ADVANCES IN CYBER-PHYSICAL SYSTEMS

Vol. 8 No. 2, 2023

A BLOCKCHAIN-ENHANCED SELF-SOVEREIGN IDENTITY PLATFORM FOR CORPORATE RESOURCE SECURITY

Busra Ozdenizci Kose[1], Vedat Coskun[2], Arslan Coskun[3], and Senol Yaya[4]

[1]*Gebze Technical University, Kocaeli, Turkey.*
[2] *Istanbul Atlas University, Istanbul, Turkey.*
[3,4] *Turcom Technology, Istanbul, Turkey.*
Authors' e-mail: [1]*busraozdenizci@gtu.edu.tr,* [2]*vedat.coskun@atlas.edu.tr,*
[3]*carslan@turcom.com.tr,* [4]*yayas@turcom.com.tr*

https://doi.org/10.23939/acps2023.02.111

Submitted on 30.09.2023

***Abstract*: In an era dominated by concerns of data breaches, and identity theft, security of corporate resources and assets has become paramount. Centralized identity management systems traditionally present vulnerabilities that can fundamentally threaten corporate security. This paper introduces a novel platform to identity management in organizations, leveraging the principles of Self-Sovereign Identity (SSI) and the technological robustness of blockchain. By giving individuals unwavering control over their digital identities and reducing dependence on centralized intermediaries, SSI provides a transformative advancement in security and privacy. When combined with blockchain's immutable, decentralized, and transparent nature, this model ensures a verifiable, tamper-proof, and holistic identity management system. Beyond individual identity management, this paradigm provides corporations with a robust mechanism to protect their assets, both digital and physical. We explore the architectural design and benefits of implementing the proposed system, BlockSSI-CRS, emphasizing its transformative potential for corporate resource protection. Through rigorous analysis, this paper highlights the feasibility of a blockchain-enhanced SSI platform in the context of corporate security needs.**

***Index Terms*: Self sovereign identity, blockchain, identity, authentication, corporate security.**

I. INTRODUCTION

In the digital age, the management and verification of identities have evolved from paper documents to electronic IDs, and now, toward decentralized digital models. In the face of growing concerns about privacy, security, and autonomy in identity management, the concept of Self-Sovereign Identity (SSI) emerges as a revolutionary paradigm shift [1-4]. SSI is a digital identity concept in which an individual or organization has sole ownership over their personal data, without the need for a centralized third party or intermediary [1, 2, 5]. The owner controls their identity and can share it with others without going through a central authority. Instead of having identities granted, verified, and stored by third-party entities, SSI empowers users to control their own identity data, granting them the ability to choose when, how, and to whom their personal information is shared.

The shift towards SSI can significantly alter the digital identity landscape [2-4]. One of the most compelling advantages is the enhanced privacy it offers users. Rather than disclosing an entire set of personal data for verification, users have the discretion to disclose only the relevant data necessary for a particular transaction. Moreover, by reducing the reliance on intermediaries, the risks linked to centralized authorities are mitigated. Fundamentally, SSI prioritizes the user, ensuring that decisions concerning one's identity originate from the individual and not external forces.

SSI typically utilizes distributed ledger technology (DLT) to provide decentralized verification, ensuring that identity records are immutable and tamper-proof [3, 4, 6]. The rise of distributed ledger technology, particularly blockchain, has provided a robust foundation for this new identity framework. With its decentralized nature, immutability, and transparency, blockchain enables the creation of verifiable and tamper-proof identity records. In this decentralized landscape, users are equipped with digital wallets containing cryptographic keys that allow them to prove their identity across multiple platforms, domains, and services.

Combining SSI with blockchain technology yields several notable benefits [1-4]. Firstly, decentralization emerges as a key advantage, freeing SSI from the potential risks of centralized systems. This leads directly to enhanced security, given blockchain's nature which prevents alterations to recorded identity data without a wide consensus, thereby offering a strong defense against identity fraud. This system also brings about a heightened level of transparency, with every action or data input on the blockchain being open to review, which in turn builds user trust [5, 6, 9]. A critical benefit of this integration is the amount of control it offers to individuals. They can manage access to their identity details, presenting proofs without having to expose the full data, a feature made possible by advanced encryption methods. Finally, the combination ensures interoperability, enabling varied entities or platforms to acknowledge and work with a uniform identity, streamlining interactions across diverse platforms.

In real-world applications, the integration of SSI with blockchain has been transformative. Digital passports have emerged, offering a tamper-proof and universally verifiable identity for border crossings. Access control mechanisms have evolved beyond passwords, providing users secure and verifiable access to digital services. The healthcare sector sees patients taking charge of their health records, deciding who can access them. Meanwhile, the financial industry benefits from streamlined Know Your Customer (KYC) procedures, with users in the driver's seat of their own financial identity data. At this point, Quality of Service (QoS) is a crucial challenge, especially with the proliferation of real-time applications [12, 13]. Evaluating the QoS for SSI platforms, especially those integrated with blockchain, requires a comprehensive approach. Key metrics include latency, which gauges the system's responsiveness; throughput, denoting the platform's capability to manage numerous operations concurrently; and availability, emphasizing consistent uptime [13, 14]. Moreover, the platform's reliability in consistently executing identity verifications, scalability to accommodate growing user demands, robust security, and privacy measures, and interoperability with diverse systems are important issues.

A. RESEARCH PROBLEM AND PURPOSE

In an era marked by rapid technological advancement and increasing cyber threats, the protection of digital assets has risen to be a top priority for companies and businesses globally. Digital identity, positioned at the crossroads of individual privacy and organizational security, represents a domain primed for groundbreaking advancements. The continual evolution of digital landscapes and the emergence of sophisticated cyber threats have propelled the need for innovative solutions to secure digital identities. In recent years, there are a number of difficulties and challenges faced by companies in terms of security and privacy. Some of these can be summarized as follows:

(a) *Complex Systems Architecture:* Modern systems often consist of intertwined infrastructures, including centralized servers, distributed systems, and cloud platforms. This complexity can make system management, monitoring, and securing more challenging.

(b) *VPN Access and Admin Rights:* Users with VPN access and admin rights can potentially access all systems, posing a considerable security risk. Such broad access can expose the system to internal threats, accidental mishaps, or even external breaches if an admin's credentials are compromised.

(c) *Diverse Support Personnel:* Different departments might have their own set of support personnel, each requiring distinct authentication methods. This fragmentation can lead to inefficiencies, inconsistencies, and potential security gaps.

(d) *Access Security in Multi-user Systems:* As personnel come and go or change roles within an organization, managing their access rights becomes intricate. It's vital to ensure that former employees or those who change departments don't retain unnecessary access, posing potential security risks.

(e) *Managing External Support Access:* Organizations often rely on third-party vendors or external support personnel for specific tasks. Managing their access and ensuring it's revoked once their task is completed is crucial to prevent lingering access points that could be exploited later.

In addition to these, other problems faced include security issues arising from the inadequacy of 1FA (One-Factor Authentication) / 2FA (Two-Factor Authentication); the complexity of managing user accounts that need to access multiple subsystems; management of accounts of users who leave the company or change positions; the independent log generation by different subsystems; handling the access procedures of external support teams with restricted permissions and time limits; the necessity for system administrator approval in suspicious scenarios; requests for secure remote access to the company's IT resources (only those granted permission); the need to identify and take precautions against malicious users; and the difficulties encountered in managing dormant or unused accounts. Addressing these challenges requires a comprehensive identity and access management solution, routine security audits, and the adoption of best practices for system and user management.

In light of the aforementioned challenges, this study proposes an innovative platform, BlockSSI-CRS that integrates the principles of SSI with the transparency of blockchain technology, specifically designed to enhance corporate asset and resource security. At the intersection of individual digital identity management and corporate security, the platform offers solutions tailored to both individuals and businesses. Employees, the primary users of corporate resources, are empowered with unparalleled control, security, and ownership over their personal data. When this individual sovereignty aligns with the platform's sophisticated access control structures, it creates a dynamic environment where entry to corporate assets becomes seamless for those who are authorized, while simultaneously establishing barriers against any unauthorized intrusions. In an age when online threats are a significant concern and protecting data is crucial, the BlockSSI-CRS platform offers a valuable solution for the safety and independence of employees, and also strengthens the security of corporate resources and assets.

The rest of this paper is organized as follows: Section II presents the system design and architecture studies, and Section III explains how the system works and development requirements. Finally, the study is concluded in Section IV.

II. SYSTEM DESIGN AND ARCHITECTURE

Many SSI solutions leverage decentralized technologies, especially blockchain, to ensure data integrity, security, and privacy. Blockchain provides a decentral-

ized ledger that can record, authenticate, and verify identity claims without a central authority, reducing the risk of data breaches and unauthorized access.

When compared with the existing studies in literature [7-11], the proposed novel BlockSSI-CRS platform distinguishes itself by empowering employee independence while ensuring data protection, addressing modern digital threats more effectively. By harnessing the power of blockchain, the platform guarantees a more transparent and traceable identity verification process, and integrates with corporate systems. The proposed platform aims to not only empower employees with greater control over their own data but also streamline the authentication procedures, making them quicker and more efficient.

B. SSI ARCHITECTURE

As mentioned, SSI is a decentralized approach to digital identity, where individuals have control over their personal data without relying on a centralized authority. As highlighted in Figure 1, a SSI platform has following components [1-6]:

(*) Decentralized Identifiers (DIDs): At the core of SSI are DIDs, which are unique identifiers that an individual creates for themselves. Unlike traditional usernames assigned by a service, a DID is generated and controlled by the user.

(*) Public/Private Key Pair: When a DID is created, a corresponding public/private key pair is also generated. The public key is stored on a distributed ledger, while the private key remains with the user, ensuring control and security.

(*) Verifiable Credentials: When an individual wants to prove something about themselves (e.g., age, nationality), they use verifiable credentials. An issuing party (like a university or government agency) provides a digital credential to the individual, which they can share without revealing the actual data.

(*) DID Document: This is a piece of data associated with a DID that contains details like public keys, service endpoints, and other information. It's stored on a blockchain or another distributed ledger and can be accessed to verify the owner of a DID.

(*) Wallets: Users store their DIDs and verifiable credentials in digital wallets. These can be apps or software, and they manage the user's private keys, allowing them to securely share or prove their identity.

(*) Proofs and Verification: When a website or service needs to verify a user's identity, the user provides a proof by signing a challenge or request with their private key. The service can then verify this using the public key from the DID Document stored on the blockchain. Since SSI is based on open standards, different systems can communicate and recognize each other's identities. This means users can use their identity across various services without creating new profiles or relying on a single centralized identity provider.

C. SYSTEM CONTEXT

The context of the proposed BlockSSI-CRS system is illustrated in Figure 2. In the BlockSSI-CRS system, five entities are highlighted: individual users, corporate resources, blockchain network, authentication services and IT administrators. Users typically employees, are the primary interactors who manage and verify their digital identities to access corporate resources based on their SSI credentials. Their interaction is governed by the trust established through the SSI and validated using the blockchain. As shown in context diagram, employees request access to assets by providing their SSI credentials.

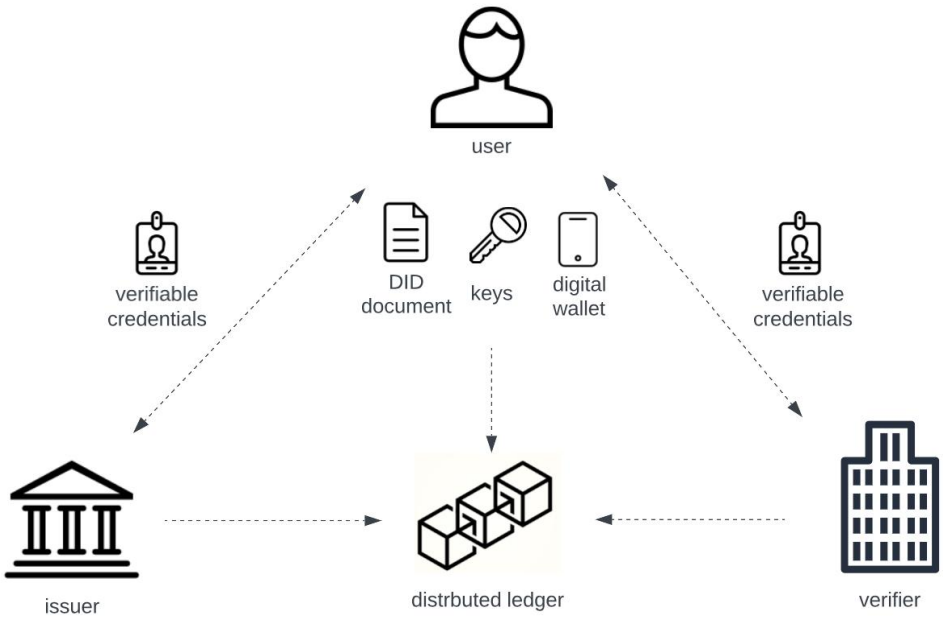


Fig. 1. SSI requirements and structure

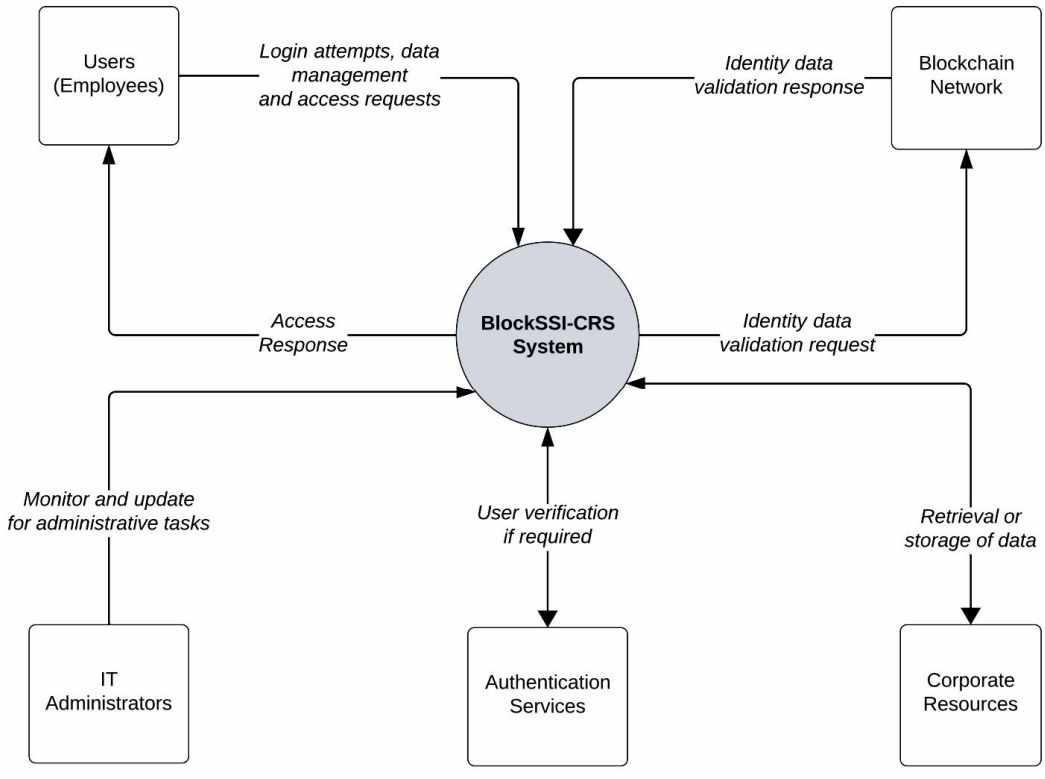


Fig. 2. Proposed system context

After validating the SSI credentials on the blockchain, the system grants or denies access. Corporate resources represent the secured databases or resources that users engage with. The blockchain network acts as the backbone, ensuring each identity transaction's integrity, security, and decentralization. Blockchain network nodes are crucial for validating and confirming transactions or access events that are recorded on the blockchain. These represent the process of validating transactions or access events on the blockchain. Authentication services, which can encompass traditional methods like 1FA, 2FA or MFA (Multi-Factor Authentication) as newer identity verification means, provide an additional layer of verification. Lastly, IT administrators oversee the system, ensuring smooth operations, granting or revoking permissions, and addressing any anomalies or special cases.

D. SYSTEM ARCHITECTURE

The proposed BlockSSI-CRS system is comprised of multiple layers and components to enhance identity management and resource access. The essential components of the proposed architecture (Figure 3) are described hereunder:

At the forefront of the system is the user interface layer, which includes both the BlockSSI-CRS app (as the digital wallet for users) and the Admin Control Panel. Through the BlockSSI-CRS app, users can view and manage various aspects of their digital identity, from DIDs and verifiable credentials to transaction histories, allowing them to assert their identity and access corporate resources from any location. The admin control panel provides IT administrators enabling them to oversee system functionalities, adjust permissions, and address potential security issues.

The application layer contains the identity management and access control modules. Identity management module is essential for users to manage their DIDs and related credentials, all centralized within the BlockSSI-CRS app. Meanwhile, the access control module operates and implements access policies and rules based on SSI credentials.

The blockchain layer, as a decentralized ledger securely stores user DIDs, DID documents, and public keys. It also deploys smart contracts which activate automatic actions based on set criteria, like granting access after identity verification.

The infrastructure layer includes the necessary hardware and software components for robustness and scalability. In this layer, BlockSSI-CRS server orchestrates the overall operation of the system, manages data flows, and interacts with the blockchain network. Within this layer, the blockchain network also operates, storing DIDs and validating identity transactions. Integrated storage solutions accommodate the vast data associated with verifiable credentials, transaction histories, and access logs. Additionally, this layer includes security protocols and firewalls, defending against cyber threats and unauthorized intrusions. Moreover, connections to external authentication services can be realized in order to offer 1FA, 2FA or MFA for heightened security scenarios. In situations where additional security layers are

needed, integration with OTP (one-time password) services via OTA (over-the air) [15, 16] or biometric controls can be added. The infrastructure layer, in essence, provides the backbone, supporting and enhancing all functionalities of the BlockSSI-CRS system.

This design offers a comprehensive strategy, guaranteeing that the BlockSSI-CRS system operates efficiently and stands strong against possible challenges. At the same time, it emphasizes user control and the safeguarding of corporate resources.

III. HOW SYSTEM WORKS

As an example, the employee wants to access to the company's database server from any location. A step-by-step process is described hereunder which details how an employee might interact with the BlockSSI-CRS system:

(1) Instead of a typical username and password prompt, the employee launches the BlockSSI-CRS app (user dashboard) on their device, which acts as their digital wallet. This app securely stores their SSI credentials, including their DID and associated private key.

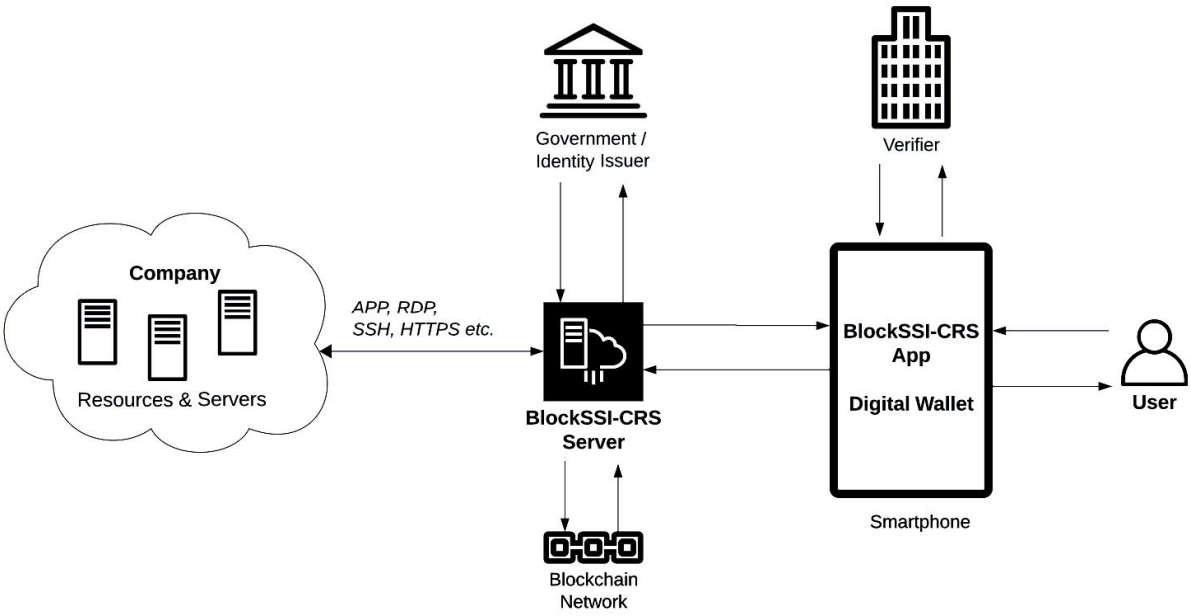


Fig. 3. Proposed system components

(2) Within the app, the employee initiates an authentication request to access the company's database server. The BlockSSI-CRS app uses the employee's DID and signs the request with their private key.

(3) The signed request is sent to the BlockSSI-CRS server for validation. The server checks the blockchain network to retrieve the public key associated with the employee's DID. It then uses this to validate the authenticity of the request.

(4) After the SSI credentials are verified, the BlockSSI-CRS server's access control module evaluates if the employee has the required permissions to access the company database server.

(5) The BlockSSI-CRS server leverages the blockchain network to validate the integrity and status of the employee's SSI credentials, ensuring they remain untampered with and are not revoked.

(6) If the credentials are verified and the access control policies allow it, the system grants the employee access to the company's database server. If any discrepancies arise or if the employee lacks the necessary permissions, access is denied.

(7) Once access is granted, the system establishes a secure, encrypted connection between the employee's device and the company's database server. This ensures that the employee can interact with the database or other resources securely, even if they're accessing it from a remote location. The employee is empowered to execute tasks, query data, or undertake any other authorized actions, all without the necessity of establishing a VPN connection.

(8) All actions undertaken by the employee during this session are recorded to the blockchain network, ensuring an immutable and tamper-evident audit trail. This blockchain-backed logging mechanism heightens security, offering a transparent record of all interactions. Once the employee has finished their tasks, they can securely end the session via their BlockSSI-CRS app.

E. DEVELOPMENT STUDIES

For the server-side, we'll consider blockchain platforms Ethereum for its well-documented smart contract capabilities or Hyperledger Fabric for private and enterprise-focused solutions. In case of smart contract development, Solidity (for Ethereum) or Chaincode (for Hyperledger) will be used to design, write, and test smart contracts. Backend development may leverage frameworks like Node.js or Django for API development and integration with frontend systems. Databases like Post-

greSQL or MongoDB will be considered to store off-chain data, user profiles, and other non-transactional information.

In case of SSI integration tools, for effective implementation and management of DIDs we'll explore tools like the Universal Resolver provided by the Decentralized Identity Foundation (DIF). Additionally, to streamline the creation and management of self-sovereign identities, established frameworks such as Sovrin and uPort will be evaluated. To ensure the BlockSSI-CRS app is robust and functional, we'll consider integrating Wallet SDKs, like those offered by Trinsic. These SDKs are crucial as they support the creation, management, and verification of digital identities and their associated credentials.

On the frontend development side, we'll be considering popular web frameworks such as React and Angular. Scalability is also crucial for the success of the BlockSSI-CRS system. To achieve this, we're looking into cloud service providers such as AWS or Google Cloud. Additionally, the nature of our blockchain choice, be it private or consortium, will dictate the need for infrastructure components dedicated to running and managing blockchain nodes.

Upon thorough examination of the aforementioned tools and solutions, decisions will be made to adopt the most suitable ones that best align with the system's goals and objectives.

IV. CONCLUSION

In the evolving digital landscape, SSI paradigm emerges as a pioneering solution, particularly for enhancing secure authentication and identity management. Accordingly, this study introduced a novel platform, BlockSSI-CRS that merged the capabilities of blockchain technology and SSI architectures for securing the corporate assets and resources. BlockSSI-CRS distinguished itself by offering a decentralized approach that empowered employee independence while ensuring identity management and secure resource access.

Upon concluding the development phase of the BlockSSI-CRS system, rigorous evaluations were initiated. Initially, tests aligned with the BlockSSI-CRS system standards and protocols were executed on the underlying blockchain infrastructure, aiming for a 100% success. Subsequently, an in-house pilot test was set to be launched within the company, leveraging an assortment of diverse endpoint devices, servers, desktops, and mobile platforms. Importantly, the blockchain network's response time to the SSI requests was projected to be consistently under 1 second. Our goal was to realize these pilot evaluations with an 100% success rate, thereby confirming the system's resilience, efficacy, and readiness for broader deployment.

With the BlockSSI-CRS framework, there was reduced dependency on traditional authentication mechanisms like 1FA and 2FA, which highlighted the robustness and efficiency of the system. The utilization of blockchain technology also allowed for enhanced security, offering transparent and immutable log management that ensures every transaction and interaction's traceability and integrity. Moreover, the system showcased its adaptability by enabling location-independent access to company assets, eliminating the traditional reliance on VPNs. Consequently, the proposed system stands out as a model for secure user identity management and authentication, offering a seamless user convenience and robust corporate resources protection.

To fully evaluate the feasibility of a blockchain enhanced SSI platform in a particular domain, some of the limitations must be carefully considered as well [2, 5, 6, 9]. These limitations include scalability challenges as the blockchain network might struggle to maintain efficiency under heavy load, integration complexities with existing corporate systems which could result in resource-intensive deployments, and the challenges of compliance with global data protection laws. The implementation and operating cost of a blockchain based SSI could be significant, which may not be justifiable for all organizations.

REFERENCES

[1] Schardong, F., & Custódio, R. (2022). Self-sovereign identity: a systematic review, mapping and taxonomy. *Sensors*, *22*(15), 5641. DOI: 10.3390/s22155641

[2] Ahmed, M. R., Islam, A. M., Shatabda, S., & Islam, S. (2022). Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey. *IEEE Access,* 10, 113436-113481. DOI: 10.1109/ACCESS.2022.3216643

[3] Nokhbeh Zaeem, R., Chang, K. C., Huang, T. C., Liau, D., Song, W., Tyagi, A., ... & Barber, K. S. (2021, December). Blockchain-based self-sovereign identity: Survey, requirements, use-cases, and comparative study. In IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (pp. 128-135). DOI: 10.1145/3486622.3493917

[4] Eddine, B. N., Ouaddah, A., & Mezrioui, A. (2021, September). Exploring blockchain-based Self Sovereign Identity Systems: challenges and comparative analysis. In 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS) (pp. 21-22). IEEE. DOI: 10.1109/BRAINS52497.2021.9569821

[5] Čučko, Š., Keršič, V., & Turkanović, M. (2023). Towards a Catalogue of Self-Sovereign Identity Design Patterns. Applied Sciences, 13(9), 5395. DOI: 10.3390/app13095395

[6] Liu, Y., Lu, Q., Paik, H. Y., Xu, X., Chen, S., & Zhu, L. (2020). Design pattern as a service for blockchain-based self-sovereign identity. IEEE Software, 37(5), 30-36. DOI: 10.1109/MS.2020.2992783

[7] Ahmed, K. A., Saraya, S. F., Wanis, J. F., & Ali-Eldin, A. M. (2023). A Blockchain Self-Sovereign Identity for Open Banking Secured by the Customer's Banking Cards. Future Internet, 15(6), 208. DOI: 10.3390/fi15060208

[8] Bai, P., Kumar, S., Aggarwal, G., Mahmud, M., Kaiwartya, O., & Lloret, J. (2022). Self-sovereignty identity management model for smart healthcare system. Sensors, 22(13), 4714. DOI: 10.3390/s22134714

[9] Bandara, E., Liang, X., Foytik, P., Shetty, S., & De Zoysa, K. (2021, July). A blockchain and self-sovereign identity em-

powered digital identity platform. In 2021 International Conference on Computer Communications and Networks (ICCCN) (pp. 1-7). IEEE. DOI: 10.1109/ICCCN52240.2021.9522184

[10] Stockburger, L., Kokosioulis, G., Mukkamala, A., Mukkamala, R. R., & Avital, M. (2021). Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation. Blockchain: Research and Applications, 2(2), 100014. DOI: 10.1016/j.bcra.2021.100014

[11] Shuaib, M., Hassan, N. H., Usman, S., Alam, S., Bhatia, S., Mashat, A., ... & Kumar, M. (2022). Self-sovereign identity solution for blockchain-based land registry system: a comparison. Mobile Information Systems, 2022, 1-17. DOI: 10.1155/2022/8930472

[12] Mantar, H. A., Hwang, J., Okumus, I. T., & Chapin, S. J. (2001). Interdomain Resource Reservation via Third-Party Agent. Accessed: https://surface.syr.edu/eecs/58

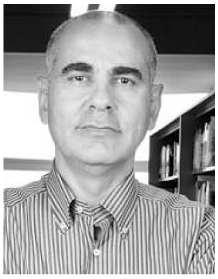
[13] Hwang, J., Chapin, S., Mantar, H., & Okumus, I. (2004, April). An implementation study of a dynamic inter-domain bandwidth management platform in DiffServ networks. In 2004 IEEE/IFIP Network Operations and Management Symposium (IEEE Cat. No. 04CH37507) (Vol. 1, pp. 321-334). IEEE. DOI: 10.1109/NOMS.2004.1317670

[14] Tuysuz, M. F., & Mantar, H. A. (2013, September). A novel energy-efficient QoS-aware handover scheme over IEEE 802.11 WLANs. In 2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC) (pp. 1045-1049). IEEE. DOI: 10.1109/PIMRC.2013.6666292

[15] Ok, K., Coskun, V., Yarman, S. B., Cevikbas, C., & Ozdenizci, B. (2016). SIMSec: A key exchange protocol between SIM card and service provider. Wireless Personal Communications, 89, 1371-1390. DOI: https://doi.org/10.1007/s11277-016-3326-5

[16] Ozdenizci, B., Ok, K., & Coskun, V. (2016). A tokenization-based communication architecture for HCE-enabled NFC services. Mobile Information Systems, 2016. DOI: https://doi.org/10.1155/2016/5046284

Assoc. Prof. Dr. Busra Ozdenizci Kose received Ph.D. degree at Informatics Department in Istanbul University. She co-authored the books titled ''Near Field Communication: From Theory to Practice'' published by John Wiley & Sons, Inc., 2012 and ''Professional NFC Application Development for Android'' published by Wrox, 2013. Her research areas include Information System Analysis and Development, Near Field Communication, Smart Cards, Mobile Communication Technologies and Blockchain.



Prof. Dr. Vedat Coskun is a Computer Scientist, Academician, Researcher, and Wiley Author. He is a founder and manager of NFC Lab@Istanbul (www.NFCLab.org), the pioneer research lab on NFC technology worldwide. He is currently Professor of Software Engineering in Istanbul Atlas University. He gives lectures in several universities all around the World. He believes in the importance of academia & industry relationship in Information Technology, and takes roles of project development, researcher, and consultant for national and international companies in this manner.

Eng. Arslan Coskun graduated from Istanbul Technical University and is a Chief Technology Officer with a distinct history of working within the industry of information technology and services, skilled in Networking, Projectand Team Management. He has been working for Turcom Technology since the day it was founded (1993). He holds Network and Management certificates including Cisco Certified Internetwork Expert (CCIE), Cisco CCNP R&S, Cisco CCNP Security, Checkpoint CCSE, Checkpoint CCSA, HP ASE Networking, Juniper JNSA, ISO 27001 ISMS, ISO 14001 EMS, Microsoft MCITP etc.

Eng. Senol Yaya is an Engineer, and is currently a post graduate student in Computer Engineering, Istanbul. He has been working in Turcom Technology for more than a decade, and currently works as the R&D Manager. He focused on various technologies such as Internet of Things, Linux systems, Machine Learning, and Agile Software Development. He has experience in software development methodologies.