DIGITAL IDENTITY VERIFICATION USING BLOCKCHAIN

[1]Dr R.G.Suresh Kumar , [2] Mrs. S.Sri Saye Lakshmi , [3] K.A.Emmanuel, [3] R.Kathiravan , [3] S.Nagaraj
[1] Head of the Department , RGCET, Puducherry
[2] Assistant Professor(CSE) , RGCET,Puducherry
[3] B.Tech(CSE) , RGCET,Puducherry

ABSTRACT

Identity verification is a crucial process in many domains, such as banking, education, healthcare, and e-commerce. However, traditional methods of identity verification are often costly, time-consuming, prone to errors, and vulnerable to fraud. Blockchain technology offers a promising solution to overcome these challenges by providing a decentralized, secure, and transparent platform for storing and verifying digital identities. In this project, we propose a novel system for digital identity verification using blockchain and non-fungible tokens (NFTs). NFTs are unique and indivisible digital assets that can represent any form of data, such as documents, certificates, images, or videos. We use NFTs to create verifiable credentials for users, which can be stored on a blockchain and accessed by authorized parties. Our system leverages the features of NFTs, such as immutability, provenance, and ownership, to ensure the authenticity, integrity, and validity of the credentials. Our system also provides several advantages over the existing systems, such as decentralization, security and privacy. We have implemented our system using Ethereum, a popular blockchain platform that supports smart contracts and NFT standards. We aim to design and develop a web-based application that will allow users to create, manage, and verify their digital identities using NFTs. We also intend to evaluate the performance, security, and usability of our system through experiments and user feedback. Our expected results are that our system will provide a fast, reliable, and user-friendly solution for digital identity verification using blockchain and NFTs.

Keywords: Block-chain, identity verification, Non fungible token

I. INTRODUCTION

Identity verification solutions need to be reliable and safe in an era where the digital landscape is constantly growing. Conventional identity management techniques frequently fail to offer the required guarantees of privacy and security. Let me introduce you to blockchain technology, a decentralized, immutable ledger system that has the potential to completely transform digital identity verification. The use of Non-Fungible Tokens (NFTs), distinct and indivisible cryptographic assets, into the identity verification procedure further strengthens this paradigm shift.

This all-inclusive solution builds a strong basis for identity management by utilizing the decentralization, immutability, and consensus processes of blockchain technology. The distinctive features of NFTs strengthen the issuance and verification of digital identities by providing tamper-proof digital certificates that may be safely provided for verification.

BLOCKCHAIN TECHNOLOGIES

A blockchain is “a distributed database that maintains a continuously growing list of ordered records, called blocks.” These blocks “are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network. [1]

Smart contracts

Smart contracts are computer programs that are hosted and executed on a blockchain network. Each smart contract consists of code specifying predetermined conditions that, when met, trigger outcomes. By running on a decentralized blockchain instead of a centralized server, smart contracts allow multiple parties to come to a shared result in an accurate, timely, and tamper-proof manner. [3]

Smart contracts are a powerful infrastructure for automation because they are not controlled by a central administrator and are not vulnerable to single points of attack by malicious entities. When applied to multi-party digital agreements, smart contract applications can reduce counterparty risk, increase efficiency, lower costs, and provide new levels of transparency into processes.[3]

Types of Blockchain

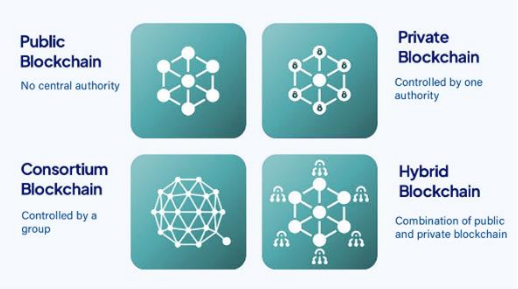

Figure 1.1 Types of Blockchain

a) Public blockchain:

A public blockchain is a permissionless distributed ledger accessible to anyone with an internet connection. In this type of blockchain, anyone can join the network, conduct transactions, and possess a copy of the ledger. Users have access to both historical and current records, and they can participate in mining operations, which involve performing complex computations to verify and add transactions to the ledger. Importantly, no valid record or transaction on the public blockchain can be altered. The open nature of the source code allows users to scrutinize transactions, identify issues, and propose fixes, ensuring transparency and security in the network.

b) Private Blockchain:

A private blockchain is a blockchain network that operates within a private context, often restricted to a specific network or controlled by a single identity. Despite sharing some characteristics, such as peer-to-peer connections and decentralization, with public blockchain networks, private blockchains are typically smaller in scale. These networks are commonly implemented within a specific firm or organization and are not open to anyone seeking to contribute processing power. Private blockchains are also referred to as permissioned blockchains or business blockchains. They provide a controlled and restricted environment, limiting participation to authorized entities within the defined network.

c) Consortium Blockchain:

A consortium blockchain, also known as a federated blockchain, is a type of blockchain that incorporates features from both private and public blockchains. Unlike a hybrid blockchain, a consortium blockchain involves multiple organizational members collaborating on a decentralized network. Consensus methods in a consortium blockchain are controlled by predetermined nodes, and there is typically a validator node responsible for initiating, receiving, and validating transactions. Member nodes within the consortium blockchain have the capability to both initiate and receive transactions. This model allows for decentralized collaboration among multiple organizations while maintaining a degree of control over the network through the consensus mechanisms established by the predetermined nodes.

d) Hybrid Blockchain:

A hybrid blockchain is a blockchain system that merges features from both private and public blockchains. This approach allows organizations to create a hybrid model by combining a private, permission-based system with a public, permissionless system. In a hybrid blockchain, organizations have the flexibility to control access to 30specific blockchain data, deciding which information remains private and which is made public.

Transactions and records in a hybrid blockchain are typically not automatically made public, but access can be granted, and validation can occur through the use of smart contracts when necessary. This combination provides a balance between the privacy and control of a private blockchain and the transparency and decentralization of a public blockchain.

DIGITAL IDENTITY

Everyone in the world appreciates a system that allows them to identify themselves securely, whether they work for a company or not. Numerous businesses are working to find a solution for the issue of digital identification, where information is stored in databases or written forms everywhere. For this kind of issue, a person's single digital identity is a good solution. Blockchain technology can help create this solution, which places all of a person's documentation under a single identity that is shared across the whole network. Among the many benefits of adopting digital identification are its high degree of accuracy, improved security, and privacy.

Another benefit of adopting digital identification is its convenience and efficiency. With a single digital identity, a person can access various services and platforms without having to create multiple accounts or provide different credentials. This reduces the hassle of remembering passwords, filling forms, or verifying identities.

Rising Importance of Digital Identity

The rising importance of blockchain lies in its ability to bring about disintermediation, transparency, and provenance in various ecosystems. Disintermediation is achieved through transaction immutability and a distributed ledger architecture, eliminating the need for a centralized enforcer of trust. Blockchain's tamper-proof distributed data ensures that all participants in the ecosystem operate with the same version of the truth, fostering trust without the need for intermediaries.

Transparency is significantly enhanced by blockchain, providing a public record of activity accessible to all market participants in real time. This increased visibility promotes trust and accountability among participants.

Shortcomings of Traditional Approaches

Traditional approaches exhibit limitations in centralization, posing risks of single points of failure and security vulnerabilities. The lack of transparency in these systems can compromise data integrity, leaving them susceptible to fraud and unauthorized alterations. Inefficiencies arise from their inability to adapt quickly to dynamic environments, hampering overall agility. These drawbacks highlight the need for improved resilience, security, and adaptability within conventional methods. Addressing these shortcomings in traditional approaches is essential to ensure their effectiveness and relevance in a rapidly evolving technological landscape without explicitly suggesting superiority to alternative solutions.

NFTs as a Unique Identifier

Non-fungible tokens (NFTs) represent a revolutionary form of digital ownership in the realm of blockchain technology. These unique assets are created by tokenizing real-world or digital items using a blockchain. The tokens are generated through complex encryption functions and carry distinct identification codes.

Unlike traditional tokens or cryptocurrencies, the value of an NFT lies not only in its cryptographic nature but also in the connection it establishes with a specific asset. Once created, NFTs are securely stored on a blockchain, providing an immutable and transparent record of ownership. It's important to note that while the tokens reside on the blockchain, the corresponding assets they represent can be stored in various locations, such as cloud servers, decentralized storage systems, or even physical storage. The uniqueness of NFTs stems from the irreplaceable link between the token and the underlying asset. This link is what sets them apart from fungible tokens like cryptocurrencies.

How NFTs works

NFTs are created through a process called minting, in which the asset's information is encrypted and recorded on a blockchain. At a high level, the minting process entails a new block being created, NFT information being validated by a validator, and the block being closed. This minting process often entails incorporating smart contracts that assign ownership and manage NFT transfers.

As tokens are minted, they are assigned a unique identifier directly linked to one blockchain address. Each token has an owner, and the ownership information (i.e., the address in which the minted token resides) is publicly available. Even if 5,000 NFTs of the same exact item are minted (similar to general admission tickets to a movie), each token has a unique identifier and can be distinguished from the others.

NFTs for identity issuance and verification

One of the promising applications of NFTs is to use them for identity issuance and verification. Identity verification is the process of proving that a person or an entity is who they claim to be online. This is essential for accessing various services and platforms, such as banking, e-commerce, social media, and more. However, current methods of identity verification are often insecure, and centralized. For example, users may have to provide multiple documents, passwords, or biometrics to verify their identity, which can be easily stolen, hacked, or compromised. Moreover, users may have to rely on third-party authorities or intermediaries, such as governments, corporations, or platforms, to issue and manage their identities, which can pose risks of censorship, surveillance, or discrimination.

NFTs can offer a better solution for identity verification by leveraging the features of blockchain technology, such as decentralization, immutability, and transparency. With NFTs, users can create and own their own digital identities, which are unique and verifiable tokens that represent their personal data and attributes. These tokens can be stored on a blockchain, where they are secured by cryptography and validated by consensus. Users can then use their NFT-based identities to prove their identity across different platforms and services, without having to reveal their sensitive information or depend on intermediaries. Users can also control how they share their data and with whom, and even monetize their data if they wish. Some of the benefits of using NFTs for identity verification are Ownership proof, Standardization, Enhanced authentication, Control over data sharing.

II. RELATED WORKS

[1] Digital Identity Using Blockchain technology

In the context, their research provides a comprehensive overview of the benefits and challenges associated with adopting digital identity systems, emphasizing their versatility, trustworthiness, and alignment with the principles of blockchain technology. Their proposed model prioritizes security, transparency, and privacy, offering robust cryptographic measures to safeguard personal user data while leveraging trusted authorities for reliable issuance and storage of cryptographic signatures. Moving forward, it's essential to address key challenges such as key management complexity and integration with legacy systems to ensure smooth implementation. Additionally, efforts to mitigate concerns about trusted authorities within decentralized blockchain environments are vital for maintaining system reliability and integrity. This research serves as a valuable reference for informing strategic decisions regarding the adoption and implementation of digital identity systems within our project. By considering the advantages, challenges of cryptographic signature approaches outlined in the research, we can develop a robust framework that prioritizes security, privacy, and transparency while effectively addressing the complexities associated with digital identity management.

[2] Digital Identity Management System Using Blockchain

In the context, their research underscores the potential benefits and limitations of implementing a digital identity system. Their system's adherence to GDPR regulations ensures legal compliance and reflects our commitment to safeguarding data privacy. By granting individuals control over their identity and personal documents, their system promotes empowerment and autonomy while streamlining identity management processes through the removal of intermediaries. However, it's crucial to acknowledge the identified drawbacks. While the system offers significant advantages, it may lack the robust digital ownership and provenance features associated with NFT-based systems, potentially impacting the tracking and verification of digital identities and personal data authenticity. Additionally, reliance on physical documents for identity verification could introduce reliability concerns. As we move forward with our project, this research serves as a valuable reference point for informing decision-making processes. By carefully considering both the advantages and challenges outlined in the research, we can develop a digital identity system that prioritizes data protection, user empowerment, and operational efficiency while addressing potential limitations and ensuring alignment with regulatory requirements.

[3] Secure and transparent KYC for banking system using IPFS and blockchain technology.

In the context, their research on "Secure and Transparent KYC for Banking System Using IPFS and Blockchain Technology" underscores the significance of leveraging innovative technologies to enhance the Know Your Customer (KYC) process within the banking sector. The integration of IPFS and blockchain technology presents a promising solution for improving data security, reducing the likelihood of data breaches, and fostering transparency between banks and customers. The findings of their research offer valuable insights for our project, highlighting the potential benefits of implementing a similar KYC system. By embracing this technology, we can streamline customer verification processes, leading to cost and time savings while upholding stringent security measures. Furthermore, the incorporation of IPFS and blockchain aligns well with our project's goals of establishing a secure financial environment, ultimately enhancing trust and compliance within the banking sector. However, it's crucial to address the challenges identified in the research, such as the additional steps required for users to digitize their data and the risks associated with data duplication and synchronization. Overcoming these obstacles will be essential to ensure the seamless integration and effectiveness of the KYC system within our project. As we move forward, this research serves as a valuable reference point, guiding our efforts to adopt and implement innovative technologies to improve the KYC process and enhance overall security and transparency within the banking sector. By leveraging the insights gained from this research, we can develop a robust and efficient KYC system that meets the evolving needs of our project and aligns with industry best practices.

III. IMPLEMENTATION

The proposed system is made up of a number of interrelated components that work together to securely digitize and manage identities on a blockchain network. The **Identity Issuer**, which is in charge of transforming paper documents into digital Non-Fungible Tokens (NFTs), is at the centre of it all. Users interact with the Identity Issuer on behalf of both individuals and organizations to begin the conversion of their physical credentials into an electronic format. This is the first step toward improving overall identity management efficiency and expediting verification processes.

The *blockchain network*, a distributed and decentralized ledger made up of nodes on various platforms like Ethereum, Sepolia, and others, is the foundation of the system. This network serves as a secure repository for recording transactions and securely storing digitalized identities. Because it is decentralized, there is less chance of unauthorized access or data manipulation because control is not centralized within one organization.

In this ecosystem, *Verifying Authorities*, or entities that require identity verification for various processes, play an important part. They quickly and securely authenticate digitalized identities by utilizing the blockchain-based system. Trusted interactions between users, Identity Issuers, and Verifying Authorities are made possible by the integration of smart contracts, which further automate and enforce predetermined conditions.

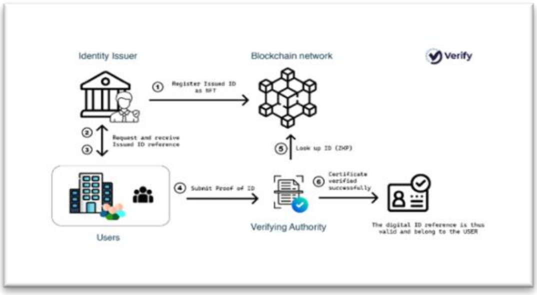
Identity Issuer
Blockchain network
Verify
① Register Issued ID as NFT
② ③ Request and receive Issued ID reference
⑤ Look up ID (ZKP)
④ Submit Proof of ID
⑥ Certificate verified successfully
Users
Verifying Authority
The digital ID reference is thus valid and belong to the USER

Figure 3.1 Proposed system architecture

A key aspect of the design is interoperability, which enables the system to function flawlessly across various blockchain networks. This guarantees that digital identities can be used seamlessly across various platforms and services, increasing the adaptability and user-friendliness of the system.

The design of the system places a high priority on privacy by utilizing cryptographic methods. The accountability and transparency are ensured by the blockchain's unchangeable audit trail. The system's philosophy is rooted in continuous innovation, with a dedication to adjusting to new technologies like zero-knowledge proofs. This guarantees that the ecosystem for identity verification stays at the forefront of security and efficiency, developing in tandem with changes in the blockchain space.

The proposed identity management system comprises three interconnected modules: the Client Module, the Issuer Module, and the Verifier Module. Each module plays a crucial role in the seamless and secure transformation of physical credentials into digital Non-Fungible Tokens (NFTs) on the blockchain network.

Only authorized personnel are permitted to use these modules to complete transactions. One of the features of the blockchain network is that any acts performed within it are irreversible, making it easy to track down any intrusion using the transaction ID or sender address and take further action against the perpetrator. Therefore, this assures that there could be no fraud done in the network.

Modules of the System

Client Module

The Client Module is designed to facilitate individuals and organizations seeking to digitize their personal credentials. Clients interact with this module to view the NFTs that have been issued to them for the physical documents. Through a user-friendly interface with the help of Meta-mask, clients provide their credentials to the system, which securely logs them into the blockchain network. This module ensures that clients can easily manage and access their digital identities while maintaining control over their privacy and security.

Issuer Module

The Issuer Module serves as the identity issuing authority responsible for processing and validating client credentials. Individuals and organizations engage with the Issuing authority to initiate the conversion of their physical documents into digital NFTs. This module verifies the authenticity of submitted credentials and ensures compliance with regulatory standards before issuing digital identities on the blockchain network. The Issuer Module plays a pivotal role in maintaining the integrity and reliability of digitalized credentials.

Verifier Module

The Verifier Module caters to institutions and entities requiring authentication of digital identities. Verifying authorities interact with this module to authenticate and verify the digitalized credentials stored as NFTs on the blockchain network. Leveraging blockchain technology, the Verifier Module ensures the integrity and immutability of identity data, expediting verification processes while minimizing errors and enhancing security.

IV. RESULT AND DISCUSSION

RESULT

The proposed system leveraging Non-Fungible Tokens (NFTs) for document verification represents a significant advancement over the existing CP-ABE-based IPFS storage project. By integrating NFTs into the document verification process, several key benefits emerge that contribute to increased efficiency and security.

Parameters	**Performance (%)**	
	Existing System	**Proposed System**
Transaction Speed	80	90
Cost Efficiency	70	83
Scalability	83	93
Security and Immutability	76	83
User Experience	85	93
Decentralization	60	75

Firstly, NFTs offer a novel approach to document verification by providing unique, immutable tokens that can be associated directly with specific documents. This eliminates the need for traditional storage methods like IPFS, where documents are stored separately and linked via cryptographic keys. With NFTs, each document is uniquely represented and can be securely verified through its tokenized form.

Secondly, the use of NFTs simplifies and streamlines the verification process. Instead of relying on complex cryptographic schemes for access control and decryption (as in CP-ABE systems), NFT-based verification relies on the inherent properties of blockchain technology. The authenticity and ownership of documents can be easily confirmed by validating the corresponding NFTs on a blockchain network.

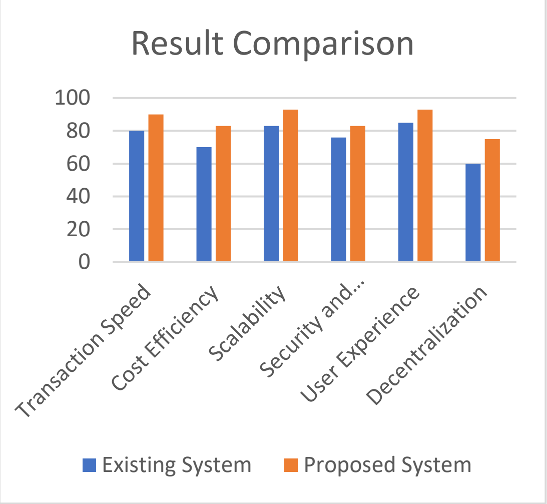

Figure 4.1 Comparison between two systems

DISCUSSION

A Token ID is generated by the smart contract for the KYC document in a local blockchain network created with the help of ganache, a software used to create a local blockchain network. This Token ID is a unique number to identify that particular transaction details (owner, document). A transaction once done cannot be denied or changed in the system and therefore paves a more secure way to record the activities done.

V. CONCLUSION

In conclusion, the integration of Block-chain technology in revolutionizing the Know Your Customer (KYC) process in the banking system. The integration of these technologies offers a secure, tamper-proof platform for storing and verifying customer identity information, thereby reducing the risk of data breaches and unauthorized access. This emphasizes the potential benefits of implementing this secure and transparent KYC system, including streamlining processes, reducing operational costs, and mitigating compliance risks. Furthermore, it highlights the transformative potential of blockchain technology in paving the way for a more secure, transparent, and efficient banking system. Our comprehensive exploration and analysis of blockchain technologies, digital identity, and the existing system, coupled with the support received, reflect our dedication and commitment to this project. Overall, it provides valuable insights into the application of blockchain for digital identity verification and its implications for the banking sector, emphasizing the need for further exploration and collaboration to realize the full benefits of this innovative approach.

FUTURE ENHANCEMENT

There are several key areas where our proposed NFT-based document verification system can be further developed and enhanced for future productivity and effectiveness. One critical aspect for future improvement is scalability and performance optimization. As the system scales to handle larger volumes of documents and transactions, it will be essential to optimize performance by exploring efficient data storage methods, enhancing smart contract efficiency, and leveraging scaling solutions such as layer 2 protocols to reduce transaction costs and improve overall throughput.

Another significant area for enhancement is security and auditing. Strengthening security measures will be paramount, requiring rigorous security audits, additional encryption layers where necessary, and continuous monitoring for vulnerabilities. Integrating robust identity management solutions and decentralized authentication mechanisms can further bolster security and ensure the integrity of the document verification process.

Interoperability and integration with other systems and platforms will be another focus for future development. This involves enhancing compatibility with different blockchain networks or standards, exploring cross-chain interoperability solutions, and integrating with existing document management systems to expand the system's reach and usability.

REFERENCES

[1] S. FUGKEAW, “Enabling Trust and Privacy-Preserving e-KYC,” p. 12, 2022.

[2] A. J. M.-A. F. and R. A. A. H. , “Blockchain-Based Identity Verification System,” p. 6, 2021.

[3] E. Androulaki, J. C. A. D. C. M. D. K. E. and B. T. , “Privacy-preserving auditable token payments in a permissioned,” p. 19, 2022.

[4] N. Sun, Y. Z. and Y. L. , “A Privacy-Preserving KYC-Compliant Identity Scheme for accounts on all public blockchain,” p. 18, 2022.

[5] Rafique and Z. , “BLOCKCHAIN IN DIGITAL IDENTITY,” no. 10.13140/RG.2.2.32462.59203, p. 11, 2021.

[6] R. MEGHANA, R. K. and S. K. , “Identity Management Using Blockchain Technology,” vol. 3, no. 10, p. 6, 2020.

[7] Z. Chen and S. W. , “Research on Digital Identity Authentication Technology based on Blockchain,” no. 10.1088/1742-6596/1802/3/032091, p. 9, 2020.

[8] W. Jie, W. Qiu, A. S. V. Koe, J. Li, Y. Wang, Y. Wu, J. Li and Z. Zheng, “A Secure and Flexible Blockchain- Based Offline Payment Protocol,” IEEE transactions on computers, vol. 73, no. 2, 2024.

[9] w. O.-B. O. Agyekum, Q. Xia, E. B. Sifah, C. N. A. Cobblah, H. Xia and J. Gao, “A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain,” IEEE Systems Journal, vol. 16, no. 1, 2022.

[10] O. Samuel, A. B. Omojo, A. M. Onuja, Y. Sunday, P. Tiwari, D. Gupta, G. Hafeez and A. S. Yahaya, “IoMT: A COVID-19 Healthcare System Driven by Federated Learning and,” IEEE Journal of Biomedical and Health, vol. 27, no. 2, 2023.

[11] O. Kuznetsov, P. Sernani, L. Romeo, E. Frontoni and A. Mancini, “On the Integration of Artificial Intelligence and Blockchain Technology: A Prespective About Security,” IEEE Access, vol. 12, 2024.

[12] Q. Liu, Y. Liu, M. Luo, D. He, H. Wang and K.-K. R. Choo, “The Security of Blockchain-Based Medical Systems: Research Challenges and Opportunities,” IEEE Systems Journal, vol. 16, no. 4, 2022.

[13] Y. Liu, G. Shan, Y. Liu, A. Alghamdi, I. Alam and S. Biswas, “Blockchain Bridges Critical National Infrastructures: E-Healthcare Data Migration Prespective,” IEEE Access, vol. 10, 2022.

[14] L. D. Xu, Y. Lu and L. Li, “Embedding Blockchain Technology Into IoT for Security: A Survey,” IEEE Internet of Things Journal, vol. 8, no. 13, 2021.

[15] S. Ramzan, A. Aqdus, V. Ravi, D. Koundal, R. Amin and M. A. A. Ghamdi, “Healthcare Applications Using Blockchain Technology: Motivations and Challenges,” IEEE Transactions on Engineering Management, vol. 70, no. 8, 2023.

[16] Z. Zulkifl, F. Khan, S. Tahir, M. Afzal, W. Iqbal, A. Rehman, S. Saeed and A. M. Almuhaideb, “FBASHI: Fuzzy and Blockchain-Based Adaptive Security for Healthcare loTs,” IEEE Access, vol. 10, 2022.

[17] Z. Liao, X. Pang, J. Zhang, B. Xiong and J. Wang, “Blockchain on Security and Forensics Management in Edge Computing for IoT: A Comprehensive Survey,” IEEE Transactions on Network and Service Management, vol. 19, no. 2, 2022.

[18] X. Chen, A. Yang, J. Weng, Y. Tong, C. Huang and T. Li, “A Blockchain-Based Copyright Protection Scheme With Proactive Defense,” IEEE Transactions on Services Computing, vol. 16, no. 4, 2023.

[19] L. K. Ramasamy, F. K. K. P., A. L. Imoize, J. O. Ogbebor, S. Kadry and S. Rho, “Blockchain-Based Wireless Sensor Networks for Malicious Node Detection: A Survey,” IEEE Access, vol. 9, 2021.

[20] S. Singh, A. S. M. S. Hosen and B. Yoon, “Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network,” IEEE Access, vol. 9, 2021.

[21] W. Dai, Y. Lv, K.-K. R. Choo, Z. Liu, D. Zou and H. Jin, “CRSA: A Cryptocurrency Recovery Scheme Based on Hidden Assistance Relationships,” IEEE Transactions on Information Forensics and Security, vol. 16, 2021.

[22] X. Yang, X. Yang, X. Yi, I. Khalil, X. Zhou, D. He, X. Huang and S. Nepal, “Blockchain-Based Secure and Lightweight Authentication for Internet of Things,” IEEE Internet of Things Journal, vol. 9, no. 5, 2022.

[23] M. Kim, I. Oh, K. Yim, M. Sahlabadi and Z. Shukur, “Security of 6G-Enabled Vehicle-to-Everything Communication in Emerging Federated Learning and Blockchain Technologies,” IEEE Access, vol. 12, 2024.