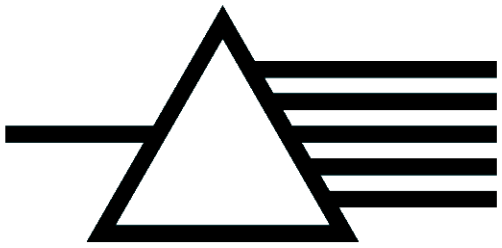
PRISM



Why

In our time, our society has 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. As current blockchain's are the backbone of many cryptocurrencies, many flaws have been present such as lengthy transaction times, lack of privacy etc.

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. With Distributed Ledgers, one of the most difficult has been the inclusion and privacy and we've designed a system to counteract this and retain this vital element.

Our goal is to be the front of the revolutionary cryptocurrency atmosphere.

Description

Smart Contract: Each transaction will be made up of a contract which can allot for data transfer if opted to. The maximum amount of usable data is 512kB per transaction.

Private Key: Every wallet contains 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 Ray, which is derived from said combination of public and private key via its list of transactions and block associated with it. The total Ray across all wallets will always be 33,554,432.

Distributed Ledgers: Every wallet will contain a specific set of transactions that 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.

Private Distributed Ledgers

Each wallet will have a secret spend and view key which is tethered to their private account which is cryptographically linked to their main account.

Ring Transactions

Each transaction has a set ring size of 11, where 10 of the transactions are not registered to the network and do not implicit any changes to values. These are verified through the private key's and hashes that are associated with each account's and they're given transactions, as well as to verify balances and prove that there is a spendable balance.

This means that the currency is fungible, and any Ray is indistinguishable from other Ray.

Summary

- Zero-fees
- Data-transmission verified and carried through smart-contracts, 512kB Data
- Private Transactions
- Untraceable Transactions
- No Public Address Balance
- First of its kind!

References

- https://content.nano.org/whitepaper/Nano_Whitepaper_en.pdf
- https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/
- https://web.getmonero.org/resources/research-lab/