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

**Introduction**

With simple changes to coin architecture described below we hope to address key flaws in existing coins and create the system of exchange and value storage with sound principles.

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.

**Design**  
Our approach merges decentralized payments and ledgers held by individual wallets with a centralized mainframe of public accounts that sum to a fixed total. The accessibility of this mainframe to the public fosters inherent trust. By instituting a mechanism where updates to accounts in the mainframe are rigorously verified to align with the fixed total, we establish a foundation of intrinsic security. This method effectively addresses and resolves several problems including double spending and fraud.

**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 with the public and private key of the next owner and the public and private key of the current owner signing the transaction and adding these to the end of their respective ledgers. They own a copy of their ledgers and this represents the currency in its physical divisible form. Each ledger verifies itself with a public key that is tied to a publicly available mainframe of accounts. Both the payee and the payer will create a copy of the transaction and consume the hash of the transaction thereby creating 2 identical copies of the original chain that can be carried off and transacted independently. Any changes to the public main frame will require 2 signatures from 2 wallets and the total sum of the 2 parties will remain the same. The genesis block is created when 2 parties sign a transaction. Therefore no one can ever own all 100% of the coin and the coin never exists without at least 2 parties verifying the creation of the block.

**Proof of work**

Double pay is avoided because any transaction you commit will need to be verified on the mainframe account structure. Once you spend your coin the quantity in your ledger and the quantity in your public address will be amended. Proof of work is driven by verification, this gets rid of the need for useless computation to give the coin weight.

**Accounts**

Accounts can only be created by the current holders of the coin. New wallets/accounts can be created when the payer hands over his payment in a transaction to a payee that has no account. A new public private key pair is created and added to the account mainframe, the transaction is verified just like any other and then you receive a copy of the payers blockchain ledger which accounts for all spending from the genesis block to the current transaction and contains your account balance. You cannot own an account without a piece of the coin and empty accounts are discarded when their coin is transferred to the new owner.

**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. You will not be able to create any new coins, and this also eliminates the need for additional security and proof of work concepts to ensure the currency does not inflate. Instead, the community of investors controls deflation of the currency with their independent expansion of the credit of their own ledger. They also determine the true value of credit in the coin and distribute new accounts at their discretion. Top of Form

Instead of creating a new coin for each new block the genesis block is initialized as 2 portions of 1.0 coins. The mainframe of accounts will contain 2 public keys with 2 quantities that sum to 1.0. In the first transaction the payer(P1) and payee(P2) freely agree to a division of the entire coin. Let’s say the genesis transaction is completed and person 1 now owns 0.25 coins and person 2; 0.75 coins. 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, P1 need only create a new block and give the agreed portion of his balance. Now P1 has 0.65 coins, P2 has 0.25 coins and P3 has 0.1 coins. All 3 participants now have a ledger that can trace their portion of the coin back to the genesis block and all the participants can continue to transact with each other. 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 and credit**

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 as the value of the coin expands.

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. 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.

Owner 1’s Ledger Owner 2’s Ledger

(T1) or Genesis Block

Owner 2's Signature

(T1) or Genesis Block

PuKey ACC. A: +0.25

PuKey ACC. B: +0.75

ACC. B\_Balance: 0.75

PuKey ACC. A: +0.25

PuKey ACC. B: +0.75

ACC. A\_Balance: 0.25

Owner 2's Private Key

Owner 2's Private Key

Owner 1's Private Key

Owner 1's Signature

Owner 2's Public Key

Owner 1's Public Key 1's Public Key

Owner 1's Signature

Owner 2's Public Key

Owner 2's Signature

Owner 1's Private Key

Owner 1's Public Key

T3 from T1 T4 from T2



Hash T1

Owner 2’s Public Key

Owner 4’s Public Key

Hash T1

Owner 3's Public Key

Owner 1's Private Key

Owner 3's Private Key

PuKey ACC. B: -0.1

PuKey ACC. D: +0.1

ACC. B\_Balance: 0.65

PuKey ACC. A: -0.1

PuKey ACC. C: +0.1

ACC. A\_Balance: 0.15

Owner 1’s Signature

Owner 2’s Signature

Owner 3's Signature

Owner 4’s Signature

Owner 4’s

Private Key

Owner 2’s

Private Key

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Time/Accounts | p1 | p2 | p3 | p4 |
| Acc. A | 0.25 | 0.25 | 0.15 | 0.15 |
| Acc. B | 0.75 | 0.65 | 0.65 | 0.4 |
| Acc. C |  | 0.1 | 0.1 | 0.1 |
| Acc. D |  |  | 0.1 | 0.35 |
| SUM | 1 | 1 | 1 | 1 |

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