THE UNBREAKABLE CODE

NAVTECH DECENTRALISATION WHITEPAPER

BETA RELEASE v0.9

INDEX

EXECUTIVE SUMMARY

Cryptocurrency technology is decentralised by design. It is believed that rigorous truth is a natural byproduct of an open source platform run by the public. The decentralisation and automation of systems enable people to make informed choices about the systems in which they choose to participate and provides an even playing field as never seen before in history.

As well as the inherently democratic nature of decentralised systems, they offer protection to the participants by providing a safety in numbers hypothesis. This limits the ability of malicious actors to threaten or attack participants in the system due to the number of people involved and the global nature of their relationships.

Another advantage is that they are extremely robust. Once a piece of software has entered the public domain, it becomes impractical and virtually impossible to shut down completely. This enables security to the future of the system and knowledge that if the public deems it valuable it will persist.

INTRODUCTION

Decentralization is the means of distributing, powers, people or things away from a central location or authority.

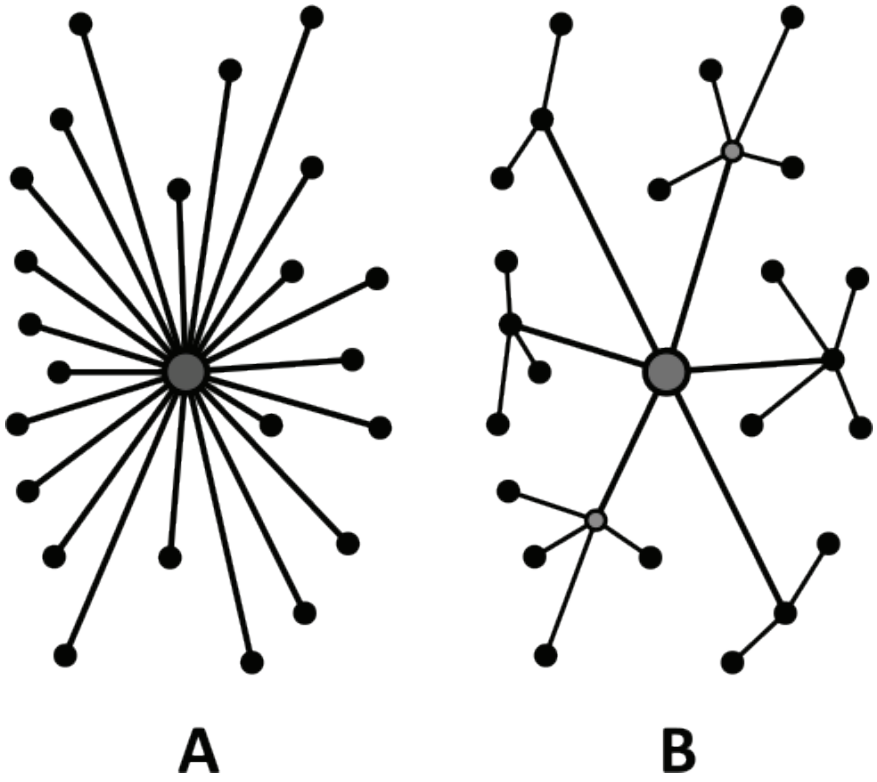


Image by Kes47 (?) [CC BY-SA 3.0 (http://creativecommons.org/licenses/by-sa/3.0)], via Wikimedia Commons

We want no central management, and no central point of failure.

Systems run by specific people, in specific locations, with specific computer systems, are susceptible to government interference, coercion, legal issues and more.

This document describes how Nav Coin can operate as a self sustaining entity. Open source code, freely distributed, with systems in place that reward and facilitate trust. Users will be free to use and operate the network in the way they think best.

PROBLEM DEFINITION

The Navtech system employs the best features of decentralised technology with some extra safety and privacy-centric network design features. The dual block-chain system, as outlined in the Navtech Whitepaper, acts as the data backbone and does not rely on any centralised systems like databases to operate.

Although the dual blockchains are decentralised, the scripts which process trans-actions have to be run on a public facing web server. This is a single network point referenced by an IP address. The processing scripts of the Navtech system are managed and maintained by a single entity; The Nav Coin Development Team.

Despite the reliance of the Nav Coin Development Team, we designed the old system to be extremely hard to shut down. We run the system on multiple servers using different service providers based in various countries. We store the pro-cessing scripts on GitHub and have backup copies scattered around the world. We store backups of the subchain and processing servers wallet files. Everything needed to restore the system has multiple backups stored on multiple continents.

If a malicious actor tried to take down the Navtech system, we could have new servers up and running in a matter of hours with minimal losses. However, this still relies on the Nav Coin Development Team being available to set up the new servers. Until now, this has meant we are the single point of failure in the Navtech system.

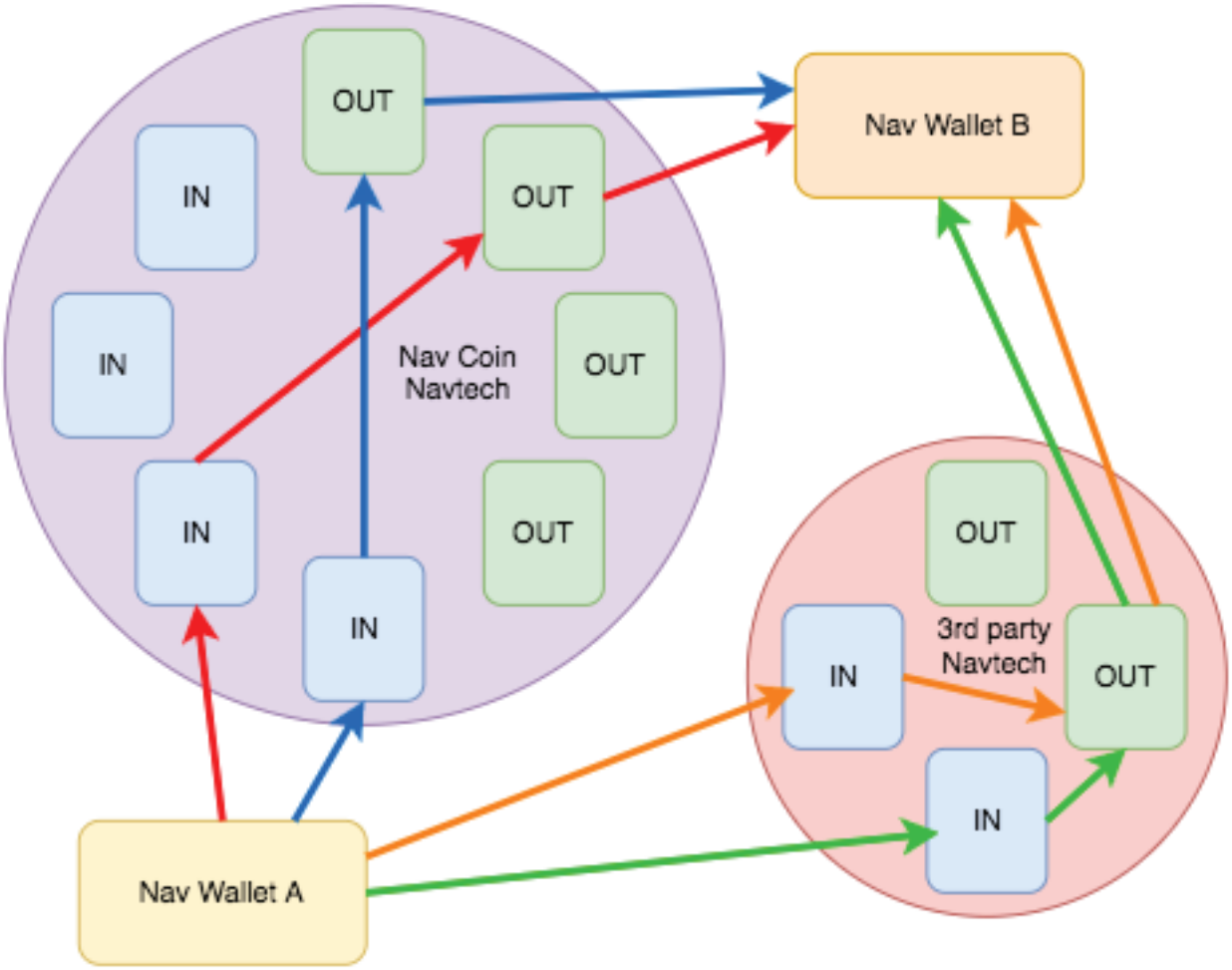
HIGH LEVEL SOLUTION

At a high level, the solution to the issue of the Nav Coin Development Team being the single point of failure for the Navtech system is simple. We decentralise the administration of the Navtech network by making the subchain and processing scripts publicly available and operational.

In creating a viable solution, there are of course many security concerns which need to be addressed before independent operators can run their own Navtech systems. These will be outlined in the Solutions Detail chapter of this document.

The primary technique for resolving most of the security concerns is to limit interactions between servers to within trusted clusters. This way, we are able to have multiple public or private clusters setup and users can choose which entities they interact with.

Figure 1.1 How Navtech Transactions travel through the network.



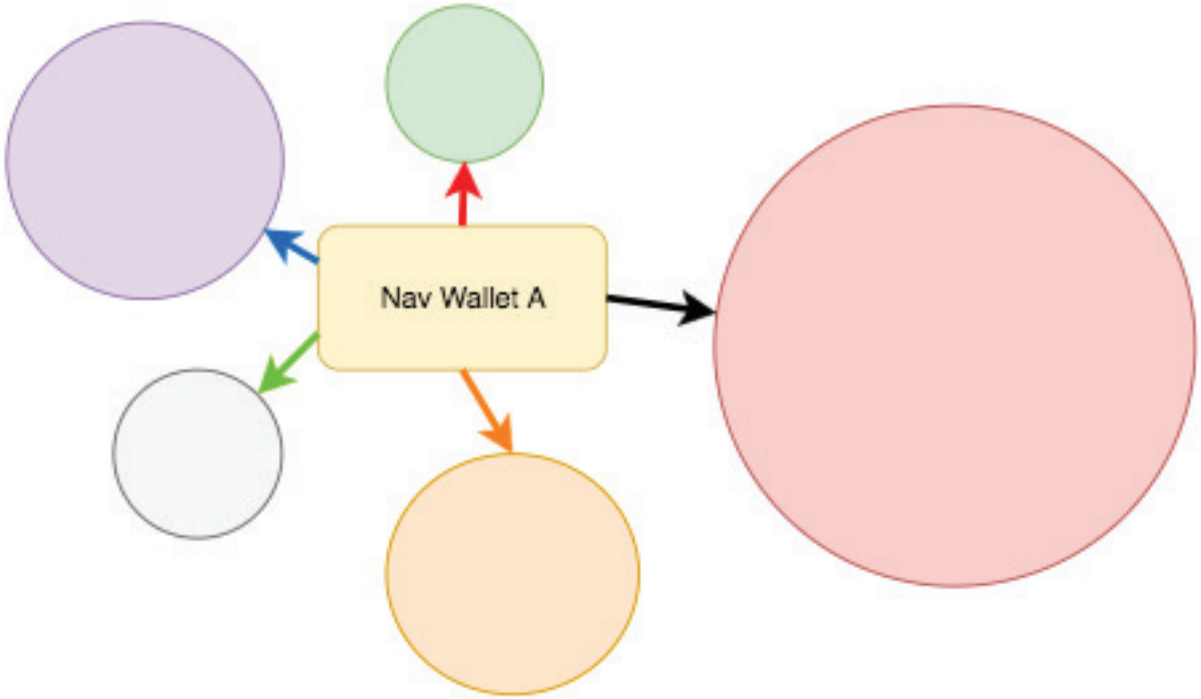
Wallet A is configured to use two Navtech Clusters. The diagram shows 4 transactions (red, blue, orage and green) and possible paths they could take through the network.

HIGH LEVEL SOLUTION

Users will have the option to use official Nav Coin Navtech Servers, switch completely to a 3rd party service or use a mixture of servers. In the later case, the software will randomly pick which network the transaction goes through.

Each cluster will have a public rating; users can upvote / downvote the cluster as well as leave feedback. This feedback and rating system will alert other users to possible scams, long wait times, high fees or hopefully the reliable service they received.

Figure 1.2 Wallet Connecting to Multiple Clusters



Wallet A can connect to as many Navtech clusters as desired. When an anonymous transaction is created the wallet will randomly pick which endpoint to use

HIGH LEVEL SOLUTION

When designing solutions we weren't looking to redesign the wheel. We looked at how existing technologies have overcome similar problems and implemented familiar solutions eg.

When using Tor, users are able to specify which nodes they use. In turn, the nodes are able to restrict themselves to operate in clusters. This eliminates the risk of using unknown Tor nodes who might be and often are logging data or performing other malicious behaviours. This was our major inspiration to opt for a cluster system over an open mesh.

MD5 hashes are used by Bitcoin and many other software providers to validate file integrity. This is the method which we have implemented to assure users that the software a cluster is using hasn't been modified.

Public voting mechanisms and lists are often used to host important public information and it is entirely possible to duplicate this information anywhere on the web.

CORE TECHNICAL OBSTACLES

Before discussing the detailed solution, it is important to understand the core technical obstacles which it is trying to solve.

SAFE DISTRIBUTION OF THE SUBCHAIN

With the subchain publicly available, it would be possible for a malicious actor to gain access to subchain coins and send intentionally incorrect instructions to an outgoing server in an attempt to extract Nav Coins from the system which they never introduced.

Servers are designed to act on the Subchain's instructions and treat them as a source of truth. Because of this, if a user can somehow figure out the receiving addresses of an outgoing servers subchain and send transactions to it, then it would be possible to attempt to instruct the server to send Nav Coins from the pool to an address which is specified by the attacker.

PROTECTING USERS FROM MALICIOUS SERVER OPERATORS

When we allow unknown members of the public to become a Navtech Server operators, we are faced with the possibility that a server operator may be malicious.

The system accrues incoming transactions and then processes them every two minutes in blocks. This gives a window for a malicious server operator to shut down their server before the pending funds have been processed and steal the Nav Coins which have been input.

As well as the possibility of stealing pending Nav Coins, it would be possible for a malicious server operator to monitor or record transactions sent through their servers.

CORE TECHNICAL OBSTACLES

GIVING THE END USER CONTROL

Using any system such as this relies upon some level of trust between the operators and the users. Users have to trust that the service operator isn't recording their information and that the funds will reach their intended destination.

Whenever there is trust needed in a system, it is imperative to give the power of choice back to the user. Without choice, there is no control, and without control, there shouldn't be any trust. In a decentralised world, this control should extend to the point where users can set and use their own systems and not rely on third parties at all.

SOLUTION DETAILS

OVERVIEW

The Navtech Whitepaper 2016 covers a lot of the technical details for solving the problems posed by decentralisation. Since that paper is describing only one cluster of servers, we will mainly be looking at how multiple servers work together and what protections against the core technical obstacles are in place.

The main security method employed to protect the system from malicious activity is forming servers into trusted clusters who transact with each other.

Servers which are in the same cluster share multiple layers of security features to stop unwanted transactions occurring.

IP RESTRICTION

In the configuration of each server in the cluster designated as accepting “incoming” transactions, there is a list of the IP addresses of all the servers designated as sending “outgoing” transactions. This is the list each incoming server uses to look up and communicate with a random outgoing server when it processes transactions.

Each of the outgoing Servers also have a list of the IP addresses of all the servers in the cluster designated as incoming. When an incoming server queries an outgoing server for the credentials required to create a valid subchain transaction, the outgoing server will reject any requests from servers who are not on its whitelist.

IP restriction is a very secure method of stopping unwanted people accessing the outgoing servers. Even if a malicious actor were to forge their IP address to match one of our incoming servers and make a request for credentials, the outgoing server would send the response to the IP which was forged, eg. our incoming server. The malicious actor would never get their response as the ISP would route the traffic back to the correct incoming server IP.

There is no IP restriction on the incoming servers unless it is in scheduled maintenance mode. The reason for this is their API needs to be open to communicate with NAV wallets from any potential IP address. It is also only the outgoing servers which have a pre-loaded pool of NAV which has the potential to be extracted, so they are the only part of the system which needs to be protected in this way.

SOLUTION DETAILS

RSA ENCRYPTION

When the incoming server attempts to process transactions and communicates with the outgoing server, first it must past the IP restriction tests as outlined above. If the request comes from a whitelisted IP address, the outgoing server will send the incoming server its public RSA encryption key.

When the subchain transaction is made, the amount, address and secret are encrypted with this public key and the transaction is committed to the block chain. When the outgoing server receives a subchain transaction, it will attempt to decrypt the transaction information and if it was unsuccessful, it will return the SUB to wherever it was sent from.

As well as hiding the information submitted to the subchain from public view, this encryption has a dual purpose.

Since it is only possible to get this public key via the IP restricted outgoing server's API, only legitimate subchain transactions from whitelisted incoming server IP addresses will be processed by the outgoing server.

SECRET TOKEN

When the first incoming server in a cluster is setup, it will generate a 42 character token. This token (or one of the same length you generate yourself) is added to the configuration file for all incoming and outgoing servers in the cluster.

When the subchain transaction is made, this secret is combined with the amount and address, then encrypted with the outgoing servers public key and committed to the block chain.

When the outgoing server decrypts the subchain transaction, the secret that's attached must match the secret that the outgoing server has in its configuration file otherwise it will return the SUB to wherever it was sent from.

Apart from being baked into the RSA encrypted subchain transaction (which is considered impossible to decode even with today's best supercomputers), the secret is never broadcast from any server in the cluster. This means there should be no way for anyone to have access to it and according to howsecureismypassword.net a secret of this length would take 143 vigintillion years to brute force.

SOLUTION DETAILS

The secret token is like an ultra paranoid failsafe. With the IP restriction in place a malicious actor should never be able to request an outgoing server's public key, but if they somehow were able to get access to that API endpoint, this secret token would make it impossible to extract NAV from an outgoing server which was outside of your trusted cluster.

NAVTECH SERVER WHITELIST

Each user gets to decide which incoming servers they add to their wallet configuration file. If you've been using the system already, this means you will have added the Official Navtech Incoming servers to your wallet config. When a service operator setups a cluster of Navtech servers which you want to use, you are able to also add their servers to your wallet config. There is no limit to how many you can add and each Navtech transaction your wallet makes it will choose a server one from the list.

NAVTECH SERVER MD5 HASH

As well as being able to add incoming servers to your configuration file, you will be able to specify a Navtech hash which you consider to be genuine. This is the hash output of the server processing scripts when they have been minified. When your wallet requests to make a transaction to an incoming server it will ask the server to hash it's currently running file and the server will return it as part of the response. If the hash the server returns doesn't match the hash you have specified as genuine, then your wallet will notify you that the server it contacted appears to have different source code than expected and you should remove it from your list. Also, it won't proceed with the transaction.

The reason why the hash is user specified and not baked into the wallet is because the project is open source. If a user wants to set up their own cluster and modify the source code to work in a slightly different way, then we don't want to lock that person out of doing that. They will have a different hash to the official source code, but they will be able to add that hash to their configuration file and their wallet will operate correctly.

Also, this allows us to put out updates and simply post a new hash for people to use rather than forcing a wallet download each time we update the Navtech source.

SOLUTION DETAILS

One thing to note is that checking the hash isn't fool proof. It would be possible for a malicious actor to modify the code to simply return a hardcoded copy of the correct hash whenever a request was made. The hash should not be used as an absolute proof the source is genuine.

PUBLIC LISTING AND VOTING ON CLUSTERS

Allowing public methods for network operators to list their servers is essential. The Nav Coin Team can not be responsible for curating the list if we are to remove ourselves as a single point of failure. Currently the server listings will be hosted through the Navtech subreddit:

https://reddit.com/r/NavtechAnon

Only posts containing server addresses, fees and hashes will be allowed. Users can use voting and commenting to alert people to the quality of the service they received with particular providers.

PUBLIC SOURCE CODE

When the system is decentralised, the source code for both the Navtech processing scripts and the Subchain will be available to the public from our Nav Coin github account:

https://github.com/navcoindev

This allows people to inspect the code we have written, set up their own servers, fork their own versions, contribute to the code base or whatever else can be imagined.

TECHNICAL BENEFITS

The solution details outlined provide a very high level of security to the Navtech system as well as confidence to the end user.

Due to the fact that servers operate in private clusters, there is virtually no point for a malicious actor to attempt to extract NAV from the Navtech network. If the network operated as one large mesh with no boundaries, it is impossible for a user to have confidence their NAV will make it out the other end because they would have no control of who was processing their coins.

The largest attack vector of sending subchain transactions to an outgoing server in an attempt to extract NAV from their pre-loaded pool has been patched.

With the user input server addresses and MD5 hashing, users can be confident they know the servers they are transacting with and have some assurances about the software running on those servers.

The community server lists and the public github source gives the guardianship of the system over to the public and truly decentralises the Navtech system.

As with any system, there is some trust involved in using our Official Navtech servers or any of the 3rd party listings. The beauty of open source software is that it provides tiers of trust which users can subscribe to. Easy to use options often entail more trust, but low level solutions are also provided for the paranoid.

If you trust our servers and the highest rated 3rd party servers, then you can add them all to your wallet config and your wallet will randomly choose which provider to use.

If you only trust the Official Navtech servers then you can continue to use only those servers which we guarantee will be running the exact source available on our github account.

If you don’t trust the Official Navtech servers (or any 3rd party servers), you can download our Navtech and Subchain source, setup your own Navtech servers and list only them in your wallet config file.

If you don’t trust our source, you can fork it or write your own source and process payments however you like using our subchain.

These layers of control truly allow the end user to be the master of their own fate when it comes to protecting their financial privacy.

BUSINESS BENEFITS AND FUTURE GROWTH

Any server operators who sets up a Navtech cluster will be able to specify the percentage fee which is charged when a user makes a transaction through their network. This provides a revenue stream for the operator and will help cover the costs of maintaining their network.

The operator can also specify the maximum value a user can send in a single transaction and how many servers they run in their cluster.

This allows for a wide range of systems to operate.

From a high end solution with hundreds of servers and high transaction limits, to a single server pair designed for personal use, to private clusters which only accept coins from whitelisted addresses. The possibilities are endless.

We will continue to provide the Official Navtech servers for as long as we are able, but we will also actively encourage and engage with competitors and alternative operators.

We also hope that open sourcing the project will encourage other people to contribute to the project and we are excited to see how the technology is used and applied in the future.

SUMMARY

KEY BENEFITS

Using these security measures, operators can safely run their Navtech servers without fear of having their pre-filled pool of NAV stolen by a malicious actor.

Users can confidently choose which operators they transact with.

The Nav Coin Development team removes themselves as the single point of failure.

RISKS

If you're using 3rd party servers there will always be the risk of malicious server operators. It is something which can't be avoided. However we hope that with the methods we have implemented, the community will weed them out quickly and the hassle will outweigh any small gains which they might make.

CONCLUSION

Used correctly, the Navtech System should be extremely safe to use and offer an unparalleled level of financial privacy. We have overcome all the core technical obstacles which have arisen when presented with the challenge to decentralise the system. When resolving challenges we have implemented solutions which have been tried and tested in parallel fields of interest rather than attempting to redesign the wheel.

We are confident that the Navtech Anon System can be decentralised in a way that is safe, secure and open.

http://navcoin.org
http://twitter.com/NAVCoin
http://facebook.com/NAVCoin
http://reddit.com/r/NAVCoin
http://reddit.com/r/NavtechAnon