A Survey of the Concept of Blockchain security Challenges and Risks

Jawed Qureshi
Sr. Quality Control Engineer,McKesson Corp, VA, USA

Abstract

The Blockchain [1] is the new buzzword in the world of technologies. All sectors have started to focus on concrete use cases, but only few actors can claim of having devised revolutionary solutions. For many reasons : Blockchain technology has been around for a while and remains very complex to understand. The Blockchain is the partie of technologies to monitor in the years to future. It could revolutionize many sectors of the economy, starting with banking and insurance. This document will presents in detail the following points: what is Blockchain and how it starts ? Blockchain security challenges and threats ? and to finish how we can secure this technology ?

Keywords — *Blockchain, decentralized, bifurcation, Security Challenges, Threats*

I. INTRODUCTION TO BLOCKCHAIN

The Blockchain is a technology that stores and transmit information transparently, securely and without a central control body. It looks like a large database that contains the history of all the exchanges made between its users since its creation. The way the Blockchain is used can be as follows: in a first linker in asset transfers (like currency, securities and shares), after alle can also be integrated for a better traceability of the assets or the products or for the automatic execution of different contracts ("smart contracts"). Blockchain has a decentralized architecture which is not hosted by a single server but by some users. As there is no intermediary so that everyone in the network can check the validity of the chain . The information contained in the blocks (transactions, property titles, contracts, etc.) is protected by cryptographic methods that prevent users from modifying them afterwards.

A. Operation of theProtocol Blockchain

This is the first part on Blockchain technology. The goal here is to understand how Blockchain technology is a natural solution to the asset transfer problem between two agents without a trusted third party.

Bitcoin [2], a project of decentralized and secure virtual money exchange, was born following the crisis of confidence of 2008 towards the financial institutions. Its stated aim was to dispense with trusted intermediaries whose role is to certify and record the history of monetary transactions, namely banks.

This decentralized system[15], made up of thousands of computers around the world, is a sort of public, anonymous and distributed registry:

- Public because everyone can access the contents of the registry without a request for permission
- Anonymous or Private because each user is associated with nothing more than a set of alphanumeric addresses containing Bitcoins
- Distributed because there is no central certificate authority for transactions.

To understand technically how these three properties, articulate to certify exchanges, consider two people. Alice and Bob want to carry out a double transaction; a transfer of a monetary asset (payment) which triggers a transfer of another type of asset (sending by mail of a good, realization of a service, etc.). We will gradually build a digital currency called for example "Infocoin" allowing a secure exchange between the two agents. The solutions to the various obstacles encountered will allow us to show how the Blockchain protocol is a "natural" solution to the problem of secure value transfer.

B. Different Steps Operating of Blockchain protocol:

There are many Application of Blockchain Technologies uses by Blockchain protocol like Bitcoin, Ethereum [3], Hyperledger [4], other… This part represents the steps of how all those applications work.

a). Step-1 The Concept of Digital Signature:

Alice, who is trying to transfer an Infocoin to Bob, can send a text file where she writes "Alice transfers an Infocoin to Bob". The fragility of such a system is obvious: a third party other than Alice can very well generate such a file or falsify the message.

The solution to this problem is the use of a digital signature.Using digital signature, Alice hash the original text, crypt with the private part of an RSA key which she transfers the public part to Bob along with the original message. Bob, using the public key, will decrypt the message, which he will compare to the original message received. If the two messages coincide, then Bob can be certain that it is Alice who sent the message (as a rule, only Alice has the private part of the key) and that the latter was not falsified on road (see Fig. 1).

b). Step-2 Serialization and the Public Registry:

Now that Alice's identity is certified, how do you prevent her from misrepresenting the same message 10 times, spending Infocoins she does not have?

- First solution: we associate a serial number to each Infocoin to make it unique, a bit like a bank note. Nevertheless, in the case of the bank, there is a central authority that certifies the serial numbers and guarantees their uniqueness, exactly what we try to avoid!
- Second solution: keep a distributed public register of the property of the serialized Infocoins. Thus, Bob can check on his local copy of the register that the Infocoin No. X belongs to Alice. It then broadcasts an acceptance message that Alice sends this Infocoin, causing all other participants to update their local copy of the registry. The

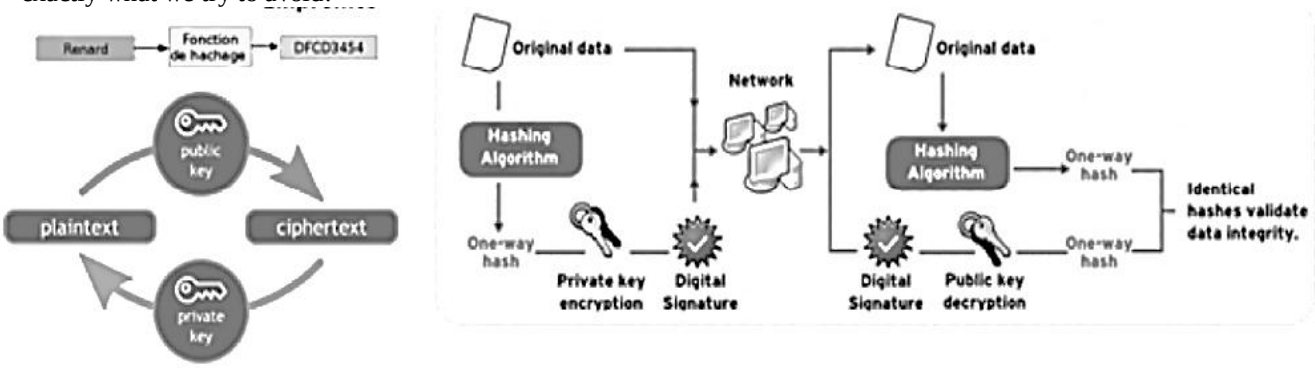

Figure 1: The concept of digital signature.

new state of the registry, shared by all, will therefore indicate that the unique Infocoin No. X of the network has been transferred from Alice to Bob.

Unfortunately, the verification of the uniqueness of the Infocoin spent by Bob via the public register is insufficient if a malicious user exploits the latency of the communication network between the different participants in the digital currency system to make double expenses. Indeed, Alice can broadcast her message twice with two different recipients for the Infocoin, Bob and Charlie. Bob, having received Alice's Infocoin No. X, will check on his local registry that he is the owner and will post a transaction validation message to the rest of the network. Charlie will do the same, his message of validation of the transaction being accepted would come first and refused would happen after that of bob. Suddenly two versions incompatible of public register will be present in the network : some of the nodes, which received the validation of Bob first will consider that it is he the owner of Infocoin No. X, the other party will consider that it's Charlie. The created system is therefore not yet a viable system.

Solving the problem of double spending is the most important challenge in building a digital currency and requires three additional steps that will lead us to the technical architecture of a blockchain.

c). Step-3 Collective Audit:

A first step in solving the double-spend problem is that Bob waits for a collective verification of the Infocoin's ownership before sending his transaction validation message, which results in an update of the records. Thus, sending two contradictory messages from Alice will result in contradictory feedback to Bob from the network, resulting in a cancellation of the transaction.

The question that arises with this system of validation by 100% of the nodes of the network is that of the presence of non-cooperative agents, which can voluntarily distort the validation of the transactions of their competitors. If the privilege of validation is granted to only a few nodes, the goal of a completely decentralized system is abandoned, whereas a vote-based system can easily be hacked by generating false identities for the nodes of the network.

d). Step-4 The proof of work:

Imagine forcing the nodes of the network to "work" and to give proof of their work before considering their return as valid. This work can take the form of the resolution of a mathematical problem; the nodes will have to provide the solution to a problem whose verification of the validity is simple, like the resolution of an equation ‘h (T + N) = 0000 ... 123’ , with ‘h’ a hash function, ‘T’ the message of the transaction, ‘N’ a random message called "nonce" in English, and ‘m’ 0 at the beginning of the member of the right of the equation which is encoded in a 16-bit format. The search for a brute-force solution would require testing ‘16 ^ m’ combinations to find the ‘N’ that is appropriate, while checking the ‘N’ solution found is very fast.

As soon as a node has found a valid ‘N’ solution, it distributes to the rest of the network, which checks, almost instantaneously, whether it is suitable or not by calculating the value ‘h (T + N)’, with update of the local copy of the register if the solution is accepted. Knowing that a calculation costs money (owning a computer, electricity consumption, etc.), agents can be encouraged to perform the calculations by paying

them for each validated transaction. With what money? This is the beauty of the Bitcoin system or its avatars: we generate bitcoin ex nihilo to just reward the work of validating a transaction.

Also, except for the initial mass of money created at the same time as the protocol, the only way to increase the money supply in Bitcoins or Infocoins is to perform transaction validation calculations. Network workers are referred to as "miners" [5], while their work is known as "mining".

For optimization reasons, we group transactions in blocks to be validated, each consisting of:

- A hash of the transaction list via a function that is part of the protocol.
- A block creation timestamp.
- The nonce found by the miner who validated the transaction block.
- The hash of the previous block, which constitutes a pointing convention establishing a temporal order between the blocks.

e). Step-5 Temporal Order of the Blocks

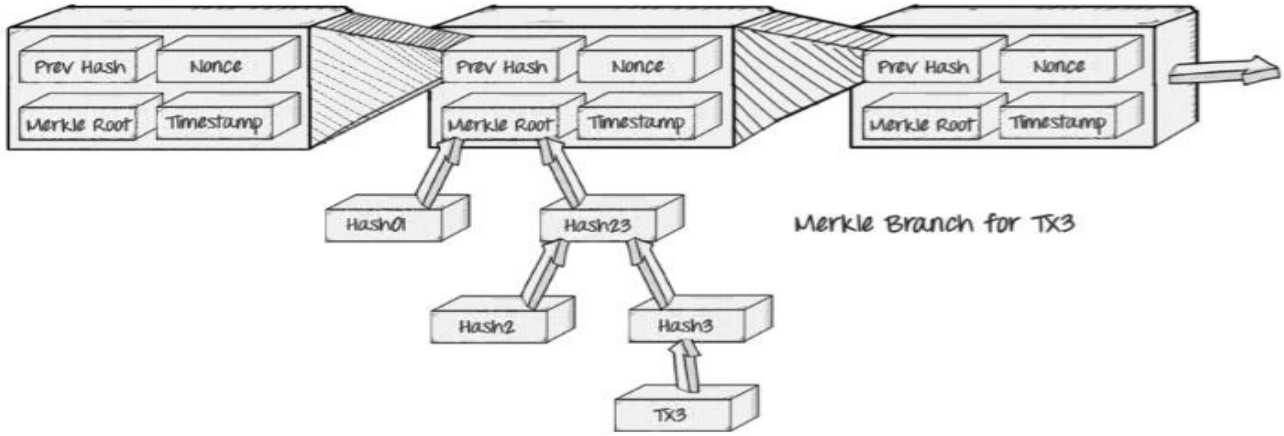

Figure 2: Temporal order of blocks by pointing [6]

Techniques for optimizing the hashing of transactions to be grouped in the block exist, but we will not go into these details in this article (see Fig. 2). The system composed of blocks and
points constitutes an ordered chain of transactions, hence the name "Blockchain".

f). Step-6 Management of Bifurcations

Several blocks being mined at the same time, a golden rule is introduced to regulate the work of the miners: "the valid branch is the longest branch". Miners working on two competing blocks must stop working on the losing block as soon as a block has been validated. After verifying the validity of the contents of the block, they update their local copy of the register, with pointing into the arrival of the new block.

What happens when two miners finish at the same time undermining a block of transactions? It creates what is called a bifurcation: the miners continue to undermine along the two branches, potentially with new sub-branches that appear when new blocks are completed simultaneously. However, as soon as a block is finished before the other along a branch that becomes the longest, all the miners check the contents of the block needto update their local register and switch to this new legitimate branch (see Fig. 3).

II. BLOCKCHAIN'S SECURITY CHALLENGES AND THREATS

So far, blockchain has been gotten many attentions in different areas, however, blockchain has problems and challenges which need to be addressed. Challenges by securing communications and transactions between connected objects, the blockchain aims to automate many trades that will be difficult to replace. In the FinTech sector, for example, the billions of savings expected by banks will come from the elimination of intermediaries responsible for auditing, clearing and so on. It will be the same in many other sectors such as notaries, lawyers, logistics, insurance, transportation, security, etc.

Apart from the technical challenges, blockchain is facing challenges in the transparency, confidentiality and security of exchange platforms.

Attackers present a major threat and have adopted several and many methods to target consumers and businesses using very well-established techniques. Following are some of the primary threats of blockchain which include: [11]

A. Phishing

There have been many phishing attempts in recent years. Many scams are intended to alarm you about an event that has occurred on the blockchain Ethereum to lead you on a fake website, a copy of a trusted site like MyEtherWallet [8]. The means to solicit you are many: sponsored links on Google, private messages in

public slacks dedicated to crypto, on reddit, in your emails, etc.

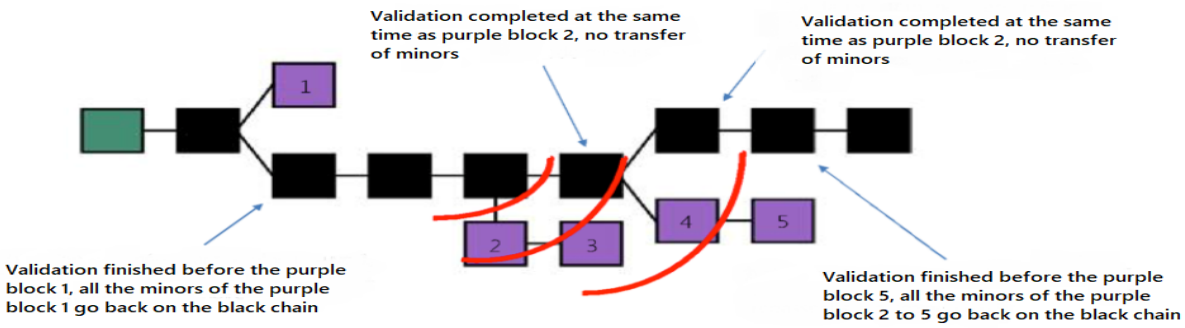

Figure 3: Management of bifurcations in a Blockchain [7]

B. Malware (examples: ransomware, miners, and cryptojacking)

A new appearance of a cyber-attack that is on the way to develop more and more: it consists in taking control of a maximum of machines (Concept of Miners) [9] in order to use them to undermine cryptocurrencies. This sophisticated attack is a discrete but rewarding method, far from massive classical attacks such as Ddos at WannaCry.

C. Implementation Vulnerabilities

Another type of threat that is the implementation of vulnerabilites turn it into an attack against the implementation of the blockchain itself, as well as its support tools. In general, all of these threats are much more like exploits of traditional software and Web applications. Generally, the closer you get to the heart of blockchain technology, the harder it is to make an attack. The Bitcoin wiki keeps [10] a list of vulnerabilities and exposures related to their official tools. These vulnerabilities include Denial of Service attacks, theft of coins, and data exposures. It is always difficult to create or maintain a secure code. Obviously the vulnerabilities can have a significant impact but they are discovered and corrected after the publication. The popularity and explosive growth of the blockchain exacerbated this problem. The discovery of serious vulnerabilities related to the main Bitcoin tools has slowed down, which is beginning to offer consumers a sense of trust.

D. Technology Attacks

In return, before the publication of the first implementation of the blockchain, there was no reliable alternative for the decentralized bank. The security issues that are related to the construction of such a system have been discussed well before that date. Years and years of research, including the block chain of Haber and Stornetta, have established confidence in the blockchain concept. However, the security of a blockchain depends on certain assumptions. If these assumptions are not satisfied, security is exposed to a threat.

III. HOW TO SECURE BLOCKCHAIN (SOLUTIONS OFFERED)

A. Verification of the Robustness of the Protocol

Let's now analyze the robustness of this protocol.

Imagine a first type of attack where Alice inserts two incompatible transactions into the same block, one sending an Infocoin to Bob, the other sending the same Infocoin to Charlie. Alice can then undermine the block, with a speed proportional to the computing abilities she possesses. It can then broadcast the validation message to the rest of the network. Nevertheless, this type of basic attack is doomed to failure because the reading of the block by the other actors of the network will clearly show that it contains two incompatible transactions, thus leading to its invalidation.

Second type of attack, Alice spreads two separate messages about mutually incompatible transactions to Bob and Charlie. A bifurcation of mining is created in the network, but in the long run, only one of the two branches that is considered as the longest will be validated ,generally that having benefited from the most important computing resources. Thus, Bob or Charlie will know that his transaction has not been validated, and the exchange will not take place. Beware of an early sending of the counterparty: the validation of the blocks and the bifurcations being a local information, it is not necessary to consider a newly validated transaction as reliable, at the risk of being deceived if the branch having validated the transaction turns out not -Legitimate later because shorter than another. Hence a recommendation to wait for 6 blocks validated after the one containing the transaction launched before sending the counterpart with confidence. Indeed, one can mathematically prove that the probability that several blocks following the bifurcation is validated simultaneously decreases exponentially with the number of blocks, as long as no node has more than 50% of the computation capacity of the network. For example, a block requires an average of 10 minutes to be validated on the Bitcoin blockchain, so you usually

have to wait one hour after the payment before sending the counterparty.

How does the condition of the absence of a node with more than 50% of the computing capacity of the network occur? This leads us to consider one last attack, the most sneaky. Alice makes two transactions on the same Infocoin, one to Bob, and the other to herself. She waits for the network to confirm the transaction with Bob and starts mining a branch that has started just before the newly validated block. The legitimization of his branch would cancel the transaction with Bob in the local registers, and if the latter has already sent the counterparty to the monetary transaction, it will be scammed. How can Alice legitimize the branch she creates? According to the golden rule, this branch must become the longest. Alice must therefore undermine only her branch (all the honest miners have switched to the branch containing the block of the transaction with Bob) and make at some point the longest branch. By definition, it must therefore have strictly more than 50% of the computing capacity of the network (see Fig. 4).

B. Quantum Key Distribution (Qkd) For Blockchain

The Blockchain is by default considered secure. However, it remains vulnerable to attacks from quantum computers. Russian researchers have developed a solution to the security problem of the large distributed registry.

However, according to a team of Russian researchers who presented the results of their research in the journal Quantum Science and Technology [13], improvements must be implemented in the security of the large distributed registry. Current Blockchain platforms rely on digital signatures which are vulnerable to security attacks from quantum computers. Those with access to quantum computing may unfairly get mining rewards snd hence the risks using digital signatures must be addressed.

The reserachers have identified and developed a new fault-tolerant service blockchain by replicating data and coordinating client interactions with replica servers without using digital signatures.

And so, solving the Blockchain's security problem lies in the Quantum Key Distribution (QKD). The latter offers secure authentication.

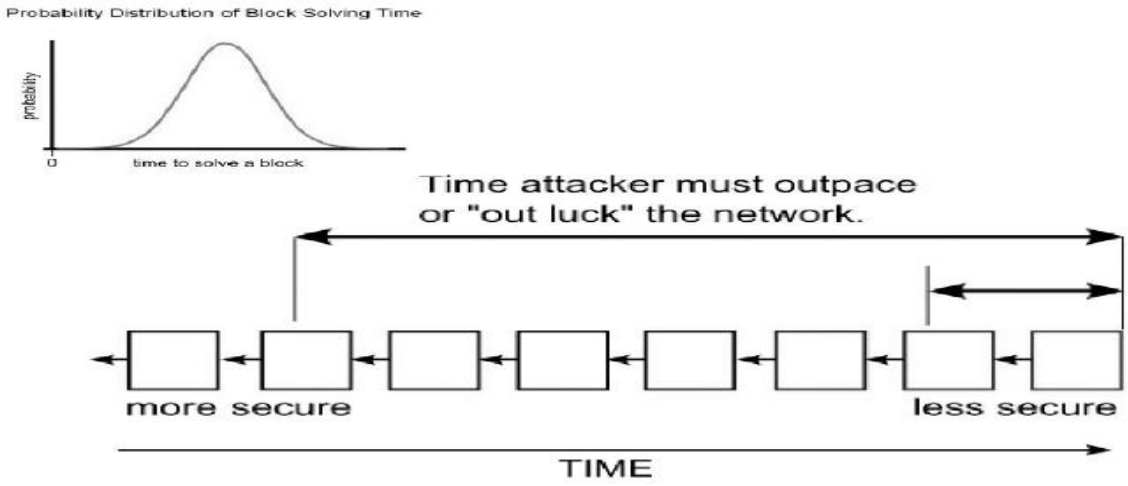

Figure 4: Mathematical race to protect transactions [12]

C. Hardware Security Modules (HSMs)

Hardware Security modules (HSMs) [14] are considered as a secury way to generate and protect store keys.HSM encompasses entire cryptographic life cycle. Starting from provisining of keys to disposing and archiving of keys.HSM provides a safe environment by protecting blockchain ledgers, digital wallets and safegroud from the hacking attacks.It becomes almost impossible for the hackers to attack such Blockchain as it can be invaded only if the hackers get access to the administrative privilegs or if they manages to get the physical access to the HSMs. Most of the security concious institutions have started using HSMs to address the secuiry risks in blockchain.

IV. CONCLUSION

Here we are! We built a digital currency step by step, showing how each addition of technical works and reveal specific type of threat. In conclusion, the blockchain protocol is interesting in that it constitutes a natural solution (each brick is necessary) and elegant (from an algorithmic point of view) to the problem of value exchange without a trust intermediary. Nevertheless, before we reach a generalization and a stabilization of this technology, we risk going through dark periods and the challenges that we will face in the near future are beyond measure.

REFERENCES

[1] Research on the Security of Blockchain Data: A Survey - LiehuangZhua, BaokunZhenga,b, Meng Shena,_, Feng Gaoa, Hongyu Lia, Kexin Shia

[2] Research Bitcoin and the Future of Digital Payments - Luther, William J., (July 15, 2015). Available at SSRN

[3] Research Ethereum: state of knowledge and research perspectives - Sergei TikhomirovSnT, University of Luxembourg

[4] https://www.hyperledger.org/

[5] Research Majority is not Enough: Bitcoin Mining is Vulnerable - IttayEyal and Emin Gun Sirer Department of Computer Science, Cornell University

[6] Research BlockChain Technology (Sutardja Center for Entrepreneurship & Technology Technical Report Authors Michael Crosby, Google - Nachiappan, Yahoo - Pradhan Pattanayak, Yahoo - Sanjeev Verma, Samsung Research America - Vignesh Kalyanaraman, Fairchild Semiconductor)

[7] Research BlockChain Technology (Sutardja Center for Entrepreneurship & Technology Technical Report Authors Michael Crosby, Google - Nachiappan, Yahoo - Pradhan Pattanayak, Yahoo - Sanjeev Verma, Samsung Research America - Vignesh Kalyanaraman, Fairchild Semiconductor)

[8] https://www.myetherwallet.com/

[9] https://dev.to/damcosset/blockchain-what-is-mining-2eod

[10] https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures

[11] Research Blockchain Threat Report – McAfee Blockchain, a Revolutionary Basis for Decentralized Online Transactions, Carries Security Risks

[12] Research BlockChain Technology (Sutardja Center for Entrepreneurship & Technology Technical Report Authors Michael Crosby, Google - Nachiappan, Yahoo - Pradhan Pattanayak, Yahoo - Sanjeev Verma, Samsung Research America - Vignesh Kalyanaraman, Fairchild Semiconductor)

[13] Research Y V Kurochkin, A I Lvovsky and A K Fedorov - Published 31 May 2018 • © 2018 IOP Publishing Ltd Quantum Science and Technology, Volume 3, Number 3

[14] Boireau, Olivier. (2018). Securing the blockchain against hackers. Network Security. 2018. 8-11. 10.1016/S1353-4858(18)30006-0.

[15] Simanta Shekhar Sarmah, Understanding Blockchain Technology, Computer Science and Engineering, Vol. 8 No. 2, 2018, pp. 23-29. doi: 10.5923/j.computer.20180802.02.

[16] Sandeep Kumar, Abhay Kumar, Vanita Verma (2019). A Survey Paper on Blockchain Technology, Challenges and Opportunities. *International Journal of Engineering Trends and Technology*, 67(4), 16-20.

.