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.

[Grab your reader’s attention with a great quote from the document or use this space to emphasize a key point. To place this text box anywhere on the page, just drag it.]

Owner 2's Signature

Transaction 1

Owner 2's Private Key

Owner 1's Private Key

Owner 1's Signature

Owner 1's Signature

Owner 2's Public Key

Owner 0's Signature

Owner 1's Public Key

Hash

Hash