CLOAK

# Decentralized P2P Crypto Currency Transaction Anonymity via Proof of Stake Protocol Extensions

By Z, Cloak Technical Services Division, June, 2014 A.D.

*Abstract*

Block chain based crypto currencies of the Bitcoin 1.0 generation are by their nature pseudonymous. The block chain consists of transaction inputs and outputs and the flow of transactions can be correlated to identify the spender and recipient of coins. In this paper, a system is proposed to provide anonymity of transactions by extending the existing protocol to broadcast, redeem-on-behalf-of, and forward inputs to outputs in such a fashion that the origination and recipient cannot be directly linked through block chain analysis. The proposed solution will be implemented in the CloakCoin alternative crypto currency.

## Overview

As of the present time there has been an explosion of alternative crypto currencies released based on Bitcoin 1.0 technology. Recent fads have brought Proof-of-Stake back to the forefront, with many currencies adopting the proof-of-stake implementation of Sunny King that originated in PeerCoin. Anonymity is the next challenge to be solved, but all implemented solutions to date have relied upon trusted and centralized nodes that act as mixers, tumblers, or arbiters of the anonymization mechanism.

The present solutions are not ideal and do not achieve the goal of true anonymity of transactions because all transactions flow through centrally controlled nodes. Those nodes may be altruistic or evil, they may log and capture de-anonymizing information, they may be controlled by adversarial entities, or they may simply be poorly maintained by inexperienced operators.

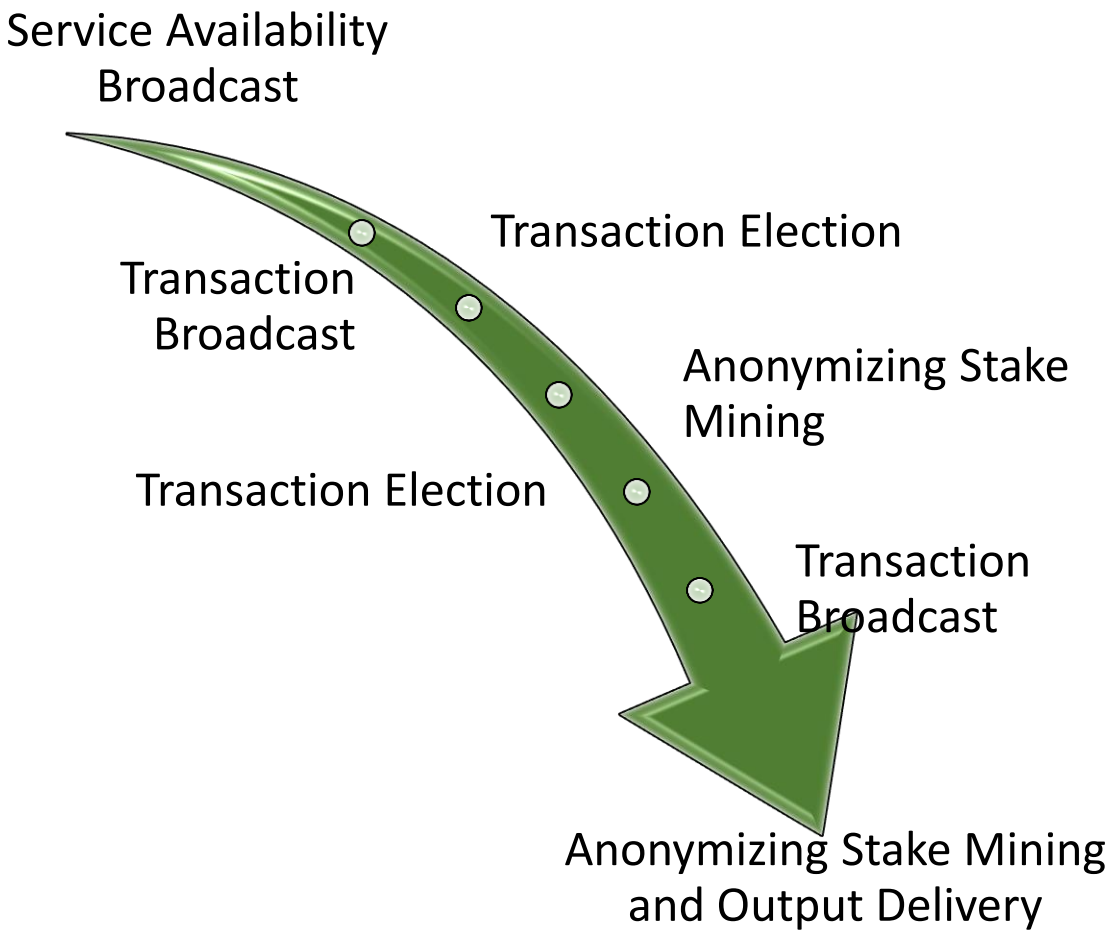
The ideal solution is peer-to-peer in nature, decentralized and trustless; with no centrally controlled "authorities" providing anonymizing services.

The existing proof-of-stake implementation already bolts on extensions to the Bitcoin protocol to handle the transmission and processing of synchronized checkpoints and stake blocks, and already includes an additional type of block generation through the "minting" or stake mining process that provides a reward to node operators as an incentive to provide network transaction processing.

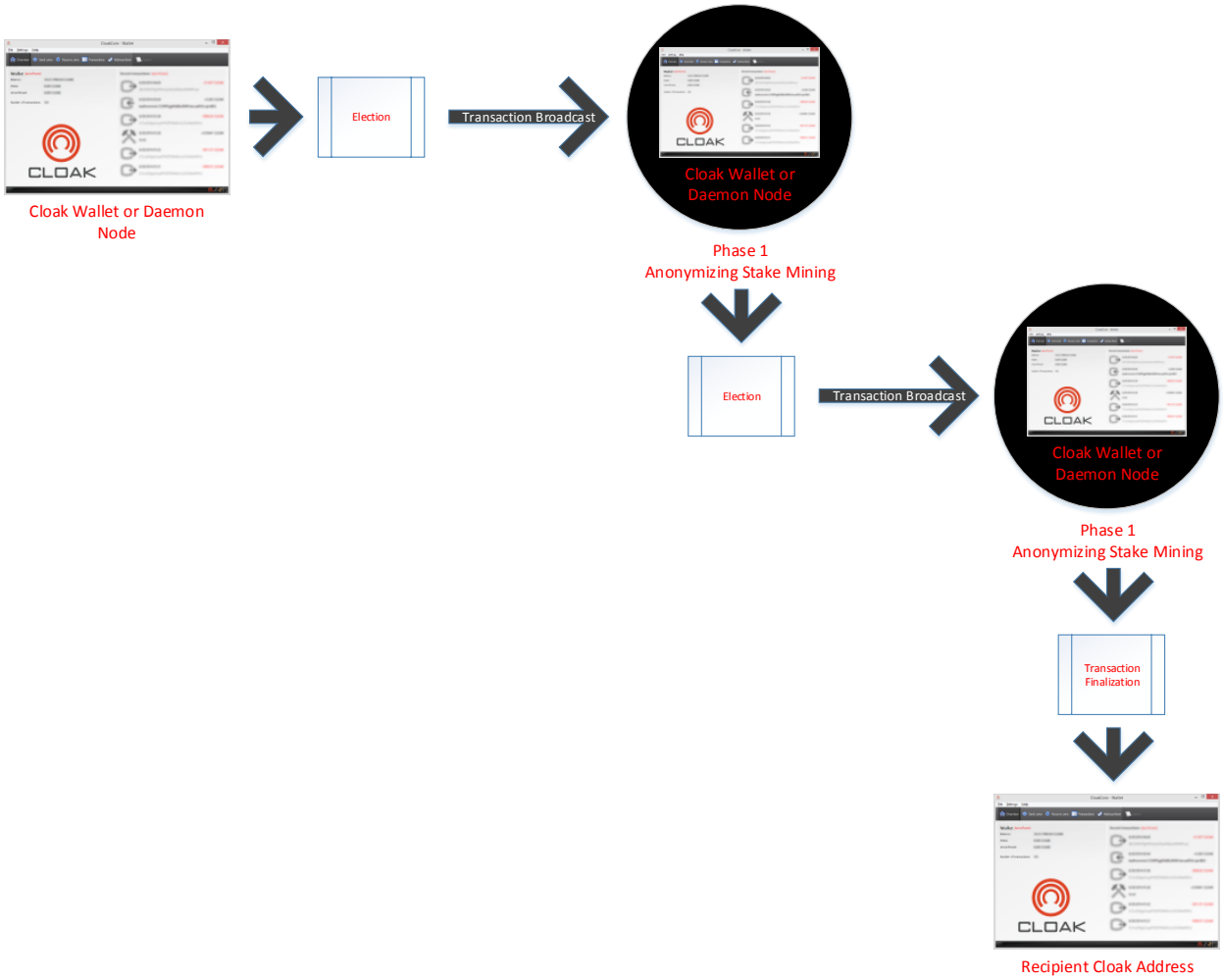
It would seem obvious, then, to leverage this existing framework as a means to provide decentralized processing of transactions in a way that decouples the origination and recipient. This document provides a high level overview of the process flow and operation of the solution, but is not a publicly shared detailed technical design document as we would like to provide a proper functioning implementation before inferior clone attempts appear.

## Extended Transaction Processing Flow

In the proposed system, all nodes are both staking and anonymizing by default. Just as most proof-of-stake coin implementations allow the user to disable staking (typically through a command line argument of configuration file entry), the system will also allow the user to disable anonymizing services. As a result, the system uses a mechanism to inform the network which nodes are available for anonymizing.




Two passes through the transaction anonymizing flow are performed before outputs are delivered to their recipient. While this adds a modest amount of latency into the transaction flow, it provides for an additional layer of anonymizing protection.




## Anonymization Service Broadcast

At wallet or daemon node startup, the node will create and broadcast a special P2P message announcing that it is providing anonymization services and is available to participate in transaction elections. This step is necessary as some nodes may opt to disable the staking process (exchange wallets, pool wallets, etc.).

Nodes that announce their availability to provide anonymization services must be compliant with the anonymization protocol. These protocol extensions provide for the transmission of anonymized transaction packages from an originator to an elected node for addition to their memory pool.

## Opt-Out System vs. Centralized Authorities

The proposed solution is decentralized, in that it is not reliant on centrally controlled authority nodes, all nodes in the P2P network participate by default. Nodes that turn staking off essentially “opt out” of the system, but they are also then ineligible to receive transaction processing fees.

The staking and anonymization protocols are merged. In some sense, one could consider the staking process to be extended as a cooperation between the originating node and the staking node as an anonymizing pair.

## Trustless

The system is trustless, in that the protocol validates the proper processing of transactions just as existing decentralized currencies do today. If an elected node fails to process a transaction and meet protocol, a re-election occurs and a ban count is incremented in a similar fashion as occurs for other parts of the existing protocol.

## Transaction Creation and Election Process

At the time that transactions are created, the wallet will go through a process of "electing" an anonymization service providing node to start transaction processing. The election process is a process of random selection from the pool of available anonymizing wallets. The transaction output is paired with the encoded destination and the raw transaction package is passed to the elected node.

**Anonymized Tx Package**

| |
|---|
| **Standard Tx Header** |
| **Elected Node Destination** |
| **Recipient** |

The cloak transaction package is broadcast to the elected node, but at the point the originator and recipient are not recorded in the blockchain.

## Stake Mining and Anonymization

As part of the stake mining process, the elected node will process the special transaction package from its memory pool. The anonymization system is a two-pass process flow. If the elected node is processing Phase 1, it will solve the block and the output will be assigned to an internal address at the node. The node will earn a fee for this service, and then redeem the input by recursing back to the election process, to elect a node for Phase 2. The node then constructs an anonymizing transaction package and broadcasts it to the elected Phase 2 node.

Again in the Phase 2 pass the originator and recipient are not recorded, instead the transaction occurs between the Phase 1 and Phase 2 nodes.

## Transaction Finalization and Output Delivery

If the elected node is a Phase 2 node, it will solve a block containing the phase 2 transaction, redeem the input and generate an output to the destination recipient address. At this point the only link from the recipient would be from the Phase 2 node.

## Re-Election

Elected transactions must be accepted and processed within an expiration window, in case nodes go down or lose connectivity. Node re-election occurs if:

- If the elected node does not respond
- If the elected node responds with a non-acceptance message (node is too busy, node has too big of a backlog, etc.)
- If verification of the anonymizing minting phase is not received within the expiration window, a new election occurs and the transaction is re-broadcast for processing.