Leveraging Digital Twins for ON/OFF-LINE Blockchain Networks: A Resilient Framework for Drone and IoT Communication

SeongSu Park
Dept. Computer Engineering
Ajou University
Suwon, Republic of Korea
parky@ajou.ac.kr

Ki-Hyung Kim
Dept. Cyber Security
Ajou University
Suwon, Republic of Korea
kkim86@ajou.ac.kr

***Abstract*—In this paper, we propose a novel framework for leveraging digital twins to enhance ON/OFF-LINE blockchain networks in drone and IoT communication systems. The proposed solution addresses critical challenges in environments where internet connectivity is intermittent or restricted, such as construction sites, remote areas, or military operations. We present a resilient communication architecture that integrates Digital Twins (DTs) to mirror the state of offline blockchain nodes in the cloud, enabling efficient synchronization and reducing data conflicts when transitioning between online and offline states. The framework also introduces a method for efficient data management and secure, decentralized identity verification by using packaged certification with DID documents and self-contained verifiable credentials. By maintaining a synchronized digital twin in the cloud, the proposed system ensures that offline nodes can operate independently while seamlessly integrating updates when connectivity is restored.**

***Index Terms*—Blockchain, Offline certification, IoT, Decentralized ID, DID, Digital Twins**

I. Introduction

A. Background and Motivation

The increasing adoption of Internet of Things (IoT) devices across a wide range of industries has introduced significant challenges in ensuring reliable, secure, and continuous communication. Many IoT networks operate in environments where internet connectivity is intermittent or completely unavailable, such as remote construction sites, disaster zones, or in military settings [1]. Traditional blockchain solutions[2], which provide a high level of security and immutability, typically rely on continuous online connectivity, which presents a limitation for IoT applications in these environments [3]. To address these challenges, the concept of Digital Twins (DTs) has emerged as a powerful tool to mirror the physical state of IoT systems and provide a mechanism for resilient, decentralized management [4]. By combining digital twin technology with blockchain networks, it is possible to create a synchronized system that can function both online and offline, enabling IoT devices to operate seamlessly under varying connectivity conditions. This is particularly critical for applications such as drone operations, construction automation, and remote IoT installations, where any interruption in connectivity can lead to operational inefficiencies or security vulnerabilities.

B. Structure of the Paper

The remainder of this paper is organized as follows: Section 2 provides an overview of related work and section 3 describes the proposed system architecture. Section 4 presents the decentralized identity management approach, and section 5 outlines the implementation details. Section 6 discusses the security analysis, section 7 provides discussions and section 8 concludes the paper.

II. Related Work

A. Digital Twins in IoT and Blockchain

Digital Twin (DT) technology has gained significant traction as a means to mirror physical devices in the virtual world, enabling real-time monitoring and decision-making [4]. The combination of blockchain and digital twins offers a promising solution for addressing the challenges of decentralized IoT management, as it allows the state of offline nodes to be mirrored in the cloud, thus facilitating effective synchronization when connectivity is restored [5]. Studies have demonstrated the use of DTs in manufacturing, logistics, and remote monitoring applications, where real-time insights and predictive analytics can significantly enhance operational efficiency [6]. Integrating DTs with blockchain can further enhance the security and reliability of IoT networks by ensuring that all data changes are securely recorded and synchronized [7].

B. Limitations of Existing Approaches

While blockchain and digital twin technologies present significant potential for IoT communication, existing

approaches have notable limitations. One of the primary challenges is the synchronization of data between offline and online nodes. Traditional blockchain networks are not designed for environments where connectivity is unreliable, leading to potential inconsistencies and data conflicts when nodes reconnect [8]. Additionally, identity management in such hybrid environments is challenging, as most identity verification processes rely on constant online access to validate credentials against the blockchain [9]. Existing approaches also struggle to provide a secure mechanism for managing decentralized identifiers (DIDs) and verifiable credentials offline, which is crucial for environments like remote construction sites or military applications [3]. Recent studies have suggested the integration of self-contained verifiable credentials as a way to mitigate these limitations, allowing credentials to be verified without requiring a real-time connection to the blockchain [10]. However, practical implementations of such systems remain limited, particularly in scenarios where high security and scalability are required. This highlights the need for a more comprehensive framework that combines digital twins, blockchain, and self-contained verifiable credentials to create a resilient communication architecture for IoT systems operating in diverse connectivity conditions.

III. System Architecture

A. Overview of the Proposed Framework

The proposed framework integrates digital twins (DTs) with ON/OFF-LINE blockchain networks to provide a resilient architecture for IoT and drone communication systems. The system leverages digital twins to maintain a synchronized state of each blockchain node in a cloud-based environment, allowing offline nodes to operate independently and efficiently. The architecture consists of three key components: the Digital Twin Integration Layer, the ON/OFF-LINE Blockchain Network, and the Decentralized Identity Management System. The Digital Twin Integration Layer ensures that all changes made to the physical IoT devices are mirrored in their digital counterparts, thereby enabling real-time monitoring and effective decision-making even when nodes are offline [4]. The ON/OFF-LINE Blockchain Network supports data integrity and security by enabling nodes to function offline while maintaining data consistency through efficient synchronization mechanisms. The Decentralized Identity Management System employs packaged certification with DID documents and self-contained verifiable credentials to facilitate secure identity verification without requiring real-time blockchain connectivity [10].

B. ON/OFF-LINE Blockchain Network Design

1) Offline Operation and Data Management: In the proposed system, blockchain nodes can operate offline, allowing IoT devices in remote or restricted environments to continue functioning without immediate internet access [8]. Each offline node maintains a local ledger that records all transactions and device data while disconnected from the broader blockchain network. The Digital Twin Integration Layer serves as a representation of these offline nodes, which helps track their states and manage any data changes in a cloud environment [4]. The offline nodes use packaged certification with DID documents to verify identities locally. This certification contains all necessary cryptographic proofs, allowing nodes to authenticate devices even without access to the online blockchain network [9]. This reduces the dependency on real-time connectivity and ensures uninterrupted access control and data logging.

2) Synchronization Mechanisms: Once connectivity is restored, offline nodes initiate a synchronization process to merge their local ledger data with the main blockchain. This process includes reconciling transactions recorded during the offline period, resolving conflicts, and updating the Digital Twin Integration Layer to reflect the current state of each node [6]. A consensus mechanism is used to determine the final state of the blockchain, ensuring that no data is lost or overwritten during the synchronization phase [11]. The system also incorporates a conflict resolution algorithm that detects any inconsistencies between the offline node and the online blockchain. If a conflict is detected, the algorithm prioritizes transactions based on timestamps, digital signatures, and other criteria to maintain data integrity across the network [5].

IV. Decentralized Identity Management

A. DID Documents and Packaged Certification

Decentralized Identifiers (DIDs) are a cornerstone of the proposed identity management system. DIDs are used to create a secure, decentralized method for managing identities without the need for centralized authorities [10]. In the proposed framework, each IoT device is assigned a DID that acts as a unique identifier. These DIDs are combined with packaged certifications, which include all necessary information for authentication, such as cryptographic proofs and metadata about the credential issuer [10]. The packaged certification is designed to be verifiable offline, which is crucial for IoT nodes operating in environments without consistent connectivity. The certification is embedded directly within the DID document, creating a self-contained unit that allows other nodes or devices to verify the identity and credentials without needing to connect to an online blockchain [10]. This ensures that identity verification can occur in a decentralized manner, even when connectivity is restricted. The DID documents are also stored and updated in the Digital Twin Integration Layer, allowing any changes made offline to be mirrored in the corresponding digital twin in the cloud. Once connectivity is restored, these updates are synchronized with the main blockchain, ensuring that all

devices and nodes have access to the most current identity information [4].

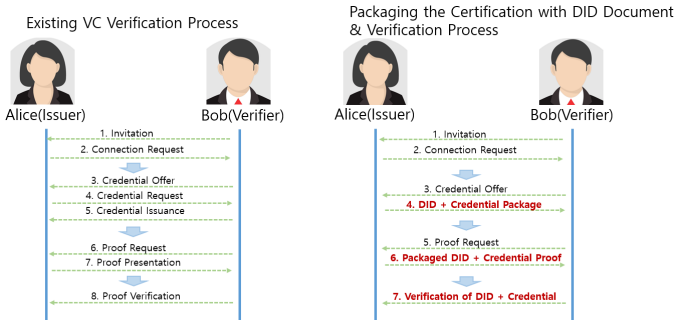

Fig. 1. Packaging the Certification with DID Document & Verification Process

B. Self-contained Verifiable Credentials

Self-contained verifiable credentials (VCs) play a critical role in ensuring that the identity of IoT devices can be securely verified without needing a constant connection to a blockchain [10]. In the proposed system, verifiable credentials are issued to each IoT device, containing information such as public keys, metadata, and cryptographic proofs that can be used to authenticate the device. The self-contained nature of these credentials means that they include all necessary data for verification within the credential itself, reducing dependency on external data sources [10]. This approach is particularly valuable in offline environments where devices need to prove their identity or authenticate themselves to other nodes. The credentials are issued by a trusted authority and are cryptographically signed, allowing other devices to verify the credential's authenticity without accessing the blockchain in real-time [9]. The self-contained VCs are embedded within the digital twin of each device, ensuring that the credentials are always synchronized with the latest device state. When connectivity is restored, any changes to the credentials or their status are updated in the main blockchain, maintaining the integrity and reliability of the identity management system [6].

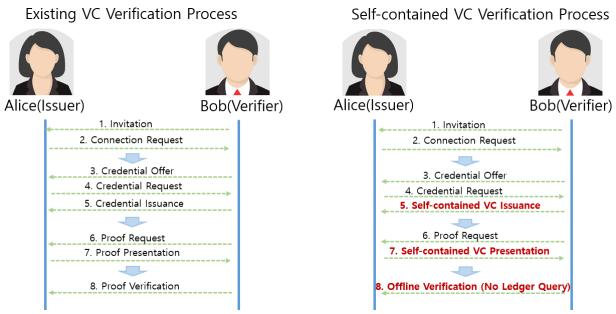

Fig. 2. Self-contained VC Verification Process

C. Identity Verification in Offline Environments

One of the main challenges of decentralized identity management is ensuring secure identity verification in offline environments. The proposed system uses a combination of DID documents and self-contained verifiable credentials to achieve this. When an IoT device needs to authenticate itself, it provides its DID document along with its verifiable credential to the verifying entity. The verifier can check the cryptographic proofs included in the credential and confirm the identity of the device without needing to query the blockchain [4]. This offline verification capability is particularly useful in scenarios such as remote construction sites or military operations, where internet connectivity is unreliable or absent. By using self-contained credentials, the system reduces the risk of identity spoofing or unauthorized access, as all verification data is included within the credential and can be independently verified [3]. Furthermore, the use of packaged certifications ensures that the verifier can trust the authenticity and integrity of the credential, even when operating in offline conditions [10]. The proposed Decentralized Identity Management System thus provides a robust solution for managing identities in IoT environments with limited connectivity. By leveraging DIDs, packaged certifications, and self-contained verifiable credentials, the system ensures secure, decentralized identity verification without the need for constant blockchain access.

V. Implementation

A. Pilot Study in IoT Communication

A pilot study was conducted to validate the real-world applicability of the proposed framework in an IoT communication scenario. The study involved deploying a small-scale IoT network consisting of sensor devices at a remote construction site. Each device was equipped with digital twin capabilities and connected to a blockchain node that operated both online and offline, depending on network availability. The gateway node served as a mediator, collecting data from offline nodes and synchronizing with the main blockchain when connectivity was restored [6]. During the pilot, we evaluated the packaged certification process for identity verification, which allowed devices to authenticate themselves even while offline. The self-contained verifiable credentials were tested under various conditions, including extended periods without connectivity, to determine their effectiveness in maintaining secure identity management [10]. The pilot study also provided insights into the practical challenges of deploying such a system, including power management, latency, and data integrity when transitioning between online and offline states.

B. Technical Specifications and Tools Used

The implementation of the proposed framework involved a combination of software and hardware tools designed to

support the integration of digital twins with blockchain technology:

- Blockchain Platform: Hyperledger Indy was used to implement the blockchain network, providing the necessary features for permissioned access, authentication, and data immutability.
- Digital Twin Modeling: Digital twins were developed using Python and integrated with the blockchain using RESTful APIs to enable real-time updates. Docker was used to containerize the digital twin services, ensuring scalability and ease of deployment [5].
- Identity Management: Aries Cloud Agent Python (ACA-Py) was utilized to manage DID documents and issue self-contained verifiable credentials. This allowed the system to facilitate decentralized identity verification for IoT devices, even in offline environments [10].

The technical implementation emphasized modularity and scalability, allowing the framework to be adapted for different IoT applications and network configurations. The use of containerization ensured that the individual components could be deployed in a distributed manner, while the integration with digital twins provided a unified view of the entire system's state, both online and offline [7].

VI. Security Analysis

A. Threat Modeling and Attack Surface

The proposed system's security was evaluated through threat modeling, which identified potential vulnerabilities and attack vectors that could be exploited in both online and offline scenarios. The key threats include data tampering, identity spoofing, replay attacks, and man-in-the-middle (MITM) attacks. Offline nodes are particularly susceptible to tampering and spoofing due to their disconnection from the main blockchain network, making it critical to establish robust local verification mechanisms [3]. The attack surface includes all communication channels between IoT devices, digital twins, and the blockchain network, as well as the data storage within digital twins and offline nodes. By identifying these areas, the system was fortified with security measures that specifically address the risks posed by intermittent connectivity [9].

B. Security Mechanisms and Protocols

To mitigate the identified threats, several security mechanisms were integrated into the framework. These mechanisms include:

- Self-contained Verifiable Credentials: The use of self-contained verifiable credentials ensures that each IoT device can authenticate itself locally, reducing the risk of identity spoofing even when offline [10]. These credentials are cryptographically signed and contain all necessary verification information, ensuring that identity can be confirmed without real-time blockchain access.
- Packaged Certification with DID Documents: The incorporation of packaged certifications in DID documents enables secure offline verification. By embedding necessary cryptographic proofs within the DID, devices can validate identities independently, preventing unauthorized access and replay attacks [9].
- Data Integrity Checks: Hashing algorithms were employed to maintain data integrity within offline nodes. Any alteration of data is detectable upon reconnection to the blockchain, as the hash values will no longer match the original state recorded on the blockchain [11].
- Encryption for Communication Channels: All communication between devices and the digital twin integration layer is encrypted using end-to-end encryption to prevent MITM attacks.

VII. Discussion

A. Connectivity, Security, and Scalability Analysis

The connectivity analysis demonstrated that the integration of digital twins effectively mitigates the challenges associated with maintaining consistent states between offline and online nodes. The digital twin layer enabled real-time monitoring of each IoT node's state, even when it was disconnected from the main blockchain network, reducing synchronization delays upon reconnection. The integration of packaged certification with DID documents provided an additional layer of security, allowing nodes to authenticate independently of the blockchain network, which was crucial for maintaining security in remote settings [10]. The scalability analysis highlighted that the proposed framework can efficiently handle increasing numbers of IoT nodes by utilizing containerized digital twin instances. The ability to manage both small-scale and large-scale deployments, while maintaining synchronization and security, underscores the scalability of the proposed framework.

B. Comparison with Existing Solutions

The proposed framework was compared with existing blockchain-based IoT solutions that do not utilize digital twins. Traditional blockchain approaches struggle with synchronization issues and data inconsistency when nodes operate offline, leading to significant data conflicts upon reconnection [3]. And identity management in existing systems typically requires real-time access to the blockchain for credential verification, which is impractical in environments with intermittent connectivity. The use of self-contained verifiable credentials in the proposed model allows for offline verification, eliminating the need for constant blockchain access [10].

VIII. Conclusion

A. Summary of Findings

This paper has introduced a novel framework for leveraging digital twins to enhance ON/OFF-LINE blockchain networks in drone and IoT communication systems. The proposed solution addresses significant challenges in environments with intermittent or restricted connectivity, such as

construction sites and remote areas. By integrating digital twins with blockchain networks, the system allows IoT devices to operate autonomously and securely, even in offline conditions. The framework's implementation of packaged certification with DID documents and self-contained verifiable credentials enabled secure identity verification and data synchronization without the need for continuous blockchain access. Our results demonstrated that the system provides effective connectivity, security, and scalability, ensuring robust IoT device authentication and communication. The use of digital twins facilitated efficient data conflict resolution, resulting in reduced synchronization delays and enhanced operational reliability.

B. Future Work

While the proposed framework has proven effective, there are areas for further exploration and improvement. One potential area of future work is to optimize the synchronization protocol for scenarios involving a large number of IoT devices attempting to reconnect simultaneously. This could involve exploring distributed synchronization mechanisms or machine learning-based predictive synchronization to further enhance the system's efficiency. Additionally, the management of self-contained verifiable credentials in offline environments requires further refinement. Future iterations of the framework may include mechanisms for time-based credential expiration or automated credential renewal to ensure the validity and security of credentials, particularly for devices that remain offline for extended periods [10]. Implementing lightweight container orchestration techniques could also help in managing the deployment and maintenance of digital twin instances in dynamic environments such as construction sites.

C. Implications for IoT and Blockchain Research

The integration of digital twins with ON/OFF-LINE blockchain networks presents a promising direction for enhancing the resilience and scalability of IoT communication systems. This research contributes to the growing body of knowledge on how blockchain and digital twin technologies can be combined to create more robust and flexible IoT solutions capable of handling diverse connectivity conditions. The findings suggest that incorporating digital twins into blockchain-based IoT systems can address many of the existing limitations related to synchronization, data integrity, and identity verification. These insights can be applied to various industries, including construction, logistics, and remote monitoring, where reliable IoT communication is critical. Future research should continue to explore how these technologies can be integrated to provide end-to-end secure and efficient solutions for IoT device management in environments with unreliable connectivity.

ACKNOWLEDGMENT

This research was supported in part by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2024-2021-0-01835) supervised by the IITP(Institute for Information & Communications Technology Planning & Evaluation), and Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (2021-0-00590, RS-2021-II210590, Decentralized High Performance Consensus for Large-Scale Blockchains).

REFERENCES

[1] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[2] E. Androulaki et al., "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, 2018.
[3] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and solutions," [Online]. Available: https://arxiv.org/abs/1608.05187, 2017.
[4] F. Tao, H. Zhang, A. Liu, and A. Y. Nee, "Digital twin in industry: State-of-the-art," *IEEE Trans. Ind. Informat.*, vol. 15, no. 4, pp. 2405–2415, 2018.
[5] R. Rosen, G. von Wichert, G. Lo, and K. D. Bettenhausen, "About the importance of autonomy and digital twins for the future of manufacturing," *IFAC-PapersOnLine*, vol. 48, no. 3, pp. 567–572, 2015.
[6] A. Fuller, Z. Fan, C. Day, and C. Barlow, "Digital twin: Enabling technologies, challenges and open research," *IEEE Access*, vol. 8, pp. 108952–108971, 2020.
[7] A. Saddik, "Digital twins: The convergence of multimedia technologies," *IEEE MultiMedia*, vol. 25, no. 2, pp. 87–92, 2018.
[8] K. Wang, Z. Tang, J. Zhenzhou, and H. Shufan, "Multi-stage data synchronization for public blockchain in complex network environment," *Comput. Netw.*, vol. 207, pp. 108952, 2023.
[9] Z. Yang et al., "BDIDA-IoT: A blockchain-based decentralized identity architecture enhances the efficiency of IoT data flow," *MDPI Sensors*, vol. 24, pp. 11–15, 2024.
[10] M. Sporny et al., "Verifiable credentials data model v2.0," 2024. [Online]. Available: https://www.w3.org/TR/vc-data-model-2.0/
[11] X. Feng et al., "Blockchain and digital twin empowered trustworthy self-healing for edge-AI enabled industrial Internet of things," *Inf. Sci.*, vol. 637, pp. 67–78, 2023.