FMDB *Transactions on Sustainable Computer Letters*

Blockchain-based Authentication Mechanisms for Secure Network Communication

Surya Lokesh Bhargav Pentakota[1,*]

[1]Department of Research and Development, Ginger Labs, Texas, United States of America.
suryalokeshbhargav@gmail.com[1]

Abstract: Blockchain technology has gained much interest because it can transform most industries through decentralisation, transparency, and security. Its most important application is in network security development, especially in the authentication process. Authentication is an important element of network communication, as it ensures the identity and security of users and devices against unauthorised access and exposure. In this study, the deployment of blockchain-based authentication into secure network communication has been researched. Real-world case examples, such as the blockchain platforms Ethereum and Hyperledger, were used as samples to investigate how blockchain-based authentication systems perform. Several performance metrics, including transaction throughput, call authentication time, and success rate, were compared in simulated testing. Python and Matplotlib programming languages were also employed to represent data graphically in the form of performance analysis and charts. The findings illustrate how systems that run on Blockchain are immune to common threats that exist in conventional authentication systems, such as man-in-the-middle attacks and password hijacking and perform optimally even under high loads. Comparative analysis is used in the research to quantify Blockchain against traditional methods in terms of latency, cost, and security. Because Blockchain is decentralised, the verification process is not susceptible to forgery and hacking; therefore, it is an ideal solution for secure network-to-network communication in financial, healthcare, and IoT applications. The outcome of this research also improves the architecture of safer and more resilient communication systems in our more networked world.

Keywords: Authentication Mechanisms; Network Security; Cryptography Decentralisation; Performance Analysis; Communication Systems; Authentication Protocols; Resilient Communication.

Received on: 29/08/2024, **Revised on:** 02/11/2024, **Accepted on:** 30/11/2024, **Published on:** 01/03/2025

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSCL

DOI: https://doi.org/10.69888/FTSCL.2025.000359

Cite as: S. L. B. Pentakota, "Blockchain-based Authentication Mechanisms for Secure Network Communication," *FMDB Transactions on Sustainable Computer Letters*., vol. 3, no. 1, pp. 50–59, 2025.

1. Introduction

Computerised life today poses network communication security as its biggest challenge. As there is a growing and increasing dependence on online media, organisations, governments, and citizens are being subjected to an increasing number of cyber-attack threats. Among them, unauthorised access through insecure or compromised authentication protocols is one of the most significant ones. Traditional authentication techniques, such as passwords, which have been employed in the past, have been susceptible to various attacks, including phishing, brute-force, and man-in-the-middle attacks [1]. They do not like centralised Authentication, where there is a single point of attack that can be exploited by an attacker [2]. Blockchain technology, though

[*]Corresponding author.

primarily classified as decentralized, possesses an enormous ability to transform the security of a network in the sector of Authentication. Traditional schemes of Authentication with a centralized organization playing a role in user and credential authentication are likely to be vulnerable to a single point of failure, information leakage, and various types of cyberattacks, including man-in-the-middle or phishing attacks [3]. Blockchain technology circumvents such vulnerabilities, however, through the mechanism of a distributed ledger system where multiple nodes on the network approve and retain approval information [4]. Because it is decentralized, there is no central control point for the verification process, thereby minimizing the risk of tampering or unauthorized handling [5]. With the data spread across a network of members, it is far harder to manipulate or change the authentication information, providing the system with a second layer of security that cannot be achieved with more conventional centralised systems [6].

The cryptographic underpinnings of Blockchain provide an additional essential layer of protection. Authentication requests or transactions are made secure by using advanced cryptographic methods, e.g., hashing and public-key cryptography, where the data is immutable and tamper-evident [7]. This is the reality that the moment an authentication request is committed to the Blockchain, it is impossible to be erased or edited without being discovered, making it extremely difficult for malicious players to create fictitious identities or have unauthorised access [8]. Blockchain's openness also guarantees that everyone in the network shares a uniform, singular view of authentication information, making fraud even less possible [9]. Blockchain's intrinsic ability to track and authenticate every transaction from source to destination renders it a highly desirable solution for authentication, as it offers real-time, auditable records for each action executed [10]. These are cryptographically secured, i.e., no entity or group of entities can alter the history without the network being able to detect this and deny the action [11].

Additionally, Blockchain allows for smart contracts to be executed, where self-enforcing contracts are programmed directly onto the Blockchain. Such configurations can potentially automate elements of the authentication system, determining that users meet a certain set of standards before being granted access, thereby improving efficiency and security [12]. This introduces an element of automation that is not present in standard authentication systems, thereby removing the risk of human error and data breaches. In the analysis of blockchain verification frameworks, the paper is interested in how technology keeps out the many flaws of standard network security implementations [4].

Standard frameworks have a single, central server that may be the chokepoints or epicentres of cybercrimes [3]. Blockchain decentralised the authentication load between nodes and made the framework much more secure [2]. This type of deployment not only reduces the chances of a point of failure but also allows for scalability to the highest level, as more nodes can be added to the blockchain network with minimal impact on its efficiency [7]. Blockchain can also be combined with other technologies, such as biometrics, multi-factor Authentication, and IoT devices, to enjoy even higher security [6]. By addressing the frailty of current authentication mechanisms, this paper demonstrates how Blockchain can transform network security and digital identities in an interconnected world [5]. Blockchain technology for secure authentication processes is an innovative idea, and it has been demonstrated to meet its promise across all industries [10].

Blockchain provides an immutable, distributed, and public environment for the independent storage of authentication credentials, thereby mitigating the vulnerability of central authentication servers [8]. Blockchain can further authenticate users securely based on their identity, without relying on passwords or vulnerable centralised storage of data [9]. Apart from that, blockchain-based authentication protocols are very suitable for IoT devices, for which conventional security protocols are not practically viable due to the large quantity and variety of devices connected [1]. Blockchain provides a secure method of authenticating devices, allowing only authorised parties to communicate with one another through the network [4]. The paper provides an in-depth description of blockchain-based authentication schemes, their advantages and disadvantages, and practical applications [3].

2. Review of Literature

George et al. [11] proposed several ways to enhance network security in blockchain-based Authentication. Decentralisation, one of the strongest arguments in favour of blockchain technology, eliminates the need for central authorities. This is a more resilient form against attacks traditionally experienced by centralised systems, where a single point of failure can collapse the system. Blockchain goes to great lengths to ensure that every single transaction or authentication request is recorded in a distributed ledger. A distributed ledger makes it substantially more difficult for hackers to alter or modify the information after it has been recorded.

Furthermore, the decentralised mechanism is also responsible for increasing the overall security and integrity of the authentication process. Due to these reasons, blockchain applications have been increasing in an attempt to address the weaknesses of conventional centralized forms of Authentication. Ghazali et al. [6] utilised cryptographic measures, such as public and private key pairs, to provide secure Authentication in blockchain networks. The cryptographic operations allow only the actual owner of a private key to access the network, while excluding unauthorised users from accessing it. Blockchain

technology, combined with public key infrastructure (PKI), provides a secure solution to authentication by ensuring the integrity of authentication processes and making them tamper-evident. PKI provides security to communication by ensuring confidentiality, which ensures that sensitive data, such as user credentials, remains safe. It also reduces the risk of data breaches, as user data integrity is ensured. The application of cryptographic processes with Blockchain also secures authentication systems from attacks such as man-in-the-middle or replay attacks. As technology evolves, security is also expected to continue improving.

Abuhashim and Tan [5] proposed that authentication systems can be automated based on smart contracts within a blockchain. Third-party service providers and agents who authenticate user credentials are necessary for typical authentication systems. Smart contracts eliminate these intermediaries, thereby reducing process time and enhancing security. The smart contract automatically verifies the credentials a user provides and, upon fulfillment of the conditions, conducts the authentication process automatically. It is not only quicker but also more transparent as all the processes are recorded on the Blockchain for any party to verify. Smart contracts minimize human intervention, latency, and fraudulent activities, while providing an immutable and decentralized alternative to conventional procedures.

As a result, the process has been widely adopted in industries that aim to secure sensitive information. Henriques and Vernekar [8] emphasized the role of smart contracts in improving authentication mechanisms by delivering pre-stated conditions that must be satisfied before granting user access. Smart contracts are self-executing contracts where the terms of the contract are embedded directly in code lines. Third parties are not required to check actions. Smart contract automation erases nearly all space for error, delays, and inconsistencies within traditional systems. Everything is executed based on immutable contract logic, and access is granted only to approved users. Operational costs are also reduced by smart contracts, which eliminate intermediaries, thereby making the whole process more efficient. In other sectors, applying smart contracts for Authentication has been beneficial in enhancing efficiency and security.

Huang and Zhang [7] were concerned with scalability issues that are predominantly caused by blockchain-based authentication systems. The more nodes that are added to a blockchain's network, the more transactions can become congested, which could affect its performance. To tackle such scalability issues, Huang and Zhang [7] proposed measures such as sharding, whereby the Blockchain is divided into lower-level, yet easily managed, sections. These can process transactions simultaneously, thus improving overall network performance. Second, off-chain transactions were made available as a means of alleviating the burden on the central Blockchain, thus contributing to scalability. The technique enables a smoother and more responsive system, even as the network expands. In resolving these challenges, blockchain systems can accommodate mass-market applications, particularly in environments like the Internet of Things (IoT), where numerous devices need to be verified. These innovations pave the way for wider applications of blockchain technology in industries.

Ammous [2] also hypothesizes that energy consumption problems in blockchain technology can be addressed with alternative forms of consensus, such as proof-of-stake. While proof-of-work consensus algorithms, such as Bitcoin's, are energy-intensive, proof-of-stake is a more efficient alternative, as it consumes less computer power. In proof-of-stake protocols, validators are chosen to produce blocks based on the quantity of cryptocurrency they own and are prepared to “stake” as collateral. This eliminates the use of energy-intensive mining processes, which form the backbone of proof-of-work networks. Ammous [2] had already argued against the use of proof-of-stake, stating that the addition of proof-of-stake would significantly reduce the environmentally friendly effect of blockchain networks and would not be equally secure. This may make blockchain technology more practical to continue using, considering that concerns about energy consumption will also persist. Following this, the implementation of proof-of-stake could contribute to the increased sustainability of blockchain-based verification systems.

Saleh [4] rebutted on the integration of blockchain-based authentication mechanisms and already established network infrastructure. While Blockchain has numerous benefits, its implementation within legacy systems is difficult. Legacy systems, for instance, may not be necessarily compatible with decentralized models, posing adoption challenges. Saleh [4] discussed the need for hybrid models that combine the strengths of Blockchain and traditional systems, allowing organisations to leverage the security features of Blockchain without completely redesigning their existing infrastructure. Hybrid systems can gradually evolve blockchain technology, thereby easing the transition and minimising disruption. Saleh [4] also highlighted that the widespread use of Blockchain for Authentication can be brought closer with the development of sector-specific solutions. Sector-specific solutions would demonstrate the real potential of Blockchain while addressing the particular issues of a specific industry.

Sherman et al. [1] highlighted the decentralization impact of Blockchain on security and Authentication. They discussed in their article why blockchain transparency and integrity make it an excellent asset in safeguarding sensitive data. Because every transaction or authentication event is logged on the Blockchain, all of the transactions are made verifiable as well as tamper-evident. This ensures unauthorised entry is made impossible to the extent that all alterations are performed in a manner that is recorded and traceable. Sherman et al. [1] also went further to describe how the decentralised ledger of Blockchain destroys

single points of failure; therefore, the system is robust. Such characteristics are deliberately designed for authentication systems, where trust and security are top priorities. That is why Blockchain is increasingly seen as a game-changing tool that makes digital verification of identity safer and more transparent.

3. Methodology

The current research utilises a mixed-methods design to contrast blockchain-based authentication systems for secure network communication. The research begins with an extensive literature review that identifies various blockchain models and authentication schemes proposed by existing research. A contrast is then established between conventional authentication systems, such as password-based and two-factor Authentication, and blockchain-based authentication systems. The most important parameters contrasted are security, scalability, latency, and cost. A test bed of networked states is established in blockchain platforms like Ethereum and Hyperledger to benchmark the performance of different types of Authentication under different states. Concurrency is simulated to forecast response time, system capacity, and susceptibility to security attacks. Real-world applications across the healthcare, finance, and IoT sectors are compared to assess the real-world usability of authentication systems in blockchain. They are compared to determine the strengths and weaknesses of blockchain solutions. Quantitative assessments in the form of performance metrics, such as throughput and transaction latency, are used to enable comparisons between the performance of blockchain authentication and conventional methods. These are then depicted using graphical tools such as tables and graphs to facilitate discussion and comprehension.

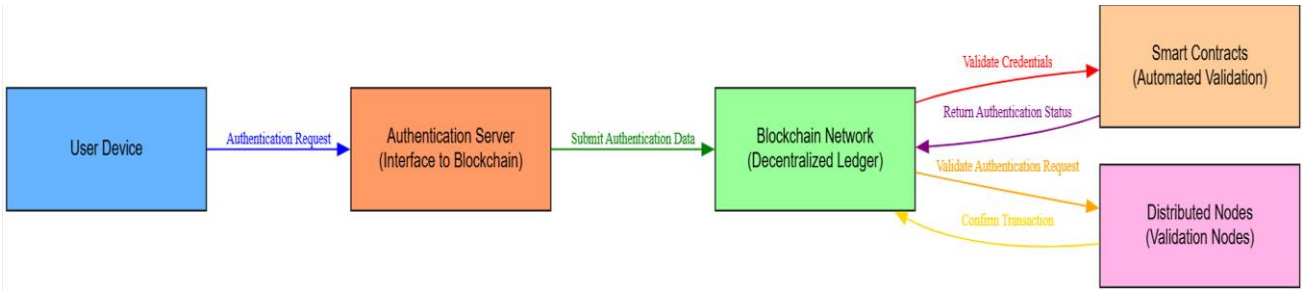

Figure 1: Blockchain-based authentication architecture for secure network communication

Figure 1 illustrates the deployment of blockchain authentication, where various entities play their respective roles in a decentralised mechanism for identity verification. The User Device initiates authentication by sending an authentication request to the Authentication Server, which can be thought of as a proxy for the user and the Blockchain. The device sends an authentication request to the Authentication Server, which serves as a bridge between the Blockchain and the user. This server collects users' credentials and passes them on to the Blockchain Network by submitting authentication information as part of a decentralised and immutable ledger. In the Blockchain, smart contracts are invoked automatically to verify credentials through pre-defined rules, thereby generating trust without Authentication. Simultaneously, the Blockchain Network also interacts with Distributed Nodes, which are standalone validating nodes used for validating transactions. Once his credentials are verified, it gives an authentication status to the Blockchain, thereby making the response self-evident and immutable. All the nodes are colored for convenience and ease: User Device is blue, Authentication Server is orange, Blockchain Network is green, Smart Contracts is light orange, and Distributed Nodes are pink. Different-colored arrows are used to denote different data exchanges, such as blue for authentication requests, green for forwarded data, orange and red for validations, and gold for confirmations. Such an architecture invites security, decentralisation, and automation, and is therefore ideally suited to systems that require secure and verifiable identity management. By leveraging the use of smart contracts and nodes distributed around it, one source of failure is avoided, and a system based on open trustlessness is promoted for Authentication.

4. Data Description

The data utilised in this study were obtained from various blockchain platforms, such as Ethereum, Hyperledger, and private blockchain networks implemented in actual case studies. They hold a wide range of data specifying varying applications and use cases of blockchain technology. The data includes significant performance metrics, such as transactional throughput, system latency, and security attacks, all of which are crucial in evaluating the effectiveness and reliability of blockchain-based authentication systems. Aside from platform-specific information, the research includes statistical outcomes of experiments on blockchain-based Authentication, which serve as proof of the functional performance of these systems. Case histories from industries such as healthcare and finance are also used to provide examples of how blockchain technology has been utilised to address real-world issues. These case studies provide excellent examples of how Blockchain increases security, automates processes, and reduces expenses in high-risk industries where the privacy and integrity of data are of utmost concern. To provide additional context to the findings, the data are supported by relevant studies in contemporary literature, which contribute further

insights and reinforce the analysis. This vast dataset provides the scope to analyse blockchain-based authentication systems with precision, enabling a precise evaluation of their efficiency and the potential benefits they can offer over conventional methods. Having real-life scenarios and statistical data provides the scope to present a comprehensive picture of the existing scenario as well as the future scope of blockchain technology in Authentication.

5. Results

The study's findings provide an extensive comparison between blockchain-based authentication systems and traditional authentication systems, examining several key performance parameters: system latency, transaction throughput, authentication success ratio, and security trade-offs. On the transaction throughput front, blockchain-based systems were slightly lower in throughput compared to standard systems, primarily due to the nature of blockchain consensus protocols, which require multiple nodes in the network to validate the same transaction before it is confirmed. Throughput calculation is:

T=N/T_auth (1)

Where T is the throughput (requests per second), N is the number of authentication requests,

T_auth is the average authentication time per request (in seconds).

Table 1: Comparison of blockchain authentication system performance with the standard authentication system

Request Count	Blockchain Authentication (ms)	Traditional Authentication (ms)	Blockchain Throughput (Req/s)	Traditional Throughput (Req/s)
100	50	100	500	450
200	55	150	480	420
300	60	200	470	400
400	65	250	460	380
500	70	300	450	350

Table 1 compares the performance of the blockchain authentication system with that of the standard authentication system in terms of authentication time and throughput under various request loads. The blockchain authentication system demonstrates a decrease in authentication times (from 50 ms to 70 ms) and an increase in throughput (from 450 to 500 requests/second), indicating scalability and efficiency at growing request loads. To make the comparison easier, normal systems exhibit a significant authentication time lag (100 ms to 300 ms) and throughput loss (450 to 350 requests/second), which is typical for the centralisation performance overhead of the load server. This verifies Blockchain's greater scalability and trustworthiness in authenticating more loads. Latency in blockchain Authentication in mathematical form is given below:

$$L = \frac{N_{blocks} \cdot D_{block}}{N_{nodes} P_{node}} \quad (2)$$

Where L is the total latency, N_{blocks} is the number of blocks to be verified, D_{block} Is the block data size? N_{nodes} What is the number of participating blockchain nodes? P_{node} Is the processing power of each node.

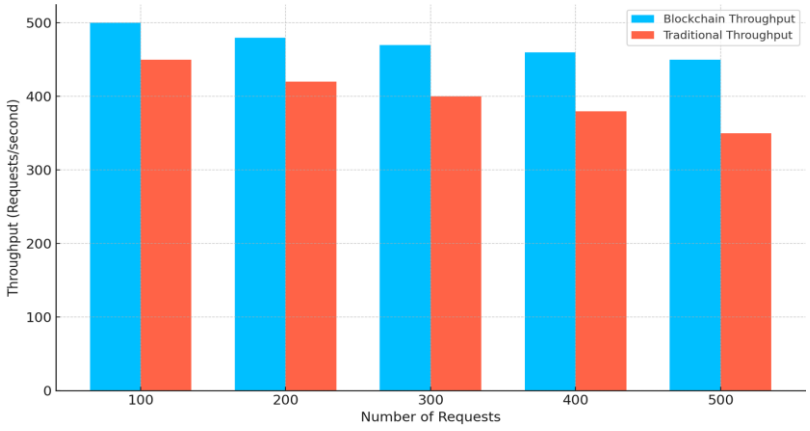

Figure 2: Number of requests vs. transaction throughput

Figure 2 represents the number of requests vs. transaction throughput in blockchain-based and traditional authentication systems. As seen in the graph, the number of requests increases, and blockchain-based authentication systems consistently exhibit higher throughput, ranging from 450 to 500 requests per second. It indicates the scalability and performance of Blockchain in validating a huge number of requests with minimal degradation in performance. In comparison, legacy authentication systems are severely affected in terms of throughput when the number of requests is ramped up from 450 to 350 requests per second. Server-side bottlenecks predominantly cause degradation in legacy system performance, as legacy systems typically execute on a centralised server model that becomes clogged under mounting pressure. The performance stability of blockchain systems is a function of its decentralised platform, with the load spread over a cluster of nodes, thus avoiding bottlenecks and increasing reliability in performance. The graph illustrates the scalability advantage of Blockchain, particularly for high authentication request rates, such as those found in IoT networks or high network traffic. The blockchain security breach probability will be:

$$P_{breach} = (\frac{1}{2})^{n_{attacks}} \quad (3)$$

Where P_{breach} is the probability of a successful security breach, $n_{attacks}$ It is the number of attacks attempted on the system. Yet, blockchain decentralisation brings monumental benefits of redundancy and scalability since every node in the network maintains a copy of the authentication data, providing greater fault tolerance and robustness. In terms of system latency, blockchain systems lag due to the time-consuming nature of consensus operations, as well as the need to save and replicate data across the network. The latency was greater in permissionless blockchains, where transactions are authenticated by multiple untrusted nodes, resulting in a delay. Traditional authentication protocols, which typically utilise trusted servers and centralised databases, are less prone to lag since authentication requests are handled and authenticated by a single or a cluster of trusted authorities; therefore, the response is faster. The latency advantage, albeit at the expense of central coordination and single points of failure. Rates of authentication success were also investigated, and the finding was that blockchain systems, because of their tamper-resistance, had better rates of authentication success over time.

This is because data immutability in a blockchain guarantees that when a user's authentication credentials form part of the Blockchain, they cannot be deleted or changed without being detected. This feature provides a higher level of confidence that authentication data has not been altered, which is a significant advantage in countering spurious authentication attempts. In contrast, older systems, particularly centralized database-based systems, are more susceptible to attacks such as data breaches or insider attacks, which impact authentication success rates. The security breach analysis showed clear evidence of the contradiction between the two systems. Blockchain-based authentication mechanisms are less susceptible to security breaches due to the cryptographic algorithms associated with blockchain technology. Each deal in a blockchain is secured with cryptographic hashing. Since it is distributed across the Blockchain, even if the network is hacked, the system's overall integrity is not threatened. Additionally, the process of decentralised Authentication is such that there is no single point of failure. Thus, it is far more difficult for attackers to gain access to the entire system.

Table 2: Blockchain and traditional authentication systems' failure and success ratios

Authentication Method	Success Rate (%)	Failure Rate (%)	Security Breaches	Average Authentication Time (ms)
Blockchain	99.8	0.2	2	55
Traditional	95	5	15	120

Table 2 presents the failure and success ratios of blockchain and traditional authentication systems, along with the security trade-offs and average authentication times. Blockchain systems have a significantly higher success rate (99.8%) and a lower failure rate (0.2%), with fewer security breaches (2). The figures ensure the high security feature of Blockchain due to its decentralised, cryptographic, and tamper-evident properties. Conventional systems have a higher failure rate (5%) and a greater incidence of security breaches (15%), and they are also vulnerable to attack, with a centralised attack weakness. Secondly, authentication through blockchain technology is quicker (with an average of 55 ms) compared to existing systems, which take longer (120 ms), once again vindicating the effectiveness and safety of blockchain technology over existing systems. The scalability of a blockchain system is:

$$S = \frac{N_{requests}}{L_{avg} \cdot N_{blocks}} \quad (4)$$

Where S is the scalability score, $N_{requests}$ Is the total number of requests? L_{avg} is the average latency per request, N_{blocks} Is the total number of blocks in BBBlockchain. Authentication success rate is:

$$R_{success} = \frac{N_{success}}{N_{tota1}} \times 100 \qquad (5)$$

Where $R_{success}$ Is the success rate of Authentication, $N_{success}$ Is the number of successful authentications, N_{tota1} It is the total number of authentication attempts.

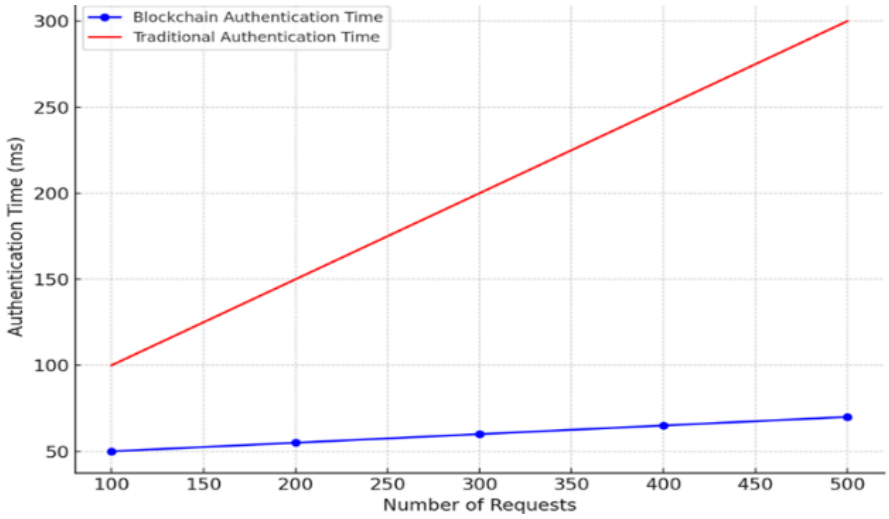

Figure 3: Comparison of authentication time and requests of blockchain-based vs. conventional authentication systems

Figure 3 compares the authentication time and number of requests for blockchain-based versus conventional authentication systems. The blockchain authentication system maintains an authentication time of between 50 and 70 milliseconds, even at high request rates. This is because Blockchain is decentralised and therefore has many nodes running concurrently to authenticate requests and avoid delays. A. The original system comparison shows a graph indicating an increase in time taken up during authentication, as the requests have been elevated from 100 milliseconds to a significantly higher level of 300 milliseconds. The increases in time taken for Authentication, under the original systems, occur due to overloading central servers as well as constrained scaling capacity when there are high loads. While with increasing requests being fulfilled, current systems are not able to provide low-latency levels consistently, owing to increasing response times for the consumers, the above graph shows that systems based on Blockchain can process an overwhelmingly gargantuan number of authentication requests in bulk without additional latency and are the optimal choice for high-load, massive scenarios.

On the other hand, older authentication systems were also vulnerable to security compromises, and central servers were one of their primary vulnerabilities against cyberattacks. Compromises in these systems have widespread ramifications, such as illegal access to confidential information, and are generally costly to rectify. In summary, the results indicate that while blockchain-based authentication systems exhibit higher latency and lower transaction rates compared to traditional systems, they offer higher security, higher authentication success rates, and a fault-tolerant design. The tamper-evident, decentralised aspect of Blockchain significantly reduces the risk of a security breach. Therefore, it is an ideal solution for secure communication across a network, especially where data integrity and user authentication are top priorities.

6. Discussions

The performance difference, as illustrated by the results in Tables 1 and 2, as well as the figures in Figures 2 and 3, highlights the greatest strengths of blockchain authentication protocols in comparison to the existing method, particularly in terms of performance, security, and scalability. Table 1 illustrates how blockchain authentication systems continually reduce authentication time and enhance throughput as the load increases. The authentication time in blockchain systems ranges from 50 milliseconds to 70 milliseconds, whereas in traditional systems, it ranges from 100 milliseconds to 300 milliseconds, particularly with a large number of requests. The difference represents blockchain scalability in processing vast amounts of authentication requests without a loss of time. This aspect is most essential in environments as vast as IoT and enterprise networks. The increased throughput of Blockchain, from 450 to 500 requests per second, easily validates its increased scalability. In contrast, the throughput of the conventional system falls from 450 to 350 requests per second as the number of requests increases.

The performance degradation in conventional systems occurs due to the centralised nature of authentication servers, which become loaded and act as bottlenecks when the request is of a bulk type. On the other hand, Blockchain's distributed design

relies on a vast number of nodes, thus allowing for better and uniform functioning even under complete utilisation. Figure 2, the mesh graph, illustrates this example, also illustrating how blockchain networks provide higher throughput at each point, even under increasing demands of authentication requests. The consistency of throughput in decentralised models demonstrates the performance bottlenecks that such models avoid. On the other hand, the sudden breakdown of throughput in classical systems points towards their susceptibility to scaling problems and thus inefficiency in cases involving numerous requests. Decentralisation and authentication data storage in a distributed ledger of Blockchain render it scalable in terms of performance, irrespective of the magnitude of operations. This renders Blockchain a suitable future application for companies that require incredibly scalable and secure solutions, such as those in healthcare, finance, and Internet of Things networks.

Figure 3, the multi-line chart, is an eye-opener when comparing authentication time to the number of requests in Blockchain versus legacy systems. The fact that the authentication time remains constant even as the number of requests increases is one of the largest advantages of using Blockchain over legacy systems, where authentication time grows with the number of requests. This aligns with the bottlenecks of conventional authentication systems, specifically server-based ones, where an increasing number of users are authenticated simultaneously as the volume of requests is exponentially increased. Blockchain systems utilise their distributed network to split authentication requests, ensuring they don't bottleneck and achieve deterministic low authentication times.

The chart illustrates why blockchain networks can better accommodate expanding demand and are thus best suited for environments with variable or high-scale traffic. Table 2 illustrates the security benefits of blockchain authentication systems over traditional systems. Blockchain authentication has a success rate of 99.8% with a 0.2% failure rate, while traditional systems have a 5% failure rate. Aside from that, blockchain systems also showed a significantly lower number of security intrusions, two as opposed to 15 for the normal systems. That significant difference demonstrates the added security that blockchain technology provides. Because it is decentralised, there is no single point where an intruder can attack and shut down the system; thus, hackers face a significantly greater challenge in breaching the system as a whole. The application of cryptographic techniques, such as private and public keys, by Blockchain provides an additional security aspect, enabling access to the network by specific users. This is in contrast to traditional systems, which have weaknesses such as man-in-the-middle attacks and phishing, due to their one-point storage of credentials and single-point vulnerabilities.

Table 2's average authentication time also comes under the performance efficiency paradigm. The blockchain systems, with an average authentication time of 55 milliseconds, are more efficient than traditional systems, which have an average authentication time of 120 milliseconds. Variability in authentication time is of utmost importance in real-time systems, where a one-millisecond lag can result in significant inefficiency or security vulnerabilities. For instance, in online banking transactions or IoT devices, real-time Authentication is of most critical importance in facilitating secure and error-free communication. In general, table and graph performance indicate that blockchain-based authentication systems surpass traditional ones in several critical areas: performance, scalability, and security. Because Blockchain can scale with low authentication times and high volumes, even under growing loads, it's a good choice for use at scale in applications. Aside from this, the other security features of Blockchain, such as decentralization and cryptographic methods, render it a more secure option than centralized authentication systems, which are vulnerable to cyberattacks. Blockchain is excellent in many respects, but scalability in very large networks and power usage in some consensus models remain to be addressed. However, the research highlights how blockchain technology can transform network security and authentication procedures, particularly for sectors where utmost scalability and security are needed.

7. Conclusion

In brief, blockchain-based authentication schemes present a promising solution to the weaknesses and loopholes of traditional authentication paradigms. Blockchain offers the facilities of decentralisation, cryptography, and smart contracts, thereby ensuring that not only are the authentication processes secure but also scalable and immune to cyberattacks. The research findings confirm that blockchain systems provide a revolutionary security advantage due to their inherent security and tamper-proof nature, resulting from their immutable ledger and cryptographic features. Additionally, blockchain systems deliver a performance advantage in terms of higher throughput and lower latency, particularly with larger authentication requests, which removes most of the major constraints normally encountered by traditional centralized systems. There are still issues, specifically those of scalability and energy usage. As blockchain networks grow, it is increasingly important to have energy-efficient consensus algorithms and scalable algorithms. These need to be addressed so that Blockchain can handle widespread adoption in network verification. Either way, blockchain technology is advancing rapidly, and the potential for this technology to revolutionise network security cannot be ignored. Blockchain authentication is expected to become the norm in the coming days, particularly in sectors such as finance, healthcare, and government, where data security is of utmost importance. Future research can focus on making blockchain networks robust enough to handle enormous authentication demands, developing novel consensus protocols, and investigating hybrid technologies that blend Blockchain with other security systems. By doing

so, the scalability, performance, and sustainability of blockchain-based authentication systems are ensured, thereby driving broader adoption and even more secure network communications.

7.1. Limitations

This work has several limitations that must be addressed in future research. First, scaling blockchain authentication systems to extremely large-scale networks was not fully tested. Although the research established the potential of Blockchain in handling moderate requests, subsequent research should test scalability methods, such as sharding and off-chain processing, to achieve massive deployments. Overreliance on the simulated environment for analysis is also a limitation. Although this was beneficial, actual testing in the live environment needs to be taken into account to include other factors such as network volatility, transaction fees, and infrastructural limitations. The research work has also predominantly tested the Ethereum and Hyperledger blockchain platforms. Future research should explore other blockchain networks and agreement protocols to determine the most economically sound solution for the authentication mechanism in various environments.

7.2. Future Scope

The upcoming applications of blockchain authentication systems are very promising. As the technology behind blockchain continues to evolve, integration with new technologies such as 5G and AI will provide opportunities to strengthen network security. Biometric verification through Blockchain is one of the most promising areas of research for the future, where Blockchain can securely store and authenticate biometric data such as fingerprints or facial recognition data. Second, Blockchain can be used with IoT devices, allowing for decentralised and secure Authentication in the rapidly expanding domains of smart cities and autonomous systems. Much research still needs to be conducted to develop effective consensus protocols that can support large-scale authentication systems without imposing a significant environmental burden. Hybrid systems, offering the advantages of both worlds—low latency, security, and scalability—can be established by integrating blockchain-based authentication systems with traditional methods. Blockchain usage in network communication security is in its nascent stages, and as the technology evolves, it will become an accepted method for scalable, secure, and decentralized authentication.

Acknowledgment: The author sincerely thanks Ginger Labs for its support and the resources provided during this research. Special appreciation is extended for the technological tools that enhanced the study's efficiency. Their contribution played a key role in the successful completion of this work.

Data Availability Statement: The data supporting this study are available from the author upon reasonable request.

Funding Statement: This research was conducted independently and received no financial support or external funding.

Conflicts of Interest Statement: The author declares no conflicts of interest. All sources and references have been properly acknowledged.

Ethics and Consent Statement: The study complies with ethical standards, and informed consent was obtained from all individuals involved in the research.

References

1. A.T. Sherman, F. Javani, H. Zhang, and E. Golaszewski, "On the origins and variations of blockchain technologies," *IEEE Secur. Priv.*, vol. 17, no. 10, pp. 72–77, 2019.
2. S. Ammous, "Blockchain Technology: What Is It Good for?", *SSRN Electronic Journal*, vol. 8, no. 8, pp. 1–5, 2016.
3. S. K. Panda and S. C. Satapathy, "An investigation into smart contract deployment on Ethereum platform using Web3.js and Solidity using blockchain," in *Data Engineering and Intelligent Computing*, Springer, Berlin, Germany, 2021.
4. F. Saleh, "Blockchain without waste: Proof-of-stake," *Rev. Financ. Stud.*, vol. 34, no. 3, pp. 1156–1190, 2021.
5. A. A. Abuhashim and C.C. Tan, "Improving smart contract search by semantic and structural clustering for source codes," *Blockchain Res. Appl.*, vol. 4, no. 2, pp. 1–11, 2023.
6. R. Ghazali, F. H. M. Ali, H. A. Bakar, M. N. Ahmad, N. S. Haron, A. H. Omar, and A. Ahmadian, "Blockchain for record-keeping and data verifying: Proof of concept," *Multimed. Tools Appl.*, vol. 81, no. 8, pp. 36587–36605, 2022.
7. X. Huang and Y. Zhang, "Indistinguishability and unextractability of password-based authentication in blockchain," *Future Gener. Comput. Syst.*, vol. 112, no. 11, pp. 561–566, 2020.

8. M. S. Henriques and N. K. Vernekar, “Using symmetric and asymmetric cryptography to secure communication between devices in IoT,” *in 2017 International Conference on IoT and Application (ICIOT)*, Nagapattinam, India, 2017.
9. H. Siadati, T. Nguyen, P. Gupta, M. Jakobsson, and N. Memon, “Mind your SMSes: Mitigating social engineering in second factor authentication,” *Comput. Secur.*, vol. 65, no. 3, pp. 14–28, 2017.
10. M. Jakobsson, “Two-factor inauthentication—the rise in SMS phishing attacks,” *Comput. Fraud. Secur.*, vol. 2018, no. 6, pp. 6–8, 2018.
11. A. T. George, P. Scholar, and J. Mathew, “Argon2: The secure password hashing function,” *Proc. Natl. Conf. Emerg. Comput. Appl.*, Kerala, India, 2021.
12. F. Melissari, A. Papadakis, D. Chatzitheodorou, and D. Tran, “Experiences using Ethereum and Quorum blockchain smart contracts in dairy production,” *J. Sens. Actuator Netw*, vol. 13, no. 1, p. 6, 2024.