Middle East Research Journal of Engineering and Technology
ISSN: 2789-7737 (Print) ISSN: 2958-2059 (Online)
Frequency: Bi-Monthly
DOI: 10.36348/merjet.2023.v03i06.002

KUWAIT SCHOLARS PUBLISHER
Website: http://www.kspublisher.com/
Email: office@kspublisher.com

A Systematic Study about the Vulnerabilities and Security Enhancement in Block Chain Technology

Dr. Gurjeet Singh[1*]
[1]Professor, Department of Computer Application, CKD Institute of Management & Technology, Guru Arjun Nagar, Putligarh, Amritsar, Punjab 143001, India

Abstract: In this paper we undertake a methodical analysis of the Block Chain system's vulnerabilities and examine security upgrade strategies that could suggest future directions for investigation into Block Chain technology and its applications. Smart contracts are self-executing programs that store cryptocurrency valued at billions of SEK on second-generation block chains like Ethereum. Once they are put into place, they cannot be changed. Although smart contracts are typically thought to be secure objects, a new class of vulnerabilities that are more likely to be ethical aspects of programming than software coding flaws are revealed by a methodical examination of technology and source code.

Keywords: Blockchain, Ethereum, SEK, Attacks & Public Key.

Research Paper

***Corresponding Author:**
Dr. Gurjeet Singh
Professor, Department of Computer Application, CKD Institute of Management & Technology, Guru Arjun Nagar, Putligarh, Amritsar, Punjab 143001, India

How to cite this paper:
Gurjeet Singh (2023). A Systematic Study about the Vulnerabilities and Security Enhancement in Block Chain Technology. *Middle East Res J. Eng. Technol*, *3*(6): 90-95.

Article History:
| Submit: 23.10.2023 |
| Accepted: 24.11.2023 |
| Published: 30.11.2023 |

1. INTRODUCTION

The structure of blockchain, which consists of discrete records called blocks connected in a chain, gave rise to the name of the technology. Blockchain is a new technology that is going to revolutionize information sharing and acquisition. Anyone with an internet connection, wherever, at any time, can access this worldwide online database. It is not held by any central organization or body, such as banks or governments, like traditional databases. As a result, it becomes almost hard to hack or tamper with the entire system based on this technology by forging documents, transactions, or any other kind of information. Compared to typical financial transactions, all transactions based on this technology are faster and more secure. To establish a new and distinct database, blockchain technology integrates a wide range of different technologies, including cryptography, peer-to-peer networks, smart contracts, and consensus processes. Every transaction is also recorded with the time, date, participant information, and any other legally or contractually required information. The main technology underlying cryptocurrencies like Bitcoin and Ethereum is called blockchain, and it secures digital trade by storing transaction records in a distributed, time-stamped manner.

2. Types of Blockchain Technology

There are two main types of blockchain technology: private and public. However, there are also two further types of blockchain: hybrid and consortium or federated. The following is a brief overview of all forms of blockchain, as previously mentioned:

2.1 Public Blockchain:

These blockchains that are open to the public are known as public blockchains. "For the people, by the people, and of the people" (Sanjay & Nabi 2020) is the slogan of this particular kind of blockchain. A public blockchain is a distributed ledger technology that operates without permission and allows any node or end user to join and complete transactions. To access, read, write, and update the blockchain, they do not need to perform unique authentication (login with user ID and password). Cryptocurrencies like Bitcoin, Ethereum, and Litecoin, among others, use this technology.

2.2 Private Blockchain:

Permission-able or restricted blockchain technology that can only be used inside of a closed network is known as a private blockchain. Typically, this blockchain is utilized inside a company or organization, and only authorized users are able to access the network and conduct transactions. To access, read, write, and update data in the blockchain, users of this network must have a unique authentication or authorization (login with

user ID and password). Generally speaking, these blockchains are not as trusted as public blockchains. A private blockchain can be applied to supply chain management, digital identity, and voting, among other things.

2.3 Hybrid Blockchain:

A hybrid blockchain is made up of elements from both private and public blockchains. This blockchain makes use of both kinds of blockchain features. "A transaction in a private network of a hybrid blockchain is usually verified within the same network, but participants may also release it in the public blockchain to get verified." This blockchain can be easily deployed by an organization that prefers not to use either a public or private blockchain. For example: Dragonchain.

3. Applications of Blockchain

Blockchain technology can be applied anywhere that security, accuracy, trust, and transparency are required. Applications of blockchain technology are clearly visible in the public and government domains. Blockchain technology can help governments manage records more effectively. Governments maintain records of people's births and property transactions. The record can be made more secure with blockchain. Files stored on decentralized storage are shielded from loss or hacking. The advantages of blockchain technology have long been recognized by the financial industry. Cryptocurrency is the most widely used application of blockchain technology. Several sectors and industries are actively looking into the possibilities of implementing blockchain technology in their respective fields and domains. This article has covered the uses of blockchain technology in the financial services, public and government sectors, industry, healthcare, and Internet of Things (IoT).

3.1 Financial Applications:

Financial institutions such as banks are particularly vulnerable to identity theft, money laundering, and digital fund transfers. In terms of services provided and reputations, these institutions are severely impacted. Blockchain technology is already being used by banking institutions to address their conventional issues.

3.2 Blockchain Applications in Government:

Governments in many nations frequently encounter issues with land registry records. It's challenging to maintain ownership of hundreds of years' worth of land records. Land registry officials deal with the following issues: missing paperwork, forged documents, and inconsistencies in the paperwork. Blockchain technology offers a cost-effective solution to the aforementioned issues. Blockchain technology offers secure storage, unchangeable records, and safe access. Blockchain can be used by governments in the following areas:

- Record management for secure record-keeping of people.
- Identity management for proof of identity
- Government services like public safety and welfare
- Payment infrastructures to collect dues, taxes and other payments fast and
- Safe Smart property to digitally record assets

3.3 Blockchain Applications in Healthcare:

The number of healthcare record hacks has increased. In 2018, 1.4 million patient medical records from the UnityPoint Health hospital network in the United States were compromised. Sensitive data, such as the patient's social security number and insurance details, was contained in the compromised records. Data security and integrity are provided by blockchain technology. The main parties involved in healthcare are patients, healthcare providers (hospitals, physicians, lab technicians, etc.), data analysts, and insurance companies. Blockchain and distributed ledger technologies in healthcare ensure the confidentiality and security of patient information for all parties involved. Information exchanged between these parties doesn't jeopardize the integrity or security of the data.

3.4 Blockchain Applications in Industry:

In every industry, tracking the flow of products and services is essential. Visibility is crucial throughout the entire production process, whether it be for the movement of raw materials or finished products. Efficient tracking of the movements of goods and services can be facilitated by blockchain technology. Blockchain technology is available to address business concerns in nearly every aspect of business operations, including supply chain management, operations management, customer relationship management, and purchase management.

3.5 Blockchain Application in the Internet of Things (IoT):

Smart devices communicate with one another over the internet in Internet of Things applications. The security of the data produced by these smart devices in distributed wireless networks is the main source of concern. Blockchain will handle the security of data produced by smart devices because it is a distributed public ledger.

4. Challenges of Blockchain

Blockchain offers many advantages, but it also has certain technical drawbacks. Here, we've covered issues with energy, selfish mining, privacy loss, and scalability.

4.1 Scalability:

As the volume of transactions rises, the blockchain network continues to expand daily. The system is being burdened by the growing blockchain network's data and resource sharing. Nodes will take

longer to synchronize data and complete the intricate computation as a result. thereby influencing the blockchain system's ability to function effectively. These problems can be solved by blockchain redesign and storage optimization.

4.2 Loss of Privacy:

The blockchain maintains a significant level of privacy by anonymizing user identities through the use of public key cryptography in transactions. However, because the identities of all transactions and the balances for each cryptographic key are available to the public, blockchain cannot guarantee transactional anonymity. The user can therefore be identified by monitoring the transactions.

4.3 Selfish Mining:

The process of creating new blocks on the Bitcoin blockchain is known as mining, and the nodes that carry out this work are known as miners. Selfish Mining is a tactic used by overly ambitious miners to retain their blocks privately and not share them. Only after a few requirements were met would it be made public.

4.4 High Energy Consumption:

The consensus mechanism used by the blockchain network is called Proof of Work, or PoW. Computing power and energy are needed in large quantities to determine a block's required hash value.

5. Impact of Blochchain Technology

Blockchain technology is having an impact on businesses. The effects could show up in a variety of ways. The business environment or business models could be the cause. The current business models might alter or change in light of the evolving demands of the market. This article has covered a few of the blockchain's effects on the financial and non-financial sectors.

5.1 Impact of Blockchain Technology in Financial Sector:

The introduction of blockchain technology can have the greatest impact on transactions that occur in the financial sector, such as banking. In the financial industry, transactions are typically conducted through a third party that is trusted. For all parties involved, this role of a third party is the primary cause for concern. Blockchain technology can eliminate this trusted third party in the financial sector, including banking. Because the typical banking system's architecture is built on a centralized server/clients model, a copy of the database is only centralized at the server level. Peer-to-peer network models will be present when blockchain technology-based systems are implemented in the banking sector, guaranteeing multiple copies.

5.2 Impact of Blockchain Technology Application in Supply Chain:

The management of the complete production flow of goods or services is known as supply chain management, or SCM. SCM considers everything from raw material handling and processing to consumer delivery of completed goods. The five main elements of SCM are as follows.

- Planning
- Sourcing
- Manufacturing
- Delivery and logistics
- Returning

6. Security Attacks in Block Chain

Since there is no single point of failure like in a client-server model, blockchain technology, which implements the peer-to-peer computing model, has greater security overall but less central control. This is because data is encrypted, making it more difficult to compromise the integrity or confidentiality of the data or penetrate the system. As for apps, there is generally no privacy because they are visible.

6.1 Distributed Denial of Service attack:

Distributed denial of service (DDoS) attacks usually target the mining pool that supplies the processing power needed to mine the blocks. The majority of mining pool providers lack defense against DDoS attacks. DDoS attacks always target trading platforms, or cryptocurrency exchanges, in addition to mining pools.

6.2 Data integrity:

Data integrity is crucial to communication, and the blockchain environment is no exception. Data must not have been altered in any way during the transmission or verification process. When a malleability attack takes place, a cryptocurrency transaction may be intercepted, modified, and rebroadcast, leading the issuer to believe that the transaction has been lost or is not verified by the service providers.

6.3 Endpoint Vulnerabilities:

The intersection of humans and blockchains is known as the end point in the blockchain; to put it another way, any individual or organization can use a computer to access blockchain services. This is actually one of the most crucial points to take into account when discussing blockchain security. The area of blockchain remains between the sender and recipient computers with the information, so any blockchain-based service—whether it be a financial institution, public or community organization, or a financial transaction in the form of a cryptocurrency exchange—that processes data is particularly vulnerable during this time because it involves shared ledgers and credentials. Because of user weakness and blockchain limitations, this is the weakest point where credentials are exposed.

6.4 Vendor Risks:

Without the fundamental components of a distributed ledger transactions in, out, and balance blockchain is worthless. As more communities and organizations embrace blockchain technology, more third-party applications will be implemented over time within the blockchain ecosystem. The need for more contemporary programs, features, and applications led to an increase in third-party vendors creating various software for various points of execution, such as:

- Client software (Wallet)
- Payment processing modules
- Smart contracts
- Blockchain payment platforms
- Integration platforms
- Cryptocurrency exchanges
- Dapps for Ecommerce

When implementing solutions developed by third parties, organizations should be mindful of the serious risks associated with malware, malfunctioning codes, and intentionally fraudulent codes that reveal sensitive information to unapproved parties.

7. Public and Private Key Security

In order to establish a connection and gain access to the blockchain, an individual must authenticate themselves using their public and private keys. These keys function similarly to a user name and password in terms of behavior, but they are structurally distinct because they are composed of long, cryptic strings of characters and numbers that are nearly impossible for both computers and humans to decipher. The blockchain's combination of private and public keys is its greatest strength because, in the wrong hands, hackers cannot ever access the data. On the other hand, this combination is also its greatest weakness because, with these keys, hackers can manipulate the game to the point where even authorized users can't play it. Hackers never waste time attempting to guess these keys; instead, they use malware, trojans, social engineering techniques, key loggers, or other malicious software. As a result, weak points on computers and mobile devices are always the target.

7.1 Lack of Standards and Regulation:

The terms blockchain and miners are therefore frequently used interchangeably. Decentralized cryptocurrencies have quickly gained popularity and are frequently cited as the next generation of financial technology based on the decentralized infrastructure of blockchain. Therefore, it is not possible to do away with the need to introduce new technical and legal standards in order to address security concerns. As cryptocurrencies are typically not owned by any legitimate institution, they lack the regulatory oversight of any particular region, nation, or business, setting them apart from other financial institutions and wealth-issuing organizations.

7.2 Vulnerabilities of Smart Contracts:

Although the underlying technology of BlockChain is secure, there are certain limitations and weaknesses. Vulnerabilities in smart contracts arise from the codes that create them, and these might be deliberate errors by developers or the result of poorly written code. By taking advantage of flaws in the smart contract code, anonymous hackers made over 500 million SEK in June 2016. A well-known Ethereum wallet was breached in July 2017 due to an additional code bug that was used, with estimated damages exceeding 300 million SEK. The introduction of the ability to transfer cryptocurrency to anonymous accounts has made it more alluring for hackers to devote time and resources to uncovering weaknesses in smart contracts. If they are successful, they stand to earn a substantial incentive.

8. Blockchain Protocols

Blockchain protocols are the set of guidelines that control a blockchain network. In essence, blockchain protocols are the standard communication guidelines that the network adheres to. Among these guidelines are the following:

- Rules for governing and validating transactions
- Application programming interface (API)
- An algorithm that defines the mechanism for all participating nodes to interact with each other

8.1 Bitcoin: The Bitcoin protocol facilitates cryptocurrency transactions across a dispersed network.

8.1.1 Characteristics of Bitcoin Protocol:

i. Every node has access to complete information on the blockchain. Therefore, it is a decentralized one.
ii. Users can conduct a nonreversible transaction without the need to explicitly trust a third party.

8.1.2 Advantages of Bitcoins:

- Payment freedom
- Control and Security
- Very low fees

8.2 Ethereum:

Ethereum is an open-source, publicly accessible blockchain protocol. The Ethereum platform makes smart contract usage possible. The concept that blockchain technology can be applied to uses other than cryptocurrency was first widely accepted by Ethereum.

8.2.1 Characteristics of Ethereum Protocol:

- This protocol enables developers to build and deploy distributed applications
- It allows users to write their own applications

8.2.2 Advantages of Ethereum Protocol

- The uptime of the network is high
- The energy efficiency is high with the help of Proof of Stakes (PoS)

8.3 Hyperledger:

An open-source blockchain platform is called Hyperledger. It supports cross-industry blockchain technologies as well as distributed ledgers based on blockchain. The primary use of the Hyperledger protocol is for business transactions. The issue of blockchain enterprise approval is resolved with Hyperledger. Only reliable parties are allowed to connect to the Hyperledger network and validate transactions.

8.3.1 Characteristics of Hyperledger Protocol:

- Hyperledger blockchain technology is mostly used for business applications
- It has a modular and versatile design
- It preserves privacy

8.4 Ripple:

An open source blockchain platform is called Ripple. For financial transactions, Ripple functions as a digital payment network in addition to a cryptocurrency.

8.4.1 Characteristics of Ripple Protocol:

- Ripple protocol is known for its digital payment network
- Ripple transactions are confirmed in seconds
- It has its own cryptocurrency XRP (digital asset Ripple)
- Ripple transactions use less energy than bitcoin.

8.5 R3's Corda

Uses for the open-source Corda blockchain protocol include digital assets, trade finance, insurance, healthcare, and financial services. This protocol was released to manage, organize, and keep track of financial agreements.

8.5.1 Characteristics of Corda:

- Corda allows businesses to transact securely and seamlessly
- This protocol organizes the business operation

8.5.2 Benefits of Corda:

- Privacy
- Interoperability
- Agile and flexible
- Open design
- Open development

9. RESULTS

These are some conclusions drawn from the body of research on blockchain technology, its financial implications, and its applications that is currently housed in various databases. The first publications on the subject of blockchain can be traced back to the beginning of 2008. Over the following three years, researchers continued to concentrate on publications that were more closely related to cryptocurrency. Approximately 400 white papers and research articles from this period were available in databases until 2011, after which there was a sharp increase in the amount of literature published after 2012. Even though bitcoin is a product (application) and a component of the blockchain system, the number of publications on bitcoin by itself more than doubles that of its underlying core technology. Regardless of whether they were written for the bitcoin blockchain or the cryptocurrency itself, research papers have generally focused on the business and financial aspects of cryptocurrencies. Early blockchain-based publications were mistaken for bitcoin (a cryptocurrency), but more recent writing has focused more on the technical aspects of blockchain technology, including its application, architecture, potential, and future prospects. Even though many researchers address security-related topics, in-depth research on technology is still needed rather than broad overviews.

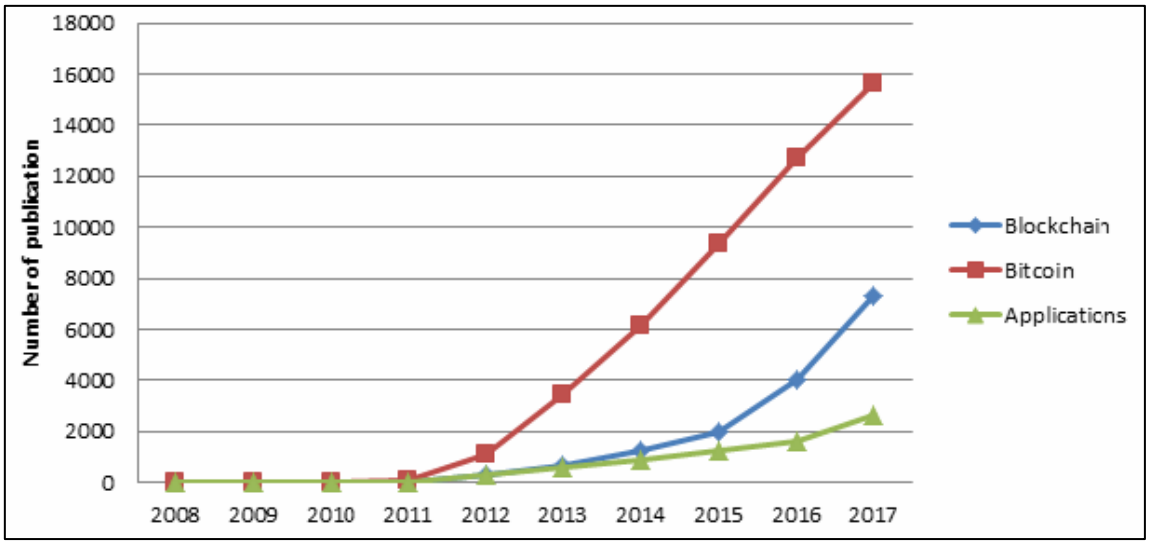

Figure 1.1: Literature Available

9.1 Untested Code

Although it is theoretically and practically possible to go through the code for verification to make sure it does the same job it was made for, one of the biggest concerns about Ethereum smart contracts is that it is difficult for the average user to check and analyze whether there isn't a hidden bug or secret piece of code that facilitates the smart contract developer to run away with some assets. The aforementioned criteria may apply to both customized and widely used distributed applications. Many applications use hundreds of thousands of smart contracts today, and as time goes on, the number of these codes gradually grows. Regretfully, conventional code analysis tools frequently fall short when attempting to analyze an application, particularly one involving smart contracts. They are effective in changing or reversing the formal terms of the contracts and cause further problems when the matter is investigated and prosecuted in court. Numerous frameworks and tools for identifying bugs in source codes are currently under development, and numerous other tools are already built to write secure smart contracts. We examined dozens of real-world source codes that are accessible as open source smart contracts on github, and the findings were unexpected.

10. CONCLUSION

This paper aims to demonstrate that open source smart contracts are not as safe as they seem, despite their widespread distribution on the internet, in electronic media, and in discussion forums. With the introduction of blockchain technology, Bitcoin has emerged as the leader in cryptocurrency, and its blockchain remains the foundation of the bitcoin ecosystem. However, Ethereum, a relatively new blockchain platform, has changed the game with its application layer capabilities for creating distributed applications and smart contracts. Smart contracts are unchangeable, self-executing programs that cannot be changed once they are implemented on the network. It offer quick and unstoppable execution, but if the flawed, incomplete, and vulnerable code was used just once, it might still be vulnerable and a target for hackers. Before the DAO attack sparked a fresh debate about smart contract security and attracted the attention of researchers, the blockchain community was experiencing a peak in the hype surrounding smart contracts' ultimate security. This paper aimed to draw attention to the vulnerabilities present in smart contracts, as well as to the element of cybercrime and its associated forensics aspect, which takes the form of deliberate frauds involving flawed software development.

REFERENCES

- Czepluch, J. S., Lollike, N. Z., & Malone, S. O. (2015). The use of block chain technology in different application domains, in: The IT University of Copenhagen, Copenhagen.
- Sompolinsky, Y., Lewenberg, Y., & Zohar, A. (2016). Spectre: a fast and scalable cryptocurrency protocol, IACR Cryptol. *ePrint Arch*, 1159.
- Juels, A., Kosba, A., & Shi, E. (2016). The ring of gyges: Investigating the future of criminal smart contracts, in: The ACM SIGSAC Conference on Computer and Communications Security.
- Zhang, F., Cecchetti, E., Croman, K., Juels, A., & Shi, E. (2016). Town crier: An authenticated data feed for smart contracts, in: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security.
- Fu, D., & Fang, L. (2016). Blockchain-based trusted computing in social network, in Proceedings of the 2016 2nd IEEE International Conference on Computer and Communications (ICCC), pp. 19–22, IEEE, Chengdu, China.
- Miller, A., M¨oser, M., Lee, K., & Narayanan, A. (2017). An empirical analysis of linkability in the monero blockchain, in: arXiv preprint: 1704.04299.
- Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking bitcoin: Routing attacks on cryptocurrencies, in: IEEE Symposium on Security and Privacy.
- Bui, T., Rao, S. P., Antikainen, M., & Aura, T. (2019). Pitfalls of open architecture: how friends can exploit your cryptocurrency wallet, in Proceedings of the 12th European Workshop on Systems Security, pp. 1–6, Dresden Germany.
- Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. (2019). A systematic literature review of blockchain cyber security. Digital Communications and Networks.
- He, D., Li, S., Li, C., Zhu, S., Chan, S., Min, W., & Guizani, N. (2020). Security analysis of cryptocurrency wallets in android-based applications. *IEEE Network*, *34*(6), 114-119.
- Su, Y., Jiang, X., & Lin, Z. (2021). Simulation and relationship strength: characteristics of knowledge flows among subjects in a regional innovation system. *Science, Technology and Society*, *26*(3), 459-481.
- Lu, S., Li, S., Zhou, W., & Yang, W. (2022). Network herding of energy funds in the post-Carbon-Peak Policy era: Does it benefit profitability and stability?. *Energy Economics*, *109*, 105948.