Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 4-A, pp. 1031–1043
DOI : 10.47974/JIOS-1889

VAiBT : Vulnerability assessment in blockchain technology

Siya Garg [§]
Department of Computer Science
Faculty of Mathematical Sciences
University of Delhi
Delhi 110007
India

Vinita Jindal [†]
Department of Computer Science
Keshav Mahavidyalaya
University of Delhi
Delhi 110034
India

Rahul Johari *
University School of Information, Communication and Technology
Guru Gobind Singh Indraprastha University
Sector 16C, Dwarka
Delhi 110078
India

Deo Prakash Vidyarthi [‡]
Parallel and Distributed System Lab
School of Computer and Systems Sciences
Jawaharlal Nehru University
Delhi 110067
India

[§] *ORCID-ID:* 0000-0001-8117-7999
[†] *ORCID-ID:* 0000-0002-0481-4840
* *ORCID-ID:* 0000-0002-7675-8550
[‡] *ORCID-ID:* 0000-0003-4151-0552

[§] *E-mail:* gargsiya90@gmail.com
[†] *E-mail:* vjindal@keshav.du.ac.in
* *E-mail:* rahul@ipu.ac.in [Corresponding Author]
[‡] *E-mail:* dpv@mail.jnu.ac.in

Veenu Bhasin [@]
Department of Computer Science
P. G. D. A. V. College
University of Delhi
Delhi 110065
India

Abstract

A Blockchain is a sequence of data blocks, each cryptographically linked to the previous one, ensuring that once a block is added, it cannot be altered. Many security experts consider the inherent cryptographic features of Blockchain technology robust enough to counteract hacking attempts and security threats. However, research into the security and privacy of Blockchain has revealed that numerous applications have been successfully targeted by cyberattacks. In this paper, a sincere effort has been made to perform **'VAiBT: V**ulnerability **A**ssessment in **B**lockChain **T**echnology', which explores various vulnerabilities in Blockchain technology. A comparative analysis is conducted through simulations using the Java programming language on a set of three (03) credit cards. The findings have been positive and promising.

Subject Classification: *68P25 Data encryption, 68M12 Network protocols.*

Keywords: *Network security, BlockChain, Cryptography, Vulnerability.*

1. Introduction

Satoshi Nakamoto created Blockchain technology, which was introduced in a 2008 white paper by the designer of Bitcoin. This technology removed the need for a third party, such as a financial institution, by creating a "peer-to-peer" online cash system [Figure1]. Blockchain offers advantages such as transparency, authenticity, and auditability because it eliminates the necessity of a trusted intermediary between parties involved in a transaction. Blockchain is a robust, dynamic, and scalable technology. Today, it is considered one of the safest, most reliable, and secure (SRS) technologies, largely due to its use of hashing. Popular hash-based algorithms like SHA (Secure Hash Algorithm) and MD5 (Message Digest 5) and are commonly employed in Blockchain technology.

Security experts typically face two main choices: (i) use predefined hashing algorithms to generate the hash values of input data or (ii) create and implement custom hashing techniques for faster access by stakeholders.

[@] *ORCID-ID:* `0000-0002-8567-4519`

[@] *E-mail:* `veenu.bhasin@pgdav.du.ac.in`

The security of the data within Blockchain blocks remains a concern. Various cryptographic cipher techniques, such as Caesar Cipher, Vigenère Cipher, Hill Climbing Cipher, and Rail Fence Cipher, are effective in generating ciphertext. However, there are limited hashing techniques available for generating hash values or digests.

Blockchain technology is being investigated for numerous innovative uses, spanning areas such as cryptocurrencies, smart contracts, communication systems, healthcare, the Internet of Things (IoT), financial services, censorship resistance, the HoReCa (**H**otel, **R**estaurant, **Ca**fé, and **Ca**tering) sector, electronic voting, and more. While Blockchain offers numerous advantages to these fields, its security vulnerabilities could be exploited by malicious actors. Several high-profile Blockchain security breaches have made headlines, highlighting the potential risks. Analyzing these incidents can provide valuable insights into the security challenges within Blockchain technology.

Exploited Code - This incident exposed significant privacy and security vulnerabilities within the Decentralized Autonomous Organization (DAO) Blockchain.While programmers were addressing a systemic code malfunction, an unidentified attacker exploited the vulnerability to siphon off the Ether accumulated from the sale of DAO tokens. In just a few hours, over $60 million worth of Ether was stolen. This event underscored the inherent fragility of the Blockchain system, highlighting its susceptibility to exploitation.

Missing Keys - There have been several cases of Bitcoin theft, with one prominent incident involving the Hong Kong-based cryptocurrency exchange Bitfinex. In this incident, approximately $72 million worth of Bitcoin was stolen. The likely cause was the compromise of private keys or personal digital signatures, highlighting vulnerabilities in the security infrastructure.

Hacking Employee System - Bithumb, South Korea's largest cryptocurrency exchanges for Bitcoin and Ethereum, fell victim to Blockchain security vulnerabilities. Hackers managed to steal $32 million in Bitcoin and obtained the personal information of roughly 30,000 individuals. This event emphasizes the importance of gaining a deep understanding of the factors that affect Blockchain security.

2. Threats, Vulnerabilities and Attacks in BlockChain Domain

2.1 *Vulnerabilities in MD5*

- Collision vulnerabilities
- Preimage vulnerability

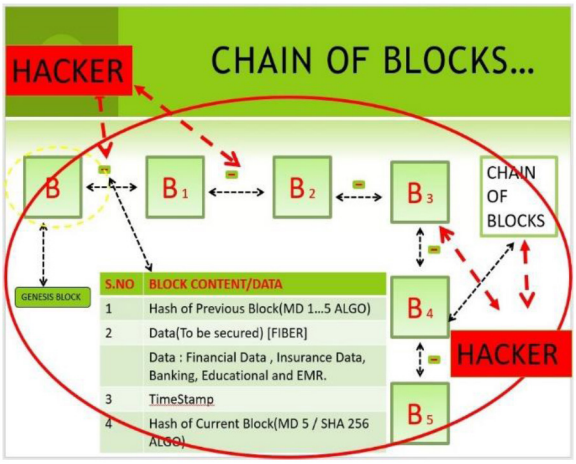

Figure 1

Chain of Blocks

Some of the BlockChain security vulnerabilities and issues are as follows:

1. **51% Attacks :** This type of attack occurs when a miner or a group of miners control over 51 percent of the mining power on the Blockchain network. With majority control, they can block new transactions from being confirmed, prevent payments between certain or all users, and reverse transactions that were previously confirmed. While being in control of the network, they could easily double-spend coins. At least five cryptocurrencies have previously been subjected to 51% attacks: Verge, ZenCash, Monacoin, Bitcoin Gold, and Litecoin Cash. Cybercriminals amassed sufficient hashing power in each of these instances to hack the network and steal millions of dollars. One needs to put in place proper control measures to prevent 51% attacks. For instance, observing transactions that are received within a listening period, forwarding double-spending attempts, adding more nodes to witness transactions, and refusing direct incoming connections.
2. **Routing Attacks** Although a Blockchain node can technically operate anywhere on Earth, the current distribution of nodes across

the globe is far from uniform. Blockchain networks and applications rely heavily on real-time data transfers, making them vulnerable to interception during transmission to internet service providers. For example, an attacker could execute routing attacks, splitting the network into two or more disconnected components. This results in the creation of parallel Blockchains by blocking communication between nodes within one component and those in other components. Any blocks mined within the isolated component, along with the related transactions and miners' earnings, become invalid once the attack ends.

Thus, routing attacks pose a significant threat, capable of causing considerable damage before detection.

3. **BlockChain Endpoint Vulnerabilities** These are important because when and where they might arise, is not known. Most frequently, it occurs whenever humans and BlockChains encounter. Essentially, an endpoint could be any place where a person accesses any kind of data. Most hackers focus on stealing keys, knowing that attempting to guess an end user's password is largely ineffective. By targeting the system's weakest link, usually a computer or mobile device, they maximize their chances of obtaining the keys. It is crucial to remember that endpoints are particularly vulnerable because they are used to access BlockChain to receive data. Every endpoint in a system gives a malicious attacker the chance to enter or exit a malicious code. The only distinction is that some are difficult to crack while others are not. Once a device has been compromised, hackers can take advantage of frequent users' credentials to damage the network.

3. **Vendor Risks** The security risks associated with faulty and exposed vendors are frequently unknown to enterprises intending to implement third-party BlockChain apps and platforms. Vendor solutions typically have a narrow focus on security controls, defective code, and even personnel vulnerabilities that make it simple for unauthorized users to obtain their clients' BlockChain credentials. Products that use Smart Contracts are particularly susceptible to this vulnerability. A vulnerability of this kind could cause substantial damage, as an organization's entire operations and policies might be stored as a Smart Contract on a Blockchain.

4. **Transaction Privacy Leakage** Transactions in public Blockchain networks are inherently transparent and traceable due to their

architecture. The dissemination of transaction data across the network ensures synchronization and allows distributed nodes to reach consensus. However, transactions often include sensitive information about their issuers, raising significant privacy concerns. Privacy leakage in transactions can have severe consequences, particularly in Blockchain applications like the Internet of Things or mobile crowdsourcing.The disclosure of transaction details and the analysis of transaction graphs can indirectly compromise privacy by revealing relationships between different transaction addresses. This association may also expose the user's identity if additional data is obtained from external sources. To mitigate transaction privacy leakage, one commonly used method is employing a mixing service. This service enables simultaneous transactions with different inputs and outputs, ensuring that the input of a transaction cannot be directly linked to its corresponding output.

5. **Phishing Attacks** Phishing is one of the most common baiting techniques employed by hackers to deceive individuals into sharing their credentials. In phishing attacks, hackers impersonate trusted sources to send emails to wallet key owners, often using misleading URLs to request sensitive information. Once hackers obtain these credentials, both users and the Blockchain network become vulnerable to further attacks. A notable example occurred in 2018 with an attack on IOTA wallets using the fraudulent online seed generator iotaseed.io. Hackers launched a phishing campaign through this service, collecting hidden seeds from unsuspecting users. As a result, in January 2018, more than $4 million worth of IOTA was stolen from victims' wallets. In 2020 alone, approximately 100,000 phishing incidents were reported.

To prevent such attacks, educating wallet owners and key stakeholders about countermeasures is essential. Product designers also bear the responsibility of integrating security measures from the very beginning, as Blockchain-based solutions, while offering exceptional security and transparency, remain susceptible to vulnerabilities. Awareness of Blockchain security vulnerabilities is crucial for building more secure networks and systems. Moreover, advancements in technology, such as AI-powered tools for code analysis, transaction monitoring, and infrastructure security, can pave the way for new trends and robust security measures in Blockchain technology.

3. Literature Survey

BlockChain is a game-changing technology with numerous advantages over traditional approaches to record-keeping, transactions etc. However, like other technologies, it is also vulnerable to security threats and attacks, making it critical to examine these risks. One such study was undertaken by the authors in [1][2], who assessed many BlockChain-based security vulnerabilities, discussed their ramifications, and proposed strategies to mitigate these threats. Authors in [3] developed a cybersecurity vulnerability mitigation framework through empirical paradigm (CyFEr) to address multi-criteria decision analysis (MCDA) problems and improve cybersecurity vulnerability assessments using rank-weight methods. The BlockChain Cybersecurity Framework (BC2F) was used to conduct the evaluation, which revealed cybersecurity flaws and weaknesses that must be addressed to ensure cyber secure transactions. The Master Node Based Clustering (MNBC) protocol, introduced in [4], seeks to address the problem of propagation delays in the Bitcoin network. By addressing this delay, the MNBC protocol helps prevent issues such as double-spending attacks. In [5] the authors provided a case study on a login authentication system developed using BlockChain to prevent data leaks. After careful consideration, the authors propose that a BlockChain-based login authentication system might safeguard data to a degree of 90.1 percent. The processes in the Network Forensic Life Cycle (NFDLC) framework are implemented because of the simplicity. To explore this, the authors of [6] proposed two risk assessment models: Quantitative and Qualitative, which organizations can use for risk analysis. Each model offers its own advantages and disadvantages, but both provide valuable insights for risk assessment. The authors of [7] claim that the corporate BlockChain system can withstand attacks on both transmitted and stored data because it eliminates the need for tokens by encrypting all transactions using electronic signatures and timestamps. In its first, authors in [8] did a complete assessment of the BlockChain threats in IoT networks. They reviewed the security threats, vulnerabilities, and difficulties associated with BlockChain technology. The potential security solutions that could be used to deal with these issues are also provided. With the growing popularity of BlockChain technology, it's more important than ever to consider the associated security problems. One such problem, Black Bird Attack (BBA), has been described in [9]. This BBA structured 51 percent hash rate attack in BlockChain systems, is a real prospect and should be taken seriously.

The authors of [10] gave a thorough explanation of BlockChain and the security risks it poses. Starting with a comparison of the six most widely used consensus algorithms (PoW, PoS, DPoS, PoET, PBFT, and DAG), smart contracts to various cryptographic techniques and hash functions employed in the BlockChain. The authors of this paper also provided a thorough analysis of network attacks, end-point attacks, code vulnerabilities, and other similar security concerns attached to the BlockChain.

The authors of [11] attempted to leverage Smart Contract by designing, developing, and deploying an advanced Smart Contract System. This system involved interactions between the customer, car dealer, and car manufacturer. It is planned to be replicated and thoroughly tested in the future to identify potential vulnerabilities. In [12], the author(s) examine Non-Fungible Tokens (NFTs) within the domain of Blockchain Technology. NFTs are frequently used to symbolize digital assets and provide evidence of ownership. The work conducted by the author(s) is set to be extended to investigate potential threats and vulnerabilities associated with Blockchain technology, with plans to explore ways of exploiting these vulnerabilities.

4. Methodology Adopted

BlockChain is stated to be very secure. However, it can be compromised due to some faults in the hashing techniques. Hashing techniques such as Message Digest (MD), Secure Hashing Algorithms (SHA) are used to build BlockChain and possess some vulnerabilities which can be compromised. In the proposed approach[figure 2], effort has been made to propose a algorithm, designed to create a BlockChain and operate on the Credit Card Number, elaborated as follows:

4.1 *Algorithm*

Trigger

1: User Input Credit Card Number

2: Fetch $\mathbf{C_n}$, $\mathbf{C_{vn}}$, 6-digit $\mathbf{E_c}$

3: $T\,\mathrm{d} \leftarrow C_{\,\mathrm{n}} + C_{\,\mathrm{vn}} + E_{\,\mathrm{c}}$

4: Split T_d into 5 symmetric B

, if need arises, do padding 5: $B \leftarrow B\,\mathrm{d1} + B\,\mathrm{d2} + B\,\mathrm{d3} + B\,\mathrm{d4} + B\,\mathrm{d5}$

6: Generate Hash Values (H_v)

7: C h $\leftarrow H$ (B d1) + H (B d2) + H (B d3) + H (B d4) + H (B d5) where H ϵM D 5 | | SH A

8: Generate $\mathbf{G_b}$

9: Generate New Block:

$$\sum_{i=1}^{5} B_D (B_d + P_h + C_h + T_s)$$

In the proposed algorithm, end user is first prompted to enter Credit Card Number (16 digit long) [CCN], Credit Card Verification Value number (3 digit long) [CVV] and the Expiry Date (6 digit long) [ED] of the credit card. All the number (16+3+6) are concatenated to create a 25 digit long. Once done, the 25-digit long credit card number is partitioned into 5 uniform, symmetric and equally sized blocks which are then hashed using the Message Digest (MD) 5 Algorithm.

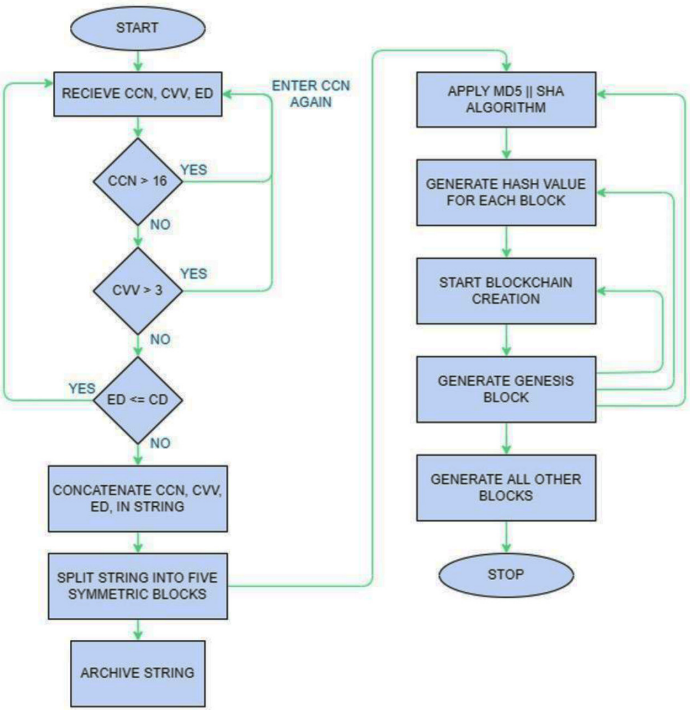

Figure 2

Flowchart of the VAiBT Framework

5. Experimental Setup

A Java code is written to simulate a basic BlockChain which uses MD5 algorithm to hash the data. For the benefit of readers, the Sample Program Code Snippet is shared on the GitHub Profile [13]

6. Result

When the BlockChain works fine and there is no problem with the hashing techniques we can see the following output. Here the credit card number was given as input:

Input 1234567890123456 117 062023
Card number: 1234567890123456
CVV: 117
Expiry Date: 062023
Concatenated letters: 25 digit Card details are not valid
java.lang.ArithmeticException: not valid
Execution Time in nanoseconds: 542400

Input 1358954993914435 657 042025
Card number: 1358954993914435
CVV: 657
Expiry Date: 042025
Concatenated letters: 25 digit Card details are valid
Chaining, first block Credit Card
Result: Success
Contents of Block are 135801630062596149[B@27bc2616
Chaining, second block Credit Card...
Result: Success
Contents of Block are 5499[B@27bc2616130062596172[B@3941a79c
Chaining, third block Credit Card...
Result: Success
Contents of Block are 9144[B@3941a79c1630062596173[B@506e1b77
Chaining, fourth block Credit Card...
Result: Success
Contents of Block are 5657[B@506e1b771630062596173[B@4fca772d
Chaining, fifth block Credit Card...
Result: Success
Contents of Block are 4202[B@4fca772d1630062596173[B@9807454
Execution Time in nanoseconds: 24555000

Figure 2 and 3 shows the difference in the hash values, when MD5(Message Digest)5 and SHA (Secure Hash Algorithm) are applied. Graph in Figure 4 presents execution time comparison of 03 credit cards.

Block Contents	Hashed block after applying MD5 algorithm for security in Blockchain
Hashed Contents of 1st Block	1358 0 1649943919911 [B@7d417077
Hashed Contents of 2nd Block	5499 [B@7d417077 1649943919990 [B@60f82f98
Hashed Contents of 3rd Block	9144 [B@60f82f98 1649943919990 [B@35f983a6
Hashed Contents of 4th Block	5657 [B@35f983a6 1649943919990 [B@7f690630
Hashed Contents of 5th Block	4202 [B@7f690630 1649943919990 [B@edf4efb

Figure 2: Blockwise hashed Content obtained by applying MD 5 Algorithm

Block Contents	Hashed block after applying SHA-256 algorithm for security in Blockchain
Hashed Contents of 1st Block	1358 0 1649944469882 [B@7dc36524
Hashed Contents of 2nd Block	5499 [B@7dc36524 1649944469924 [B@35f983a6
Hashed Contents of 3rd Block	9144 [B@35f983a6 1649944469925 [B@7f690630
Hashed Contents of 4th Block	5657 [B@7f690630 1649944469926 [B@edf4efb
Hashed Contents of 5th Block	4202 [B@edf4efb 1649944469926 [B@2f7a2457

Figure 3: Blockwise hashed Content obtained by applying SHA Algorithm

Figure 3

Comparative difference between Hashed Contents obtained after applying MD 5 and SHA Algorithm

Figure 4

Execution Time Comparison of 3 Credit Cards

7. Conclusion

In the current research work, the case study, of creation of the BlockChain using the credit card has been successfully demonstrated and a detailed account on the vulnerability assessment of the BlockChain has been successfully accomplished. The security mechanism built using the MD5 and SHA algorithms to create BlockChains in the real world have been found to vulnerable to attacks and should therefore be further strengthened.

References

[1] G. Morganti, E. Schiavone, and A. Bondavalli, "Risk assessment of BlockChain technology," in *2018 Eighth Latin-American Symposium on Dependable Computing (LADC)*, Foz do Iguaçu, Brazil, pp. 87–96 (Oct. 2018), doi: 10.1109/LADC.2018.00020.

[2] Nikhil Gupta Gourisetti, Michael Mylrea, and Hirak Patangia, "Application of rank-weight methods to BlockChain cybersecurity vulnerability assessment framework," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, pp. 0206–0213 (Jan. 2019), doi: 10.1109/CCWC.2019.8666451.

[3] Muntadher Sallal, Gareth Owenson, Dawood Salman, and Mo Adda, "Security and performance evaluation of master node protocol based reputation BlockChain in the bitcoin network," *Blockchain: Research and Applications*, vol. 3, no. 1, p. 100048 (2022), doi: 10.1016/j.bcra.2021.100048.

[4] Imam Riadi, A. Ifani, and R. Kusuma, "Optimization and Evaluation of Authentication System using BlockChain Technology," *Emerging Science Journal*, vol. 4, pp. 225–240 (2022), doi: 10.28991/esj-2022-01289.

[5] Ihab M. Abdelwahed, Nagy Ramadan, and Hesham Ahmed Hefny, "Cybersecurity risks of BlockChain technology," *International Journal of Computer Applications*, vol. 177, no. 42, pp. 8–14 (2020), doi: 10.5120/ijca2020920745.

[6] Nikita V. Kuchin and Natalia G. Butakova, "Vulnerability analysis of corporate BlockChain systems to network attacks," in *2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)*, St. Petersburg, Russia, pp. 2366–2371 (Jan. 2021), doi: 10.1109/ElConRus51938.2021.9396249.

[7] Saurabh Singh, ASM Sanwar Hosen, and Byungun Yoon, "BlockChain security attacks, challenges, and solutions for the future distributed IoT network," *IEEE Access*, vol. 9, pp. 13938–13959 (2021), doi: 10.1109/ACCESS.2021.3052063.

[8] Zexi Xing and Zhengxin Chen, "Black bird attack: A vital threat to BlockChain technology," *Procedia Computer Science*, vol. 199, pp. 556–563 (2022), doi: 10.1016/j.procs.2022.01.070.

[9] Huaqun Guo and Xingjie Yu, "A survey on blockchain technology and its security," *Blockchain: Research and Applications*, vol. 3, no. 2, p. 100067 (2022), doi: 10.1016/j.bcra.2022.100067.

[10] Mohammad Kamrul Hasan, Ali Alkhalifah, Shayla Islam, Nissrein B. M. Babiker, A. K. M. Ahasan Habib, Azana Hafizah Mohd Aman, and Md Arif Hossain, "Blockchain technology on smart grid, energy trading, and big data: security issues, challenges, and recommendations," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 9065768 (2022), doi: 10.1155/2022/9065768.

[11] Parth Khandelwal, Rahul Johari, Varnika Gaur, and Dharm Vashisth, "BlockChain technology based smart contract agreement on Remix IDE," in *2021 8th International Conference on Signal Processing and Integrated Networks (SPIN)*, Noida, India, pp. 938–942 (Feb. 2021), doi: 10.1109/SPIN52536.2021.9565943.

[12] Suhas Harbola, Jyotsna Yadav, Rahul Johari, Ekta Verma, and Deo Prakash Vidyarthi, "Securing Digital Ownership Using Non-Fungible Tokens (NFTs), an Application of BlockChain Technology," in *International Conference on Internet of Things and Connected Technologies*, Singapore: Springer Nature Singapore, pp. 327–337 (2022), doi: 10.1007/978-981-19-4216-5_28.

[13] R. Johari, "VAIBT - Vulnerability Analysis in Blockchain Technology," GitHub Repository (2022). [Online]. Available: https://github.com/rahuljohaari/VAIBT

Received October, 2024