Horizon | Journal of Humanity and Artificial Intelligence

BLOCKCHAIN IN CYBERSECURITY

Matthew N. O. Sadiku
Department of Electrical & Computer Engineering Prairie View A&M University Prairie View, TX USA

Uwakwe C. Chukwu
Department of Engineering Technology South Carolina State University Orangeburg, SC, USA

Janet O. Sadiku
Juliana King University Houston, TX, USA

Abstract

Cyber security is the practice of protecting systems and networks from digital attacks. Block chain is the latest cyber security technology that is gaining popularity and recognition. Block chain provides security, anonymity, and data integrity without the need of a third party. Block chain is regarded as a new weapon in cyber security. Cyber security is built into block chain technology because of its inherent nature of being a decentralized system based on principles of security, privacy, and trust. In today's digital world, where cyber threats are a major concern, the use of block chain technology can provide a robust solution to enhance cyber security. This paper provides an overview of block chain security.

Keywords: block chain, distributed ledger technology, Bitcoin, cyber security.

INTRODUCTION

Today, data is a new oil for any business growth. As enterprises amass tons of sensitive data, they require means of storing and processing the data smartly and securely. In other words, as the world goes online it is imperative to maintain the security of online data. Any attempt to gain unauthorized access to computers or online data with the intent to cause harm is a cyber attack. Cybercriminals are increasing the frequency and sophistication of cyber attacks by pooling their knowledge and leveraging new technologies. Cybercrime costs the global economy an estimated $450 billion every year. Our current security protocols simply cannot keep up with the relentless and clever attacks.

Cybersecurity is a major concern for business in the digital environment. With the increase in cyber attacks, organizations seek innovative methods to secure their data and assets. Blockchain technology is emerging as the ultimate weapon in the fight against cybercrime. It is a revolutionary technology poised to change the future of computing and disrupt several industries with innovative solutions. By leveraging blockchain-based storage solutions that provide decentralized storage capability, organizations can protect their digital information and assets. The decentralized nature of blockchain means that it is not controlled by a single entity, making it more resistant to attacks. The popularity of blockchain has increased worldwide due to its lasting impact on the world [1]. Blockchain is associated with benefits including high level of transparency, integrity, trust, and confidence for the participants.

OVERVIEW OF BLOCKCHAIN

Blockchain (BC) technology is a permanent record of online transactions. It is a distributed tamper-proof database, shared, and maintained by multiple parties. It is a new enabling technology that is expected to revolutionize many industries, including business. It has the potential for addressing

significant business issues. The BC technology allows participants to move data in real-time, without exposing the channels to theft, forgery, and malice.

The term "blockchain" refers to the way BC stores transaction data – in "blocks" that are linked together to form a "chain." The chain grows as the number of transactions increases. Since every entry is stored as a block on a chain, the care you receive is added to your personal ledger. The first Blockchain was conceived in 2008 by an anonymous person or group known as Satoshi Nakamoto, who published a white paper introducing the concept of a peer-to-peer electronic cash system he called Bitcoin [2]. A typical blockchain architecture is shown in Figure 1 [3]

At its core, blockchain is a distributed system recording and storing transaction records. In a blockchain system, there is no central authority. Instead, transaction records are stored and distributed across all network participants. Rather than having a centrally located database that manages records, the database is distributed to the networks and transactions are kept secure via cryptography. BC eliminates the need for a middleman that traditionally may facilitate such transactions. Figure 2 shows how blockchain works [4].

Fundamentally, blockchains are distributed digital database that record and maintain a list of transactions taking place in real time. They may also be regarded as decentralized ledgers that sequentially record transactions or interactions among users within a distributed network. They have the following properties [5]:

- Firstly, they are autonomous. They run on their own, without any person or company in charge.
- Secondly, they are permanent. They are like global computers with 100 percent uptime. Because the contents of the database are copied across thousands of computers, if 99 per cent of the computers running it were taken offline, the records would remain accessible and the network could rebuild itself.
- Thirdly, they are secure and tamper-proof. Each record in blockchain is time stamped and stored cryptographically. The encryption used on blockchains like Bitcoin and Ethereum is industry standard, open source, and has never been broken.
- Fourthly, they are open, allowing anyone to develop products and services on them.
- Fifthly, as blockchain is a shared system, costs are also shared between all of its users.

The blockchain was designed so transactions are immutable, i.e. they cannot be deleted. Thus, blockchains are secure and meddle-free by design. Data can be distributed, but not copied. When it comes to digital assets and transactions, you can put almost anything on a blockchain. Different scenarios call for different blockchains. Blockchain is used in different areas such as depicted in Figure 3 [6].

The BC technology currently has the following features [7,8]:

1. **Peer-to-Peer (P2P) Network:** The first requirement of BC is a network, an infrastructure shared by multiple parties. This can be a LAN at a small scale or the Internet at a large scale. All nodes participating in a BC are connected in a decentralized P2P network. Transactions are broadcast to the P2P network. Due to some limitations of P2P networks, some vendors have provided cloud-based BCs.
2. **Cascaded Encryption:** A BC uses encryption to protect transaction data. Blocks are encrypted in a cascaded manner, i.e. the encryption result of the previous block is used in encrypting the current block. The BC is secured by public key cryptography, with each peer generating its own public-private key pairs.
3. **Distributed Database:** A BC is digitally distributed across a number of computers. Each party on a BC has access to the entire database and no single party controls the data or the information. Since BC is decentralized, there is no need for central authorizes such as banks.

4. **Transparency with Pseudonymity:** Each node or participant on a blockchain has a unique 30-plus-character alphanumeric address that identifies it. Users can choose to remain anonymous or provide proof of their identity to others.
5. **Irreversibility of Records:** Once a transaction is entered in the database and the accounts are updated, the records cannot be altered. Records on the database is permanent, chronologically ordered, and available to all others on the network.

There are two types of Blockchains: public and private. Public Blockchains are cryptocurrencies such as Bitcoin, enabling peer-to-peer transactions. Private Blockchains use Blockchain-based platforms such as Ethereum or Blockchain-as-a-service (BaaS) platforms running on private cloud infrastructure. A private BC is an intranet, while a public BC is the Internet. Companies will be disrupted the most by public Blockchains.

CYBERSURITY BASICS

Cybersecurity refers to a set of technologies and practices designed to protect networks and information from damage or unauthorized access. It is vital because governments, companies, and military organizations collect, process, and store a lot of data. As shown in Figure 4, cybersecurity involves multiple issues related to people, process, and technology [9].

A typical cyber attack is an attempt by adversaries or cybercriminals to gain access to and modify their target's computer system or network. Cyber attacks are becoming more frequent, sophisticated, dangerous, and destructive. They are threatening the operation of businesses, banks, companies, and government networks. They vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists) [10].

The cybersecurity is a dynamic, interdisciplinary field involving information systems, computer science, and criminology. The security objectives have been availability, authentication, confidentiality, nonrepudiation, and integrity. A security incident is an act that threatens the confidentiality, integrity, or availability of information assets and systems [11].

- **Availability:** This refers to availability of information and ensuring that authorized parties can access the information when needed. Attacks targeting availability of service generally leads to denial of service.
- **Authenticity:** This ensures that the identity of an individual user or system is the identity claimed. This usually involves using username and password to validate the identity of the user. It may also take the form of what you have such as a driver's license, an RSA token, or a smart card.
- **Integrity:** Data integrity means information is authentic and complete. This assures that data, devices, and processes are free from tampering. Data should be free from injection, deletion, or corruption. When integrity is targeted, nonrepudiation is also affected.
- **Confidentiality:** Confidentiality ensures that measures are taken to prevent sensitive information from reaching the wrong persons. Data secrecy is important especially for privacy-sensitive data such as user personal information and meter readings.
- **Nonrepudiation:** This is an assurance of the responsibility to an action. The source should not be able to deny having sent a message, while the destination should not deny having received it. This security objective is essential for accountability and liability.

Everybody is at risk for a cyber attack. Cyber attacks vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists). The following are typical examples of cyber attacks or threats [12]:

- **Malware:** This is a malicious software or code that includes traditional computer viruses, computer worms, and Trojan horse programs. Malware can infiltrate your network through the Internet, downloads, attachments, email, social media, and other platforms. Spyware is a type of malware that collects information without the victim's knowledge.

- **Phishing:** Criminals trick victims into handing over their personal information such as online passwords, social security number, and credit card numbers.
- **Denial-of-Service Attacks:** These are designed to make a network resource unavailable to its intended users. These can prevent the user from accessing email, websites, online accounts or other services.
- **Social Engineering Attacks:** A cyber criminal attempts to trick users to disclose sensitive information. A social engineer aims to convince a user through impersonation to disclose secrets such as passwords, card numbers, or social security number.
- **Man-In-the-Middle Attack:** This is a cyber attack where a malicious attacker secretly inserts him/herself into a conversation between two parties who believe they are directly communicating with each other. A common example of man-in-the-middle attacks is eavesdropping. The goal of such an attack is to steal personal information.

These and other cyber attacks are shown in Figure 5 [13].

Cybersecurity involves reducing the risk of cyber attacks. Cyber risks should be managed proactively by the management. Cybersecurity technologies such as firewalls are widely available [14]. Cybersecurity is the joint responsibility of all relevant stakeholders including government, business, infrastructure owners, and users. Cybersecurity experts have shown that passwords are highly vulnerable to cyber threats, compromising personal data, credit card records, and even social security numbers. Governments and international organizations play a key role in cybersecurity issues.

BLOCKCHAIN SECURITY

Blockchain technology is based on decentralization and encryption. Each user has a private key to add blocks and make changes, and a public key to enable others to access the database so they can observe the modifications. Blockchain offers several opportunities to maintain a high level of data security through reliable data encryption mechanisms, data integrity, network resilience, and scalability. By leveraging the power of blockchain technology, organizations can ensure that their data are safe from manipulation, unauthorized access, and malicious attacks. Blockchain security deals with assurance services, cybersecurity frameworks, and best practices to mitigate the risk of fraud and cyber-attacks.

As shown in Figure 6 [15], blockchain security relies on three fundamental elements [15,16]:

- **Confidentiality:** Confidentiality refers to the privacy of information stored and processed digitally. It means to ensure that only interested and authorized parties access the appropriate data.
- **Integrity:** Blockchains built-in characteristics of immutability and traceability help organizations ensure data integrity.
- **Availability:** Data remains available through various nodes and thus full copies of the ledger can be accessed at all times. All the blockchain nodes will have a complete blockchain database so that if a node is unavailable, it will affect the blockchains performance.

The CIA triad is an industry standard and all people who operate in the field of cybersecurity must know the three terms.

Blockchain security is a complete risk management system for blockchain systems. It describes the measures to guard against unwanted access, manipulation, and interruption of a blockchain network. These measures include network architecture, cryptographic mechanisms, and consensus algorithms. With them, it becomes possible to safeguard the integrity and immutability of a blockchain network [17].

APPLICATIONS OF BLOCKCHAINN SECURITY

Different industries can use blockchains to improve the security of their data, financial transactions, and communication. The industries that can benefit the most from applying the blockchain for cybersecurity include [18]:

- **Finance:** In the finance sector, the biggest value of a blockchain is in its data immutability and transaction transparency.
- **Healthcare:** The healthcare industry endures a constant barrage of cyber attacks. The most common examples of blockchain implementation in healthcare are related to securely storing and quickly transferring medical data. Blockchain technology could be the badly-needed solution to a problem that puts patients and hospitals at severe risk.
- **Real Estate:** The real estate platforms use blockchains for solving two major tasks: ensuring safe data storage and automating key processes such as validating property ownership and transferring funds. A blockchain also offers reliability and automation, which are crucial for the successful operation of real estate businesses.
- **Supply Chain:** A blockchain can store tamper-proof records of all operations, transactions, and freight data to simplify the analysis of a supply chain's efficiency and operations. Global giants like Walmart, BMW, and FedEx deploy blockchains for improving data security and operational transparency.
- **Governance:** Blockchains can also be useful for improving the security and transparency of many government processes: tax collection, information governance, elections, etc. During elections, a blockchain can be used to speed up vote counting and ensure the accuracy of results. For example, the Australian government has plans to develop a cybersecurity network based on blockchain. China's government is attempting to secure vital government and military information using blockchain cybersecurity.

BENEFITS

Blockchain technology is not only an innovative technology that revolutionizes the way we store and share data, it is also a powerful cybersecurity tool. It can be used to prevent any data breach, identity theft, cyberattacks, or criminal acts in transactions. The cybersecurity industry can benefit from blockchain's unique features, which create a virtually impenetrable wall between a hacker and your information. The combination of blockchain and cybersecurity has intrigued executives and technology experts. Other benefits include [13,15]:

- **User Confidentiality:** The public key cryptography in a blockchain network helps maintain the confidentiality of the users.
- **Data Transparency and Traceability:** The history of all these transactions is maintained so that they can be traced anytime. The transaction data is digitally signed by members of the blockchain network to ensure transparency.
- Secure Data Storage and Processing: Blockchain's key feature of immutability and records of any changes to the data help store the data safely and securely.
- **No Single Point Failures:** Blockchain systems are decentralized, so the failure of a single node does not affect the entire network.
- **Safe Data Transfers:** The blockchain enables fast and secure transactions of data. PKI in blockchain maintains authentication during data transfers. Smart contracts help to automatically execute agreements between two parties during a transfer.
- **Decentralized Architecture:** One of the main advantages of blockchain technology is its decentralized architecture. This means that there is no single point of control, making it more difficult for hackers to attack and compromise the system.
- **Immutable Records:** One of the popular qualities of blockchain is its immutability. The data stored on a blockchain is immutable, meaning that once a transaction is recorded, it cannot be altered or deleted. This helps prevent data tampering and ensures the integrity of the data, making blockchain technology very good at fraud prevention.

CHALLENGES

Blockchain technology is neither perfect nor completely secure. There will always be people looking for vulnerabilities and means to manipulate the technology in ways the developers never intended. While

the blockchain technology has great potential as a cybersecurity measure, it is also associated with several risks. Other challenges include [13,15]:

- **Reliance on Private Keys:** Blockchain relies heavily on private keys for encrypting data. The keys are long sequences of random numbers automatically generated by a wallet. Private keys are used for interacting with the blockchain and, in contrast to user passwords, cannot be restored. These private keys cannot be recovered once lost.
- **Scalability Challenges:** Scalability may become a constraint when implementing blockchain, mostly due to block size and response times blockchain networks have a preset block volume and limits for transactions per second. Integrating blockchain technology requires a complete replacement of existing systems, which is why companies may find this difficult.
- **Adaptability Challenges:** Though blockchain technology can be applied to almost any business, companies may face difficulties integrating it. Blockchain applications can also require complete replacement of existing systems, so companies should consider this before implementing blockchain technology.
- **High Operating Costs:** Blockchain requires high computing power and storage capabilities. This leads to higher costs compared to non-blockchain applications.
- **Lack of Regulation:** Blockchain concepts are not globally regulated yet. Many countries already have or are working on cryptocurrency regulations. Any blockchain implementation should be carried out with a close eye on regulatory requirements.
- **Blockchain Literacy:** Learning blockchain technology requires a profound knowledge of various development, programming languages, and other tools. There are not enough blockchain developers, blockchain experts, and cryptography experts.
- **Risk of Cyberattacks:** Blockchain technology greatly reduces the risk of malicious intervention, but it's still not a panacea to all cyber threats. The blockchain also has its weak spots. If attackers manage to exploit any of these vulnerabilities, it may risk the security of the entire system.
- **Theft of Keys:** As secure as a blockchain may be, things can go badly if a cybercriminal manages to steal keys.
- **Interoperability:** Weak interoperability limits scalability. From the developer perspective, roadblocks can also be created from platform misconfiguration, communication mistrust, specification errors in application development, and cross-chain smart contract logic problems.
- **High Operating Costs:** Blockchain requires high computing power and storage capabilities. This leads to higher costs as compared to non-Blockchain applications.
- **Irreversibility:** There is a risk that encrypted data may be unrecoverable in case a user loses or forgets the private key necessary to decrypt it.

Some of these challenges are illustrated in Figure 7 [18]. In spite of the mixed feelings about blockchain and its challenges, many industries have invested millions in blockchain projects

CONCLUSION

Although blockchain is a relatively new technology, it seems to be revolutionary. With the maturity of the technology, blockchain will become far more seamless to adopt as the main guard against cyber threats. Blockchain security is the security measures that aid in keeping the blockchain network safe and the data stored on it away from unauthorized access, manipulation, and disruption. It is a complete risk management system for blockchain systems.

The adoption of blockchain technology is taking place at a fast pace. Its potential to enhance cybersecurity is significant. As the technology continues to evolve, it is likely to play an increasingly role in protecting against cyber threats. While it may not be the silver bullet to cybersecurity's problems, blockchain has great potential to help solve some of the many challenges the industry faces. More information about blockchain in cybersecurity can be found in the books in [19-27].

REFERENCES

1. P. J. Taylor et al., "A systematic literature review of blockchain cyber security," *Digital Communications and Networks*, vol. 6, no. 2, May 2020, pp.147-156.
2. M. N. O. Sadiku, Y. Wang, S. Cui, and S. M. Musa, "A primer on blockchain," *International Journal of Advances in Scientific Research and Engineering,* vol. 4, no. 2, February 2018, pp. 40-44.
3. M. J. Tuyisenge, "Blockchain technology security concerns: Literature review," https://www.diva-portal.org/smash/get/diva2:1571072/FULLTEXT01.pdf
4. E. Zamani, Y. He, and M. Phillips, "On the security risks of the blockchain," *Journal of Computer Information Systems*, vol. 60, no. 6, 2018, pp. 495-506.
5. S. Depolo, **"**Why you should care about blockchains: The non-financial uses of blockchain technology," March 2016, https://www.nesta.org.uk/blog/why-you-should-care-about-blockchains-non-financial-uses-blockchain-technology
6. O. Bheda, "What is blockchain?" https://builtin.com/blockchain
7. M. Iansiti and K. R. Lakhani, "The truth about blockchain," *Harvard Business Review*, Jan./Feb. 2017. https://hbr.org/2017/01/the-truth-about-blockchain
8. W. T. Tsai et al., "A system view of financial blockchains," *Proceedings of IEEE Symposium on Service-Oriented System Engineering*, 2016, pp. 450-457.
9. "Eliminating the complexity in cybersecurity with artificial intelligence," https://www.wipro.com/cybersecurity/eliminating-the-complexity-in-cybersecurity-with-artificial-intelligence/
10. M. N. O. Sadiku, S. Alam, S. M. Musa, and C. M. Akujuobi, "A primer on cybersecurity," International *Journal of Advances in Scientific Research and Engineering*, vol. 3, no. 8, Sept. 2017, pp. 71-74.
11. M. N. O. Sadiku, M. Tembely, and S. M. Musa, "Smart grid cybersecurity," *Journal of Multidisciplinary Engineering Science and Technology*, vol. 3, no. 9, September 2016, pp.5574-5576.
12. "FCC Small Biz Cyber Planning Guide," https://transition.fcc.gov/cyber/cyberplanner.pdf
13. R. Chintawar and M. Sampath, "Blockchain: The weapon for cybersecurity," March 2023, https://www.encora.com/insights/blockchain-the-weapon-for-cybersecurity#:~:text=Blockchain%20technology%20can%20be%20used,fraudulent%20activities%20through%20consensus%20mechanisms.
14. Y. Zhang, "Cybersecurity and reliability of electric power grids in an interdependent cyber-physical environment," Doctoral *Dissertation*, University of Toledo, 2015.
15. Blockchain for Cybersecurity: Pros and Cons, Trending Use Cases," February 2021, https://www.apriorit.com/dev-blog/462-blockchain-cybersecurity-pros-cons
16. N.L. Lincy and N. Kuriakose, "Cybersecurity aspects of blockchain," *International Journal of Creative Research Thoughts,* vol. 9, no. 5, May 2021, pp. 310-312.

17. "Blockchain security v/s cybersecurity: Answering the unanswered!"
January 31, 2023 https://www.immunebytes.com/blog/blockchain-security-vs-cybersecurity-answering-the-unanswered/

18. A. Banafa, "Second line of defense for cybersecurity: Blockchain," April 2018,
https://www.bbvaopenmind.com/en/technology/digital-world/second-line-of-defense-for-cybersecurity-blockchain/#:~:text=Using%20cryptography%20and%20the%20hashing,keys%20stored%20in%20the%20systems. 0000

19. R. Agrawal and N. Gupta (eds.), *Transforming Cybersecurity Solutions using Blockchain*. Springer, 2021.

20. R. Agrawal, R. Agrawal, and N.Gupta (eds.), *Blockchain Applications in Cybersecurity Solutions.* Bentham Science Publishers, 2023.

21. S. Mahankali, A. Bhattacharya, and G. B. Alex, *Secure Chains: Cybersecurity and Blockchain-powered Automation.* BPB PUBN, 2020

22. H. E. Poston, *Blockchain Security from the Bottom up: Securing and Preventing Attacks on Cryptocurrencies, Decentralized Applications, NFTs, and Smart Contracts.* Wiley, 2022.

23. U. P. Rao et al. (eds.), *Blockchain for Information Security and Privacy*. Auerbach Publications, 2021.

24. Y. Maleh et al. (eds.), *Blockchain for Cybersecurity and Privacy: Architectures, Challenges, and Applications.* Boca Raton, FL: CRC Press, 2020.

25. K. R. Choo, A. Dehghantanha, and R. M. Parizi (eds.), *Blockchain Cybersecurity, Trust and Privacy*. Springer, 2020

26. I. Romdhani, M. Alazab, and Y. Maleh (eds.), *Blockchain for Cybersecurity in Cyber-Physical Systems.* Springer, 2023.

27. R. Gupta, *Hands-On Cybersecurity with Blockchain:Implement DDoS Protection, PKI-based Identity, 2FA, and DNS Security Using Blockchain.* Packt Publishing, 2018.

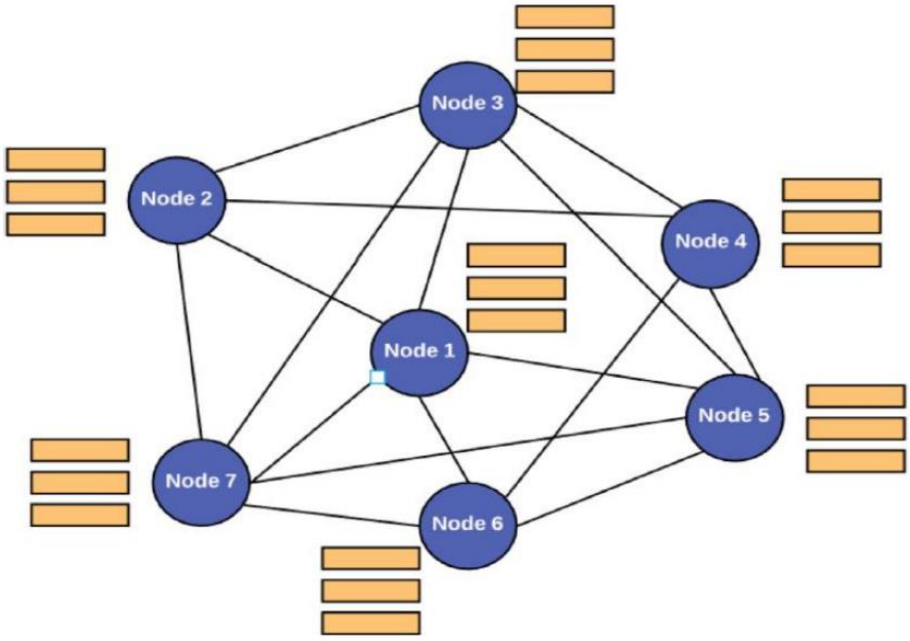

Figure 1 the blockchain architecture [3].

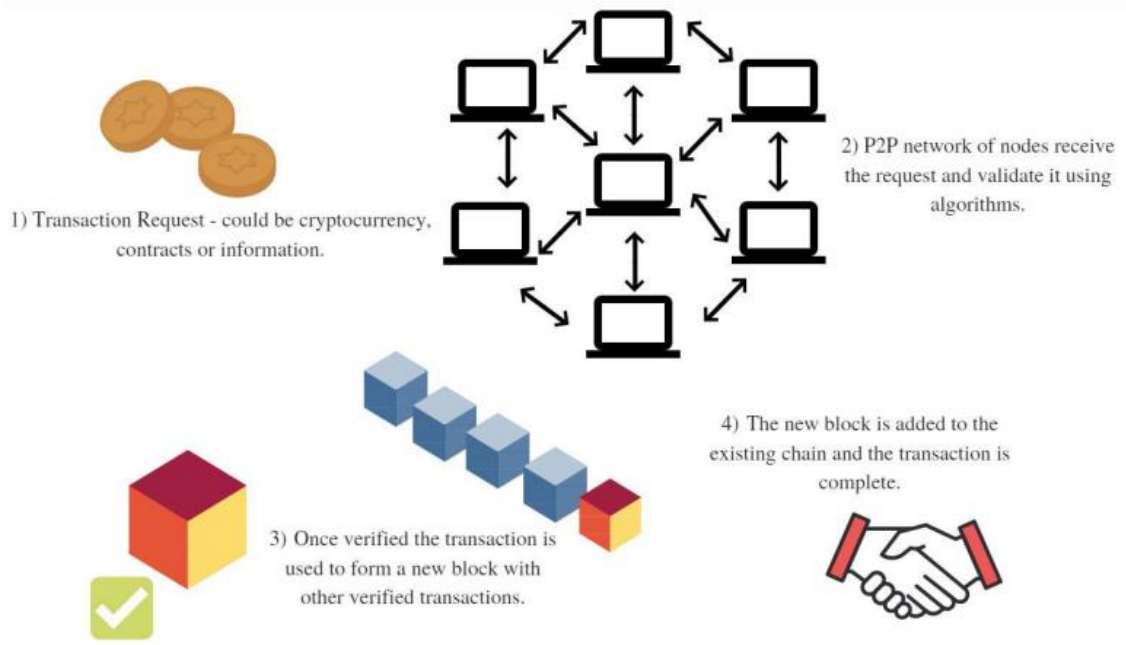

Figure 2 How the blockchain works [4].

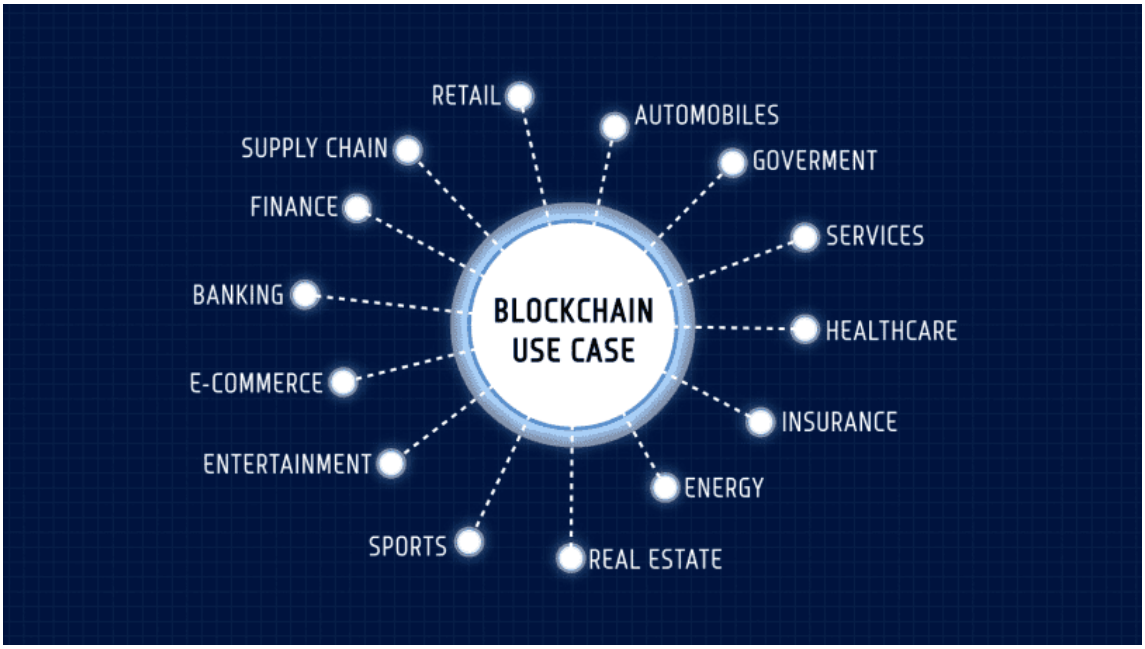

Figure 3 Different uses of blockchain [6].

Figure 4 Cybersecurity involves multiple issues related to people, process, and technology [9].

Figure 5 Common types of cyber attacks [13].

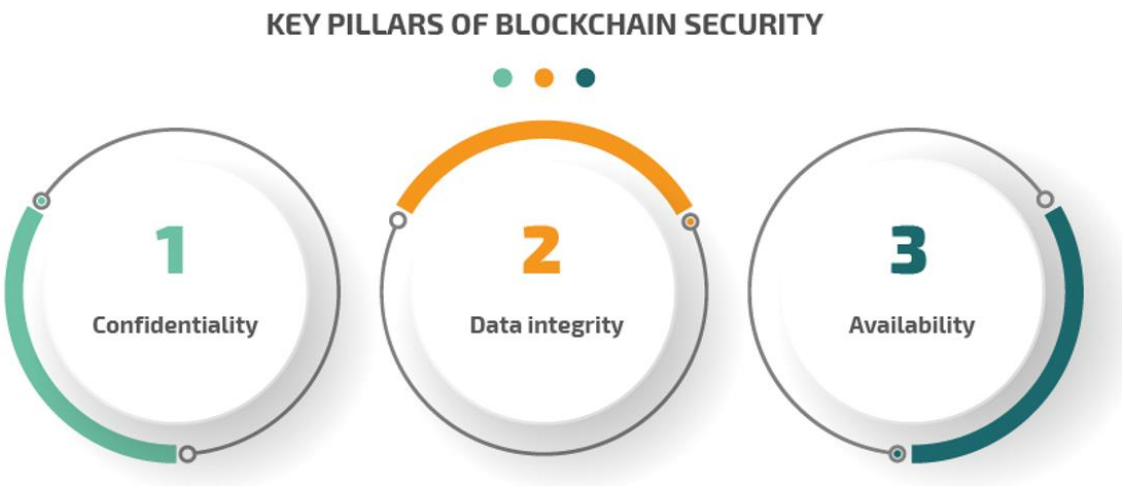

Figure 6 Three fundamental elements of blockchain security [15].

Figure 7 Some of these challenges of using blockchain in cybersecurity [18].