Peersend: Anonymous Transaction Peer to Peer System for Halcyon Cryptocurrency

By: HAL9000

halcyondevs@gmail.com
www.halcyon.pw

August 19th, 2014

Abstract:

When a Halcyon block is generated, or a transaction is sent, it is recorded in the public ledger known as the blockchain. We propose adding a layer to this model by allowing transactions to be sent without a record at all. This method must be fast and secure, while adding no cost to the end user, in order to stimulate commerce. We must also ensure this method is easy for newcomers to master, and does not become centrally managed by early adopters and wealthy parties. Finally, this method should protect transactions by allowing no risk of theft. The technology proposed will be referred to as: “Peersend”.

Scope of this Document:

This is a technical document, designed to explain to the common user the technology behind Peersend. This is not a marketing brochure, or solicitation for investment. We will navigate through the steps required for a successful Peersend, while explaining the technical aspect of how this is accomplished. In order to keep this document brief and informative, a visual aid for each step will be available on Halcyon public wiki. There will be a brief section on the economic impact of Peersend, which we believe fits the criteria of a technical document because the technology involved is directly related to digital currency.

Introduction:

Peersend is a decentralized mixing service, that sits as a layer on top of the Halcyon network. This layer allows participating Halcyon users (wallets) to connect with others, and mix coins in an untraceable manner. An example of how this works:

1. User A chooses to send 100 coins to User B.
2. The wallet generates an encrypted key that is sent to other participating users over a peer to peer network in the form of a signed message. This verifies that they will have enough funds to engage in the mixing process. This also gives every wallet baseline instructions in order for them to generate new, compatible addresses to send to other scramblers.

3. User A's coins get sent to many participating wallets, which then change their sending addresses, and relay the coins many times until 100 coins are delivered to UserB. Please note that network transaction fees will incur.
4. User B receives coins from many participants, with no way to trace where it originated. It will not be possible to trace the origin of User A, because the original transaction was not sent as a lump sum at the exact same time.

Requirements

a) There must be no risk of theft or fraud.
b) Security of the network must not be compromised.
c) Execution of Peersend must have minimal impact on the network.
d) Must be easy to use, to promote mass adoption.
e) Shall be opt-in only, but everyone can participate.
f) Will not incur additional mixing fees.
g) Must be implemented in a manner that does not inhibit future development of Halcyon.
h) Will not exclude merchants from accepting Halcyon.
i) Invisible transactions, scrutineers must not be able to 'reverse trace' sent coins.
j) Must never be centralized, require coin deposits, or investments.
k) Will not place an unreasonable burden on end user's hardware.

Technical Analysis:

Peersend operates above the Halcyon network. It is a layer, that acts as peer-to-peer network and allows users to discover each other, in order to scramble transactions. This method permits the communication required to 'plan the scramble'. This involves sending a signed message, with an encrypted key, explaining to each participant how many coins they will need in their wallet to take part in the scramble, when the transaction should take place, and where they need to go next. This key also verifies that the participant creates a new wallet address to send from, and tells them what the destination is. The next participant in the scramble is told how many coins to expect, and where to send them. Multiple transactions will be sent to many peers from the original sender. In order to prevent traces of origin, an initial send may require the wallet to be taking part in an already ongoing scramble, which will further add to the web of transactions.

Threats:

Multiple scenarios can arise that malicious users may try to capitalize on, in this section, we will explore 6 examples and provide solutions.

Peersend User Attempts to Steal Coins:

During each step of the scramble phase, instructions are sent to each participant using a signed key belonging to the Halcyon network. If a malicious user attempts to empty the coins that are required in the newly generated wallet address meant for this scramble, the system will catch this during the due dilligence phase and simply not sign the key and the transaction will never be posted to the Halcyon blockchain.

Peersend User Attempts to Modify Transaction Details

This is referred to as a "man-in-the-middle" style of attack and will not work. This key that sends instructions to each scrambler is encrypted using a one-way set of instructions. Trying to manipulate this would result in the key never being signed, thus preventing the scramble from taking place and making it to the block chain.

Peersend User Attempts to Generate Unnecessary Network Traffic

This is considered a DOS (Denial of Service) attack on the network. The only way this would be achievable would be to plant a wallet (peer) into the mix with the hopes it can cancel the transaction during the due dilligence phase. This would require luck, and would not be sustainable. The other option would be to send many transactions of a tiny nature, but transaction fees required by the Halcyon ledger are in place to prevent this style of attack already.

Peersend User Absent During Execution of Scramble.

This could happen if a user tries to disrupt as many services as possible, or generally has software or hardware issues. Once again, the key will not get signed and the transaction will be cancelled at the end of the due dilligence phase. One could argue that a script be made to start and stop a wallet could cause issues, but the software involved loads too slow for this to be effective.

Peersend User is Identified by IP address.

This is the most probable issue, and can be addressed by accessing the Halcyon and Peersend network with Tor.

Economic Analysis:

Halcyon proposes prosperity through reduced transaction costs compared to traditional banking models and unsurpassed economic freedom. Transaction costs are costs incurred in making an economic exchange, creating resistance to growth. Nobel prize-winning economist Ronald Coase introduced that economic growth and the most efficient distribution of resources were only possible in a world where transaction costs are reduced or eliminated.[1] Douglass C. North agrees that, “typically throughout history [it] has resulted, in economies with high transaction (and production) costs that have prevented economic growth.”[2] And David Bywaters couldn’t say it more explicitly: “A reduction in transaction costs, or a reduction in resource per transaction, increases economic growth, and economic welfare.”[3] By eliminating banking intermediaries, Halcyon significantly lowers transaction costs, grants access to capital, and promotes financial liberty and prosperity for all.

Halcyon’s Peersend technology affords unprecedented economic freedom for its users, offering a level of anonymity unmatched by any other cryptocurrency. True to the core principles of Bitcoin, Halcyon’s decentralized mixing service allows users (wallets) to connect and mix coins in an untraceable manner. This additional layer of anonymity is unprecedented, inspiring complete confidence in the anonymity of transactions and further encouraging economic growth.

Executive Summary

Peersend brings anonymous transactions to the Halcyon network using a top-level peer-to-peer layer. This technology was built from the ground up for Halcyon, and is not a clone of existing protocols. There is no threat of coin theft, or centralization in this model. We gave an example how this technology would be used in a common manner, and then laid out requirements that must be upheld. Satisfaction for each request should be addressed in this paper but some sections cannot be proven in this document (Requirements: D, G, H, K). We examined earlier that this technology makes use of signed keys and scrambler nodes. The only security issue we found was the IP address linking the user to the Halcyon wallet could be exposed, which could be fixed by utilizing the Tor network. A brief section discussing the positive outcome of an anonymous financial economy was added to highlight how this technology fits into the core ideology of the cryptocurrency community as a whole, strengthening such cornerstones as decentralized money and economic anonymity.

References

Tim Ruffing, Pedro Moreno-Sanchez, Aniket Kate, *CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin,* http://crypsys.mmci.uni-saarland.de/projects/CoinShuffle/coinshuffle.pdf

R. Coase, "*The Problem of Social Cost*," The Journal of Law and Economics (1960) 3:1-44

North,Douglass Cecil, "*Transaction Costs, Institutions, and Economic Performance*," International Center for Economic Growth (1992), 30:6

Bywater, David, "*The Role of Transactions Costs in Economic Growth,*" The International Journal of Economic Policy Studies (2012), 7:65