HYDRA-X: A Proof-of-Stake Protocol PoS, Peer-to-Peer Electronic Cash System

hydra-x.org • hydra-x.org@protonmail.com

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-

spending problem using a peer-to-peer network and Proof of Stake (POS) blockchain. Everyone can become a full node and stake HYDRA-X (HDX) to value his coins while helping to maintain the network.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust-based model. Completely non-reversible transactions are not possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need.“ Satoshi Nakamoto wrote these words on his white paper and posted them on October 31, 2008! Today December 2021. 13 years passed. What has changed? A lot has changed! Bitcoin is used by millions of people around the world, and thousands of new users, investors, Bitcoin institutions, or other crypto coins are added daily. Bitcoin has a dominant position on the market. Even small children know about Bitcoin, which is great news! But there is the other side of the coin ...

Consensus in a decentralized digital currency like Bitcoin is achieved by requiring generated blocks to contain proof that the node which generated the block solved a computational hard task. Unfortunately, the concept of the Proof-of-Work (PoW) based system tends to lean towards eventual self-destruction. Proof-of-Work was a fantastic innovation that formed the backbone of the original Bitcoin protocol. The idea is that by solving a computationally intensive math problem, one can prove the effort they've done to secure the protocol. This is how a blockchain is generated, and the effort that is required to perform this computation contributes to a coin's scarcity and value. However, Proof-of-Work eventually becomes an extraordinarily expensive and uneconomical system.

2. Proof-of-Stake (PoS)

Proof-of-Stake (PoS) aims to replace the way of achieving consensus in a distributed system; instead of solving the Proof-of-Work, the node which generates a block has to provide proof that it has access to a certain amount of coins before being accepted by the network. Proof of Stake solves this issue in a very elegant way. Rather than using computer power as a scarce resource to generate security, Proof of Stake uses the scarcity of the coin itself. A user

may choose to "stake" his coins to generate the next block in the chain, and his chance of doing so is proportional to the weight of their coins.

Generating a block involves sending coins to oneself, which proves the ownership. The required amount of coins (also called target) is specified by the network through a difficulty adjustment process similar to PoW that ensures an approximate, constant block time. As in PoW, the block generation process will be rewarded through transaction fees and a supply model specified by the underlying protocol; which can also be seen as an interest rate by common definition. The initial distribution of the currency is usually obtained through a period of PoW mining. The first PoS based currency was PeerCoin which is still in a period of PoW mining. Further development of the PeerCoin PoS protocol leads to NovaCoin which uses a hybrid PoS / PoW system. **HYDRA-X is a cryptocurrency that uses a pure PoS protocol** which is based on the development of the above described projects.

3. The Fine Print

- Block time - 60 seconds
- # of PoW blocks - 5000
- Block reward PoS phase - 5 HDX
- Premine - 666000
- Coin age before staking starts - 2 hours

OPEN SOURCE SOFTWARE - The software (wallet) is open source, so its safety can be audited.

FAST TRANSACTIONS - It is extremely fast, you can send (HDX) to anyone in the world within seconds.

ANONYMOUS - Anyone can run the wallet and transact with anonymity. No personal identifying information.

4. Staking Economy

HYDRA-X is a Proof of Stake (POS) blockchain. Everyone can become a full node and stake HYDRA-X (HDX) to value his coins while helping to maintain the network.

Users who keep their wallets open to secure the network via staking will get from 1% to X% rewards per year (varies according to network weight). Once you start to Stake, you will notice that a certain amount of coins will be placed into your Stake balance (you can see this

under the Overview tab on your wallet) and those coins will begin to stake. The more coins you have, the more coins you will earn by Staking. Proof-of-Stake is eco-friendly and efficient and avoids the vast waste of energy and hardware overhead of Proof-of-Work based networks. Through its multiple features, HYDRA-X offers a complete solution for a healthy ecosystem.

Every computer is capable of STAKING! The performance of the computer does not matter The only thing required is an internet connection and supported operating system (Mac OS 10.13+ x86_64, Windows x86_64, Linux 18.04 x86_64).

5. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were. As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

HYDRA-X is open-source too, meaning that the software that makes it function is completely available for public scrutiny giving you peace of mind. The transaction history is also called a "Blockchain". This history is shared by everyone. So when you download the program you save a copy of the history and share it! In addition, you will stake while the software is running and make sure the blockchain transaction history is secure. So it is impossible to counterfeit. Your account is a collection of keys. You can use those keys to sign transactions and even contracts! Nobody else in the world has a copy of those keys, only you. So it is impossible to forge your digital signature.

Thanks to the brilliant combination of digital signatures and torrents, cryptocurrency has risen to popularity.

6. Conclusion

The ability to manage transactions and issue additional HYDRA-X coins (HDX) is all handled by the network of users utilizing HYDRA-X (HDX). You are your financial manager, no third

party! Because the HYDRA-X network is run by the people, holders of HYDRA-X coins, who receive rewards through a process called staking. Your account can't be frozen, it's free forever, it's anonymous, more secure than traditional banking, and payments can be sent to anyone in the world in seconds.

References

[1] Satoshi Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,“ bitcoin.org, 2008.

[2] Sunny King and Scott Nadal, “Ppcoin: Peer-to-peer crypto-currency with proof-of-stake peercoin.net,“ 2013.

[3] Peercoin, "en.wikipedia.org/wiki/Peercoin"

[4] Nicolas T. Courtois, “On the longest chain rule and programmed self-destruction of cryptocurrencies“, 2014.

[5] Prof-of-Stake, “en.wikipedia.org/wiki/Proof_of_stake“