Blockchain and Cyberattacks: Is Blockchain a safe and hacker-proof technology?

di Pierguido Iezzi
Cybersecurity Strategy Director – Co Founder di Swascan

A graduate in Information Sciences and with a lifelong passion for CyberSecurity and Digital Innovation, I have been able to work both at a national and international level in large business environments, with a particular focus on major technological trends.
A founder of a number of start-up companies, among which Swascan, the first platform of CyberSecurity services wholly cloud-based, I am able to combine my strong technological background with the experiences I gained in the Security sector.
I am strongly innovation-oriented, and the phrase that best describes me is: “Each of us is the answers to the questions we ask ourselves”.

Blockchain and Cyberattacks

Many consider Blockchain the evolution of Internet. A solution that comprises 5 fundamental principles:

– Trasparency
– Decentralization
– Democracy
– Trust
– Security

Let us focus on the last point: ***Security***.
Is Blockchain a safe and hacker-proof technology? Many people, indeed too many, confirm the impossibility to hacker the system. History taught us that nothing is safe, it is just a matter of **time and money**.

The Equifax cases of 2017, together with the worldwide diffusion of Wannacry, raised the problem of Cybercrime and the word Cybersecurity has become customary by now.
The need for security thus leads us, too often, to overestimate the capabilities and characteristics of the new technologies.
Blockchain is one of these new technologies overestimated in terms of security. Blockchain technologies are not hacker-proof and can suffer from cyberattacks.
We will not talk about the attacks on the encrypting system because, for the time being, it is a renowned security "critical point", but also one that is not feasible for a mere economic reason. The computational power that is necessary is huge and the investment is just as enormous.
We will analyse, instead, techniques and methods that a Criminal Hacker can use to exploit Blockchain's weakness points.

Blockchain: 51% ATTACK
The Blockchain technology provides for blocks and transitions to be validated by the majority of the participants of the Blockchain.
Attack 51 per cent exploits precisely this principle.
For instance, the "security" of a Blockchain is in fact guaranteed by the total computational power of the devices

making up the Blockchain itself. Transactions and blocks are in fact validated only if more than 50% of the computational power of the network “certifies” the transaction and the block.
That is where the name 51% attack comes from.
Therefore, in fact, a third ill-intentioned person, if he/she managed the majority (+50%) of the computational power of a Blockchain network may in fact validate false transactions or also fail to validate real transactions.
It is a kind of attack whose cost is a result of the overall computational power of the Blockchain network.
How can we have 51% of the computational power?
– Investing on computational power
– Building a Botnet

Blockchain: 51% Attack: investment on computational power
In practice, we may make an investment on machines having a computational power.
If we take the example of the Blockchains of cryptocurrencies, for a 51% attack against the two big players Bitcoin and Ethereum an investment of 400.000/500.000 dollars an hour is necessary.
Obviously, the cost decreases drastically if we target the Blockchain of smaller cryptocurrencies. In this case, to launch a 51% attack against Bytecoin and Bitcoin Private 700 dollars an hour is enough.

Fonte: Crypto51.app

Blockchain: 51% Attack: Botnet
We can obtain the necessary computational power also at almost

zero cost through the construction of a Botnet. The Botnets are in fact a network of infected devices. For example, a Criminal hacker takes over the complete management and possession of a series of devices of unaware users.
If the Botnet exceeds 50% of the blockchain's computational power, the 51% attack is guaranteed.

Blockchain: 51% Attack: Real cases

The 51% attacks against Blockchain networks of cryptocurrencies are quite widespread.
The following are some case histories:
– **Verge** (damages evaluated at about 1,7 $ million);
– **Coinrail** (over 35 million dollars loss);
– **Bitcoingold** (about $17.5 million loss);
– **Zencash** ($550.000 loss).

Blockchain Attack on the Routing

An attack on the routing is a direct attack on the centralized node of the network. It is necessary to make a preliminary statement. The design of the Blockchain provides for the nodes to be distributed, but the truth is that they are often centralized on specific Internet Service Providers that guarantee and carry the network traffic from and to.
Always taking as an example the cryptocurrencies of the Blockchain networks, a research undertaken by ETHZurich assessed that 13 ISP accommodated about 30% of the Bitcoin network, while only 3 Internet Service Providers directed 60% of all the traffic of the transactions throughout the network. This "concentration" obviously represents a critical element and a weakness point.

Blockchain: Distributed Denial of Service

A DDoS attack (Distributed Denial of Service) occurs when a server is overloaded with connections.
Basically, the aim is to saturate the target device so that it

can no longer manage any transaction, making it inaccessible for hours or days.
Obviously also the Blockchain network devices can be victims of this type of attack. The only operational risk is related to the shutdown of the activity.
As in the case of the 51% attack, the Distributed Denial of Service reaches the target as a result of the computational power of the blockchain network.

Always taking as an example the Bitcoin's Blockchain network, in 2015 it was the object of a DDOS attack. Through a spam operation, about 80.000 very small transactions were sent at the same time thus blocking the transactions.

Blockchain: an opportunity for the future?
The Blockchain networks represent undoubtedly one of the most interesting technologies in terms of opportunities and possibilities of verticalization of the processes.
The model of the Blockchain itself is surely inspiring and exciting. The principles it is based on in fact bring us back to the time of the French revolution.
The same story also taught us that nothing is safe and, in our case, nothing is hacker-proof.
Eric Fromm used to say that "The task we must work on is not to reach security, but go so far as to tolerate the lack of security", I believe instead that our task is to manage the lack of security correctly being fully aware of the risk.

23 July 2018