International Journal of Intelligent Communication and Computer Science
Vol. 2, No. 1, 2024, Pages 72-81.

Honeypot Deployment: A Blockchain-Based Distributed Approach

Neharika Nishad[1] and Rahul Singh[2]

[1]Research Scholar, Department of Computer Science and Engineering, Kanpur Institute of Technology, Affiliated to AKTU, Lucknow
[2] Department of Computer Science and Engineering, Kanpur Institute of Technology, Affiliated to AKTU, Lucknow

Research Paper

Email: nehariikanishad1@gmail.com
Received: 10 Mar 2024, Revised: 29 May 2024 Accepted: 28 May 2024

Abstract:
In the realm of cybersecurity, the deployment of honeypot systems stands as a crucial strategy for detecting and thwarting malicious activities. However, traditional honeypot architectures often face challenges related to centralized management and vulnerability to attacks. In this paper, we propose a novel approach to honeypot deployment leveraging blockchain technology to establish a distributed and resilient system. Our system design incorporates blockchain's inherent features of immutability, decentralization, and transparency to enhance the security and reliability of honeypot networks. By distributing honeypot instances across the blockchain network, we mitigate the risks associated with single points of failure and provide a robust defense against sophisticated cyber threats. We present the architecture of our distributed honeypot system, detailing the integration of blockchain mechanisms for secure data storage, tamper-resistant logging, and consensus-based decision-making. Through experimental validation and analysis, we demonstrate the effectiveness and efficiency of our proposed solution in detecting and mitigating cyber threats. Our research contributes to the advancement of cybersecurity paradigms by harnessing the potential of blockchain technology to fortify honeypot deployments against evolving cyber threats.

Keywords: Honeypot, Distributed system, Blockchain

1. Introduction

Cybersecurity is a critical concern in today's digital landscape, with organizations facing increasingly sophisticated and persistent cyber threats. Among the arsenal of defensive measures, honeypot systems serve as valuable tools for detecting and analyzing malicious activities [1]. Honeypots are decoy systems designed to lure attackers, providing insights into their tactics and techniques while diverting them away from real assets [2]. However, traditional honeypot architectures often suffer from centralized vulnerabilities, posing risks to the integrity and reliability of the data collected [3,4]. To address these challenges, we propose a novel approach to honeypot deployment leveraging blockchain technology [5]. Blockchain, originally conceived as the underlying technology behind cryptocurrencies like Bitcoin, offers a decentralized and tamper-resistant framework ideally suited for enhancing the security and resilience of honeypot networks [6]. By harnessing the core principles of blockchain, including immutability, decentralization, and transparency, we aim to create a distributed honeypot system capable of withstanding sophisticated cyber threats [7].

In this paper, we present the design and implementation of a distributed honeypot system based on blockchain technology. We outline the motivations driving the adoption of blockchain in honeypot deployment and discuss the inherent limitations of traditional centralized architectures. Our proposed solution leverages blockchain's decentralized ledger to distribute honeypot instances across a network of nodes, thereby mitigating the risks associated with single points of failure and enhancing the system's

resilience to attacks. Furthermore, we detail the architecture of our distributed honeypot system, highlighting the integration of blockchain mechanisms for secure data storage, tamper-resistant logging, and consensus-based decision-making. We provide insights into the deployment and management of blockchain-enabled honeypots, addressing key considerations such as node synchronization, data synchronization, and consensus protocols.

Through experimental validation and analysis, we evaluate the effectiveness and efficiency of our proposed solution in detecting and mitigating cyber threats.

Overall, our research contributes to the advancement of cybersecurity paradigms by harnessing the potential of blockchain technology to fortify honeypot deployments against evolving cyber threats. We believe that the insights gained from this study will inform the development of more robust and resilient cybersecurity solutions in the future.

2. Introductory Concepts

In this section introductory concepts are discussed.

2.1 Honeypot System

In the constantly evolving landscape of cybersecurity, organizations face an ever-growing array of threats and vulnerabilities. One of the most effective strategies for detecting and mitigating these threats is the deployment of honeypot systems. Honeypots are decoy systems designed to mimic legitimate assets or services, enticing attackers to interact with them and revealing their tactics, techniques, and intentions [8]. The concept of honeypots dates back several decades, with their primary objective being to serve as early warning systems for cybersecurity professionals. By strategically placing honeypots within a network, organizations can gain valuable insights into the methodologies employed by adversaries, identify vulnerabilities in their defenses, and proactively strengthen their security posture. Honeypots come in various forms, ranging from low-interaction honeypots that simulate basic services and collect minimal information, to high-interaction honeypots that emulate entire systems and engage with attackers in real-time. Regardless of their complexity, honeypot systems play a crucial role in cybersecurity operations, enabling organizations to gather threat intelligence, analyze attack patterns, and develop effective countermeasures [9].

In this paper, we delve into the design, implementation, and utilization of honeypot systems in contemporary cybersecurity environments. We explore the various types of honeypots, their deployment strategies, and the challenges associated with their operation. Additionally, we discuss the role of honeypots in incident response, threat detection, and penetration testing, highlighting their value as indispensable tools in the cybersecurity arsenal.

2.2 Blockchain System

Among the innovative encryption schemes, blockchain technology has emerged as a highly secure option with diverse applications across engineering and technology fields [10]. Particularly in the realm of smart e-health applications, blockchain stands out for its ability to provide a comprehensive solution for decentralized devices while ensuring robust encryption techniques [11]. By establishing a trustworthy network of interconnected devices, blockchain-based e-health systems eliminate the need for intermediaries, thereby streamlining processes and enhancing data security. The concept of decentralization has gained traction in the development of e-health systems, driven by its potential to enhance accessibility and efficiency. However, decentralization also introduces vulnerabilities to cyberattacks, raising concerns about trust and accountability within such systems. In response to these challenges, blockchain technology offers an immutable ledger that records all transactions, safeguarding data integrity and providing a transparent audit trail. A blockchain functions as a series of interconnected blocks, each linked through historically generated hash values, ensuring data immutability and integrity. The genesis block, representing the initial block in the chain, marks the inception of the blockchain [12]. Every subsequent block in the chain maintains a connection to the hashed address of the preceding block, forming a continuous sequence of data.

Hash values, akin to unique fingerprints, serve as identifiers for blocks and their contents, ensuring authenticity and integrity. These hash values are computed for each block upon its creation, and any modification to the block results in a change in its hash value. Moreover, each block includes the hash value of its preceding block, creating a chain-like structure that enhances security and transparency.
Operating as a peer-to-peer network without centralized control, blockchain ensures that each node maintains a complete copy of the entire chain. This redundancy enables nodes to verify the integrity and authenticity of blocks, thereby upholding the network's security. Furthermore, the inclusion of timestamps in each block makes it challenging to alter data retroactively, bolstering the overall integrity of the blockchain. As new blocks are added to the chain, each node reaches a consensus to validate the integrity of the newly produced block, ensuring the network's resilience against manipulation and unauthorized access.

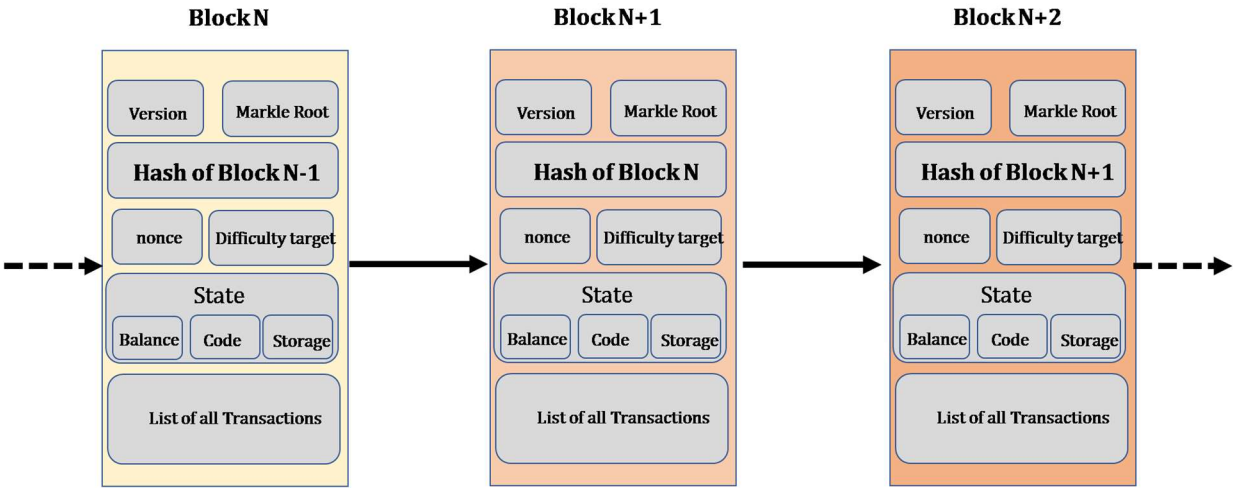

Figure 1: Schematic of blocks in Blockchain

3. Proposed Method

Designing a dynamic distributed honeypot system based on blockchain entails integrating blockchain technology to bolster the decentralization, security, and transparency of the honeypot network. This innovative approach aims to address the limitations of traditional centralized honeypot architectures and fortify the system against evolving cyber threats. Below, we outline an algorithm detailing the key steps involved in establishing such a dynamic distributed honeypot system:

3.1 Setup Blockchain Network:

Establishing a decentralized blockchain network for a dynamic distributed honeypot system involves selecting an appropriate blockchain platform, such as Ethereum or Hyperledger, to serve as the foundation for the network infrastructure. These platforms offer robust frameworks and tools for building decentralized applications (dApps) with features like smart contracts, consensus mechanisms, and cryptographic security. By leveraging blockchain technology, organizations can create a secure and transparent ecosystem for managing honeypots across distributed nodes. Once the blockchain network is established, the next step is to deploy smart contracts to facilitate the registration, configuration, and operation of honeypots within the network. Smart contracts are self-executing contracts with predefined rules and conditions encoded on the blockchain, ensuring trustless and immutable execution of transactions. These smart contracts can be designed to handle various aspects of honeypot management, including:

1. **Registration:** Smart contracts can manage the registration process for new honeypots joining the network, ensuring that each honeypot is authenticated and authorized to participate in the system.

Configuration: Smart contracts can specify the parameters and configurations for each honeypot, such as network settings, monitoring rules, and response actions, ensuring consistency and standardization across the network.

2. **Operation:** Smart contracts can govern the operation of honeypots, including data collection, analysis, and incident response, ensuring that all actions are recorded transparently on the blockchain and executed according to predefined rules.

By deploying smart contracts on the blockchain, organizations can automate and streamline the management of distributed honeypots, reducing manual intervention and enhancing operational efficiency. Additionally, the use of smart contracts ensures the integrity and transparency of honeypot operations, as all transactions and interactions are recorded immutably on the blockchain, providing a verifiable audit trail for accountability and compliance purposes. Overall, integrating blockchain technology and smart contracts into the management of distributed honeypots offers a secure, decentralized, and efficient approach to cybersecurity threat detection and mitigation.

3.2 Honeypot Registration:

In the establishment of a dynamic distributed honeypot system based on blockchain, the registration of honeypot nodes onto the blockchain network begins with the deployment of a registration smart contract. This smart contract serves as the gateway for honeypot nodes to authenticate themselves and securely join the decentralized network. Upon deployment, each honeypot node generates a unique identifier, which serves as its digital fingerprint within the blockchain ecosystem. This identifier is crucial for maintaining the integrity and accountability of honeypot operations across the network.

Subsequently, each registered honeypot node proceeds to publish its configuration details onto the blockchain. These configuration details encompass a comprehensive array of parameters, including the types of services emulated by the honeypot, the network protocols supported, and the geographical location of the node. By transparently broadcasting this information to the blockchain, honeypot nodes contribute to the collective intelligence of the distributed system, enabling network administrators to gain insights into the diverse capabilities and coverage of the honeypot network.

Furthermore, the publication of configuration details facilitates the orchestration of honeypot operations and enhances the effectiveness of threat detection and response strategies. Network administrators can leverage this information to strategically deploy honeypot nodes across different regions and network segments, thereby maximizing coverage and increasing the likelihood of capturing a diverse range of cyber threats. Additionally, the transparency provided by blockchain technology ensures the integrity and reliability of the configuration data, mitigating the risk of tampering or falsification by malicious actors.

In essence, the registration and configuration process on the blockchain network lay the foundation for the seamless integration and collaboration of honeypot nodes within the distributed system. By harnessing the power of blockchain technology, organizations can establish a dynamic and resilient honeypot infrastructure capable of detecting, analyzing, and mitigating cyber threats with unprecedented efficiency and transparency.

3.3 Blockchain-Based Reputation System:

Implementing a reputation system on the blockchain introduces a mechanism to evaluate the trustworthiness and reliability of honeypot nodes within the distributed network. In this setup, nodes accrue reputation points based on their performance in capturing and analyzing malicious activities, as well as their overall contribution to bolstering the security posture of the network. By leveraging blockchain technology, the reputation system ensures transparency and immutability, allowing for fair and accurate assessment of each node's capabilities and effectiveness in combating cyber threats.

3.4 Dynamic Configuration Updates:

Dynamic configuration updates for honeypot nodes are facilitated through the utilization of smart contracts, which serve as the conduit for seamless adjustments to emulation profiles, network settings, and monitoring parameters. This dynamic flexibility enables nodes to adapt in real-time to evolving threat landscapes and changing network conditions, enhancing their responsiveness and efficacy in detecting and mitigating

emerging cyber threats. By leveraging smart contracts, organizations can ensure that honeypot nodes remain agile and proactive in their defense strategies, thereby fortifying the overall resilience of the distributed system.

3.5 Consensus Mechanism:

The incorporation of a consensus mechanism, such as proof-of-stake or delegated proof-of-stake, ensures the integrity and validity of transactions recorded on the blockchain. Through consensus, only legitimate transactions related to honeypot registration, configuration updates, and reputation scoring are accepted and confirmed, safeguarding the integrity of the distributed honeypot system. By leveraging a robust consensus mechanism, organizations can mitigate the risk of fraudulent activities and maintain the reliability and transparency of the blockchain-based infrastructure.

3.6 Decentralized Threat Intelligence Sharing:

Facilitating decentralized threat intelligence sharing among honeypot nodes is paramount to enhancing the collective defense capabilities of the distributed network. By enabling nodes to securely exchange threat intelligence and attack signatures, organizations can amplify their ability to detect and respond to sophisticated cyber threats effectively. Utilizing encrypted channels and decentralized storage solutions ensures the confidentiality and integrity of shared information, safeguarding sensitive data from unauthorized access or tampering.

3.7 Anomaly Detection and Alerting:

Implementing advanced anomaly detection algorithms within each honeypot node enables proactive identification of suspicious activities and potential security threats. By leveraging blockchain-based anomaly detection techniques, organizations can detect deviations from normal behavior patterns and trigger real-time alerts and notifications to network administrators and security analysts. This proactive approach to threat detection empowers organizations to mitigate risks promptly and minimize the impact of security incidents on their operations.

3.8 Blockchain-Based Logging and Auditing:

Leveraging the blockchain for logging and auditing purposes ensures the integrity and immutability of all transactions, events, and interactions within the honeypot network. By maintaining a tamper-proof log of activities on the blockchain, organizations can establish a transparent and verifiable audit trail for regulatory compliance and forensic investigations. This blockchain-based logging and auditing framework provide auditors and regulatory authorities with the assurance that honeypot data is authentic and unaltered, enhancing trust and accountability within the distributed system.

3.9 Continuous Improvement and Optimization:

Continuous monitoring and analysis of the honeypot network using blockchain-based analytics tools enable organizations to identify areas for optimization and enhancement. By soliciting feedback from honeypot operators, security researchers, and threat intelligence sources, organizations can iteratively improve the performance and efficacy of their cybersecurity defenses. Leveraging blockchain technology for continuous improvement and optimization ensures that the distributed honeypot system remains adaptive, resilient, and effective against evolving cyber threats.

By implementing the above strategies, organizations can establish a dynamic distributed honeypot system that leverages blockchain technology to enhance the resilience, efficiency, and effectiveness of their cybersecurity defenses against evolving cyber threats.

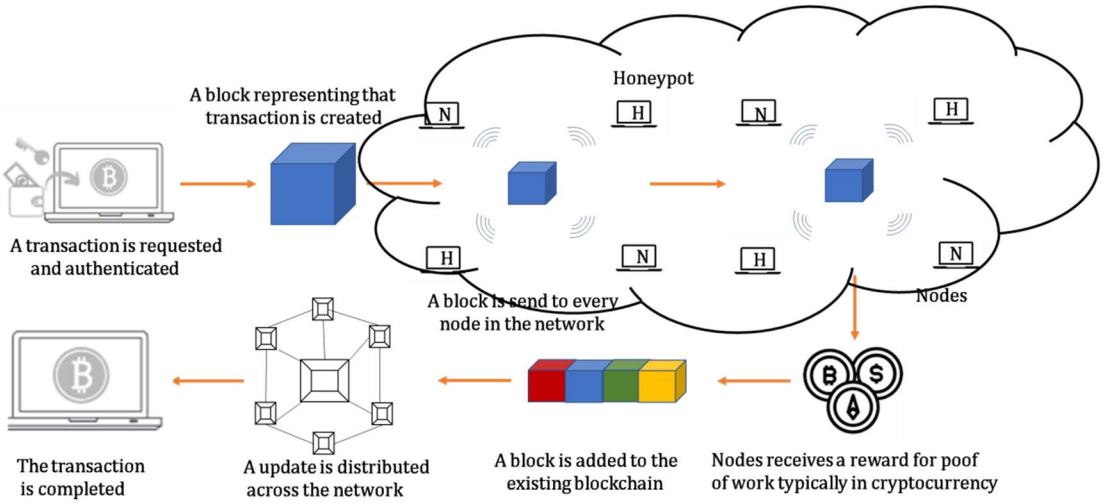

Figure 2: Schematic of Decentralized Honeypot system based on Blockchain Networks

In Figure 2, the depicted network illustrates the assignment of keys and states to each node, distinguishing between Normal (N) and Honeypot (H) nodes. Each node is equipped with a unique key and is designated a state based on its role within the network, either as a normal operational node or as a honeypot designed to attract and monitor malicious activity. This differentiation is crucial for the effective functioning of the network, as it enables the identification and segregation of honeypot nodes from the regular operational nodes. During the initial phase of operation, a symmetric key technique is employed to encrypt the records of each node within the network. This encryption process is governed by Equation 1, which defines the cryptographic algorithm utilized to secure the node records. Symmetric key encryption involves the use of a single key for both the encryption and decryption of data, ensuring that only authorized parties possessing the key can access the encrypted information. By leveraging symmetric key encryption in the first phase, the network ensures the confidentiality and integrity of node records, safeguarding sensitive information from unauthorized access or tampering. This cryptographic technique adds an additional layer of security to the network, mitigating the risk of data breaches and unauthorized disclosures. Furthermore, the utilization of symmetric key encryption facilitates efficient and streamlined communication between nodes, enhancing the overall robustness and reliability of the network infrastructure.

$$S_{NR} = E(K, S) \tag{1}$$

In this context, S_{NR} represents the cipher-text node record, with E indicating the encryption process, K representing the symmetric key, and S denoting the node state. Following this encryption process, further annotated key is generated.

L= node key (K_1) ||encryption key K_2 || node lofile key K_3,

In this scenario, key K_1, key K_2 and key K_3 serve as node keys associated with different processes. The process of calculating the hash value for the current block entails a series of steps designed to ensure data integrity and security within the blockchain network. Specifically, this calculation involves the concatenation of two essential components: the hash value of the previous block (referred to as Hprev) and the data contained within the current block (referred to as L). This concatenation process is guided by Equation 2, which outlines the specific algorithm used to compute the hash value.

$$H_{Curr} = Hash(H_{prev} \,||\, \mathrm{L}) \tag{2}$$

The generation of the hash value is executed through the application of a cryptographic hash function, such as SHA-256 [13], renowned for its robustness and security properties. This function processes the data within the block, creating a unique fixed-length string of characters that represents the block's contents. Once this hash value is computed, a simple consensus mechanism is utilized to append the newly created block to the existing network of the blockchain. Upon the completion of this process, the newly added block undergoes validation by the network's peers. This validation entails the verification of the block's integrity and adherence to the established rules of the blockchain protocol. Once the block receives approval from the majority of the network's peers, it is officially incorporated into the blockchain network, becoming an

immutable part of the distributed ledger. Subsequently, when a receiver interacts with the blockchain network, they perform a verification process to ensure the authenticity and integrity of the data they receive. This verification involves computing a new hash value using the same cryptographic hash function (SHA-256) that was employed during the block creation process. Equation 17 outlines the specific steps involved in this verification process, allowing the receiver to confirm the validity of the received data (L) by comparing its hash value with the computed hash value.

$$H'_{Curr} = Hash(H_{prev} \| \mathrm{L}) \quad (3)$$

In the final step of the validation process, the calculated hash value, denoted as H'_{Curr}, is compared with the hash value of the current block within the blockchain. This comparison serves as a critical checkpoint to determine the integrity and authenticity of the block.

If the calculated hash value H'_{Curr} matches precisely with the hash value of the current block H_{Curr} in the blockchain, it signifies that the block has been received untampered. In other words, the data within the block remains unchanged from its original state, and the block can be considered valid and trustworthy.

However, if there is any discrepancy between the calculated hash value H'_{Curr} and the hash value of the current block H_{Curr}, it indicates that the block has been tampered with or altered in some way. This discrepancy serves as a clear indicator of unauthorized modifications to the block's data or structure.

3.10 Security Assessment

The blockchain system is susceptible to attacks, necessitating a thorough examination to validate its security measures.

1. **Confidentiality:** Even if the attacker gains access to the data L, they are unable to retrieve the node data due to the encryption and security measures in place. The attacker remains unaware of the keys K1, K2, and K3, which are essential for decrypting the node data. These keys serve as cryptographic safeguards, ensuring that only authorized entities possessing the correct keys can access and decipher the encrypted data. By maintaining strict control over the distribution and management of keys K_1, K_2, and K_3, the system effectively prevents unauthorized access to sensitive node data. Without knowledge of these keys, the attacker is unable to decrypt the encrypted data L, rendering it effectively inaccessible and unintelligible. This multi-layered approach to security ensures that even if an attacker manages to obtain encrypted data, they are unable to compromise the confidentiality and integrity of the node data without the requisite keys. As a result, the system maintains robust protection against unauthorized access and data breaches, safeguarding the integrity and privacy of the blockchain network.
2. **Integrity:** Even if an attacker attempts to generate fake data (L') and counterfeit keys (K'_1, K'_2, and K'_3), they would face significant challenges in compromising the integrity of the blockchain. Firstly, altering the data or generating fake data would result in a different hash value compared to the one stored in the blockchain. As a result, any attempt by the attacker to manipulate the blockchain would be immediately detected by the network. Moreover, changing even a single record within the blockchain would require the attacker to recalculate the hash values of all preceding blocks, a process that demands considerable computational power and time. Furthermore, to successfully compromise the blockchain, the attacker would need to control more than 51% of the total nodes in the network, a feat that is exceedingly difficult to achieve in a decentralized and distributed system. Attempting to gain control of the majority of nodes would require significant resources and coordination, making it an unrealistic scenario in practice. Additionally, the consensus mechanisms employed by blockchain networks, such as proof-of-work or proof-of-stake, further enhance security by requiring broad agreement among network participants before validating and adding new blocks to the blockchain. This distributed consensus ensures that any attempts at malicious manipulation are thwarted by the collective integrity of the network.

4. Results

In this section, we provide a comprehensive overview of the simulation results obtained from our study. Through rigorous experimentation and analysis, we present findings that shed light on various aspects of the simulated scenarios. These results offer valuable insights into the performance, behavior, and outcomes of the simulated systems or processes under investigation.

Table 1: Blockchain basic data

Block	Previous Hash	Self Hash	Nonce
0Genesis	[]	'075c27741a3506846368fa6e5b3477f85 b31ceee71a5716e2f12b40fa21d23aa'	[]
index: 1	'075c27741a3506846368fa6e5b3477f8 5b31ceee71a5716e2f12b40fa21d23aa'	'00064df66af5ad32e5e11bcf16f3ef24'	4330
index: 2	00064df66af5ad32e5e11bcf16f3ef24'	'0009d61b5a9e8e370a57ca8ae4e03dd7'	4046
index: 3	'0009d61b5a9e8e370a57ca8ae4e03dd7'	'000f28bbe1d35d89bfbeab5c4dbb014a'	278
index: 4	'000f28bbe1d35d89bfbeab5c4dbb014a'	'0001c241ebcc982417beb8a9df5b3b36'	3041
index: 5	'0001c241ebcc982417beb8a9df5b3b36'	'000fd8fd84c9cdafd876d16da6bb40b1'	1
index: 6	'000fd8fd84c9cdafd876d16da6bb40b1'	'000038fa393bd937fa0e0f7f78861fe1'	3886

The data provided appears in table 1, the structure and content of a blockchain, with specific focus on individual blocks within the chain. The term "0Genesis" suggests the initial block in the blockchain, known as the genesis block, which lays the foundation for the entire chain. Each subsequent entry in the data represents a block within the blockchain, with an associated index indicating its position in the sequence. The hash values provided serve as unique identifiers for each block, computed through cryptographic hash functions based on the block's contents. These hash values play a crucial role in ensuring the integrity and immutability of the blockchain, as any alteration to a block's data would result in a different hash value.
The elapsed times provided offer a glimpse into the temporal dynamics of operations within a blockchain network comprising six nodes as shown in Figure 3. Each duration represents the time taken for specific tasks or processes to unfold within the network's operational framework. For instance, durations of approximately 12.4 and 10.7 seconds suggest relatively longer processes or operations within the blockchain network, potentially involving complex computations or data transactions. Conversely, significantly shorter durations, such as 0.74 and 0.007 seconds, point towards swift task completions, possibly indicating routine or less computationally intensive operations. These elapsed times underscore the varying complexities and efficiencies inherent in the functioning of a blockchain network, influenced by factors like task intricacy, network congestion, and computational resources. Understanding these temporal aspects provides valuable insights into the operational dynamics and performance characteristics of blockchain networks, facilitating optimization and refinement efforts for enhanced efficiency and effectiveness in real-world applications.

Figure 4 illustrates the relationship between total computational time (measured in seconds) and the number of transactions per block within a blockchain network. This analysis considers a scenario where there are five peer-to-peer nodes in the network, and a total of 25 blocks are mined. Notably, as the number of transactions per block varies, it directly impacts the total computational time required to process these transactions within the blockchain network. For instance, when there are 10 transactions per block, the total computational time amounts to 5.7 seconds. This relatively shorter duration reflects the efficient processing of a lower number of transactions within each block. However, as the number of blocks mined increases to 25 while maintaining the same transaction rate of 10 transactions per block, the total computational time escalates to 8.214 seconds. This increase in computational time can be attributed to the cumulative effect of processing a larger volume of transactions across a higher number of blocks. This trend underscores the importance of optimizing transaction processing efficiency within blockchain networks, especially as the scale of transactions and network activity grows. It highlights the need for scalable solutions and resource management strategies to ensure the continued performance and reliability of blockchain systems. By understanding and analyzing the relationship between transaction volume, block size, and computational

time, blockchain developers and network operators can make informed decisions to enhance the efficiency and scalability of their systems, thereby facilitating seamless transaction processing and network operation.

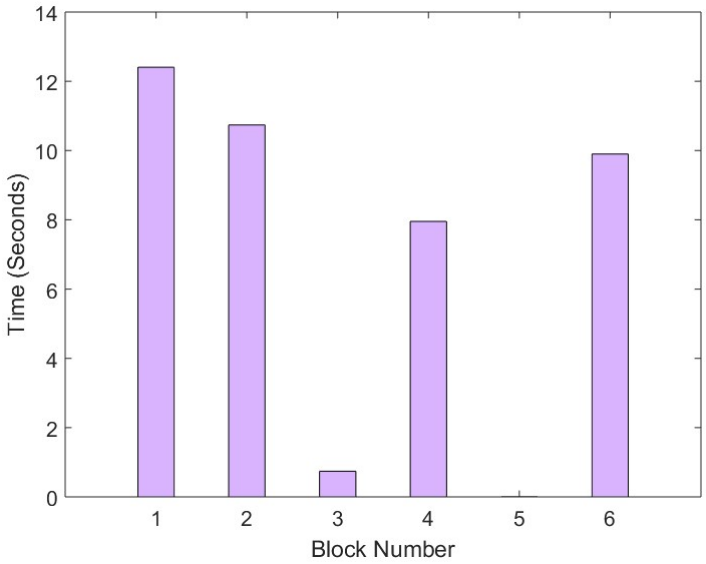

Figure 3: Block mining time

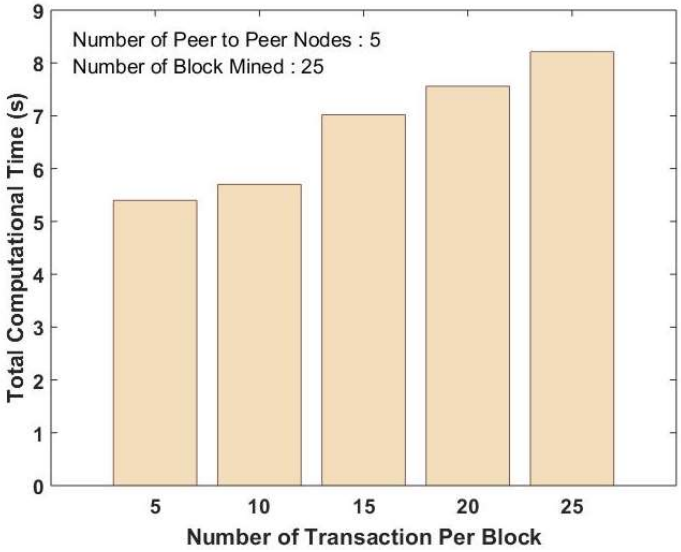

Figure 4: Analyzing Total Computational Time in Relation to Number of Transactions per Block

5. Conclusion

In this paper, we have addressed the challenges associated with traditional honeypot architectures in cybersecurity by proposing a novel approach that leverages blockchain technology. Our research introduces a distributed honeypot system designed to enhance security and resilience against malicious activities. By integrating blockchain's immutability, decentralization, and transparency features, we establish a robust defense mechanism against sophisticated cyber threats. The architecture of our distributed honeypot system utilizes blockchain mechanisms for secure data storage, tamper-resistant logging, and consensus-based decision-making, thereby mitigating risks associated with centralized management and single points of

failure. Through experimental validation and analysis, we have demonstrated the effectiveness and efficiency of our solution in detecting and mitigating cyber threats. By distributing honeypot instances across the blockchain network, our approach provides a resilient defense against attacks. In conclusion, our research contributes to the advancement of cybersecurity paradigms by harnessing the potential of blockchain technology to fortify honeypot deployments, thereby addressing the evolving challenges posed by cyber threats.

References

1. Mairh, Abhishek, Debabrat Barik, Kanchan Verma, and Debasish Jena. "Honeypot in network security: a survey." In *Proceedings of the 2011 international conference on communication, computing & security*, pp. 600-605. 2011.
2. Amal, M. R., and P. Venkadesh. "Review of cyber attack detection: Honeypot system." *Webology* 19, no. 1 (2022): 5497-5514.
3. Bao, Jian, Chang-peng Ji, and Mo Gao. "Research on network security of defense based on Honeypot." In *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, vol. 10, pp. V10-299. IEEE, 2010.
4. Negi, Poorvika Singh, Aditya Garg, and Roshan Lal. "Intrusion detection and prevention using honeypot network for cloud security." In *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, pp. 129-132. IEEE, 2020.
5. Gad, Ahmed G., Diana T. Mosa, Laith Abualigah, and Amr A. Abohany. "Emerging trends in blockchain technology and applications: A review and outlook." *Journal of King Saud University-Computer and Information Sciences* 34, no. 9 (2022): 6719-6742.
6. Guo, Huaqun, and Xingjie Yu. "A survey on blockchain technology and its security." *Blockchain: research and applications* 3, no. 2 (2022): 100067.
7. Bhutta, Muhammad Nasir Mumtaz, Amir A. Khwaja, Adnan Nadeem, Hafiz Farooq Ahmad, Muhammad Khurram Khan, Moataz A. Hanif, Houbing Song, Majed Alshamari, and Yue Cao. "A survey on blockchain technology: Evolution, architecture and security." *Ieee Access* 9 (2021): 61048-61073.
8. Amal, M. R., and P. Venkadesh. "Review of cyber attack detection: Honeypot system." *Webology* 19, no. 1 (2022): 5497-5514.
9. Franco, Javier, Ahmet Aris, Berk Canberk, and A. Selcuk Uluagac. "A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems." *IEEE Communications Surveys & Tutorials* 23, no. 4 (2021): 2351-2383.
10. Liu, Gao, Huidong Dong, Zheng Yan, Xiaokang Zhou, and Shohei Shimizu. "B4SDC: A blockchain system for security data collection in MANETs." *IEEE transactions on big data* 8, no. 3 (2020): 739-752.
11. Sun, Shuang, Rong Du, Shudong Chen, and Weiwei Li. "Blockchain-based IoT access control system: towards security, lightweight, and cross-domain." *IEEE Access* 9 (2021): 36868-36878.
12. Berdik, David, Safa Otoum, Nikolas Schmidt, Dylan Porter, and Yaser Jararweh. "A survey on blockchain for information systems management and security." *Information Processing & Management* 58, no. 1 (2021): 102397.
13. Martino, Raffaele, and Alessandro Cilardo. "Designing a SHA-256 processor for blockchain-based IoT applications." *Internet of Things* 11 (2020): 100254.