Anonymous Transfer/Payments

The primary invention enabling a crypto currency to overcome the double spending problem is the blockchain record. This blockchain record is public and therefore can be used to track payments to and from an address. Proposed is a system to use the CINNI encrypted messaging system and onion routing (similar to TOR) in combination with "reserve relay nodes", to enable completely anonymous transfers/payments within the blockchain system. This paper is intended to be a simple explanation of the proposed anonymous transfer system, a more detailed explanation of the system will follow after development has been completed.

Risk to anonymity:

The anonymity of transactions can be compromised in several ways.

1) Transfers can be tracked using the public blockchain.

> **a)** A search of the blockcahin will reveal the address to address transfer history and therefore create a path coins have followed from sender to receiver.
>
> **b)** A search of the blockchain for a specific amount of coins leaving one address and arriving at another address can give confirmation of a suspected transfer.

2) An intermediary such as a coin mixer/node could be a shill or could be compromised and have the log of transactions searched which would destroy the anonymity of transactions.

Using the CINNI encrypted messaging system and onion routing (similar to TOR) in combination with "reserve relay nodes", the anonymous transfer system in development for CINNI will address each of the listed situations and therefore enable truly anonymous payments.

Blockchain Path/Amount Search:

The encrypted messaging system allows encrypted instructions to be sent with payments to the "reserve relay nodes". With these instructions, each reserve relay node, will create a complete break in the blockchain, where the path of transactions cannot be tracked back to the sender. The sender will have the option to add a "surplus" amount to the payment. The surplus will be returned to a different sender controlled address, on a time delay in order to obfuscate the transaction amount. See diagram.

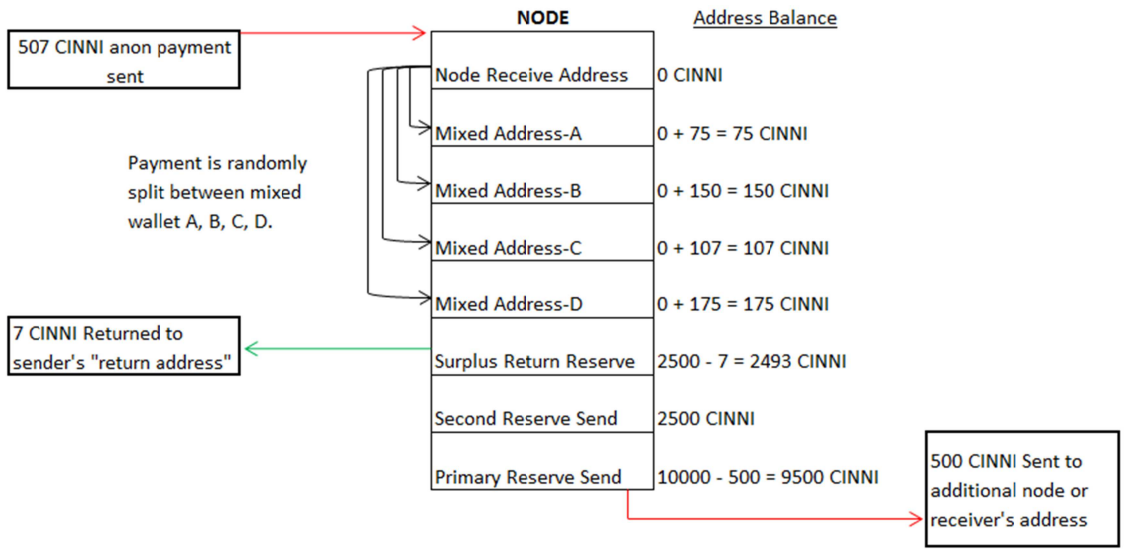
Onion Routing EM with Payments:

Using encrypted message onion routing, specific instructions can be sent to nodes along the transaction path. The onion allows control of the information each node has access to. Using this system we can ensure that no one node will have the access to the addresses of both the sender and receiver. If a node is compromised, it will not affect the anonymity of the transaction. See examples on following pages.

*To start a Reserve Relay Node 15,000 CINNI must be held in a wallet/address structure as shown below.
*The Reserve Relay Node will be compensated in transaction fees for processing anon payments.

NODE	Address Balance
Node Receive Address	0 CINNI
Mixed Address-A	0 CINNI
Mixed Address-B	0 CINNI
Mixed Address-C	0 CINNI
Mixed Address-D	0 CINNI
Surplus Return Reserve	2500 CINNI
Second Reserve Send	2500 CINNI
Primary Reserve Send	10000 CINNI

*Reserve Relay Node receives payment from sender and splits the 507 CINNI payment into four mixed addresses A, B, C, D.
*Anon payment is then sent from reserve CINNI held by node in the "primary reserve send" address. The coins received from the sender remain in the node's mixed addresses A, B, C, D. This process will create a complete break in the blockchain transaction path.
*7 CINNI is returned to a sender controlled address. This process will obscure the transaction amount.



Onion Routing Payments

*In this example, the first node (X) would know the address of the payment sender and the address of the second node (Y). Node X would not know the address of Node Z or the final payment destination address.

*Node Y would know the address of node Z but not know the address of the payment sender or the final destination address.

*Node Z would know the address of the final destination (receiver) but not know the address of the sender or node X.

Node X unlocks 1st layer of message with its receiving wallet private key.

Information received:
*Public address of next node
*Payment amount / ID
*Sender's surplus return address

Node X sends the remaining encrypted message to node Y. Payment is sent to node Y from node X's "mixed reserve wallet".

Surplus payment is returned to sender's "surplus return address"

Node Y unlocks 2nd layer of message with its receiving wallet private key.

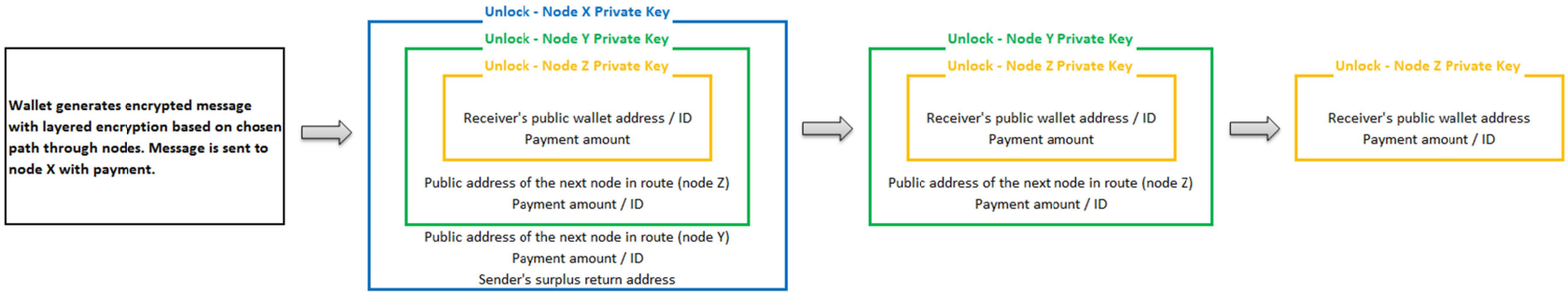
Information received:
*Public address of next node
*Payment amount / ID

Node Y sends the remaining encrypted message to node Z. Payment is sent to node Z from node Y's "mixed reserve wallet".

Node Z unlocks 3rd layer of message with its receiving wallet private key.

Information received:
*Receiver's wallet address
*Payment amount / ID

Node Z sends payment to receiver's wallet from node Z's "mixed reserve wallet"



In conclusion, this is a simple explanation of the anonymous transfer system. There are many scenarios not addressed in the examples that have been accounted for by the developers of this system. A more detailed explanation and formal whitepaper will follow completion of the system and accompany the rollout of the feature.