Rencoin Cryptocurrency Whitepaper

Acknowledgements
Rencoin would not have been possible without the prior works of the respective Bitcoin, Peercoin, Blackcoin, Talkcoin, Dash and PIVX teams. Open source software and its contributors are constantly paving the way toward new and exciting innovations. When information and knowledge are free to build upon, society as a whole benefit. We are grateful to our predecessors for the opportunity to contribute to this growing ecosystem.

Table of Contents

Chapter 1

A Brief Introduction to Cryptocurrency

1.1 Background

In 2009, Satoshi Nakamoto released a paper entitled *Bitcoin: A Peer-to-Peer Electronic Cash System* detailing his vision of commerce. Nakamoto's vision detailed a peer-to-peer currency system backed by a hash based proof-of-work. The network would timestamp transactions by hashing them into an ongoing ledger that could not be changed without redoing the proof-of-work. Nodes would choose the longest chain as proof of events witnessed by the largest pool of hashing power. As long as ≥ 51% of the network hashing power is controlled by nodes not intending to facilitate an attack, the chain they generate will remain the longest. (Nakamoto 2009)

1.2 The Block

Each block on the network is prefaced with an 80 byte header containing a double SHA256 hashed copy of the previous block's header, merkle root (a double SHA256 hashed derivation of all the hashes that occurred in the block), the time stamp at which proof-of-work began, diffilty target this header's hash must be less-than or equal to, and the nonce at which miners reached the diffilty target. As such, any attempts to modify any transaction in any block will result in the rejection of the block by the network's miners. (Bitcoin Core Team 2017)

1.3 The Blockchain

Groups of transactions are formed into blocks and those blocks are placed chronologically into a chain - forming the blockchain. The blockchain creates a moving history of all of the activity within the network and serves as a distributed consensus model where any transaction can be verifid at any time (Crosby et al. 2015).

1.4 Proof-Of-Work

Proof-of-work is a system of verifiation in which miners must devote tangible resources (electricity, hardware costs) to solve an arbitrary probabilistic *word puzzle*. In order for a bad actor to taint the blockchain with a fraudulent transaction, they must complete all proof-of-work up to the present point. (Okupski 2016)

1.5 The problem with POW

Cryptocurrencies relying solely on the POW system are susceptible to a potential tragedy of commons. This

refers to a future point in the cryptocurrency landscape where potentially there are fewer miners available

due to little/no block reward from mining. The only fees being in the future from validating transactions.

When fewer miners are required for mining coins, it puts the network under vulnerability to a 51% attack.

This happens when a miner/mining pool controls more than 51% of the computational power and creates

fraudulent transactions for him/herself while invalidating transactions for other users on the network.

1.6 Proof- Of-Stake (POS): POS allows a holder of cryptocurrency on the Rencoin chain to validate transactions

on the chain according to the amount he/she holds. Simply put, the more coins held,

the more transactions are validated (or mined) by the holder. POS eliminates the need

for miners on the network to validate transactions. The first cryptocurrency to adopt

the POS method was Peercoin, after which other forks have been adapted upon

1.7 POS Positives:

With a POS based algorithm, the attacker would need to obtain 51% of the cryptocurrency to carry out a

51% attack. A proof of stake network avoids this by making it disadvantageous or a miner with 51% stake in

the cryptocurrency as it's almost firstly near impossible to obtain such a large stale in the network and it

would not be in the interest to attack a network he/she holds in the network as it would affect the value of

holdings. Simply put for an attack to happen, it's much less likely as POS does not rely solely on computing

power from miners, instead it's users staking their currency for rewards.

Chapter 2

Introducing Rencoin

2.1 A solid foundation

Rencoin is built upon *PIVX*, which itself is built upon the popular *DASH* cryptocurrency. While lineages can all be traced back to the original Satoshi Core, each project has chosen a particular direction with goals and ideals that represent the communities they serve. We will extend, and place emphasis on, the privacy coin features of our predecessor platforms and on extending that platform to creating a decentralised exchange

2.2 Our community

Rencoin's number one priority is the community. With giveaways, contests, a lively discussion platform on Discord and zerotolerance towards harassment of any kind. Rencoin strives to be the cryptocurrency for all varieties of end-users.

2.3 Coin Specifications

Algo Quark

Block Time 60 Seconds

Difficulty retargeting Every Block

Max Coin Supply (POW Phase) 49,750

Max Coin Supply (POS Phase, pre Infnite) 30,259,115 XN

Premine 4,000,000 REN

Block Maturity 60 Minutes

2.4. Rencoin POS block rewards

Rencoin is a proof of stake focused cryptocurrency, which primarily rewards its masternode holders. However, there is a reward given to stakers

2.5. Reward Distribution

Phase Block Height Reward Master node Staking

Phase 1 201-50000 200 REN 80% (160 REN) 20%

Phase 2 50001-75000 150 REN 80% (120 XN) 20%

Phase 3 75001-100000 100 REN 80% (80 XN) 20%

Phase 4 100001-150000 75 REN 80% (60 XN) 20%

Phase 5 150001-200000 50 REN 80% (40 XN) 20%

Phase 6 200001-250000 30 REN 80% (24 XN) 20%

Phase 7 250001-300000 15 REN 80% (12 XN) 20%

Phase 8 300001-400000 10 REN 80% (8 XN) 20%

Phase 9 400001-500000 5 REN 80% (4 XN) 20%

Phase X 500001-Infnity 5 REN 80% (4 XN) 20%

2.6 On our Pre-Mine

At the time of writing, there are a huge number of cryptocurrency projects and communities utilizing a similar technical foundation. As well as scams. While the underlying technology is solid, often times a deeper examination of their specifications and blockchain reward parameters reveal less-than-fair practices.

The Rencoin Team recognizes this, and has decided to be upfront. Our pre-mine of 4,000,000 coins (4%) is going to be used to promote and market the coin. We aim to develop a robust network of nodes running the Rencoin blockchain. community as a whole.

Chapter 3

Feature Set

3.1 Masternodes

Masternodes are, essentially, a decentralized web of computers that serve the Rencoin network. Masternodes on the Rencoin network perform very important network functions and receive part of the block rewards. They serve the Rencoin ecosystem by stabilizing coin supply, processing transactions, and securing the network. Masternodes require 10000 REN and modest technical knowledge to operate. Any wallet controlling 10000 REN can set up a masternode.

3.2 SwiftTX

SwiftTX provides masternodes with locking and consensus authority for transactions. When a transaction is submitted to the network, a group of masternodes will validate the transaction. If those masternodes reach consensus on the transaction's validity it will be locked for later introduction into the blockchain, greatly increasing transaction speed compared to conventional systems. SwiftTX makes it possible for multiple transactions to take place before a block on the network is mined with the same inputs. This system is based on Dash's InstantSend. (Kiraly 2017a).

3.3 Sporks

The Rencoin network employs the multi-phased fork mechanism known as "sporking". This will enable the REN network to implement new features while minimizing the chances of an unintended network fork during rollout. Spork changes are deployable via the network and can be turned on and of as necessary without requiring node software updates (Strophy 2017). This feature is extremely useful and allows the network to react quickly to security vulnerabilities.

3.4 TOR & IPV6 Masternodes

Rencoin allows the user to run their full node or masternode from either an onion address or an IPV6 address. We have been working to add full TOR nodes to both strengthen

the TOR network itself, and the Rencoin user experience operating in TOR only mode. A unique feature of TOR masternode support is being able to operate your masternode as a TOR hidden service. TOR nodes enable users with stable internet connections to operate masternodes out of their home network without the privacy implications of revealing their location or the dangers of exposing their home network to potential attacks or compromise.

Chapter 4

Conclusion

4.1 Summary

Rencoin is a privacy-oriented coin with masternodes, governance, and an evolving ecosystem of tools. For a start, the project will focus on broad coin distribution to create opportunities for significant community participation. Rencoin is launching with a variety of important privacy coin features and the development team is hard at work to introduce new features and build upon existing technologies. Rencoin aims to empower its community and those who join its community with choice through privacy and will focus considerable effort to this end.

4.2 One goal in mind

The masternode privacy coin ecosystem has been flooded by coins and projects seeking to entice new users through promises of substantial returns on investment, with road maps filled with unachievable goals or deadlines, with a focus on marketing instead of technology development. Rencoin is opposed to this approach. Beyond the initial marketing necessary to launch the coin and get it listed on exchanges – An important step in the creation of value for the coin, the Rencoin development team will focus its energy on developing the coin and network. The main goal of the Rencoin project is to create a global decentralized exchange backed by a network of masternodes securing the transactions occurring and in the process, creating value and rewarding our community.

References

Bitcoin Core Team, T., 2017. Bitcoin developer reference. Available at: https://bitcoin.org/en/developer-reference#block-headers.

Crosby, M., Nachiappan, Pattanayak, P., Verma, S., et al., 2015. BlockChain technology. Available at: http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.

Kiraly, B., 2017a. InstantSend. Available at: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146928/InstantSend.

Kiraly, B., 2017b. PrivateSend. Available at: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146924/PrivateSend.

Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system. Available at: https://bitcoin.org/bitcoin.pdf.

Okupski, K., 2016. Bitcoin developer reference., pp.3–4. Available at: https://lopp.net/pdf/Bitcoin_Developer_Reference.pdf.

Jakiman, 2017. PIVX purple paper. Available at: https://pivx.org/wp-content/uploads/2017/03/PIVX-purple-paper-Technincal-Notes.pdf.

Strophy, 2017. Understanding sporks. Available at: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/128319489/Understanding+Sporks.