How does a blockchain operate?

Gautier Marin-Dagannaud,
engineering student at Télécom ParisTech-Institut-Mines Télécom and Master's student at École Polytechnique, currently at Ledgys

In J.P. Dardayrol, editor of the special issue *Blockchains and smart contracts: The technology of trust?* of *Réalités industrielles*, 2017

Abstract:
Blockchain technology is disruptive. To gauge its potential, we must understand how it operates by examining its original use for bitcoins. A blockchain is a distributed ledger shared among participants in a network. Like any register, the users have to be identified; and transactions modify the ledger's state. Unlike nearly all current ledgers however, blockchains work without a central controlling authority… whence several issues and technical problems.

All current software platforms (Facebook, Amazon, Uber, on-line banks) have a point in common: they are organized around a central actor whose duty is to maintain the platform's integrity and oversee its development. This centralization has advantages, in particular scalability and the rapid management of conflicts; but it also has several disadvantages, such as censorship, monopolies or the vulnerability to attacks.[1]

Blockchain technology allows for a decentralized sharing of a database, *i.e.*, between parties who do not necessarily trust each other and without any central controlling authority. Software platforms of a new type — decentralized — can thus be set up. To grasp this paradigm shift, let us examine this technology's origins.

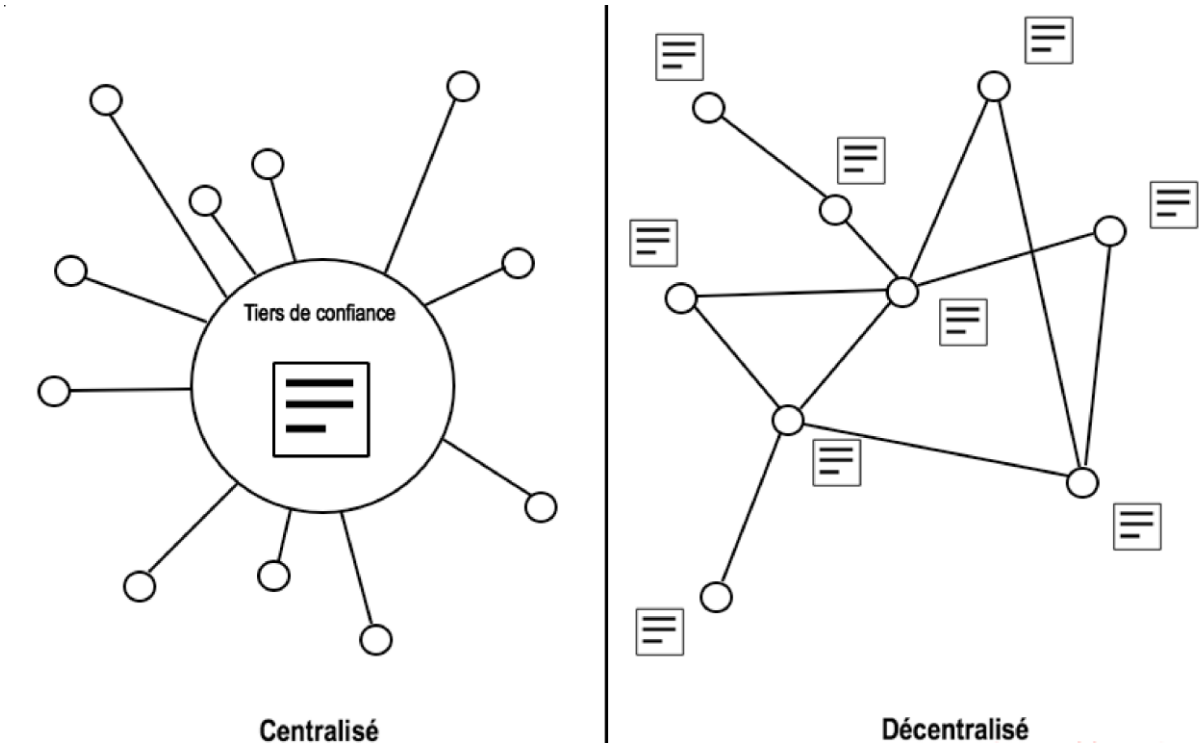

Figure 1: Two systems for keeping a ledger: Centralized (the trusted third party at the center) vs. decentralized

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France).

How does a blockchain work? The example of Bitcoin

Blockchain technology was originally invented to create the first digital currency, bitcoins (BTC). Bitcoin is a decentralized network of digital payment based on this cryptocurrency. As in any payment system, a ledger of accounts has to be updated in order to know each user's balance. In the "real" world, banks keep the ledger. When sending money to someone, you have to go through your bank, the centralizing organization, since it keeps the ledger of your accounts. At the foundation of Bitcoin is a fairly simple principle: instead of a single private party keeping the ledger, it will be "distributed" to be kept in a decentralized way. Each computer, called a "node", in the network contains a copy of the ledger and helps update it. This decentralization protects the ledger. Even if one or more nodes are altered or destroyed, the ledger will remain in tact as long as honest nodes exist in the network.

User identification

Network users are identified by their addresses, where other users can send them bitcoins. Each address has a private key for "unblocking" bitcoins. An address is generated by a user locally via his/her private key. This operation involves complicated mathematical functions that, suffice it to say, operate in a single direction. It is nearly impossible to discover the private key associated with a given address, but it is very easy to find the address corresponding to a private key.

To unblock funds, the user does not have to communicate his private key to the network. If he did that, the nodes receiving the information could spend the bitcoins linked to his address. Instead, he generates, always locally, an electronic signature associated with the transaction to be made. This signature proves that the person possessing the private key has definitely approved the transaction. It is unique and cannot, therefore, be reused for another transaction. Furthermore, the mathematical function for creating the signature is one-way. Nodes in the network cannot, therefore, guess the private key associated with a signature.

The electronic signature procedure serves to authorize transactions without revealing private keys over the network. Although electronic signatures are indispensable to the operation of Bitcoin, they are not an innovation specific to blockchain technology.

Foundational techniques

What is innovative about blockchain technology is the procedure for forming a "consensus". This innovation proposes a solution to what is called the double spending problem, which weighs heavily on any decentralized system. Let's suppose that a user signs and sends at the same time two transactions (*A* & *B*), each to a different seller but to be paid with the same bitcoin. Some nodes will receive the transaction *A* first; and this will invalidate the second transaction when it is received; whereas other nodes will receive *B* first, thus causing the other transaction to be invalidated when it is received. At the scale of the network, there will be a disagreement between nodes on the state of the ledger.

To settle this problem, Bitcoin records in chronological order (using a timestamp) each transaction in a chain of blocks, and every node in the network has to synchronize with this blockchain. Thanks to this chain, which is unique, all nodes manege to agree on the state of the ledger. The blocks contain a list of the transactions that have modified the ledger. Blocks are added at the node level. All nodes thus possess an identical copy of the blockchain (identical save for a few subtle differences). Each block references the preceding block, thus forming a chain stretching back to the "genesis block", the very first block on the chain. To know the ledger's state at any given time, a user can trace the chain from the original block to the last block added.

The operation of a blockchain simplified

After a transaction is generated by a user, it is transmitted to neighboring nodes and then relayed peer-to-peer over the network. The transaction will be validated only if the user has the funds on account and if his/her signature is valid. However a transaction is not finalized until it is included in a block. Furthermore, two transactions that are trying to spend the same bitcoin cannot be included in the same block. In this system, double spending is, therefore, impossible.

But which node has the right to create the next block? The nodes that create blocks are special. They are called “”miners”. Any node may become a miner. A cybernaut needs but to have appropriate hard- and software. When miners receive a new, unvalidated transaction, they place it in a set of unconfirmed transactions. Each miner has its own set, which might be different from those of other miners because of the lead time in transmitting transactions over the network. A transaction leaves this waiting list once it has been placed in a block.

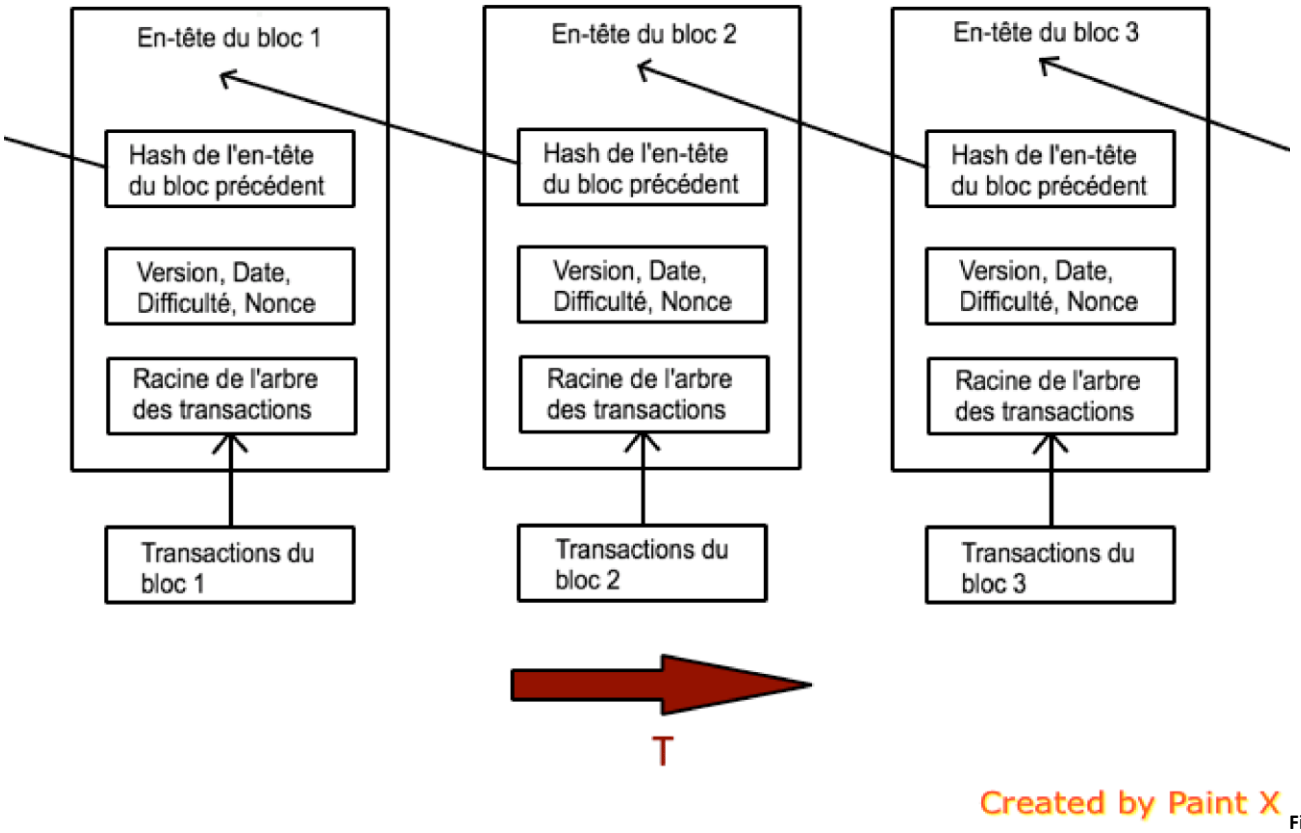

Figure 2: The operation of a blockchain simplified: A bock’s header (hash from the header of the preceding block; Bitcoin version, timestamp, difficulty target & nonce, the counter for generating a correct hash; the Merckle root) followed by its transactions.

Creating a block: Proof of work

Any miner can collect a certain number of transactions on its list, verify their validity and form a block. However this block will not be validated as long as the miner has not produced the “proof of work” associated with the block. This proof is hard to make but easy to check. Without it, nodes in the network cannot validate the block, not even if the transactions on the block are valid. The difficulty of bringing this proof is the basis of the decision about which of the blocks created by miners will be added to the chain.

To bring this proof, miners have to calculate the value of a function that uses the preceding block's hash, the current block's hash and a variable called "nonce".[2] Miners make variations on this nonce until the result of the function meets the conditions preset by the protocol, in particular the parameter called "difficulty", which defines the range of valid results. The greater this difficulty, the more this range is restricted. This makes it more complicated to discover a valid nonce. Once again, the function is one-way. Predicting in advance a nonce that will meet the conditions set by the protocol is, therefore, impossible. So, the only way to find a valid nonce is for computers to calculate a very large number of nonces, evaluate for each of them the value of the function, and verify whether or not the result is valid. At a node's scale, it would take several years to find a valid block. At the network's scale, the difficulty to be solved is set so that a node needs, on the average, ten minutes to find a valid block.

Though hard to bring, this proof of work is easy to verify. A sufficient condition for checking the validity of a proof is to evaluate the value of the function for the proposed nonce. To make an analogy: finding a padlock's combination through trial-and-error iterations is a very long process, but it is very easy to verify whether a given combination opens the lock, *i.e.*, whether it is valid.

Adding blocks to the chain

Once the proof has been brought, the winning node adds its block to the chain. It is said to have "mined" the block. It receives, along with eventual transaction fees, a payment in bitcoins, the amount set by the network (currently 12.5 BTC). Bitcoin provides this payment as an incentive to miners who see to the upkeep of the ledger. This is the point of entry of bitcoins in this system.

This miner then transmits the block over the network. All the receiver nodes verify the validity of the transactions on the block and the proof of work, and then add the block to the chain. If the node is a miner trying to mine a block, it has to add this new block and then resume the process of mining. Recall that each block refers to the preceding block.

A node might receive concurrent blocks, or series of blocks, that have been validated. When this happens, the rule is to accept the longest chain. This rule implies that an attacker must be capable of producing a valid chain of blocks longer than the chains on which "honest" miners are working. In other words, the attacker has to have more than 50% of the network's computing power, whence the name: a 51% attack. The higher, the combined computing power of miners; the safer; the network. Take note, however, that such an attack would not enable the hacker to steal bitcoins, since the digital signature procedure protects them. The hacker could, at most, spend some bitcoins twice or cause a denial of service.

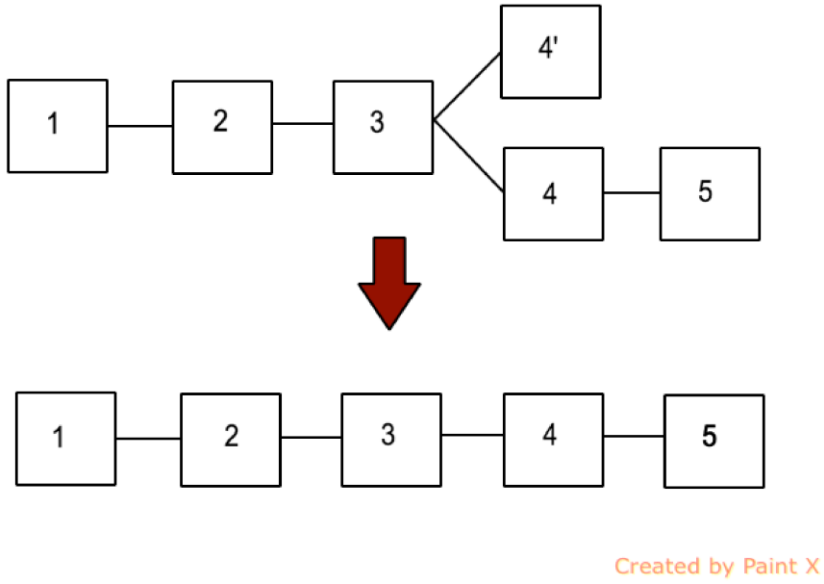

Figure 3: Forking and the switch toward the longest blockchain.

[2] A hash, or hash value, is the result of a one-way hashing function that is applied to input data. It is normally a hexadecimal number (base 16) of a fixed length (256 bits, for example). For the same input, the same hash will be obtained. On the contrary, determining the input data from its hash is nearly impossible.

Beyond currencies…

The “Internet of value”

The technological innovation represented by blockchains has been overshadowed by its initial application, the cryptocurrency bitcoins. But an awareness of its potential soon emerged.

Bitcoins are but a series of *0*’s and *1*’s that can easily be duplicated. How to secure the value of an asset that can be indefinitely duplicated? In the case of fiat money, a central authority sees to the ledger’s integrity. In the case of bitcoins, the blockchain guarantees that the money supply will not be increased. A blockchain’s principal merit is to endow digital assets with value without recourse to a central authority.

There are other digital assets than cryptocurrencies. For example, the “colored coin” protocol can be used for real assets (deeds for real estate, stocks, bonds) via the Bitcoin blockchain. Other blockchains have been set up to create tokens. For example, Ethereum is a blockchain with smart contracts, which are programs executed by nodes in the network. Contract-making can thus be automated and transposed to digital assets. Via Ethereum, an infinite number of digital assets can be deployed in the blockchain; and their management, automated thanks to these smart contracts. Once such a contract is on the chain, it is impossible to cancel it or halt its preset execution. Only a worldwide consensus of all parties in the network (miners, developers, and users) can roll back the contract’s execution. For this reason, a blockchain is the system that most stoutly resists third-party interventions that we have ever had.

New platforms, new issues

There are now hundreds of blockchains for hundreds of different uses. Several decentralized platforms have been created. They are not proprietary, they are open source. This implies several changes in the distribution of value along the chain for producing it. Cryptocurrencies play a major role in this redistribution. When a platform is launched, a cryptocurrency specific to it is also usually created. It is distributed following the programmed rules governing the platform, rules that evolve in compliance with the platform’s governance, such that the distribution of the currency tends toward an optimum. In line with this free-enterprise rationale, stakeholders are rewarded as a function of their contributions. This contrasts with existing platforms where a central authority distributes value and responsibility.

Points of centralization still exist however. In particular, centralized organizations run the immense majority of platforms for cryptocurrency transactions. Nonetheless, decentralized transactions are growing. There are even plans for interconnecting blockchains in a decentralized way. This would open the way toward a world of platforms interoperating without friction. Nonetheless, several issues — technical, legal and organizational — must be addressed before entering this new world.

References

https://bitcoin.org/en/developer-guide#block-chain

http://bitcoin.stackexchange.com/questions/22/is-it-possible-to-brute-force-bitcoin-address-creation-in-order-to-steal-money

http://bitcoin.stackexchange.com/questions/11054/understanding-spv-simple-payment-verification

https://en.bitcoin.it/wiki/Main_Page

https://github.com/ethereum/wiki/wiki/White-Paper

http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html