Scroda: Bringing True Privacy to a Decentralized Exchange

Through the Introduction of a Non-Distributed Singular Ledger and The Removal of Third Parties

Christian Liz-Fonts

NonDistributed@gmail.com

March 28, 2018

Abstract

Satoshi Nakamoto had to release Bitcoin as a Distributed Ledger because it needed to be since at the time of its creation there was no Decentralized Virtual Machine created to be able to store and secure the Ledger in. For this reason there is a Consensus Mechanism to validate the transactions that partake in the Distributed Ledger. After the creation of Ethereum or the First Decentralized Virtual Machine the concept of a Distributed Ledger was not to be needed anymore as a Secured Environment was finally created to be able to store the Ledger in. It can be said that Ethereum blindly followed the use of the Distributed Ledger and any/all Blockchains using a distributed ledger after the creation of a Decentralized Virtual Machine is also blindly following this concept. For this reason no Cryptocurrency has been able to achieve true privacy not even any current Privacy Coins out at the moment, whether it is Monero, DeepOnion or any others as they are required to mix the transactions in with others in order to be able to hide as best as possible who the true sender is. The reason being that transactions that partake in the blockchain have to be publicly broadcasted in order for users to ensure that the third parties presented in a Distributed Ledger are uploading the validated ledger in which was agreed upon and that the ledger has not been tampered or altered by these Third Parties even if they are "trustless".

Content

Introduction

Scroda is a Decentralized Exchange that focuses on Introducing True Privacy through the use of a Non-Distributed Ledger, Scroda uses no PoW, PoS or any Consensus Mechanism as there is only ever one True Ledger, this brings a enormous amounts of benefits to Decentralization that would have never been possible with a Distributed Ledger. There is no denying that the creation of a Distributed Ledger was needed at the time of the creation of Bitcoin by Satoshi Nakamoto and gave way for vast advancements in the field of Decentralization, Still it is something that has been deemed to not be needed anymore after the creation of Decentralized Virtual Machines and Decentralized Storage Networks.

Fundamentals of the Blockchain

To understand the Blockchain you have to first be able to understand the fundamentals that make the Blockchain which are/is

P2P - This is what allows for Decentralization, it is a group of Nodes who work together to create a Network.

Private/Public Keys - The Private Key being the key that gives you access to your account what makes your Identity while the Public Key is what others identify you by publicly allowing your Private Key to remain secure.

Distributed Ledger/Conensus Mechanism - The Distributed Ledger is what allows for a trustless third party, it makes sure that all the users on the Network act as one by coming to an agreement through the use of a **Concensus Mechanism** which is a Mechanism that allows for a User to win the right to upload the ledger onto the Blockchain this Ledger must be verified/validated to be true my matching more than 51% of all the Ledgers provided by other users trying to win this right, thus giving no central authority to a single user.

Timestamp - All blocks connected in the Blockchain come with a Timestamp that connects it to the previous and the future block in which makes the Ledger.

The Problems in Distributed Ledgers

A quote by IBM and HyperLedger "First, we learned that permissioned blockchain networks that require every peer to execute every transaction, maintain a ledger and run consensus can't scale very well and can't support true private transactions and confidential contracts." (Wolpert, 2016)

Hyperledger was able to take Smart Contracts out of the Blockchain and split the process down between user, still it could not get past the use of a Distributed Ledger requiring them to require a Third Party and still use a Consesus Mechanism.

Latency - One of the many problems presented in a Distributed Ledger is the time it takes to validate a block, the reason being is that all active users who partake in the participation of winning the right to upload the validated ledger must verify with all other user that they have the same file as the majority. This has been tried to be worked around by reducing the numbers of user needed to come to an agreement still a delay will always be present during the time elapesed for a mutual agreement.

Privacy - Another problem also introduced in a Distributed Ledger is privacy, the reason that true privacy can not be reached is because there always has to be a group of people validating the ledger in which transaction must be publicly broadcasted . Thus this is why there is a Block/Blockchain Explorer because everyone who uses the Blockchain has to have the ability to see all transactions that are going on in the Blockchain to maintain assurance that no wrong doing is going on by others in terms of validation.

Fees - Fees have to be present as those who verify single transactions and not a whole block are rewarded the fees present in single transaction in return for the validation.

The Solution that a Non-Distributed Ledger Provides

Latency - Since there is no one validating the Block or any third parties present in a Non-Distributed Ledger this allows for a real-time transaction period, the only reason it will not be in real time in the use of currency and be brought to merely milliseconds to a second is through the implementation set in place to restrict double transaction on currencies.

Privacy - Transactions will not be publicly broadcasted as there will be no users or third party needed to validate the ledger allowing for a truly private system to be able to take place meaning that no Block/Blockchain Explorer will be used/needed as users do not need to verify what is happening in the networking due to the trust given to Third Parties.

Fees -As there is no one verifying single transactions, this will allow for truly Feeless Transactions.

What Scroda Pride Itself in

Scroda Prides itself in being able to provide Anonymous, Untraceable, and Fungible Transactions not only to Scroda Coins but to all Cryptocurrencies accepted in our Exchange while at the same time providing a Feelees system through the use of Scroda.

How Scroda Works

Scroda Implements a Non-Distributed Ledger by being built on top of a Decentralized Virtual Machine which allows for the storage of Scroda's Ledger. Apart from Scroda using a Decentralized Virtual Machine to store its Ledger in it also creates a separate environment inside of Scroda's Decentralized Virtual Machine that allows for the storage of Scroda's own Physical Wallets that pertains to each Cryptocurrency Scroda supports. All Cryptocurrencies supported will automatically be converted to Scroda Coins and be accounted for through our system, Users wil be able to see the balance to each specified coin in which they have deposited in and be able to Withdraw, Transfer and Exchange them. By transferring all coins to Scroda Coins while at the same time accounting for them it ensures that everything that happens in Scroda stays in Scroda. Since no user has actual acess to the Ledger stored inside of Scroda's Decentralized Virtual Machine funds can only be seen going in and out of Scroda.

How Double Transactions are prevented

Double Transactions are prevented by enforcing a restriction of 1 transaction per block per user.

Rewarding Node Participants

Node Participants will be rewarded on the contribution of participating in upholding Scroda through the use of Block Rewards. Rewards will be randomly distributed to active online Node Participants ensuring that everyone gets a fair share in being able to get rewarded.

(Formula will be released at a future date.)

What Scroda Is Not!

Scroda is not a Platform such as Ethereum or Lisk in where we allow others to build inside of our Virtual Machine/Environment. All users are strictly forbidden from accessing our Decentralized Virtual Machine and/building on top of it.

What Scroda is!

Scroda is a Truly Private Decentralized Exchange featuring the first use of a Non-Distributed Ledger in a Decentralized Environment that is not controlled by a central authority or any third party. Scroda is created by all that support it while still being controlled by none through pure automation.

What Scroda is introducing

True Privacy in a Decentralized Environment

Feeless Transactions

Removal of Private Keys (TBA at a later date)

Removal of Third Parties

Real Time Transactions (Brought to Milliseconds to 1 second through restrictions placed on the transactions of Currency to prevent Double Spending.)

Fiat to Crypto/Crypto to Fiat (TBA at a later date)

Conclusion

Through the introduction of a Third Party problems will always occur even if that Third Party is not Central Authority, Even if that Third Party is a Trusless System some sort of action will have to be implemented to make sure that a Consensus is reached which is why Privacy Coins mix their transactions in with others and still are not able to reach True Privacy as all transactions have to be publicly broadcasted on the Network and Validated.

Reference List

Wolpert, J.(2016). Building a blockchain for business with Hyperledger. Retrieved from https://developer.ibm.com/tv/the-creation-of-hyperledger-fabric-v1-for-stable-blockchain-networks/