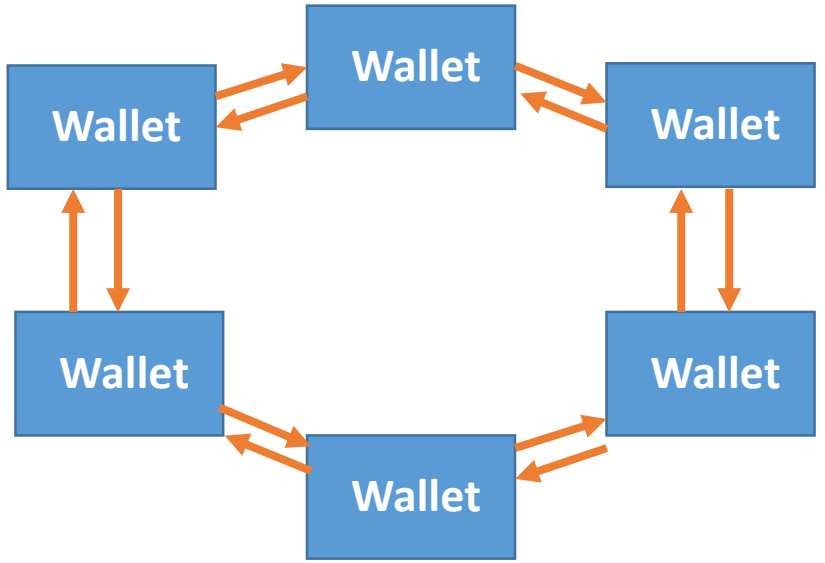
VeriCoin Anonyminity

VeriSend - How does it work?

Ring Nodes – Continuous Local Mixing

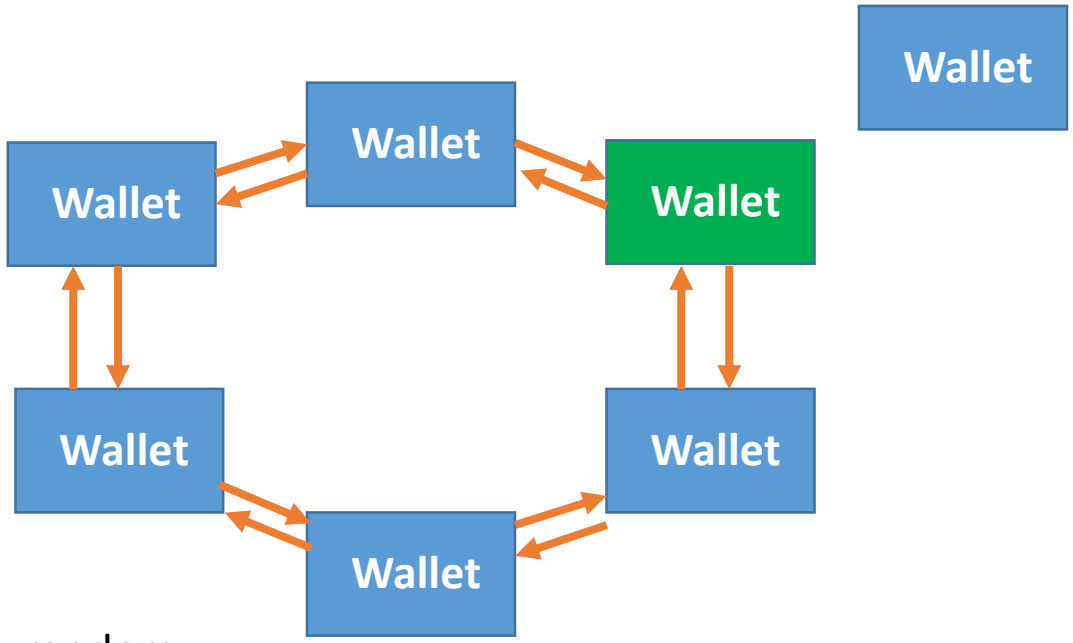
Each Ring Node will be in full stake mode providing even greater mixing power



Internal Node Wallets continuously cycle coins (random amount) and validate the total wallet balance to ensure node stability.

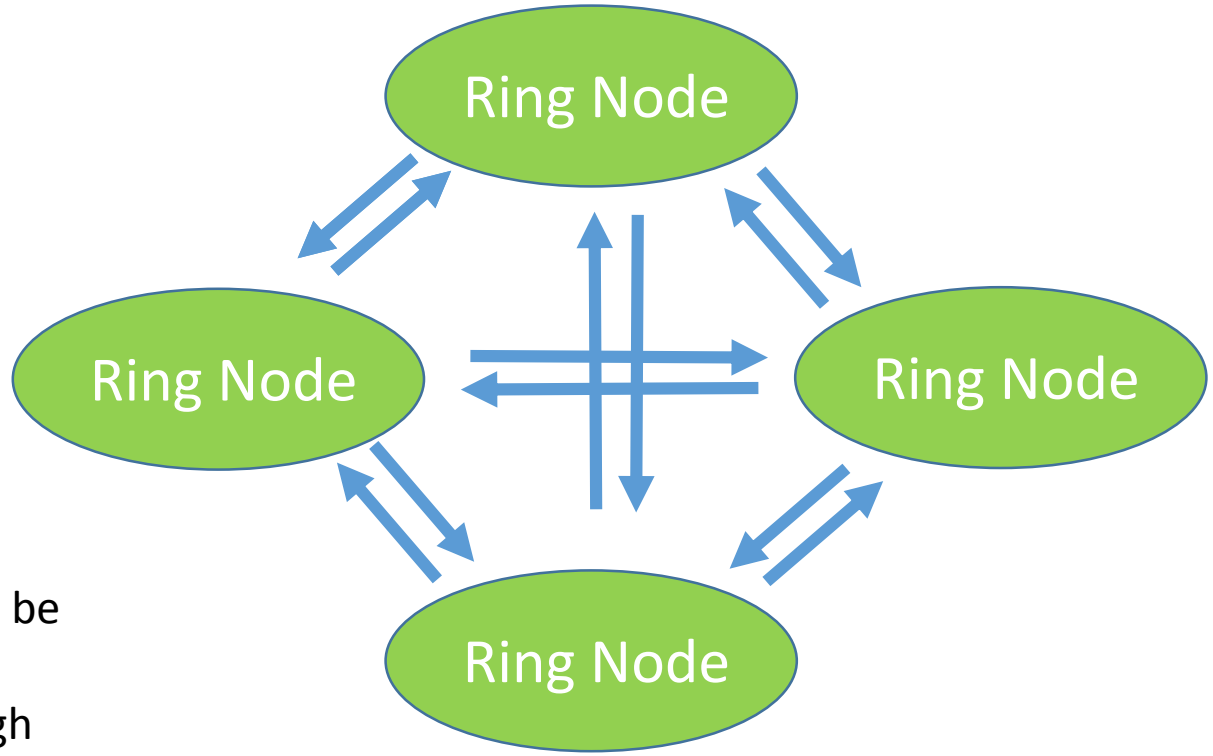
With cycle times of 5 minutes, the total cost of operation will be ~12 VRC per day per node.

Ring Nodes – Random Wallet Swaps



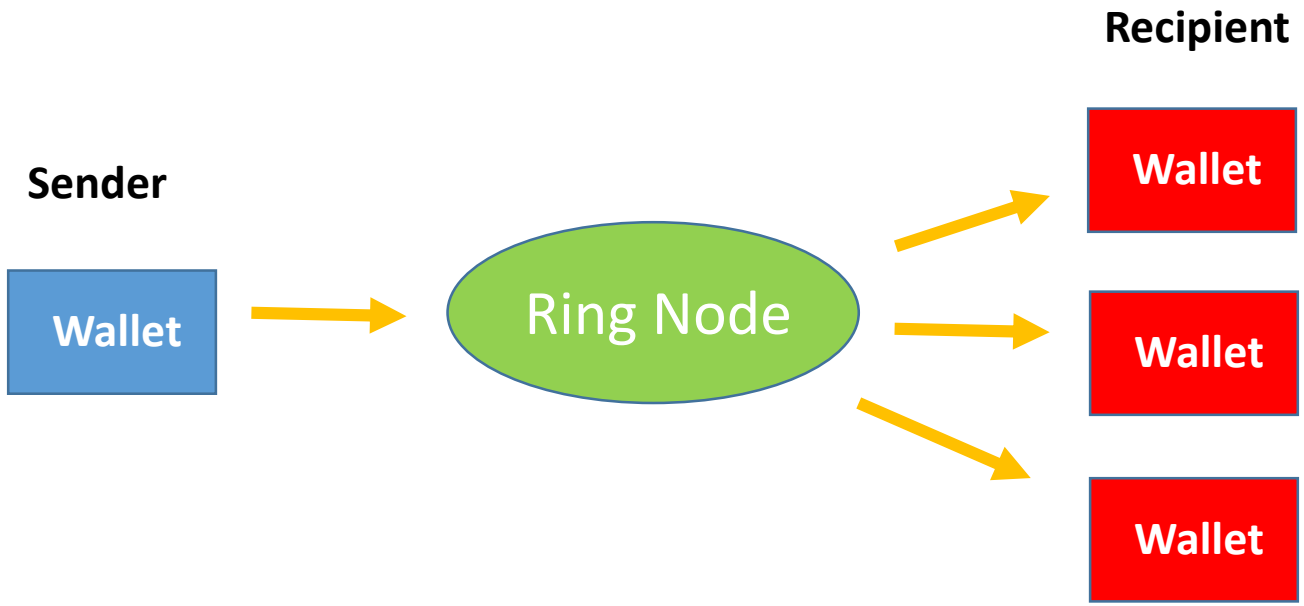
To further anonymize transactions, random node-level wallet swaps will occur causing 5 of the 6 wallets on the node to contain the total balance while the last of the 6 swaps out for a new wallet address. This will lead to further obfuscation of any transaction details.

Node Mixing – Greater Security



Even greater mixing can be specified by requesting your payment go through more nodes and node-mix-cycles.

Single-in/Multi-out



If the sender knows multiple blank addresses owned by the recipient, he/she can make a single payment to the Ring Node and request redirection/splitting of the funds to various addresses at once. This can also be used to pay multiple recipients.

How it works

Utilizing VeriCoin's ANON feature will utilize PGP/GPG encryption techniques with new keys unrelated to the wallet keys. The ring node system will have publically available keys for signed messages to be sent with. Messages will be transferred using a JSON string to the listening VeriCoin ring node.

The initial send will include a signed message following our VeriSend protocol. This protocol will include an encrypted message specifying the amount of mixing requested, the mixing time requested, whether node mixing should be used, and payments to each address. This allows flexibility with a trade-off between security and timeliness of payment. The ring node will then verify that the data is correct by comparing it to incoming transactions. If the signed message data is validated it will then the send will be executed.

Effectiveness

- The current ability for a system to determine where a transaction is going (Factor of Identity) using Bitcoin is set for 100.
- VeriCoin's Rapid PoS blocktimes already increases the resources required for determining the identities of transaction participants down to 30.
- With mixing via a single node and no minimum time coin requirement, the factor of identity is now 0.01.
- Adding time mixing in reduces this factor to 0.00001.
- Adding mixing via node mixing reduces this factor to below 0.000000001.
- Adding mixing via the above and Single-in/Multi-out reduces the factor to 0.00000000000000000000000001, essentially impossible to calculate given current computing technologies.

Timeline

- The VeriCoin team prides itself on not publically releasing deadlines so we can ensure our code works very well before release.
- For example, our multipool featuring our Optimal Buying Algorithm is not yet released officially while we test our features despite being used for mining for over a week.
- We have no set timeline for implementation of these features in the release wallet however we are testing our concept internally and believe it offers the best feature-set and speed compared to other ANON send technologies, none of which are even available to use.

Case Use

- Max wants to subscribe to VeriCoinPorn.com but doesn't want anyone to know he paid for a subscription
- Max sends a payment to one of the mixing nodes. He signs the message with the mixing node's public key and inside the signature the VeriCoin wallet includes details about where the transaction should go and how to send the transactions.
- Max can simply choose a button to anonymize the send, pay a small fee (disincentivizes ANON sending when unnecessary as to not flood the blockchain), and off the payment is sent. Within 10 minutes, the recipient should have the VeriCoin and nobody ever knows that Max now has a VeriCoinPorn.com subscription.