As cryptocurrencies continue to expand several problems have come to the surface. The desire for peer-to-peer exchange has been overwhelmed by the incentives of speculators and the coins are not actually being used to transact real goods and services. As large coins such as bitcoin continue to grow computational power required to maintain the network grows with it. The need to build and maintain a huge network bites at heels of privacy and large large institutions are profiting from mining in speculative trades rather than investing in real goods and services. We can take from the milestones already established and make some fundamental adaptations to solve several key problems in the current technology.

Transactions

We still define a coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

The problem begins with how the chain is built. By adding block after block to the chain the technology depends on a single chain in order to maintain the integrity of the network. From here other problems arise as now a single chain proof is required to transact and information has to be shared across a “network”. Instead the solution comes from changing the way the chain is built.

Now the key to the next iteration comes from the ability of the blocks to then transact independently.

Hash T1

Hash T0

Owner 3's Private Key

Owner 1's Private Key

Owner 1's Signature

Owner 3's Signature

Owner 3's Public Key

Transaction 2

Owner 1's Public Key 1's Public Key

Owner 1's Signature

Owner 2's Public Key

Transaction 1

Owner 2's Private Key

Owner 2's Signature

Owner 1's Private Key

Owner 1's Public Key

from T1 Each owner is given a copy of the transaction, as each independent owner continues to transact they only consume the hash of the payer in the transaction and the payee “Mines” the new block to receive the coin. In this way mining is naturally distributed across independent nodes and the coin does not depend on a network to continue functioning.

Owner 1’s Signature

Owner 4's Public Key

Hash T1

Owner 4's Signature

Owner 1's Private Key

Owner 4's Private Key

Transaction 3



Proof of work

Proof of work will still be required and using the nonce method the chain will maintain its integrity. Double pay is avoided as the genesis block hash will still be included in all proceeding blocks and changing your coin will mean that you will no longer be able to transact with the other nodes in the network unless every node agrees to make a change.