УДК 004.056.5:004.8 **DOI:10.30837/rt.2025.2.221.05**

D.O. KOZIUBERDA, M.V. YESINA, cand. techn. sciences, Yu.L. GOLIKOV

DIGITAL IDENTITY AND ZKP: ANONYMOUS DATA AND SECURE AUTHENTICATION

Introduction

The way we verify our identity and interact in the digital environment is rapidly changing. For decades, digital identification has relied on centralized mechanisms – passwords, social logins, and centralized registries maintained by single providers or authorities. This approach creates critical vulnerabilities: from data leaks and hacks to mass surveillance and manipulation, depriving users of control over their personal information. In this model, centralized intermediaries act as controllers of personal data, which is often collected and processed without proper notification or consent, significantly limiting the individual's ability to influence how their digital identity is used.

In response to these challenges, a new model is emerging – decentralized digital identity (Decentralized Identity, DID). It is based on blockchain technologies and cryptographic primitives that allow individuals to own and store their data independently, as well as control their attestations – without intermediaries or a central authority [1].

One of the key technologies enabling this is zero-knowledge proofs (ZKP). This technology allows verifying the validity of a certain fact without revealing the information itself.

This paradigm of anonymous attestations opens the way to secure authentication that minimizes the amount of personal data transmitted or stored and eliminates the need for constant verification through centralized structures. Moreover, it creates conditions for self-sovereign identity (SSI) – the concept where the user is the sole owner of their digital persona [2].

In this article, we will examine the fundamentals of decentralized identity, the key role of ZKP in privacy protection, standardization initiatives, as well as the practical implications and prospects of combining these technologies in real-world applications.

1. Decentralized Digital Identity

Decentralized identity is an innovative approach to managing digital identity that enables individuals and organizations to independently create, own, and control their digital credentials and identifiers without relying on centralized authorities [1, 3].

Unlike traditional systems governed by governments, corporations, or third-party platforms, decentralized identity utilizes technologies such as Verifiable Credentials (VC), Digital ID Wallets, and blockchain to provide secure, verifiable, and privacy-oriented interactions in the digital space.

A key advantage is that credentials can be issued once, stored by the user in a secure digital wallet, and reused across different systems. This significantly reduces risks, eliminates the need for repeated verifications, and creates a consistent and reliable method of information verification – in finance, healthcare, education, organizational access management (IAM), or supply chains.

By placing the user at the center of the system, decentralized identity offers an effective alternative to fragmented and error-prone traditional identification models.

Key components of decentralized identity [4]:

• Verifiable Credentials (VC) are digital, cryptographically secured representations of identification information that cannot be forged or altered. They are issued by trusted organizations – government agencies, identity verification companies, banks, or other institutions. VCs guarantee the authenticity and integrity of the data, enabling the verification of a user's identity without risk of forgery or fraud. Users store these credentials (attestations) in digital wallets and can present them to verifying parties, disclosing only the necessary information.

• Digital ID Wallets are software tools designed for storing and managing verifiable credentials. They can be implemented as mobile applications or cloud-based solutions, providing conven-

ience and control over personal data. Through these wallets, users can securely share their credentials with various services while maintaining privacy and protection.

• Decentralized Identifiers (DIDs) are globally unique identifiers created and controlled by the user without involvement of a centralized authority. DIDs are typically stored on a blockchain, ensuring their immutability and security. Importantly, DIDs do not contain personal data – they point to decentralized documents that describe the identity subject and include means for authentication.

At the core of decentralized identity is a tripartite trust model that includes [4]:

1. Issuer – a trusted party that creates and signs a verifiable credential. This can be a university, government agency, financial institution, or an identity verification platform.

2. Holder – an individual or organization that receives credentials and stores them in a digital wallet. The holder independently decides how and when to share them.

3. Verifier – a party that needs to verify certain information about the holder: age, license status, education, employment, etc. The verification is performed without direct contact with the issuer, using cryptographic verification.

Fig. 1 depicts this three-party trust model, or decentralized identification system.

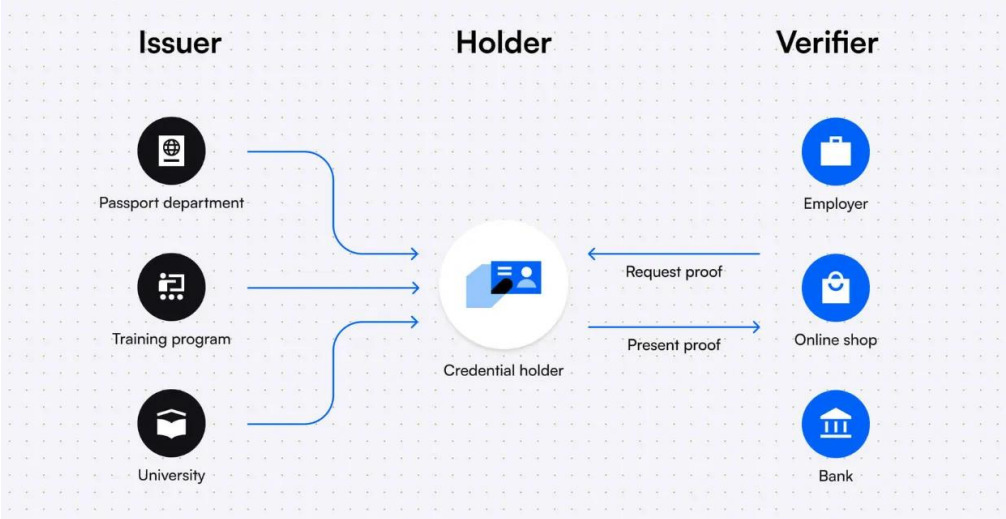

Fig. 1. Three-Party Trust Model (Decentralized Identification System)

This ecosystem enables secure and confidential data exchange between participants without the need to store or repeatedly request sensitive information.

It is also worth examining self-sovereign identity (SSI) in more detail. The terms decentralized identity (DID) and self-sovereign identity (SSI) are often used interchangeably, although there are distinctions between them.

Both concepts are based on the idea that an individual should own and control their digital identity rather than relying on centralized entities – such as governments, online platforms, or corporations – to manage identity on their behalf. However, SSI is a specific approach within the broader landscape of decentralized identity, with a particular focus on user autonomy.

Self-sovereign identity (SSI) is an identity management model in which an individual fully controls their digital attributes: how they are stored, shared, and used – without involving centralized trusted intermediaries. SSI is based on three main components: verifiable credentials, blockchain, and decentralized identifiers (DIDs).

The main difference between decentralized and self-sovereign identity:

• Decentralized identity is a broad concept that encompasses identity systems not governed by a single central authority. It includes both models where the user controls their own identity (e.g., SSI), as well as enterprise-focused models in which control is exercised collectively (e.g., federated Identity and Access Management (IAM) networks that utilize verifiable credentials).

• Self-Sovereign Identity (SSI) is a philosophy and implementation model within the broader decentralized identity paradigm that emphasizes full user control, data minimization, and the principle of privacy by design. In an SSI system, it is the user – not a company or government – who makes the final decision about which data to share, when, and with whom.

Fig. 2 illustrates the components of Self-Sovereign Identity.

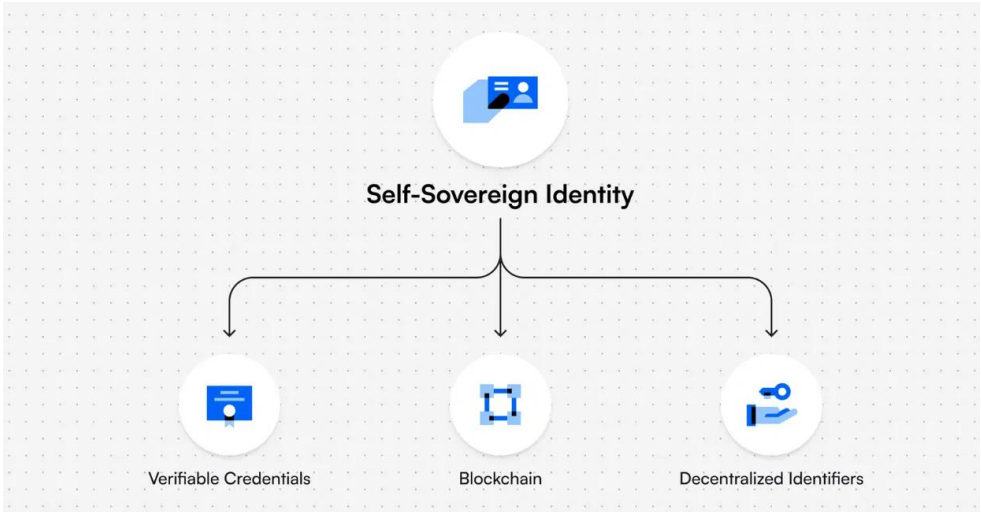

Fig. 2. Self-Sovereign Identity

2. Use of ZKP in decentralized identifiers

Zero-knowledge proof/protocol (ZKP) is an interactive cryptographic protocol that allows one party (the verifier) to be convinced of the truth of any statement (usually mathematical) without gaining any additional information from the other party (the prover).

Zero-knowledge proofs (ZKP) add a new level of privacy and control for the user in decentralized identity solutions. Here is how they enhance DID capabilities in various use cases [4, 5]:

• Selective disclosure. Users can prove specific attributes about themselves (e.g., "I am over 18 years old," "I have a valid driver's license") without revealing the underlying data. This ensures necessary verification while preserving privacy.

• Minimal data sharing. Instead of sharing entire documents or personal data, ZKPs enable precise identity verification using only the minimally required information. This reduces disclosure of sensitive data and lowers the risk of misuse.

• Enhanced trust. ZKPs guarantee the authenticity of information without requiring centralized trust in the identity data provider. They facilitate interaction between parties that otherwise would not trust each other with personal data.

• Reputation systems. ZKPs can support privacy-preserving reputation systems based on verified credentials. Users can prove they possess certain qualifications or meet requirements without fully revealing their identity.

• Decentralized access control. ZKPs can provide fine-grained access control in decentralized systems. Users can prove they have access rights to specific resources or services without disclosing unnecessary personal information.

• Correlation prevention. ZKPs can be used to create unique, unlinkable proofs each time credentials are used. This prevents tracking and the creation of detailed behavioral and identity profiles of individuals.

• Private electronic voting. Election integrity is critical, but voter anonymity is also important. Systems combining DID and ZKP enable mechanisms where a voter's identity can be verified without linking to a specific vote. ZKPs allow verification of voting eligibility and prevent double voting while preserving ballot secrecy.

• Medical data protection. Medical information is among the most sensitive data categories. ZKPs within the decentralized identity model give patients control over their medical records. Users can decide themselves who and to what extent can access their data – for example, doctors for treatment or researchers for scientific purposes – without revealing the full content of records. This opens possibilities for confidential medical research without compromising patient privacy.

There are two types of zero-knowledge proofs for identification: interactive and non-interactive.

In the interactive version, the prover must perform a series of tasks to confirm their knowledge of certain facts. For providing self-sovereign identity, this method often uses principles of mathematical probability.

The non-interactive zero-knowledge proof utilizes decentralized identity management and does not require interaction between the prover and the verifier.

Both types of zero-knowledge proofs include the following three requirements:

1. Soundness. If the prover provides incorrect or missing information, the verifier will not be convinced, since the statement cannot be falsified.

2. Completeness. If the statement is true, the verifier is confident that the prover possesses all the necessary information.

3. Zero-knowledge. The verifier gains no additional information about the prover, ensuring the anonymity of personal and sensitive data.

One of the earliest scientific works on zero-knowledge proofs, first published in 1988, presents a new identification scheme based on such proofs, which is a more efficient alternative to RSA-based schemes. In identification schemes, subject A verifies their identity to subject B using some constant value S in the form of a value or a physical card, without giving subject B the ability to later impersonate A. Traditional identification schemes use encryption and/or hashing together with credentials such as digital passwords, PIN codes, credit card chips, etc. This work proposes a practical scheme that makes it impossible even for an experienced attacker to collude with a dishonest verifier B to create forged credentials and impersonate A.

The methodology is based on interactive proofs, where a subject can confirm their identity by proving knowledge of the secret key of their credentials without revealing the secret itself. It is sufficient to provide proof of knowledge of the secret, which serves as a digital signature unique to each individual. The article describes a scheme that does not require a directory (i.e., a centralized repository of public keys or identity data). It also proposes implementing such a scheme using hypothetical "smart cards," which can act as physical credentials generating zero-knowledge proofs of identity using microprocessors – for use in everyday identity verification.

The zk-creds protocol uses zero-knowledge proofs (specifically zk-SNARKs) to transform existing identity documents into anonymous credentials, eliminating the need for issuers of such credentials to store signing keys. This system differs from traditional methods where issuers sign credentials and identity documents for verification. By integrating with existing identification infrastructures – such as government ID cards or university diplomas – zk-creds transforms these traditional credentials into a digital, anonymous, yet verifiable format [5].

3. Architecture and Standards of the Ecosystem: Trends and Innovations

Key points highlighting the importance of standardization:

• Compatibility. Common standards ensure seamless interaction between different decentralized identity solutions and platforms.

• Adoption. Standardization fosters trust and lowers barriers for businesses and users interested in decentralized identity.

• Ecosystem development. A harmonized set of standards stimulates innovation and collaboration across the decentralized identity space.

Table 1 below presents key initiatives and their role in the standardization of digital identity.

Table 1

Major frameworks and projects in digital identity standardization

Initiative	Focus	Role in Standardization
W3C Verifiable Credentials	Establishes standards for the format and structure of verifiable credentials, covering their issuance, presentation, and cryptographic signatures.	Provides a common representation of verifiable credentials, enhancing interoperability between different systems.
Decentralized Identity Foundation (DIF)	Develops open-source protocols, specifications, and tools to ensure interoperability within the decentralized identity ecosystem.	Promotes collaboration and the creation of common standards so that various decentralized identity solutions can interoperate.
Hyperledger Indy and Aries	Projects focused on developing decentralized enterprise-grade identity solutions with built-in privacy protection features, including integration of zero-knowledge proofs (ZKP).	Support standardization in enterprise environments by ensuring implementations meet scalability, security, and business process requirements.

The field of decentralized identity based on zero-knowledge proofs (ZKP) is dynamic, focused on addressing challenges and pushing the boundaries of what is possible. Let's consider several promising research directions [6]:

• Advanced ZKP schemes. Research into more efficient zero-knowledge proof systems tailored to the specific requirements of decentralized identity use cases, improving performance.

• Credential (attestation) aggregation. The ability to use ZKP to simultaneously prove compliance with multiple criteria will expand applications in complex identity-related scenarios.

• Hybrid privacy solutions. In some cases, combining ZKP with other privacy-enhancing technologies, such as secure multiparty computation, can offer the best balance between efficiency, privacy, and functionality.

• Social recovery mechanisms. Providing convenient ways for users to recover lost or compromised DIDs and related credentials in a decentralized manner is a key usability challenge.

It is also worth mentioning several leading solutions driving the development of decentralized identity based on ZKP [6, 7]:

1. zkKYC by Polygon. Polygon's solution utilizes zero-knowledge proofs to verify identity while preserving privacy, simplifying registration on decentralized finance (DeFi) platforms and other services. Built on Polygon ID, a decentralized identity platform, zkKYC enables users to prove compliance with specific criteria (e.g., being over 18 years old or residency) without revealing the exact values of those attributes.

From a technical standpoint, Polygon ID is based on the Iden3 protocol and the Circom language for constructing zk-proofs. This stack is used to create so-called zkSNARKs (Succinct Non-interactive Arguments of Knowledge) – concise cryptographic proofs that can be verified without revealing the underlying information on which they are based.

The system supports:

• Self-Sovereign Identity (SSI) – a model where identity belongs directly to the user without reliance on centralized providers.

• Selective disclosure – the ability to provide only the portion of information necessary for a specific verification.

• On-chain verification – verification performed by a smart contract directly on the blockchain, enabled by a specialized proof query language (ZK Query Language).

This solution is actively used in the context of decentralized finance (DeFi), where it is important to combine service accessibility with compliance to AML/KYC requirements (anti-fraud mechanisms). zkKYC also enables the creation of trust systems in which individuals retain full control over their credentials.

zkKYC is an example of an effective implementation of privacy, scalability, and regulatory compliance principles through the use of advanced cryptographic methods.

2. Sismo Protocol. Sismo applies ZKP to reputation systems and privacy-preserving badges within Web3 communities, allowing users to prove their contributions while controlling what information they disclose.

Its architecture is based on zero-knowledge proofs, enabling users to demonstrate their activity or status without revealing any link to specific identifiers (such as wallet addresses or social media accounts).

Sismo consists of several key components:

• Data Vault – a local storage of attributes (identifiers) fully controlled by the user. Attributes may include data from Ethereum, Twitter (X), or GitHub, for example.

• ZK Badges – unique cryptographic badges that act as soulbound tokens (tokens that cannot be transferred to others). They certify membership in a particular group or achievement without revealing the source of these achievements.

• Sismo Connect – an interface (SDK/API) that allows web applications to receive ZK proofs from users to grant access or verify certain conditions.

Unlike classical authentication systems where a user provides a login or password, Sismo allows confirming statements like "I am a member of DAO X" or "I have more than 1 ETH in my wallet" without revealing who you actually are.

This approach opens possibilities for:

• Confidential voting within DAOs;

• Reputation systems for participation in airdrops;

• Anonymous access to Web3 services based on attributes or achievements.

Sismo plays a crucial role in the development of Web3 identities by simultaneously providing privacy, verifiability, and flexibility for integration with existing decentralized services.

3. Self-Sovereign Identity (SSI) by Evernym. A comprehensive decentralized identity platform that uses standards and is oriented towards interoperability, supporting zero-knowledge proofs (ZKP) for selective disclosure of attributes.

In this model, users receive, store, and manage their verifiable credentials independently of centralized authorities.

Technological foundation of the platform:

• Hyperledger Indy – a specialized blockchain for identity, supporting decentralized registries of DIDs (Decentralized Identifiers).

• Hyperledger Aries – a set of protocols and tools for agents (software interfaces) that exchange credentials between users, organizations, and services.

• Verifiable Credentials – standardized W3C documents that can be issued, verified, and revoked.

The platform supports zero-knowledge proofs, enabling users to selectively disclose only parts of credential attributes.

Key features of Evernym:

• User control over data – all credentials are stored in a local "agent" (an app or module) that shares data only with the owner's permission.

• High integration capability – supports enterprise needs such as revocation, auditing, and credential lifecycle management.

• Participation in global standardization – Evernym has played a key role in developing W3C specifications and the Decentralized Identity Foundation.

Conclusions

The combination of Decentralized Identity (DID) and Zero-Knowledge Proofs (ZKP) represents a radical step toward a safer, more private, and user-centric internet. Such a system enables individuals to control their own data, interact in the digital space without relying on centralized intermediaries, and prove facts (e.g., age or education) without revealing unnecessary information.

Although the technology is rapidly evolving, it faces several challenges: usability complexity for ordinary users, the risk of key loss, a limited number of trusted credential issuers, and the need for interoperability at a global level. Additionally, legal recognition of digital credentials across different jurisdictions remains an open issue.

Decentralized identity based on ZKP is key to secure, private, and scalable digital interactions. It addresses fundamental problems of centralized systems such as data breaches, redundant verifications, and limited user autonomy. The combination of DID and ZKP forms a new paradigm of digital identity management focused on security, privacy, and user autonomy. DID ensures the storage and control of credentials in a personal environment, while ZKP allows attribute verification without revealing the underlying data. Despite existing technical, regulatory, and user adoption barriers, the intensive development of standards, infrastructure, and governmental initiatives indicates a transition of this model from conceptual stages to practical implementation. In the future, it has the potential to become the foundation of a secure, interoperable, and sovereign digital identity on a global scale.

Further research and development in this field will contribute to improving existing mechanisms, increasing their accessibility, and adapting them to diverse application scenarios – from the financial sector to government services and everyday digital interactions.

References:

1. Camenisch J., Drijvers M., Lehmann A. Anonymous attestation using the strong Diffie-Hellman assumption revisited. Trust and Trustworthy Computing: 9th International Conference, TRUST 2016, Vienna, 29–30 August 2016. 2016. P. 1–20.

2. Reed D., Preukschat A. Self-Sovereign Identity. 2nd ed. Shelter Island, NY : Manning, 2021. 374 p.

3. Decentralized Identifiers (DIDs) v1.0: core architecture, data model, and representations. World Wide Web Consortium (W3C). [Electronic resource]. Available at: https://www.w3.org/TR/did-1.0/.

4. A Survey on Decentralized Identifiers and Verifiable Credentials / C. Mazzocca et al. IEEE Communications Surveys & Tutorials. 2025. P. 7.

5. A Survey on the Applications of Zero-Knowledge Proofs / R. Lavin et al. arXiv preprint arXiv:2408.00243. 2024. [Electronic resource]. Available at: https://arxiv.org/abs/2408.00243.

6. Fischlin S. Formalising Zero-Knowledge Proofs in the Symbolic Model : master's thesis. Zurich, 2021. 76 p.

7. Decentralized Identity: The Ultimate Guide. dock labs. [Electronic resource]. Available at: https://www.dock.io/post/decentralized-identity.

Received 15.03.2025

Information about the authors:

Koziuberda Dmytro Olexandrovych – Cybersecurity Master, Faculty of Computer Sciences, V.N. Karazin Kharkiv National University; development employee of LLC “LADYZAIN”, Ukraine; e-mail: koziuberda.dmytro@gmail.com; ORCID: https://orcid.org/0009-0005-3088-9685

Yesina Maryna Vitaliivna – cand. techn. sciences, associate professor, acting duties of the head of the Department of Cybersecurity of Information Systems, Networks and Technologies in V.N. Karazin Kharkiv National University; Researcher and Head of the international department in JSC "IIT", Ukraine, e-mail: m.v.yesina@karazin.ua; ORCID: https://orcid.org/0000-0002-1252-7606

Golikov Yurii Leonidovych – CEO and Founder of DevBrother tech company, USA, e-mail: yuriy@devbrother.com, ORCID: https://orcid.org/0009-0008-7946-4663