NAVAJOCOIN

The Unbreakable Code

NAVAJO “COIN” ANONYMOUS TECHNOLOGY

Decentralized anonymity through double Encryption

Presented By:
The Developer Services of the
NavajoCoin Foundation
13th July, 2014

Abstract

Optional Decentralized Anonymity in cryptocurrency is a feat yet to be achieved. It would provide the ultimate union between transparency/verifiability and today's much sought after privacy. To achieve ODA, we will be introducing a new concept to cryptocurrencies which we will call SubChains and whose application is to be stretched far beyond anonymity. Sub-chains are partial chains that still depend on and are verified along the main chain but are not essential to the running of the main network and therefore an individual node's involvement in a subchain is optional. They are the plugins/add-ons/extensions of the blockchain!

1 | 0 | 0 | Introduction

Bitcoin along with many other cryptocurrencies of its generation have revolutionized the world of today. Though very few are aware of its potential and future applications, the decentralized consensus ledger is a solid basis for applications beyond our imaginations.

During the past year, the light was shed on the criminal activities of various governments around the world which involved illegal and abusive mass surveillance and data collection. The cryptoworld was deeply struck by this revelation and started rooting for coin functions that would insure their right to both financial and communication privacy.

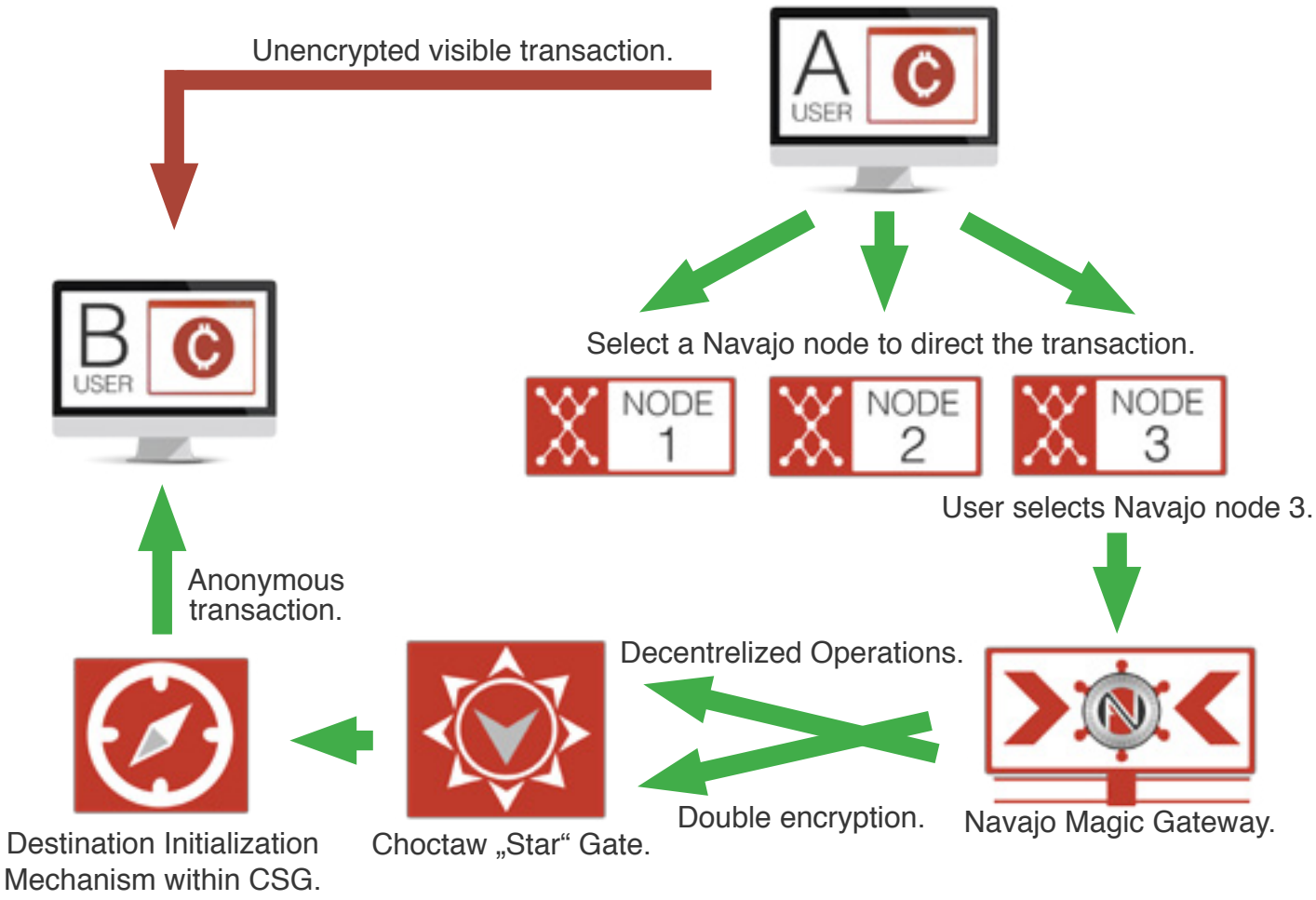
Bitcoin and other cryptocurrencies based on its protocol have a transparent block chain which is the equivalent of a public ledger. With this implementation, your privacy is protected only as far as your link with an address. Today, with the presence of exchanges and other services that require your personal identification, keeping your identity separate from your coins is proving to be an impossible feat.

New coins emerged and on the financial privacy scale centralized mixers appeared, followed by decentralized mixers and a new blockchain technology based around anonymity called Cryptonote. Zerocoin is also a major contender in the anonymity race and a highly anticipated technology. Each have been criticized for their weaknesses with the centralized mixer obviously being the weakest as it has a single point of failure. Decentralized mixers actually do not offer anonymity and blockchain analysis can mathematically link (no direct link in the blockchain) addresses. Another weakness lies in the fact that anyone, especially at a coins infancy age where it is cheap, can acquire a majority of the mixing nodes and have a full visibility of the supposedly anon transactions along with irrefutable blockchain proof. To summarize, mixers of any kind only obfuscate transactions. Cryptonote is majorly criticized for its blockchain bloat which limits its scalability along with its inability to offer transparency but offers a solid basis for anonymity. Zerocoin offers the greatest privacy but offers zero transparency and in the case of being compromised, no one will know. This is both a scary and impractical truth for an economy on which thousands or millions depend.

Thereby in this whitepaper we would like to introduce a completely unique state-of-the-art anonymous technology. Its use of decentralized nodes, a subchain, and double encryption right from the nodes guarantees true anonymity while still maintaining the option of having fully transparent transactions and in no way bloating the backbone of the system (main chain). The inputs and outputs will be in such a manner that the origin of the transaction as well as the recipient cannot be correlated, linked to one another, or be traced on the block chain as there will be no evidence on it. This technology will therefore be implemented in the next NavajoCoin Wallet Version which will be released on the 9th of March 2015.

1 I 1 I 0 I Navajo Anonymous Technology Whitepaper Infographics

This System is a Hybrid Crypto System and is a hybrid of with Centralized and Decentralized Operations.



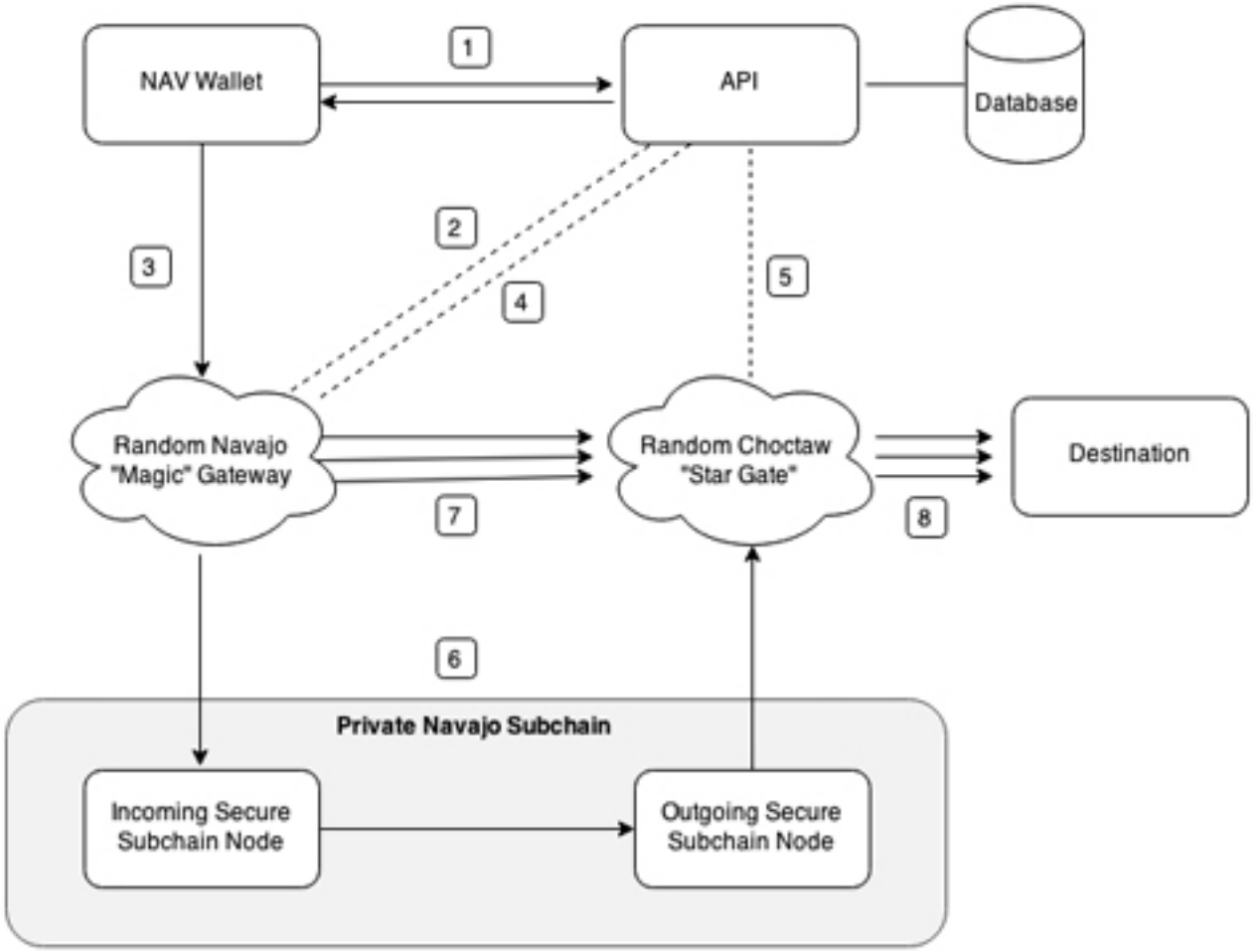
1I A random node will be selected from the online nodes to direct the transaction through.

2I This will be the beginning of the anonymous transaction phase.

3I The technologies discussed here are highly anonymous in nature thus you will experience a real sense of Anonymity.

4I The nomenclature of the above technologies are provided for anyone to identify them when needed and Navajo „Magic“ Gateway and Choctaw „Star“ Gate are a decentralized part of the network.

1 | 2 | 0 | Navajo Anonymous Technology Whitepaper Infographics Dataflow



1. The Navajocoin wallet talks to the Navajo API and asks for a random Navajo Magic Gateway (NMG) send NAV through anonymously.
2. The API finds a random NMG, checks that it is running and able to process incoming anonymous transactions, then sends the chosen NMG's details back to the wallet.
3. The wallet sends the coins to the random NMG with the encrypted destination information attached.
4. The incoming NMG node talks to the API and asks for a random Choctaw Star Gate (CSG) to send the coins out to the destination.
5. The API finds a random CSG, checks that it is running and able to process outgoing anonymous transactions, then sends its details back to the NMG.
6. The destination address is decrypted then re-encrypted with a new key and sent through the private Navajo Subchain.
7. The NMG strips the destination information from the incoming transaction, mixes the coins with other pending transactions and sends the Navajo coins to the CSG in a series of small, randomized transactions to further obfuscate their route.
8. The CSG node receives the subchain transaction and decrypts the destination address from the transaction. The CSG then sends out the correct amount of Navajocoins to its intended destination in a series of small randomized transactions.

2 | 0 | 0 | Transactions

2 | 1 | 0 | Visible and Transparent Transactions

These transactions are sent the same way as any bitcoin transaction. The coins are sent from the sender's wallet directly to the receiver's address and are fully visible and verifiable on the blockchain.

2 | 2 | 0 | Anonymous Transactions

2 | 2 | 1 | Transaction Origin

In order to conduct an anonymous transaction, the wallet will need to select a node through which the transaction will be channeled, present the recipient's address, and get into Navajo mode through an available GUI button. The nodes are decentralized, and as transaction volume grows, more nodes will be added.

2 | 2 | 2 | The Node

When a transaction is received at the Anonymizing node, the destination information is encrypted by a cryptographic hash function and then that information is broadcasted through the subchain to instruct the outgoing node where to send the NAV funds. The node is the gateway to the subchain.

2 | 2 | 3 | Navajo Magic Gateway (NMG) & Choctaw Star Gate (CSG)

The NMG and CSG are the most important part of the entire operation and work in conjunction. They run on an independent subchain and are of course fully decentralized. The NMG is the decryption mechanism and the CSG is the gateway back to the main chain.

The NMG receives the encrypted transaction information that only includes the destination address and the amount, decrypts it, then re-encrypts it with another public key and relays it to the CSG through the subchain. The CSG receives the subchain transaction, decrypts the destination information and verifies the transaction integrity before broadcasting the final transaction on to the main chain; sending the coins to its recipient address in smaller, random denominations.

2 | 2 | 5 | Recipient

The recipient will receive the respective amount of coins intended to be sent to their destination address, therefore completing the transaction and thus the coins in no way can be traced back to the original address through any analysis of the Block Chain / Public Ledger, the subchain or in any other way. What appears on the main blockchain is a transaction with a destination and amount only and without an origin.

2 | 2 | 6 | Anonymity

The Coins received in this manner are in no way traceable to the original and there will never exist documented proof on either chain linking any addresses. To counter the type of analysis where one would just look for similar amounts we have mixed and then split the transactions into a smaller random denominations.

2 | 2 | 7 | Latency

The efficiency of the system plays an important role in evaluating this system. It takes 3 confirmations all within the network for the coins to be sent and received using the anonymous technology therefore there are no disadvantages of using the technology against the conventional sending and receiving of coins between two addresses.

2 | 2 | 8 | Node Maintenance

The nodes will be decentralized, but to begin with they will be maintained by the Navajo Coin Foundation. We are working to find a secure way that we could distribute the code for users to setup their own nodes, while still being able to guarantee the integrity of the Anonymous Network.

3 I 0 I 0 I Further applications of the Subchain Technology

3 I 1 I 0 I Anon Wallet Messaging

Previously we released the Navajo Chat Client which features group chat and private messaging as well as username reservation and recovery. While already encrypted, will be migrating all this communication to being conducted over SSL. The next feature we're working on will be an anonymous, decentralized messaging system that runs on the main network. The idea being that it will allow users to share information by broadcasting encrypted messages using a decentralised subchain in the same manner that the transactions are conducted. We consider the messaging system to be another backbone of other subchain features we plan on releasing.

The on Wallet Messaging service will have its own subchain which will act as a register of nicknames. Nicknames will be tied to addresses instead of having passwords. An available balance will also be required to chat. The reason for this is to prevent spam and abuse of the system. Since the system is decentralized, banning someone is in effect not possible. However, we have come up with a feature where each node is able to ban/stop listening to a nickname for a specified period of time or forever. If all the network does the same, then the user is as good as banned.