Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications

Journal homepage:
https://akademiabaru.com/submit/index.php/arca/index
2462-1927

Prototyping Contactless Authentication Application using Blockchain-Based Smart Contract for Secure Remote Attendance Automation

Putra Roskhairul Fitri Kaha[1], Afiqah Mohammad Azahari[1], Najah Alsubaie[2], Venkatesan K[3], Syarifah Bahiyah Rahayu[1,4*]

[1] Faculty of Defense Science and Technology, National Defence University of Malaysia (UPNM), Malaysia
[2] Department Computer Science, College of Computer and Information, Sciences, Princess Nourah bint Abdulrahman University (PNU), Saudi Arabia
[3] Department of Computer Science and Engineering, Amrita School of Computing, Amrita Vishwa Vidyapeetham, Chennai, India
[4] Cyber Security and Digital Industrial Revolution Centre, Institute of CyberSecurity and Electronic Systems, National Defence University of Malaysia (UPNM), Malaysia

ARTICLE INFO

Article history:
Received 23 September 2025
Received in revised form 20 November 2025
Accepted 21 November 2025
Available online 9 December 2025

Keywords:
Attendance, Blockchain; Face recognition; Location-based; Smart contract.

ABSTRACT

Accurate and tamper-proof attendance recording remains an essential requirement for organizations especially when currently organizations have been adapting to flexible and remote working models. Traditional attendance systems, whether manual or biometric, often face issues in accessibility, manipulation, and data vulnerability particularly when managed through centralized databases. This paper presents W@RK, an IoT-based contactless attendance system that integrates facial recognition, geolocation validation, and blockchain-based smart contracts to solve issues related to secure, verifiable, and transparent attendance management. The system employs facial recognition for user authentication, geo-fencing to validate the user's physical location, and blockchain technology to record attendance data as immutable transactions. Smart contracts define the operational rules and automatically execute attendance validation and record submission. The prototype was developed using Python and Solidity, with a private Ethereum network established through Geth and Brownie for blockchain interaction. Performance evaluation focused on the blockchain layer under varying workloads, achieving up to 99.86% transaction success rate with 1,000 virtual users, demonstrating stability and reliability of W@RK even under high demand. These results indicate that W@RK provides a secure and efficient alternative to traditional attendance systems, offering transparency, data integrity, and scalability for modern organizational environments.

1. Introduction

Accurate and tamper-proof attendance system remains a persistent challenge in organization. Traditional attendance systems whether manual registration or on-premises biometric scanners often face reliability issue, manipulation risks with limitation on adaptability to remote or hybrid work

[*] *Corresponding author.*
E-mail address: syarifahbahiyah@upnm.edu.my

https://doi.org/10.37934/arca.41.1.9099

arrangements. This highlights the need for attendance mechanisms that are not only accurate but also verifiable and secured against manipulation.

Blockchain technology provides a promising foundation for addressing these challenges. As a distributed ledger, it ensures transparency, immutability, and trust, allowing attendance data to be recorded without centralized control. Since its conceptual introduction [1] blockchain has evolved from a prototype technology into a mature infrastructure supporting a wide range of secure applications. Blockchain architecture that build upon consensus protocol, peer-to-peer (P2P) networking, and private key cryptography will help in solving the risk of current attendance system.

In parallel with the blockchain as the secure attendance storage, a biometric technology, particularly facial recognition has become essential for digital identity verification in attendance systems [2]. Face recognition allows for seamless and contactless authentication, eliminating the need for physical interaction with devices. Research by [3] demonstrated how facial encoding and comparison techniques can accurately identify individuals in real-time, strengthening digital attendance verification. Complementing this, geolocation-based methods such as geo-fencing add an additional layer of assurance by confirming that users are within the designated area when marking attendance [4].

Building upon these technologies, this paper presents W@RK, an IoT-based, contactless attendance system, designed to ensure secure and verifiable attendance management. W@RK build with facial recognition, geolocation validation, and a blockchain-based smart contract mechanism to automate secure, tampered free, attendance logging. This approach provides a transparent, decentralized, and tamper-proof attendance infrastructure, supporting both in-office and remote working environments.

An organization needs a reliable method for recognizing and recording employees' daily attendance. Fingerprint and face recognition-based systems have increasingly replaced traditional methods that are often prone to manipulation. However, many organizations still rely on relational databases to store employee login and logout data. These conventional databases present a major limitation: although effective for data management, they cannot guarantee data integrity, allowing unauthorized individuals to alter or delete records [5]. To address this challenge, several studies have proposed attendance methods.

Numerous research has employed face recognition in attendance systems [6] which primarily concentrate on face recognition algorithms. Nevertheless, there are few studies on attendance systems that used face recognition integrated with blockchain systems [7]. A study done by Mohammad Azahari, et al., does facial recognition through a convolutional neural network and maintains the attendance data on a blockchain system [8]. Since then, the framework has been deployed for the attendance of conference [9] attendance and university class attendance as well [10]. On top of that, an attendance system that developed by [11]., can automatically tracks the user's behaviour over the screen and it will define the exact location of the device to avoid proxy attendance or false check-ins performed from unauthorized locations. In another study, Bálint proposed an attendance system that utilized Wi-Fi router addresses to allow students to log in only when connected to a predefined network, thereby avoiding false attendance marking from unauthorized locations or external networks. The login information is stored on a distributed and decentralized blockchain – cite please.

Blockchain technology has proven to have a significant impact on various sectors, particularly in terms of data integrity and security. Due to its advantages, such as crypto-security, immutability, transparency, and decentralized data networks, blockchain technology has potential applications in almost every domain [12]. Recent research has focused on the design of a digital evidence security system using blockchain technology, emphasizing the need for security measures to maintain the authenticity of digital evidence [13]. Additionally, Mekdad et al., highlight the potential for blockchain to enhance data security and privacy in IoT environments [14]. Furthermore, the development of a blockchain-enabled device authentication and authorization system for the Internet of Things (IoT) [15].

Despite the potential benefits, there are challenges in integrating and implementing blockchain in attendance systems. [16] highlight the difficulty in establishing mutual trust among multiple certificate authority nodes (CA) and the potential failure of a single point in the traditional PKI method when deploying a decentralized cross-domain identity authentication protocol based on blockchain. These articles highlight the potential of blockchain technology in ensuring the accuracy and credibility of the attendance data by addressing all concerns related to data tampering and unauthorized access [17]. Furthermore, these studies also demonstrate the technical and operational challenges that must be overcome to address blockchain in attendance systems and become a valuable reference to assist in developing attendance systems.

Smart contracts are code scripts that run on blockchain platforms and automate legal agreements, which find applications such as crowdfunding [18]. Smart contracts act as intermediaries, executing predefined tasks and processes in blockchain, making them essential for creating a secure remote attendance automation system. Smart contract security relies on cryptographic techniques that protect transaction confidentiality and integrity [19]. By using multiple layers of techniques, smart contracts will play a leading role in the security infrastructure of secure attendance systems. However, smart contracts also come with security vulnerabilities and bugs that can pose a significant risk, potentially leading to operational disruptions [20]. This poses a threat to the attendance systems. Implementing secure coding and a proper code design process will help in preventing security vulnerabilities and bugs. Integrating smart contracts with blockchain can create a tamper-resistant and auditable ledger, which ensures the integrity of attendance data. Since the blockchain is transparent and immutable, any modification does not affect the smart contract code and execution, ensuring high-level security and trust in the process [21].

Furthermore, smart contracts play a vital role in interoperability between different blockchain networks. According to [22], smart contracts are “Digital Twins” of devices that can enhance the security, reliability, and interoperability of IoT systems. By bridging attendance systems, smart contracts can store attendance records on one blockchain platform while executing the verification process on another. Thus, smart contracts can contribute to creating a comprehensive and efficient contactless attendance system through interoperability and enabling data transfer across various blockchain platforms. The interconnectedness ensures that the effectiveness of the attendance application is enhanced and remains versatile while utilizing different technologies and platforms [23]. Smart contracts are a promising solution, but they face some challenges that must be addressed. For example, blockchain systems may experience performance issues like limited scalability, transaction latency [24] and throughput bottlenecks, which affect the scalability of smart contracts. Additionally, smart contracts are vulnerable to security threats, and proper secure coding must be implemented to overcome these challenges. Thus, all these challenges need robust solutions to address them.

Many things must be considered to develop a secure contactless authentication prototype using blockchain-based smart contracts. The first thing to consider is the type of contactless authentication to be used. Based on the above discussion, the most suitable authentication is facing recognition and GPS systems. Incorporating GPS technology into the attendance system can provide numerous benefits. By integrating GPS into the attendance system, the organization and educators can ensure that attendance records are precise and reliable. The GPS location tracking accurately verifies the individual’s presence at a specific location. This ensures that attendance records are based on actual physical presence at designated locations, enhancing the integrity of the attendance system [25]. Additionally, this data also enables analysis of employee and student attendance patterns and behaviours, helping to develop attendance management strategies and identifying potential areas for improvement.

In integrating blockchain technology into a secure attendance system, a comprehensive approach is needed to ensure the integrity and security of attendance records. Blockchain can be used to securely record attendance records data, timestamp it, and make it immutable, which prevents unauthorized alterations and ensures the trustworthiness of the records [26]. Additionally, the decentralized nature of blockchain technology can ensure the security and privacy of attendance data in remote systems. This ensures that sensitive information is only accessible to authorized users. Smart contracts can be built on top of blockchain technology to provide additional benefits of automation, transparency, and reliability. This is done by automating the recording and validation of attendance data, which enhances the accuracy and reliability of the attendance tracking. This can significantly reduce the potential for errors and fraudulent activities and ensure the integrity of attendance records [6]. Furthermore, by implementing predefined rules and conditions, smart contracts can ensure that all the attendance data is securely and transparently recorded in the blockchain. This enhances the trustworthiness and immutability of attendance records, addressing the challenges associated with remote attendance monitoring and verification [25]. Smart contract codes have been introduced since the worker’s location is very crucial to know if they have connected from home or the office to validate their working location. Therefore, a W@RK attendance system prototype has been proposed which uses a smart contract for recording employee attendance through face recognition with location-based tracking.

2. Methodology

Previous research has established the conceptual groundwork for contactless attendance technologies. The study by [8], conducted during the COVID-19 pandemic, introduced a contactless attendance framework that integrated temperature detection as a preventive health measure. As the public health situation has since improved, this feature has become less critical. Furthermore, a subsequent study by [27] has refined the concept by specifying the system architecture and describing its principal components, namely biometric recognition, location identification, and blockchain-based data storage. Building upon these conceptual contributions, this paper focuses on translating the existing framework into a working prototype and demonstrating its operational feasibility.

The W@RK system is composed with three main components: face recognition, geolocation, and blockchain. The face recognition module utilizes OpenCV and the MobileNetV2 architecture, enabling a seamless recognition and authentication processes. The second core component is geolocation, which ensures that attendance is recorded only within an authorized area. The workspace boundaries are defined by a specific geographic range, and during the authentication process, W@RK determines the user’s real-time location and validates it against the predefined latitude and longitude coordinates.

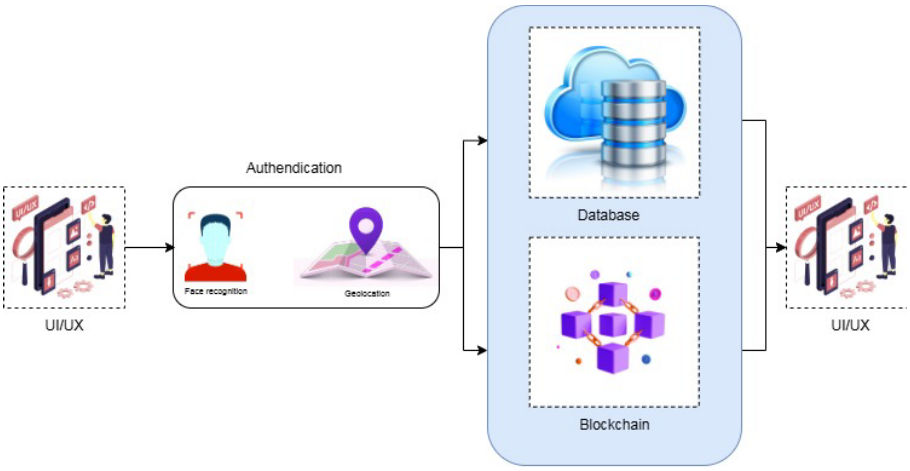


Fig. 1. W@RK system architecture

The last main components of W@RK are blockchain layer. W@RK integrate with blockchain to ensure secure and verifiable record management. The blockchain framework that we use in W@RK is Geth, a Go-based framework for building a local Ethereum network which operates on the Proof of Authority (PoA) consensus mechanism.

The PoA consensus mechanism enables fast and secure agreement among nodes making it suitable for attendance verification processes that require both speed and trust. Within this configuration, Geth provides a private Ethereum environment that allows controlled experimentation while maintaining high performance and adaptability. This environment is integrated into the W@RK system through Brownie, a middleware that connects the Python-based backend with the local Ethereum network. Brownie enables the backend application to send and receive blockchain transactions automatically, removing the need for manual interaction with the network. This middleware serves as the communication bridge that links real-time user verification results such as facial recognition and location confirmation to the blockchain.

The blockchain environment is built on top of operational logic that governed by smart contracts provided by Solidity. These contracts define the rules that determine when an attendance record is considered valid. The conditions include successful face recognition, verified geolocation, and the generation of a timestamp during verification. When these criteria are met, Brownie triggers the corresponding smart contract function, which records the verified attendance data on the blockchain. The blockchain network, that is managed by Geth, then validates and stores the transaction permanently, ensuring data integrity, transparency, and resistance to tampering. The smart contracts are executed autonomously within the network to guarantee that each attendance record is securely verified and immutably stored as illustrated in the pseudocode (refer to Pseudocode: Contactless Authentication and Pseudocode: Smart Contracts). This design allows seamless communication between the blockchain layer, the authentication modules, and the web application, achieving complete end-to-end verification within the W@RK system.

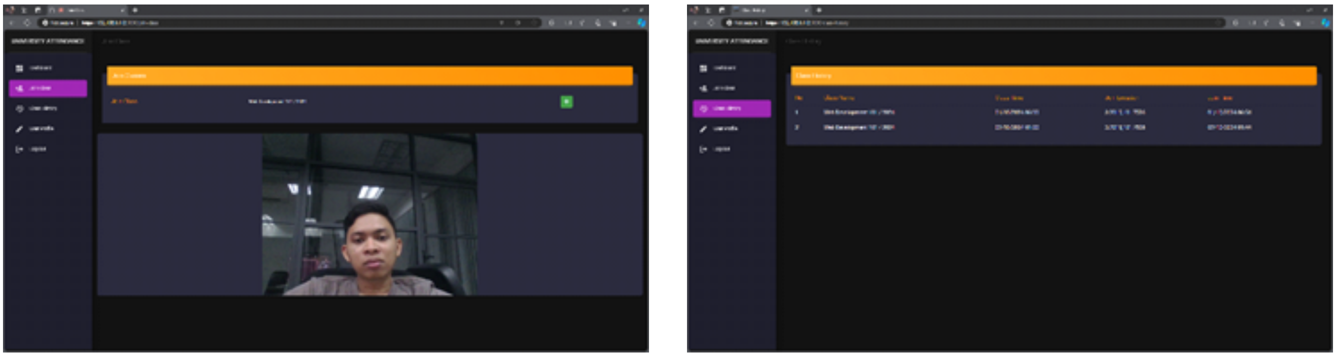
Pseudocode: Contactless Authentication

```
Function register_attendance(class_id, matric_id, image, user_location):

    # Step 1: Load Known Faces Database
    known_faces ← load from database or memory
    If known_faces is empty:
        Return "Error: No face data available for comparison"
    # Step 2: Perform Face Recognition
    faces, locations ← detect_faces(image)
    If faces is empty:
        Return "Error: No face detected in the image"

    recognized_user ← None
    For each face in faces:
        face ← preprocess(face)  # resize, normalize
        embeddings ← get_face_embedding(face)

        For each embedding in embeddings:
            If embedding matches any entry in known_faces:
                recognized_user ← matched_user_id
                Break

    If recognized_user is None OR recognized_user ≠ matric_id:
        Return "Error: Face recognition failed or user mismatch"

    # Step 3: Validate Geolocation
    latitude, longitude ← parse(user_location)
    allowed_location ← get_allowed_location(class_id)
    distance ← calculate_haversine(latitude, longitude, allowed_location)

    If distance > 1 km:
        Return "Error: Geolocation mismatch"

    # Step 4: Record Attendance on Blockchain
    timestamp ← get_current_unix_time()
    location_data ← format_location(latitude, longitude)

    transaction ← attendance_contract.functions.recordAttendance(
        matric_id, class_id, timestamp, location_data
    ).build_transaction({
        from: account_address,
        nonce: web3.eth.get_transaction_count(account_address),
        gas: 2000000,
        gasPrice: web3.to_wei('0', 'gwei')
    })

    signed_tx ← sign_transaction(transaction, private_key)
    receipt ← send_transaction(signed_tx)

    If receipt indicates failure:
        Return "Error: Blockchain transaction failed"

    Return "Success: Attendance registered successfully"

End Function
```

Pseudocode: Smart Contracts

```
Contract Attendance:

    # Define structure for attendance records
    Structure AttendanceRecord:
        matrix_id
        class_id
        timestamp
        location
    # Declare storage arrays and mappings
    Declare attendanceRecords as array of AttendanceRecord
    Declare studentAttendanceMapping as mapping of matrix_id → array of
AttendanceRecord
    Declare classAttendanceMapping as mapping of class_id → array of
AttendanceRecord

    # Constructor
    Function Constructor():
        Initialize contract state

    # Function to record attendance
    Function recordAttendance(matrix_id, class_id, timestamp, location):
        # Validate input parameters
        If matrix_id is empty OR class_id is empty OR timestamp is empty OR
location is empty:
            Reject transaction with message "Invalid input parameters"

        # Create new attendance record
        newRecord ← AttendanceRecord(matrix_id, class_id, timestamp, location)

        # Store record in main array
        Append newRecord to attendanceRecords

        # Update student and class mappings
        studentAttendanceMapping[matrix_id].push(newRecord)
        classAttendanceMapping[class_id].push(newRecord)

    # Function to get total number of attendance records
    Function getTotalRecords() returns integer:
        Return length of attendanceRecords

    # Function to retrieve a specific attendance record by index
    Function getRecord(index) returns AttendanceRecord:
        Require index < length of attendanceRecords
        Return attendanceRecords[index]

End Contract

# Deployment
Deploy Attendance contract to blockchain network using deployment script
```

The system is primarily developed in Python, which handles the face recognition logic, geolocation validation, and communication with the blockchain network. The user interface implemented using HTML, CSS, and JavaScript, provides an interactive platform for user registration (Figure 1(a)) and attendance verification (Figure 1(b)), serving as a crucial element in evaluating the system’s functionality and usability prior to deployment.



(a) Class attendance registration (b) Attendance verification

Fig. 2. User interface for remote attendance system

3. Results

To evaluate the system's efficiency, a performance test was conducted on the blockchain layer, focusing on transaction handling under varying loads. In a multi-component system such as W@RK, performance evaluation can target several layers, including the face recognition module, geolocation service, and blockchain network. However, among these components, the blockchain layer plays a critical role W@RK because this specific system is the main system that hold data integrity, security, and transaction validation. Since every attendance record is stored as a transaction within the blockchain, system performance directly depends on how efficiently the blockchain can process and confirm these transactions under varying loads.

The performance test to evaluates the system's ability to handle high volumes of concurrent users and multiple simultaneous requests. The blockchain layer is subjected to increasing transaction loads to measure response time, throughput, and stability. The test ensures that the prototype can maintain secure, reliable, and fast performance even under extreme usage conditions.

Table 1 presents the results of the performance testing, showing the system's performance under different levels of Virtual Users (VU). The recorded metrics include the Application Performance Index (APDEX), Transactions Per Second (TPS), Passing Rate, Duration, Number of Transactions, and the Projected Transactions Per Month. These measurements provide a quantitative basis for analysing how well the blockchain network sustains performance under stress and whether it meets the operational requirements of a real-world deployment.

Table 1
Performance Testing Results

No	VU	APPDEX	TPS	Passing Rate	Duration	No. of Transactions	Projection Transaction Per-month
1	60	0.647	2.99	78.17%	100 mins	22951	9914832
2	200	0.698	1.58	71.64%	60 mins	7944	5719680
3	150	0.483	0.47	99.82%	60 mins	1685	1213200
4	200	0.526	0.54	97.05%	60 mins	1999	1439280
5	1000	0.505	0.96	99.86%	60 mins	3478	2504160

The results showed that the network-maintained stability even when tested with up to 1,000 virtual users, achieving a passing rate of 99.86% and processing over 3,400 transactions per hour, despite lower APPDEX and TPS scores under heavier load. These findings confirm the reliability of W@RK's design and demonstrate its potential for secure, transparent, and verifiable attendance management across diverse working environments.

This concludes that the blockchain network could handle a large amount of transaction stability from all these components despite some performance issues with APDEX scores and TPS. Proper optimizations could improve the performance and ensure it scales effectively to meet future demands.

4. Conclusions

This study presented W@RK, a blockchain-based contactless attendance system that integrates facial recognition and geolocation verification to ensure secure and transparent attendance management. The proposed system addresses the limitations of traditional attendance methods by enabling tamper-proof record keeping through blockchain and automated validation via smart contracts. The integration of these technologies demonstrates that reliable attendance tracking can be achieved in both remote and on-site work environments without compromising data integrity or security. W@RK underwent performance testing on its blockchain layer which confirmed system stability under heavy transaction loads, maintaining a 99.86% success rate with 1,000 virtual users. These findings show that W@RK offers a practical and secure alternative for modern workforce management, where flexibility and trust are equally critical.

Acknowledgement

This research received financial funding publication from UPNM.

References

[1] Eyal, Ittay, Adem Efe Gencer, Emin Gün Sirer, and Robbert Van Renesse. 2016. "Bitcoin-NG: A Scalable Blockchain Protocol." *Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, 45–59. https://doi.org/10.48550/arXiv.1510.02037.

[2] Jain, Arnav, Rahul Gupta, Mohd. Shariq Ansari, and Tanveer Ikram. 2022. "Attendance Monitoring System Using Face Recognition." *International Journal for Research in Applied Science and Engineering Technology* 10 (5): 3024–3029. https://doi.org/10.22214/ijraset.2022.42389.

[3] Sarath Krishnan, P., and Athira Manikuttan. 2022. "Attendance Management System Using Facial Recognition." In *Proceedings of International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS 2022)*, 1–6. IEEE. https://doi.org/10.1109/ic3sis54991.2022.9885693.

[4] Babatunde, A. N., Afeez A. Oke, R. S. Babatunde, O. Ibitoye, and E. R. Jimoh. 2022. "Mobile Based Student Attendance System Using Geo-Fencing With Timing and Face Recognition." *Advances in Multidisciplinary and Scientific Research Journal Publication* 10 (1): 75–90. https://doi.org/10.22624/AIMS/MATHS/V10N1P8.

[5] Ardina, Hasna, and I Gusti Bagus Baskara Nugraha. 2019. "Design of A Blockchain-Based Employee Attendance System." In *Proceedings of the 2019 International Conference on ICT for Smart Society (ICISS)*, 1–4. IEEE. https://doi.org/10.1109/ICISS48059.2019.8969840.

[6] Biswas, Sourav, and Sameera Khan. 2021. "Smart Attendance Management System Using Facial Recognition." *International Journal of Advanced Research in Computer and Communication Engineering* 10 (4): 273–283. https://doi.org/10.17148/IJARCCE.2021.10446.

[7] Adetiba, Emmanuel, A. E. Opara, O. T. Ajayi, and F. O. Owolabi. 2021. "DeepFacematch: A Convolutional Neural Network Model for Contactless Attendance on e-SIWES Portal." *Communications in Computer and Information Science* 1350: 196–205. https://doi.org/10.1007/978-981-16-7610-9_16.

[8] Mohammad Azahari, Afiqah, Ahmad, and Syarifah Bahiyah Rahayu. 2021. "Contactless Attendance Method with Face Recognition, Body Temperature Measurement and GPS System Using Blockchain Technology." *Lecture Notes in Electrical Engineering* 741: 87–94. https://doi.org/10.1007/978-981-15-9938-1_11.

[9] Liu, S., R. Zhang, C. Liu, and D. Shi. 2023. "P-PBFT: An Improved Blockchain Algorithm to Support Large-Scale Pharmaceutical Traceability." *Computers in Biology and Medicine* 154: 106590. https://doi.org/10.1016/j.compbiomed.2022.106590.

[10] Gad, A. G., D. T. Mosa, L. Abualigah, and A. A. Abohany. 2022. "Emerging Trends in Blockchain Technology and Applications: A Review and Outlook." *Journal of King Saud University - Computer and Information Sciences* 34 (9): 6719–6742. https://doi.org/10.1016/j.jksuci.2022.03.002.

[11] Sarumi, Usman Abidemi, Zubaida Said Ameen, Fadi Al-Turjman, C. Altrjman, and Auwalu Saleh Mubarak. 2022. "A Novel Attendance System Via Integrated Wi-Fi and Blockchain Technologies." In *Proceedings of the 2022 International Conference on Artificial Intelligence in Everything (AIE 2022)*, 209–215. IEEE. https://doi.org/10.1109/AIE57029.2022.00046.

[12] Sriman, B., S. Ganesh Kumar, and P. Shamili. 2021. "Blockchain Technology: Consensus Protocol Proof of Work and Proof of Stake." *Advances in Intelligent Systems and Computing* 1172: 395–406. https://doi.org/10.1007/978-981-15-5784-8_36.

[13] Viswanadham, Y. V. R. S., and K. Jayavel. 2023. "A Framework for Data Privacy Preserving in Supply Chain Management Using Hybrid Meta-Heuristic Algorithm with Ethereum Blockchain Technology." *Electronics* 12 (6): 1462. https://doi.org/10.3390/electronics12061462.

[14] Mekdad, Y., A. Aris, L. Babun, A. El Fergougui, M. Conti, R. Lazzeretti, and A. S. Uluagac. 2023. "A Survey on Security and Privacy Issues of UAVs." *Computer Networks* 224: 109476. https://doi.org/10.1016/j.comnet.2023.109476.

[15] Dorri, A., and R. Jurdak. 2020. "Tree-Chain: A Fast Lightweight Consensus Algorithm for IoT Applications." In *Proceedings of the Conference on Local Computer Networks (LCN)*, 369–372. IEEE. https://doi.org/10.1109/LCN48667.2020.9314792.

[16] Zhou, T., X. Li, and H. Zhao. 2019. "DLattice: A Permission-Less Blockchain Based on DPoS-BA-DAG Consensus for Data Tokenization." *IEEE Access* 7: 39273–39287. https://doi.org/10.1109/ACCESS.2019.2906444.

[17] Venkatesan, K., and Syarifah Bahiyah Rahayu. 2024. "Blockchain Security Enhancement: An Approach Towards Hybrid Consensus Algorithms and Machine Learning Techniques." *Scientific Reports* 14 (1): 1149. https://doi.org/10.1038/s41598-024-01149-7.

[18] Shafay, M., R. W. Ahmad, K. Salah, I. Yaqoob, R. Jayaraman, and M. Omar. 2023. "Blockchain for Deep Learning: Review and Open Challenges." *Cluster Computing* 26 (1): 197–221. https://doi.org/10.1007/s10586-022-03513-4.

[19] Ometov, A., Y. Bardinova, A. Afanasyeva, P. Masek, K. Zhidanov, and S. Bezzateev. 2020. "An Overview on Blockchain for Smartphones: State-of-the-Art, Consensus, Implementation, Challenges and Future Trends." *IEEE Access* 8: 103994–104015. https://doi.org/10.1109/ACCESS.2020.2999303.

[20] Fernandes, C. P., C. Montez, D. D. Adriano, A. Boukerche, and M. S. Wangham. 2023. "A Blockchain-Based Reputation System for Trusted VANET Nodes." *Ad Hoc Networks* 140: 103071. https://doi.org/10.1016/j.adhoc.2022.103071.

[21] Tsai, C.-W., Y.-P. Chen, T.-C. Tang, and Y.-C. Luo. 2021. "An Efficient Parallel Machine Learning-Based Blockchain Framework." *ICT Express* 7 (3): 300–307. https://doi.org/10.1016/j.icte.2021.03.002.

[22] Sasikumar, A., S. Vairavasundaram, K. Kotecha, V. Indragandhi, L. Ravi, G. Selvachandran, and A. Abraham. 2023. "Blockchain-Based Trust Mechanism for Digital Twin Empowered Industrial Internet of Things." *Future Generation Computer Systems* 141: 16–27. https://doi.org/10.1016/j.future.2022.10.012.

[23] Frimpong, S. A., M. Han, E. K. Boahen, R. N. Ayitey Sosu, I. Hanson, O. Larbi-Siaw, and I. B. Senkyire. 2023. "RecGuard: An Efficient Privacy Preservation Blockchain-Based System for Online Social Network Users." *Blockchain: Research and Applications* 4 (1): 100111. https://doi.org/10.1016/j.bcra.2022.100111.

[24] Xu, G., Y. Liu, and P. W. Khan. 2020. "Improvement of the DPoS Consensus Mechanism in Blockchain Based on Vague Sets." *IEEE Transactions on Industrial Informatics* 16 (6): 4252–4259. https://doi.org/10.1109/TII.2019.2948083.

[25] Bachani, V., and A. Bhattacharjya. 2023. "Preferential Delegated Proof of Stake (PDPoS)—Modified DPoS with Two Layers Towards Scalability and Higher TPS." *Symmetry* 15 (1): 1–18. https://doi.org/10.3390/sym15010118.

[26] Zhou, C., L. Xing, Q. Liu, and H. Wang. 2023. "Effective Selfish Mining Defense Strategies to Improve Bitcoin Dependability." *Applied Sciences* 13 (1): 345. https://doi.org/10.3390/app13010345.

[27] Kaha, Putra Roskhairul Fitri, Syarifah Bahiyah Rahayu, Afiqah M. Azahari, Mohd Hazali Mohamed Halip, and K. Venkatesan. 2024. "W@rk: Attendance Application Framework Using Blockchain Technology." In *Data Science and Emerging Technologies*, edited by Bee Wah Yap, Dhiya Al-Jumeily, and Michael W. Berry, 479–492. Lecture Notes on Data Engineering and Communications Technologies, vol. 191. Singapore: Springer. https://doi.org/10.1007/978-981-97-0293-0_34.