Factorial Coin (FCC)

White papers

2017 Michel Kuipers

1. Introduction

In the year 2009 Satoshi Nakamoto introduced Bitcoin as a new digital currency that is secured by encrypted signatures, decentralized and anonymous. It would ensure fast transactions, world width at very low fees, creating a competitive money system compared to centralized banking systems.

After eight years we can evaluate the long-term implications Bitcoin’s design has in practical use and derive the imperfections from it to determine what is necessary to redefine the fundamental needs to create the perfect Crypto Currency.

We will define the solutions for every imperfection we’ll find and in this manner create Factorial Coin (FCC) from scratch to suggest it to the Ecosystem as a new big player in the Crypto Currency world.

1. Preconditions

A crypto currency should respect certain conditions which defines the necessity and therefore right of its existence. To determine these conditions we need to look at the ideas that originally have created the existence of Bitcoin.

The problem the banking systems face can be found in numerous observations:

1. Security. Your money is protected by your identity. Anyone who gains access to your personal data can access your bank-account.
2. Speed. Bank systems have a delay sending money between each others, controlled by a correspondent banking system, like for international transactions, SWIFT.

Especially in weekends this can be a bother.

1. Trust. Banks are their own entities, which you lend your money to reclaim it, but the banks actually own your money and can relend it, invest it, or choose to do with it as they please, creating an insecure system where you are dependent of the acting of the participants of the banking system, which can be quite insane watching the movie ‘The Wolf of Wall Street’.
2. Costs. Bank transfers, especially through credit cards, are quite expensive. You even pay for depositing fiat money to make it digital. You pay for your card, and you pay for your account.

So our new Crypto should respect the facts that it satisfies the conditions to be secure, fast, and trustworthy and make transactions possible at very low costs.

We cannot escape the fact that all transactions should somehow be collected into a ledger, which should be protected at such a way that not a single bit in this ledger ever may be changed to keep it valid.

We will now look at the original design and at each point determine if the practical outcome meets the given standards of the principles our new Crypto Currency should comply to.

1. Evaluation

At the base the original design of crypto currency is very secure. There are multiple levels of insurance, considering the ledger, transactions and ownership. Data is secured by hashing it under the SHA256 algorithm twice, avoiding rainbow table attacks, and which also forms a searchable ID to find the transaction in the ledger. The ledger consists of blocks of transactions; each pointing to the previous one, keeping a consistent chain of validated data, the transactions in a block is signed using Merkle trees to ensure they are original, validated and unmodified in the block. The ownership of claimed money is checked by the Elliptic Curve algorithm Secp256k1 which creates unique digital signatures out of a private key which can be validated with a public key but there is no way to create a signature without the private key. The public keys form wallets-addresses which are used as bank-accounts to claim outstanding (unclaimed) money.

In the original design we have miners and nodes connected in a distributed core-system keeping an individual copy of the ledger and verifying the ledger is correct by taking the longest block chain in time. This design made it necessary to make it unlikely to add blocks at the same time. To establish the goal of dividing blocks in time, a mathematical challenge was invented which must be solved to add the block to a ledger. If a miner solves this problem, the block will be added to the block chain and the miner is rewarded by newly created coins, which brings the supply of the coin into existence. By adjusting the difficulty in time Satoshi could guarantee every node in the system would eventually receive a block in a predetermined averaged interval. In the case two chains were formed, the longest would eventually win, and every transaction in so called Orphan blocks would be refilled into the outstanding transactions. The miners collect and verify transactions to fill a block which they generate and sign, then this block is distributed in the core-network and everyone is trying to solve the mining-process which consists of adding some data, called a nonce, to make the hash begin with a certain amount of zeros.

1. Analytics

Although the current block chain technology is well protected we have to look at the lowest level possible to find its imperfections. When we search for a certain transaction, it is stored in a block, so we have to search the block for the transaction, which is speeded up by using Merkle trees. After this we can validate a transaction is valid. To create a transaction we will have to compare which transactions contain unspent money, these are part of transactions in the blocks that contain the wallet of the receiver, and the valid signature of the sender which have no following block in the ledger, where the receiver has, at his turn, has spent this money. Likewise we have to walk through the whole ledger from the beginning to see if money is spendable or not, which takes up a really long time if not implemented wisely. In most crypto currency implementations the wallet-software calls a known API dedicated to provide spendable blocks to create a transaction.

To avoid inflation, Satoshi reasoned that there only could be a finite amount of Bitcoin. Since the miners create the money out of nothing by creating and validating the block chain, the miners receive less and less reward in time. The specifics can be found here: <https://en.bitcoin.it/wiki/Controlled_supply>

Now the problem arises that it takes up a lot of effort and therefore energy (electric power) to earn newly created Bitcoin, and the consequence may be people stop mining. The solution the core-developers suggested is that transactions have to pay more fees to the miners, who collect the transactions in the first place, making it an actual problem some transactions are delayed a long time before being integrated into the block chain. This has the implicit danger of raising the fees on a transaction before even being considered to be integrated into the block chain. Another problem is a block is limited to 1 Megabytes of data, so if the miners are limited in time to be able to solve blocks to add them to the ledger, there may be more blocks then there could be mined in time, delaying transactions. To verify a miner has mined a valid block, it has to wait 100 blocks to be added to the block chain to spend their earned money.

Since Bitcoin is a minable coin, more and more people started to mine, and where you used to be able to mine with CPU and GPU, now you can only effectively mine with dedicated hardware devices called ASIC. A few companies, especially based in China, have built such large mining farms of ASIC devices; they actually control the creation of blocks into the system. This give them an advantage over the future developments of Bitcoin, which have already lead to many hard-forks like B2X, BCH and BTG, in which case a part of the network developers insisted that Bitcoin should stay decentralized at its principle values, and speed up transactions under lower fees, therefore decided to split up from the centralized core.

1. Conciliation

To solve the defined imperfections current Crypto Currency faces we must not be afraid to redefine the fundamental base of which it’s consist.

* A transaction is a transfer of spendable money sent to a wallet that is property of anyone who has access to it by signing it with their private key. The recipient can spend the money, which corresponds to its wallet, by claiming it, through singing it with its private key. Anyone can verify this transaction by verifying the signature corresponds to the public key and wallet that has spent the money.
* A ledger is a collection of transactions validated by a hashing verification and signed by the spender.
* A miner creates new (called coinbase) money to add to the circulation supply by verifying mathematical problems biased on a certain time-interval.
* The system at any point has to validate the transactions are valid and are not already spent on the ledger, and does not invalidate pending transactions. Illegal transactions should be ignored and deleted.
* Fees must be low, always, to buy anything without extra costs.
* The time it costs for transactions to be included in the ledger must be as short as possible. This determines the time the receiver can spend the money again. Also miners should be able to spend their deserved coinbase money as quick as possible.
* The core network is a decentralized collection of interconnected nodes, validating the ledger’s accuracy, where every node should have the same abilities as any other in the whole network, making it impossible for anyone to gain power over the whole.
* Every node should be able to individually act as an API for wallet-applications that want to create a transaction and send it. The node should respond with appropriate information.

1. Inspiration

A transaction basically consists of a collection of spendable blocks, that are gathered together, validating they come from the same wallet that spent the money, signed by the owner of this wallet, to give to wallets, connected to public keys, who can claim this money again by signing it through their public and private keys. To validate a transaction we need to make sure the wallets are corresponding with the signing public key, the signature and the amount spent. To create a transaction we have to find all spendable blocks corresponding to a wallet and see if the amount spendable is enough for the transaction to be created.

The ledger can connect these transactions at any manner, as long as all decentralized nodes agree on the order. So we need to build in a security that guarantees the order in which transactions will appear in the ledger, and exclude any disconsent of cores to a consensus the absolute majority of nodes have agreed upon.

We absolutely must ensure we use the finest, best, fastest encryption possible keeping an eye on Moore’s law, hackers and all development in the future.

Since a miner’s basic function is to create new coinbase money in time, the question arises if the core-nodes or the miners should validate and collect transactions into blocks, or even use a block chain to collect transactions, or just add transaction to a ledger. The function of nodes and miners may be redesigned from scratch.

Since at any point the actual process that writes data into the ledger, it would be a wise choice to let the core-nodes validate the transactions, raising the questions why miners should too, since their main goal is to create coinbase coins.

Every node in the network should have the exact possibilities of any other node in the network, there must never be a main node controlling other nodes.

No application, we call a leaf, like a wallet, may ever control a node. Should miners control a node?

Core-nodes are able to keep a list of transactions that are not yet added to the ledger, but can validate that they will be at some point in time by comparing these ‘pending transactions’ to the list of to be processed transactions. This makes it possible to have very quick conformations in stores when buying your bread, where the store-holder is secured it will receive its money to spend again very quickly.

When somebody wants to make a transaction it should be very easy to contact the FCC-network and get the necessary information to create and verify a transaction. This never should be done by a centralized API, but every node in the core-network should be able make a transaction by exploring the ledger to search for spendable blocks corresponding to the spending wallet of the transaction.

When the supply of the coin is limited, the miners will no longer be interested in mining the coin; therefore the fees of the transactions must rise to provide miners their rewards. This is in contrast to our principle goal, so there must be an unlimited amount of coins to be mined, to control this, the difficulty of the to be mined problem must vary, to stay in synchronization with the amount of coins we want to create, which should be rather little then more, to not overflow demand in time and in time keep the value of FCC stable.

The processes which actually validate the transactions should be rewarded for it. This should be a very quick process.

1. Creation

The main problem that can be deduced is that although it takes some time to find a transaction to be validated, because they are collected in blocks, it takes a hell of a time to find all spendable blocks a wallet may claim. Since the ledger is huge and only huge databases determine such answers quickly, most wallets use an API to generate their spendable blocks. Our design asks for a system where any node can perform this task.

The only way to solve this is to split the spendable blocks into separate entities we can mark as being spent or spendable. By doing this we separate the not-spendable blocks, we can use to identify the spendable blocks, so we call these Ident-blocks, which can be input-blocks for transactions, or coinbase blocks. Also form a logical base for the genesis block to initiate the whole system.

Since miners are mining hashes at very high electric costs, and we want to give them a meaningful task, it would be advisable to derive the miners of the task of validating and collecting transactions into blocks and give this role to the nodes, where the main task of miners will be to create new FCC-coins by calculating random given problems to solve, which can actually benefit fields of research.

Since nodes now fulfil the task of keeping the ledger intact and validating the transaction, it’s fair to give everybody who is running a node, a share of all profit, which is translated into fees which everybody must pay to make a transaction. This guarantees the network is always alive and decentralized, because there will always be running nodes wanting to earn some money, just like miners will always want to earn coinbase FCC.

Since we want the transactions to be cheap we must allow a minimum fee of 0.01% and you should never have to pay a higher fee. Why higher fees are possible is very simple, the core-network will earn more money, which pleases the whole network, which will protect your money and allow it to be transferred very quickly, but also a higher fee means your transaction will be added to the ledger more quickly, enabling the receiver to verify that they can spend your spent money, building more trust between you as sender of the money and the receiver of the money, so trust is worth the value of the fee.

1. Implementation

By splitting transaction into Ident-blocks and spendable blocks, we get a structure as follows: