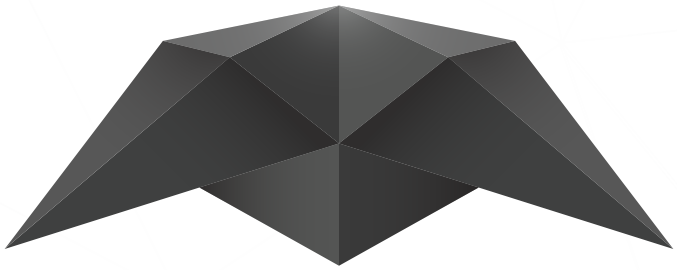

MANTA

FAST, SECURE AND PRIVATE

Purpose

In our present decade, we've been at the forefront of an economic revolution. Cryptocurrencies have brought us a game changing piece of technology.

Contrary to popular belief, the power does not side in the ability to store a currency electronically, but with the strength of data decentralization. With blockchain's bearing the crux of most Cryptocurrencies, they've exposed a significant flaw in the technology, lengthy transaction times.

Distributed Ledgers have served as the solution, allowing transactions to not rely on a long public chain, giving the speed we've always longed for. However with Distributed Ledgers, a significant problem is posed, privacy.

With Manta, we've devised a solution utilizing a combination of Distributed Ledgers and a modified implantation of zkSNARKs to bridge the strengths of both technologies. We strive to be the cutting edge with our new currency to truly change the way commerce is enacted.

Description

Private Key:

Each wallet is allotted a private key which allows access to the specified wallet upon connecting to the platform. This key allows access to funds which must be kept secret.

Public Key:

Each wallet is assigned a public key to serve as a target recipient for payments. The wallet balance is not visible on public ledger which means there are no rich lists and privacy is given.

Balances:

Each combination of a public key and private key can contain a balance of MANTA, which is derived from said combination of public and private key via its list of transactions and block associated with it. The total MANTA across all wallets will always be 133,248,290.

Distributed Ledgers:

Every wallet will contain a specific chain of transactions that work to create the 1 main ledger. This serves as a combination of sharing a large data set with each wallet serving its own non shared data as well. The distributed ledger is the main focal point of the node's, as all nodes work in conjunction to create a unified but separate ledger.

Nodes:

A node serves as a bridge between the private ledgers and the MANTA protocol to verify and modify the combined status of the ledger. Any wallets connected to a node are controlled by it, with a node requiring the private key the access and modify a wallet. To serve as a node, the node must have the full ledger of an individual wallet synched.

Implementation of privacy and deviation from the RaiBlocks protocol:

The strength and uniqueness of MANTA lies in its ability to utilize zkSNARKs, making privacy mandatory yet efficient. When a user wants to create a transaction with MANTA, a unique sub-payment address is created specifically for the transaction. The only information required to send a payment is the receiver's main wallet address.

After specifying an amount to be sent, the MANTA protocol will perform an atomic swap of MANTA to our uncollectable subcurrency, zMANTA. At this same moment, the receiver will have a sub-address specifically created for receiving the zMANTA, unique to the transaction.

The zMANTA will then be sent to the specified sub-address using a modified implementation of zkSNARKs, the privacy protocol of Zcash.

To verify and confirm a transaction, the receiver simply has to be connected to a node with their account, and will serve the appropriate POW (Proof of Work) to confirm and authenticate the transaction.

Synopsis:

- Private transactions are mandatory.
- No rich lists/ balance lookup.
- Max tx/s is 1750
- 0 fees.
- Unique currency that solves a multitude of problems.

References:

https://raiblocks.net/media/RaiBlocks_White-paper__English.pdf

http://zerocash-project.org/media/pdf/zero-cash-extended-20140518.pdf