US - PUBLIC SYSTEM (USPS)

other.arkitech 2017-2020

Running version: **alpha-22 481bd8fd3d85e61f1ec5be37572dc2f47b23e40b81cdb7ae1797e35c7f782c51 2020-05-08**

Main-net:	Nodes	Accounts	Software:	Release notes	Setup instructions Linux / Windows	OS Image Raspberry Pi

TL; DR;

A multi-coin platform with enhanced trading capabilities. For the shake of privacy and self-managed societies.

Overview

An anonymous distributed P2P system based on a flat organization of nodes contributing to secure a database in a way that:

The Public System

- No central authority can control it, decide to perform successful amendments, take over the network or shut it down. It is censorship resistant.
- The database can be only updated per address or account providing cryptographic proof of ownership of such address.
- Nodes can be inexpensive computers, starting from a raspberry pi. They have a negligible energy and bandwidth consumption.
- Scales up to 100 Billion nodes. Under such enormous deployment the global network will consist of 1.000.000 sub-networks (or clusters) of 10.000 nodes each. Each network takes care of 1 millionth of the address space.
- Is cooperative rather than competitive. The network achieves consensus using a tailored implementation of a Byzantine Fault Tolerant algorithm which is very lightweight and efficient. It is implemented in such a way that a form of universal salary is achieved, because all cooperating nodes doing validation work are paid every consensus cycle, which is variable depending on the network load and configured to be a minimum of 1 minute.
- Anyone can access, participate, send transactions, earn cryptocurrency by running a node anonymously from home. Anonymous participation solves every major discrimination problem in our current society.
- It is borderless and neutral. It doesn't care about countries (those territorial structures invented in ancient times) and any transaction can go from anyone to anyone. This is a tool for the electronic world. 1 world, 100B people.
- It is NOT immutable. Immutability is considered harmful to privacy. In other words the system does not preserve old data, the blockchain is not a blockchain, is only the last block, the current state. While Bitcoin and the rest of blockchains preserve the trajectory, USPS only cares about the last trusted state and forgets the previous one. Indeed you can trust a new state provided you trust the previous plus the algorithm that computes the

next from the previous. This paradigm improves:

  - The efficiency of the system, helping to be run in inexpensive hardware.
  - The size of the database grows at a considerably slower pace than other systems. The growth across time can actually be zero if no new accounts were created.
  - Avoid the most critical event any blockchain will suffer in the future. It will happen in the future, the cypher-suite will be compromised. Any data stored in any immutable blockchain will be broken. In USPS, upgrading the cypher-suite is a non-brainer.
- All nodes are the same, There are no roles (validator, coordinator, ...) none of it. Just nodes with validation responsibilities executing the consensus algorithm.
- The security increases with the number of nodes, because one node means 1 vote. To take over the network (51% attack) an attacker must incorporate as many colluding nodes as needed to convince the rest that the evil hash of the next block created maliciously has been voted as the legitimate block by a majority.
- Sybil attack is prevented by using the convenient scarcity of network addresses offered by the protocol IPv4. The network is programmed to control the number of nodes operating behind a given IPv4 address. Any extra nodes above a programmed threshold will be ignored when it comes to voting, providing a limit for which an attacker instantiating thousands of node processes from a single machine does not harm the network. When the network is big enough, an attacker planning a Sybil attack would have to run nodes from a large pool of IPv4 addresses, limiting their chances given the difficulty and price to obtain such type of addresses.
- Users can create their own coins, and manage their own cryptoeconomic laws of supply/inflation/deflation.
-

The Private System

- Nodes form a parallel network of P2P encrypted interactions running tailored trading protocols designed to automate the private economy. These R2R (Role-to-Role, a new name specializing the term P2P) protocols can be installed as plugins of the wallet.
- Enables total control on the way and context your private data can be exchanged. Allows to run negotiators that care about your self interests, scanning data, interviewing other nodes in search of opportunities, chatting, watching video and an unlimited range of activities, including politics why not.
- Multiple trades can be performed in parallel with or without human intervention.

Values

- Designed for Global Privacy: Financial, Identity, Medical records,
- Multiple anonymous personalities can be developed by a single person, or by a group of people. It does not matter who is/are behind a personality. What matters is what this individual/group/company does.
- Free software. Complete sources with reproducible builds will soon be published for public review.
- 100% Decentralized. Decentralization is a process and has different sides. Although the resiliency model is already decentralized the governance of the system is not yet. Once the software is fully tested by alpha testers, as soon as the beta version started getting traction the governance decentralization process will begin. The idea is to create a skilled community of developers and interested parties that shall be distributed and non colluding. The power to rule the system will be transferred from other.arkitech to such big structure organized by skill where anyone could form part.
- Safe. Nodes are controlled and maintained by their respective owners, who are root.

During the period when source code is not available the only potential risk that a user may care of is the network activity of the node. Whether or not it tries to scan maliciously the local LAN, or which other sites it connects to. The node can be put in an isolated v-LAN, for those concerned. The node, must be said forefront, does not scan the LAN at all, and the connections to the outside are to other nodes that are listed here . It is easy for anyone with networking skills to verify this is true monitoring the traffic from inside the node using standard Linux tools, or from the outside using network traffic analyzers like wireshark. Those who demand open source would need to wait until the sources are released, probably as GPL, before the release of version 1.0.

Description of the system.

- The software is being written in C++ std17 since February 2017, when this project was envisaged for the first time. See release_notes for a chronological sequence. See also codebase stats.
- Designed for Debian/Raspbian GNU/Linux. Presumably, it can be adapted to other GNU/Linux distributions, FreeBSD, NetBSD or other alike OS with little effort.
- Components
  - libusgov.so - The governance library. Implements the public system protocol.
  - libuswallet.so - The trader library. Implements the private system. Plugin architecture where R2R protocols for different purposes can be easily added or removed.
  - us-gov - The command-line program runs either as the protocol daemon or as an RPC client where everything regarding the public system can be monitorized and operated.
  - us-wallet - The command-line program runs either as the protocol daemon or as an RPC client where everything regarding the private system can be monitorized and operated. Integrates a shell to create new or operate ongoing R2R trades. It can create and sign cryptocurrency transactions that are broadcasted through the public system.
  - us-walletj - RPC client similar to the RPC mode of us-wallet written in java.
  - wallet-SDK in various languages. Java, c#. More languages will be appended to this list. Particularly WASM. Complex applications can be built using the SDK.
  - Android App - Example of application using the java SDK.
- Software updates are pulled from the other foundation account 4NwEEwnQbnwB7p8yCBNkx9uj71ru

Main-net

The main-net has been running since October 2018. See the nodes. It is distributed across the world, run by people that I've 'persuaded' one by one. The mostly see it as an amazing technological experiment that has huge potential with little cost. A good investment.

The Name

The name US comes after the notion of WE as a society. Apologies for the misleading resemblance to other structures like the United States of America, which is completely unrelated.

It was set up as a codename at the beginning of the project with the intention to change it before releasing to public. This haven't happened yet. The definitive name will be set before 1.0 release

Test it

I'd be delighted if you decide to form part of the genesis of this network. The cryptocurrency earned for the mere act of contributing to secure the network accumulates in your wallet each minute. If the value of the system grows with time, your wealth might be positively affected, let's desire it.

To get started, spare a raspberry pi 3B+ or higher with 16Gb SDCard or higher and an Ethernet cable and follow the setup steps (see link above)

Any issue or question send me an email. Thank you.

other.arkitech[at]protonmail[dot]com