8 Convict

Even though servers are allowed to register without a deposit, convicting is still a hard punishment. In this case, the server is not part of the registry anymore and all its connected clients are treated as not having a signature. The device or app will likely stop working or be extremely slow (depending on the freeScore configured in all the nodes).

18.9 Handling conflicts

In case of a conflict, each client now has at least one server it knows it can trust since it is run by the same owner. This makes it impossible for attackers to use blacklist-attacks or other threats which can be solved by requiring a response from the "home"-node.

18.10 Payment

Each registered node creates its own ecosystem with its own score. All the clients belonging to this ecosystem will be served only as well as the score of the ecosystem allows. However, a good score can not only be achieved with a good performance, but also by paying for it.

For all the payments, a special contract is created. Here, anybody can create their own ecosystem even without running a node. Instead, they can pay for it. The payment will work as follows:

The user will choose a price and time range (these values can always be increased later). Depending on the price, they also achieve voting power, thus creating a reputation for the registered nodes.

Each node is entitled to its portion of the balance in the payment contract, and can, at any given time, send a transaction to extract its share. The share depends on the current reputation of the node.

$$payment_n = \frac{weight_n \cdot reputation_n \cdot balance_{total}}{weight_{total}}$$

Why should a node treat a paying client better than others?

Because the higher the price a user paid, the higher the voting power, which they may use to upgrade or downgrade the reputation of the node. This reputation will directly influence the payment to the node.

That's why, for a node, the score of a client depends on what follows:

$$score_c = \frac{paid_c \cdot requests_{total}}{requests_c \cdot paid_{total} + 1}$$

The score would be 1 if the payment a node receives has the same percentage of requests from an ecosystem as the payment of the ecosystem represented relative to the total payment per month. So, paying a higher price would increase its score.

18.11 Client Identification

As a requirement for identification, each client needs to generate a unique private key, which must never leave the device.

In order to securely identify a client as belonging to an ecosystem, each request needs two signatures:

1. **The Ecosystem-Proof**This proof consists of the following information:

```
proof = rlp.encode(
   bytes32(registry_id),       // The unique ID of the registry.
   address(client_address),    // The public address of a client.
   uint(ttl),                  // Unix timestamp when this proof expires.
   bytes(signature)            // The signature with the signer-key of the␣
↪ecosystem. The message hash is created by rlp.encode, the client_address, and␣
↪the ttl.
)
```

For the client, this means they should always store such a proof on the device. If the ttl expires, they need to renew it. If the ecosystem is a server, it may send a request to the server. If the ecosystem is a payer, this needs to happen in a custom way.

2. **The Client-Proof**This must be created for each request. Here the client will create a hash of the request (simply by adding the `method`, `params` and a `timestamp`-field) and sign this with its private key.

```
message_hash = keccack(
   request.method
   + JSON.stringify(request.params)
   + request.timestamp
)
```

With each request, the client needs to send both proofs.

The server may cache the ecosystem-proof, but it needs to verify the client signature with each request, thus ensuring the identity of the sending client.

CHAPTER 19

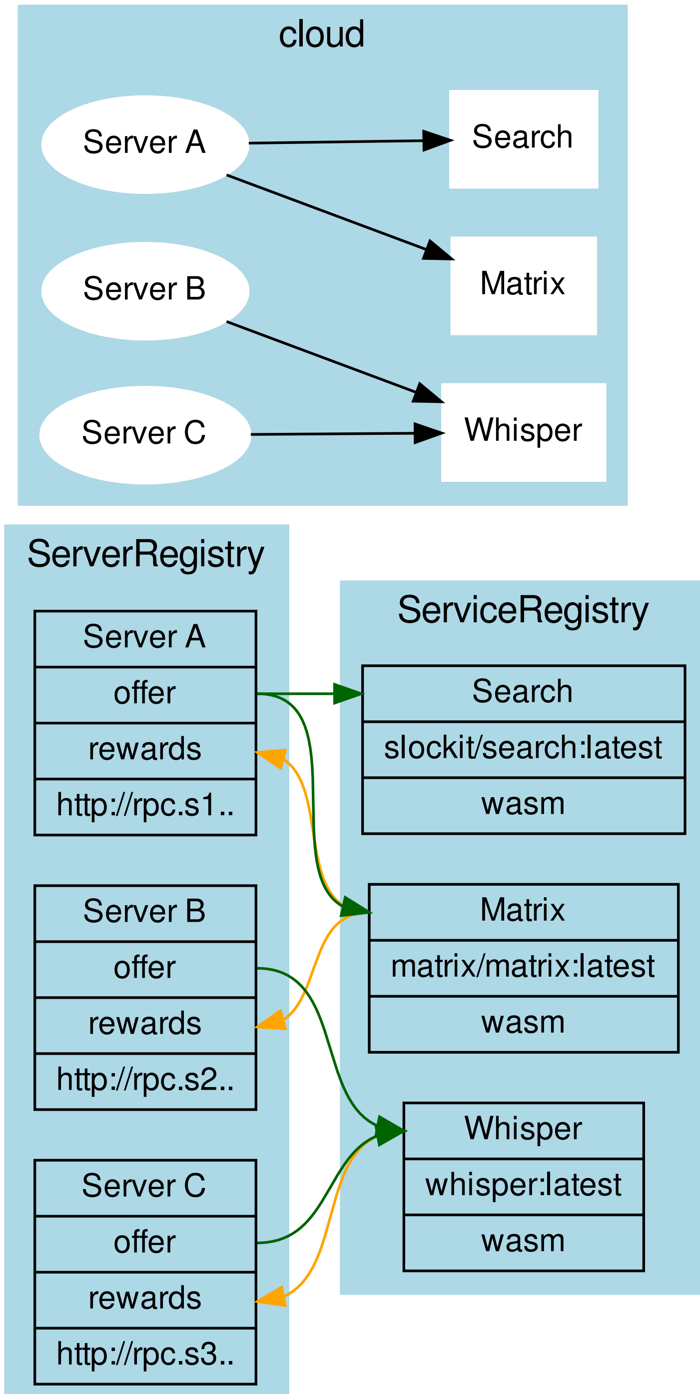
Decentralizing Central Services

Important: This concept is still in early development, meaning it has not been implemented yet.

Many dApps still require some off-chain services, such as search services running on a server, which, of course, can be seen as a single point of failure. To decentralize these dApp-specific services, they must fulfill the following criteria:

1. **Stateless**: Since requests may be sent to different servers, they cannot hold a user's state, which would only be available on one node.
2. **Deterministic**: All servers need to produce the exact same result.

If these requirements are met, the service can be registered, defining the server behavior in a docker image.


cloud
Server A
Search
Server B
Matrix
Server C
Whisper
ServerRegistry
Server A
offer
rewards
http://rpc.s1..
Server B
offer
rewards
http://rpc.s2..
Server C
offer
rewards
http://rpc.s3..
ServiceRegistry
Search
slockit/search:latest
wasm
Matrix
matrix/matrix:latest
wasm
Whisper
whisper:latest
wasm

19.1 Incentivization

Each server can define (1) a list of services to offer or (2) a list of services to reward.

The main idea is simply the following:

> **If you run my service, I will run yours.**

Each server can specifiy which services we would like to see used. If another server offers them, we will also run at least as many rewarded services as the other node.

19.2 Verification

Each service specifies a verifier, which is a Wasm module (specified through an IPFS hash). This Wasm offers two functions:

```
function minRequests():number

function verify(request:RPCRequest[], responses:RPCResponse[])
```

A minimal version could simply ensure that two requests were running and then compare them. If different, the Wasm could check with the home server and "convict" the nodes.

19.2.1 Convicting

Convicting on chain cannot be done, but each server is able to verify the result and, if false, downgrade the score.

CHAPTER 20

Threat Model for Incubed

20.1 Registry Issues

20.1.1 Long Time Attack

Status: open

A client is offline for a long time and does not update the NodeList. During this time, a server is convicted and/or removed from the list. The client may now send a request to this server, which means it cannot be convicted anymore and the client has no way to know that.

Solutions:

> CHR: I think that the fallback is often "out of service." What will happen is that those random nodes (A, C) will not respond. We (slock.it) could help them update the list in a centralized way.
>
> But I think the best way is the following: Allow nodes to commit to stay in the registry for a fixed amount of time. In that time, they cannot withdraw their funds. The client will most likely look for those first, especially those who only occasionally need data from the chain.
>
> SIM: Yes, this could help, but it only protects from regular unregistering. If you convict a server, then this timeout does not help.
>
> To remove this issue completely, you would need a trusted authority where you could update the NodeList first. But for the 100% decentralized way, you can only reduce it by asking multiple servers. Since they will also pass the latest block number when the NodeList changes, the client will find out that it needs to update the NodeList, and by having multiple requests in parallel, it reduces the risk of relying on a manipulated NodeList. The malicious server may return a correct NodeList for an older block when this server was still valid and even receive signatures for this, but the server cannot do so for a newer block number, which can only be found out by asking as many servers as needed.
>
> Another point is that as long as the signature does not come from the same server, the DataProvider will always check, so even if you request a signature from a server that is not part of the list anymore, the DataProvider will reject this. To use this attack, both the DataProvider and the BlockHashSigner must work together to provide a proof that matches the wrong blockhash.

CHR: Correct. I think the strategy for clients who have been offline for a while is to first get multiple signed blockhashes from different sources (ideally from bootstrap nodes similar to light clients and then ask for the current list). Actually, we could define the same bootstrap nodes as those currently hard-coded in Parity and Geth.

20.1.2 Inactive Server Spam Attack

Status: partially solved

Everyone can register a lot of servers that don't even exist or aren't running. Somebody may even put in a decent deposit. Of course, the client would try to find out whether these nodes were inactive. If an attacker were able to onboard enough inactive servers, the chances for an Incubed client to find a working server would decrease.

Solutions:

1. **Static Min Deposit**

   There is a min deposit required to register a new node. Even though this may not entirely stop any attacker, but it makes it expensive to register a high number of nodes.

   Desicion :

   Will be implemented in the first release, since it does not create new Riscs.

2. **Unregister Key**

   At least in the beginning we may give us (for example for the first year) the right to remove inactive nodes. While this goes against the principle of a fully decentralized system, it will help us to learn. If this key has a timeout coded into the smart contract all users can rely on the fact that we will not be able to do this after one year.

   Desicion :

   Will be implemented in the first release, at least as a workaround limited to one year.

3. **Dynamic Min Deposit**

   To register a server, the owner has to pay a deposit calculated by the formula:

   $$deposit_{min} = \frac{86400 \cdot deposit_{average}}{(t_{now} - t_{lastRegistered})}$$

   To avoid some exploitation of the formula, the `deposit_average` gets capped at 50 Ether. This means that the maximum `deposit_min` calculated by this formula is about 4.3 million Ether when trying to register two servers within one block. In the first year, there will also be an enforced deposit limit of 50 Ether, so it will be impossible to rapidly register new servers, giving us more time to react to possible spam attacks (e.g., through voting).

   Desicion :

   This dynamic deposit creates new Threads, because an attacker can stop other nodes from registering honest nodes by adding a lot of nodes and so increasing the min deposit. That's why this will not be implemented right now.

4. **Voting**

   In addition, the smart contract provides a voting function for removing inactive servers: To vote, a server has to sign a message with a current block and the owner of the server they want to get voted out. Only the latest 256 blockhashes are allowed, so every signature will effectively expire after roughly 1 hour. The power of each vote will be calculated by the amount of time when the server was registered. To make sure that the oldest servers won't get too powerful, the voting power gets capped at one year and won't increase further. The server being voted out will also get an oppositional voting power that is capped at two years.

For the server to be voted out, the combined voting power of all the servers has to be greater than the oppositional voting power. Also, the accumulated voting power has to be greater than at least 50% of all the chosen voters.

As with a high amount of registered in3-servers, the handling of all votes would become impossible. We cap the maximum amount of signatures at 24. This means to vote out a server that has been active for more then two years, 24 in3-servers with a lifetime of one month are required to vote. This number decreases when more older servers are voting. This mechanism will prevent the rapid onboarding of many malicious in3-servers that would vote out all regular servers and take control of the in3-nodelist.

Additionally, we do not allow all servers to vote. Instead, we choose up to 24 servers randomly with the blockhash as a seed. For the vote to succeed, they have to sign on the same blockhash and have enough voting power.

To "punish" a server owner for having an inactive server, after a successful vote, that individual will lose 1% of their deposit while the rest is locked until their deposit timeout expires, ensuring possible liabilities. Part of this 1% deposit will be used to reimburse the transaction costs; the rest will be burned. To make sure that the transaction will always be paid, a minimum deposit of 10 finney (equal to 0.01 Ether) will be enforced.

Desicion:

Voting will also create the risc of also Voting against honest nodes. Any node can act honest for a long time and then become a malicious node using their voting power to vote against the remaining honest nodes and so end up kicking all other nodes out. That's why voting will be removed for the first release.

20.1.3 DDOS Attack to uncontrolled urls

Status: not implemented yet

As a owner I can register any url even a server which I don't own. By doing this I can also add a high weight, which increases the chances to get request. This way I can get potentially a lot of clients to send many requests to a node, which is not expecting it. Even though clients may blacklist this node, it would be to easy to create a DDOS-Atack.

Solution:

Whenever there is a new node the client has never communicated to, we should should check using a DNS-Entry if this node is controlled by the owner. The Entry may look like this:

```
in3-signer: 0x21341242135346534634634,0xabf21341242135346534634634,
↪0xdef21341242135346534634634
```

Only if this DNS record contains the signer-address, the client should communicate with this node.

20.1.4 Self-Convict Attack

Status: solved

A user may register a mailcious server and even store a deposit, but as soon as they sign a wrong blockhash, they use a second account to convict themself to get the deposit before somebody else can.

Solution:

> SIM: We burn 50% of the depoist. In this case, the attacker would lose 50% of the deposit. But this also means the attacker would get the other half, so the price they would have to pay for lying is up to 50% of their deposit. This should be considered by clients when picking nodes for signatures.

Desicion: Accepted and implemented

20.1.5 Convict Frontrunner Attack

Status: solved

Servers act as watchdogs and automatically call convict if they receive a wrong blockhash. This will cost them some gas to send the transaction. If the block is older than 256 blocks, this may even cost a lot of gas since the server needs to put blockhashes into the BlockhashRegistry first. But they are incentivized to do so, because after successfully convicting, they receive a reward of 50% of the deposit.

A miner or other attacker could now wait for a pending transaction for convict and simply use the data and send the same transaction with a high gas price, which means the transaction would eventually be mined first and the server, after putting so much work into preparing the convict, would get nothing.

Solution:

Convicting a server requires two steps: The first is calling the `convict` function with the block number of the wrongly signed block `keccak256(_blockhash, sender, v, r, s)`. Both the real blockhash and the provided hash will be stored in the smart contract. In the second step, the function `revealConvict` has to be called. The missing information is revealed there, but only the previous sender is able to reproduce the provided hash of the first transaction, thus being able to convict a server.

Desicion: Accepted and implemented

20.2 Network Attacks

20.2.1 Blacklist Attack

Status: partially solved

If the client has no direct internet connection and must rely on a proxy or a phone to make requests, this would give the intermediary the chance to set up a malicious server.

This is done by simply forwarding the request to its own server instead of the requested one. Of course, they may prepare a wrong answer, but they cannot fake the signatures of the blockhash. Instead of sending back any signed hashes, they may return no signatures, which indicates to the client that the chosen nodes were not willing to sign them. The client will then blacklist them and request the signature from other nodes. The proxy or relay could return no signature and repeat that until all are blacklisted and the client finally asks for the signature from a malicious node, which would then give the signature and the response. Since both come from a bad-acting server, they will not convict themself and will thus prepare a proof for a wrong response.

Solutions:

1. **Signing Responses**

   SIM: First, we may consider signing the response of the DataProvider node, even if this signature cannot be used to convict. However, the client then knows that this response came from the client they requested and was also checked by them. This would reduce the chances of this attack since this would mean that the client picked two random servers that were acting malicious together.

   Decision:

   Not implemented yet. Maybe later.

2. **Reject responses when 50% are blacklisted**

   If the client blacklisted more than 50% of the nodes, we should stop. The only issue here is that the client does not know whether this is an 'Inactive Server Spam Attack' or not. In case of an 'Inactive Server Spam Attack,' it would actually be good to blacklist 90% of the servers and still be able to work with the remaining 10%, but if the proxy is the problem, then the client needs to stop blacklisting.

CHR: I think the client needs a list of nodes (bootstrape nodes) that should be signed in case the response is no signature at all. No signature at all should default to an untrusted relayer. In this case, it needs to go to trusted relayers. Or ask the untrusted relayer to get a signature from one of the trusted relayers. If they forward the signed reponse, they should become trusted again.

SIM: We will allow the client to configure optional trusted nodes, which will always be part of the nodelist and used in case of a blacklist attack. This means in case more than 50% are blacklisted the client may only ask trusted nodes and if they don't respond, instead of blacklisting it will reject the request. While this may work in case of such a attack, it becomes an issue if more than 50% of the registered nodes are inactive and blacklisted.

Decision:

The option of allowing trusted nodes is implemented.

20.2.2 DDoS Attacks

Status: solved (as much as possible)

Since the URLs of the network are known, they may be targets for DDoS attacks.

Solution:

SIM: Each node is reponsible for protecting itself with services like Cloudflare. Also, the nodes should have an upper limit of concurrent requests they can handle. The response with status 500 should indicate reaching this limit. This will still lead to blacklisting, but this protects the node by not sending more requests.

CHR: The same is true for bootstrapping nodes of the foundation.

20.2.3 None Verifying DataProvider

Status: solved (more signatures = more security)

A DataProvider should always check the signatures of the blockhash they received from the signers. Of course, the DataProvider is incentivized to do so because then they can get 50% of their deposit, but after getting the deposit, they are not incentivized to report this to the client. There are two scenarios:

1. The DataProvider receives the signature but does not check it.

   In this case, at least the verification inside the client will fail since the provided blockheader does not match.

2. The DataProvider works together with the signer.

   In this case, the DataProvider would prepare a wrong blockheader that fits the wrong blockhash and would pass the verification inside the client.

Solution:

SIM: In this case, only a higher number of signatures could increase security.

20.3 Privacy

20.3.1 Private Keys as API Keys

Status: solved

For the scoring model, we are using private keys. The perfect security model would register each client, which is almost impossible on mainnet, especially if you have a lot of devices. Using shared keys will very likely happen, but this a nightmare for security experts.

Solution:

1. Limit the power of such a key so that the worst thing that can happen is a leaked key that can be used by another client, which would then be able to use the score of the server the key is assigned to.
2. Keep the private key secret and manage the connection to the server only off chain.
3. Instead of using a private key as API-Key, we keep the private key private and only get a signature from the node of the ecosystem confirming this relationship. This may happen completly offchain and scales much better.

Desicion: clients will not share private keys, but work with a signed approval from the node.

20.3.2 Filtering of Nodes

Status: partially solved

All nodes are known with their URLs in the NodeRegistry-contract. For countries trying to filter blockchain requests, this makes it easy to add these URLs to blacklists of firewalls, which would stop the Incubed network.

Solution:

> Support Onion-URLs, dynamic IPs, LORA, BLE, and other protocols. The registry may even use the props to indicate the capabilities, so the client can choose which protocol to he is capable to use.

Decision: Accepted and prepared, but not fully implemented yet.

20.3.3 Inspecting Data in Relays or Proxies

For a device like a BLE, a relay (for example, a phone) is used to connect to the internet. Since a relay is able to read the content, it is possible to read the data or even pretend the server is not responding. (See Blacklist Attack above.)

Solution:

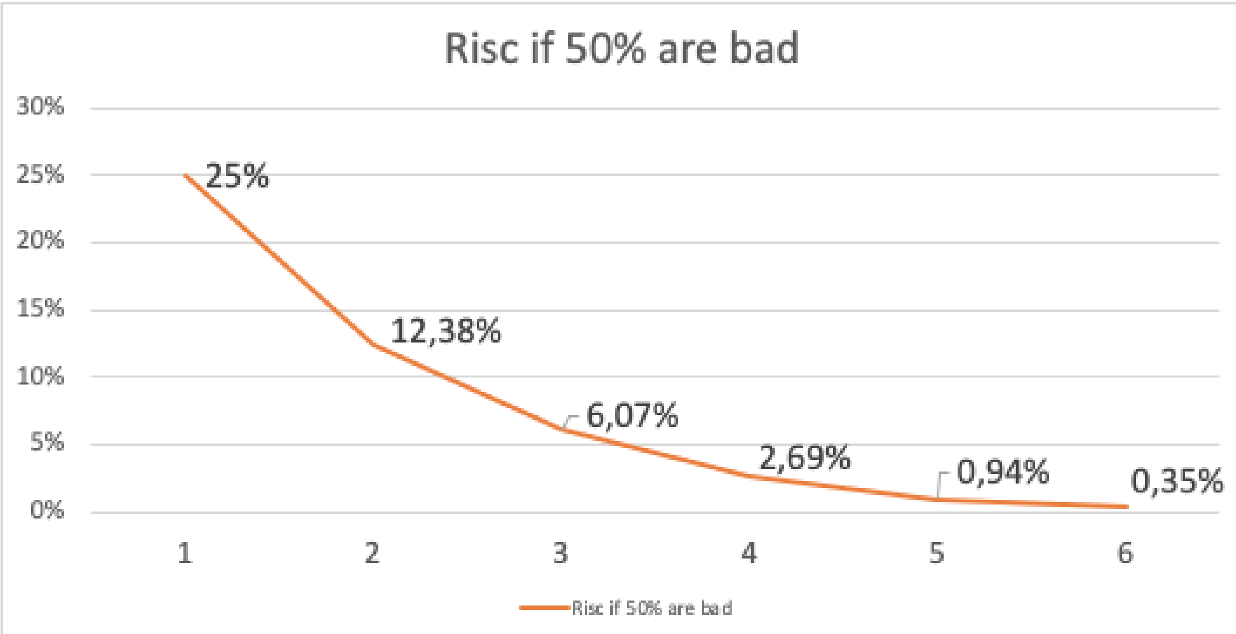
> Encrypt the data by using the public key of the server. This can only be decrypted by the target server with the private key.

20.4 Risk Calculation

Just like the light client there is not 100% protection from malicious servers. The only way to reach this would be to trust special authority nodes to sign the blockhash. For all other nodes, we must always assume they are trying to find ways to cheat.

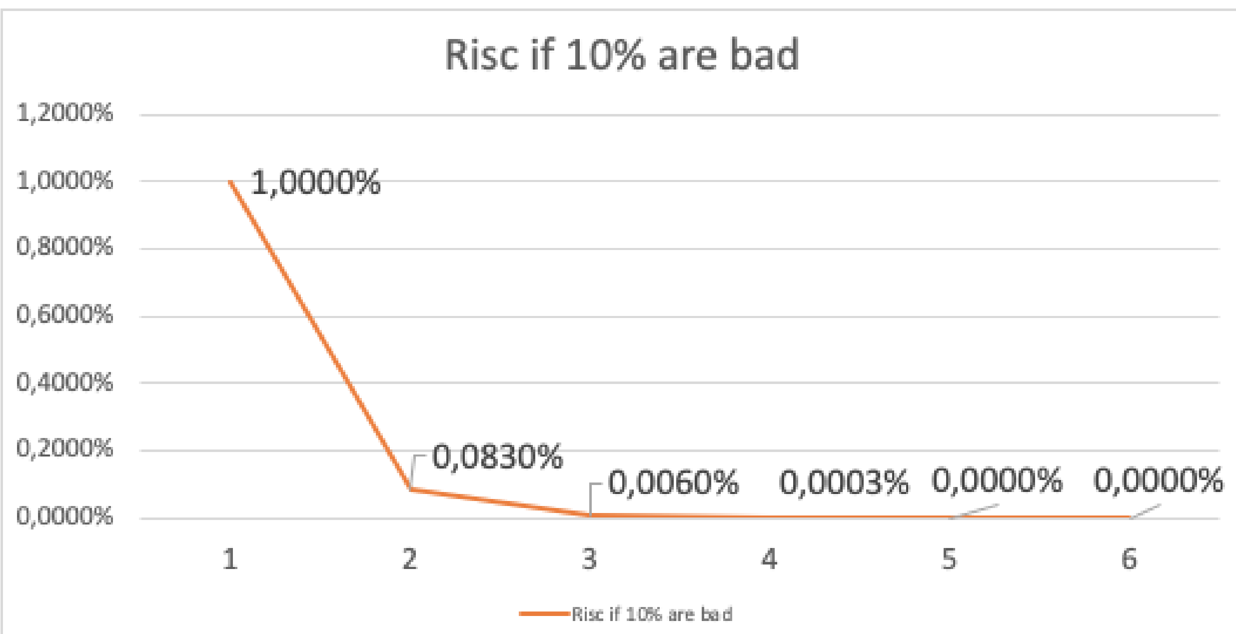
The risk of losing the deposit is significantly lower if the DataProvider node and the signing nodes are run by the same attacker. In this case, they will not only skip over checks, but also prepare the data, the proof, and a blockhash that matches the blockheader. If this were the only request and the client had no other anchor, they would accept a malicious response.

Depending on how many malicious nodes have registered themselves and are working together, the risk can be calculated. If 10% of all registered nodes would be run by an attacker (with the same deposit as the rest), the risk of getting a malicious response would be 1% with only one signature. The risk would go down to 0.006% with three signatures:



50% bad

In case of an attacker controlling 50% of all nodes, it looks a bit different. Here, one signature would give you a risk of 25% to get a bad response, and it would take more than four signatures to reduce this to under 1%.



10% bad

Solution:

> The risk can be reduced by sending two requests in parallel. This way the attacker cannot be sure that their attack would be successful because chances are higher to detect this. If both requests lead to a different result, this conflict can be forwarded to as many servers as possible, where these servers can then check

the blockhash and possibly convict the malicious server.

- genindex

Index

Symbols

<JSON-RPC>-method, **388**

A

abi_decode <signature> data, **388**
abi_encode <signature> ...args, **388**

C

call <signature> ...args, **388**
Code, **389**
createkey, **389**

E

ecrecover <msg> <signature>, **389**

I

IN3_CHAIN, **388**
in3_nodeList, **388**
IN3_PK, **388**
in3_sign <blocknumber>, **388**
in3_stats, **388**

K

key <keyfile>, **389**

N

NodeLists, **389**

P

pk2address <privatekey>, **388**
pk2public <privatekey>, **388**

R

Reputations, **389**

S

send <signature> ...args, **388**
sign <data>, **388**

V

Validators, **389**