ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 6, June 2023

Blockchain Security - Current Threats and Mitigation Strategies

[1] Sanskar Bhushan, [2] Prakhar Gupta, [3] Nitish Chauhan, [4] Anita Thakur, [5] Ritu Agarwal

[1] [2] [3] Department of Applied Physics, Delhi Technological University, Delhi, India
[4] [5] Department of Information Technology, Delhi Technological University, Delhi, India
Corresponding Author Email: [1] pranita.devadkar.cs@ghrcem.raisoni.net, [2] prashant.more.cs@ghrcem.raisoni.net, [3] Rahul.gupta.cs@ghrcem.raisoni.net , [4] pranay.jaiswal.cs@ghrcem.raisoni.net, [5] sarita.patil@raisoni.net

Abstract— Blockchain technology has gotten a lot of interest in recent years because of its decentralized and secure nature. However, with the rise of blockchain technology, new security threats have emerged. This research paper examines existing vulnerabilities to blockchain security and suggests mitigation measures to mitigate these concerns. The paper gives an overview of the main forms of infrastructure assaults and investigates the best practices for avoiding them. The study's main goal is to discover and analyze every possible risk and assault that could happen at all levels of blockchain technology. The application layer, smart contract layer, consensus layer, and network layer are all part of this. The research intends to give a full knowledge of the numerous dangers and assaults that can occur in each layer by evaluating each layer. These solutions may include technical measures such as implementing secure coding practices and using secure network protocols, as well as organizational measures such as regular audits. By addressing the threats and attacks in each layer of blockchain technology and providing effective mitigation strategies, the objective of the research is to boost the safety and reliability of blockchain systems.

Index Terms—Blockchain, Threats, Attack, Mitigation Solutions, 51% Attack.

I. INTRODUCTION

Blockchain technology has emerged as a paradigm shifter, offering a decentralized and impenetrable way for a network of individuals to record and share data. Several fundamental concepts that ensure security, immutability, and transparency underpin the architecture of blockchain-based systems. A distributed ledger that maintains an ever-expanding chain of ordered entries known as blocks is the fundamental concept underpinning a blockchain. Each block is made up of a number of transactions, a hash of cryptography that links it to the previous block, and a nonce that acts as an identification number. Since network members, or nodes, collaborate to validate and build arrangements on new transactions and blocks, the system is immune to individual points of failure and censorship. Furthermore, the data is shielded against unauthorized access and manipulation by sophisticated cryptographic procedures.

Blockchain technology has the potential to disrupt a wide range of industries, including financial services, management of supply chains, and medical care, by delivering secure, trans-parent, and effective alternatives to many of the difficulties that plague centralized systems today.[1]

Although blockchain technology offers numerous advan-tages, it is essential to deal with the security and privacy concerns it generates. The potential of a majority assault is a critical security challenge that must be acknowledged. A 51 percent assault occurs when a single entity controls more than half of the network's computing power, allowing them to change or remove transactions in order to influence the blockchain. This increases the likelihood of fraud and theft. To prevent 51% attacks, blockchain networks use consensus mechanisms that require a certain level of computing power to validate transactions. The vulnerability of smart contracts is another security problem to consider. Smart contracts are au-tomated programs that complete transactions themselves based on established scenarios. However, if an automated contract's code comprises a vulnerability, attackers can use it to gain access to or tweak important data. Smart contracts should be extensively tested and inspected before their execution in order to minimize potential vulnerabilities. Overall, tackling the security and privacy dangers associated with blockchain technology is vital for maximizing its wide adoption and success.

Privacy is a significant concern in blockchain technology since all transactions are permanently recorded on the ledger, making them accessible to anyone [2]. Although transac-tions are anonymous, tracing the flow of funds through the blockchain can potentially link transactions to individuals or organizations. Some blockchain-based systems have incorpo-rated safeguards for privacy which include secret keys for encrypting transaction data as well as zero-knowledge proofs in order to verify transactions without exposing sensitive information.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 6, June 2023

Table I. Analysis of Blockchain Vulnerabilities and Solutions to Eliminate Them by Different Security Researchers

Researchers	Year	Vulnerability	Acting Layer	Solution	Improvement Evaluation
Duc-Hiep Chu, Loi Luu, Hrishi Olickel, Prateek Saxena and Aquinas Hobor [16].	2016	DAO Attack (Reentrancy Attack) and other common Ethereum smart contract vulnerabilities	Application Layer	Enhanced smart contract drafting structures, formal verification, and static inspection.	Enhanced security and reduced risk of vulnerabilities in contracts.
Nitish Amrit Kumar, Ilya Sergey, and quinas Hobor [17].	2017	General smart contract vulnerabilities	Application Layer	Designing a smart contract intermediate-level language, Scilla, that simplifies formal verification and reduces front-running vulnerabilities.	Improved security and reduced risk of having vulnerabilities in smart contracts by providing ways to do formal verification, typed variables support and explicit error handling.
Ivan Ivanitskiy, Ekaterina Voskresenskaya, Ramil Takhaviev, Sergei Tikhomirov and Evgeny Marchenko [18].	2018	General smart contract vulnerabilities	Application Layer	a tool for analyzing smart contracts for security flaws called ”SmartCheck” that employs static analysis and symbolic execution to find potential security holes.	SmartCheck is shown to effectively detect a range of smart contract vulnerabilities with low overhead.
Qingshan Li, Han Liu, Chao Liu, Jianbo Gao, Zhi Guan and Zhong Chen [19].	2019	Overflow and Underflow Attack on smart contract	Application Layer	Presented EASYFLOW, a tool to identify overflow risks in smart contracts built on Ethereum, which could end up in monetary damage. It divides smart contracts into secure contracts, manifested overflows, adequately safeguarded overflows, and probable overflows employing a taint assessment-based tracking approach.	The study attempts to solve the Ethereum smart agreement overflow attack risk, which might lead to instability and monetary damage.
Ittay Eyal and Emin Gun¨ Sirer [20].	2013	Selfish Mining Attack	Consensus Layer	Implementing a modified Bitcoin client which includes a “spy miner” that monitors the network for selfish mining behavior and can reveal it to honest miners.	The solution was shown to be effective in preventing selfish mining attacks, but it did require a small increase in network bandwidth and storage space.
Jae-Kwon [21].	2014	”Nothing at Stake” problem in PoS (Proof of Stake) consensus mechanism	Consensus Layer	A solution called ”Slasher” that penalizes validators who attempt to fork the blockchain	The Slasher solution was shown to be effective in preventing the ”Nothing at Stake” problem in PoS consensus algorithms.
Aggelos Kiayias and Giorgos Panagiotakos [22].	2015	Blockchain PoW Forking and Chain Quality	Consensus Layer	Introduced the ”chain of activity” concept, a new metric to evaluate chain quality and proposed a refined version of the GHOST protocol.	Improved chain quality, increased security, and better scalability in blockchain networks.
Phil Daian, Rafael Pass and Elaine Shi [23].	2019	Long-range attacks on PoS consensus in blockchain based systems	Consensus Layer	A consensus protocol called ”Snow White” that is designed to prevent long-range attacks by using a form of ”liquid democracy”	Snow White was shown to be more resistant to long-range attacks than traditional proof-of-stake consensus protocols.

Olanrewaju Sanda, Michalis Pavlidis, Saeed Seraj and Nikolaos Polatidis [24].	2023	Long-Range attacks on Permissionless blockchain	Consensus Layer	Deep Learning-based long-range ttack detection on permissionless blockchains	It can reduce detection costs of such attack and thus improve the performance of the systems.
Ethan Heilman, Alison Kendler, Aviv Zohar and Sharon Goldberg [25].	2015	Eclipse attacks on peer to peer networks in blockchain-based systems	Network Layer	a system for identifying and thwarting eclipse attacks in the P2P network of bitcoin	The proposed mechanism was able to detect and mitigate eclipse attacks with minimal impact on system performance.
Gian Marti, Maria Apostolaki, Jan Muller¨ and Laurent Vanbever [26].	2018	Eclipse attack on the Bitcoin network layer	Network layer	Proposed a protocol-level ountermeasure called "SABRE" which mitigates the effects of the Eclipse attack by allowing nodes to verify the legitimacy of incoming connections.	Showed that SABRE successfully resists Eclipse attacks while imposing negligible overhead on network bandwidth and latency.
Swarup Bhunia. Michael S. Hsiao, Mainak Banga and Seetharam Narasimhan [27].	2014	Trojan Attacks	Hardware Layer	Use secure hardware design and manufacturing processes, hardware attestation techniques, or hardware security modules to prevent or detect tampering with the hardware.	Minimal impact on performance
Francisco Eugenio Potestad-Ordo´ne,˜ Erica Tena-Sanchez´ and Ricardo Chaves [28].	2020	Fault Injection Attack on Blockchain Hardware	Hardware Layer	A flaw detection system that detects variations in the running time of cryptographic algorithms and compares them to the intended time of execution.	Negligible overhead in terms of power consumption and latency.
Silvio Micali, Yossi Gilad, Rotem Hemo, Georgios Vlachos and Nickolai Zeldovich .	2017	Double-spending attacks in blockchain-based systems	Multilayer Vulnerability	A new cryptocurrency called Algorand that uses novel mechanisms based on Verifiable Random Functions (VRFs) to attain scalability amongst participants in Byzantine Agreement (BA).	The authors demonstrate that the Algorand protocol can achieve high throughput, fast confirmation times, and high security while maintaining decentralization.
Linus Gasser, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Nicolas Gailly, Ewa Syta and Bryan Ford [29].	2018	Double-spending attacks in blockchain-based systems	Multilayer Vulnerability	A solution called "Omniledger" that uses sharding and Byzantine consensus to prevent double-spending attacks	Omniledger was shown to be efficient and effective in preventing double-spending attacks in blockchain-based systems.

II. VULNERABILITIES IN DIFFERENT BLOCKCHAIN LAYERS AND SECURITY APPROACHES TO ELIMINATE THEM

A.Application Layer

DAO Attack (Decentralized autonomous organization)- An attempt to steal money or property from a (DAO) via a blockchain network is known as a DAO attack. The attacker takes advantage of flaws in the smart contract code that controls the organization's functioning, such as voting rights or fund distribution regulations. To take over the organization's operations and steal money or property from its treasury, the attacker fabricates accounts or manipulates the voting process. One well-known instance of a DAO attack took place in 2016, when an attacker used a flaw in the code of the DAO, an investment fund operating in a decentralized manner using Ethereum, to steal ether of worth about $50 million. This sparked a contentious discussion among Ethereum users about the advantages and disadvantages of decentralized autonomous organizations, which led to a hard split of the Ethereum blockchain to recover the assets that had been taken. It's important to note that the Reentrancy attack is a particular kind of DAO attack [3].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 6, June 2023

Solution - Decentralized autonomous organizations (DAOs) and smart contract writers must make sure that their code is thoroughly tested and audited to find and repair vulnerabilities before deploying it on the blockchain network in order to prevent DAO attacks. To prevent unauthorized access to the organization's operations or treasury, it is crucial to install strong security measures, such as multi-factor authentication. Organizations can use this to protect their assets and stop any loss brought on by harmful attacks. The implementation of preventive measures by network operators and developers is necessary to safeguard blockchain networks.

Reentrancy Attack - Reentrancy attacks are a type of vul-nerability that target smart contracts on a blockchain network by preying on smart contract codes' weakness. The attack is referred to as "reentrancy" because it gives the attacker the ability to call a smart contract function more than once before the first call has concluded. This flaw enables the attacker to steal the contract's resources, including money and assets. An attacker may, for instance, repeatedly call a smart contract's function that permits users to withdraw money from their accounts before the contract updates the account balance, depleting the contract's funds. It's crucial to note that a reentrancy attack is a specific type of exploit that can be used in DAO attacks as well. It is essential to implement robust security mechanisms and thorough testing to prevent such attacks and ensure the security and integrity of smart contracts of a blockchain [4].

Solutions - Developers must make sure that their code is extensively tested and built to thwart reentrancy attacks on smart contracts. Best practices include employing secure coding patterns, separating data storage and execution to prevent reentrancy, and putting access restrictions in place to prevent unauthorized access to functions. Additionally, to

stop attackers – from carrying out too many transactions quickly, blockchain networks can add security features like petrol limitations. Reentrancy attacks can be avoided by using the "checks-effects-interactions" pattern or using mutexes to lock functions while they are being executed. Developers can lower the danger of reentrancy attacks and safeguard smart contracts by adhering to these preventative steps.

B. Transaction Layer

Transaction Replay Attack - A cyberattack known as a "transaction replay attack" occurs when an attacker copies a valid transaction and then replays it on the same or a different blockchain network. As a result, identical digital assets are duplicated, enabling the attacker to make double purchases. The use of the same private key to sign numerous transactions across various networks or inadequate encryption of the transaction data might also result in this [5].

Solution - The techniques available to blockchain developers to stop transaction replay attacks are numerous. To avoid processing duplicate transactions, they can use strategies like coming up with special transaction identifiers or sequence numbers. To prevent key reuse, they can also utilize distinct private keys for separate blockchain networks or apps. Fur-thermore, encryption of transaction data helps thwart replay and interception threats.

Time-Locked Transaction Attack - A cyberattack known as a "Time-Locked Transaction Attack" takes advantage of a transaction's time-ock feature to access funds without au-thorization. Funds are locked during this kind of attack for a certain amount of time before they may be accessed by the intended recipient. By manipulating the time-lock period and taking advantage of system flaws, the attacker can access the funds before the intended receiver. The integrity of the system may be jeopardized or cash may be lost as a result of this assault. Time-Locked Transaction Attacks can happen in a variety of blockchain-based systems, including Bitcoin and Ethereum, and are not exclusive to any one particular blockchain [6].

Solution - Developers must make sure that their time-lock methods are secure and dependable, put in place validation procedures to stop tampering with transaction information, and routinely monitor the network for any unusual behavior if they are to stop Time-Locked Transaction Attacks. Users should also exercise caution while sending or receiving time-locked transactions and should only utilize reliable platforms that have taken the appropriate security precautions. Before sending any money, users should authenticate the recipient's identification and the time-lock period.

C. Consensus Layer

Uncle Block Attack - In this attack, a miner tries to create a new block based on a block that has already been uploaded to the blockchain by another miner, with the aim of double-spending a transaction. This can result in a split in the blockchain, where different nodes have varying versions of the blockchain, potentially causing financial losses and network instability [7].

Solutions - Adopting a consensus algorithm that favors honest mining, such as PoS or a hybrid of PoW and PoS, which discourages uncle block generation and encourages building on the longest chain, is a robust method to reduce the danger of uncle block attacks. The likelihood of such assaults can be further decreased by adopting a checkpoint system, accelerating network propagation, and encouraging alternatives for transaction finality such as layer 2 protocols or off-chain transactions. It is also more challenging to carry off an uncle block assault when there is a robust, decentralized network of nodes that ensures no single miner or mining pool can meaningfully impact the blockchain.

Fork After Withholding Attack - A fork after withholding (FAW) attack in the context of blockchain technology is when a miner withholds some blocks from the network while

mining on a private fork. The blockchain is reorganized once the miner has completed a lengthier private split and released the delayed blocks to the public network. In a form of a 51% assault, this kind of attack could let the miner double-spend their money. Any layer of a blockchain, including the consensus and network layers, is susceptible to FAW attacks [8].

Solutions - Some blockchains use checkpointing, a system that enables nodes to confirm the legitimacy of the blockchain by verifying against specified points, to prevent FAW attacks. Additionally, some blockchains employ delayed block submis-sion, which can prevent miners from keeping blocks off the network for a long time.

D.Network Layer

Sybil Attack - A Sybil attack uses multiple false identities created by one person or entity to take over a network or system. Through the employment of numerous false identities, the attacker is able to exert more influence or authority over the network than anyone real user. A number of nefarious actions can be carried out with this technique, including the launch of spam or DDoS assaults, the acquisition of excessive voting power in a decentralized network, or the manipulation of a reputation system. With a Sybil Attack, an attacker may generate an extensive amount of imaginary nodes—also known as Sybil nodes—and use them to control a network or system. The attacker can employ a number of strategies, like IP address spoofing, to make it challenging for the network to recognize the false identities. In decentralized networks where each participant is equal and has an equal amount of voting power, this attack can be more damaging. In order to outvote any single real user, the attacker can generate a huge number of false identities. This can be used to influence how the network makes decisions [9].

Solution - Network administrators can use a number of strategies, including Proof-of-Work, Proof-of-Stake, or social trust algorithms, to thwart Sybil Attacks. An attacker would find it difficult or expensive to construct numerous false identities and take over the network using these procedures. Furthermore, reputation systems can be implemented to track and monitor participant behavior and spot any questionable activities. Before engaging in any transactions or communications, network users can verify the identities of other users.

Eclipse Attack - In a blockchain network attack known as an eclipse attack, an attacker can isolate By adjusting the incoming and outgoing connections to the targeted node, it is possible to isolate a certain node or nodes from the rest of the network. Once the node has been isolated, the attacker has the ability to change the data being sent to and received from it, which could lead to double spending, transaction censorship, or other forms of attacks. The Eclipse Attack can be carried out by building numerous fictitious nodes and sending them in the direction of the target node. This will overwhelm the target node with requests, causing it to reject other genuine nodes. By altering the targeted node's view of the blockchain network and its transactions, the attacker can subsequently compromise the blockchain's security.

Solution - A node can take precautions to diversify and confirm its network connections, such as connecting to nodes in various regions or with different IP addresses, to fend off an eclipse attack. In order to identify and isolate suspect connections or activity, the node can also continuously monitor the network. Finally, the node can implement algorithms and protocols, such as the Sybil control or the Dandelion++ protocol, that restrict an attacker's ability to control a sizable fraction of the network connections and lower the likelihood that an Eclipse Attack will be successful.

E.Hardware Layer

ASICs Mining Centralization - The blockchain community is becoming increasingly concerned about the concentration of ASICs (Application-Specific Integrated Circuit) mining. ASICs are specialized hardware tools created for a single task, like cryptocurrency mining. ASICs can be more effective than general-purpose gear, but their high initial cost can make them prohibitively expensive for smaller miners. This could lead to the concentration of mining power in a small number of large mining pools or enterprises, which could be harmful to the network's decentralisation and security.The centralized mining of ASICs can cause a variety of problems, such as the potential for a network attack if one party controls the majority of the network's mining power, or a 51 percent attack. This might compromise the blockchain's integrity by allowing the attacker to double-spend money or stop other transactions. Furthermore, it may lead to a lack of diversity in the network, which would reduce decentralization and make the system more susceptible to manipulation [10].

Solution - Some blockchain projects are investigating different consensus procedures to overcome this problem, such as Proof of Stake (PoS), which does not require specialised hard-ware and may offer greater user accessibility. Other projects are looking into the creation of ASIC-resistant algorithms to level the playing field for miners using less specialised equipment. Last but not least, several initiatives are thinking into implementing decentralized mining methods to make sure that no one organization can obtain excessive control over the network.

Side-Channel Attack - A sort of cyberattack known as a side-channel assault takes use of data leaks from a system's physical implementation rather than flaws in the algorithms or protocols themselves. To learn about secret keys or other sensitive information, side-channel assaults can involve keeping an eye on the system's power usage, electromagnetic emissions, or even the sounds it makes while running. Because they don't rely on common flaws in software or

hardware but rather exploit implementation or design flaws in the system, these attacks are frequently challenging to identify and stop. Applications that require security-critical functionality such as cryptographic systems are seriously threatened by side-channel attacks [11].

Solution - Implementing defenses at the system design stage is crucial to defending against side-channel attacks. These defenses can include electromagnetic radiation filtering, the use of masking techniques to obfuscate critical data, and the use of random operations to cover a system's power use. Shielding and secure locations are two additional physical security methods that might lessen the likelihood of side-channel assaults. In order to keep systems safe from the most recent known side-channel attack methods, it is also crucial to regularly monitor and upgrade them.

III. ARCHITECTURAL SOLUTIONS

SMPC (Secure Multi-Party Computation) - Secure Multi-Party Computation (SMPC) permits a lot of people to work together to compute a set of values on their own personal inputs while keeping those inputs concealed from one an-other. A safe and private computation process is achieved by enabling distributed computations in which each participant contributes their data without disclosing it to other parties. The fundamental concept is to distribute encrypted shares of private data among the involved parties. Then, without ever disclosing the real inputs, each side computes its individual portions, and the outcomes are combined to produce the final output. Encrypted shares and distribute them among the par-ticipating parties. Each party then performs computations on their respective shares, and the results are combined to produce the final output without ever revealing the actual inputs. This is accomplished by combining cryptographic primitives like homomorphic encryption, secret sharing, and secure protocols for handling encrypted data. SMPC provides an extensive variety of applications, including secure auctions, automated voting, and confidentiality data mining, among others. By enabling secure data exchange and privacy-preserving calcula-tions across numerous participants in an environment devoid of trust, SMPC can play a significant role in strengthening privacy and security in decentralized apps and smart contracts in the context of blockchain [12].

DAG (Directed Acyclic Graph) - In place of the conven-tional linear blockchain, it is an alternate data structure. Trans-actions are represented as vertices in a DAG, and the edges denote the order in which they occurred. DAG enables many transactions to be added concurrently, as opposed to a linear blockchain where transactions are collected into blocks and added sequentially, resulting in a more scalable and possibly speedier network. There are no loops because of the graph's acyclic structure, and the transactions retain some degree of order. Transactions are verified in DAG-based blockchain systems like IOTA [15] and Nano [14] by comparing them to earlier transactions, which increases decentralization and re-duces dependency on miners or stakers.This enables improved scalability, quicker confirmation times for transactions, and perhaps higher throughput

ASY (Asynchronous Consensus) - Asynchronous Consen-sus (ASY) is a consensus technique that enables nodes to come to an agreement without relying on synchronized com-munication. It is employed in distributed systems, includ-ing blockchain networks. Asynchronous consensus algorithms work under the assumption that message delivery durations are unpredictable and nodes may not receive messages simul-taneously, in contrast to synchronous consensus algorithms, which call for nodes to communicate within a predetermined time period. Given the prevalence of delays and inconsistent communication in large-scale, decentralized networks, ASY is particularly crucial. Asynchronous consensus techniques that provide robustness against network delays and failures, including Practical Byzantine Fault Tolerance (PBFT) and Honey Badger, enable the system to continue operating even in challenging circumstances [13].

ZKP (Zero-Knowledge Proofs - ZKPs are encrypted tech-niques that make it possible a prover show the truth of a claim without providing any further information about the claim itself. ZKPs have gotten a lot of interest in the context of given blockchain's potential to enhance privacy and security in a range of programs, such as confidential trades, management of identities, and secure voting. One of the key advantages of ZKPs is that they give users the option to demonstrate certain characteristics of their data without revealing the data itself, protecting privacy while assuring the verifiability of the underlying information. There are other ZKP system types, such as zk-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge) and zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge). In terms of efficiency, trust assumptions, and cryptographic assump-tions, these systems make a variety of trade-offs

IV. CONCLUSION

It's essential to draw lessons from past studies and assaults in order to build better and more secure distributed ledger technologies (DLTs) and blockchain systems. Here are the top five areas that need work:

Robust Consensus Algorithms - Create and put into use new consensus algorithms that can fend off attacks like Sybil, long-range mining, and selfish mining. To reduce the dangers of centralization and environmental effect associated with proof of work (PoW), take into account alternate consensus techniques such as proof of stake (PoS), delegated proof of stake (DPoS), or proof of authority (PoA).

Scalability and Performance Enhancements - increasing the speed at which blockchain platforms can handle transactions without compromising security. To increase overall perfor-mance and alleviate network congestion, employ tactics like as sharding, off-chain transactions, or layer-2 solutions such as the Lightning Network for Bitcoin or Plasma for Ethereum.

Formal Verification and Security Audits - Use formal verifi-cation techniques to carefully assess and confirm the accuracy of smart contracts and other blockchain components. Utilize bug bounty programmes and routine security audits to find and patch such vulnerabilities before attackers can take advantage of them.

Interoperability and Cross-Chain Communication - Cre-ate standardized communication protocols between various blockchain networks to enable safe and effective cross-chain transactions. This can make it possible for value to be trans-ferred between blockchains without any delays and make it easier to create decentralized applications that work across networks.

Enhanced Privacy and Security - Implement cutting-edge cryptographic methods to improve transaction privacy and data security, Secure multi-party computing (SMPC), homomorphic encryption, and zero-knowledge proofs (ZKP) are some of the instances. These methods can maintain the decentralized nature of DLTs and blockchains while ensuring data integrity and confidentiality.

REFERENCES

[1] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," National Institute of Standards and Technology, Oct. 2018, doi: https://doi.org/10.6028/nist.ir.8202.

[2] J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, "Privacy-preserving solutions for Blockchain: re-view and challenges," IEEE Access, vol. 7, pp. 1–1, 2019, doi: https://doi.org/10.1109/access.2019.2950872.

[3] M. I. Mehar et al., "Understanding a Revolutionary and Flawed Grand Experiment in Blockchain," Journal of Cases on Infor-mation Technology, vol. 21, no. 1, pp. 19–32, Jan. 2019, doi: https://doi.org/10.4018/jcit.2019010102.

[4] I. Nikolic, A. Kolluri, I. Sergey, P. Saxena, and A. Hobor, "Finding The Greedy, Prodigal, and Suicidal Contracts at Scale," arXiv:1802.06038 [cs], Mar. 2018, Available: https://arxiv.org/abs/1802.06038.

[5] P. Ramanan, D. Li, and N. Gebraeel, "Blockchain-Based Decentralized Replay Attack Detection for Large-Scale Power Systems," IEEE Trans-actions on Systems, Man, and Cybernetics: Systems, pp. 1–13, 2021, doi: https://doi.org/10.1109/tsmc.2021.3104087.

[6] I. Tsabary, M. Yechieli, A. Manuskin, and I. Eyal, "MAD-HTLC: Because HTLC is Crazy-Cheap to Attack," IEEE Xplore, May 01, 2021. https://ieeexplore.ieee.org/abstract/document/9519476

[7] S.-Y. Chang, Y. Park, S. Wuthier, and C.-W. Chen, "Uncle-Block Attack: Blockchain Mining Threat Beyond Block Withholding for Rational and Uncooperative Miners," Springer Link, 2019. https://link.springer.com/content/pdf/10.1007%2F978-3-030-21568-2 12.pdf.

[8] S. Shalini and H. Santhi, "A Survey on Various Attacks in Bitcoin and Cryptocurrency," 2019 International Conference on Communication and Signal Processing (ICCSP), Apr. 2019, doi: https://doi.org/10.1109/iccsp.2019.8697996.

[9] G. Bissias, A. P. Ozisik, B. N. Levine, and M. Liberatore, "Sybil-Resistant Mixing for Bitcoin," Proceedings of the 13th Workshop on Privacy in the Electronic Society, Nov. 2014, doi: https://doi.org/10.1145/2665943.2665955.

[10]S. Chu and S. Wang, "The Curses of Blockchain Decen-tralization," arXiv:1810.02937 [cs], Oct. 2018, Available: https://arxiv.org/abs/1810.02937.

[11]S. Saravanan, M. Hailu, G. M. Gouse, M. Lavanya, and R. Vijaysai, "Optimized Secure Scan Flip Flop to Thwart Side Channel Attack in Crypto-Chip," Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 410–417, 2019, doi: https://doi.org/10.1007/978-3-030-15357-1 34.

[11]H. Zhong, Y. Sang, Y. Zhang, and Z. Xi, "Secure Multi-Party Computation on Blockchain: An Overview," Communications in computer and information science, pp. 452–460, Dec. 2019, doi: https://doi.org/10.1007/978-981-15-2767-8 40.

[12]A. Miller, Y. Xia, K. Croman, E. Shi, and D. Song, "The Honey Badger of BFT Protocols." Available: https://eprint.iacr.org/2016/199.pdf

[13]C. Lemahieu, "Nano: A Feeless Distributed Cryptocurrency Network." Available: http://media.abnnewswire.net/media/cs/whitepaper/rpt/91948-whitepaper.pdf.

[14] Y. Li et al., "Direct Acyclic Graph-based Ledger for Internet of Things: Performance and Security Analysis." Accessed: May 02, 2023. [Online]. Available: https://files.iota.org/papers/DirectAcyclicGraph-based Ledger for Internet of Things.pdf.

[15]L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making Smart Contracts Smarter," 2016, doi: https://doi.org/10.1145/2976749.2978309.

[16]I. Sergey, A. Kumar, and A. Hobor, "Scilla: a Smart Contract Intermediate-Level LAnguage," arXiv:1801.00687 [cs], Jan. 2018, Accessed: Apr. 11, 2023. [Online]. Available: https://arxiv.org/abs/1801.00687.

[18]S. Tikhomirov, E. Voskresenskaya, I. Ivanitskiy, R. Takhaviev, E. Marchenko, and Y. Alexandrov, "SmartCheck: Static Analy-sis of Ethereum Smart Contracts," IEEE Xplore, May 01, 2018. https://ieeexplore.ieee.org/document/8445052.

[19]J. Gao, H. Liu, C. Liu, Q. Li, Z. Guan, and Z. Chen, "EASYFLOW: Keep Ethereum Away from Overflow," 2019 IEEE/ACM 41st Inter-national Conference on Software Engineering: Companion Proceed-ings (ICSE-Companion), May 2019, doi: https://doi.org/10.1109/icse-companion.2019.00029.

[20]I. Eyal and E. G. Sirer, "Majority Is Not Enough: Bitcoin Mining Is Vulnerable," Financial Cryptography and Data Security, vol. 8437, pp. 436–454, 2014, doi: https://doi.org/10.1007/978-3-662-45472-5 28.

[21] J.Kwon, "Tendermint :Consensus with-out Mining," www.semanticscholar.org,2014. https://www.semanticscholar.org/

paper/Tendermint-%3A-Consensus-without-Mining-Kwon/df62a45f50aac8890453b6991ea115e996c1646e.

[22]A. Kiayias and G. Panagiotakos, "On Trees, Chains and Fast Transac-tions in the Blockchain." Accessed: May 02, 2023. [Online]. Available: https://eprint.iacr.org/2016/545.pdf.

[23]P. Daian, R. Pass, and E. Shi, "Snow White: Robustly Reconfig-urable Consensus and Applications to Provably Secure Proof of Stake," Financial Cryptography and Data Security, pp. 23–41, 2019, doi: https://doi.org/10.1007/978-3-030-32101-7 2.

[24]O. Sanda, M. Pavlidis, S. Seraj, and N. Polatidis, "Long-Range at-tack detection on permissionless blockchains using Deep Learning," Expert Systems with Applications, vol. 218, p. 119606, May 2023, doi: https://doi.org/10.1016/j.eswa.2023.119606.

[25]E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Open access to the Proceedings of the 24th USENIX Security Symposium is sponsored by USENIX Eclipse Attacks on Bitcoin's Peer-to-Peer Network Eclipse Attacks on Bitcoin's Peer-to-Peer Network," 2015. Available: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-heilman.pdf.

[26]M. Apostolaki, G. Marti, J. Muller,¨ and L. Vanbever, "SABRE: Pro-tecting Bitcoin against Routing Attacks," arXiv:1808.06254 [cs], Aug. 2018, Available: https://arxiv.org/abs/1808.06254.

[27]S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware Trojan Attacks: Threat Analysis and Countermeasures," Proceedings of the IEEE, vol. 102, no. 8, pp. 1229–1247, Aug. 2014, doi: https://doi.org/10.1109/jproc.2014.2334493.

[28]F. E. Potestad-Ordo´nez,˜ E. Tena-Sanchez,´ A. J. Acosta-Jimenez,´ C. J. Jimenez´-Fernandez,´ and R. Chaves, "Hardware Countermeasures Benchmarking against Fault Attacks," Applied Sciences, vol. 12, no. 5, p. 2443, Jan. 2022, doi: https://doi.org/10.3390/app12052443.

[29]E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding," IEEE Xplore, May 01, 2018. https://ieeexplore.ieee.org/document/8418625.