A Deep Introduction to the Blockchain

Martin Rupp
SCIENTIFIC AND COMPUTER DEVELOPMENT (SCD)

Introduction

Blockchain technology is everywhere, and many sales managers, engineers, specialists, and developers use the term every day in the context of their work. But do they really and can they really define blockchain technology accurately enough? The goal of this article is to give them some insight into the topic.

A first overview of the Blockchain concept

The main idea of blockchain is creating a cryptographically secured chain of blocks that no one can tamper with.

The initial idea originates in the 1990s from a 1991 paper entitled "How to Time-Stamp a Digital Document" authored by Stuart Haber and W. Scott Stornetta.

The ideas behind blockchain existed even before, in theoretical computer science, with the Paxos protocol for example.

Timestamping a document can be done for legal acts or patents for example. An existing scheme is described by the author, it consists of hashing the document, and sending it to a trusted time-stamping service (TSS), which will add the time and date it receives it and sign the whole data.

The objection to that scheme is that no matter how “trusted’ The TSS is, it *still* could be a rogue provider and could emit false certificates.

The paper details ways to perform timestamping of documents by two methods which prevent attackers from defeating the use of signatures or hash functions and guarantee that even if rogue TSS exist, they couldn't tamper with the documents.

Therefore the origin of the blockchain is to be found in a general distrust towards the "established" chain of trust with "legitimate" bodies (notaries, attorneys, etc..).

The two solutions proposed by Haber and Stornetta consist of using either a centralized authority - with the risk that this centralized authority still could be untrusted- or distributing the trust requirements among all the users.

The first solution ("linking") uses indeed a central authority that controls the certificates emitted by the TSS, making fake certificate emission almost impossible - at least very hard.

The second solution (“distributed trust”) can be seen as the origins of blockchain technology. The requirements are :

- A secure signature scheme ζ
- A pseudo-random number generator *G*

We suppose that clients are identified by their IDs and that there are n clients $Id_1 .. Id_n$.

A client needs to sign a document x It will first hash x to get a value $y = H(x)$. Then the client will use *y* in the PRNG G to get *k* random clients id:

$$(Id_1, ..., Id_k) = G(y)$$

The client sends a request to these *k* clients to sign his data. Each client returns - using the secure signature scheme - the signed data $\zeta_i = \zeta(t, y, Id_i)$.

The timestamp τ is then defined as:$\{(y, Id), (\zeta_1, \zeta_2, ..., \zeta_k)\}$.

Haber and Stornetta then claim that the timestamp τ is secure. Indeed the only way the timestamps could be fake is because *all* the k chosen clients would cooperate to produce such a counterfeited signature, either by commonly changing the date and time t and/or by changing the hash data.

Since the clients are chosen randomly (via a "lottery") this is practically an impossible scenario. Indeed we can reasonably expect only a fraction of the chosen clients to form a machination/conspiracy against the requesting client. Not only are these clients not in advance that they are chosen but the probability that k random clients are malevolent must be extremely small. As a matter of fact, if *e* is the proportion of rogue clients in the total population of the client. The probability *p* for k randomly and independently picked clients to be rogue is $p = e^{k}$

This simple mechanism is, in fact, *the blockchain*.

For instance, if we consider a rate of 5% of rogue clients (which is considerably high), we get the following values of p:

k	p
5	~0.00004%
10	~0.00000000001%
20	$\sim 10^{-25}$%

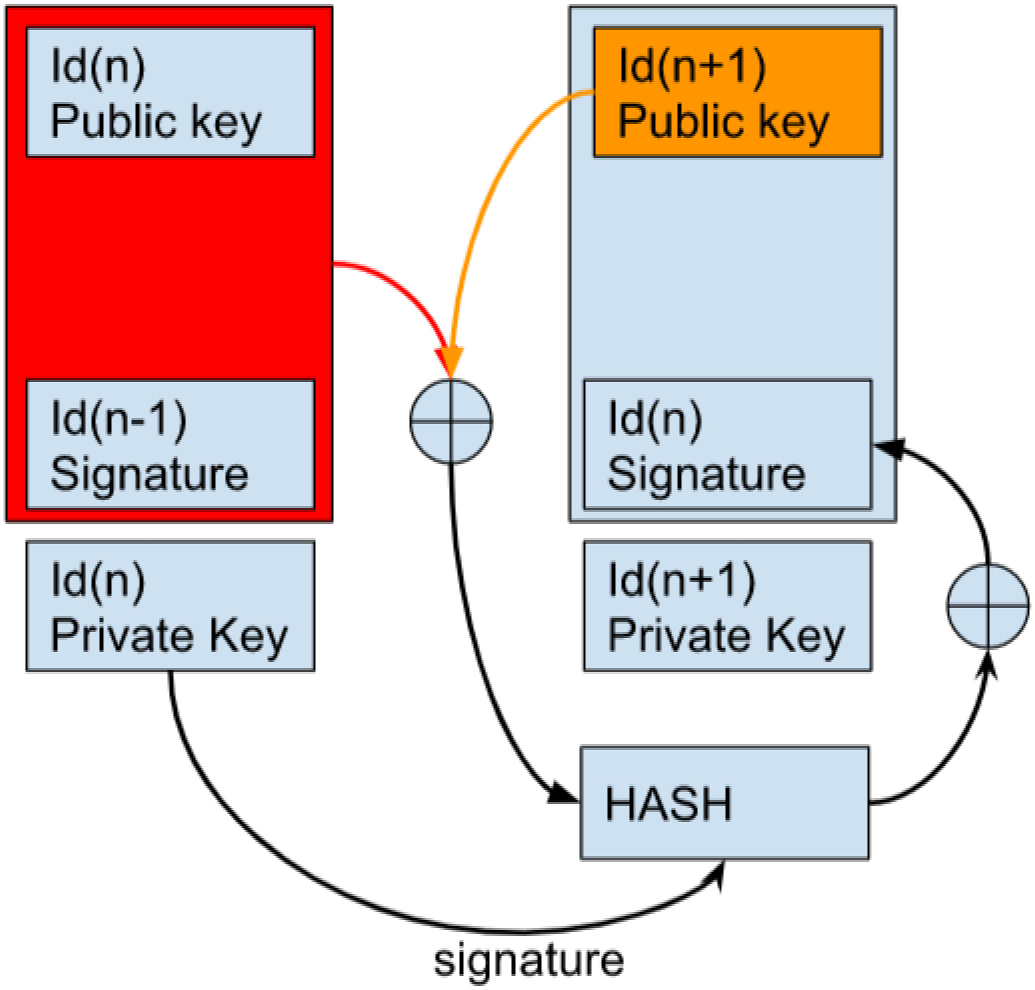
This simple computation shows the power of the blockchain. While technically possible, collusion between randomly chosen clients has such a low probability that it is simply concretely impossible.

Evolution of the blockchain

The Blockchain concept evolved from the original idea, after a paper named “Bitcoin: A Peer-to-Peer Electronic Cash System” and authored by a certain Satoshi Nakamoto was published in October 2008.

The paper from Nakamoto re-uses the blockchain concept in the context of peer-to-peer financial transactions. An electronic coin is defined as a chain of signatures. It’s different from the initial concept introduced by Haber and Stornetta because the signatures are *chained* and not concatenated, independently of each other.

Each time the coin is transferred to another user, the chain of signature - which represents the coin - increases.



In the peer-to-peer system (The "Bitcoin") described by Nakamoto, each time the coin is transferred from the owner with ID(n) to the owner with ID(n+1) then the transaction is hashed with the public key of ID(n+1) and then the hash is signed by ID(n) and finally concatenated to the coin itself.

In such a system the chain of signatures can be verified to prove ownership.

Such a system needs an authority to prevent coins from being double-spent for example. A central authority is not considered a valid solution because all the trust relies on a single entity.

The solution chosen by Nakamoto is to publish the transactions, using a timestamp server. Rather than publishing the transaction to a web server like Usenet or any public chat group, Nakamoto prefers to develop the concept of proof-of-work.

The proof-of-work consists of proving that a certain hash containing a certain amount of leading zeros has been generated. Then some reinforcement systems are described to make the whole system more secure and finally reach a decision whether the transaction is approved (or not).

The puzzle to solve is the following. Find a nonce (and therefore a hash) such that :

```
SHA256(“blockchain” + Nonce) = Hash Digest starting with
“000000”
```

The number of leading zeros defines the difficulty of the challenge.

The proof-of-work is a cryptographic puzzle that can be solved by anyone equipped with enough hardware. It is usually called *mining*. Mining is a rewarding operation where miners compete against each other. The idea is - again - that ‘honest’ miners are dominating and that therefore the chosen block will always be trustworthy.

Mining is also a protection against denial-of-service because of the inner difficulty of the challenge and as such, it acts as a protective and defensive barrier.

Mining is a consensus since the competition will lead to a decision.

Other such consensus systems are the following:

- Proof of stake
- Delegated proof of stake
- Round Robin
- Proof of Authority/Identity
- Proof of Elapsed Time

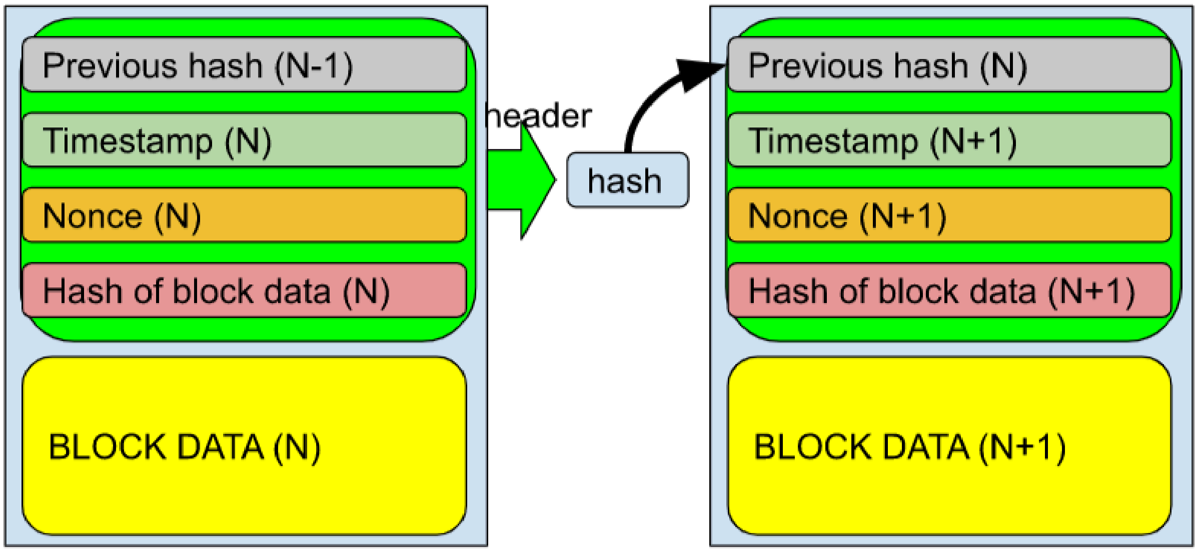
Since the computed hashes containing the timestamps are incorporated into each block, the whole blockchain cannot be modified at all by an attacker.

The system proposed allows trusted transactions ... without relying on trust at all.

Actual blockchain technology

The actual blockchain technology is almost entirely consumed by cryptocurrencies, especially the Bitcoin (BTC).

The “typical” blockchain used by Bitcoin and many other cryptocurrencies consists of a chain of so-called blocks, containing a header and block data. The block data represents the transactions and other similar data.



The block data represents a list of transactions and not just one transaction.

Blocks are *published* over time. Determining which ones (“miners”) will publish the next block lies in the consensus process.

The motivation to publish blocks is purely and simply financial gains. The users who are inside the blockchains are not seeking especially the well-being or harmony of the system. Nevertheless, a consensus model is needed so that distrusting users will cooperate.

Every blockchain network has a genesis block (e.g. the "initial one" without a predecessor) and after it, blocks are added one after the other.

The proof of work is also referred to as *mining* because it consumes real physical energetical resources such as electricity and processor power for instance.

The proof of work is often - if not always - motivated by a financial reward and miners are generally not interested in the ‘well-being’ and harmony of the blockchain network that they have joined.

As we mentioned earlier, the proof of work is not the only possible consensus. There exists as well the proof of stake for example.

While the proof of work is used in Bitcoin, proof of stake is also of interest. For example, the Ethereum network is imminently moving to proof of stake. The proof of stake, the same as the proof of work, allows a user to demonstrate an interest in the system with the idea that the more a user has invested time, resources, energy, etc.. in a system, the less he is prone to be malevolent against it.

Attacks against a Blockchain

Despite its apparent impressive security, a blockchain is not at all a silver bullet. There are several flaws in the protocol and the implementation of the protocol which to the difference of bank transactions, like credit card processing, is not at all mature.

Cryptocurrencies, the largest consumers of blockchain technologies, are very new and lack the experience in security that the oldest and largest financial institution possesses.

Proof-of-work and proof-of-stakes are not exactly new concepts. They have been existing for decades in the banking industry.

Several attacks do exist against a blockchain, for example, the 51% attack or the Sybil attacks.

There had been, at the start of 2019, several attacks against the Ethereum classic, where attackers could get control of more than half of the network computing power (51% attack) and start rewriting transaction history, allowing double-spends. This is just the tip of the iceberg and sooner or later the network will be forced to evolve and introduce some sort of control systems, therefore killing the very idea of blockchain.

Conclusion: in that article, we saw the main functioning and features of blockchain technology. This is a relatively new technology and far from being mature and may still be considered very experimental despite its many strengths. The future will decide on its final shape.