IJEEMCS : International Journal of Electrical Engineering, Mathematics and Computer Science
Vol. 1, No.3 September 2024
e-ISSN: 3048-1945, p-ISSN : 3048-1910, Page 43-61
DOI: https://doi.org/10.62951/ijeemcs.v1i3.20
Available online at: https://international.arteii.or.id/index.php/IJEEMCS/==

Enhancing Security In Industrial IoT Through Blockchain-Based Authentication Mechanisms

Phiang Jun Kong[1], Vivian Yong Siew Yee[1], Hafizuddin bin Hilmi[1], Dedree Leonna Lai[1], Ng Ee Zoe[1], &Muhammad Faisal[2]

[1.] Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, 94200 Kota Samarahan, Sarawak, Malaysia
[2.] Human Resource Information Management System, Ministry of Human Rights, Pakistan;
76569@siswa.unimas.my, 74938@siswa.unimas.my, 77106@siswa.unimas.my, 77282@siswa.unimas.my, 76013@siswa.unimas.my, dr.faisalshabbir88@gmail.com

Address: Jln Datuk Mohammad Musa, 94300 Kota Samarahan, Sarawak, Malaysia
Author Corresprodence : 76569@siswa.unimas.my

Abstract. *The Industrial Internet of Things (IIoT) has revolutionized industrial processes, offering automation and data-driven decision-making. However, this interconnectedness brings new security challenges, especially in crucial infrastructure sectors. Traditional security measures are inadequate, leading to the exploration of innovative solutions. Blockchain technology has emerged as a promising solution due to its decentralized and immutable nature. This paper proposes a Hybrid Blockchain-Based Authentication Mechanism for IIoT, combining Delegated Proof of Stake (DPoS) and Elliptic Curve Cryptography (ECC). The hybrid architecture utilizes public and private blockchains to ensure scalability, efficiency, and security. Lightweight consensus algorithms, DPoS, are incorporated to optimize performance, while ECC provides efficient cryptographic techniques suitable for IIoTenvironments. An interoperable framework facilitates seamless integration with existing infrastructure, ensuring regulatory compliance and compatibility. Decentralized identity management further enhances security and privacy. Results and analysis demonstrate the effectiveness of the proposed solution, positioning hybrid blockchain architecture as the most suitable approach for enhancing security in IIoT environments.*

Keywords *: Industrial Internet of Things (IIoT), Blockchain technology, Authentication mechanism, Security, Hybrid blockchain, Delegated Proof of Stake (DPoS), Elliptic Curve Cryptography (ECC)*

1. INTRODUCTION

Industrial processes have received a major boost from the development of Industrial Internet of Things(IIoT), facilitating automation, efficiency, and data-driven decision-making. However, [1] highlighted that this interconnectedness also introduces new security challenges, as IIoT systems are often deployed in criticalinfrastructure sectors where a breach could have severe consequences. Traditional security mechanisms, such as centralized authentication systems, are proving inadequate to address the evolving threats landscape in IIoT environments, as emphasized by [2] and [3]. Hence, there is much incentive in exploring innovative approaches to enhance security in IIoT ecosystems.

Received: Juni 09, 2024; Revised: Juni 21, 2024; Accepted: Juli 12, 2024; Online Available: Juli 15, 2024;
** Phiang Jun Kong, 76569@siswa.unimas.my*

Originally created as the foundation for cryptocurrencies such as Bitcoin, as explained by [1], blockchain technology has shown promise in addressing security issues across a number of fields, including IIoT. According to [4] and [5], blockchain employs a decentralized network of computers to log transactions, creating a transparent and secure ledger that cannot be altered. It uses cryptographic techniques and consensus protocols to enable reliable and direct data transfers, cutting out intermediaries and reducing the risk of data tampering and system failures.

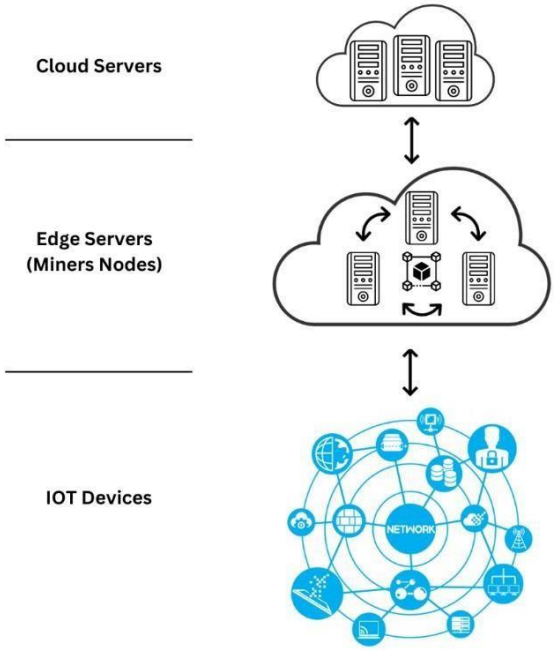

Figure 1: Standard structure of a blockchain- enabled environment for the Internet of Intelligent Things.[6]

Figure 1 illustrates a generic architecture for a blockchain-based authentication mechanism in an IIoTenvironment, as presented in [6, Fig. 3]. The figure depicts a network of IIoT devices connected to a blockchain network, where each device maintains its identity and transaction history on the blockchain. When a device initiates a transaction or seeks access to resources, it broadcasts a request to the blockchain network. Through consensus mechanisms, the network validates the transaction and updates the ledger, thereby ensuring the integrity and authenticity of the interactions.

The decentralized nature of blockchain helps to mitigate the severe privacy and security risks posed by centralized authentication schemes, as noted by [2], [4], [7], and [8]. With that said, the integration of decentralized authentication schemes using blockchain with IIoT

presents its own set of challenges and risks, which form the problem statements for this research. One of the primary concerns, as highlighted by [1] and [3], is the scalability and performance limitations of blockchain networks, especially when there is a large constant output of data from IoT devices. Additionally, the resource-intensive nature of blockchain consensus algorithms and cryptographic operations may introduce latency and overhead. Moreover, the inherent complexity of blockchain technology coupled with the diverse requirements of IIoT applications necessitates careful consideration of design choices to ensure easy interoperability of the authentication scheme with existing IIoT infrastructures. All these issues need to be addressed in order to realize the full potential of blockchain authentication in IIoT.

In this research, we aim to explore how blockchain-based authentication mechanisms can help to bolster security in IIoT environments while maintaining an acceptable level of performance efficiency. By investigating existing literature and case studies, we seek to identify the key challenges, risks, and effective approaches for incorporating blockchain technology into IIoT ecosystems. Furthermore, we intend to propose novel solutions and frameworks to address these challenges, ultimately contributing to the development of more secure and resilient industrial systems in the era of digital transformation.

2. RELATED WORK

A. Blockchain-Based Secure and Lightweight Authentication for Internet of Things

The Internet of Things (IoT) is rapidly growing, fuelled by continuous development and proliferation of communication devices. According to [1], security and privacy are significant concerns due to vulnerabilities like data tampering and identity spoofing, compounded by the limited processing capabilities of many IoT devices. The article proposes a "blockchain-based secure and lightweight authentication scheme" utilizing the Modular Square Root (MSR) technique. The solution enhances security, scalability, and authentication efficiency at the cost of increased latency and network management complexities due to blockchain reliance. The solution was assessed by implementing it on an Ethereum test network to evaluate practicality and efficiency, focusing on computation and communication costs.

B. *A Blockchain-Assisted Privacy-Aware Authentication Scheme for Internet of Medical Things*

According to [2], ensuring data security and privacy within Internet of Medical Things (IoMT) ecosystems is challenging due to diverse entities and networks. Existing authentication mechanisms for IoMT tend to depend on centralized infrastructures, leading to single points of failure and privacy vulnerabilities. The proposed solution is elliptic curve cryptography (ECC) for public-key cryptosystems, which utilizes the discrete logarithm problem (DLP) and computational Diffie–Hellman problem (CDHP) for secure key exchange. ECC offers a high level of security while being lightweight due to its relatively small key sizes. However, ECC implementation can be complex, which may introduce potential vulnerabilities if not implemented correctly. The proposed solution was assessed by examining resource utilization during cryptographic operations.

C. *Blockchain-based Device Identity Management with Consensus Authentication for IoT Devices*

The authors in [3] proposed a blockchain-based identity management approach with consensus authentication for IoT devices to enhance security against threats like fake nodes and identity theft. The scheme would be able to oversee device identity and authentication in a scalable manner by leveraging an unmanipulable ledger and a lightweight consensus-based authentication system. The results highlight the decentralized system’s scalability. The work addresses the limitations of existing authentication mechanisms for IoT devices, emphasizing the need for scalable solutions that reduce delays and computations. The proposed solution's scalability was assessed as the system expanded with more nodes. The evaluation also focused on the efficiency of the authentication process compared to traditional approaches, highlighting reduced delays and computations.

D. *Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network*

The authors in [4] explored blockchain technology's potential to secure distributed IoT networks, focusing on how blockchain's decentralized nature can enhance data management. IoT networks are vulnerable to security threats and need robust security solutions that

blockchain technology can potentially offer. The solutions proposed include using decentralized applications (DApps) and smart contracts for managing and securing IoT data transactions within blockchain frameworks. The solutions provide enhanced security, increased transparency, and reduced risks of tampering, but suffer from scalability issues and highenergy consumption. While specific metrics aren't provided, typical evaluation would include transaction speed, throughput, response times to security breaches, and effectiveness of data encryption methods.

E. *An Efficient and Privacy-Preserving Blockchain-Based Authentication Scheme for Low Earth OrbitSatellite-Assisted Internet of Things*

The authors in [5] proposed an authentication scheme suitable for IoT networks that use low earth orbit (LEO) satellites. Conventional lightweight authentication mechanisms use true identity information for certificates, which presents privacy concerns. The proposed solution is called blockchain-based authentication scheme (BC-Authen). This solution uses consortium blockchain and certificateless encryption, which preserves privacy by using pseudonyms for identity verification. However, the usage of a satellite communication system results in an inevitable transmission delay in the IoT network. The system’s security features, storage overhead, query time, and transmission time are used to evaluate its effectiveness.

F. *Authentication and Key Management in Distributed IoT Using Blockchain Technology*

The authors in [7] explored the challenges in securing interconnected devices due to their differences, limited resources, and the need for scalable security solutions. Existing security mechanisms are centralized, making them prone to scalability issues and security threats such as spoofing and data tampering. The proposed solution implements blockchain technology for IoT applications, focusing on authentication and key management. One-way hash chains offer efficient cryptographic security, while fog and cloud layers are implemented to optimize performance and scalability, allowing for efficient communication and management of IoT devices. However, this scheme is complex to implement and manage, and there are potential scalability challenges with large- scale deployments. The proposed scheme was evaluated by implementing it using smart contracts on the Ethereum platform that involves writing smart contracts in Solidity.

G. *Blockchain-Based Privacy-Preserving Authentication Model Intelligent Transportation Systems*

The rise of Intelligent Transportation Systems (ITS) necessitates improved data security and privacy.

[8] stated that ITS face significant security and privacy risks from centralized systems, highlighting the need for a decentralized approach. A Blockchain-based Privacy-Preserving Authentication (BPPAU) model is proposed, using blockchain to decentralize authentication. This reduces data breach risks and enhances security and privacy while being scalable for large networks. However, the model is complex to implement and maintain, and has high computational overhead. The model's performance was assessed using metrics such as transaction costs, transactions per second, and computational time, emphasizing efficiency and scalability.

H. *Efficient and Privacy-Preserving Blockchain-Based Multifactor Device Authentication Protocol for Cross- Domain IIoT*

As IIoT expands across domains, there is an urgent need for enhanced security for cross-domain communications. [9] observed that existing multifactor authentication systems are prone to attacks and struggle with efficiency and privacy in cross-domain settings. The solution is a blockchain- based multifactor authentication protocol, using hardware-assisted key derivation and an on-chain accumulator for efficient key management. The solution improves security and reduces blockchain storage overhead but is complex to implement and not easily scalable. The protocol was evaluated on storage overhead, authentication efficiency, and privacy maintenance, demonstrating balance between security and performance.

I. *BTAA: Blockchain and TEE-Assisted Authentication for IoT Systems Authentication Protocol for Cross-Domain IIoT*

The authors in [10] looked into developing a blockchain authentication scheme that is suitable for cross- domain IoT systems. Currently used blockchain- based authentication schemes for cross-domain contexts are vulnerable to being manipulated by malicious domain managers. The proposed solution for this is called blockchain and TEE-assisted authentication (BTAA). Shared management of the blockchain improves security, while TEE provides a secure space for code execution to prevent malicious interference. However, the use of TEE also results in additional computation overhead. This proposed solution was evaluated based on confidentiality, integrity, traceability, and computation and communication overhead.

J. *Towards A Lightweight Identity Management and Secure Authentication for IoT Using Blockchain*

According to [11], the Internet of Things (IoT) faces security challenges due to limited capabilities of devices, necessitating identity management and authentication schemes that are lightweight and secure. IoT networks require trustworthiness for secure communication, highlighting the need for blockchain-based solutions for identity management and authentication. This article proposed a system that authenticates cluster heads and monitor nodes internally using a private blockchain, and end-users using a public blockchain. The framework attempts to protect cluster head nodes from denial-of-service attacks by including a machine learning-based detection module. Blockchain systems enhance security by decentralizing device administration, ensuring immutability of data, and protecting against malicious changes. The authors used a Hyperledger platform to evaluate the proposed framework's security and compare its computation, storage, and energy metrics with similar blockchain-based identity management solutions.

K. *Other Contributions*

Several other researchers have also contributed in end-to-end security mechanism even with the assistance of the counter partners i.e. universities or industries for broaden implications [12-22]. This research article can act as the guidelines for future young researchers in end-to-

end security measures in 6th generation networks. This improved work (proposed solution) for the given problem statement is adopted from [1-11], which act as a benchmark for this research article.

3. PROPOSED SOLUTION

To address the limitations and challenges identified in the current authentication mechanisms for IIoT environments, we propose a Hybrid Blockchain-Based Authentication Mechanism using Delegated Proof ofStake (DPoS) and Elliptic Curve Cryptography (ECC). This proposed solution combines the strengths of both public and private blockchains, ensuring a scalable, efficient, and secure authentication process tailored specifically for IIoT applications.

The use of a hybrid blockchain that combines the characteristics of public and private blockchains hasalready been demonstrated by [11], and ECC's potential as a lightweight and secure encryption method has also been highlighted by [2]. Our proposed solution contributes to these blockchain authentication technologies by additionally incorporating DPoS as the consensus algorithm and Decentralized Identifiers (DIDs) for decentralized identity management. The overall blockchain authentication scheme is also designed to be easily interoperable with existing IIoT infrastructures through the help of smart contracts, application programming interfaces (APIs), and middleware.

A. Hybrid Blockchain Architecture

Our proposed scheme utilizes a hybrid blockchain architecture that leverages both public and private blockchains, which are DPoS and ECC. These two techniques are selected as both of them can be implemented in both public and private blockchains. The public blockchain is employed for global authentication, ensuring transparency and immutability of critical authentication data across the entire IIoT network. On the other hand, the private blockchain is implemented within industrial networks to handle local authentication processes. This dual-layer approach significantly reduces the data load on the public blockchain, enhancing scalability and performance by allowing faster and more efficient handling of local transactions [23] [24].

Table 1 below shows the comparison table of characteristics of hybrid blockchain architecture andtraditional blockchain architectures.

Feature	**Hybrid (DPoS + ECC)**	**POA**	**POW**	**POS**	**DIDS**
Security	High	Moderate	High	Moderateto High	High
Efficiency	High	High	Low	High	Moderate
Scalability	High	High	Low	Moderate	Moderate to High
Energy Usage	Low	Low	High	Low	Low
Decentralization	Moderate	Low	High	Moderate	High
Complexity	High	Low	High	Moderate	High
Governance	High	Low	Low	Moderate	High
Vulnerability	Moderate	High	Low	Moderate	Moderate

Table 1: Comparison table of characteristics of hybrid blockchain architecture and traditional blockchainarchitectures.

B. Lightweight Consensus Algorithms

To further optimize performance, our scheme incorporates lightweight consensus algorithms, specifically Delegated Proof of Stake (DPoS). DPoS is a consensus algorithm designed to improve the efficiency and scalability of blockchain networks while maintaining a level of decentralization. It is chosen for its ability to provide fast transaction speeds and lower resource consumption. It involves a small, selected group of nodes (delegates) that validate transactions, significantly reducing the computational overhead compared to traditional Proof of Work (PoW) or Proof of Stake (PoS) systems [25]. This choice of consensus

mechanism ensures that the authentication process remains efficient even as the network scales. This is crucial for authentication systems that require fast and reliable validation of identities and transactions.

DPoS enhances security in blockchain-based authentication. The DPoS consensus mechanism highly improves decentralization and the speed of block confirmation [26]. The election of delegates through a voting process adds a layer of security. Since delegates are chosen based on their reputation and trustworthiness within the network, the system is less susceptible to attacks and collusion, ensuring secure authentication. By having a limited number of delegates involved in transaction validation, DPoS reduces the attack surface. Fewer nodes mean there are fewer potential points of failure or targets for attackers, making the network more resilient against attacks. The rapid transaction validation process also minimizes the window of opportunity for attacaks such as double-spending, further enhancing the security of the authentication system.

Energy efficiency is a vital characteristic of DPoS over traditional PoW and PoS systems. Unlike PoW, which requires intensive computational work to solve complex mathematical puzzles, DPoS relies on a small group of elected delegates to validate transactions. This process consumes significantly less energy becauseit eliminates the need for continuous, high-power computations. Consequently, DPoS is much more energy-efficient, making it suitable for lightweight applications, such as authentication, where minimizing resourceconsumption is crucial.

Decentralization and flexibility are maintained in DPoS despite the centralization of delegate selection.While DPoS introduces a level of centralization by designating delegates, it still maintains decentralization by allowing stakeholders to vote for and replace delegates. This dynamic governance model ensures that thesystem remains flexible and can adapt to changing trust dynamics. Therefore, this enable DPoS to be selected as one of the techniques in the hybrid blockchain architecture instead of other traditional systems.

C. Efficient Cryptographic Techniques

Elliptic Curve Cryptography (ECC) is a highly efficient cryptographic technique that used in hybrid blockchain architecture with DPoS in this project. ECC offers robust security with smaller key sizes compared to traditional cryptographic methods like RSA. This

efficiency results in faster computations and reduced storage requirements. This makes it well-suited for IIoT environments where devices often have limited processing power. By using ECC, the proposed mechanism ensures robust encryption and decryption processes while minimizing the computational load on IIoT devices.

In a hybrid blockchain architecture, ECC ensures secure and efficient cryptographic operations. The smaller key sizes of ECC provide strong encryption with lower computational overhead, enhancing the overall performance of the blockchain. This is particularly beneficial when combined with DPoS, as the reduced computational burden aligns well with DPoS's energy-efficient consensus mechanism.

By integrating ECC into the hybrid architecture, the blockchain can achieve high levels of security and efficiency, making it suitable for various applications, including secure authentication systems. The combination of ECC's cryptographic strength and DPoS's consensus efficiency provides a balanced approach to maintaining security and performance in blockchain networks

D. Interoperable Framework

The proposed solution includes an interoperable framework designed to ensure seamless integration with existing IIoT infrastructure, which is crucial for the hybrid blockchain architecture utilizing DPoS and ECC.

In this framework, smart contracts are deployed within the blockchain to automate compliance and regulatory checks. This automation facilitates seamless interactions between different blockchain layers andIIoT systems by ensuring that data and processes comply with predefined rules and regulations without manual intervention. These smart contracts leverage the efficient cryptographic techniques of ECC, ensuring secure and rapid execution of these automated processes.

Besides, to ensure compatibility and smooth data exchange across various IIoT applications, APIs andmiddleware are developed. These tools bridge the gap between different systems, allowing data to flow freely and securely between the blockchain and IIoT devices.

The middleware acts as an intermediary that handles the translation and routing of data, ensuring that the diverse systems involved can communicate effectively without compatibility issues.

E. Decentralized Identity Management

Furthermore, the scheme features a decentralized identity management system based on DecentralizedIdentifiers (DIDs), which enhances the security and privacy of the IIoT network.

DIDs are a new type of identifier that is self-sovereign and decentralized. Unlike traditional identifierscontrolled by central authorities, DIDs are created, owned, and managed by the entities they identify, ensuring greater control and privacy. In this DIDs decentralized identity management system, each IIoT device is assigned a unique DID, which is stored on the blockchain. This document is used to verify the identity and integrity of the device. This ensures that every device has a distinct, verifiable identity that is securely recorded in a decentralized ledger.

By managing device identities in a decentralized manner, the system eliminates single points of failure. Unlike traditional centralized systems, where a single compromised point can lead to the failure of the entire network, decentralized management distributes the risk, significantly enhancing network resilience. Decentralized identity management ensures that device identities are securely managed and verified withoutrelying on a central authority. This enhances privacy, as it reduces the risk of sensitive identity information being exposed or misused by a single entity.

By preventing a single point of attack from compromising the entire system, decentralized identity management significantly enhances the overall security of the IIoT network. Each device's identity is independently verified, making it difficult for attackers to manipulate or spoof device identities. The system also maintains relatively low communication costs by efficiently managing and verifying identities using blockchain technology. This is crucial for IIoT applications where numerous devices need to interact frequently.

4. RESULT AND ANALYSIS

The formula to generate a block in a hybrid blockchain architecture using DPoS and ECC under an interoperable framework of DIDs can be represented as follow:

$Block_i = \{previous\_block\_hash_{i-1}, m_i, H_{i,(}r_i,s_i), Q_i\}$

Where:

$previous\_block\_hash_{i-1}$: Hash of the previous block $i - 1$

m_i: Block content of block i

H_i: Hash of the block content for block i, H_i = h(m_i)

(r_i,s_i) : ECC signature of the block content hash H_i

k_i : Random integer selected for the signature

$R_i = k_i \,.\, G$

$r_i = x_{Ri} \bmod n_1$ wheere x_{Ri} is the x-coordinate of R_i

$s_i = k^{-1}{}_i(h(m_i) + d_i \,.\, r_i) \bmod n_1$ wheere d_i is the delegate's private key

Q_i: Public key of the delegate for block i, $Q_i = d_i \,.\, G$

Additionally, the DPoS mechanism determines the delegate d_i for block i through the voting process, and the DID framework verifies the delegate's identity. Combining all elements into a single formula:

$Block_i$ = {Hash($Block_{i-1}$), m_i, h(m_i), (x_{Ri} mod n, $k^{-1}{}_i$ (h(m_i) + d_i . (x_{Ri} mod n)) mod n) , $d_i \,.\, G$}

This formula encapsulates the entire process of generating a block in the hybrid blockchain model.

Figure 2 below shows the representation graph of hybrid blockchain block generation.

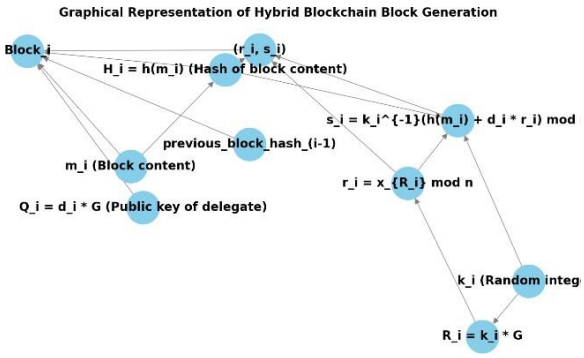

Figure 2: Representation graph of hybrid blockchain block generation.

The graph represents the process of generating a block in a hybrid blockchain architecture that uses Delegated Proof of Stake (DPoS) and Elliptic Curve Cryptography (ECC) within an interoperable framework of Decentralized Identifiers (DIDs). Each node in the graph represents a specific component or step in this process.The central node, Block_iis the block being generated. It incorporates several key elements: the hash of the previous block(previous_block_hash_(i-1)), the content of the current block (m_i), the hash of the block content (H_i), the ECC signature ((r_i, s_i)), and the public key of the delegate (Q_i).

The process begins with hashing the content of the block (m_i) to produce H_i. A random integer k_i is selected to compute R_i as $k_i \,.\, G$, where G is the generator point on the elliptic curve. The x-coordinate of R_i is then used to calculate r_i as x_{Ri} mod n. The second part of the ECC signature, s_i, is computed using the formula $k^{-1}{}_i(h(m_i) + d_i \,.\, r_i)$ mod n_1 where d_i is the private key of the delegate. This results in the ECC signature (r_i,s_i).

The final block, Block_i, is formed by integrating the previous block's hash, the current block's content, the hash of the content, the ECC signature, and the delegate's public key. The public key Q_i (computed as
$d_i \,.\, G$) is included in the block to allow verification of the signature. This comprehensive process ensures theintegrity, authenticity, and continuity of the blockchain, leveraging the strengths of DPoS for efficient block production and ECC for secure digital signatures. The DIDs framework further ensures that the delegates' identities are verifiable and securely managed.

Figure 3 below shows the energy consumption comparison (GPU) of different blockchain architectures.
The graph is referred to [28] with suitable assumption made for each blockchain architectures.

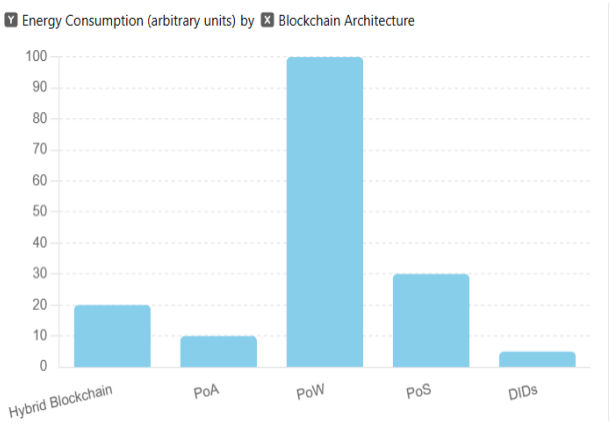

Figure 3: Energy consumption comparison (GPU) Of different blockchain architectures.

The energy consumption comparison chart illustrates the relative GPU energy usage of different blockchain architectures: Hybrid Blockchain, PoA, PoW, PoS, and DIDs. Hybrid Blockchain, which combines features of multiple blockchain types which are DPoS and ECC, has a moderate energy consumption of 20 units due to its optimized consensus mechanisms. Proof of Authority (PoA) consumes 10 units of energy by relying on a small number of trusted validators, thus reducing the need for extensive computational resources. Proof of Work (PoW), used by cryptocurrencies like Bitcoin, has the highest energy consumption at 100 units because it requires significant computational power to solve cryptographic puzzles. Proof of Stake (PoS), which selects validators based on the number of tokens they hold, consumes 30 units of energy, lower than PoW because it avoids complex cryptographic puzzles.

Finally, Decentralized Identifiers (DIDs) have the lowest energy consumption at 5 units, as they primarily involve lightweight cryptographic operations for identity verification. This chart highlights the trade-offs between different blockchain architectures, particularly regarding energy consumption and efficiency.

Figure 4 below shows the comparison graph of blocks generated by different blockchain

architectures.

The graph is referred to [27] with suitable assumption made for each blockchain architectures.

Figure 4: Comparison graph of blocks generated by different blockchain architectures.

The graph compares the number of blocks generated by different blockchain architectures in a networkof 1000 nodes, highlighting the efficiency and performance of each approach.

The Hybrid Blockchain architecture, which combines features from multiple consensus mechanisms which are DPoS and ECC, generates 950 blocks. This high number indicates that the hybrid model effectively balances security, decentralization, and performance, resulting in efficient block production.

PoA architecture, which relies on a small number of trusted validators for generating and validating blocks, produces 980 blocks. The centralized nature of PoA allows for faster block production and lower energy consumption, making it one of the most efficient architectures in this comparison.

PoW, the consensus mechanism used by cryptocurrencies like Bitcoin, generates only 600 blocks. This relatively low number underscores the resource-intensive and time-consuming nature of PoW, which requires significant computational power and energy to solve complex cryptographic puzzles.

PoS architecture, which selects validators based on the number of tokens they hold and are willing to "stake" as collateral, generates 850 blocks. PoS is more efficient than PoW, as

it avoids the need for solvingcomplex puzzles, but it does not achieve the same level of efficiency as PoA or the DIDs.

DIDs focus on creating decentralized, verifiable digital identities using lightweight cryptographic operations. This architecture generates the highest number of blocks, 990, indicating that the operations involved are less computationally intensive and allow for rapid block generation.

In summary, the graph clearly illustrates the efficiency differences in block generation capabilities among various blockchain architectures when applied to a network of 1000 nodes. PoA and DIDs show the highest efficiency, with the highest number of blocks generated due to their streamlined consensus mechanisms. The Hybrid Blockchain also performs well, leveraging a combination of mechanisms for optimal efficiency. PoS demonstrates moderate efficiency, while PoW generates the fewest blocks due to itshigh computational and energy costs. This comparison emphasizes the trade-offs between efficiency, energyconsumption, and computational intensity across different blockchain models.

5. CONCLUSION

Overall, the results and the analysis show that hybrid blockchain architecture is the most suitable solution for this project problem statement. Though PoA and DIDs emerge as the most efficient architectures, consume the least GPU energy and generating the highest number of blocks due to their streamlined and less resource-intensive consensus mechanisms, hybrid blockchain also demonstrates strong performance by effectively balancing multiple consensus methods to lower GPU energy consumption and optimize block production while keeping the computing and validation cost of the project at the lowest rate at the same time. Therefore, hybrid blockchain architecture is the most suitable and optimum solution for this project.

6. ACKNOWLEDGEMENT

This research work is the outcome of a class project for a computer security course at Faculty ofComputer Science and Information Technology, Universiti Malaysia Sarawak, Malaysia.

REFERENCES

Ismail, S., Dawoud, D., & Reza, H. (2022). Towards a lightweight identity management and secure authentication for IoT using blockchain. In *2022 IEEE World AI IoT Congress (AIIoT)*, Seattle, WA.

Jia, X., Luo, M., Wang, H., Shen, J., & He, D. (2022). A blockchain-assisted privacy-aware authentication scheme for Internet of Medical Things. *IEEE Internet of Things Journal, 9*(21), 21838-21850. https://doi.org/10.1109/JIOT.2022.3181609

Mukhandi, M., Damião, F., Granjal, J., & Vilela, J. P. (2022). Blockchain-based device identity management with consensus authentication for IoT devices. In *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA (pp. 433-436). https://doi.org/10.1109/CCNC49033.2022.9700534

Mao, W., Jiang, P., & Zhu, L. (2023). BTAA: Blockchain and TEE-assisted authentication for IoT systems. *IEEE Internet of Things Journal, 10*(14), 12603-12615. https://doi.org/10.1109/JIOT.2023.3252565

Panda, S. S., Jena, D., Mohanta, B. K., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2021). Authentication and key management in distributed IoT using blockchain technology. *IEEE Internet of Things Journal, 8*(16), 12947-12954. https://doi.org/10.1109/JIOT.2021.3063806

Singh, S., Hosen, A. S. M. S., & Yoon, B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed IoT network. *IEEE Access, 9*, 13938-13959. https://doi.org/10.1109/ACCESS.2021.3051602

Wang, B., Chang, Z., Li, S., & Hämäläinen, T. (2022). An efficient and privacy-preserving blockchain-based authentication scheme for low Earth orbit satellite-assisted Internet of Things. *IEEE Transactions on Aerospace and Electronic Systems, 58*(6), 5153-5164. https://doi.org/10.1109/TAES.2022.3187389

Wazid, M., Das, A. K., Shetty, S., & Jo, M. (2020). A tutorial and future research for building a blockchain-based secure communication scheme for Internet of Intelligent Things. *IEEE Access, 8*, 88700-88716. https://doi.org/10.1109/ACCESS.2020.2992467

Yang, X., et al. (2022). Blockchain-based secure and lightweight authentication for Internet of Things. *IEEE Internet of Things Journal, 9*(5), 3321-3332. https://doi.org/10.1109/JIOT.2021.3098007

Zhang, Y., Li, B., Wu, J., Liu, B., Chen, R., & Chang, J. (2022). Efficient and privacy-preserving blockchain-based multifactor device authentication protocol for cross-domain IIoT. *IEEE Internet of Things Journal, 9*(22), 22501-22515. https://doi.org/10.1109/JIOT.2022.3176192

Qureshi, K. N., Jeon, G., Hassan, M. M., Hassan, M. R., & Kaur, K. (2023). Blockchain-based privacy-preserving authentication model for intelligent transportation systems. *IEEE Transactions on Intelligent Transportation Systems, 24*(7), 7435-7443. https://doi.org/10.1109/TITS.2022.3158320