Articolo pubblicato a marzo 2022 per la partecipazione al simposio annuale (“***The Cambridge International Symposium on Economic Crime”),*** presso il Jesus College di Cambridge, nella rivista dei papers dei docenti.

BLOCKCHAIN AND CYBER SECURITY

WHAT IS A BLOCKCHAIN?

Blockchain is a term widely used to represent an entire new suite of technologies. There is substantial confusion around its definition because the technology is early-stage, and it can be implemented in many ways.

“At a high level, blockchain technology allows a network of computers to agree at regular intervals on the true state of a distributed ledger,” says professor Christian Catalini, an expert in blockchain technologies and cryptocurrency. “Such ledgers can contain different types of shared data, such as transaction records, attributes of transactions, credentials, or other pieces of information. The ledger is often secured through a clever mix of cryptography and game theory, and does not require trusted nodes like traditional networks. This is what allows bitcoin for ex to transfer value across the globe without resorting to traditional intermediaries such as banks.”

On a blockchain, transactions are recorded chronologically, forming an immutable chain, and can be more or less private or anonymous depending on how the technology is implemented. The ledger is distributed across many participants in the network — it doesn’t exist in one place. A block could represent transactions and data of many types — currency, digital rights, intellectual property, identity, or property titles, to name a few.

There are two types of costs blockchain could reduce for us: the cost of verification and the cost of networking.

Every business and organization engages in many types of transactions every day. Each of those transactions requires verification. In many cases, that verification is easy. Companies know their customers, clients, and colleagues, and their business partners.

“But when, there’s a problem, and when a problem arises, they often have to perform some sort of audit”.

“The reason distributed ledgers become so useful in these cases is because if we recorded those attributes we don’t need to verify securely on a blockchain. It’s costless verification.

In short: Because the blockchain verifies trustworthiness, we don’t have to. And the friction of the transaction is reduced, resulting in cost and time savings. Using a blockchain can also reduce the cost of running a secure network. The internet has already allowed for a faster, exchange of goods and services. But it still needs intermediaries, however efficient they may be — think eBay, Airbnb, and Uber. Those intermediaries are costly and earn rents for processing payments, maintaining a reputation system, matching demand and supply.

Blockchain technology could mean greater privacy and security also for companies and theirs customers.

Information disclosure is increasingly becoming a cost because of data breaches. We have the opportunity to imagine a new model where it is possible verify if certain attributes are true or false, potentially using a decentralized infrastructure.

THE NEW MODEL

Blockchain makes it nearly impossible for a hacker to corrupt or mutate the data and documentation related to the platform. Anonymity provides a layer of protection for users to conduct business. Nearly every transaction can be automated via smart contracts and sellers are voted into the platform via token holders.

Blockchain can improve data mapping, strengthen authentication, and protect edge computing with authentication.

It is easy to indicate a few ways blockchain can contribute to cybersecurity: Blockchain technology can be used to prevent data theft, fraud, identity theft, and other forms of cybercrime.

-Bitcoin transactions are recorded in a digital ledger called a blockchain. Blockchain technology and users' constant review of the system have made it difficult to hack bitcoins.

Blockchain, as a Distributed Ledger Technology (DLT), is focused on creating trust in an untrusting ecosystem, making it a potentially strong cybersecurity technology. All members (or nodes) can record, pass along and view any transactional data that is encrypted onto their blockchain.

A successful cyber-attack can be the downfall of any well-positioned business.

Data breaches not only cause significant financial losses but are also the leading cause of a bad reputation for victim companies.

Blockchain started out as the technology behind Bitcoin but its popularly grown into a promising mitigation technology for cybersecurity.

It is quite a tough and challenging time for businesses that operate on digital network platforms. Cyber-attacks and breaches continue to haunt online activities at even more sophisticated and damaging levels. As this nightmare continues to escalate, it is not only for small businesses but also large IT companies like Siemens, Facebook, Yahoo, Microsoft, and LG, just to mention a few, are in a serious dangerous position.

Ransomware attacks and other forms of data breaches have now become a day to day challenge for companies. Recent analysis and statistics indicate that even state procedures like Presidential elections are not safe from these attacks. This shows that cybersecurity is no longer an issue to companies alone, but also to governments and other agencies.

For the development of viable cybersecurity protection strategies, it would be prudent to analyse the recent cyber-attack trends and statistics and learn from it.

The damages caused by cyber-attacks in 2019 amounted to $2 trillion. With such tremendous financial impacts, companies continue to increase their investment in cybersecurity.

"Ransomware Attack Every 14 Seconds": This is according to the 2019 Official Annual Cybercrime Report (ACR) that also indicated that most of these attacks go unreported. With a new person joining social media platforms every 15 seconds, the ransomware vulnerability scope continues to widen.

"Small Businesses are the primary targets of Cyber-attacks": Small businesses continue being the smallest investors in cybersecurity despite making up 13% of the cybercrime market.

"Cyber threat Costs": The average cost of a cyber-attack data breach as of 2019 was $3.92 million.

The current fast-paced advancement in technology also offers an incubating effect to cyber-attacks to continue becoming more sophisticated and executable. Faster speeds will increase the chances of more devices being hacked and the execution of larger cyber-attacks.

There is a huge criminal appetite for the Internet of Things (IoT). Home automation features could lead to more homes being vulnerable to cyber-attacks by criminals.

We can say that Blockchain technology is a distributed and decentralised ledger system that can record transactions between multiple computers.

Notably, human error remains to be the leading cause of data breaches. Blockchain fully automates data storage hence reducing the human element in these data storage systems.

Blockchain can be utilised in any sector or industry. This is because any kind of digital asset or transaction can be inserted in blockchain, from any industry.

The new technology is considered a reliable cybersecurity protocol due to its capabilities of indicating any foul play and providing certainty in the integrity of transactions.

Blockchain technology was designed to be transparent. Therefore, blockchain offers no privacy or confidentiality of any transactions made through it. “Secure”, meant to describe the integrity of the transactions, not its privacy.

Actually, while no system is "unhackable," blockchain's simple topology is the most secure today. A 51 percent attack refers to a bad actor. Such attacks are generally limited to smaller blockchains with fewer nodes because they're more susceptible to a single person seizing control.

Although not unbreakable, blockchain has evolved to become one of the most foolproof forms of transacting in the digital network realm. As designed and intended, the technology has been credited for its information integrity assurance. If well-utilised, many sectors can benefit from it. With the potential of being practical to many utilisations, blockchain can be implemented into many uses. One of the best uses would be utilising its integrity assurance for building cybersecurity solutions for many other technologies.

We can describe some cases of future beneficial use of blockchain to strengthen cybersecurity:

1. **Securing Private Messaging**: With the internet the world has been designed as a global village, more and more people are joining social media. Huge amounts of metadata are collected during these interactions. Most social media platform users protect the services and their data with weak, unreliable passwords.

Most messaging companies are warming up to blockchain for securing user data as a superior option to the end-to-end encryption which they currently use. Blockchain can be used to create a standard security protocol.

In the recent past, numerous attacks have been executed against social platforms like Twitter and Facebook. These attacks resulted in data breaches with millions of accounts being breached and user information landing into the wrong hands. Blockchain technologies, if well implemented in these messaging systems, may prevent such future cyberattacks.

2. **IoT Security**: Hackers have increasingly used edge devices, to gain access to overall systems. With the obsession for Artificial Intelligence (AI), it has become easier for hackers to access overall systems like home automation.

In this case, blockchain can be used to secure such overall systems or devices by decentralising their administration.

Normally, hackers penetrate the central administration of a device and automatically gain full control of the devices and systems. By decentralising such device authority systems, blockchain ensures such attacks are harder to execute.

3. Securing DDoS: A **Distributed Denial of Service** (DDoS) attack occurs when users of a target resource, such as a network resource, server, or website, are denied access or service to the target resource. These attacks shut down or slow down the resource systems.
On the other hand, an intact Domain Name System (DNS) is very centralised, making it a perfect target for hackers who infiltrate the connection between the IP address and the name of a website. This attack renders a website inaccessible.
Blockchain can be used to diminish such kinds of attacks by decentralising the DNS entries. By applying decentralised solutions, blockchain would have removed the vulnerable single points exploited by hackers.

4. **The Provenance of Computer Software**: Blockchain can be used to ensure the integrity of software downloads to prevent foreign intrusion. Blockchain can be applied to verify activities, to prevent the entry of malicious software in computers.
In the case of blockchain technology, the hashes are permanently recorded in the blockchain. The information recorded is not mutable or changeable; hence blockchain may be more efficient in verifying the integrity of software by comparing it to the hashes against the ones on the blockchain.

5. **Protecting Data Transmission**: Blockchain can be used to prevent unauthorized access to data while in transit. By utilising the complete encryption feature of the technology, data transmission can be secured to prevent malicious actors from accessing. This approach would lead to a general increase in integrity of data transmitted through blockchain.

Conclusion

The key component of blockchain technology is its ability to decentralise.
This feature removes the single target point that can be compromised. As a result, it becomes impossible to infiltrate systems or sites whose access control, data storage, and network traffic are no longer in a single location.

Therefore, blockchain may be one of the most efficient mitigation strategies for cyber threats in the coming days.

Palermo, 28.3.2022

Bibliography

1. A. WRIGHT, P. DE FILIPPI, Decentralized Blockchain Technology and the Rise of Lex Cryptographia, 12 marzo 2015, 2-3, reperibile su SSRN: https://ssrn.com/abstract=2580664.

2. K. LAW, E. MIK, Pause the blockchain legal revolution, in British Institute of International and Comparative Law, 69, 2020.

3. R. MAULL, P. GODSIFF, C. MULLIGAN, A. BROWN, B. KEWELL, Distributed ledger tecnology: Applications and implications, in Strategic Changes, 26, 2017.

4. Y. BENKLER, The Wealth of Networks: How Social Production Transforms Markets and Freedom, New Haven, Yale University Press, 2006.

5. A. WALCH, The Path of the Blockchain Lexicon (and the law), in Review of Banking and Financial Law, 36, 2016.

6. S. SAYEED, H.M. GHISBERT, Assessing blockchain consensus and security mechanism against the 51% attack, in Applied Sciences, 9, 2019, p. 1778, reperibile su https:// www.mdpi.com/2076-3417/9/9/1788.

7. L. LESSIG, Code and Other Law of Cyberspace, New York, 1999.