**ALMAGIL: A Proposition for updating blockchain technology**

**Introduction**

We admit that we are not experts in cryptography however with the help of experts in that field and the simple changes to coin architecture described below we hope to address key flaws in existing coins and create the system of decentralized exchange and value storage that was originally intended at the outset of the blockchain phenomena.

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 coin networks continue to grow computational power required to maintain the network grows with it. The need to build and maintain a huge network makes new transactions exponentially more expensive and large institutions are profiting from mining in speculative trades rather than investing in real goods and services. Because coins are not widely held prices are subject to substantive volatility which disincentivizes users from using the coin as a medium of exchange. However, the fundamentals of peer-to-peer cryptography continue to be effective. We can take from the significant milestones already established by the community 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 authenticity of the genesis hash and the size of the payers chain to establish trust. Both the payee and the payer will create a copy of the transaction and consume the hash of the payer thereby creating 2 identical copies of the original chain that can be carried off and transacted independently. Instead of creating a new coin during the mining process the original coin is divided and a portion of the payers coin is given to the payee, naturally any fees associated with mining would be built into the price.

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. The attacker would be better off creating a new genesis block and circulating their own coin. As the original network continues to grow he will fall behind the authentic chain created by mining just one block. As new coins are built the most trusted coins will continue to transact, because both the payer and payee must sign off a transaction coin can only be accepted from an authentic source. As both the payer and payee get a copy of the new block mined the original payer can gain trust while still maintaining a majority portion of the coin.

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

T2 from T1

Owner 1's Public Key 1's Public Key

Owner 1's Signature

Owner 2's Public Key

Transaction 1 (T1)

Owner 2's Private Key

Owner 2's Signature

Owner 1's Private Key

Owner 1's Public Key

T3 from T1

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



**Proof of work**

We cannot alter the amount of coin in our wallet without forging the signatures of all the participants in the chain back through to the genesis block, therefore the quantity of coin can never be altered without receiving the coin from another node and creating a new block.

Both the payee and the payer mine contribute to mining the new coin as both signatures are required to create the new block and 2 copies of the new block will be added to both the payer and payees chain. In this way mining is naturally distributed across independent nodes. It also creates the trust needed to verify the transaction as both parties must agree to the details of the transaction. They will verify the authenticity of the coin from the payer in order to create the next block in the chain both will agree on the amount transacted and both will keep a copy of the transaction.

**Infinite Divisibility of coin**

One key feature of this new version of the blockchain will need to be infinite or at least highly divisible coin. 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.

**Incentive**

As more persons transact with the coin the value of the coin naturally inflates without altering the quantity of coin in existence. Instead, prices of goods and services will decline continually. As ownership spreads the coins intrinsic value will continue to 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 (mining new blocks) quickly as the value of the coin inflates exponentially.

As value can be determined easily (all portions adding to 1) a certain level of transparency is also inherent. As certain coins grow in value they will naturally consume weaker coins as trusted coins are 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 participant’s 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.

**Call to action**

Please assist us with creating a usable version of the coin and may your ventures be profitable.

References

Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." Retrieved from <https://bitcoin.org/bitcoin.pdf>

Thank you,

Lucian Dell’Acqua

dellacqua.lucian@gmail.com