Privacy-preserving model for Decentralized Digital Identity under EU compliance*

Mykolas Rutkauskas[*,†,1], Laura Atmanavičiūtė[1,†], Saulius Masteika[1,†]

[1] *Vilnius University, Kaunas Faculty, Muitinės g. 8, 44280 Kaunas, Lithuania*

Abstract

The growing demand for secure digital identity systems in the EU requires GDPR-compliant solutions that address accountability and data control in decentralized technologies. This research enhances privacy by using IPFS for decentralized storage and BBS+ cryptography to enable selective disclosure of credential attributes, without storing sensitive information directly on-chain. It explores secure issuance, verification, and storage of DIDs and VCs while ensuring GDPR compliance, including data minimization and the "right to be forgotten." BBS+ commitments enable selective disclosure and unlinkability, reducing traceability risks. IPFS ensures sensitive data remains off-chain. This conceptual study lays the groundwork for integrating these techniques, with future work assessing their feasibility and scalability in real-world identity verification.

Keywords

EU Digital identity, Blockchain, Decentralized Digital Identity systems, IPFS, BBS+ cryptography

1. Introduction

As digital identity adoption increases, governments and organizations are transitioning to digital identity solutions for security, efficiency and user convenience reasons [1]. However, centralized identity management systems often not able to meet fundamental requirements like privacy, user autonomy and cyber resilience. These challenges have led to decentralized digital identity (DDI) solutions using blockchain to enhance security, privacy and user control. As digital identity frameworks evolve, decentralized approaches are emerging to address security challenges across finance, healthcare, e-commerce and government services [2], [3], [4], [5].

Conventional digital identity solutions rely on public key infrastructure (PKI) and centralized certificate authorities, which pose security risks as single points of failure. Many suffer from data leaks due to weak security. Blockchain provides a decentralized alternative, ensuring tamper-proof storage through cryptography. By reducing reliance on central authorities, it strengthens security while giving users control over their data, minimizing unauthorized access [4].

Self-sovereign identity (SSI) gives individuals authority over their digital identities, allowing them to manage and share personal data while ensuring privacy and security. Blockchain enables verifiable identity claims without intermediaries [1], [2]. Some countries, like Estonia, have integrated blockchain into national digital identity programs for secure authentication [23].

To standardize decentralized identity, the World Wide Web Consortium (W3C) introduced Decentralized Identifiers (DIDs), using cryptographic proofs for authentication. The European Digital Identity (EUDI) Regulation and eIDAS 2.0 expand digital identity frameworks, introducing the EUDI Wallet for interoperability across Europe [6], [7].

* *IVUS 2025: Information Society and University Studies 2025, May 15, Kaunas, Lithuania*

* Corresponding author.

† These authors contributed equally.

mykolas.rutkauskas@knf.stud.vu.lt (M. Rutkauskas); laura.atmanaviciute@knf.vu.lt (L. Atmanavičiūtė); saulius.masteika@knf.vu.lt (S. Masteika)

Despite blockchain technology potential, decentralized identity faces challenges, particularly in regulatory compliance. Blockchain's open nature raises concerns about GDPR and eIDAS 2.0. Ensuring compliance with legal and security requirements remains a complex but essential step in advancing digital identity solutions [8], [9].

This research aims to design privacy-preserving model for decentralized digital identity that comply with EU regulations, particularly GDPR. By integrating robust encryption, blockchain technology and IPFS within the EU Digital Identity ecosystem, the study explores how Decentralized Identifiers (DIDs), Verifiable Credentials (VCs) and Zero-Knowledge Proofs (ZKP) can enhance privacy and security in identity management. The analysis focuses on developing method for secure issuance, verification and storage of identity credentials while addressing challenges related to data immutability, selective disclosure and the 'right to be forgotten' in a decentralized environment.

Research objective 1. To evaluate how Blockchain technology can be effectively integrated into the EU Digital Identity project while ensuring compliance with the General Data Protection Regulation (GDPR) by keeping personal data off-chain and leveraging cryptographic techniques to maintain both security and efficiency. This objective will be tested by demonstrating a technically feasible approach for integrating blockchain while maintaining GDPR compliance.

Research objective 2. To assess whether Verifiable Credentials in the EU Digital Identity project can be securely stored on the InterPlanetary File System (IPFS) to ensure decentralized storage; however, since IPFS does not natively support data deletion, additional mechanisms must be implemented to align with GDPR's 'right to be forgotten' principle. This objective will be tested by evaluating the feasibility of implementing an efficient revocation or deletion mechanism within IPFS.

2. Methodology

This study follows a systematic approach to developing privacy-preserving components model for decentralized digital identity using blockchain and IPFS within the EU Digital Identity ecosystem. The methodology consists of four phases, focusing on analyzing existing solutions, reviewing prior research, assessing regulatory requirements, evaluating technical feasibility and exploring implementation strategies to ensure compliance with GDPR and enhance privacy and security in decentralized identity management (Fig 1).

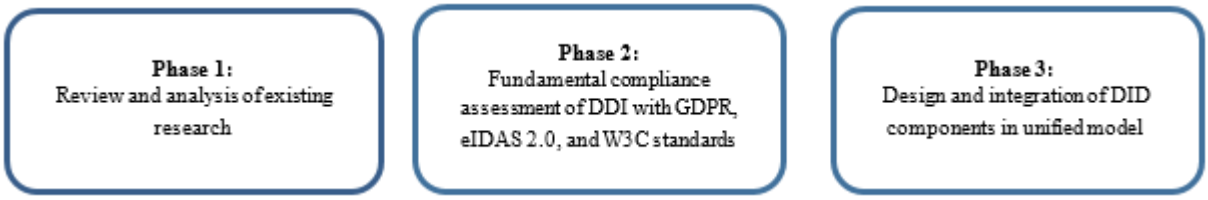

Figure 1: Research methodology for developing DDI model

The first phase includes a comprehensive review of previous research on decentralized identity (DID) solutions, cryptographic mechanisms and blockchain-based identity management. This review provides insights into technological advancements, privacy-preserving techniques and decentralized storage models relevant to the study.

The second phase conducts a fundamental compliance assessment of decentralized identity (DID) solutions with GDPR, eIDAS 2.0 and W3C standards. This phase identifies the essential regulatory and technical requirements that decentralized identity systems must address. The focus is to evaluate fundamental components such as Verifiable Credentials (VC), Decentralized Identifiers (DID) and selective disclosure, ensuring their compliance with privacy and security standards during VC issue,

storage and verification. The assessment involves analysis of publicly available data, regulatory documents and research analysis documents to determine the extent to which DID-based identity management solutions align with W3C guidelines and EU legal requirements. The outcome of this phase establishes a regulatory and technical foundation for the design and implementation of a compliant decentralized identity system.

The third phase evaluates cryptographic mechanisms, including BBS+, PS and CL signatures to evaluate their suitability for privacy-preserving Verifiable Credentials (VCs) and compliance with GDPR and eIDAS 2.0. Based on this assessment, it designs and integrates Decentralized Identifier (DID) components into a unified, privacy-preserving model, implementing encrypted data storage on blockchain, secure identity verification and IPFS-based VC storage. Schematic representations illustrate the technical processes of DID issuance, cryptographic verification and encrypted storage, ensuring compliance with EU regulatory standards.

3. Design Privacy-Preserving model for Decentralized Digital Identity system

Developing a privacy-preserving Decentralized Digital Identity (DDI) system requires evaluating existing research and ensuring compliance with GDPR, eIDAS 2.0 and W3C standards. This analysis identifies gaps and research opportunities for improving DDI components, which are integrated into a unified model for empirical validation. Research highlights fundamental challenges in adoption, regulatory compliance and impact assessment, specifically in defining blockchain role within digital identity ecosystems. Addressing these issues is essential for advancing secure and effective decentralized identity frameworks.

3.1. Conceptual overview of decentralized digital identity system regulatory and research analysis

Research on decentralized digital identity systems reveals several critical gaps that must be addressed to enhance adoption, regulatory compliance and impact assessment. Existing studies highlight the necessity of identifying key adoption factors, evaluating regulatory implications and establishing standardized metrics to assess blockchain's role in digital identity ecosystems [10]. Addressing these gaps is crucial for advancing secure and efficient decentralized identity frameworks.

A significant area of concern involves the risks associated with blockchain-based identity management. One of the primary challenges is the potential leakage of identity wallets, which, if compromised, can lead to unauthorized access, identity theft and other malicious activities. The immutability of blockchain further complicates identity management, as it restricts the ability to modify or revoke identities efficiently, unlike traditional systems. Additionally, the adoption of Self-Sovereign Identity (SSI) entails substantial infrastructure costs, requiring investments in authentication mechanisms, personnel training and continuous maintenance. Another critical challenge is key management; losing private keys results in permanent access loss, while outsourcing key management contradicts SSI's core principles. Addressing these vulnerabilities is essential for ensuring the security, efficiency and economic feasibility of blockchain-based identity solutions [11].

Cybersecurity risks present further obstacles to the implementation of decentralized digital identity systems, particularly in relation to potential attack surfaces. Research identifies threats such as identity spoofing, identity theft and Distributed Denial-of-Service (DDoS) attacks, which can disrupt authentication and verification mechanisms, indirectly affecting identity integrity. Attackers may impersonate issuers, exploit misconfigurations, or disrupt verification mechanisms, undermining the reliability of decentralized identity frameworks. While attack tree modeling and risk matrix evaluations provide valuable methodologies for assessing these risks, further research is required to enhance

authentication mechanisms, optimize consensus protocols and develop privacy-preserving verification methods [12]. Additionally, the integration of zero-knowledge proofs (ZKPs) and the application of quantitative risk modeling represent critical research gaps in enhancing the security of SSI systems [13]. Despite these threats, decentralized identity solutions built on blockchain technology offer significant security advantages over conventional identity management systems due to decentralization, cryptographic protections and user-controlled identity management. However, further technological advancements are necessary to ensure full compliance with regulatory requirements [14].

Access control mechanisms in decentralized identity management represent another key area of research. Traditional access control systems are often characterized by centralization, making them vulnerable to single points of failure, data breaches and unauthorized access due to a lack of transparency and inadequate user control over identity data. In contrast, blockchain-based identity management and access control (BADIMAC) systems mitigate these risks by leveraging decentralization, self-sovereign identity principles and advanced cryptographic techniques such as ZKPs for privacy-preserving verification [14]. By eliminating intermediaries, blockchain enhances transparency, ensures immutability and provides more robust control over identity verification across multiple organizations. Research demonstrates the necessity of exploring hybrid models that integrate blockchain with off-chain storage solutions, privacy-enhancing cryptographic methods and interoperability frameworks to facilitate seamless adoption across different industry sectors [14].

Beyond access control, the integration of advanced cryptographic methods and hybrid storage models is critical for achieving a balance between decentralization and regulatory compliance. The development of GDPR-compliant privacy-preserving techniques is necessary to ensure that blockchain-based identity systems meet legal requirements while maintaining decentralization. Technologies such as zero-knowledge proofs, ring signatures and homomorphic encryption provide mechanisms for secure identity verification without exposing personal data. Furthermore, hybrid storage models that combine on-chain authentication with off-chain data storage present a potential solution to the immutability challenges of blockchain while ensuring compliance with the Right to Be Forgotten (RTBF). These advancements are essential for addressing regulatory challenges while preserving the fundamental benefits of blockchain technology in decentralized digital identity management [15].

3.2 Evaluation overview of fundamental compliance components for Decentralized Digital Identity systems under GDPR, eIDAS 2.0 and W3C Standards

The selection of appropriate technological components for decentralized digital identity (DI) frameworks must align with legal and regulatory standards to ensure privacy, security and interoperability. EU regulations, including the General Data Protection Regulation (GDPR) and the Electronic Identification, Authentication and Trust Services (eIDAS 2.0), alongside W3C standards, establish essential compliance requirements for digital identity ecosystems. These regulations mandate privacy-preserving mechanisms, secure identity verification and controlled access to personal data [6], [7]. To meet these criteria, digital identity architectures must integrate solutions that maintain regulatory compliance while ensuring system security and scalability.

Regulatory challenges significantly impact decentralized digital identity frameworks. GDPR imposes strict requirements on data processing, including the right to erasure (Article 17), which conflicts with blockchain immutability and data minimization (Article 5), requiring that personal data be retained only when strictly necessary. Data protection by design (Article 25) mandates privacy-centric architectures, while cross-border data governance (Article 3) enforces strict accountability across jurisdictions. Additionally, controlled processing (Article 28) and traceability obligations (Article 30) introduce further challenges, particularly for decentralized systems. eIDAS 2.0 reinforces these requirements by mandating privacy-preserving design (Article 5a), cybersecurity measures (Article 5e) and vulnerability assessments (Article 12a) to ensure the continuous mitigation of security risks. These regulations shape the technical

and governance frameworks for decentralized identity, emphasizing compliance with European legal standards (Fig 2).

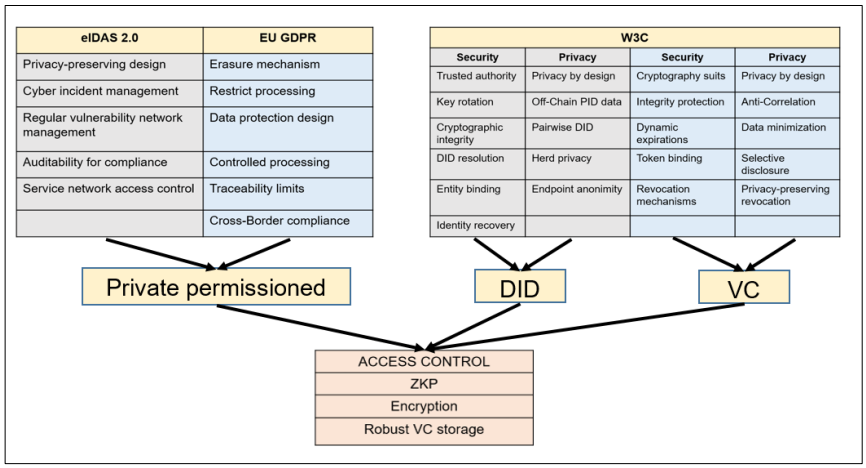

Figure 2: Fundamental requirements for Blockchain-based DDI selection

Assessing decentralized digital identity government-led projects such as Bhutan's National Digital Identity and Argentina's QuarkID leverage permissionless blockchains. Compliance challenges persist, particularly with GDPR's right to erasure, eIDAS 2.0 cyber resilience and DID correlation risks that impact traceability. In addition, scalability and interoperability with EBSI remain critical. Given these constraints, private permissioned blockchains may better align with regulations.

Private permissioned blockchains offer controlled access, governance oversight, and regulatory compliance, mitigating risks of public blockchain models. They enable privacy-focused architectures while supporting decentralized identifiers (DIDs) and verifiable credentials (VCs) within a secure framework [16]. Beyond blockchain selection, decentralized digital identity systems must define clear DID and VC requirements for security, scalability, and privacy. Key features include off-chain storage, cryptographic integrity, and Zero-Knowledge Proofs (ZKP) for selective disclosure. Encryption enhances security, enabling computations on encrypted data, while modular cryptographic frameworks support credential issuance, lifecycle management and revocation [18].

Private permissioned blockchains have robust potential to align with W3C standards, supporting secure DID resolution, cryptographic timestamping, key rotation, and privacy-preserving identity recovery [16]. Pairwise DIDs, off-chain storage, and enhanced access controls address GDPR privacy requirements [15]. Modular cryptographic protocols ensure privacy-preserving credential issuance, verification and revocation, maintaining compliance with W3C and EU frameworks.

Advanced cryptographic techniques, structured governance, and compliance-driven architectures support secure, regulation-compliant digital identity frameworks. Aligning DID and VC models with evolving regulations is fundamental for adoption and interoperability [17]. Cryptographic layers have potential to mitigate risks of individual correlation. The integration of InterPlanetary File System (IPFS) for VC storage enhances immutability, redundancy and security [20].

3.3 Robust encryption appliance and GDPR-compliant storage of Verifiable Credentials using IPFS

In decentralized digital identity projects, ensuring verifiable credentials or selective disclosure while maintaining privacy and unlinkability is fundamental. Based on the findings of the article "On Cryptographic Mechanisms for Selective Disclosure of Verifiable Credentials," BBS+ signatures emerge as the most suitable choice (Table 1). Compared to other cryptographic mechanisms, BBS+ offers a strong

balance between credential size, verification time and unlinkability. While PS signatures are optimized for efficiency, they have medium unlinkability due to their fixed public parameters, making them more susceptible to correlation risks. Similarly, CL signatures, while offering high unlinkability, are impractical due to their large credential size and slow verification time. In contrast, BBS+ signatures use randomized proof generation, reducing the chances of repeated-use linkability, which is essential for preventing user tracking in decentralized identity ecosystems [18].

The comparative analysis in the article highlights that BBS+ signatures outperform other zero-knowledge proof-based mechanisms in scenarios where both privacy and efficiency are required. Unlike hash commitments and Merkle trees, which rely on structured data and require additional zero-knowledge proofs to maintain unlinkability, BBS+ inherently provides strong privacy guarantees. Merkle trees, while efficient for batch verification, can leak metadata that exposes credential structure. Hash commitments, though lightweight, do not inherently support predicate proofs, making them less adaptable for complex verifications [18]. BBS+ signatures, on the other hand, support full randomization, ensuring that every proof is unique, thereby eliminating the risk of correlation attacks in repeated identity verification scenarios. This makes them particularly suited for compliance with frameworks such as eIDAS 2.0 and GDPR, where privacy protection is paramount.

For blockchain-based decentralized identity systems, where privacy and unlinkability are critical, BBS+ signatures provide an optimal solution. They support predicate proofs, allowing users to prove statements such as "age > 18" without revealing their exact birthdate. Additionally, compared to Merkle tree commitments, which require additional zero-knowledge proofs for unlinkability, BBS+ natively supports strong unlinkability without extra computational overhead [19]. The randomized proof generation of BBS+ ensures that no two verifications are linkable, reinforcing privacy while maintaining cryptographic security. Given these advantages, BBS+ signatures stand out as the best choice for preventing user correlation while ensuring secure and privacy-preserving verifiable credentials in decentralized digital identity projects.

Based on BBS+ robustness and optimal applicability, the theoretical framework suggests its integration for ISSUER DID, user VC and selective disclosures anonymization. This analysis suggests these components theoretically without empirical proof, which has to be developed.

Table 1
Privacy and performance comparison of BBS+, PS, CL signatures [18], [19]

Feature	BBS+ Signatures	PS Signatures	CL Signatures
Type	ZKP-Based	ZKP-Based	ZKP-Based
Credential size	Medium ~512–1024 bytes	Optimized ~256–768 bytes	Largest ~2048+ bytes
Verification time	Medium ~10–20ms	Fastest ~5–15ms	Slowest ~50–100ms
Unlinkability	Strong (unlikability score 4/5) (If nonce not properly randomized by mistake)	Medium (unlikability score 3/5)	Strongest (unlikability score 5/5)
Randomized proof generation	Yes (fully randomized) (nonce-based re-randomization score 5/5)	Partial (fixed proof structure with partial blinding score 3/5)	Yes (blinded commitments score 5/5)
Fixed public parameters in proofs	No (randomized public keys and blind signature techniques score 5/5)	Yes (fixed pairing elements, leading to potential correlation risks score 2/5)	No (fully blinded public keys score 5/5)
Risk of linkability in repeated use	Low	Medium	Very low
Best use case for privacy	High-security identity verification	Scalable systems with efficient verification	Maximum privacy for High-security scenarios

The application of BBS+ encryption in the issuance of Verifiable Credentials (VCs) follows a structured sequence to ensure privacy and authenticity (Fig 3). First, a user requests Verifiable Credential (VC) from the issuer. The issuer then generates and signs a Verifiable Credential (VC) using its private key, producing a signed VC that ensures selective disclosure and authenticity. The issuer provides the signed VC along with the organization's public key to the user, ensuring that the recipient can verify the credential's legitimacy.

To enhance security and enable privacy-preserving storage, the issuer encrypts the VC using a randomly generated 32-byte symmetric key and stores an encrypted copy on IPFS and DWN. The issuer's Decentralized Identifier (DID) remains open and publicly accessible. On-chain, main elements are stored: the issuer's DID and the Merkle tree root hash representing the revocation status of issued VCs. No commitments, encryption, or additional data are stored on-chain. This design ensures minimal on-chain footprint while enabling decentralized verification and revocation checking.

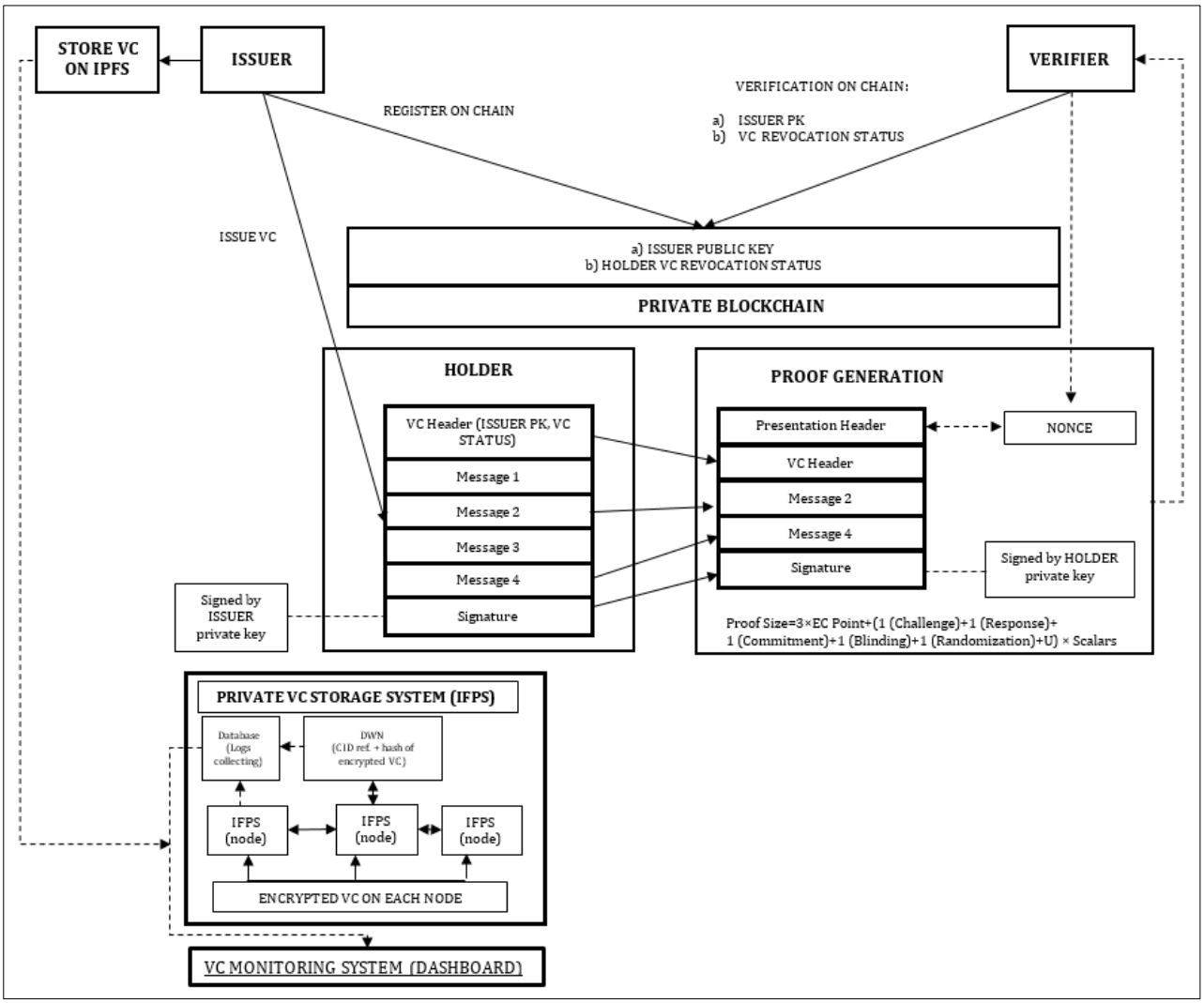

Figure 3: Privacy-preserving model for DDI

When a verifier needs to authenticate a user's Verifiable Credential without revealing unnecessary information, a Zero-Knowledge Proof (ZKP) mechanism using BBS+ is employed (Fig. 3). The process begins with the user requesting a nonce from the verifier, which serves as a countermeasure against replay attacks. The verifier generates a random nonce and sends it to the user, ensuring freshness in the authentication process.

Using the received nonce, the user generates a Zero-Knowledge Proof (ZKP) using BBS+ from VC attributes. This proof is signed using the user's private key to prevent forgery. The user then submits the ZKP proof to the verifier for validation. Upon receiving these elements, the verifier checks the validity of the ZKP proof. If proof is verified successfully, then it is accepted and authentication is confirmed. If any of the cryptographic checks fail, the proof is rejected, preventing fraudulent claims. This mechanism ensures that users can authenticate themselves without exposing their full credentials, supporting privacy-preserving verification that aligns with GDPR requirements and decentralized identity principles. The integration of BBS+ signatures in Zero-Knowledge Proofs enables unlinkable and secure authentication, safeguarding users from identity correlation and privacy violations in decentralized identity systems.

Recent studies demonstrate that IPFS is widely integrated in image copyright protection, keeping healthcare records and other data-sensitive applications due to its decentralized, immutable and content-

addressed storage capabilities [20]. Unlike traditional databases that rely on centralized servers, IPFS equally distributes files across the network on each network node, reducing the risk of data loss, censorship and unauthorized alterations. One of the key findings in recent research is that IPFS significantly enhances data security and integrity, making it an ideal choice for industries requiring tamper-resistant and verifiable storage [21]. However, one of its primary drawbacks has been slow retrieval times, as IPFS relies on a Distributed Hash Table (DHT) to locate and fetch file chunks from multiple nodes. This challenge has limited its efficiency in high-speed data access scenarios, particularly for large-scale applications requiring frequent retrieval [20].

To overcome the retrieval time issue, advancements in indexing structures have been introduced, such as the dual-layer Distributed Hash Table (DHT) indexing structure. This improvement enhances file location efficiency by adding a local index layer to the traditional global DHT, reducing the number of network queries required to fetch a file. Studies show that this optimization increases retrieval efficiency by up to 33% [20], making IPFS more viable for applications needing fast and reliable data access. These enhancements expand IPFS's usability in digital identity management, where secure, decentralized and easily retrievable identity verification records are essential. By improving retrieval speed and network efficiency, IPFS is becoming a more practical solution for identity verification, healthcare data storage and digital record-keeping, ensuring data availability and authenticity without relying on centralized authorities [21].

Model suggests a possible integration solution within a decentralized digital identity framework, leveraging private IPFS for secure verifiable credential (VC) storage and management (Fig 3). The IPFS-based private VC storage system consists of four key components: (1) a Decentralized Web Node (DWN), which manages CID storage, access control, VC verification and recovery; (2) equally distributed IPFS nodes, where encrypted VCs are stored across the network, ensuring decentralization and redundancy; (3) an additional database for logs collection, which records system interactions and access events; and (4) a VC monitoring dashboard, responsible for detecting VC tampering by comparing stored CIDs, monitoring access control logs and tracking erasure events.

By implementing IPFS within a decentralized identity framework, data security, integrity and verifiability are enhanced, ensuring that VCs remain protected from unauthorized alterations or deletions. In cases where VC erasure is required, the process demands unpinning the VC from all nodes and executing a garbage collection procedure, making accidental deletion highly unlikely. Unlike conventional databases where deletion is simple, this multi-step approach reinforces immutability, security and resilience against cyber threats or data leaks, ensuring stronger protection for sensitive identity records in decentralized ecosystems.

4. Research results, conclusion and future research directions

This research establishes a GDPR- and eIDAS 2.0-compliant decentralized digital identity (DDI) model by integrating private blockchain, IPFS, Verifiable Credentials (VCs), and Zero-Knowledge Proofs (ZKP). Unlike public blockchain models like QuarkID, which pose traceability and immutability risks, the proposed private blockchain enhances regulatory oversight, security, and cyber resilience while keeping personal data off-chain to comply with GDPR's data minimization (Article 5(1)(b)) and privacy by design (Article 25). It also supports VC revocation (Article 17) and meets eIDAS 2.0's cybersecurity mandates, including incident management (Article 45) and vulnerability monitoring (Article 46). The model leverages BBS+ cryptography and selective disclosure to prevent identity correlation and unauthorized tracking. IPFS-based off-chain storage ensures secure credential management while maintaining technical decentralization with regulatory control. This framework offers a privacy-compliant alternative to centralized identity models, strengthening data security, credential revocation, and regulatory compliance. Future research should focus on real-world implementation, optimizing BBS+

commitments for enhanced privacy-preserving authentication and aligning blockchain identity frameworks with evolving EU regulations. As the EU Digital Identity framework evolves, addressing scalability, retrieval efficiency, and interoperability will be crucial for widespread adoption. This study lays a foundation for secure, scalable, and privacy-preserving decentralized identity architectures, ensuring trust and compliance in the digital economy.

Acknowledgements

The publication was prepared during the implementation of the project “Implementation of R&D activities, creating APV products by Deverium, UAB" (Project No. 02-020-K-0034). The project is co-financed by the European Union.

Declaration on Generative AI

During the preparation of this work, the authors used CHAT-GPT-4 in order to: Grammar and spelling check. After using this tool, the authors reviewed and edited the content as needed and take (full responsibility for the publication’s content.

References

[1] Goodell, G., Aste, T., 2019. A Decentralised Digital Identity Architecture. Front. Blockchain 2, 17. https://doi.org/10.3389/fbloc.2019.00017.

[2] World Economic Forum: Blockchain can help create privacy-preserving digital ID, https://www.weforum.org/agenda/2023/03/blockchain-privacy-preserving-digital-id/, last accessed 2025/02/23.

[3] Ahmed, Md.R., Islam, A.K.M.M., Shatabda, S., Islam, S., 2022. Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey. IEEE Access 10, 113436–113481. https://doi.org/10.1109/ACCESS.2022.3216643

[4] Mole, C., Chalstrey, E., Foster, P., Hobson, T., 2023. Digital identity architectures: comparing goals and vulnerabilities. https://doi.org/10.48550/arXiv.2302.09988

[5] Mazzocca, C., Acar, A., Uluagac, S., Montanari, R., Bellavista, P., Conti, M., 2024. A Survey on Decentralized Identifiers and Verifiable Credentials. https://doi.org/10.48550/arXiv.2402.02455

[6] W3C: Decentralized identifiers (DID) v1.0 – core architecture, data model and representations. W3C Recommendation, July 19, 2022. https://www.w3.org/TR/did-core/, last accessed 2025/02/23.

[7] W3C: Verifiable credentials data model v1.1. W3C Recommendation, March 3, 2022. https://www.w3.org/TR/vc-data-model/, last accessed 2025/02/23.

[8] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European digital identity framework.

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

[10] Lei, C.F., Ngai, E.W.T., 2023. Blockchain from the information systems perspective: Literature review, synthesis and directions for future research. Information & Management 60, 103856. https://doi.org/10.1016/j.im.2023.103856

[11] Liu, Y., He, D., Obaidat, M.S., Kumar, N., Khan, M.K., Raymond Choo, K.-K., 2020. Blockchain-based identity management systems: A review. Journal of Network and Computer Applications 166, 102731. https://doi.org/10.1016/j.jnca.2020.102731

[12] Gugueoth, V., Safavat, S., Shetty, S., Rawat, D., 2023. A review of IoT security and privacy using decentralized blockchain techniques. Computer Science Review 50, 100585. https://doi.org/10.1016/j.cosrev.2023.100585

[13] Lavin, R., Liu, X., Mohanty, H., Norman, L., Zaarour, G., Krishnamachari, B., 2024. A Survey on the Applications of Zero-Knowledge Proofs. https://doi.org/10.48550/arXiv.2408.00243

[14] Agarkar, A.A., Karyakarte, M., Chavhan, G., Patil, M., Talware, R., Kulkarni, L., 2024. Blockchain aware decentralized identity management and access control system. Measurement: Sensors 31, 101032. https://doi.org/10.1016/j.measen.2024.101032

[15] x Belen-Saglam, R., Altuncu, E., Lu, Y., Li, S., 2023. A systematic literature review of the tension between the GDPR and public blockchain systems. Blockchain: Research and Applications 4, 100129. https://doi.org/10.1016/j.bcra.2023.100129

[16] Amiri, M.J., Agrawal, D., El Abbadi, A., 2021. Permissioned Blockchains: Properties, Techniques and Applications, in: Proceedings of the 2021 International Conference on Management of Data. Presented at the SIGMOD/PODS '21: International Conference on Management of Data, ACM, Virtual Event China, pp. 2813–2820. https://doi.org/10.1145/3448016.3457539

[17] Butincu, C.N., Alexandrescu, A., 2024. Design Aspects of Decentralized Identifiers and Self-Sovereign Identity Systems. IEEE Access 12, 60928–60942. https://doi.org/10.1109/ACCESS.2024.3394537

[18] Flamini, A., Sciarretta, G., Scuro, M., Sharif, A., Tomasi, A., Ranise, S., 2024. On cryptographic mechanisms for the selective disclosure of verifiable credentials. Journal of Information Security and Applications 83, 103789. https://doi.org/10.1016/j.jisa.2024.103789

[19] Ramić, Š.B., Cogo, Ehlimana, Prazina, I., Cogo, Emir, Turkanović, M., Mulahasanović, R.T., Mrdović, S., 2024. Selective disclosure in digital credentials: A review. ICT Express 10, 916–934. https://doi.org/10.1016/j.icte.2024.05.011

[20] Cong, X., Feng, L., Zi, L., 2024. Research on IPFS Image Copyright Protection Method Based on Blockchain. CMC 81, 663–684. https://doi.org/10.32604/cmc.2024.054372

[21] Doan, T.V., Psaras, Y., Ott, J., Bajpai, V., 2022. Toward Decentralized Cloud Storage With IPFS: Opportunities, Challenges and Future Considerations. IEEE Internet Comput. 26, 7–15. https://doi.org/10.1109/MIC.2022.3209804

[22] Dunphy, P., 2022. A Note on the Blockchain Trilemma for Decentralized Identity: Learning from Experiments with Hyperledger Indy. https://doi.org/10.48550/arXiv.2204.05784

[23] Karm, A., n.d., Estonia – the Digital Republic Secured by Blockchain. https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf