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.

Infinite Divisibility of coin

One key feature of this new version of the blockchain will need to be infinite divisibility or at least highly divisible coin. This may seem counter intuitive but is actually the key to understanding the main attributes of the blockchain. Instead of creating a new coin for each new block the genesis coin is initialized as 1.0 coins. In the first transaction the payer(P1) pays the payee(P2) a fraction of 1.0 say 0.25. The payee now owns 0.25 coins and the payer 0.75. Both can now continue to transact with their portion of the coin. If P3 would like some of P1’s coin say 0.1 coins, he need only create a new block and take a portion of P1’s balance. Now P1 has 0.65 coins, P2 has 0.25 coins and P3 has 0.1 coins. As more transactions occur the coin begins to divide into smaller and smaller portions. Because P1 will always want to hold on to some of his coin a fixed number of decimal places can be created say 100 which will be more than sufficient to carry all the value of goods and services transacted by the coin.

Deflationary effect

Now we come to the real economic impact of the coin. As more persons transact with the coin the value of the coin naturally inflates without effecting the coin itself. Instead prices of goods and services will decline continually and as ownership spreads the coins value will continue improve as more people store more value in a decreasing quantity of coin. This also creates a natural incentive to get hold of the coin quickly as the value of the coin inflates exponentially.

Incentive

As described above Incentive to use the coin will grow as more people transact with the coin. As value can be determined easily (all portions adding to 1) a certain level of transparency is also inherent. Anyone will be able to create a new genesis coin but only the coins with the most transactions will accumulate value and as certain coins grow in value they will naturally consume weaker coins as one coin is exchanged for the other. Therefore the value of the coin can only be determined by an open market as no one will be able to trace the actual goods and services transacted. Despite this value will not be easy to forge as each payer will only have his portion of the source coin and each participants intrinsic value will have to be settled by an open market in the form of a new block. The coins value as always can only be determined by the full faith and credit of those who hold the coin. If too many speculators sit on their coin without making new transactions the value of the coin will not grow and other coins will naturally consume the stale coins with too many speculators. Still savers are rewarded for paying low prices and everyone benefits from holding some portion of the coin thereby increasing the security of the coin in the market.