Blockchain-Based Self-Sovereign Identity in 6G Non-Public Networks: Enhanced Security in Industrial Cyber-Physical Systems

Abdullah Aydeger[†] and Engin Zeydan[*]
[†] Dept. of Electrical Engineering and Computer Science, Florida Institute of Technology, Melbourne, FL, USA
[*]Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Barcelona, Spain, 08860.
Email: aaydeger@fit.edu, ezeydan@cttc.cat

***Abstract*—The industrial sector's digital transformation under Industry 4.0 necessitates robust, scalable, and secure communication frameworks. 6G technology, particularly its non-public network (NPN) configurations, offers promising solutions for industrial cyber-physical systems (ICPS). However, security and privacy remain significant challenges, especially concerning identity management in these networks. This paper proposes the integration of blockchain-based Self-Sovereign Identity (SSI) within 6G NPNs as a novel approach to enhance security and data privacy. We explore how this combination can provide decentralized identity management, reduce reliance on centralized authorities, and increase trustworthiness within industrial networks. The paper also examines real-world scenarios and provides a detailed analysis of deployment models, highlighting the potential benefits and challenges of integrating blockchain-based SSI into 6G networks.**

***Index Terms*—SSI, Blockchain, NPN, 6G**

I. Introduction

The evolution of industrial communication systems is heavily driven by the emergence of 6G technology, which supports various demanding applications within Industry 4.0. Among the various deployment models, 6G Non-Public Networks (NPNs) are of particular interest for their ability to offer customized, secure, and efficient communication solutions tailored to specific industrial needs. However, identity management within these networks remains a critical issue, particularly with the increasing number of connected devices and the need for secure access control. Self-Sovereign Identity (SSI) is an emerging paradigm that allows entities to manage their identities independently, without relying on a central authority. When combined with blockchain technology, SSI offers a decentralized and tamper-proof identity management system that enhances security and privacy. Blockchain-based SSI has emerged as a promising solution for decentralized identity management that offers more security and privacy compared to traditional identity systems. Previous Works have shown the effectiveness of SSI in various domains, including transportation,supply chain management and smart cities, where secure and verifiable identities are crucial [1], [2]. The application of SSI in wireless networks, particularly in 5G environments, has been explored in studies such as [3], [4], which highlight the potential of blockchain to eliminate central points of failure and provide tamper-proof identity verification. The evolution of mobile networks from 5G to 6G is expected to bring significant advances in terms of speed, latency and the number of connected devices. However, these improvements also bring new security challenges, especially in the context of NPNs used for industrial applications. Existing research has begun to address these challenges, with a focus on integrating secure communication protocols, improving data privacy, and ensuring the reliability of critical infrastructure. For example, [5] and [6] investigate the impact of 5G networks on industrial security, identify key vulnerabilities and propose mitigation strategies.

Several studies have investigated the integration of blockchain with 5G networks to improve security and trust in decentralized environments [7]. For example, [8] proposes a blockchain-based framework for managing IoT devices in 5G networks, which ensures that only authenticated and authorized devices can access network resources. Similarly, [9] explores the use of blockchain for secure spectrum sharing in 5G and highlights the benefits of decentralized control in managing network resources. While these studies provide a solid foundation, the transition to 6G networks is likely to bring new opportunities and challenges, especially in the context of industrial NPNs. Security analysis of blockchain-integrated networks has been a focus of recent research, with studies investigating the robustness of blockchain-based systems against various attack vectors. The research in [10] addresses the specific security benefits of using blockchain for identity management and data integrity in IoT and cyber-physical systems, emphasizing the importance of decentralized trust mechanisms. These studies highlight the need for comprehensive security frameworks that can adapt to the evolving threat landscape in 6G environments. The authors in [11] consider enablers of 5G and investigate industrial use cases and deployment choices. However, their options are not integrated with potential benefits of blockchain and blockchain-based SSI.

As 6G networks aim to support a variety of applications with stringent performance requirements, the need for robust security solutions becomes even more important. Recent research papers such as [12] and [13] discuss the potential

978-3-903176-66-9 ©2024 IFIP

of 6G to revolutionize the industry through the integration of AI, edge computing and blockchain technologies. These studies suggest that 6G will not only improve the connectivity and efficiency of industrial systems, but will also require new approaches to ensure security and privacy in these increasingly autonomous and connected environments. However, while significant progress has been made in researching the integration of blockchain and 5G networks, the transition to 6G brings new challenges and opportunities for improving security in industrial cyber-physical systems. The convergence of blockchain technology and next-generation wireless networks has attracted considerable interest in recent years, particularly in the context of improving security for Industrial Cyber-Physical Systems (ICPS). As mentioned above, previous research has explored various aspects of integrating blockchain with 5G networks, focusing on identity management, data integrity and secure communications. However, as the vision for 6G networks begins to take shape, there is a growing need to investigate how these advanced technologies can be used to address new security challenges in increasingly complex and interconnected industrial environments. This paper builds on existing research and proposes a novel approach for the integration of blockchain-based SSI into non-public 6G networks. It targets the specific security requirements of next-generation industrial applications and specifically addresses the current challenges in identity management, while improving the overall security posture of industrial cyber-physical systems.

II. Background

A. Blockchain-Based Self-Sovereign Identity (SSI)

Blockchain technology provides a decentralized and immutable ledger, making it an ideal foundation for SSI systems [14]. In a blockchain-based SSI framework, each entity (such as a device, user, or application) holds a unique cryptographic identity stored on the blockchain. This identity is controlled solely by the entity itself, ensuring that no third-party can alter or revoke it without permission. This decentralized control over identity significantly reduces the risks associated with traditional identity management systems, which often rely on centralized databases that are vulnerable to breaches, manipulation, and unauthorized access.

The integration of SSI with 6G NPNs addresses several critical challenges in identity management. First, the decentralized nature of blockchain ensures that identities are not stored in a single, centralized location, thereby reducing the risk of large-scale identity theft and centralized attacks, such as data breaches or distributed denial-of-service (DDoS) attacks. Blockchain's cryptographic security further enhances the protection of identity data, making it nearly impossible for unauthorized entities to access, alter, or impersonate the stored identities. Each identity transaction—such as the creation, updating, or verification of identity—is recorded on the blockchain in an immutable, time-stamped ledger, providing a transparent and auditable history that strengthens trust and accountability. Moreover, the use of smart contracts within blockchain-based SSI frameworks introduces automation and conditional logic to identity management processes. For example, a smart contract can be programmed to automatically grant or revoke access to network resources based on predefined conditions, such as the expiration of credentials or a change in the entity's status. This level of automation not only enhances the efficiency of identity management but also reduces the potential for human error, further strengthening the security and reliability of the system.

Blockchain-based SSI also supports interoperability across different platforms and networks. As 6G networks are expected to support a diverse range of applications and devices, the ability of blockchain SSI to function seamlessly across different environments is a crucial advantage. Interoperability ensures that identities can be securely verified and authenticated across multiple networks, including public and private 6G NPNs, without the need for duplicate identity registrations or reliance on third-party identity providers. In summary, blockchain-based SSI offers a robust, decentralized, and secure solution for identity management in 6G NPNs, addressing the limitations of traditional identity systems and paving the way for more secure and efficient network operations in the context of industrial cyber-physical systems.

B. 6G Non-Public Networks Overview

6G Non-Public Networks (NPNs) represent the next evolution of private network solutions, specifically tailored to meet the increasingly demanding requirements of industrial and enterprise applications. Building on the advancements of 5G, 6G NPNs are designed to offer unparalleled levels of performance, flexibility, and security. These networks can be deployed in various configurations, ranging from fully isolated environments to more integrated setups where they interact with public networks, depending on the specific operational needs and security requirements of the application. One of the defining features of 6G NPNs is their ability to support ultra-reliable low-latency communication (URLLC), massive machine-type communications (mMTC), and enhanced mobile broadband (eMBB) within a single, cohesive network. This versatility allows 6G NPNs to cater to a wide array of industrial use cases, such as real-time process control in manufacturing, remote operation of critical infrastructure, and seamless integration of autonomous systems. The enhanced capabilities of 6G, including peak data rates in the terabit range, sub-millisecond latency, and the ability to connect millions of devices per square kilometer, make 6G NPNs ideally suited for complex, high-stakes environments like smart factories, energy grids, and autonomous transportation systems. Another critical aspect of 6G NPNs is their focus on data ownership and privacy. In industrial settings, the ability to maintain control over data is paramount, particularly when dealing with sensitive operational information or proprietary technologies. 6G NPNs allow organizations to keep data processing and storage within the confines of their own networks, thus minimizing the risk of data leakage or unauthorized access. This level of control is especially important in industries where intellectual property, regulatory compliance, and competitive advantage are tightly linked to data security. The architecture of 6G NPNs also emphasizes the integration of advanced technologies such as artificial intelligence (AI), machine learning (ML), and edge computing. AI and ML can be utilized to optimize network performance, predict and prevent security threats, and automate decision-making processes in real-time. Edge computing, on the other hand, brings computational resources closer to the data source, reducing latency and enabling faster processing of large datasets generated by industrial IoT devices and sensors. This edge-centric approach is particularly beneficial in scenarios where real-time processing is critical, such as in autonomous vehicles or critical infrastructure management.

Security is a cornerstone of 6G NPNs, which are designed to be resilient against a wide range of cyber threats. The integration of quantum-resistant encryption algorithms and secure multi-party computation ensures that sensitive data remains protected, even against future quantum computing attacks. Moreover, the concept of network slicing—first introduced in 5G—has been further refined in 6G to provide even more granular control over network resources, allowing for the creation of highly secure, isolated network slices tailored to specific applications or user groups. In summary, 6G NPNs represent a significant leap forward in private network technology, offering enhanced performance, security, and flexibility. These networks are poised to become the backbone of next-generation industrial and enterprise applications, supporting a wide range of use cases with stringent requirements for reliability, latency, and data security.

III. 6G Non-Public Networks Scenarios

Each 6G NPN deployment models can have its own set of advantages and challenges, particularly concerning data security and privacy. In an isolated deployment, the 6G NPN can operate independently of any public network, providing the highest level of security and control. Public Network Integrated NPNs (PNI-NPNs), on the other hand, share certain components with public networks, which can introduce vulnerabilities if not properly managed. Regardless of the deployment model, secure identity management is crucial to protect against unauthorized access and data breaches. Detailed scenarios for each deployment option are described below.

1. Isolated Deployment (Private 6G NPN): In an isolated deployment, the 6G network is entirely private, with no connection to public networks. This setup is typically used for highly secure environments, such as industrial plants or military bases, where control over network resources and data is crucial as shown in Fig. 1. *In a secure manufacturing facility scenario,* a secure manufacturing facility uses an isolated 6G NPN to connect various devices, including robotic arms, sensors, and industrial machines. Each device is equipped with a blockchain-based SSI. Each device and operator within the network has a unique, SSI recorded on a blockchain. This ensures that only authenticated devices and personnel can interact with critical systems, reducing the risk of unauthorized access. When a new machine or device is added to the network, it must first be registered on the blockchain, where its identity is verified and stored. The blockchain-based SSI system automatically checks and authenticates the identity of each device or user before they are allowed to access the network. If a device tries to connect without a valid identity, it is automatically blocked. This setup ensures that even in a fully isolated environment, security is maintained at the highest level, with no single point of failure for identity management.

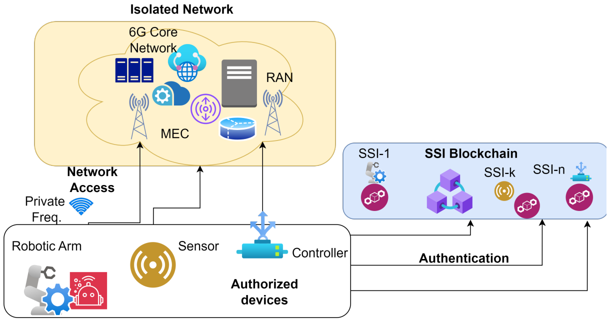

Fig. 1: Blockchain-Based SSI in Isolated 6G NPN Deployment.

2. Public Network Integrated NPN (PN-I-NPN) - Shared Access Network: In this deployment model, the 6G NPN shares the Radio Access Network (RAN) with a public network, but the core network remains private as shown in Fig. 2. *In a smart grid management scenario,* a smart grid system uses a shared access network PNI-NPN to connect its sensors and control systems. The grid management system needs to ensure that only authorized devices and operators can control the grid. Blockchain-based SSI can be used to manage the identities of all devices and users connected to the smart grid. Each device, whether it's a sensor or a control system, has a blockchain-verified identity. The smart contracts on the blockchain enforce access control policies based on these identities. When a control signal is sent to adjust the grid's operations, the system first verifies the sender's identity via the blockchain. Only signals from authorized, blockchain-verified identities are accepted. If an identity is compromised or an unauthorized device attempts to send commands, the system automatically rejects the signal. This model allows the smart grid to maintain high levels of security and operational integrity while benefiting from the broader coverage and flexibility of a shared public network.

3. Shared Access Network and Control Plane: In this deployment option, both the RAN and control plane are shared with the public network, but the user plane and data remain within the private network as shown in Fig. 3. *In an autonomous vehicle fleet management scenario:* A company manages a fleet of Autonomous Vehicles (AVs) for delivery services. The AVs are connected through a 6G NPN that shares the access network and control plane with a public 6G network. Each vehicle in the fleet has a blockchain-based SSI that verifies its identity. This identity is used to manage access to network resources and to communicate securely with other vehicles and the central management system. As

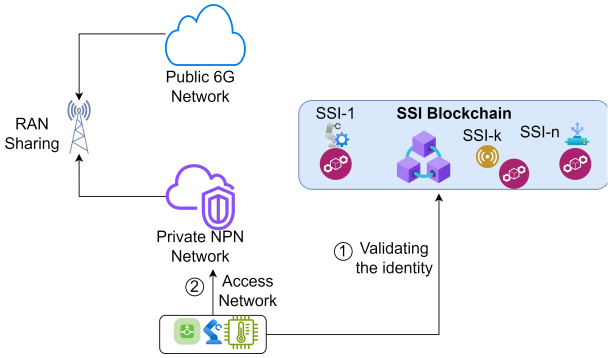

Fig. 2: Blockchain-Based SSI in 6G NPN with Shared Access Network.

vehicles move between different geographic regions, they maintain connectivity through the public network's RAN and control plane. However, all sensitive data and operational commands are managed within the private user plane of the NPN. Blockchain SSI ensures that only vehicles with verified identities can access these resources or communicate with each other, preventing potential hijacking or unauthorized commands. This approach allows for secure, seamless operation across wide areas, utilizing the public network's coverage while ensuring that sensitive operations are protected within the private network infrastructure.

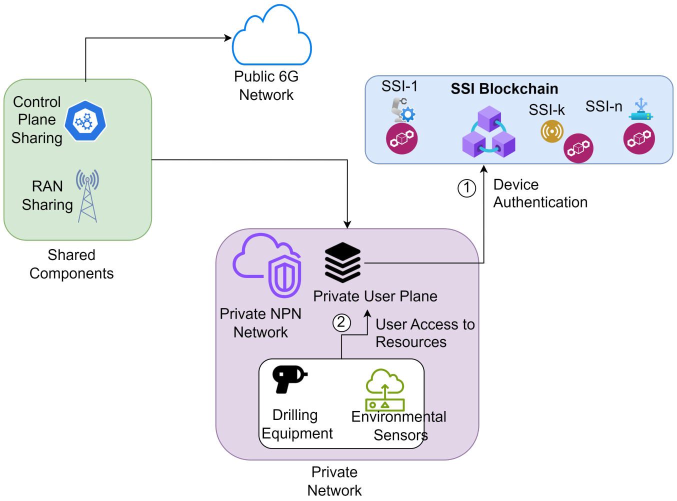

Fig. 3: Blockchain-Based SSI in 6G NPN with Shared Access Network and Control Plane.

4. PN-I-NPN - Hosted by Public Network Operator: In this option, the entire 6G NPN is hosted by a public network operator, with the network infrastructure provided and managed by the operator, but logically separated for the private network's use as shown in Fig. 4. *In an industrial IoT network for a multi-site enterprise scenario,* a large enterprise operates several manufacturing sites across the country, connected through a 6G NPN hosted by a public network operator. The enterprise uses blockchain-based SSI to manage the identities of all devices, machines, and operators across all sites. Each site's devices are registered on the blockchain, ensuring that only authorized entities can interact with the network. When an operator at one site attempts to access resources or send commands to another site, their identity is verified through the blockchain. The system automatically enforces access policies based on the verified identity, ensuring that only authorized actions are allowed across the network. The hosted deployment allows the enterprise to scale its operations across multiple sites while maintaining a high level of security and control over its network resources through blockchain-based identity management.

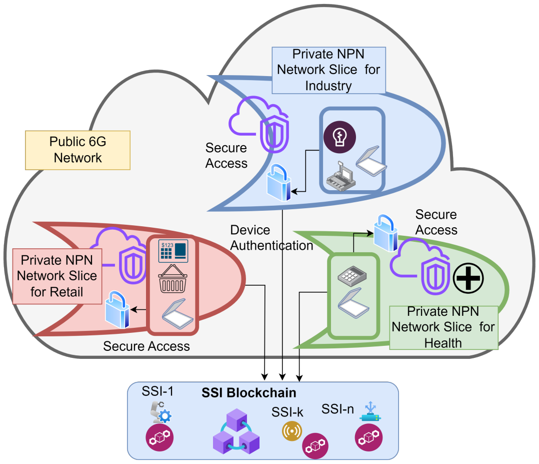

Fig. 4: Blockchain-Based SSI in Fully Hosted 6G NPN by Public Network Operator

5. PN-I-NPN - Shared Access Network and Control Plane with Cloud-Native Approach: In this deployment, the network shares both the RAN and the control plane with the public network, and the core network functions are hosted in the cloud as given in Fig. 6. *In a smart healthcare network scenario,* a smart healthcare system operates across multiple hospitals and uses a cloud-hosted 6G NPN to manage patient records, medical devices and communication systems. Blockchain SSI ensures that all medical devices, patient records and healthcare personnel are authenticated before they can access or share sensitive healthcare data. Medical devices and systems use blockchain-verified identities to communicate securely with cloud-hosted health information systems. Only authorized personnel can access patient data or issue commands to medical devices. This enables secure, scalable healthcare operations with decentralized identity management and centralized cloud resources, ensuring patient data protection and system integrity.

6. PN-I-NPN - Fully Hosted by Public Network Operator with Cloud-Native Approach: This deployment is similar to option 5, but all elements, including the user plane, are hosted by the public network operator. In a smart city Infrastructure scenario, a city's infrastructure is managed via a fully hosted 6G NPN, covering everything from traffic management to public utilities. The blockchain-based SSI is used to manage and authenticate all devices and systems within the city's infrastructure, such as traffic lights, surveillance cameras and utility meters. The blockchain verifies the identity of each device and user and ensures that only authorized entities can

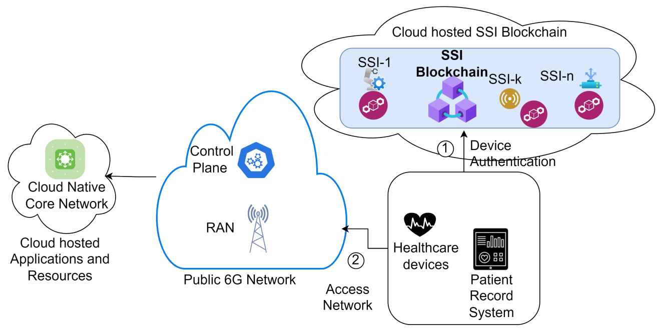

Fig. 5: Blockchain-Based SSI in Cloud-Native 6G NPN with Shared Access Network and Control Plane

control or modify the city's infrastructure. For example, traffic signals can only be altered by verified city employees. The blockchain provides a secure, efficient and scalable solution for managing city infrastructure, with the added security of decentralized identity management ensuring the integrity and security of critical public systems.

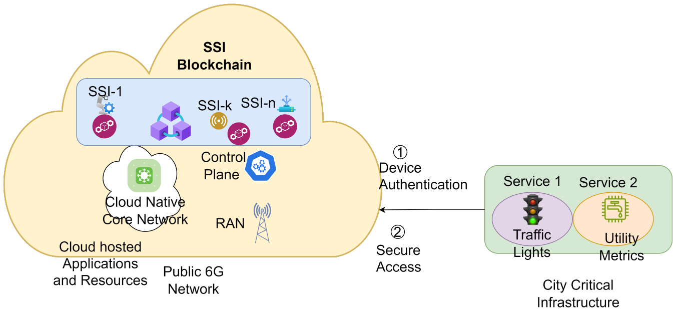

Fig. 6: Blockchain-based SSI in fully hosted cloud-native 6G NPN by Public Network Operator.

IV. Security Threats and Analysis of Deployment Scenarios

In all of the above scenarios, the success of integrating blockchain-based SSIs depends on careful implementation and ongoing security management to ensure that the benefits of decentralized identity management are fully exploited without creating new vulnerabilities.

A. Security Threats

This section outlines the potential security threats specific to each deployment scenario involving the integration of blockchain-based SSI with 6G NPNs. We highlight both the strengths of blockchain SSI in mitigating certain risks and the new challenges introduced by the network configurations.

1. Isolated Deployment (Private 6G NPN) Security Threats: *(i) Insider Threats:* Employees or devices within the isolated network could potentially misuse their access to sensitive data or systems. This is particularly dangerous since the threat originates from within a trusted environment. *(ii) Physical Security Breaches:* Because the network is isolated, physical access to network components or devices could allow an attacker to gain unauthorized access to the network or tamper with blockchain nodes. *(iii) Malware Introduction:* Malware could be introduced into the network through infected devices or removable media, potentially disrupting operations or corrupting the blockchain ledger. *(iv) Denial of Service (DoS) Attacks:* While external DoS attacks are less likely, an insider could initiate a DoS attack that overwhelms the network, causing disruptions to services and potentially hindering access to the blockchain for identity verification.

2. PN-I-NPN) - Shared Access Network Security Threats: *(i) Man-in-the-Middle (MitM) Attacks:* In a shared RAN environment, attackers could potentially intercept communications between devices and the core network, leading to data breaches or unauthorized access. *(ii) RAN Exploitation:* The shared RAN might be targeted for attacks such as jamming, eavesdropping, or unauthorized access, which could disrupt the operation of the private NPN. *(iii) Side-Channel Attacks:* Attackers could exploit side-channel information from the shared RAN or public network components to infer sensitive data or identity information. *(iv) Spillover Attacks:* Vulnerabilities in the public network could spill over into the private NPN, especially if there are insufficient isolation mechanisms in place between the public and private network segments.

3. Shared Access Network and Control Plane Security Threats: *(i) Control Plane Hijacking:* Since the control plane is shared with the public network, there is a risk that attackers could hijack control plane traffic, leading to unauthorized configuration changes or resource allocation. *(ii) Identity Spoofing:* Despite the presence of blockchain SSI, if the control plane is compromised, attackers could potentially attempt to spoof identities or manipulate identity data before it reaches the blockchain for verification. *(iii) Protocol Exploitation:* The shared control plane may be vulnerable to protocol-level attacks that exploit weaknesses in communication protocols, leading to service disruption or unauthorized access. *(iv) Service Degradation:* Attackers could target the control plane with signaling storms or other forms of service degradation, impacting the availability and performance of the private user plane.

4. PN-I-NPN - Hosted by Public Network Operator Security Threats: *(i) Operator-Level Threats:* Since the NPN is hosted by a public network operator, any compromise at the operator level could affect the security of the entire private network. This includes insider threats or breaches within the operator's infrastructure. *(ii) Cross-Tenant Attacks:* In a multi-tenant environment, there is a risk of attacks where one tenant's compromised resources are used to launch attacks against another tenant, potentially affecting the private NPN. *(iii) Data Exfiltration:* An attacker could attempt to extract sensitive data from the private NPN by exploiting weaknesses in the operator's infrastructure or through misconfigured network slices. *(iv) Trust Exploitation:* The private network's reliance on the public operator introduces a level of trust that could be exploited if the operator's systems or personnel are compromised.

5. PN-I-NPN - Shared Access Network and Control

Plane with Cloud-Native Approach Security Threats: *(i) Cloud Provider Compromise:* Since the core network functions are hosted in the cloud, a compromise of the cloud provider's infrastructure could lead to unauthorized access, data breaches, or service disruptions. *(ii) Data Breaches:* Sensitive identity and network data could be exposed if cloud storage or processing resources are compromised, especially if encryption or access control mechanisms are weak. *(iii) Service Availability Attacks:* Attacks targeting cloud resources, such as distributed denial-of-service (DDoS) attacks, could significantly impact the availability of critical network functions and the blockchain SSI system. *(iv) Shared Resource Exploitation:* The shared nature of cloud resources introduces the risk of side-channel attacks or exploitation of shared infrastructure vulnerabilities, potentially leading to data leakage or identity spoofing.

6. PN-I-NPN - Fully Hosted by Public Network Operator with Cloud-Native Approach Security Threats: *(i) Total Infrastructure Dependency:* The full reliance on the public network operator and cloud provider for all network functions introduces significant risk if either is compromised. A breach at the operator level could have cascading effects across all aspects of the NPN. *(ii) Inter-Slice Contamination:* Although network slices are logically isolated, a sophisticated attack could potentially bridge slices, leading to data leakage or unauthorized access between different tenant environments. *(iii) Quantum Threats:* As 6G introduces quantum-resistant cryptography, the transition period may introduce vulnerabilities where attackers could exploit legacy encryption methods before the full implementation of quantum-safe algorithms. *(iv) Supply Chain Attacks:* The use of third-party cloud services introduces risks related to the supply chain, where vulnerabilities in third-party software or hardware could be exploited to gain unauthorized access to the network or blockchain.

B. Security Analysis

A detailed security analysis for each of the six deployment scenarios when integrating blockchain-based SSI into 6G NPNs is as follows.

1- In an isolated deployment, security is particularly robust due to the complete isolation of the network from external threats, which significantly reduces the risk of attacks such as Distributed Denial-of-Service (DDoS). The integration of the blockchain-based SSI further enhances this by decentralizing identity management and thus eliminating single points of failure. This decentralized approach ensures that even if a device's identity is compromised, it cannot be used to access the network without blockchain verification. The immutable nature of blockchain records prevents identity spoofing and unauthorized access, while smart contracts can enforce strict access control policies that ensure only verified entities can interact with critical systems. However, this setup is not without its challenges. The biggest risk in an isolated deployment comes from insider threats, where a legitimate user could abuse their access. Even though the blockchain offers a high level of security, the system could be vulnerable if the blockchain infrastructure itself is compromised, although this is highly unlikely in a private blockchain scenario. Furthermore, managing a private blockchain can be resource-intensive, which can lead to performance bottlenecks in high-throughput environments.

2- In NPN-I-PN - Shared Access Network deployment model, where the private non-public network (NPN) shares the radio access network (RAN) with a public network, blockchain-based SSI plays a crucial role in securing access to the private core network. By ensuring that only authenticated devices and users can interact with the private core, the risk of unauthorized access from the public network is mitigated. Blockchain also improves data integrity by protecting against tampering and man-in-the-middle attacks during data transmission. In addition, the use of network slicing helps to isolate different services and ensures that even if one slice is compromised, the others remain secure. However, the shared RAN has some vulnerabilities. The RAN could be a target for attacks such as jamming or eavesdropping, which could compromise the availability and confidentiality of the private NPN. In addition, vulnerabilities in the public network could potentially impact the private network, although blockchain SSI helps mitigate identity-related risks. The complexity of managing blockchain SSI in a shared RAN environment is another consideration, as it requires careful coordination to avoid latency.

3- In the Shared Access Network and Control Plane scenario, both the RAN and the control plane are shared with the public network, but the user plane remains private. Blockchain SSI provides robust identity verification across these components. This setup protects against identity spoofing and ensures that sensitive resources within the private user plane are only accessible to verified entities. However, sharing the control plane with the public network increases the risk of attacks such as signaling storms on the control plane or hijacking, which could disrupt the availability of services. The shared infrastructure also poses a risk: Vulnerabilities in the control plane of the public network could affect the private network. In addition, the need to verify identities via the blockchain before access is granted could lead to latency, especially for time-critical industrial applications.

4. In NPN-I-PN - Hosted by Public Network Operator scenario, the entire 6G NPN is hosted by a public network operator. Blockchain-based SSI provides a scalable and secure means of managing identities across multiple locations. This approach allows enterprises to maintain control over identity verification and access policies, even within a public operator's infrastructure, reducing dependence on the operator's security measures. Logical isolation of the NPN within the public network minimizes the attack surface, and the blockchain ensures that only authorized entities can interact with critical enterprise systems. However, trust in the operator of the public network is a potential vulnerability, as any compromise of the operator's infrastructure could affect the enterprise's operations. There are also risks with multiple tenancies, as there is a possibility of data leakage or cross-contamination between different tenants, although blockchain SSI mitigates identity-related risks. In addition, the enterprise is dependent on the operator's infrastructure, which could be a problem if the operator's security is compromised.

5- In NPN-I-PN - Shared Access Network and Control Plane with Cloud-Native deployment, the network shares both the RAN and the control plane with the public network and the core network functions are hosted in the cloud. Blockchain-based SSI integrated with cloud-native services provides strong security for identity management. This setup protects against unauthorized access to distributed cloud resources and ensures the secure handling of sensitive data such as healthcare records. The cloud-native approach enables dynamic resource allocation, with the blockchain SSI ensuring that only authenticated devices and users can access these resources. However, hosting network functions in the cloud introduces potential risks such as data breaches or denial of service attacks on the cloud infrastructure. Integrating blockchain SSI with cloud-native functions could also lead to latency, especially if multiple blockchain nodes are required to verify transactions. In addition, managing blockchain SSI over cloud-native infrastructure requires sophisticated security orchestration to ensure efficient identity verification processes that do not compromise performance.

6- In NPN-I-PN - Fully Hosted by Public Network Operator with cloud-native deployment scenario, all network functions are managed by a public network operator. Blockchain-based SSI offers decentralized yet secure identity management. This ensures that only authenticated devices can interact with critical infrastructures such as smart city systems. The public network operator can offer comprehensive security services, while the blockchain SSI adds an additional layer of decentralized, tamper-proof security. Even if the operator's infrastructure is compromised, blockchain SSI ensures that identity management remains secure. However, the security of the entire infrastructure is highly dependent on the trustworthiness of the public network operator, so it is essential to establish strong security agreements and oversight. Hosting all network functions in the cloud also increases the attack surface, especially if the cloud provider's security is compromised. Furthermore, in a multi-tenant environment, despite logical isolation, there is still a risk of contamination between the individual slices. Although blockchain SSI mitigates identity-related risks, it cannot completely prevent problems that can arise from a shared infrastructure.

V. Conclusion

The integration of blockchain-based SSI with 6G non-public networks presents a promising approach to enhance security and data privacy within industrial cyber-physical systems. By leveraging the decentralized nature of blockchain, this approach addresses key challenges in identity management and offers a robust solution for secure communication in industrial environments. Future research should focus on addressing the challenges of scalability, latency, and regulatory compliance to fully realize the potential of this technology. We have considered six deployment options to show that integrating blockchain-based SSI into 6G NPNs can significantly improve security, especially in environments that require strict access control, data integrity and privacy. Each deployment scenario shows how blockchain SSI can be used at different levels of network integration, providing flexible, secure and scalable solutions for various industrial and public applications.

A. Acknowledgment

This work was partially funded by Grant PID2021-126431OB-I00 funded by MCIN/AEI/ 10.13039/501100011033 and by "ERDF A way of making Europe", Generalitat de Catalunya grant 2021 SGR 00770 and Spanish MINECO - Program UNICO I+D (grants TSI-063000-2021-54 and -55)

References

[1] L. Stockburger, G. Kokosioulis, A. Mukkamala, R. R. Mukkamala, and M. Avital, "Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation," *Blockchain: Research and Applications*, vol. 2, no. 2, p. 100014, 2021.

[2] P. C. Bartolomeu, E. Vieira, S. M. Hosseini, and J. Ferreira, "Self-sovereign identity: Use-cases, technologies, and challenges for industrial iot," in *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 2019, pp. 1173–1180.

[3] E. Zeydan, J. Baranda, J. Mangues-Bafalluy, S. S. Arslan, and Y. Turk, "A trustworthy framework for multi-cloud service management: Self-sovereign identity integration," *IEEE Transactions on Network Science and Engineering*, 2024.

[4] E. Zeydan, J. Mangues-Bafalluy, S. Arslan, and Y. Turk, "Blockchain-based self-sovereign identity solution for aerial base station integrated networks," *Vehicular Communications*, vol. 47, p. 100759, 2024.

[5] S. K. Rao and R. Prasad, "Impact of 5g technologies on industry 4.0," *Wireless personal communications*, vol. 100, pp. 145–159, 2018.

[6] J. Yuan, F. Zhang, L. Yu, H. Zhang, and Y. Sang, "Research of security of 5g-enabled industrial internet and its application," in *2021 IEEE Conference on Telecommunications, Optics and Computer Science (TOCS)*. IEEE, 2021, pp. 428–435.

[7] E. Zeydan, L. Blanco, J. Mangues-Bafalluy, A. Aydeger, S. Arslan, and Y. Turk, "Integrating quantum-secured blockchain identity management in open ran for 6g networks," in *2024 IEEE 49th Conference on Local Computer Networks (LCN)*. IEEE, 2024, pp. 1–7.

[8] B. Goswami and H. Choudhury, "A blockchain-based authentication scheme for 5g-enabled iot," *Journal of Network and Systems management*, vol. 30, no. 4, p. 61, 2022.

[9] Z. Zhou, X. Chen, Y. Zhang, and S. Mumtaz, "Blockchain-empowered secure spectrum sharing for 5g heterogeneous networks," *IEEE Network*, vol. 34, no. 1, pp. 24–31, 2020.

[10] U. Ghosh, D. Das, S. Banerjee, and S. Mohanty, "Blockchain-based device identity management and authentication in cyber-physical systems," in *2024 IEEE 21st Consumer Communications & Networking Conference (CCNC)*. IEEE, 2024, pp. 1–6.

[11] R. Muzaffar, M. Ahmed, E. Sisinni, T. Sauter, and H.-P. Bernhard, "5g deployment models and configuration choices for industrial cyber-physical systems–a state of art overview," *IEEE Transactions on Industrial Cyber-Physical Systems*, 2023.

[12] A. Jahid, M. H. Alsharif, and T. J. Hall, "The convergence of blockchain, iot and 6g: potential, opportunities, challenges and research roadmap," *Journal of Network and Computer Applications*, vol. 217, p. 103677, 2023.

[13] R. Sekaran, R. Patan, A. Raveendran, F. Al-Turjman, M. Ramachandran, and L. Mostarda, "Survival study on blockchain based 6g-enabled mobile edge computation for iot automation," *IEEE access*, vol. 8, pp. 143 453–143 463, 2020.

[14] E. Zeydan, L. Blanco, J. Mangues-Bafalluy, A. Aydeger, S. S. Arslan, Y. Turk, J. Bas, and S. K. Mishra, "Enhanced security with quantum key distribution and blockchain for digital identities," in *2024 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*. IEEE, 2024, pp. 489–494.