How digital money faces double-spending in decentralized environments

Money has value if and only if other people believe that it has value. Money can be represented by coins and banknotes, or by any other arbitrary elements, no matter whether they are of physical or virtual nature.

One property is common for all kinds of money: People need to trust the market. If the rest of the market decides that the currency is worthless, then you cannot e.g. buy a loaf of bread for the money you have. More specifically, if a baker doesn't believe that he will be able to buy a bag of salt for the money you are going to give him for the loaf of bread, then the baker will refuse to sell you his bread for your money. In this aspect, virtual money is no different from physical money.

In usual financial systems, you must also trust a central bank. The national bank could easily nullify all financial value stored if the national bank was driven by a malicious leader. Cryptocurrencies (Bitcoin, Ethereum, etc.) aim to avoid this issue by decentralizing the currency. Everybody can contribute to administrating the currency and nobody can significantly impact the currency on their own.

Using digital signatures, we can enforce authorization of payments. Nobody can create a transaction that subtracts money from someone else's account. Furthermore, the list of all transactions is cryptographically protected from changing only a part of it. The technology is called blockchain.

New blocks are added into the blockchain in a process called mining. Miners contribute to maintaining this distributed database of transactions. At the same time, miners receive a predefined amount of digital money for providing this service. A miner who extends the blockchain with a new block can potentially "cheat" by including only some selected transactions into the new block, but transactions from all older blocks are secured. The miner cannot edit already-confirmed transactions in the blockchain without allowing everybody to discover what he did. If there are enough honest miners in the network, all frauds get eventually revealed.

The other problem, which is much worse, is called double-spending. With physical money, it is no issue. When I spend a banknote, I no longer own the banknote. Someone else has it; and I am not able to make a copy of the banknote on my own[1]. However, if money are represented by a file in my computer, there is no guarantee that once I send this file to someone, I will not use the same file again and again.

Let's say I want to buy something for my digital money. I put the record about the outgoing transaction into the blockchain; and after the second party is sure this transaction has been performed[2] and I obtain the goods, I delete the record of the transaction from my local copy

[1] Such an act is called forgery. Banknotes are designed in such a careful way, that forgery is hard to perform and easy to spot. You will see that we often want a similar property in cryptography.

[2] Somebody confirmed the transaction by adding it to the blockchain. This entity also had to calculate it into the new hash.

of the financial history. Now, I claim that I have the full transaction history, and I can spend the same money again. In case of “conventional” internet banking, there is a central authority (the bank) which keeps track of all transactions, so the bank knows the balance of every account registered in the bank. The central authority effectively prevents such a blatant fraud.

What happens with decentralization? I can argue with other parties about which transaction really took place. The blockchain can get “forked” and nobody knows for sure which “branch” is trustworthy. Nobody has implicit priority to be trusted by others.

The canonical solution is to make users vote about which transactions are valid. If the voting is done carefully, we can obtain a consensus about the legality of transactions, without any single entity being in charge of everything. As long as most voting users in the network are honest, it is impossible to double-spend one’s money.

How to perform this voting? We could, for example, count the number of accounts voting for vs voting against. However, this process would be vulnerable, because anybody can create as many accounts as they want, if the accounts were e.g. bound to an e-mail addresses. Thus, we need something that isn’t easy to have a large amount of. Keep in mind that there cannot be a central authority which registers all accounts, so that we could restrict e.g. one account per person. Moreover, this would undermine the Bitcoin’s pseudonymity, which is appreciated by many users in the network.

One way to make excessive voting too expensive, is to force users to spend a lot of computing power on creating their vote. Have you heard of hash functions? They are functions that can be easily calculated, but are hard to be inversed. If we force voters to find a value x such that h(x) is a very small number, then it takes a long time to find such x. We skip many details here, but the main idea is simple. You vote by crunching some codes which take a long time to crunch.

This idea of Satoshi Nakamoto was revolutionary in 2008. It was quickly adopted by many decentralized services in the growing world of the internet. Unfortunately, Bitcoin is not sustainable in a long term. The more users the network contains, the more computational power is wasted on producing these so-called Proofs-of-Work. Moreover, this computation, which was originally supposed to be performed by idle CPUs of Bitcoin users connected to the internet, is now performed by highly specialized hardware. This hardware is manufactured specifically for calculating Proofs-of-Work very fast. Normal users, who don’t possess this hardware, have only a negligible voting power. As a result, Bitcoin faces a severe crisis with respect to its economy, its ecology and its security, too.

As a natural consequence, there is an increasing demand for replacing Proof-of-Work by a different mechanism. The current state-of-the-art solution to this problem is a cryptocurrency named Chia, proposed by Bram Cohen and Krysztof Pietrzak. They abandoned the Proof-of-Work mechanism.

Chia uses two new mechanisms instead: Proof-of-Space and Proof-of-Time. These mechanisms lead to a cheaper and eco-friendlier cryptocurrency.

Instead of voting by computational power, users vote by their dedicated disk space. Unlike the heavy processor machinery, buying a large hard drive is just a one-time investment. The more memory a user has, the higher chance the user has to obtain a good Proof-of-Space instance. Proof-of-Space is basically a fast lookup into a precomputed table. When the Proof-of-Space has been found, other users compute a Verifiable Delay Function. This Verifiable Delay Function is a long serial computation, performed by only a few users in the whole network. These steps make all participants equal, as the calculation slows down the mining process, without wasting any significant amount of energy. Bram Cohen, the CEO of the Chia Network, describes the technique as follows:

"You need to have a system where not only don't you need a CPU to farm it, but you can't use a CPU to farm it. (...) Let's mix together Proofs of Space and Proofs of Time. (...) The combination of those needs to take a while, but it doesn't use up a lot of electricity. Instead of everyone in parallel burning electricity until they come up with the winning lottery ticket [an analogy to a sufficiently low hash], everyone looks up in advance, using the Proof of Space, who is going to win in the end, and then you sit around waiting for his Proof of Time to be done."

available online: https://youtu.be/tWa_ztvU4Nw