International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 21 No. 3 (1) 2025

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, No. 3(1), 2025

Research Paper

A PRIVACY PRESERVING AND ACCOUNTABLE SELF-SOVEREIGN IDENTITY PROTOCOL

Sumaiya Nazneen[1], Sara Fatima[2]

[1]PG Scholar, Department of CSE, Shadan Women's College of Engineering and Technology, Hyderabad, sumaiyanazneen708@gmail.com

[2] Assistant Professor, Department of CSE, Shadan Women's College of Engineering and Technology, ssarafatima17@gmail.com

ABSTRACT:

Self-Sovereign Identity (SSI) has emerged as a result of the opposition and concern regarding the centralized control of user identities by third-party authorities. Although SSI successfully restores users' control over their own identities with the aid of blockchain, its viability has been called into question by privacy concerns arising from blockchain transparency as well as the lack of accountability measures like Know Your Customer (KYC) and Anti-Money Laundering (AML). In order to close this gap, we present AASSI, a groundbreaking SSI protocol that has been painstakingly created to strike a balance between the two requirements of accountability and privacy. In particular, AASSI offers support for selective revocation, self-derivation, fine-grained tracing, and anonymity. In order to improve privacy protection and self-management capabilities, AASSI presents redactable signatures, which enable users to independently generate unique credentials for every user service-provider contact. Regarding fine-grained tracing, the protocol uses a dual-tag approach that makes it easier to track down users' true identities and detailed history records of credentials that have been derived. AASSI uses dynamic accumulators as a building component for selective revocation, which allows problematic users to be revoked. Finally, we present a functional comparison that demonstrates the robustness of AASSI's features, namely its support for unique self-derived attributes that further enhance user control over their identification and fine-grained tracking that gives tracers greater freedom. Through an off-chain time-consuming comparison, we illustrate the protocol's efficiency and show that AASSI significantly lowers the credential verification time overhead. Additionally, we demonstrate the viability of AASSI experimentally and test the on-chain communication overhead.

KEYWORDS: Self-sovereign identity, blockchain, anonymity, accountability, revocation

Received: 06-08-2025 Accepted: 08-09-2025 Published: 15-09-2025

1. INTRODUCTION

Digital IDs [1] are identifiers that display a person's true identity as the only information available online. The majority of digital identities are still authenticated & managed by a central authority that is connected to a service provider. To create an account, a user must submit sensitive personal data that satisfies the service provider's access controls, after which the service provider grants the user restricted access rights. According to this concept, users' digital identities are kept on servers run by the central authority. By assaulting the servers, attackers can get malicious access to users' private information, putting users at danger of data misuse & privacy breaches. Data leaks still happen even if regulatory bodies have put laws & rules in place to safeguard individual privacy, such as the California Consumer Privacy Act (CCPA) & the General Data Protection Regulation (GDPR) [2], [3]. The user-centric approach & the federated identity management (FIM) paradigm were established in succession to combat the centralized control of user identification. The former suggests using trust connections in place of a central authority to select a service provider & determine whether to authorize the sharing of their identify with another service provider. Regretfully, the crucial problems of privacy leakage & identity control are still ignored. A user controlled decentralized digital identification concept called SSI was projected, drawing stimulus from BC networks & cryptography technology [5]. Verifiable credentials (VCs) [7] & decentralized identifiers (DIDs) [6] are the building blocks used by SSI to deliver users whole regulator completed their identity information & the ability to independently generate digital identities. Users have the ability to administer many VCs under their names & self-create DIDs. Users can use their VCs as needed in online conversations by managing the private keys linked to DIDs. In a traditional SSI scenario, the issuer signs the user-selected personal information to create a digital identity, or VC. Depending on the access restriction of various service providers, the user can choose a compatible digital identity for communication when they gain access to a service provider. In the end, the service provider can confirm the user's identity by gaining access to the user's DID & the VC-related data kept in the BC. While the verifiable credential data format allows users to utilize their registered identities indefinitely, BC's distributed & tamper-proof architecture guarantees the integrity & decentralization of users' digital identities [8]. Existing SSI protocols have three main issues, notwithstanding their benefits in terms of

control & persistence. (1) Privacy: Although users must divulge certain personal information on the BC as part of the verification process, the BC's transparency makes user data readily available to BC participants, raising the possibility of user privacy being compromised. (2) Over-reliance: Despite SSI's implementation of user identity self-control, users must frequently communicate with issuers to gain credentials on various attributes. This makes the issuer's job more complex & the user more dependent on them. (3) Accountability: Despite the necessity for total privacy, laws like KYC & AML stipulate that certain economic organizations should have the authority to ascertain the private information & real identity of individuals participating in any transaction. Thus, a crucial topic is how to strike a compromise between accountability & privacy. This study suggests AASSI, an SSI protocol that can concurrently offer privacy, low reliance, & accountability, as a answer to the aforementioned issues. AASSI presents redactable signatures as building blocks for minimal dependence & privacy. Because the origin process does not need the issuer's involvement, it allows users to derive derived signatures that contain partially properties from a master signature, hence lowering the user's dependence on the issuer. Furthermore, users' anonymity can be significantly protected because the verification of generated signatures only requires knowledge of some properties. When used in conjunction with zero-knowledge proofs, users can establish their acquiescence with admission regulator without disclosing particular characteristics. For instance, the user is older than eighteen. Regarding accountability, the protocol uses a dual-tag approach that makes it easier to track down users' true identities & maintain detailed historical records of credentials that consume remained derived. However, in instruction to facilitate the revocation of violating users, AASSI makes use of dynamic accumulators. The main contributions of the work are summed up as follows: ¬ We suggested AASSI, a novel SSI protocol that can strike a balance between accountability & privacy. In particular, AASSI offers support for selective revocation, fine-grained tracing, anonymity & SD. Users can derive credentials in general mode that just include the necessary qualities & the issuer is not required to be involved in the derivation process. Furthermore, simply by watching the BC & chatting online, no one can discover the genuine identify of a regular user. When a tracer is in accountability mode, it can determine the real identify of the offending user & execute FGT on their past actions. Additionally, the protocol has an optional revocation capability that makes it possible to revoke an unauthorized user. ¬ We codified the AASSI protocol's components, threat model & security model. The accuracy, unforgeability, anonymity & traceability security requirements are shown to be met by the protocol. ¬ We put AASSI into practice & evaluated its effectiveness. We started by calculating its complexity & contrasting AASSI's features & time overhead with those of current SSI protocols. Second, we used both on-chain & off-chain experiments to assess its viability & effectiveness. According to experimental results, AASSI is feasible, offers reliable characteristics & requires little time to verify credentials.

OBJECTIVE

Our goal was to implement AASSI & analyze its effectiveness. We started by calculating its complexity & contrasting AASSI's features & time overhead with those of current SSI protocols. Second, we used both on-chain & off-chain experiments to assess its viability & effectiveness. According to experimental results, AASSI is feasible, offers reliable characteristics & requires little time to verify credentials.

PROBLEM STATAMENT

According to this paper, the majority of digital identities are still verified and managed by a central authority that is connected to a service provider. To create an account, a user must submit sensitive personal data that satisfies the service provider's access controls, after which the service provider grants the user restricted access rights. This paradigm exposes users to the danger of data exploitation and privacy leakage since users' digital identities are kept on the servers of the central authority, and adversaries can deliberately obtain users' sensitive data by simply assaulting the servers.

EXISTING SYSTEM

SSI emerged as a outcome of the opposition & concern regarding the centralized control of user identities by third-party authorities. SSI successfully restores users' control over their own identities with BC's assistance; but, privacy issues brought on by BC's transparency, composed with the lack of accountability such as KYC & AML, have raised doubts about SSI's sustainability. Digital IDs are identifiers that display a person's true identity as the only information available online.

Existing System Disadvantages:

- The situation becomes progressively complex owing to edge computing's versatility.
- There are issues with the present edge computing architecture.
- There are too many task requests on the edge node.

PROPOSED SYSTEM

In order to close this gap, we present AASSI, a ground-breaking SSI protocol that consumes been thoroughly created to strike a balance among the two demands of responsibility & privacy. In particular, AASSI offers support for selective revocation, fine-grained tracing, anonymity & SD. AASSI uses dynamic accumulators as a building block for

selective revocation, which allows problematic users to be revoked. In conclusion, we present a functional comparison that demonstrates the robustness of AASSI, namely its support for innovative self-derived attributes that further improve user regulator over their identification & FGT, which gives tracers greater flexibility. Through an off-chain time-consuming comparison, we illustrate the protocol's efficiency & reveal that AASSI significantly lowers the credential verification time overhead. Additionally, we experimentally demonstrate the viability of AASSI & test the on-chain communication overhead.

Proposed System Advantage

- Both low latency & high bandwidth.
- Increase user happiness significantly.
- Dispersed edge computing nodes

2. RELATED WORK

A thorough analysis of BDSCA was carried out in this study. The use of large information in supply chain management & its advantages for businesses & society were examined in the article. The study also looked at the operational, privacy, security & principled matters with big data tools, as healthy as the possible harm to a company's reputation. Four main aspects were described in the review: big statistics analytics, requests, ethics & privacy concerns, & how businesses used this new technology to plan ahead & even foresee the future. Seven themes & fourteen sub-themes represent the many levels & distinct conceptual stances upon which these fundamental aspects are constructed. These subjects were industrialized using 120 publications from 2005 to 2020, mostly from prestigious scholarly journals. Generally speaking, there is broad agreement in the works today that big data analytics includes much extra than only supply chain innovation. It could help the next generation of multinational corporations, who are functioning in a more difficult & unpredictable environment, be more responsive. **[1]**

In the age of the internet, when many applications enable online communication & service use, privacy is essential. By letting users to verify themselves without skimpy their factual individualities, the PPIdM system helps manage users' identities & safeguards their privacy. Additionally, the PPIdM system enables users to selectively expose certain minor identifying features while keeping others concealed. However, because their true identities remain secret, anonymity also incentivizes malevolent individuals to violate system policies & conduct crimes. In order to confirm users' identity attributes, document all users' true identities & guarantee that the identities of malicious users can be tracked down, existing PPIdM systems use the identity provider (IP) as a medium. Users' identities are so concealed from everyone except the IP. However, since there is no assurance that the IP is always truthful & not interested in the private information & actions of its users, the discretion of the users is at risk. In order to assist user's control their identity attributes & conceal their true identities from all parties, including the IP, this study suggests a PPIdM system on the BC. However, if malicious individuals break the system's rules, the consensus inside the system can identify their true identities. The game-based proof scheme is used to examine & show the security needs of the PPIdM in an informal manner. Combining Shamir's secret sharing (SSS), a kind of ZKP, zk-SNARK & a number of other cryptographic approaches is the primary concept of this paper. **[2]**

Coconut is a threshold-issued, attribute-based credentialing system. We examine its security characteristics. In order to do this, we specify the optimal functionality for threshold-issued attribute-based access control. Our functionality is realized by a construction that we describe. With a few modifications, our construction is based on Coconut. Specifically, it alters the procedures for credential show & blind credential issuance to protect user privacy from adversaries with infinite computing power. Compared to Coconut, the adjusted methods are somewhat more effective. In order to demonstrate unforgeability, our architecture also extends the public key. **[3]**

Due to the involvement of a Third Party Auditor (TPA), the conventional system that was created by integrating the Wireless Sensor Network (WSN) has significant problems, including information centralization, a single source of trust, & an inability to offer a reliable data-auditing solution. By utilizing the Distributed Data Storage Service (DDSS) system & the BC concept, this article offers an innovative way to address the aforementioned problems. Since the BC keeps a permanent record of the sensor nodes' logs, the sensor nodes in our perfect are accountable for their actions. Decentralized authentication of sensor nodes & data saved in the fully distributed system is offered by the suggested method. Additionally, a decentralized data-auditing scheme that does not comprise the TPA is proposed, which ultimately helps the user by saving money & bandwidth. The Scythe simulator tool is used for the formal verification of the suggested protocol, demonstrating its safety & 100% correctness in defending against the pertinent threats. We have calculated the computational efficiencies & time complexity of the suggested scheme & contrasted them with the current one. When compared to the Khalid et al. (2020) approach, the suggested method's computation & communication overhead is decreased by 22.143% & 12.5%, respectively. Finally, our approach is simulated on the Ethereum platform, demonstrating that less than USD 2 is needed to implement the suggested method. **[4]**

By creating an interoperable European identity management framework based on innovative cryptographic techniques applied to already used identity management technologies, the OLYMPUS EU project is tackling the difficulties related to the

usage of PPIdM systems. To prevent any one authority from impersonating or tracking its users, OLYMPUS specifically uses distributed cryptography techniques to divide the function of the online IDP across several authorities. This document outlines the key components, specifications & use cases of the IdM ecosystem being built as part of OLYMPUS. **[5]**
A new, user-centered, decentralized identity method that makes use of decentralized technology is called SSI. In addition to improving security & privacy, it gives entities the ability to manage their identity & data flow during digital interactions by offering a method of digital identification independent of any outside authority. As BC technology advances, SSI is gaining traction in both academia & industry, and the quantity of research articles is rising quickly. SSI is still a relatively new, unorganized discipline that is still in its infancy. In order to structure the research area & give a coarse-grained overview of decentralized & SSI, a systematic mapping methodology was used. This involved identifying, evaluating & categorizing the research papers based on predetermined criteria, such as their contribution, application domain, IT field, research type, research method & publication location. Additionally, the research's nature & scope were established & current research topics, demographics, trends, gaps, obstacles & forecasts for additional education were provided. The findings imply that validation studies & solution suggestions are successful in tackling decentralized identity in a broad sense. Few studies examine usability, user experience, patterns & best practices; instead, papers mostly provide systems/solutions, architectures & frameworks with an emphasis on authentication, security, privacy & trust.**[6]**

3. METHODLOGIES

To lower the possibility of user privacy violations, several academics are dedicated to decentralizing issuer rights. When combined with BC, the threshold credential issuance protocol Coconut makes it possible to employ selective disclosure credentials in situations where there isn't a single trusted party. Multiple issuers must be involved in the credential generation process, & integration of the credentials is only allowed after the user has gathered sufficient incomplete credentials. This allows for confidentiality to be guaranteed, even in cases where some of the issuers are unavailable or malevolent. Nevertheless, credential verification is excessively costly & its computing complexity & communication bandwidth increase linearly with the amount of attributes**.**

MODULE DESCRIPTION:

User Interface Design:

We create the project's windows in this module. All users can securely log in using these windows. Users must enter their name & password in instruction to connect to the server; only then may they do so. The user can log in to the server directly if they have already left; if not, they must register their information, including their username, password & email address. To maintain the upload & download speeds, the server will generate an account for every user. The user ID will be assigned to the name. Usually, logging in allows you to access a certain page.

Issuer:

The first module issuer is this one. With a user ID, password & created port number, the issuer can login. A user request can be sent to the issuer, who must then authorize it.

Identifiers:

This project's third module is this one. Identifiers in this project have a register with all the information & can log in using their user ID & password. A file containing a text or doc file has been uploaded to the data along with the identifiers. Data that may be viewed from a database is shared by the IDs.

User:

This project's fourth module is this one. After registering with all the necessary information, the user logs in using their email address & password. Both a public key & a private key are produced by the user. Following approval of the request, the private & public keys will be removed. The user browses & we can exploration for statistics using the identifier's repository. After the user has verified that the keys are correct, a file download will be decrypted.

Tracer:

The first module issuer is this one. The user ID & password for Tracer are generated at random. With a user ID & password, Tracer can log in. The user may receive keys from Tracer. The user will receive the private keys that the tracer has obtained.

Service Providers:

The service providers were able to log in using the system's original IP address. There are 2 facilities offered by the service providers. The service must confirm the request's identity. The second service has a request to verify an identify. The services are interconnected with one another. The service provider verifies & provides the user with keys. The user is then able to download a file.

4. ALGORITHM

1. AASSI MODEL

Setup, Key Gen, Issue Cred, Derive DCred, Verify Cred, Trace User & Revoke are the seven algorithmthat make up AASSI. Each algorithm's brief definition is displayed as follows:

- Setup(1k , n, m) −→ (params): This algorithm returns the public parameters params on input security parameter k, upper limit for users n & upper limit for attributesm.
- KeyGen: The issuer, user & identifier key pair creation algorithms are all included in this algorithm. – AKeyGen(params) −→ (apk, ask, RL, AT): The issuer is responsible for executing

this algorithm. It returns a list of attribute types AT & an issuer key pair (apk, ask) based on the provided public parameters params.

– UKeyGen(params) −→ (upk, usk, U): The user is responsible for executing this algorithm. It returns a private value U & a user key pair (upk, usk) on input public parameters params.

– TKeyGen(params) −→ (tpk, tsk): The tracer is responsible for executing this algorithm. It produces a tracer key pair (tpk, tsk) based on the provided public parameters parameters.

IssueCred: This method, known as the master credential generation algorithm, is used by both the issuer & the user. It includes the two algorithms listed below:

Request(params, upk, U, {ai}ni =1, tpk) −→ (C, tag, πu): Utilizing the attribute set {ai}ni =1, user public key upk & private value U, the user initiates this process to get the master credential issued by the issuer. It produces a zero knowledge proof (πu), commitment C & tag.

Issue(params, πu, C, β, ask, apk) −→ (σ′, W, β): The issuer starts this algorithm to provide the user with credentials. This method receives the identification value β that has been merged in accumulator 1 along with the received C & πu. It first validates πu &, if successful, produces the blind signature σ′, identification value β & witness W.

- DeriveCred(params, cred, {ai}ni =1, I , φ, β, U, upk, apk, AT , tpk) −→ (credI): The user starts this algorithm to get a derived credential that meets the needs of the service provider. The derived credential credI is produced upon receiving the master credential cred, the attribute set {ai}ni =1, the partial set I ⊂ ⌈1, n⌉, the requirements φ, the identifying value β, the private value U & a collection of attribute types AT, upk, apk & tpk.
- VerifyCred(params, AT , apk, credI) −→ (0/1): The service provider uses this algorithm, which is the derived credential verification algorithm. If the verification is successful, it returns 1; if not, it returns 0. It takes as input a set of attribute types AT, derived credential credI, & apk.
- Trace User(params, tsk, credI) −→ (upk): The tracer initiates this algorithm. It outputs upk based on input tsk & derived credential credI that must be traced. ¬
- Revoke(params, apk, RL, β) −→ (RLnew, 1new): The issuer uses this algorithm to revoke β.

The updated revocation list RLnew & updated accumulator 1new are produced upon input of the revocation list RL, the identification value β that has to be revoked & the apk. The remaining authorized users are able to update their witness on their own.

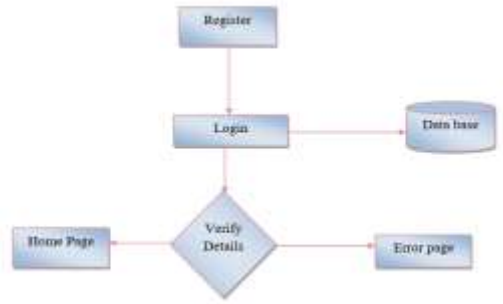
2. AES Algorithm, Hash algorithm & Sorting Algorithm.

Data encryption & decryption are accomplished using the symmetric-key block cipher method known as the Advanced Encryption Standard (AES). AES is extensively utilized in many different applications, such as communication networks, cloud storage & safe online transactions. A hash algorithm is a one-way function that accepts input data of arbitrary length & outputs a message digest or hash value, which is a fixed-length string of characters. Digital signatures, password storage & data integrity are just a few of the uses for hash algorithms. There are several kinds of hash algorithms, such as: SHA-256: A secure hash algorithm that generates a 256-bit hash value is called SHA-256. A sorting algorithm is a process that puts a list of items in a particular order, such numerical or alphabetical. Applications for sorting algorithms include file systems, database administration, & data analysis. 1. Choose the Sorting Algorithm: Depending on the needs, choose a suitable sorting algorithm (e.g., time complexity, space complexity, stability). 2. Initialize Data Structure: Get the data structure (such as an array or list) with the elements that need to be sorted ready. 3. Implement the Algorithm: To carry out the sorting, write the code. This usually entails:

- Element comparison.
- Changing components as needed.
- Preserving the elements' order.

5. DATA FLOW DIAGRAM

LEVEL 0



6. SYSTEM ARCHITECTURE

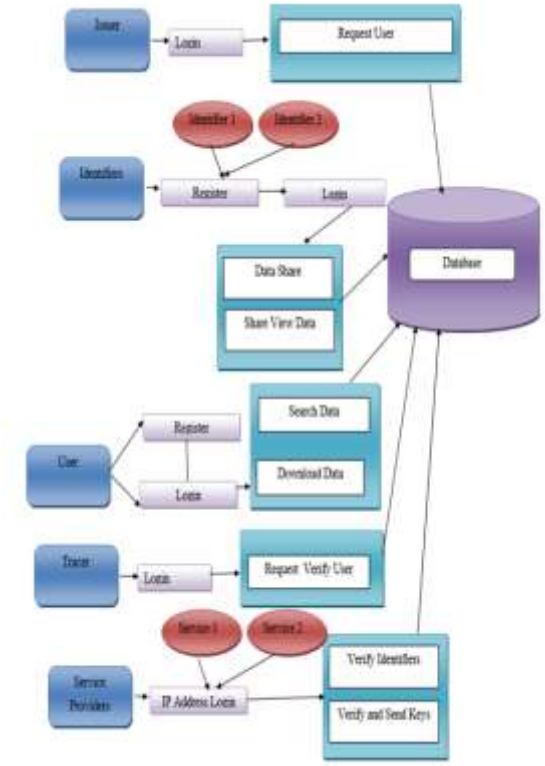


FIG:6 System Architecture

7. RESULT

The implementation of the proposed **Network Security System** has demonstrated its effectiveness in providing a secure and reliable framework for user authentication, identity management, and data sharing. The system allows users to register by submitting essential details such as name, email, age, gender, and password, thereby ensuring that only authenticated users gain access. In addition, the introduction of identifiers adds a secondary layer of security, enabling unique identity mapping and verification through the issuer. The issuer module plays a vital role by validating identifiers and approving requests, which enhances trust and prevents unauthorized access. Furthermore, the tracer login feature ensures proper monitoring of user activities by generating dynamic credentials that can be refreshed as needed, thereby adding traceability to the framework.

The system also incorporates a secure data-sharing module, allowing users to upload files with relevant metadata such as file name and description. Access to shared files is strictly controlled through the assignment of unique file IDs and decryption keys, ensuring that only authorized users can retrieve and view the data. This layered security approach successfully integrates confidentiality, integrity, authentication, and traceability within the system. The overall results confirm that the proposed framework not only mitigates risks associated with unauthorized access and data leakage but also provides a user-friendly platform for secure communication and controlled information exchange in network environments.

8. CONCLUSION

We have introduced a novel SSI protocol in this study that has been painstakingly created to strike a compromise between the two demands of responsibility & privacy. In particular, AASSI offers support for selective revocation, fine-grained tracing, anonymity, & SD. By simply seeing the BC & interacting online, no one can discover the privacy characteristics & actual identity of a general user in the general mode. In accountability mode, the issuer has the power to selectively remove users who have violated the rules & there is a tracer that can track down users' true identities as well as detailed history records of generated credentials. Innovatively, AASSI supports two new features: FGT & SD. The former gives tracers more flexible tracking options, while the latter effectively enhances privacy protection & user control over their identity by allowing the user to independently derive unique credentials for each user-service-provider interaction. We suggest the particular AASSI structure & show that it meets the security criteria of traceability, unforgeability, anonymity, & accuracy. Lastly, we evaluate AASSI's functionality & complexity in comparison to current SSI. Off-chain & on-chain studies are used to assess its computational efficiency & viability, respectively.

9. FUTURE ENHANCEMENT

The suggested protocol's validity, robust features, low communication overhead & strong security are demonstrated by the experimental findings. The further task is left until later.

1. Identifying practical methods to increase SSI algorithms' efficiency.
2. The amount of characteristics has a significant impact on the TraceDCred algorithm's execution time in the AASSI protocol, & the follow-up work will further lessen the correlation between the two.
3. Looking for more methods, besides threshold procedures, to undermine issuer trust.

REFERNCES

[1] N. J. Ogbuke, Y. Y. Yusuf, K. Dharma, and B. A. Mercangoz, "Big data supply chain analytics: Ethical, privacy and security challenges posed to business, industries and society," Prod. Planning Control, vol. 33, nos. 2–3, pp. 123–137, Feb. 2022.

[2] D. A. Luong and J. H. Park, "Privacy-preserving identity management system on blockchain using zk-SNARK," IEEE Access, vol. 11, pp. 1840–1853, 2023.

[3] A. Rial and A. M. Piotrowska, "Security analysis of coconut, an attributebased credential scheme with threshold issuance," Tech. Rep., 2022.

[4] S. K. Dwivedi, R. Amin, and S. Vollala, "Design of secured blockchain based decentralized authentication protocol for sensor networks with auditing and accountability," Compute. Commun., vol. 197, pp. 124–140, Jan. 2023.
[5] R. Torres Moreno, J. B. Bernabe, J. G. Rodriguez, T. K. Frederiksen, M. Stausholm, N. Martinez, E. Sakkopoulos, N. Ponte, and A. Skarmeta, "The Olympus architecture-oblivious identity management for private user-friendly services," Sensors, vol. 20, no. 3, p. 945, 2020
[6] S. Cucko and M. Turkanovic, "Decentralized and self-sovereign identity: Systematic mapping study," IEEE Access, vol. 9, pp. 139009–139027, 2021.
[7] A. J. Zwitter, O. J. Gstrein, and E. Yap, "Digital identity and the blockchain: Universal identity management and the concept of the 'selfsovereign' individual," Frontiers Blockchain, vol. 3, p. 26, May 2020.
[8] B. Hu, Q. Yan, and Y. Zheng, "Tracking location privacy leakage of mobile ad networks at scale," in Proc. IEEE INFOCOM Conf. Compute. Commun. Workshops, Apr. 2018, pp. 1–2.
[9] A. A. Malik, H. Anwar, and M. A. Shibli, "Federated identity management (FIM): Challenges and opportunities," in Proc. Conf. Inf. Assurance Cyber Secure. (CIACS), Dec. 2015, pp. 75–82.
[10] C. Allen. (2016). The Path to Self-Sovereign Identity. [Online]. Available: html
[11] Z. A. Lux, D. Thatmann, S. Zickau, and F. Beierle, "Distributed- Ledger-based authentication with decentralized identifiers and verifiable credentials," in Proc. 2nd Conf. Blockchain Res. Appl. for Innov. Netw. Services (BRAINS), Sep. 2020, pp. 71–78.
[12] WWW Consortium. (2019). Verifiable Credentials Data Model 1.0: Expressing Verifiable Information on the Web. [Online]. Available: https://www.w3.org/TR/vc-data-model/?#core-data-mode
[13] J. Sedlmeir, R. Smethurst, A. Rieger, and G. Fridgen, "Digital identities and verifiable credentials," Bus. Inf. Syst. Eng., vol. 63, no. 5, pp. 603–613, Oct. 2021.
[14] O. Dib and K. Toumi, "Decentralized identity systems: Architecture, challenges, solutions and future directions," in Proc. Annal. Emer. Technol. Compute. (AETiC), 2020, pp. 0281–2516.
[15] S. K. Foundation, "Self-sovereign identity for more freedom and privacyselfkey," Tech. Rep., 2017.
[16] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena. (2017). UPORT: A Platform for Self-Sovereign Identity. [Online]. Available: https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf
[17] Veramo. Performant and Modular APIs for Verifiable Data and SSI. [Online]. Available: https://veramo.io/
[18] Serto. [Online]. Available: http://www.serto.id/
[19] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," Sovrin Found., vol. 29, p. 18, Sep. 2016.
[20] C. Cachin, "Architecture of the hyperledger blockchain fabric," in Proc. Workshop Distrib. Cryptocurrencies Consensus Ledgers, vol. 310, Chicago, IL, USA, 2016, pp. 1–4.
[21] J. Lee, J. Hwang, J. Choi, H. Oh, and J. Kim, "SIMS: Self sovereign identity management system with preserving privacy in blockchain," Tech. Rep., 2019.
[22] J. Lee, J. Choi, H. Oh, and J. Kim, "Privacy-preserving identity management system," Tech. Rep., 2021.
[23] A. Sonnino, M. Al-Bassam, S. Bano, S. Meiklejohn, and G. Danezis, "Coconut: Threshold issuance selective disclosure credentials with applications to distributed ledgers," 2018, arXiv:1802.07344.
[24] R. Mukta, J. Martens, H.-Y. Paik, Q. Lu, and S. S. Kanhere, "Blockchain based verifiable credential sharing with selective disclosure," in Proc. IEEE 19th Int. Conf. Trust, Secure. Privacy Compute. Commun. (TrustCom), Dec. 2020, pp. 959–966.
[25] R. Johnson, D. Molnar, D. Song, and D. Wagner, "Homomorphic signature schemes," in Proc. Cryptographers' Track RSA Conf. Springer, 2002, pp. 244–262.
[26] O. Goldreich, S. Goldwasser, and S. Micali, "How to construct random functions," J. ACM, vol. 33, no. 4, pp. 792–807, Aug. 1986.
[27] J. Groth and A. Sahai, "Efficient noninteractive proof systems for bilinear groups," SIAM J. Compute., vol. 41, no. 5, pp. 1193–1232, Jan. 2012.
[28] O. Sanders, "Efficient redactable signature and application to anonymous credentials," in Public-Key Cryptography—PKC (Lecture Notes in Computer Science). Springer, 2020, pp. 628–656.
[29] D. Pointcheval and O. Sanders, "Short randomizable signatures," in Proc. Cryptographers' Track RSA Conf., San Francisco, CA, USA. Springer, 2016, pp. 111–126.
[30] S. Figueroa-Lorenzo, J. Añorga Benito, and S. Arrizabalaga, "Modbus access control system based on SSI over hyperledger fabric blockchain," Sensors, vol. 21, no. 16, p. 5438, Aug. 2021.
[31] B. Alangot, P. Szalachowski, T. T. A. Dinh, S. Meftah, J. I. Gana, K. M. M. Aung, and Z. Li, "Decentralized identity authentication with auditability and privacy," Algorithms, vol. 16, no. 1, p. 4, Dec. 2022.
[32] D. Maram, H. Malvai, F. Zhang, N. Jean-Louis, A. Frolov, T. Kell, T. Lobban, C. Moy, A. Juels, and A. Miller, "CanDID: Can-do decentralized identity with legacy compatibility, Sybil-resistance, and accountability," in Proc. IEEE Symp. Secure. Privacy (SP), May 2021, pp. 1348–1366.
[33] Y. Yu, Y. Zhao, Y. Li, X. Du, L. Wang, and M. Guizani, "Blockchain-based anonymous authentication with selective revocation for smart

industrial applications,'' IEEE Trans. Ind. Informant., vol. 16, no. 5, pp. 3290–3300, May 2020.