Chapter 2

Blockchain and Cybersecurity: Building Digital Trust*

DOI: https://doi.org/10.25062/9786287818064.02

Jaider Ospina Navas
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Abstract: This chapter explores the cutting-edge developments in blockchain technology to identify its role in creating a secure digital ecosystem. To achieve this, it outlines the key characteristics of blockchain, including decentralization, immutability, and consensus; discusses its benefits regarding security, transparency, and resistance to tampering; examines the various types of attacks on immutability that are recognized to date; describes the different applications of blockchain; and presents the current challenges and limitations, offering a comprehensive view of the possibilities and obstacles in this evolving field.

Keywords: blockchain; digital trust; decentralization; digital ecosystem; immutability; transparency

* Book chapter resulting from the research project *Disruptive Technologies, Logistics, and National Security and Defense in Cyberspace* conducted by the Cyberspace, Technology, and Innovation research group of Escuela Superior de Guerra "General Rafael Reyes Prieto," categorized C by the Ministry of Science, Technology and Innovation (MinCiencias) and registered under code COL0181179. The points of view and results of this chapter belong to the authors and do not necessarily reflect those of the participating institutions

Jaider Ospina Navas
PhD student in Information Systems. Master's in Information and Communications Sciences and Bachelor of Electronic Engineering, Universidad Distrital Francisco José de Caldas, Colombia. Cybersecurity consultant and cloud solutions architect.
https://orcid.org/0000-3251-3017 - Contacto: **jaider.ospina@esdeg.edu.co**

APA Citation: Ospina Navas, J. (2025). Blockchain and Cybersecurity: Building Digital Trust. In M. E. Realpe Díaz & A. M. González González (Eds.), *Disruptive Technologies, Logistics, and National Security and Defense in Cyberspace* (pp. 43-68). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818064.02

DISRUPTIVE TECHNOLOGIES, LOGISTICS, AND NATIONAL SECURITY AND DEFENSE IN CYBERSPACE
Print ISBN: 978-628-7818-05-7
Digital ISBN: 978-628-7818-06-4
DOI: https://doi.org/10.25062/9786287818064

Cybersecurity and Cyber Defense Collection
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

Introduction

This chapter explores the state of the art of blockchain technology to identify its role in building a secure digital ecosystem. The general objective is to specify the characteristics that allow for creating a reliable digital ecosystem through enabling agents that guarantee data privacy, confidentiality, and availability, as well as to provide a view of the main limitations of its adoption. For this, we review articles that evaluate aspects of cybersecurity, documentation of applications or initiatives to improve digital trust, and studies in which a systematic literature review is carried out.

Birth of Blockchains

Although the origin of the blockchain (BC) is associated with the publication of the whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System," it should actually be attributed to the work of Stuart Haber and W. Scott Stornetta. In their article "How to Time-Stamp a Digital Document," published in the *Journal of Cryptology* in 1991, they introduced a digital time-stamp system to certify the date of creation or modification of an electronic document, without depending on the physical medium, using cryptographic hashes to generate unique summaries of documents and store them in a blockchain (Haber & Scott, 1991).

Subsequently, on November 1, 2008, Satoshi Nakamoto, a pseudonym used by the person or group that created the concept and underlying technology of Bitcoin, sent a message to the cryptography mailing list metzdowd, announcing a new electronic money system based on peer-to-peer (P2P) networks. This document laid the theoretical and technical foundations of blockchain technology

and concisely explained the technical aspects proposed by a new digital currency, as well as the main objective of its creation: to dispense with trusted third parties.

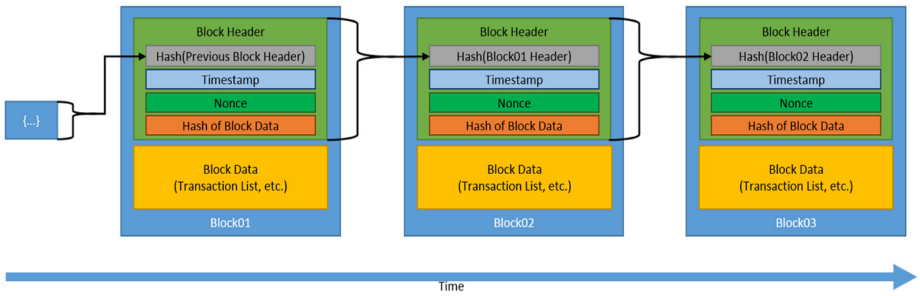
"What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party" (Nakamoto, 2008, p. 1).

Thus, the most recognized digital currency, Bitcoin, was born, and a solution is proposed for one of the biggest problems of this type of currency: double-spending. By using a decentralized blockchain and a distributed consensus to validate and record transactions securely and transparently, different systems and applications inherit characteristics to protect data and create a reliable digital ecosystem.

Fundamentals of Blockchain Technology

Blockchain is a distributed and secure database that has revolutionized data storage and verification (Xu et al., 2019). Each block in the chain contains a cryptographic hash of the previous block intertwined by a hash guaranteeing a "digital signature" 1 for its integrity and eventual manipulation, a timestamp, and data of the transaction made (Figure 1).

Figure 1. *Generic Blockchain*



Source: NISTIR 8202 (2018).

Generally, BC can be conceived as a decentralized and secure data logging technology, which has emerged as a fundamental component in the digital era. According to Nakamoto (2008), blockchain is defined as a "public transaction ledger" that stores information immutably and transparently. The strength of BC lies in its decentralized nature, where multiple network nodes verify and validate

transactions, eliminating the need for a central trusted intermediary (Swan, 2015). This guarantees the security and integrity of the stored data since any attempted alteration would require the consensus of the majority of participants, making it highly resistant to tampering and cyberattacks (Krichen et al., 2022; Mougayar, 2016; Yli-Huumo et al., 2016). As already mentioned, BC's unique structure makes it resistant to tampering, as any change to one block would require changes to all subsequent blocks to maintain chain coherence (Popchev et al., 2021).

Speaking specifically of the Bitcoin protocol described initially by Nakamoto, it is based on the TCP/IP protocol stack from which a network of nodes is built overlaid on the internet. The nodes make up a P2P network where all nodes provide and consume services simultaneously while collaborating via consensus services Vamsi_Cz5cgo and Vamsi_Cz5cgo (2020).

Blockchain and Distributed Ledger Technology

Distributed Ledger Technology (DLT)

Strictly speaking, BC is a specific type of DLT, and, in turn, DLT is a particular case of distributed database characterized by its consensual validation process (Romero, 2018). DLT is characterized by three articulated technological elements to make up its architecture: P2P networks, asymmetric cryptography, and consensus algorithms. A significant difference between DLT and BC lies in their structure and operation. While DLT can have different degrees of decentralization and can be public or private, BC is entirely decentralized and generally public (Hurtado, 2021). Examples of DLT platforms are Hyperledger Fabric, Corda, and Quorum, which are some of the most representative ones. These technologies can be public or private and customized to adapt to the specific needs of an application or industry.

Types of Blockchains

There are several types of BC, each with its characteristics and capabilities that adapt to different needs.

Public Blockchains

Networks that anyone can join to verify transactions and participate in block validation. Users are generally anonymous, and no participant has more rights than

the others, so there are no network administrators. They are considered drivers of distributed ledger technologies (DLT) and P2P networks for data distribution (Haleem et al., 2021). The most well-known public networks are Bitcoin, Bitcoin Cash, Ethereum, and Litecoin.

Private Blockchains

Networks where access is restricted to a specific group of entities. They are commonly used by companies that want to take advantage of BC technology but maintain control over who can participate in the network and all management tasks, such as creating and accepting blocks.

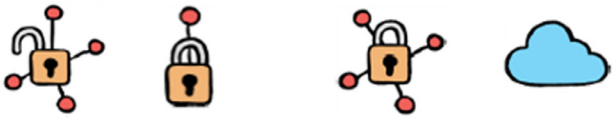
Federated or Consortium Blockchains

A hybrid implementation of the previous types. Control does not rest with a single entity but with a group, allowing a certain level of privacy to be maintained while taking advantage of the security and transparency of BC technology.

Blockchain as a Service (BaaS)

Products enabling users to build their networks and concentrate on developing applications without concern for the underlying infrastructure and the technical aspects. Figure 2 shows some particularities of the different types of BCs.

Figure 2. *Types of Blockchain Networks*



	Públicos Bitcoin, Ethereum, Litecoin	**Privados** Hyperledger, Corda, Quorum	**Federados** Hyperledger, Corda, Quorum	***Blockchain as a Service*** IBM, Microsoft, Amazon
Cualquiera puede participar	✓	✗	✗	NA
Los participantes actúan, en general, como nodos	✓	✗	✗	NA
Transparencia	✓	~	~	NA
Hay un único administrador	✗	✓	✗	NA
Hay más de un administrador	✗	✗	✓	NA

No hay administradores	✓	✗	✗	NA
Ningún participante tiene más derechos que los demás	✓	✗	✗	NA
Se pueden implementar Smart *Contracts*	✓	✓	✓	NA
Existe recompensa por minado de bloques	≈	✗	✗	NA
Soluciona problema de falta de confianza	✓	✗	≈	NA
Seguridad basada en protocolos de consenso	✓	✗	≈	NA
Seguridad basada en funciones *hash*	✓	≈	≈	NA
Provee servicios en la nube	NA	NA	NA	✓

✓ Sí ✗ No ≈ A veces **NA** No Aplica

Source: López (2018).

Blockchain Generations

In the article "Evolution of Industry and Blockchain Era: Monitoring Price Hike and Corruption Using BIoT for Smart Government and Industry 4.0," Hasan et al. (2022) identify five generations of BC since its appearance: 1st generation: It focuses on the creation of bitcoin by Satoshi Nakamoto in 2008, a decentralized digital currency that allows P2P transactions without an intermediary; 2nd generation: It introduces the idea of Smart Contracts, programs that run automatically when certain conditions are met. Ethereum is the best-known example; 3rd generation: It revolves around solving scalability and interoperability issues faced by previous generations. Projects like Cardano and Polkadot are working on solutions to allow different BCs to interact and handle a higher number of transactions, going from six transactions per second (TPS) to 100,000 TPS. This generation introduced decentralized applications (dApps); 4th generation: It deals with integrating existing business and government systems, providing solutions for interoperability, privacy, and security issues (Banafa, 2022). A level of 300,000 TPS has already been reached, and the range of applications increases in fields such as the supply chain, electronic voting, and Smart Grid; and 5th generation: It is the current one and is in the process of gestation, which according to experts, emerges with projects such as Relictum

Pro (Bitcoin.es, 2020). It is characterized by the use of intelligent machines and data analytics to automate smart application processes (Choi & Siqin, 2022).

Distinctive Features of Blockchain Technology

Some characteristics of BC that have become potentiating elements of cybersecurity strategies are decentralization, immutability, transparency, and consensus. These pillars have transformed reliability and security in online operations, and understanding them is essential to appreciate the potential of this technology.

Decentralization

According to Tapscott and Tapscott (2016), decentralization means no central authority controls the network. Instead of relying on a centralized entity like a bank or government, transactions are verified and recorded on a distributed network of collaborative nodes. Eliminating intermediaries builds trust and reduces single points of failure, making the network highly resistant to censorship and eventual attacks that compromise data. Decentralization has several advantages:

- Provides a trustless environment: In a decentralized BC network, no one has to know or trust anyone else. Each member holds an exact copy of the same data in a distributed ledger.
- Improves data reconciliation: All nodes can access a shared, real-time data view.
- Reduces points of weakness: Decentralization can reduce points of weakness in systems that depend on specific actors. A point of weakness may be due to a dependency on specific resources such as storage or computing capacity.
- Optimizes resource distribution: Optimized resource distribution enhances network performance and consistency through strategies such as improving content delivery times.

Immutability

According to Mougayar (2016), immutability is a principle that refers to the inability to change or delete once a transaction has been recorded on the blockchain. Each block of data in the chain is cryptographically linked to the previous one, making it extremely difficult, if possible, to modify the contents of one block without altering

all of the following. This ensures that recorded transactions are permanent and reliable, essential in applications where data integrity is crucial, such as healthcare and identity management.

Transparency

In a BC network, all transactions are visible to all network participants, providing high transparency. However, this transparency can pose challenges, especially when sensitive data is involved.

According to Sedlmeir et al. (2022), transparency presents challenges to companies and the public sector related to an excessive degree of it. They point out how the types of sensitive data involved in different blockchain use case patterns and argue that the implications of BC information exposure caused by the storage and execution of replicated transactions go beyond the conflict often mentioned with the "right to be forgotten" of the GDPR and may be more problematic than anticipated. The authors describe the balance between protecting sensitive information and increasing process efficiency through smart contracts. They also explore the extent to which permissioned blockchains and new applications of cryptographic technologies, such as autonomous identities and zero-knowledge proof, can help overcome the challenge of transparency and, therefore, act as catalysts for the adoption and dissemination of BC in organizations.

As mentioned, one proposal to attack this problem is through zero-knowledge proof (ZKP). This cryptographic technique can be used in the blockchain environment to verify if the prover has a sufficient number of transactions without leaking private transaction data (Konkin & Zapechnikov, 2023).

Similarly, Sun et al. (2021) conducted a study on ZKP in the blockchain environment to highlight security issues and challenges and discuss the framework, models, and applications of ZKP. In conclusion, ZKP is a valuable tool for improving privacy and security in blockchain transactions, allowing transactions to be verified without revealing sensitive details.

Consensus

Consensus is achieved through algorithms, thanks to which the "network makes consensual decisions, validates the information, and assigns tasks to each of the nodes comprising it" (Criptodemy, n.d.). This concept was initially introduced by Adam Back in May 1997 and sought to regulate the excessive abuse of internet resources, such as emails and anonymous remailers (Back, 2002).

In the words of Narayanan et al. (2016), consensus can be defined as a process by which nodes agree on the validity of a transaction before adding it to the blockchain. The most significant example of this type of consensus protocol can be found in the proof of work (PoW) used by Bitcoin. This protocol involves miners competing to solve complex mathematical problems, and the first to do so has the right to add a new block. This mechanism ensures that all parties in the network agree on the status of the blockchain and that transactions are valid and secure.

Consensus Algorithms

There are various consensus protocols and algorithms to ensure network security and reliability; each one defines its characteristics and advantages. Some are:

Proof of Work (PoW)

PoW is the most well-known consensus protocol, primarily associated with Bitcoin and Ethereum, although it is used in other cryptocurrencies and blockchain networks. In essence, proof of work requires network nodes to perform computationally intensive calculations to demonstrate that they have invested time and resources into verifying transactions. This process is known as *mining,* and the participants are called *miners.* It is continually repeated to keep the blockchain secure and distributed.

According to Narayanan et al. (2016), proof of work is a complex mathematical puzzle requiring a large amount of computing power to solve. Miners compete to solve this puzzle, and the first to do so has the right to add a new block to the chain and is rewarded with new coins (e.g., bitcoins) and transaction fees.

Nakamoto (2008) first introduced the concept of *proof of work* in the context of Bitcoin and provided the theoretical foundations for its operation. In Nakamoto's own words, its adoption is similar to that presented by Back (2006), Hashcash. This algorithm was initially used to address email spam and DDoS attacks and is currently used for transaction verification purposes.

PoW, as a consensus protocol, has proven effective in preventing malicious attacks and creating a secure and reliable record of transactions on the blockchain network. However, its greatest weakness is its poor scaling capacity and limited performance in terms of transactions per second (TPS). This protocol is perhaps one of Nakamoto's most outstanding contributions to the creation of BC. At the

same time, it has solved one of the most challenging problems in computing, known as the Byzantine generals problem. Advantages: proven security, high attack resistance of 51%. Disadvantages: high energy consumption, centralization in mining.

Proof of Stake (PoS)

In PoS, validators lock a certain amount of cryptocurrency as collateral, and the probability of being selected to validate a block is based on the number of coins at stake. Ethereum has migrated PoS with Ethereum 2.0. This type of consensus was introduced as a more efficient and less expensive alternative to (PoW). Instead of requiring miners to perform intense computational calculations, PoS allows network participants to create blocks and validate transactions based on the number of coins they own and are willing to "stake" for consensus (Ge et al., 2022).

There is a wide variety of consensus algorithms derived from PoS, including, but not limited to, DPoS, Snow White, Sleepy Consensus, Ouroboros, Ouroboros Praos, Ouroboros Genesis, Ouroboros Crypsinous, EOS, Improvement of DPoS (Ge et al., 2022).

Advantages: energy efficiency, less centralization, incentivizes coin holders, fewer barriers to entry (the network accepts participants without the need to purchase and configure expensive hardware), faster transactions compared to PoW networks. Disadvantages: possible centralization based on wealth, as those with more coins have more opportunities to create blocks; the "nothing at stake" problem; there is no actual cost associated with validating incorrect blocks, which can lead to security issues.

Delegated Proof of Stake (DPoS)

This is a variant of PoS in which a community-chosen group of validators is responsible for validating transactions. EOS is an example of a blockchain that uses DPoS. Advantages: high scalability and speed in confirming transactions. Disadvantages: less decentralization and power concentration in the chosen nodes.

Proof of Authority (PoA)

Algorithms are based on reputation, where validators do not risk cryptocurrencies but their reputation; consequently, they are chosen arbitrarily as they are considered trustworthy. Its use primarily occurs in private networks, including

logistics, where it is seen as an efficient and sensible solution because its nature enables the harnessing of the characteristics of BC while preserving participants' privacy. Advantages: energy efficiency, high speed compared to PoW and PoS, monetary incentives. Disadvantages: less decentralization since it is based on a limited number of block validators; vulnerable to collusion, as a limited number of validators are trusted, with the risk that they may collude to act maliciously.

Proof of Space and Time (PoST)

This is a new cryptographic primitive that allows a prover to convince a verifier that they have spent a "space-time" resource. In the words of Ortega (2023), "... in the Proof of Space and Time algorithm, network nodes must demonstrate that they are storing a specific amount of data through a process called farming." Advantages: energy efficiency, which may be possible to mine with this algorithm on standard devices; accessible to more participants; decentralization of the process. Disadvantages: permanent growth because as more miners are added to the network, more storage space is required (Moran & Orlov, 2019).

Round Robin

Round Robin in BC has been studied in several scientific papers. A proposal for its use is presented by Raikwar and Gligoroski (2021), who propose the R3V consensus protocol. This selects a set of leader candidates rotating based on seniority. They then compete to be the leader of the block by solving a puzzle based on a verifiable delay function (VDF) (Raikwar & Gligoroski, 2021). Advantages: greater resistance against most attacks common in PoS protocols, lower power consumption, less communication complexity, and greater fairness. Lastly, other existing less widespread algorithms are proof of weight (PoW), proof of importance (PoI), proof of coverage (PoC), and directed acyclic graphs (DAG).

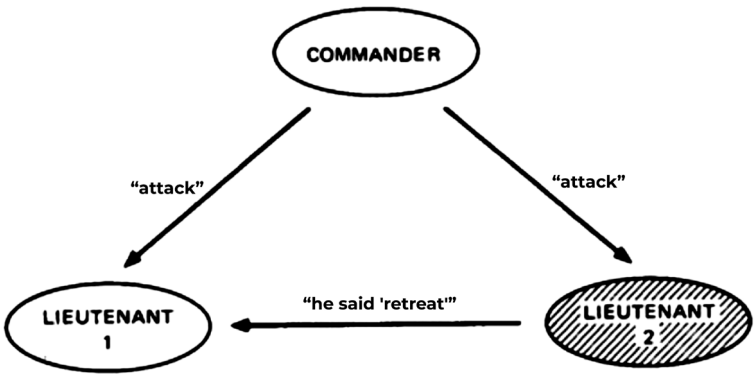
The Byzantine Generals Problem: A Military Perspective

The Byzantine generals problem was stated by Robert Shostak and developed with Leslie Lamport and Marshall Pease in 1982 at the scientific and technological research center SRI International (BBC News Mundo, 2020). It undoubtedly captures the essence of the problem of consensus in a network with untrustworthy agents.

From a game theory perspective, it describes the extent to which decentralized parties experience difficulties in reaching consensus without a trusted central agent.

In essence, a war scenario is proposed where a group of Byzantine generals besieges a city from various points, and it must be agreed whether to attack or retreat in a coordinated manner. Only one general can give the order to the entire force since he is the commander. The rest of the generals are considered lieutenants. Lieutenants communicate with each other when they receive orders from the commander, and the two possible orders from the commander are "attack" and "retreat." It is known that one or more generals can be traitors. The goal is for all loyal generals NOT to agree. To do this, they may provide incorrect information. For example, if the commander is a traitor, he may send conflicting orders to different lieutenants. If the lieutenant is a traitor, he can show it to the other lieutenants to confuse them and make them believe that the traitor is the commander and that the commander sent them orders contrary to his orders (Soto, 2020). A successful battlefield solution must lead to one of two outcomes: 1) all loyal lieutenants make the same decision, and 2) if the commander is loyal, all lieutenants will faithfully carry out his orders. Figure 3 illustrates the case where "Lieutenant 2" is a traitor.

Figure 3. *Lieutenant 2 Is a Traitor*



Source: Lamport et al. (1982).

These problems are associated with the need for consensus and the possibility of unreliable actors in the system. A reliable computer system must deal with malfunctioning components that provide conflicting information to various system parts. The problem is finding an algorithm that guarantees loyal generals reach an

agreement. It was shown that using only verbal messages could solve this problem if more than two-thirds (2/3) of the generals were loyal. A traitor can confuse two loyal generals. This problem is transferred to the blockchain world when it is necessary to add a new block to the chain, where each node must agree on the status of the system before becoming part of it. Clearly, in our context, "loyalty" is a constitutive aspect of trust.

Threats in a Blockchain Network

The most outstanding aspect of building a secure system that BC offers is its immutability. However, this is not 100 % guaranteed to be invulnerable. BC can be compromised under certain circumstances. Some of these possible scenarios are:

- 51 % attack: This type of attack is caused by the possibility that a group of miners controls more than 50 % of the network's computing power, thereby being able to change and reorganize the blockchain (affecting its integrity), override previous transactions, and create an alternative chain. However, performing a 51 % attack on a network with many miners is highly costly, although such attacks have been identified (Sayeed & Marco-Gisbert, 2019).
- Sybil attack: It is named after the book *Sybil* (Schreiber, 1973) and the story of a woman diagnosed with dissociative disorder. The attack is characterized by P2P networks corrupted through the creation of false identities. The vulnerability of a BC network to this attack will depend on the cost of generating identities, the degree to which the reputation system accepts new identities, and whether the reputation system treats all entities identically. Mohaisen and Kim (2013) identify three main defense strategies: 1) trusted certification entities, 2) resources testing (IP testing, network coordinates, and algorithm resolution, among others), and 3) social networks (Mohaisen and Kim, 2013).
- Double-spending attacks: Although most blockchains are designed to prevent double-spending, in certain circumstances, an attacker could attempt to spend the same cryptocurrency twice before the network updates its status. This risk occurs in chains with slow transaction confirmations. There are different types of double-spending attacks. A recent study presents an attack called Adaptive Double-Spending Attack (Adaptive DSA) as an advanced double-spending attack in PoW-based BCs.

The attacker duplicates a valid transaction in the network and converts it into a Markov decision process (MDP), and through focused exploitation in stochastic dynamic programming (SDP), optimized Adaptive DSA attack strategies are exploited (Zheng et al., 2023).

- Presence of protocol vulnerabilities: Bugs or vulnerabilities in a blockchain's software or protocol can be exploited to compromise immutability. For instance, errors in the code implementation can allow an attacker to make invalid transactions or alter the status of the chain.
- Forks and protocol upgrades: Sometimes, a blockchain may experience a fork or protocol upgrade that could affect immutability. If a community disagrees with changes to the protocol, it could result in two separate chains (hard forks), which could have implications for the immutability and continuity of the chain.

Blockchain, Disruptive Technology

BC technology is one of the greatest innovations of the 21st century, with a significant impact on sectors such as finance, manufacturing, electronic voting, and education, to name a few. This section includes systematic reviews conducted by third parties that assess the impact of BC on various areas. The aim is to validate the hypothesis that implementing blockchain technology can significantly enhance digital trust by providing a decentralized and transparent system. This guarantees data integrity and immutability, which could lead to greater adoption of digital services, a reduction in fraud, and improved efficiency of digital transactions.

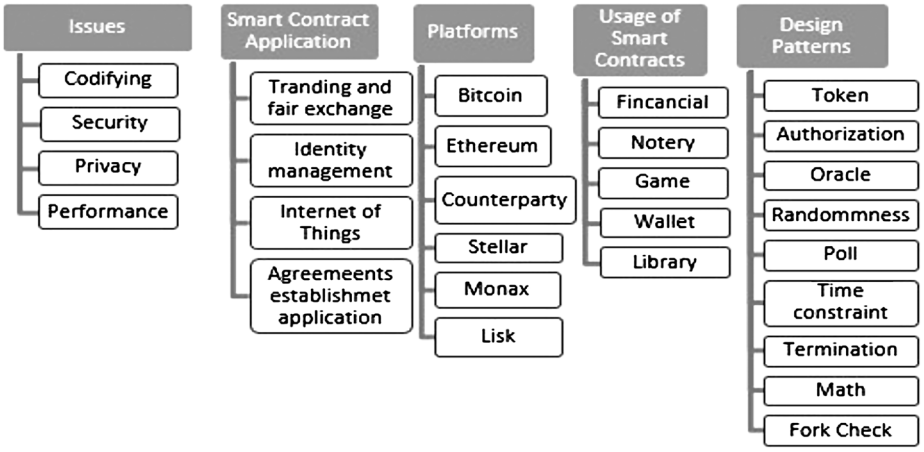
Works such as Baena and García's (2022) establish, after a rigorous bibliographic review, a consensus regarding the benefits of security, transparency, traceability, trust, authenticity, privacy, and the reduction of costs in supply chains through blockchains.

For their part, Xu et al. (2019) studied 756 articles, which were narrowed down to 119 under the economics and business criteria. They highlight the potential impact in areas such as crowdfunding and accounting management, data storage and sharing, supply chain management, and smart trading to benefit from BC characteristics (Xu et al., 2019).

Leka et al.'s study examines 292 papers extracted from databases such as IEEE, ACM, Science Direct, and Springer, focusing its final diagnosis on 28 papers regarding the use of blockchain (BC) in smart contracts. It identifies code

errors, malicious attacks, and exploitations of miners and users as the principal vulnerabilities. Additionally, it reviews various tools and methods for verifying and auditing smart contracts. Figure 4 presents an interesting classification diagram that includes aspects such as coding, security, privacy, and performance, all of which are relevant to any application and field where BC is used. Therefore, it is advisable to adopt its taxonomic approach when evaluating particular use cases (Leka et al., 2019).

Figure 4. *Smart Contract Classification Diagram*



Source: Leka et al. (2019).

Romero (2018) highlights the use of distributed ledger technology (DLT) in financial transactions, with advantages such as accelerating the settlement process of financial transactions, reducing the number of intermediaries, and improving the efficiency of the reconciliation process. He shows how it can enhance the transparency and traceability of transactions, which is especially useful in international trade, where there are many actors, and facilitates the negotiation and post-negotiation of securities, regulatory compliance, and digital identity management. Besides, the trend toward a total digitalization of the economy is clear. Aspects such as the digital transformation based on the Fourth Industrial Revolution have led to an economy considered digital (Bogdanov et al., 2021), where BC is used as a technological enabling element.

At this point, it is evident that the impact of BC has expanded beyond its use in cryptocurrencies. BC has become a mainstay in various fields such as supply chain, healthcare, and intellectual property protection. According to Tapscott and

Tapscott (2016), blockchain provides greater visibility and traceability in the supply chain, allowing for real-time tracking of products from origin to destination. In the healthcare sector, Griggs et al. (2018) point out that blockchain guarantees the security and privacy of electronic medical records, facilitating the secure exchange of information between doctors and patients. Furthermore, blockchain offers an immutable record of authorship and ownership of digital content in copyright and intellectual property, which can be fundamental for protecting creators' rights (Lorenzo, 2020).

All-in-all, BC can help improve trust and collaboration among different parties in sectors such as Industry 4.0. Haleem et al. (2012, 2022) highlight several enabling aspects of BC in smart cities, smart factories, smart products, and supply chains.

Regarding social responsibility, the proposal to use BC as an audit instrument and operating model is interesting (Martínez et al., 2020), thanks to the data logging model that can be employed in wallets.

Authors such as Haleem et al. (2021) identify a wide range of BC applications and features, such as distributed accounting that enables secure and audited transmission of patient medical records and drug supply chain management. However, the main obstacle is the lack of experience in the field of applications that use BC technology. Another example of the use of BC is the drug supply chain (Casino et al., 2019).

On the other hand, architectural scenarios in which BC is used as a solution to problems in the centralization of resources in IoT networks enable the storage of sensor data centrally instead on the distributed basis of BC, where sensor data can be managed similarly to the blockchain philosophy (Conoscenti et al., 2017).

Blockchain and Cybersecurity

While some characteristics that make BC a dynamic agent of cybersecurity have already been mentioned, some aspects that they reinforce are:

Advantages and Benefits

- Greater security and data protection due to its immutable structure
- Improved data transparency and integrity through distributed auditing and verification
- Highly available and resilient architectures

- Reduced points of vulnerability and risk through decentralization and resistance to cyberattacks

Practical Applications of Blockchain in Cybersecurity

- Identity protection and authentication through IDMS (identity management systems) systems to manage authentication, authorization, and file sharing
- Logging and verification of security events for intrusion detection and forensic analysis
- Data access and control management through smart contracts
- Distributed accounting and operational transparency
- Redundant and resilient architectures

Challenges and Considerations Regarding the Use of Blockchain in Cybersecurity

- Scalability and performance
- Privacy and protection of personal data in transparent BC environments
- Update and maintenance of BC infrastructure to ensure long-term security
- Collaboration and development of BC standards focused on cybersecurity
- Cooperation among the actors involved, such as developers, researchers, and end-users
- Statement of good practices for BC implementation in cybersecure environments

Building a Digital Trust Ecosystem

There are numerous and diverse fields of use of blockchain technology and its potential for building digital trust. But this, like all technology, is not a panacea. Its adoption is a process that must be built daily and with the participation of all stakeholders and, above all, guarantee its use as a means and not as an end. A priori, BC conceives security by design based on immutability, integrity, and transparency characteristics. Once transactions are confirmed, the data is permanently stored in the tamper-proof ledger, and these transactions are safeguarded. In terms of design, BC technology includes cryptography and distributed consensus as

preventive mechanisms to reduce cyberattack risks and a distributed architecture without requirements for central "trusted" entities. Without trusted intermediaries, trust within a BC network is made possible by four key features: 1) ledger: It provides transactional traceability. Unlike traditional databases, transactions in BC are not deleted; 2) security: Data is considered cryptographically secure, guaranteeing non-tampering; 3) sharing: The ledger is shared among several participants, which provides transparency; and 4) distributed nature: It allows the number of nodes in a BC network to be scaled to make it more resistant to possible cyberattacks and optimize the delivery and consumption of content.

Thus, the key pillars of information security (immutability-integrity, availability-distributed and redundant networks, transparency-distributed audit), combined with the construction and adoption of practices and strategies in cybersecurity, ultimately allow us to build a reliable digital ecosystem.

At the national level, it is worth highlighting that the Ministry of Information and Communications Technologies expressly states the potential for building digital trust:

> The key of DLT/Blockchain is to build "trust" in the transactions carried out on the network, to the point that neither physical documents (papers) nor centralized entities (banks or notaries) are required to possess a security that represents social or economic value. (MinTIC, 2022)

In the national context, it is important to highlight the integration between the government and the Inter-American Development Bank (IDB) to promote BC through initiatives such as the space for experimenting with BC projects in the public sector, which was born from the signing of a memorandum of understanding with IDB Lab, the IDB's innovation laboratory.

Likewise, the MinTIC published the "Reference Guide for the Adoption and Implementation of Projects with Blockchain Technology for the Colombian State." This facilitates the State's approach to this technology, promotes an ethical and compliance approach, introduces a governance approach, presents guidelines for developing projects in government agencies, and provides tools so that projects are designed and operated in an organized, staggered, and structured manner.

Discussion

Conversely, the promise of BC as a high-impact technology in different fields and its potential to ensure cybersecurity practices must be responsibly addressed.

Problems such as the limitation in scalability derived from the size that BC can reach would be solved by implementing chain pruning algorithms, which implies that "old transactions could be eliminated, saving only their hash, to preserve the integrity of the chain" (Pérez & Joancomartí, 2014).

The challenges BC faces in decentralized environments can be overcome using network protocols such as Named Data Networking (NDN). This can contribute to driving BC by enhancing effective content delivery through name-based routing and caching in the network. This approach allows for efficient content delivery and improved data transfer, particularly in decentralized networks where efficiency is crucial (Guo et al., 2019; Kharjana et al., 2023). However, it is worth clarifying that NDN is not directly compatible with BC since BC applications (without permissions) generally require the transmission of transactions and blocks in real time, which is not compatible with the "pull" design of NDN.

Under this premise, BoNDN (BC over NDN) becomes an integration alternative. This is based on a core NDN design and processes each type of data that needs to be transmitted individually (Guo et al., 2019). BoNDN proposes a push-subscription approach to support block transmission, in which each miner makes a subscription. Once a block is generated, the subscribed miner will receive the block (Benmoussa et al., 2023).

In the field of application development, the emergence of architectural patterns specific to BC is already a reality that heralds the evolution of the technology in question. Alzhrani et al. (2023) describe twelve patterns applicable to 400 existing applications.

Along these lines is the development of Byzantine fault-tolerant (BFT) algorithms and libraries. Castro and Liskov (2001) describe a new BFT replication algorithm developed to design highly available systems that tolerate Byzantine faults. The algorithm is used in asynchronous environments such as the internet, and it incorporates mechanisms that prevent faulty nodes and allow for proactively rapid recovery of replicas. Its fault tolerance is guaranteed if less than 1/3 of the replicas fail in the failure window. Castro and Liskov (2001) also present an implementation of the algorithm as a generic library and its application to build the first Byzantine fault-tolerant NFS file system.

Having said that, authentication alternatives other than traditional ones, such as attribute-based encryption (ABE), guarantee that only those with specific attributes can access information, which can be an effective solution for access control and encrypted data sharing (Hong et al., 2022). ABE can generally be

divided into two patterns: ciphertext-policy ABE (CP-ABE) and key-policy ABE (KP-ABE). The access policy is incorporated into the ciphertexts, and the user's private key is associated with a collection of attributes such as location, age range, email addresses, etc. However, ABE can be vulnerable to attacks such as key abuse and custody (Arshad et al., 2023). In summary, ABE is a powerful tool for access control and data sharing, but it presents challenges that must be addressed for effective implementation.

In terms of trust, so-called permissionless BC networks provide trust capabilities among parties without prior knowledge of each other. This principle can allow transactions to be carried out directly, delivering transactions faster and at lower costs. On the other hand, a BC network that more strictly controls access, called a permissioned network, where there is a certain level of trust among the parties, has capabilities that help reinforce that trust.

Another fundamental aspect is the performance that results from the high relevance to allow for the evolution of technology; this is promising given the increase in transactions per second (TPS), going from 4–6 TPS in the first generation BC to 100,000–300,000 TPS in the fourth and the potential that will be unlocked in a fifth generation with the adoption of technologies such as 6G (Hasan et al., 2022).

The availability of BC networks could not be left out of this discernment. Permanently interacting with cyberspace has created a strong dependence on applications and interaction spaces that constitute a "vital" ecosystem. In this context, the construction of high resource availability is decisive, guaranteeing a service without failures and interruptions (Castro & Liskov, 2001).

It is well known that the first strategy in availability is replication. Thanks to this, redundancy is achieved by providing resources that may eventually fail and "taking over" redundant resources. In BC, replication and fault-tolerant algorithms such as BFT (Byzantine-fault-tolerant) help build hierarchical structures that optimize the use of resources and increase scalability (Rahulamathavan et al., 2017).

The latter may be undesirable in devices with low storage capacity, which shows that BC must be able to adapt to different scenarios, knowing how to "exploit" particular features for specific needs. So, the advantage that total and cumulative data protection on the blockchain may represent might not be desirable in other scenarios.

Blockchain storage is carried out with great redundancy: Every full node in the network contains an entire copy of the BC (and its transactions), allowing these nodes to validate each new transaction correctly. However, maintaining a complete

copy of the chain can be a problem for nodes that operate on lightweight devices such as mobile devices (Pérez & Joancomartí, 2014).

Finally, it is worth reflecting on whether BC is "magic" capable of solving all modern problems, as suggested by many articles, and as Clarke (1962) stated in his third "law": "Any sufficiently advanced technology is indistinguishable from magic." The answer is no. This must be considered alongside the development of an information security culture, after evaluating its engineering implications in the field of exploration.

Conclusions

Blockchain introduces disruptive aspects in constructing information systems and applications that preserve immutability and transaction records. Concepts such as decentralization, immutability, and consensus are fundamental in BC and have revolutionized how we handle and trust digital data. Decentralization eliminates the need for intermediaries; Immutability ensures data integrity, and consensus ensures that all parties reach reliable agreements in a distributed network. These principles are the foundation of security and trust in BC-based applications and can potentially transform numerous industries.

Although transparency is one of the main advantages of blockchain technology, it can also pose challenges, especially when protecting sensitive data and complying with privacy regulations. Aspects like this, along with high energy consumption and growth in node size, can limit the adaptation of BC as a technology. However, several strategies have been documented in this work to overcome it.

Thus, combinations such as using NDN and BoNDN to address connectivity problems with the immutable and reliable distributed ledger feature of BC can guarantee that the data exchanged is trustworthy and less susceptible to packet losses and cyberattacks.

Blockchain is not a solution on its own. It is a technological tool that must be accompanied by a strategic plan that understands the project's needs, identifies the degree of transparency and decentralization, determines the members who will act as nodes, and establishes the appropriate blockchain structure, defining the transactions or smart contracts to be executed (MinTIC, 2020).

This critical review includes aspects of the different considerations for developing solutions that, through BC, ensure cybersecurity and, thus, build a reliable digital ecosystem.

References

Ali, R., Clarke, D., & McCorry, P. (2017). Towards developing a blockchain-based approach for the secure storage of patient records. In I*EEE International Conference on E-Health Networking, Applications and Services* (pp. 400-406). IEEE.

Alzhrani, F., Saeedi, K., & Zhao, L. (2023). Architectural patterns for blockchain systems and application design. *Applied Sciences, 13*(20), 11533. https://doi.org/10.3390/app132011533

Amazon Web Services. (n.d.). What is decentralization? https://aws.amazon.com/es/blockchain/decentralization-in-blockchain/

Arshad, H., Picazo-Sanchez, P., Johansen, C., & Schneider, G. (2023). Attribute-based encryption with enforceable obligations. *Journal of Cryptographic Engineering,* (13), 343-371. https://doi.org/10.1007/s13389-023-00317-1

Back. A. (2002). Hashcash - A denial of service counter-measure [Technical report]. http://www.hashcash.org/papers/hashcash.pdf

Baena-Luna, P., & García-Río, E. (2022). Tecnología Blockchain: Desafíos presentes y futuros en su aplicación. *Revista Conocimento Online,* (2), 258-273. https://doi.org/10.25112/rco.v2.2859

Banafa, A. (2022, December 22). Blockchain 4.0. https://www.bbvaopenmind.com/tecnologia/mundo-digital/blockchain-4-0/

Benmoussa, A., Kerrache, C. A., Calafate, C. T., & Lagraa, N. (2023). NDN-BDA: A Blockchain-Based decentralized data authentication mechanism for vehicular named data networking. *Future Internet, 15*(5), 167. https://doi.org/10.3390/fi15050167

Bitcoin.es. (2020, November 17). Vamos por la 5ta generación de la Blockchain ¿Cuáles son? https://bitcoin.es/actualidad/vamos-por-la-5ta-generacion-de-la-blockchain-cuales-son/

Brooks, D. (2020, February 9). Criptomonedas: Qué es el "problema de los generales bizantinos" y por qué explica el origen del bitcoin. https://www.bbc.com/mundo/noticias-51380491

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification, and open issues. *Telematics and informatics,* (36), 55-81. https://doi.org/10.1016/j.tele.2018.11.006

Castro, M., & Liskov. B. (2001). Practical byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems,* (20)4, 398-461. https://doi.org/10.1145/571637.571640

Choi., T.-M., & Siqin., T. (2022). Blockchain in logistics and production from Blockchain 1.0 to Blockchain 5.0: An intra-inter-organizational framework. *Transportation Research Part E: Logistics and Transportation Review,* (160), 102653. https://doi.org/10.1016/j.tre.2022.102653

Conoscenti, M., Vetrò, A., & De Martin, J. C. (2017). Peer to peer for privacy and decentralization in the internet of things. In *2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C), Buenos Aires, Argentina* (pp. 288-290). https://doi.org/10.1109/ICSE-C.2017.60

Criptodemy. (2023, January 20). Guía sobre algoritmos de consenso Blockchain. Criptodemy ®. https://criptodemy.com/guia-algoritmos-consenso-blockchain/

Guo, J., Wang, M., Chen, B., Yu, S., Zhang, H., & Zhang, Y. (2019). Enabling Blockchain applications over named data networking. In *2019 IEEE International Conference on Communications (ICC), Shanghai, China* (pp. 1-6). IEEE. https://doi.org/10.1109/ICC.2019.8761919

Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. In A. J. Menezes & S. A. Vanstone (Eds.), Advances in Cryptology-CRYPTO' 90 (pp. 437-455). Springer. https://doi.org/10.1007/3-540-38424-3_32

Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks,* (2), 130-139. https://doi.org/10.1016/j.ijin.2021.09.005

Hasan, M. K., Akhtaruzzaman, Md., Kabir, S. R., Gadekallu, T. R., Islam, S., Magalingam, P., Hassan, R., Alazab, M., & Alazab, M. A. (2022). Evolution of industry and Blockchain era: Monitoring price hike and corruption using BIoT for smart government and industry 4.0. *IEEE Transactions on Industrial Informatics, 18*(12), 9153-9161. https://doi.org/10.1109/tii.2022.3164066

Hong, L., Zhang, K., Gong, J., & Qian, H. (2022). A practical and efficient blockchain-assisted attribute-based encryption scheme for access control and data sharing. *Security and Communication Networks,* (2022), 4978802. https://doi.org/10.1155/2022/4978802

Hurtado, J. S. (2021, July 1). Qué son las DLT y en qué se diferencian de Blockchain. https://www.iebschool.com/blog/que-son-las-dlt-y-en-que-se-diferencian-de-blockchain-digital-business/

Kharjana, M., Pohrmen, F. H., Sahana, S. C., & Saha, G. K. (2023). Blockchain-based key management system in named data networking: A survey. *Journal of Network and Computer Applications,* (220), 103732. https://doi.org/10.1016/j.jnca.2023.103732

Konkin, A., & Zapechnikov, S. (2023). Zero knowledge proof and ZK-SNARK for private blockchains. *Journal of Computer Virology and Hacking Techniques,* (19), 443-449. https://doi.org/10.1007/s11416-023-00466-1

Krichen, M., Ammi, M., Mihoub, A., & Almutiq, M. (2022). Blockchain for modern applications: A survey. *Sensors, 22*(14), 5274. https://doi.org/10.3390/s22145274

Leka, E., Selimi, B., & Lamani, L. (2019). Systematic literature review of blockchain applications: Smart contracts. In *2019 International Conference on Information Technologies (InfoTech)* (pp. 1-3). IEEE. https://doi.org/10.1109/InfoTech.2019.8860872

Lorenzo, C. (2020). Blockchain for copyright and intellectual property protection. In *Handbook of research on emerging business models and managerial strategies in the nonprofit sector* (pp. 180-198). IGI Global.

Martínez-Ríos, F. O., Marmolejo-Saucedo, J. A., & Abascal-Olascoaga, G. (2020). A new protocol based on blockchain technology for transparent operation of corporate social responsibility. In S. García-Álvarez & C. Atristain-Suárez (Eds.), *Strategy, power, and CSR: Practices and challenges in organizational management* (pp. 205–233). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83867-973-620201012

Ministerio de Tecnologías de la Información y Comunicaciones [Mintic]. (2022). *Guía de referencia de Blockchain para la adopción e implementación de proyectos en el Estado colombiano.* Mintic. https://gobiernodigital.mintic.gov.co/692/articles-161810_Ley_2052_2020.pdf

Mohaisen, A., & Kim, J. (2013, December 22). The Sybil attacks and defenses: A survey. https://arxiv.org/abs/1312.6349

Moran, T., & Orlov, I. (2019). Simple proofs of space-time and rational proofs of storage. In A. Boldyreva & D. Micciancio (Eds.), *Advances in Cryptology–CRYPTO 2019* (pp. 381-409). Springer International Publishing. https://eprint.iacr.org/2016/035.pdf

Mougayar, W. (2016). *The business Blockchain: Promise, practice, and application of the next internet technology.* Wiley.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.* https://bitcoin.org/bitcoin.pdf

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction.* Princeton University Press.

Ortega Llorente, P. O. (2023). Estudio comparativo de algoritmos de consenso para una Blockchain orientado al consumo de energía [Bachelor's thesis, Universidad Politécnica de Madrid]. Repositorio UPM. https://oa.upm.es/75158/1/TFG_PABLO_ORTEGA_LLORENTE.pdf

Pérez Solà, C., & Joancomartí, J. (2014). Bitcoins y el problema de los generales bizantinos. In R. Álvarez Sánchez, J.-J. Climent Coloma, F. Ferrández Agulló, F. Martínez Pérez, L. Tortosa Grau, J. F. Vicent Francés, A. Zamora Gómez (Coords.), *Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información RECSI XIII: Alicante, 2-5 de septiembre de 2014* (pp. 241-246). https://rua.ua.es/dspace/handle/10045/40461

Popchev, I., Radeva, I., & Velichkova, V. (2021). Blockchains in enterprise global risk management. In *2021 International Conference Automatics and Informatics (ICAI)* (pp. 282-287). IEEE. https://doi.org/10.1109/ICAI52893.2021.9639500

Raikwar, M., & Gligoroski, D. (2021). R3V: Robust round robin VDF-based consensus. In *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)* (pp. 81-88). IEEE. https://doi.org/10.1109/BRAINS52497.2021.9569781

Relictum Pro. (n.d.). Is blockchain 5.0 of the latest generation. https://relictum.pro/

Romero Ugarte, J. L. (2018). Distributed ledger technology (DLT): Introduction. *Economic Bulletin,* (4) 2-11. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3269731

Sayeed, S., & Marco-Gisbert, H. (2019). Assessing Blockchain consensus and security mechanisms against the 51% attack. *Applied Sciences, 9*(9), 1788. https://doi.org/10.3390/app9091788

Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations. *Electron Markets,* (32), 1779-179. https://doi.org/10.1007/s12525-022-00536-0

Soto, M. G. (2018, August 6). El problema de los generales bizantinos (PGB). https://marvin-soto.medium.com/el-problema-de-los-generales-bizantinos-pgb-e0cb8c4279c2

Sun, X., Yu, F. R., Zhang, P., Sun, Z., Xie, W., & Peng, X. (2021). A survey on zero-knowledge proof in blockchain. *IEEE Network, 35*(4), 198-205. https://doi.org/10.1109/MNET.011.2000473

Swan, M. (2015). *Blockchain: Blueprint for a New Economy* (1st ed.). O'Reilly Media, Inc.

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the Technology behind Bitcoin Is Changing Money, Business, and the World.* Penguin.

Vamsi_Cz5cgo. (2016, January 28). The Architecture of Blockchain (4/5). https://www.vamsitalkstech.com/blockchain/the-architecture-of-blockchain-45/

Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. *Financial Innovation,* 5, 27. https://doi.org/10.1186/s40854-019-0147-z

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain Technology? A systematic review. *PLoS ONE, 11*(10), e0163477. https://doi.org/10.1371/journal.pone.0163477

Zheng, J., Huang, H., Zheng, Z., & Guo, S. (2023). Adaptive double-spending attacks on PoW-based Blockchains. In *IEEE Transactions on Dependable and Secure Computing* (pp. 1-13). IEEE. https://doi.org/10.1109/TDSC.2023.3268668