Journal of Information Security and Applications 80 (2024) 103678

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities

Lu Zhou [a], Abebe Diro [a,*], Akanksha Saini [a], Shahriar Kaisar [a], Pham Cong Hiep [b]

[a] Department of Information Systems, RMIT University, 124 La Trobe Street, Melbourne, 3000, Victoria, Australia
[b] The Business School, RMIT University Vietnam, 702 Nguyen Van Linh, 700000, Ho Chi Minh City, Viet Nam

ARTICLE INFO

Keywords:
AIndex terms-blockchain
Identity sharing
Privacy
User identity
Zero-knowledge proof

ABSTRACT

Identity sharing systems, regardless of their architectural models, share common vulnerabilities. These systems compel users to divulge personal information and furnish proof of identity for accessing services, leaving them susceptible to data breaches that can culminate in identity theft and jeopardize online data security. While blockchain technology offers a potential remedy, delivering enhanced security, immutability, and traceability, it simultaneously raises pertinent concerns surrounding privacy and transparency. The integration of zero-knowledge proof (ZKP) technology has emerged as a promising solution, particularly in enhancing privacy within the transparent blockchain ecosystem. Our paper conducts an exhaustive survey of the existing literature, with a particular focus on the assimilation of ZKP technology into blockchain for the secure sharing of user identities. We undertake a critical evaluation of the advancements achieved in this domain, pinpoint the formidable challenges that must be confronted, and uncover nascent opportunities for further exploration. Our contribution transcends the realms of mere summarization and analysis; we go a step further by offering recommendations drawn from real-world case studies and delineating future research directions.

1. Introduction

1.1. Background and motivation

In the increasingly interconnected and digital world of today, identity sharing has transcended its role as a mere procedural step and become integral to the fabric of our modern, interconnected world. The proliferation of online services, from financial transactions to healthcare consultations, underscores the centrality of identity verification in ensuring secure access and privacy protection. The fundamental concept of identity sharing extends beyond individuals to encompass a diverse spectrum of entities, including devices, systems, and organizations. It entails the selective disclosure of specific attributes or credentials that serve as confirmatory evidence of an entity's identity. This multifaceted process, applied to individuals, devices, and institutions alike, is a linchpin in a variety of online interactions. For instance, individuals must reliably confirm their identity to access and manage bank accounts, conduct e-commerce transactions, or interact with governmental services. In a world dominated by digital services, ensuring the integrity of these interactions and safeguarding sensitive personal data against fraudulent access and misuse is paramount. Devices and systems, including smartphones, IoT devices, and cloud services, are required to verify their identities to establish secure connections and engage in collaborative operations within an intricate web of interconnected nodes. Similarly, organizations often need to assert their identity credentials to access digital platforms, engage in business-to-business interactions, and participate in digital ecosystems such as supply chains and consortiums. This collective reliance on identity sharing underscores its pivotal role in maintaining the trust, security, and privacy that underpin the digital age [1].

Despite the undeniable importance of identity sharing, this practice is not without its challenges. Traditional identity management systems, particularly those reliant on centralized authorities or intermediaries, have exhibited noteworthy drawbacks. They often compel users to divulge a plethora of personal information and identity proofs to multiple service providers, thereby increasing the risk of data breaches and identity theft. The centralized architecture of these systems concentrates sensitive data in a limited number of nodes, rendering them

* Corresponding author.
E-mail address: abebe.diro3@rmit.edu.au (A. Diro).

https://doi.org/10.1016/j.jisa.2023.103678

Available online 3 January 2024

attractive targets for malicious actors. The ramifications of a successful breach can be severe, encompassing unauthorized access, fraudulent activities, and financial loss for individuals. For organizations, data breaches can lead to reputational damage, legal liabilities, and operational disruptions.

1.2. Identity theft and consequences

Identity theft, a criminal act rooted in the illicit acquisition and unauthorized utilization of an entity's identifying information, poses a substantial challenge in the digital era. Perpetrators of identity theft may target various forms of identities, ranging from an individual's personal details (e.g., name, date of birth, social security number, credit card information) to a device's unique identifiers (e.g., MAC addresses, IP addresses) or an organization's proprietary credentials (e.g., digital certificates, authentication tokens). Once in the hands of malicious actors, these stolen identities can be wielded as potent tools for a diverse array of fraudulent activities. Individuals who fall victim to identity theft may witness unauthorized access to their financial accounts, fraudulent applications for loans or credit cards, falsified tax returns, or even criminal acts committed under their name. For organizations, the consequences of identity theft can be far-reaching, including financial losses, disclosure of sensitive data, and the erosion of reputation and trust [2].

There have been numerous recent instances of data breaches have produced far-reaching consequences by involving unauthorized sharing of identity information. Among these incidents, the SolarWinds data breach stands out as one of the most extensive and intricate cyber-attacks in history. In December 2020, it came to light that Russian hackers had infiltrated SolarWinds, a software provider widely used by government agencies and Fortune 500 companies [3]. The attackers introduced malicious code into SolarWinds' software updates, enabling them to gain access to the systems of the company's clients. The breach had repercussions for thousands of organizations, exposing sensitive data such as email. In March 2021, Microsoft revealed that hackers had exploited vulnerabilities in its Exchange Server email software, which allowed unauthorized access to the email accounts of entities across the globe. This breach affected an estimated 250,000 organizations, leading to the exposure of personal information like email addresses, phone numbers, and other sensitive data [4]. Subsequently, in August 2021, T-Mobile reported a breach where hackers managed to breach its servers, compromising the personal data of more than 50 million customers. Stolen information encompassed names, addresses, birthdates, and social security numbers, inciting concerns over the potential for identity theft and fraudulent activities [5]. Air India also disclosed a breach in May 2021, affecting approximately 4.5 million customers. This breach involved unauthorized access to personal data, comprising names, birthdates, contact details, passport information, and credit card particulars. The incident raised apprehensions about the security of passenger data within the airline industry and the potential repercussions linked to identity theft and fraud [6]. Australia has experienced its share of notable data breaches in recent times that involved unauthorized sharing of personal information, impacting millions of individuals and underscoring vulnerabilities within organizational data security practices. In 2022, Medibank, one of Australia's largest health insurance providers, faced a data breach involving unauthorized access to health claims of 160,000 customers. This incident emphasized the fragility of healthcare data and the potential consequences for individual privacy and healthcare-related fraud. Often, data breaches of this nature lead to instances of identity theft, as the stolen data may be sold on the dark web or made public by hackers.

The scale and impact of identity theft underscore the urgency of devising robust, privacy-focused, and secure identity management solutions that can effectively mitigate these risks. While centralized identity management systems have traditionally been employed to address these needs, their limitations have become increasingly evident. Users often find themselves compelled to relinquish control over their sensitive personal information, with limited insight into how this data is stored, accessed, and shared by centralized authorities. This centralized architecture is not only susceptible to data breaches but also raises concerns related to trust and reliability [7]. To address these challenges and enhance identity security, blockchain technology has emerged as a promising solution. Blockchains offer a decentralized, tamper-resistant ledger that can potentially revolutionize identity management. By providing enhanced security, immutability, and traceability, blockchains offer a robust foundation for building secure identity sharing systems. However, the integration of blockchain technology introduces its own set of challenges, particularly in the realms of privacy and transparency [1].

In response to these challenges, the incorporation of zero-knowledge proof (ZKP) technology has gained prominence. ZKPs empower users and organizations to assert their identities without disclosing sensitive information, thereby preserving privacy while ensuring the accuracy of transactions. This paper embarks on a comprehensive survey of the existing literature to explore how ZKP technology has been integrated into blockchain for secure identity sharing. Through this survey, we critically assess the advancements, identify persistent challenges, and unveil novel opportunities in this dynamic domain. By synthesizing and analyzing the collective wisdom of the research community, we aim to contribute to a deeper understanding of harnessing blockchain and ZKPs for robust identity sharing solutions that can address the shortcomings of centralized and traditional models. This survey extends beyond a mere cataloging of existing approaches, offering valuable insights and recommendations based on case studies and emerging trends. By outlining specific future research directions, we endeavor to equip readers with the knowledge and guidance needed to navigate the evolving landscape of blockchain-based identity sharing [8].

2. Existing works and our contributions

In this section, we discuss related works in the field of zero-knowledge proofs for identity sharing on blockchain, focusing on studies that have contributed to our understanding of this topic.

2.1. Previous surveys

The study in [9] predominantly explores general zero-knowledge proofs within blockchain technology but notably lacks discussions on identity management. Conversely, other studies such as [10] and [11] center their focus on blockchain-enabled identity sharing; however, they fall short in addressing the utilization of zero-knowledge proofs specifically for managing identities. While these studies provide valuable insights into blockchain-based identity sharing mechanisms, they do not delve into the application or integration of zero-knowledge proofs for enhancing identity management within blockchain systems. There exists a noticeable gap in research where the intersection of blockchain-enabled identity sharing and the incorporation of zero-knowledge proofs for more secure and private identity management remains unexplored. Further research addressing this gap could offer innovative approaches for leveraging zero-knowledge proofs to enhance the security and privacy of identity management systems within blockchain technology.

2.2. Our contributions

Our survey distinguishes itself by narrowing its focus to zero-knowledge proofs for identity sharing on blockchain, specifically adopting ZK-STARKs. We conduct a more in-depth analysis, tailor our approach to identity sharing, include case studies, offer targeted recommendations, and outline specific future research directions. These aspects collectively contribute to the survey's novelty in the landscape of related studies.

Table 1
Comparison of studies.

Attributes	[8]	[10]	[11]	Our paper
Scope of study	Focus on ZK-SNARKS	Blockchain-based identity but missing ZKP	Identity management in blockchain	Targets ZK-STARKS
Depth of analysis	Broad overview	Moderate analysis	In-depth analysis	Delves deeper analysis
Technological approaches	Traditional blockchain	Traditional self-sovereign identity	Blockchain-based identity	Tailored for identity sharing
Case studies	No	No	Case studies included	Yes
Recommendations	Offer broad recommendations	No recommendations	Recommendations provided	Provide targeted recommendations
Future directions	Discuss general future trends	No future directions	Future research directions discussed	Outline specific future research directions

As far as we are aware, there has not been a recent exploration specifically on zero-knowledge proofs on blockchain for identity sharing, with the exception of Sun et al. [8]. Nonetheless, there are notable limitations and gaps in their survey, which underscore the need for this comprehensive review. Our survey provides the following benefits when compared to [8]. Table 7 also summarizes the contributions of our paper when compared to state-of-the-art research.

Scope: The paper by [9] offers a broad perspective on generic Zero-Knowledge Proofs (ZKP) in the blockchain. In contrast, [8] narrows its focus specifically on ZK-SNARKs. Our study, however, shifts its attention towards ZK-STARKs, providing a unique angle in the realm of zero-knowledge proofs.

Depth of Analysis: While [9] presents a comprehensive analysis of the topic, [8] provides a more general overview. Our paper, on the other hand, delves deeper, offering a more thorough analysis of the subject matter using specific challenges, limitations, and recommendations for implementing ZKPs in blockchain-based identity sharing. The current survey aims to address this gap by offering a detailed examination of the challenges, providing insights into potential solutions, and presenting recommendations for addressing identified issues.

Exploration of zk-STARKs: The technological approach of [9] emphasizes generic blockchain applications and their integration with zero-knowledge proofs. [8] leans towards traditional blockchain methodologies. Our paper, however, is tailored specifically for identity sharing on the blockchain, marking a distinct approach from the other two. The current survey introduces the novel concept of zk-STARKs and their potential role in privacy-preserving identity sharing. By incorporating this emerging ZKP solution, the survey extends the analysis to include cutting-edge technologies that were not covered in the previous survey.

Case Studies: Interestingly, both [8,9] do not incorporate case studies into their research. This is where our paper stands out, as we provide real-world case studies to further elucidate our findings and arguments.

Recommendations: [9] offers guidance to its readers, while [8] sticks to more broad-based recommendations. Our paper, in contrast, provides targeted recommendations, ensuring that readers receive specific and actionable insights.

Future Directions: The future of zero-knowledge schemes is the primary focus of [9]. [8] discusses general future trends in the domain. Our paper, however, outlines specific future research directions, offering a clear path for subsequent studies and developments in the field.

Building upon the analysis, the survey offers specific recommendations for addressing challenges related to implementing ZKPs in identity sharing systems. These recommendations provide actionable insights that can guide the design and development of more secure and privacy-preserving systems. The survey also identifies potential research directions and areas for further exploration in the field of blockchain-based identity sharing using ZKPs. By highlighting these opportunities, the survey encourages researchers to focus on untapped areas and contribute to the advancement of the domain (see Table 1).

2.3. Organization of the survey

The remainder of the paper is organized as follows. Section 3 explores different identity sharing strategies. Section 4 highlights how blockchain technology can be effectively used in identity sharing. Section 6 presents ZKP and blockchain-based identity-sharing techniques while different case studies for ZKP-based identity sharing techniques are studied in Section 7. Finally, recommendations and challenges in this research area are explored in Section 8 and Section 9 concludes the paper.

3. Identity sharing systems: An overview

In contemporary digital ecosystems, identity management systems come in various architectural models, including centralized, federated, and self-sovereign identity management. Each of these models presents unique characteristics and challenges, reflecting different approaches to handling user identities and personal information. Table 2 compares these major architectures of identity management.

3.1. Centralized identity management

Centralized identity management represents a widely adopted model that relies on intermediaries, often trusted third parties, to oversee identity verification and data management processes. In this model (as illustrated in Fig. 1), users are obliged to disclose their personal and financial information to these intermediaries as a prerequisite for accessing various services. Despite the implementation of security measures, centralized architectures remain vulnerable to a multitude of security risks and privacy breaches, which are well-documented in the literature [12].

One of the primary drawbacks of centralized identity management is the concentration of user data within a limited number of nodes or centralized repositories. This concentration makes these systems enticing targets for malicious actors, who can exploit vulnerabilities for nefarious purposes. For instance, centralized architectures are susceptible to cyberattacks such as Denial-of-Service (DoS) attacks and malware intrusions [12]. These attacks can disrupt services, compromise user data, and even lead to a single point of failure where a breach in one central node can have catastrophic consequences. Furthermore, users often possess limited control over their identification data within centralized systems. They may not have visibility into the mechanisms governing how the central authority manages, shares, or secures their sensitive information. This lack of transparency and user agency can exacerbate concerns related to data privacy and user control. These inherent limitations in centralized identity management underscore the need for innovative approaches to address security and privacy concerns, particularly as digital interactions become increasingly integral to our lives.

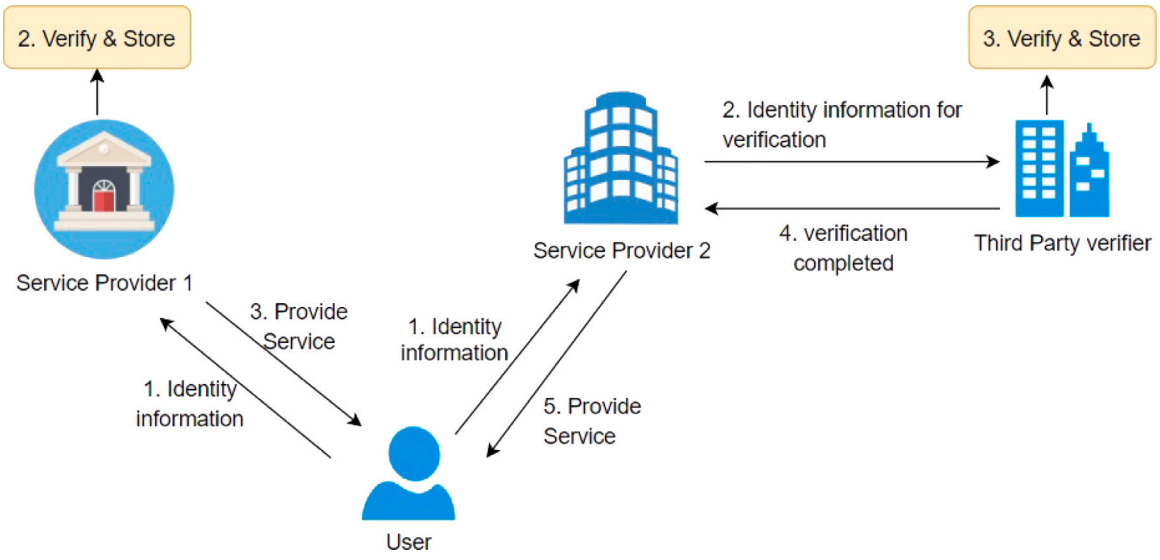

Fig. 1. Centralized identity sharing architecture.

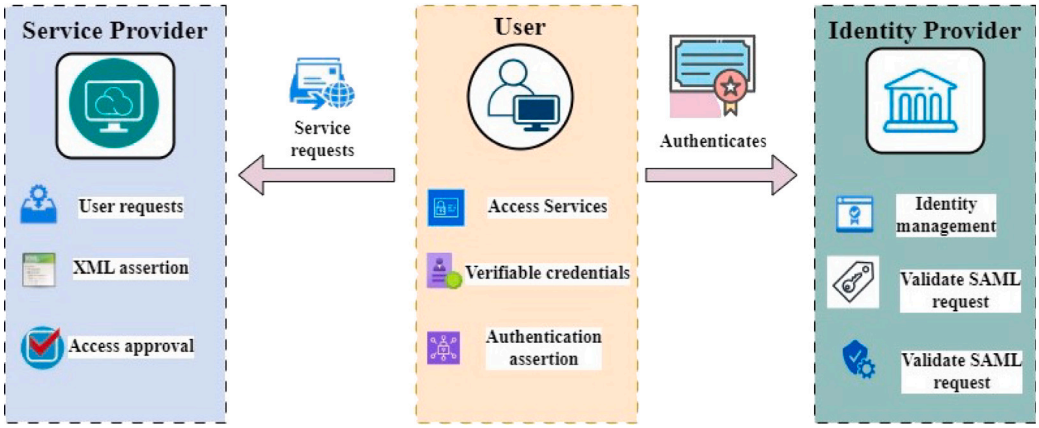

Fig. 2. Federated identity management.

3.2. Federated identity management

Federated identity management represents a departure from the centralized identity model by distributing control and responsibilities across multiple entities within a networked ecosystem [13]. These entities can encompass a diverse range of participants, such as service providers, identity providers, or trusted third parties as depicted in Fig. 2. Despite their diverse roles, they collaborate within the federated framework while retaining a degree of autonomy.

One of the primary advantages of federated identity systems lies in their capacity to enhance user privacy. By distributing responsibilities and reducing the concentration of sensitive data, federated systems mitigate the risks associated with centralization [14]. This decentralization also contributes to a reduced centralization risk, making the system less susceptible to single points of failure and potential data breaches. Scalability is another key benefit of federated identity management. As the network expands to include various entities, it can accommodate an increasing number of users and services seamlessly. This scalability ensures that federated systems can effectively adapt to the dynamic demands of a growing user base. Moreover, federated systems offer a high degree of flexibility to both users and service providers. Users have the liberty to select from a variety of identity providers and service providers, aligning their choices with their preferences and requirements. This flexibility fosters a user-centric approach to identity management, empowering individuals to tailor their digital interactions.

However, the federated identity model is not without its challenges. The foremost among these is interoperability, which presents a significant hurdle. Since federated systems involve multiple entities with varying protocols and data formats, users often find themselves repetitively providing identification details to different entities for validation and access to services [15]. This issue arises due to the lack of standardized protocols and a common framework across platforms. To address the interoperability challenge, comprehensive agreements and trust relationship management are essential. Establishing standardized protocols and clear rules of engagement among participating entities become critical tasks. These agreements aim to ensure seamless interactions and data sharing across the federated ecosystem, maintaining the security and privacy of user identities. Hence, federated identity management offers distinct advantages, including enhanced privacy, reduced centralization risk, scalability, and flexibility. Nevertheless, it introduces challenges related to interoperability that necessitate the development of standardized protocols and robust trust relationships among participating entities in the federated ecosystem.

3.3. Self-sovereign identity (SSI)

Self-sovereign identity (SSI) represents a transformative paradigm shift in digital identity management, offering users unprecedented

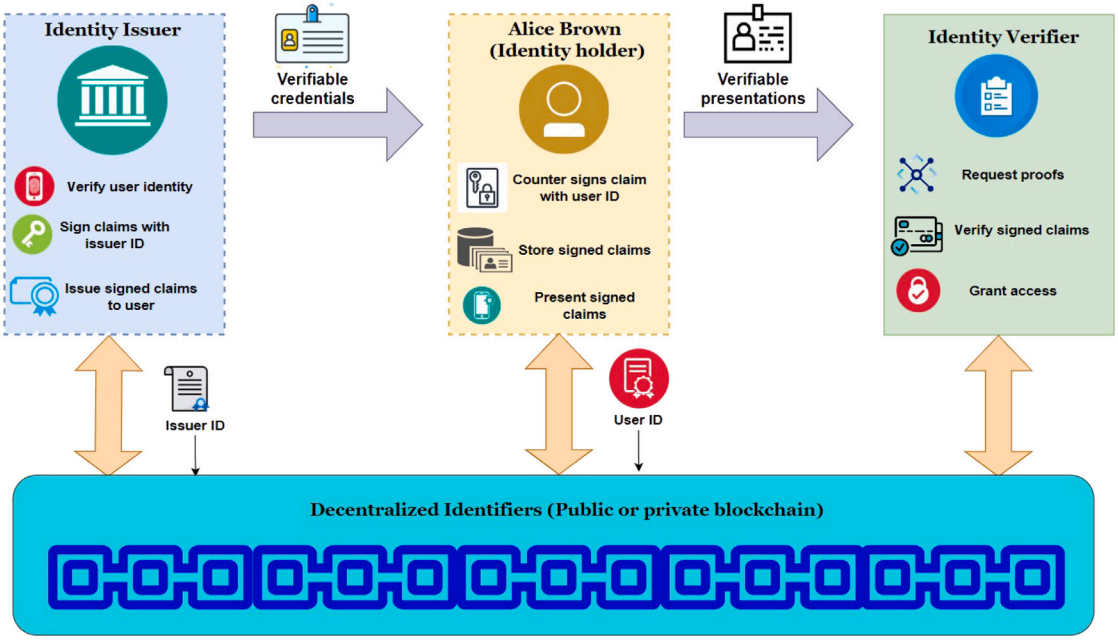

Fig. 3. Self-sovereign identity sharing architecture.

control and privacy over their online personas. At its core, as shown in Fig. 3, SSI aligns with the principles of user empowerment and data privacy, emancipating individuals from reliance on intermediaries or central authorities in asserting and managing their identities. This empowerment extends to the way users share their identity attributes, allowing them to disclose personal information selectively, sharing only what is necessary in a given context. These foundational principles collectively enhance both the security and privacy aspects of digital identity.

SSI's emergence has been catalyzed by the growing awareness of the limitations and vulnerabilities of traditional identity management systems. In an era characterized by ever-expanding digital interactions, the need for robust, secure, and privacy-focused identity management solutions has surged. Centralized identity systems, once the dominant model, have revealed their susceptibilities through data breaches and incidents of unauthorized access. These critical vulnerabilities have underscored the urgency of exploring innovative approaches to safeguarding personal information and preserving user identities. One notable catalyst for the evolution of digital identity management is blockchain technology. Recognized for its inherent traits of decentralization and tamper-resistance, blockchain holds significant promise in redefining conventional identity systems. By utilizing blockchain as an underlying infrastructure, identity management can leverage the technology's core principles of transparency, immutability, and cryptographic security.

In this evolving landscape of identity management, Zero Knowledge Proofs (ZKPs) have risen to prominence as advanced cryptographic tools. ZKPs have the potential to revolutionize identity sharing within the blockchain context, presenting solutions to multifaceted challenges. These cutting-edge technologies enable the verification of information without the need to expose sensitive data, ensuring the accuracy of transactions while preserving user privacy. The combination of SSI principles, blockchain technology, and ZKPs form a powerful alliance poised to address the contemporary complexities of identity sharing. This alignment offers users unparalleled control, security, and privacy over their digital identities, presenting a transformative path forward for the future of identity management in an increasingly digitized world.

Table 2
Identity model attributes.

Attribute	Centralized identity	Federated identity	Self-sovereign identity	Blockchain-based identity
Identifier generation	No	No	Yes	Yes
Credentials ownership	No	No	Yes	Yes
Optional disclosure	No	No	Yes	Yes
Support pseudonyms	No	No	Yes	Yes
Central storage	Yes	No	No	No
Multiple access	No	Yes	Yes	Yes
Trust and	No	No	No	Yes
Identity verification	No	No	No	No

4. Blockchain-based identity sharing

4.1. Blockchain technology

The evolution of blockchain technology has unfolded across distinct generations, each marked by advancements and innovations that have expanded its capabilities and applications. The initial generation centered around cryptocurrency and financial use cases, exemplified by the advent of Bitcoin [16]. This debut showcased a decentralized, tamper-resistant ledger tailored for transaction records. Transitioning to the second generation, the introduction of smart contracts brought forth a paradigm shift [17]. These contracts enabled automated execution of agreements, eliminating intermediaries. Ethereum emerged as a prominent second-generation blockchain platform [18]. The third generation's focal point was addressing scalability and interoperability challenges plaguing prior platforms [19]. Platforms like EOS [20] and Cardano [21] aimed for faster transactions and improved cross-chain compatibility. As the fourth generation unfolds, emerging features include quantum-resistant cryptography and heightened privacy safeguards [22], rectifying previous limitations and ushering in more potent decentralized applications.

Structure: At its core, a blockchain operates as a decentralized, distributed ledger, secure and tamper-resistant through a fusion of cryptographic hashing, consensus mechanisms, and decentralization [23]. This amalgamation assures resilience against tampering and hacking. Once data is recorded, it becomes resistant to alteration or deletion. This transparent and decentralized framework serves as an ideal

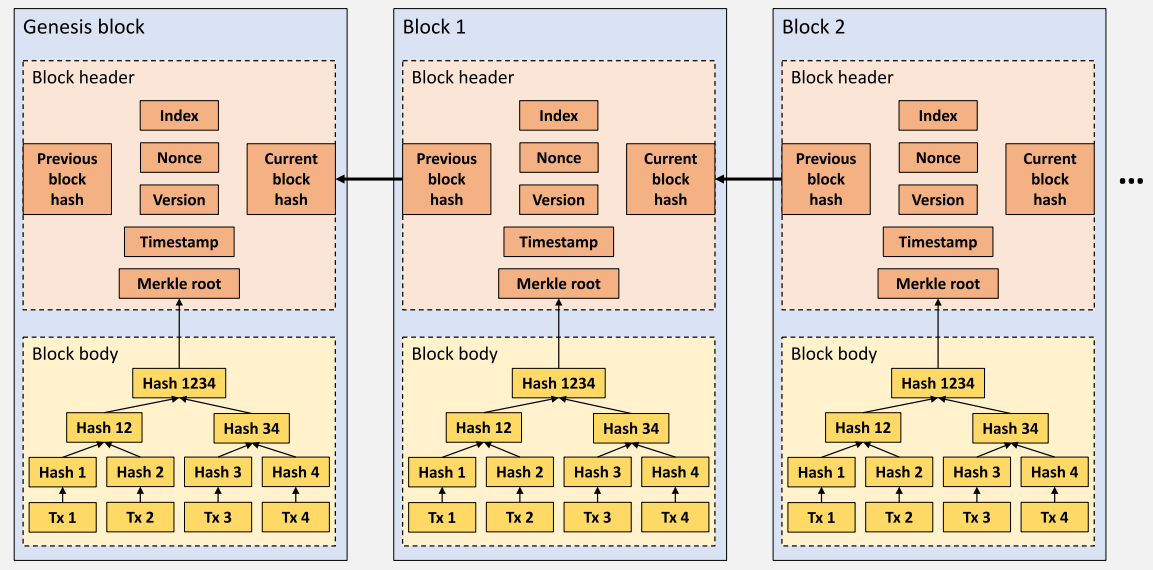

Fig. 4. A typical structure of a blockchain.

platform for sharing and recording data and transactions. A typical blockchain comprises three key components: blocks, consensus mechanisms, and smart contracts.

Block: Blocks interlink, forming an immutable ledger within a blockchain. Transactions are pivotal in this construct, as they form the basis of each block. A unique cryptographic hash identifies each block, serving as its signature of authenticity [24]. A block consists of two main parts: the block header and the block body. The header offers metadata like index, version, hash of the previous block, hash of the current block, timestamp, Nonce, and Merkle root. The body encompasses an ordered list of transactions, arranged using a Merkle tree for efficient verification of integrity and existence. Fig. 4 illustrates a typical block structure, with fields such as:

- **Index:** Denoting the block's position within the blockchain hierarchy.
- **Timestamp:** Sequencing block creation.
- **Version number:** Reflecting protocol versions.
- **Merkle root:** Ensuring transaction integrity.
- **Nonce:** Facilitating unique hash creation.
- **Hash of the current block:** Uniquely identifying the block.
- **Hash of the previous block:** Linking to the preceding block.

Consensus Algorithms: Blockchain's decentralized nature dispenses with central authority, relying on distributed nodes for validation and recording. Consensus mechanisms ensure secure and tamper-resistant operation. Four main algorithms prevail: Proof of Work (PoW) [25], Proof of Stake (PoS) [26], Practical Byzantine Fault Tolerance (PBFT) [27], and Delegated Proof of Stake (DPoS) [28]. PoW, utilized by Bitcoin, involves nodes racing to generate a nonce for transaction validation and block addition. PoS ties validation chances to node stakes. PBFT guarantees operation amidst malicious nodes. DPoS lets nodes delegate transaction validation to elected delegates.

Smart Contracts: A pivotal blockchain component is the smart contract, an autonomous program enforcing predefined agreement terms [29]. These contracts execute automatically, void of intermediaries. They operate on the decentralized network, ensuring transparency, immutability, and contract integrity. Ethereum's Solidity, Hyperledger Fabric's Java, and others empower smart contract execution. Their autonomy, tamper resistance, and decentralization catalyze transformative shifts in industries, redefining traditional agreements.

Leveraging advanced cryptographic techniques and decentralized consensus, blockchain technology holds the potential to reshape industries. Enhancing security and privacy, integration of robust cryptographic systems like post-quantum technologies is pivotal, enabling identity sharing without divulging personal data.

4.2. Leveraging blockchain for identity sharing

Blockchain technology has emerged as a potential solution to the challenges facing traditional identity management systems [30]. Blockchain's decentralized structure, cryptographic techniques, and consensus mechanisms offer a secure and transparent framework for identity sharing. By leveraging blockchain, individuals can have greater control over their personal data and decide who can access it and for what purpose [31]. Moreover, blockchain-based identity systems can eliminate the need for intermediaries and reduce the risk of data breaches. However, blockchain is not immune from data leakages that may lead to privacy violations. To further enhance privacy and security concerns, blockchain technology can be integrated with zero-knowledge proofs for identity sharing, which is a way for individuals or entities to share information about their identity without revealing their actual identity [32]. This can be particularly essential in situations where privacy is paramount, such as medical records or financial transactions.

Decentralization: Blockchain's decentralized nature obviates the need for a central authority or intermediary governing personal information, minimizing the risk of single points of failure and heightening security, reliability, and robustness [33]. The rise in data breaches [34] underscores the pitfalls of centralized storage. A blockchain-based identity-sharing system could alleviate these concerns.

Immutability: Blockchain's immutability fosters secure storage of sensitive personal information, as once recorded, data remains unchangeable. This feature mitigates the risks of identity theft and fraud, ensuring permanence and integrity [24].

Security: Employing advanced cryptographic hashing, blockchain's security thwarts alterations by linking blocks through intricate mathematical methods. The consensus algorithm makes breaching numerous nodes nearly insurmountable, establishing blockchain as a secure medium for transactions and data storage, ideal for managing and sharing personal data.

Interoperability: Blockchain-based identity sharing bridges identity providers and systems, enabling easier access and sharing of personal information across platforms and services. This contrasts with

the conventional scenario where separate entities request identical information [7,35].

Traceability: Traceability safeguards identity-related information by tracking its access and verification. This ensures adherence to intended usage and authorized parties. Blockchain's decentralized data verification and linking mechanism facilitate tracing through the flow of data and user access behaviors [7,35].

Availability: Blockchain's data availability ensures accessible and validated data for participating nodes, eliminating the need for mutual trust. Availability maintains data reliability and accessibility, vital for identity sharing, preventing individual submission to multiple entities and curbing data alteration.

Integrity: Ensuring accuracy, completeness, and consistency, blockchain guarantees data integrity through consensus algorithms, encryption, and digital signatures. These mechanisms inhibit data tampering and loss, upholding data consistency and secure exchange [7,35].

While blockchain's transparency is a fundamental feature that ensures trust and immutability, it can indeed clash with privacy requirements, especially in identity sharing contexts. Public blockchains expose transaction details to all participants, potentially revealing sensitive identity-related information. This challenge is particularly relevant when dealing with personal data that needs to be shared selectively or in a controlled manner. Striking the right balance between transparency and privacy is essential to ensure that only authorized parties have access to sensitive identity information.

Quantum computing's potential to break existing encryption algorithms is a valid concern for the security of data stored on blockchains. Many of the cryptographic methods used in current blockchain systems are based on classical computing assumptions, and the rise of quantum computers could render these methods vulnerable to attacks. This could impact the confidentiality and integrity of identity-related data stored on the blockchain. Preparing for the post-quantum era involves researching and implementing quantum-resistant cryptographic techniques to ensure that the security of blockchain systems remains intact.

These challenges emphasize the need for techniques such as zero-knowledge proofs that help mitigate the concerns while retaining the benefits of blockchain technology. ZKP offers a powerful tool for addressing privacy challenges in blockchain-based identity sharing and other contexts. They enable parties to validate information while preserving confidentiality, which is especially valuable as concerns about data privacy and security continue to grow.

5. Zero knowledge proofs in identity sharing

Zero-knowledge proof (ZKP) is a technique used in cryptography to prove the authenticity of certain information without revealing any additional details about the identity of the individual sharing that data [36]. Zero-Knowledge Proofs (ZKPs) play a crucial role in enhancing identity sharing on blockchain platforms by providing a secure and privacy-preserving mechanism. This approach is particularly useful in situations where privacy and security are paramount, such as identity management and sharing. ZKP-based identity sharing protocols leverage cryptographic systems that allow individuals to demonstrate that they possess certain information, such as a specific credential or authorization, without revealing any sensitive data that could compromise their privacy. To achieve this, ZKP-based identity-sharing protocols typically rely on post-quantum cryptographic systems, which utilize mathematical algorithms that are resistant to attacks from quantum computers. These systems ensure that the information shared during identity verification is protected against unauthorized access or manipulation. In addition to providing enhanced privacy and security, ZKP-based identity-sharing protocols have the potential to improve the efficiency and scalability of identity verification processes. By eliminating the need for intermediaries or central authorities to verify the authenticity of data, these protocols can streamline the verification process and reduce the risk of data breaches.

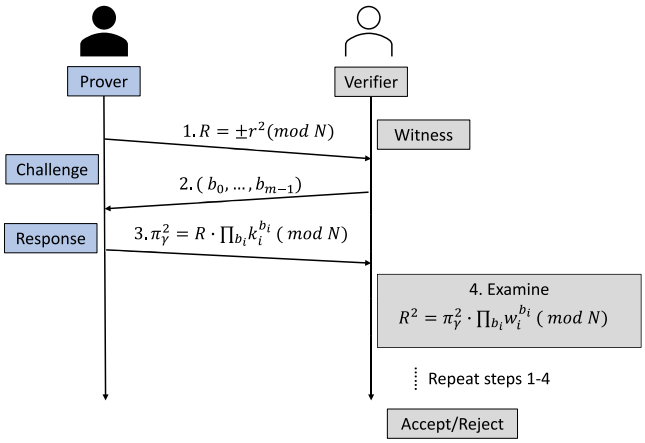

Fig. 5. The framework of the interactive ZKP.

5.1. Zero-Knowledge Proof protocols

Zero-Knowledge Proof (ZKP) protocols are cryptographic techniques that allow one party (the prover) to demonstrate the truth of a statement to another party (the verifier) without revealing additional information [37]. ZKPs play a crucial role in enhancing privacy and security in various applications, including digital identity verification within the context of blockchain. There are two main categories of ZKP technology: interactive and non-interactive [38].

Interactive ZKP (Inter-ZKP): In an interactive ZKP, the prover and the verifier engage in an iterative exchange protocol to establish the validity of the statement. During each iteration, the prover aims to convince the verifier of the statement's truth without disclosing sensitive information [37]. The interactive nature of Inter-ZKP involves challenge–response requests, leading to multiple rounds of interaction.

Non-Interactive ZKP: Non-interactive ZKPs enable the prover to authenticate information without requiring direct communication with the verifier. This type of ZKP does not involve back-and-forth interactions and is particularly relevant in scenarios where direct communication is not feasible [39].

The ZKP system involves the use of large prime numbers p and q, derived from the equation $4r+3$, where $N = pq$. Each node is assigned a set of m keys $(k_1, \ldots, k_m)$, along with corresponding multiplicative inverses $(w_i = \pm 1/k_i^2 (mod\ N))$ assigned randomly by the verifier. These inverses serve as witnesses for each node.

The Inter-ZKP algorithm's structure is illustrated in Fig. 5 and follows these steps:

(1) The prover generates a random value R as $R = \pm r^2 (mod\ N)$ and sends it to the verifier.
(2) The verifier generates a random binary string $(b_0, \ldots, b_{m-1})$ and sends it along with the corresponding keys (k_i) to the prover as a challenge.
(3) The prover computes the response $\pi_\gamma^2 = R \cdot \prod_{b_i} k_i^{b_i} (mod\ N)$ and sends it to the verifier.
(4) The verifier checks that $R^2 = \pi_\gamma^2 \cdot \prod_{b_i} w_i^{b_i} (mod\ N)$.
(5) Steps 1 to 4 are repeated for a total of n iterations $(1 \le \gamma \le n)$ to authenticate the prover.

Several non-interactive ZKP protocols have been proposed in the literature. zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) and zk-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge) are notable techniques with potential applications in blockchain, offering post-quantum capabilities.

zk-SNARKs: Zero-Knowledge Succinct Non-Interactive ARguments of Knowledge (zk-SNARKs) are a significant cryptographic technique employed in various applications, including blockchain systems [40]

Table 3
zk-SNARKs: Advantages, use cases, and challenges.

Advantages of zk-SNARKs	Use cases and applications	Challenges and considerations
Privacy: Strong privacy guarantees without revealing data.	Blockchain and cryptocurrencies: Enhancing privacy and scalability in blockchain networks.	Trusted setup: Some implementations may require a trusted setup, which could be compromised.
Efficiency: Compact proofs independent of computation size.	Privacy-preserving authentication: Identity verification without exposing personal data.	Complexity: Implementing zk-SNARKs requires cryptographic expertise and careful validation.
Non-interactivity: No back-and-forth communication for proof generation.	Secure voting: Verifiable and anonymous voting systems with private choices.	Limited use cases: Overhead may not be justified for small computations.
Post-quantum security: Resistant to quantum attacks.	Decentralized identity: Proving identity attributes without revealing excessive information.	Performance overhead: Proof generation can be computationally intensive.
Decentralization: Trustless verification in decentralized systems.		Public parameters: Ensuring integrity and security of setup parameters.

and protocols such as ZETH [41]. A distinguishing feature of zk-SNARKs is their ability to allow a prover to convince a verifier of the truth of a statement without revealing any additional information. zk-SNARKs are particularly valuable in scenarios where privacy and efficient verification are paramount.

In blockchain and cryptocurrency applications, zk-SNARKs enable users to prove the validity of transactions while maintaining privacy. One notable example is the cryptocurrency Zcash, which uses zk-SNARKs to shield transaction details such as sender, receiver, and transaction amount [42]. This confidentiality-preserving property makes zk-SNARKs attractive for various other use cases, including secure voting systems [43], decentralized identity solutions [44], and more.

The underlying mathematical concept that enables zk-SNARKs is the concept of pairings, which are bilinear maps that allow for efficient computation of certain operations. zk-SNARKs leverage elliptic curve cryptography for generating cryptographic keys and performing cryptographic operations.

The zk-SNARK process involves several key algorithms within its framework:

- Setup Algorithm (Setup(1^λ) → pp): In this phase, a set of public parameters pp is generated using a security parameter λ. These parameters constitute the common reference string (CRS) and are derived from secret parameters during a trusted setup process.
- Key Generation Algorithm (KeyGen(C) → (pk, vk)): Given a circuit C, the key generator algorithm $KeyGen$ generates a proving key pk and a verification key vk. The proving key is used by the prover to create proofs, while the verification key is utilized by the verifier to verify proofs.
- Proof Generation Algorithm (Prove(pk, x, (a) → π): With a proving key pk, a public statement x, and a private witness a as inputs, the prover executes the proof generation algorithm $Prove$ to produce a non-interactive proof π for the statement x. This proof π demonstrates the relationship established by the circuit C between the variables x and a.
- Proof Verification Algorithm (Verify(vk, x, π) → b): Using a verification key vk, a public statement x, and a zk-SNARK proof π as inputs, the verifier executes the proof verification algorithm $Verify$ to determine whether the proof is valid. If the verification succeeds, the output b is set to 1; otherwise, b is set to 0.

The zk-SNARK framework, illustrated in Fig. 6, allows for succinct and efficient zero-knowledge proofs, making it a valuable tool for enhancing privacy and security in various applications, particularly those within the blockchain ecosystem.

As shown in 3, zk-SNARKs offer a promising approach to achieving privacy and efficiency in various applications, particularly in blockchain and cryptography. Their non-interactive nature, compact proofs, and security features make them a valuable tool for addressing privacy concerns while maintaining the benefits of public verifiability. However, careful implementation, scrutiny of security assumptions, and consideration of specific use cases are essential for their successful adoption.

zk-STARKs: Scalable Transparent ARguments of Knowledge (STARKs) are a type of ZKP system that allows for efficient and secure verification of large computations. They are similar to zk-SNARKs in that they enable a party to demonstrate to another that they have performed a computation correctly, without disclosing any additional information beyond the confirmation of the correct computation. The key difference between STARKs and other types of zero-knowledge proofs is that STARKs are transparent, requiring no trusted setup or pre-processing. This makes them particularly well-suited for use in public blockchains and other decentralized systems, where trust is distributed among many participants. STARKs achieve scalability by using advanced mathematical techniques, such as polynomial evaluation and error-correcting codes, to reduce the size of the proof and improve its verifiability. They also provide strong security guarantees, as they are resistant to attacks from quantum computers and other advanced computational techniques. zk-STARKs use polynomial interpolation to generate a polynomial function that approximates the original computation. The polynomial function is generated using a set of random coefficients and evaluated at a set of points. It uses error-correcting codes to ensure that the proof is accurate even in the presence of errors or noise in the input data. zk-STARKs use a set of constraints that are defined in advance to verify the proof. The constraints ensure that the proof is accurate and that the computation was performed correctly [45].

- **Setup:**
  - Choose a security parameter k, which determines the size of the field F used for the polynomial coefficients.
  - Choose a constraint system $C = \{c_1, c_2, \ldots, c_m\}$, where each c_i is a polynomial in the input variables x and the output variables y, and represents a constraint that the computation being proven must satisfy.
  - Choose a random oracle $H(x)$ that takes an input x and produces a random output, and a fixed "randomness seed" value that is publicly known.
  - Choose a degree bound d for the polynomials used in the proof.
  - Choose a number t of trace points, which are points at which the polynomials used in the proof will be evaluated.
- **Encoding:**
  - Convert the input and output values of the computation being proven into elements of the field F using a fixed encoding scheme. This produces a vector of input values $x = (x_1, x_2, \ldots, x_n)$ and a vector of output values $y = (y_1, y_2, \ldots, y_n)$.
- **Trace:**
  - Compute a trace of t polynomials $P_1, P_2, \ldots, P_t$, where each polynomial P_i is a degree-d polynomial that satisfies the following conditions:

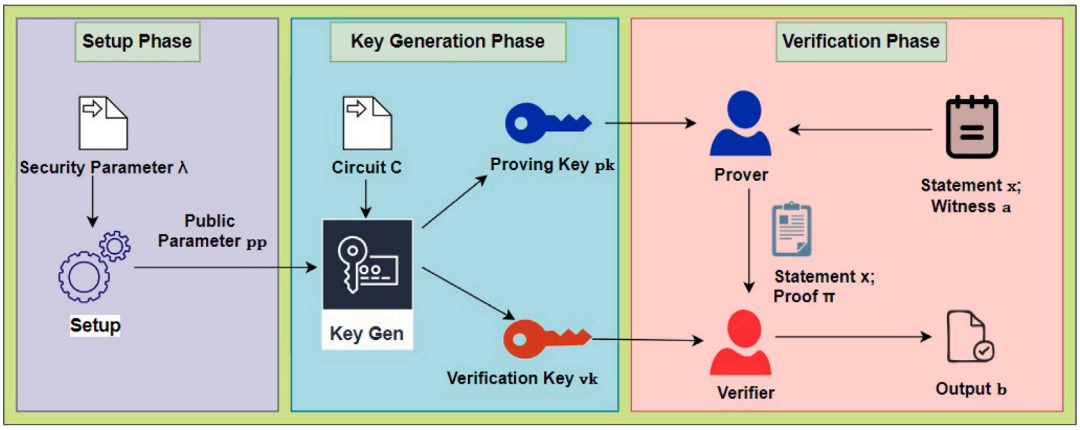

Fig. 6. The framework of the zk-SNARK.

  - $P_i(0) = 1$ for all i.
  - $P_i(j) = 0$ for all $j \neq i$.
- This can be done by starting with a base polynomial $P_0(x) = 1$ and iteratively computing the next polynomial in the trace as $P_i(x) = P_{i-1}(x) * (x - i)$.

- **Evaluation:**
  - Evaluate the polynomials in the constraint system C at each of the t trace points, producing a set of evaluations $z = (z_1, z_2, \ldots, z_m)$, where each z_i is a vector of length t representing the evaluations of the polynomial c_i at the trace points. This can be done using the Fast Fourier Transform (FFT) algorithm to efficiently evaluate the polynomials in the Fourier basis.

- **Prover:**
  - Choose a random polynomial $s(x)$ of degree less than d, and compute a polynomial $q(x) = H(x\|\text{“randomness seed”}) * s(x) - z_1[0] * P_1(x) - z_2[0] * P_2(x) - \cdots - z_m[0] * P_m(x)$.
  - Evaluate the polynomial $q(x)$ at each of the t trace points, producing a vector $r = (r_1, r_2, \ldots, r_t)$.
  - Encode the polynomial $s(x)$ and the vector r as elements of a Reed–Solomon code of length t, using a fixed encoding scheme.
  - This produces a proof polynomial $p(x)$ of degree less than $2d$ that satisfies the following conditions:
    - $p(0) = H(s(0)\|\text{“randomness seed”})$.
    - $p(i) = s(i)$ for all i in $\{1, 2, \ldots, n\}$.
    - $p(i) = r_i$ for all i in $\{n+1, n+2, \ldots, t\}$.

- **Verifier:**
  - Evaluate the polynomial $p(x)$ at each of the t trace points, producing a vector $v = (v_1, v_2, \ldots, v_t)$.
  - Decode the vector v using the Reed–Solomon code to recover the polynomial $s(x)$ and the vector r.
  - Verify that $p(0) = H(s(0)\|\text{“randomness seed”})$, and that for each constraint polynomial c_i, we have:
    - $c_i(x, y) = 0$ for all (x, y) that satisfy the constraints.
    - The vector of evaluations of c_i at the trace points z_i matches the vector of evaluations of c_i at the trace points produced by evaluating the constraint polynomial on the input and output values x and y.

- **Soundness:**
  - The soundness of the proof is based on the fact that if the computation being proven does not satisfy the constraints in C, then the prover cannot find a polynomial $s(x)$ that produces a valid proof polynomial $p(x)$.
  - The security of the proof is based on the assumption that the random oracle H is collision-resistant and that the Reed–Solomon code used for encoding the proof is error-correcting.

Table 4 provides a concise overview of the advantages, use cases, and challenges associated with zk-STARKs.

5.2. Applying Zero-Knowledge Proofs to identity sharing

Identity sharing involves the transfer of personal attributes and information while maintaining the privacy of the parties involved. Traditional methods often involve revealing extensive details, leading to potential risks such as identity theft, data breaches, and misuse of personal information. ZKPs offer an elegant solution by allowing a prover to demonstrate the validity of a statement without revealing any additional information beyond the proof's validity. This mechanism enables identity sharing without exposing the underlying attributes.

In the context of blockchain-based identity sharing, consider a scenario where a user wants to prove their age to access age-restricted content without revealing their exact birthdate. Using ZKPs, the user can generate a proof that verifies their age lies within the permissible range, without disclosing the precise birthdate. This proof can be verified by the recipient without gaining knowledge of the user's birthdate. Benefits of Using Zero-Knowledge Proofs:

- **Data Minimization**: ZKPs enable data minimization by allowing users to share only the necessary information without revealing additional details. In the identity sharing scenario, ZKPs enable the verification of a specific attribute (e.g., age) without disclosing other personal information (e.g., birthdate). This minimizes the exposure of sensitive data, reducing the risk of data breaches.
- **Non-Interactivity**: ZKPs operate in a non-interactive manner, meaning that the proof generation and verification process happens without the need for back-and-forth interactions between the prover and verifier. This is particularly advantageous in blockchain transactions, where minimizing interactions enhances efficiency and reduces transaction time.
- **Privacy Preservation**: The core advantage of ZKPs is privacy preservation. Users can prove the validity of a statement without revealing the underlying data. In the identity sharing context, this means that a user can prove their identity attributes (e.g., age, citizenship) to access services while keeping their personal information hidden from the service provider.

Table 4
zk-STARKs: Advantages, use cases, and challenges.

Advantages of zk-STARKs	Use cases and applications	Challenges and considerations
Transparency: No trusted setup is required, making them suitable for public blockchains.	Decentralized systems: Providing transparent and verifiable proofs in public blockchains.	Complexity: Implementing zk-STARKs can be more complex compared to other ZKP techniques.
Scalability: Efficiently verify large computations with short proofs.	Data auditing: Verifying the correctness of computations in cloud storage or distributed databases.	Proof size: While shorter than some alternatives, zk-STARK proofs can still be large.
Quantum resistance: Offers resistance against quantum attacks.	Supply chain tracking: Ensuring data integrity and validation in supply chain management.	Setup parameters: Ensuring security and integrity of setup parameters without trusted parties.
Verifiability: Proofs can be efficiently verified without high computational costs.	Finance and transactions: Verifying financial transactions and commitments without revealing details.	Knowledge gap: Implementing zk-STARKs requires specialized knowledge and expertise.
No trusted party: Relies on cryptographic techniques instead of trusted intermediaries.	Autonomous machines: Validating computations performed by IoT devices or autonomous systems.	Performance: Generating proofs can be computationally intensive.
Post-quantum security: Offers security against quantum computer attacks.		Public adoption: Adoption might require standards and interoperability efforts.
		Privacy considerations: Ensuring privacy for sensitive applications.

- **Trustless Verification**: ZKPs enable trustless verification, eliminating the need for parties to trust each other. The verifier can independently verify the proof's validity without relying on the prover's honesty.
- **Immutable Records**: When ZKPs are integrated into blockchain systems, the resulting records are immutable and tamper-resistant. This ensures the integrity of identity sharing transactions and prevents unauthorized modifications.

Consider Alice, who wishes to prove her eligibility for a service that requires verifying her citizenship without revealing her specific country of origin. Alice employs a ZKP to generate a proof that her citizenship falls within the permissible range of countries. The service provider verifies the proof, confirming Alice's eligibility without gaining access to her specific citizenship details. In this illustration, the benefits of ZKPs are evident. Data minimization ensures only the necessary information is shared, non-interactivity streamlines the verification process, and privacy preservation safeguards Alice's sensitive information.

Zero-Knowledge Proofs revolutionize identity sharing on blockchains by enabling users to prove attributes without exposing underlying data. This technology offers data minimization, non-interactivity, privacy preservation, trustless verification, and immutable records. These advantages collectively empower individuals to share identity attributes securely, without compromising their privacy or security. By leveraging ZKPs, blockchain-based identity sharing becomes a powerful tool for enhancing digital interactions while preserving confidentiality.

6. ZKP-enabled blockchain systems for privacy protection: State of the art

Zero-Knowledge Proof (ZKP) protocols offer a powerful solution to enhance privacy and security within blockchain systems. By allowing one party (the prover) to demonstrate the validity of a statement to another party (the verifier) without revealing additional information, ZKPs can be harnessed to protect user data and transaction details [9]. ZKP offers a significant advantage by removing the necessity of a trusted intermediary to validate transactions. This direct transaction capability between parties eliminates the need for intermediaries, leading to reduced financial costs, increased efficiency, and enhanced privacy.

A blockchain functions as a distributed database that acts as a public ledger, containing records of all processed transactions. This architecture allows individuals to access, transmit, and verify transactions [16]. While blockchain provides decentralized and immutable data storage, users maintain pseudonymity rather than complete anonymity, which raises privacy concerns [46]. To address this, cryptographic techniques like ZKP are adopted to enhance user anonymity within the blockchain.

Numerous studies in the literature have integrated zero-knowledge proof methods into blockchain technology to ensure user privacy [8, 39]. These studies can be categorized into two main domains: *transaction privacy preservation* and *user identity privacy preservation*. The former focuses on safeguarding the confidentiality of transaction attributes, such as sender and receiver addresses, transaction amount, and linkage between sender and receiver [47]. Conversely, the latter centers on protecting an individual's identity attributes, like name, date of birth, age, and their connections to their identity [48].

6.1. Transaction privacy

In transaction privacy preservation, the primary objective is to enhance the confidentiality of various transaction attributes, including sender and receiver addresses, transaction amounts, and the linkage between the transaction parties. By ensuring the anonymity of both sender and receiver addresses, the identities of the parties involved can be effectively concealed. Additionally, obscuring the transaction amount prevents external observers from deducing the precise transaction value and calculating account balances. Moreover, the obfuscation of the transaction linkage between the sender and the receiver adds an extra layer of privacy by preventing the easy inference of relationships between different transactions.

Several innovative approaches have been proposed to achieve transaction privacy preservation through the integration of zero-knowledge proof (ZKP) techniques. Notably, the Zerocoin and Zerocash protocols stand out as pioneers in enhancing privacy within distributed e-cash systems. Miers et al. introduced Zerocoin [49], utilizing zk-SNARKs to anonymize the linkage between transactions. However, this approach still disclosed transaction amounts and sender/receiver addresses. Building upon this foundation, Sasson et al. proposed Zerocash [40], which employed zk-SNARKs to extend the privacy guarantees to conceal sender and receiver addresses, along with transaction amounts.

In the pursuit of even stronger transaction privacy preservation, the BlockMaze scheme was introduced by Guan et al. [47]. Leveraging zk-SNARKs, BlockMaze aimed to safeguard account balances, transaction amounts, and the linkage within account-model blockchains. This was achieved by employing a secure commitment scheme for transaction amounts and account balances, coupled with zero-knowledge transactions between senders and receivers to obscure transaction linkages. Furthermore, the concept of a decentralized mixing scheme, as presented by Duffield et al. [50], also contributed to the preservation of transaction privacy. This approach specifically focused on concealing the linkage between transactions as well as the sender and receiver addresses.

In a different vein, Xu et al. [51] proposed a blockchain-based privacy-preserving system utilizing zk-SNARKs. This system introduced

the concept of proxy agents to conduct transactions on behalf of real users, effectively severing the connection between actual users and transactions, thus preserving user address privacy. Additionally, privacy preservation within energy trading systems was addressed by Hou et al. [52]. This study combined blockchain with a double auction scheme and employed zk-SNARKs to verify bid accuracy without revealing private data, ensuring privacy during energy trading. Innovative applications also extended to fields such as music education.

Zhang [53] introduced a novel approach that combined Inter-ZKP technology with blockchain to safeguard privacy. This framework allowed one party to convincingly demonstrate the validity of their claims to another party without divulging sensitive information, thus ensuring privacy in music education contexts. Yuan et al. [54] explored the integration of blockchain and ZKP technology to securely share credit data within a credit investigation system. Although they focused on protecting user addresses and achieving anonymous identity authentication, they did not explicitly address privacy concerns related to transaction amounts and linkages.

Similarly, in the realm of IoT access control, Song et al. [55] proposed the Blockchain and Zero-knowledge Token-Based Access Control (BZBAC) framework. By employing blockchain to store device owner identifiers and attributes securely, and utilizing ZKP to preserve the privacy of owner addresses, this framework addressed privacy challenges in IoT environments. Moreover, the application of ZKP techniques extended to the enhancement of security within power systems data transactions. Liu et al. [56] introduced a blockchain-based framework that utilized zk-SNARKs to ensure both data availability and privacy. This approach safeguarded data transactions by enabling smart contracts to access only zero-knowledge proofs rather than the original data, thereby ensuring security during transactions.

Collectively, these various initiatives within the realm of transaction privacy preservation underscore the diverse applications and potential of zero-knowledge proof techniques in enhancing privacy within blockchain systems (see Table 5).

6.2. User identity privacy preservation

In the context of user identity privacy preservation, researchers have focused on safeguarding the attributes associated with individual users while ensuring the protection of their linkages. The primary objective is to enhance user privacy by either concealing specific identity attributes or presenting them within a range of possible values. Moreover, these studies can be categorized based on their ability to selectively disclose certain user identity attributes. A comprehensive comparison of various contributions in this area is presented in Table 6, which highlights key aspects such as the protection of Identity Attributes, utilization of Attribute Ranges, capability for Selective Disclosure, and preservation of Linkages.

Ren et al. [57] proposed a novel lightweight scheme for user identity preservation. This scheme utilizes an Inter-ZKP protocol that establishes a disconnect between users' actual identities and their interactions with cloud service providers. By employing zero-knowledge proofs, this approach effectively breaks the link between users' behaviors and their real identities, thus ensuring the preservation of privacy. Addressing the challenges of medical data sharing within healthcare, Al-Aswad et al. [58] introduced a blockchain-based system. This system not only stores invoice data but also employs an Inter-ZKP scheme to protect the privacy and integrity of the data. The zero-knowledge proof technology ensures that sensitive medical information remains confidential.

In the context of COVID-19 contact tracing, Uk et al. [59] proposed a comprehensive framework that combines blockchain and zero-knowledge range proofs. This novel approach allows the concealment of user exact locations while only storing location ranges on the blockchain. This approach strikes a balance between preserving privacy and enabling efficient contact tracing. Wang et al. [7] addressed the privacy concerns within Internet of Vehicle (IoV) systems. By leveraging zk-SNARKs technology, they designed a blockchain-based framework to protect the identities of vehicles involved in data sharing. Furthermore, the introduction of a multi-sharding blockchain protocol optimized communication costs for IoV systems characterized by high mobility. Yan and Li [60] presented an innovative identity claim model within the blockchain context. This model employs zero-knowledge proofs to hash private attributes, effectively severing the link between sensitive information and user identity. This approach enables selective disclosure of attributes while preserving privacy.

Zheng et al. [61] tackled the challenge of privacy in medical data transactions, especially during insurance claims. Their proposed blockchain-based solution employs a combination of zk-SNARKs, homomorphic encryption, and the Schnorr protocol. This combination ensures both transaction privacy and patient identity protection during interactions. Rasheed et al. [62] introduced an Inter-ZKP system tailored for Internet of Things (IoT) networks. This system aims to enhance data traceability, authentication tracking, and validation. By computing and storing IoT raw data on the blockchain, the system uses zero-knowledge proof-based identification to trace and authenticate data. Bai et al. [38] devised a user identity authentication system specifically for healthcare applications. To address identity privacy during authentication, they harnessed zk-SNARKs technology. This approach ensured the concealment of registration and attribute information, maintaining privacy throughout the authentication process. Namazi et al. [63] introduced the zkFaith protocol, designed to safeguard individual identity attributes while ensuring secure authentication. The protocol combines the validation of personal documents with the generation of zero-knowledge-based identifiers, enabling privacy-preserving authentication.

Tomaz et al. [64] proposed a privacy-preserving authentication scheme for mobile health systems. To overcome challenges related to data storage, management, and sharing their blockchain framework employed attribute-based encryption. The scheme also incorporated zk-SNARKs for secure communication, enhancing overall privacy protection during interactions. Pop et al. [65] tackled privacy concerns in consumer energy data sharing. Their blockchain-based framework utilized zk-SNARKs to protect the privacy of energy consumption data. This approach ensured that energy data could be recorded, stored, and shared while maintaining confidentiality. Li et al. [66] addressed privacy issues within multiple blockchain-based traffic management systems. They introduced a privacy-preserving framework that protected vehicle location information as vehicles crossed blockchain boundaries. Leveraging zero-knowledge range proofs (ZKRP), this approach enabled the validation of vehicle locations without revealing precise coordinates.

Jeong et al. [67] applied blockchain to real estate contract systems, enhancing data integrity and privacy. Employing zk-SNARKs technology, they concealed transaction data, bolstering the system's reliability by safeguarding sensitive information. Song et al. [48] proposed a blockchain-based identity verification system using zk-SNARKs to protect user identities and attributes. By leveraging zk-SNARKs, they ensured that both identity attributes and identity identifiers were safeguarded, enabling secure authentication while maintaining privacy.

In recent years, the maritime transportation sector has increasingly integrated data-driven applications to enhance its operational efficiency, particularly in areas of communication and safety. A prime example of this integration is the sharing of position data between vessels within the framework of the maritime Internet of Things (IoT). Such advancements, while promising, bring forth challenges related to data accuracy and privacy, especially when deployed on a large scale. A growing body of literature, including the study presented in Gai et al. [68], underscores the potential of blockchain technology in addressing these challenges. This paper, in particular, delves into the utilization of blockchain for privacy-preserving data sharing. It introduces a novel scheme based on zero-knowledge proofs to safeguard vessel identities

Table 5
Comparison of privacy-preserving schemes for transaction.

Article	Privacy-preserving				Techniques	Contributions & limitations
	Sender address	Receiver address	Transaction amount	Linkage		
[49]	×	×	×	✓	zk-SNARKs	Transaction linkage privacy can be protected, but transaction addresses and amounts may remain vulnerable to exposure.
[40]	✓	✓	✓	✓	zk-SNARKs	Protect the privacy of transaction addresses, amount, and linkage by constructing a decentralized anonymous payment scheme using zk-SNARKs.
[47]	✓	✓	✓	✓	zk-SNARKs	Utilize zk-SNARKs to obscure transaction amount and balance; implement a two-step fund transfer process to dissociate the transaction linkage.
[50]	✓	✓	×	✓	Mix	Protect the privacy of transaction addresses and linkage by randomly mixing the order of the same denominated funds.
[54]	✓	✓	×	×	zk-SNARKs	Protect the privacy of transaction addresses, but transaction amount and linkage remain vulnerable to exposure.
[55]	✓	✓	×	×	zk-SNARKs	Protect the privacy of transaction addresses by using an encrypted access control token scheme to gain access permission in the IoT environment.
[51]	✓	✓	×	✓	zk-SNARKs	Use proxies to hide the user's information and ZKP to protect the privacy between them.
[52]	✓	–	✓	×	zk-SNARKs	Employ zk-SNARKs to obscure the quantities of energy demand and production in energy trading.
[53]	✓	–	✓	×	Other	Protect the privacy in authentication process by proposing a single and robust identification scheme in music education.
[56]	✓	–	✓	×	zk-SNARKs	Protect the privacy of power data by employing zk-SNARKs, and propose a trusted execution environment to ensure security.

In this table, "✓" represents instances where the paper has proposed methods aimed at ensuring the privacy of the given attribute; "×" is employed when the paper has not taken measures to protect the privacy of the attribute; "–" is used when there is no mention of attribute protection within the paper.

during data sharing. Additionally, it proposes a commitment-based strategy to maintain privacy concerning relationship dynamics during data trading among participants. Through rigorous security and performance assessments, the study underscores the efficacy and utility of the proposed methodologies.

The rapid growth of the Internet of Things (IoT) has spurred new business models where data owners monetize their data. However, incentivizing participation in data trading remains a challenge. While many studies have explored motivational mechanisms and profit distribution, security and privacy concerns persist. A significant risk highlighted in the literature is the potential exposure of sensitive data when providers claim rewards using their real identities. Addressing this, [69] introduces a blockchain-based, privacy-centric data sharing mechanism for IoT. It proposes an anonymous certificate-based policy to obscure data providers' identities and introduces two non-interactive zero-knowledge proofs to maintain anonymity during reward claims. The mechanism's effectiveness is validated through security analyses and performance evaluations, contributing to the IoT data sharing and privacy discourse. In essence, the study not only addresses current challenges in IoT data sharing but also paves the way for a more secure, transparent, and user-friendly IoT environment.

These studies collectively emphasize the crucial role of zero-knowledge proof techniques in preserving user identity privacy within blockchain systems. They illustrate a diverse array of applications spanning various domains, showcasing the versatility and effectiveness of these techniques in ensuring user privacy.

6.3. Potential challenges in ZKP-enabled blockchain systems for privacy protection

The integration of Zero-Knowledge Proof (ZKP) protocols into blockchain systems for enhancing privacy has yielded valuable insights and advancements. Through various studies focused on transaction and user identity privacy preservation, the following lessons and potential challenges have emerged:

Lessons Learned:

- Diverse Applications: ZKP-enabled blockchain systems have showcased their applicability across diverse domains, including finance, healthcare, IoT, and education. This versatility demonstrates the potential for these techniques to address privacy concerns in a wide range of scenarios.
- Enhanced Privacy: ZKP techniques have proven effective in enhancing both transaction privacy and user identity privacy. By concealing transaction attributes and selectively disclosing identity information, users can maintain higher levels of privacy while participating in blockchain interactions.
- Decentralization and Trustlessness: ZKP-enabled blockchain systems eliminate the need for trusted intermediaries to validate transactions or authenticate identities. This aligns with the core principles of decentralization and trustlessness in blockchain technology.
- Flexible Attribute Protection: Studies have demonstrated that ZKP techniques offer flexibility in protecting specific attributes while

Table 6
Comparison of privacy-preserving schemes for user identity.

Article	Privacy-preserving				Techniques	Contributions & limitations
	Identity attribute	Attribute range	Selectively	Linkage		
[57]	✓	–	×	✓	Inter-ZKP	Use ZKP to break the association between a user's identity and behavior.
[58]	✓	–	×	✓	Inter-ZKP	Use proxies to hide the user's information and ZKP to protect the privacy between them.
[59]	✓	✓	×	×	Inter-ZKP	Use zero-knowledge range proof to hide the user's exact location.
[7]	✓	–	×	×	zk-SNARKs	Use zk-SNARKs to protect privacy during the . authentication procedure in vehicular data sharing systems.
[60]	✓	–	✓	✓	zk-SNARKs	Use the hash of attributes to conceal users' properties, and employ zk-SNARKs to verify ownership during the authentication process.
[61]	✓	–	×	✓	zk-SNARKs	Use zk-SNARKs to protect the privacy of transactions between patients and insurance companies.
[62]	✓	–	×	✓	Inter-ZKP	Employ a ZKP identification system to enable anonymous authentication for IoT devices.
[38]	✓	–	×	✓	zk-SNARKs	Protect the user's identity privacy by using zk-SNARKs in the authentication process for healthcare systems.
[63]	✓	–	×	✓	Inter-ZKP	Verifies the integrity of the individuals' documents and issues a zk-based id for authentication.
[64]	✓	–	×	✓	zk-SANRKs	Protect the patient's privacy in the authentication process by using ZKP in the mobile health system.
[65]	✓	–	×	×	zk-SNARKs	Implement a privacy-preserving solution by using zk-SNARKs to hide the energy data and requested profiles.
[48]	✓	–	×	✓	zk-SNARKs	Use zk-SNARKs to protect the privacy of user's identities and behaviors.
[66]	✓	✓	×	×	zk-SNARKs	Utilize ZKRP to conceal the precise location information of a vehicle as it traverses the boundaries within multiple blockchain networks.
[67]	✓	×	×	×	zk-SNARKs	Protect the privacy of contract data using zk-SNARKs to improve the scalability in online real state contract system.

In this table, "✓" represents instances where the paper has proposed methods aimed at ensuring the privacy of the given attribute; "×" is employed when the paper has not taken measures to protect the privacy of the attribute; "–" is used when there is no mention of attribute protection within the paper.

allowing for selective disclosure when necessary. This flexibility strikes a balance between privacy and transparency.
- Efficient Zero-Knowledge Proofs: Advancements in zero-knowledge proof technology, such as zk-SNARKs and zk-STARKs, have led to more efficient and scalable solutions. This enables privacy enhancements without compromising system performance.

Potential Challenges:

- Scalability: As blockchain networks grow, the scalability of ZKP-enabled systems becomes crucial. Ensuring that zero-knowledge proofs do not hinder the throughput and responsiveness of the blockchain requires ongoing research and optimization.
- Usability and Adoption: Integrating ZKP technology into existing blockchain systems may pose usability challenges for end-users. Simplifying the user experience and ensuring seamless integration of privacy features are essential for widespread adoption.
- Privacy vs. Regulation: Striking a balance between privacy protection and compliance with regulatory requirements presents a challenge. While ZKP techniques can enhance privacy, they must also allow for lawful access when needed.
- Complexity: Implementing ZKP techniques can be complex and resource-intensive. Developers and users need to understand the intricacies of these cryptographic methods to ensure their correct and secure implementation.
- Trusted Setup and Auditing: Some ZKP techniques, like zk-SNARKs, require a trusted setup phase. Ensuring the integrity of this setup and conducting regular audits is critical to prevent potential vulnerabilities.
- Interoperability: Achieving interoperability between different ZKP-enabled blockchains and legacy systems can be challenging. Efforts are needed to establish standards and protocols that facilitate seamless data exchange.
- Privacy Assurance: While ZKP techniques offer enhanced privacy, ensuring their effectiveness against advanced attacks and vulnerabilities is an ongoing concern. Rigorous testing, research, and continuous improvement are necessary to maintain robust privacy protections.
- Resource Requirements: Generating and verifying zero-knowledge proofs can demand significant computational resources. Balancing privacy benefits with the resource overhead is crucial for practical implementation.

- Education and Awareness: Educating users, developers, and decision-makers about the benefits and risks of ZKP-enabled systems is essential for their successful adoption and proper usage.
- Emerging Threats: As ZKP-enabled blockchain systems become more prevalent, new attack vectors and threats may emerge. Staying vigilant and adaptive to emerging security challenges is essential to safeguard privacy.

In summary, ZKP-enabled blockchain systems have the potential to revolutionize privacy preservation. The lessons learned from past studies highlight their versatility and effectiveness, but challenges related to scalability, usability, regulation, and complexity must be addressed to fully harness their benefits. Through ongoing research, collaboration, and innovation, the blockchain community can navigate these challenges and create robust, privacy-enhancing solutions that align with the principles of decentralization and security.

7. Case studies: Adopting ZKPs for identity sharing on blockchain

7.1. ZK-SNARKs for identity sharing on blockchain

Desirable Features: Desirable characteristics of Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (ZK-SNARKs) for blockchain-based identity sharing revolve around privacy, efficiency, and security. Privacy is paramount, enabling users to verify their identity attributes on the blockchain without revealing sensitive information. The system must be computationally efficient, ensuring swift verification and proof generation, vital for real-time interactions. Additionally, succinctness, smaller proofs, and reduced storage enhance scalability and minimize transaction costs.

Security is fundamental, safeguarding the system against cryptographic attacks and ensuring data integrity. Selective disclosure empowers users to share specific attributes as needed. Non-interactivity streamlines operations, and flexibility supports various identity attributes. Post-quantum resistance future-proofs the system against quantum threats. User-friendliness promotes broad adoption.

Standardization ensures consistency and interoperability, while transparency and immutability offer auditability and data integrity. Cross-platform compatibility ensures accessibility across devices and operating systems. These characteristics collectively underpin a robust and user-friendly blockchain-based identity sharing system, respecting privacy, enhancing efficiency, and maintaining security.

Algorithm for Generating Identity Proofs (Prover):

(1) **Input**:

- User's identity-related information, denoted as $I = \{attribute_1, attribute_2, \ldots, attribute_n\}$.
- zk-SNARK parameters for blockchain, denoted as $Params$, and blockchain-specific constraints.

(2) **Proof Generation**:

(a) Construct a set of constraints, denoted as $Constraints = \{constraint_1, constraint_2, \ldots, constraint_m\}$, that represent the required attributes based on the user's input data and blockchain-specific requirements.

(b) Generate a secret key and public key pair for the zk-SNARKs within the blockchain, denoted as (sk, pk).

(c) Create a proof object specific to the blockchain, denoted as $Blockchain\_Proof\_Object$, that includes the user's input data (I), blockchain-specific constraints ($Constraints$), secret key (sk), and public key (pk).

(d) Using the zk-SNARKs proof generation algorithm adapted for blockchain, produce a succinct proof, denoted as $Blockchain\_Proof$, that attests to the validity of the identity-related information without revealing the actual values. This involves solving the zk-SNARK equation within the blockchain context:

$$Blockchain\_Proof = Prove(Params, Blockchain\_Proof\_Object)$$

where $Prove$ is the zk-SNARKs proof generation function tailored for blockchain-based identity sharing.

(e) Store the generated blockchain-specific proof ($Blockchain\_Proof$) on the blockchain, associating it with the user's blockchain address or identifier.

Algorithm for Verifying Identity Proofs (Verifier):

(1) **Input**:

- User's blockchain address or identifier, denoted as $Blockchain\_Address$.
- Identity proof retrieved from the blockchain, denoted as $Retrieved\_Blockchain\_Proof$.
- zk-SNARK verification parameters for blockchain, denoted as $Blockchain\_Verification\_Params$, and blockchain-specific constraints.

(2) **Proof Verification**:

(a) Retrieve the blockchain-specific identity proof ($Retrieved\_Blockchain\_Proof$) associated with the user's blockchain address or identifier ($Blockchain\_Address$) from the blockchain.

(b) Using the zk-SNARKs proof verification algorithm adapted for blockchain and the blockchain verification parameters ($Blockchain\_Verification\_Params$), validate the proof's authenticity by checking the zk-SNARK verification equation within the blockchain context:

$$Is\_Blockchain\_Proof\_Valid = Verify(Blockchain\_Verif\_Params, Blockchain\_Address, Retrieved\_Blockchain\_Proof)$$

where $Verify$ is the zk-SNARKs proof verification function tailored for blockchain-based identity sharing.

(c) The verification process within the blockchain context involves evaluating the blockchain-specific constraints specified in the proof and ensuring that they hold true without revealing the actual identity attributes.

(d) If $Is\_Blockchain\_Proof\_Valid$ is true, the blockchain-specific proof successfully verifies, and the verifier can trust the validity of the identity attributes within the blockchain context without gaining access to the user's sensitive information.

(3) **Privacy Preservation on the Blockchain**: - The verification process within the blockchain context only reveals whether the blockchain-specific identity proof is valid or not; it does not expose the actual identity attributes to the blockchain network.

(4) **Selective Disclosure within the Blockchain**: - If the user chooses to interact with different blockchain applications or services, they can selectively disclose specific identity attributes from I as needed within the blockchain context without revealing the entire set of information.

Let us consider a scenario where Alice wants to prove to a blockchain-based system that she is over 18 years old, holds Australian nationality, and has a Bachelor's Degree, without revealing her actual age, nationality, or degree.

Input: User's identity-related information, denoted as I:

- Age (I_{Age})

- Nationality ($I_{\text{Nationality}}$)
- Education Level ($I_{\text{Education}}$)

Proof Generation:

1. Construct a set of constraints, denoted as $Constraints$, representing the required attributes based on the user's input data and blockchain-specific requirements. In this scenario, the constraints are:

- $Constraint_{\text{Age}} = I_{\text{Age}} \geq 18$
- $Constraint_{\text{Nationality}} = \text{Hash}(I_{\text{Nationality}}) = \text{Hash}(\text{“Australia”})$
- $Constraint_{\text{Education}} = \text{Hash}(I_{\text{Education}}) = \text{Hash}(\text{“Bachelor's Degree”})$

2. Generate a secret key (sk) and a public key (pk) pair for zk-SNARKs within the blockchain context.

3. Create a proof object specific to the blockchain, denoted as $Blockchain\_Proof\_Object$, that includes:

- User's input data (I)
- Blockchain-specific constraints ($Constraints$)
- Secret key (sk)
- Public key (pk)

4. Use the zk-SNARKs proof generation algorithm adapted for blockchain to produce a succinct proof ($Blockchain\_Proof$) that attests to the validity of the identity-related information without revealing the actual values. This involves solving the zk-SNARK equation within the blockchain context:

$$Blockchain\_Proof = \text{Prove}(Params, Blockchain\_Proof\_Object)$$

where Prove is the zk-SNARKs proof generation function tailored for blockchain-based identity sharing.

5. Store the generated blockchain-specific proof ($Blockchain\_Proof$) on the blockchain, associating it with Alice's blockchain address or identifier.

Proof Verification:

1. Retrieve Alice's blockchain-specific identity proof ($Retrieved\_Blockchain\_Proof$) associated with her blockchain address.

2. Use the zk-SNARKs proof verification algorithm adapted for blockchain and the blockchain verification parameters ($Blockchain\_Verification\_Params$) to validate the proof's authenticity. Check the zk-SNARK verification equation within the blockchain context:

$$Is\_Blockchain\_Proof\_Valid = \text{Verify}(Blockchain\_Verification\_Params, Blockchain\_Address, Blockchain\_Proof)$$

where Verify is the zk-SNARKs proof verification function tailored for blockchain-based identity sharing.

3. The verification process within the blockchain context involves evaluating the blockchain-specific constraints specified in the proof and ensuring that they hold true without revealing the actual identity attributes.

4. If $Is\_Blockchain\_Proof\_Valid$ is true, the blockchain-specific proof successfully verifies, and the verifier can trust the validity of Alice's identity attributes within the blockchain context without gaining access to her sensitive information.

The verification process within the blockchain context only reveals whether Alice's blockchain-specific identity proof is valid or not; it does not expose her actual identity attributes to the blockchain network. If Alice chooses to interact with different blockchain applications or services, she can selectively disclose specific identity attributes from I as needed within the blockchain context without revealing the entire set of information.

7.2. ZK-STARKs for identity sharing on blockchain

zk-STARKs can be integrated with blockchain for identity sharing to address some of the limitations of zk-SNARKs. By leveraging zk-STARKs in blockchain-based identity systems, individuals can securely and privately share their identity information while maintaining control over their personal data. The integration of zk-STARKs provides efficiency, trustlessness, and enhanced privacy, addressing the limitations of zk-SNARKs and offering a robust framework for identity sharing on the blockchain.

Desirable Features: zk-STARKs can eliminate the need for a trusted setup, which is required in zk-SNARKs. This simplifies the implementation and deployment process, as it removes the dependence on a trusted party to generate the initial parameters. Without a trusted setup, zk-STARKs offer enhanced security guarantees and avoid potential risks associated with a compromised setup. Unlike zk-SNARKs, zk-STARKs can also provide transparency in their construction. They do not rely on a trusted setup, making them more trustless and resistant to potential vulnerabilities arising from a compromised setup. This transparency aspect is crucial for identity sharing on a public blockchain, as it ensures that the proof generation process is verifiable and immune to tampering. Furthermore, zk-STARKs offer improvements in efficiency compared to zk-SNARKs. The proof size in zk-STARKs is succinct, meaning it is significantly smaller, making it more practical for storage and transmission on a blockchain. The verification process in zk-STARKs is faster, enabling quicker validation of identity proofs, which is crucial for real-time use cases. Finally, zk-STARKs maintain the privacy features inherent in zero-knowledge proofs. They allow for the sharing of identity-related information without revealing sensitive details. Individuals can prove their identities and authenticate specific attributes without exposing unnecessary personal data, which is crucial for privacy-sensitive applications.

zk-STARKs enable privacy-preserving identity sharing on the blockchain by only revealing the necessary information. Users can selectively disclose specific attributes without exposing their complete identity. For instance, an individual can prove their age without revealing their date of birth or authenticate their educational qualifications without exposing the entire academic record. This enhances privacy protection and minimizes the risk of identity theft or unauthorized access to sensitive personal information. Integrating zk-STARKs with blockchain for identity sharing also ensures trustless and transparent operation. The proofs can be verified by any node on the blockchain, eliminating the need for reliance on a central authority or trusted intermediaries. The transparency aspect ensures that the proof generation process is verifiable, enabling participants to validate the integrity and correctness of the identity-related information without compromising security.

High-level Protocols for Identity Sharing: zk-STARKS can be leveraged for identity sharing on blockchain. The actual verification process involves more detailed calculations and operations, including polynomial evaluations, interpolations, and comparisons. In practical implementations, the specific choice of trace points, polynomial representations, and cryptographic hash functions may vary depending on the zk-STARK construction and implementation. The high-level workflow of zk-STARKs protocol is given in Fig. 7. The following procedures provide a simplified overview of the process.

- Generating Identity Proofs:
  - An individual who wants to share their identity on the blockchain generates an identity proof using zk-STARKs.
  - The individual inputs their identity-related information, such as name, age, or credentials, into the proof generation algorithm.
  - The algorithm constructs a set of constraints based on the required attributes and verifies their correctness using polynomials and evaluations.

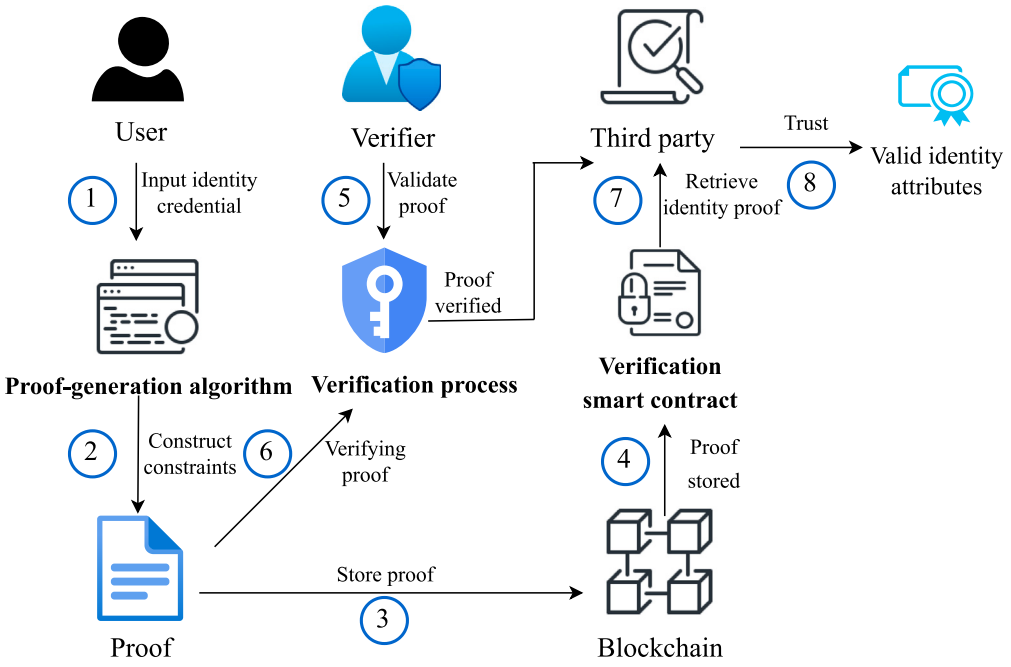

Fig. 7. The high level zk-STARKs protocol.

  - The result is a succinct proof that attests to the validity of the identity-related information without revealing the actual values.

- Storing Identity Proofs on the Blockchain:
  - The generated identity proofs are stored on the blockchain, associating them with the corresponding user's address or identifier.
  - The proofs are added to the blockchain's data structure, such as transactions or smart contracts, in a secure and immutable manner.
  - The size of the proofs is significantly smaller than zk-SNARKs, allowing for efficient storage and retrieval of identity-related information on the blockchain.

- Verifying Identity Proofs:
  - When a third party wants to verify the identity of an individual on the blockchain, they retrieve the corresponding identity proof.
  - Using the zk-STARK verification process, the verifier can validate the proof without needing to access the underlying identity-related information directly.
  - The verification process involves evaluating the constraints specified in the proof and ensuring that they hold true.
  - If the proof is successfully verified, the third party can trust the validity of the identity attributes without needing to know the actual values.

The *proof generation algorithm* in the zk-STARKs can be explained as follows. Let us denote the identity-related information for an individual as $\{attribute_1, attribute_2, \ldots, attribute_n\}$. A set of constraints $C = \{c_1, c_2, \ldots, c_m\}$ that represent the required attributes can be constructed, where each constraint c_i is a polynomial that evaluates to zero when the corresponding attribute is satisfied. Each constraint polynomial c_i at specific trace points $z_1, z_2, \ldots, z_t$ can be evaluated to provide corresponding vector of evaluations $[c_1(z_1), c_1(z_2), \ldots, c_1(z_t)], [c_2(z_1), c_2(z_2), \ldots, c_2(z_t)], \ldots, [c_m(z_1), c_m(z_2), \ldots, c_m(z_t)]$. The evaluated constraint polynomials and trace point evaluations are used to generate a succinct proof polynomial $p(x)$. The proof polynomial $p(x)$ represents the combination of the constraint evaluations and is constructed using mathematical operations like polynomial addition, multiplication, and interpolation. Let us consider a simple scenario where an individual wants to prove possession of multiple attributes, such as age, nationality, and education level, using zk-STARKs. The constraints are age $\geq$ 18, Nationality = "Australia", and EducationLevel = "Bachelor's Degree". Constraint polynomials c1(Age) = Age - 18, c2(Nationality) = Hash(Nationality) - Hash("Australia") and c3(EducationLevel) = Hash(EducationLevel) - Hash("Bachelor's Degree") can be evaluated at specific trace points. This process generated a succinct proof polynomial $p(x)$ that represents the evaluations of the constraint polynomials at the trace points. Once the identity proof is generated, it can be stored on the blockchain. The specific data structure and storage mechanism may vary depending on the blockchain platform being used.

To verify the identity proof retrieved from the blockchain, the verifier retrieves identity proof polynomial $p(x)$ and constraint polynomials c_i such as c1(Age) = Age - 18, c2(Nationality) = Hash(Nationality) - Hash("Australia") and c3(EducationLevel) = Hash(EducationLevel) - Hash("Bachelor's Degree") representing the required attributes. Each constraint polynomial c_i at the same trace points used during proof generation is evaluated $[c_1(z_1), c_1(z_2), \ldots, c_1(z_t)], [c_2(z_1), c_2(z_2), \ldots, c_2(z_t)], \ldots, [c_m(z_1), c_m(z_2), \ldots, c_m(z_t)]$. For instance, constraints c1(Age), c2(Nationality) and c3(EducationLevel) are evaluated at trace points $[z_1, z_2, \ldots, z_t]$. It must be verified that the evaluations of the constraint polynomials match the corresponding values in the proof polynomial $p(x)$ at the trace points. For instance, $c_1(z_1) = p(z_1), c_1(z_2) = p(z_2), \ldots, c1(zt) = p(z_t)$ for constraint 1, $c_2(z_1) = p(z_1), c_2(z_2) = p(z_2), \ldots, c_2(z_t) = p(z_t)$ for constraint 2, and $c_3(z_1) = p(z_1), c_3(z_2) = p(z_2), \ldots, c_3(z_t) = p(z_t)$ for constraint 3 should be verified. If all the constraint evaluations match the values in $p(x)$, the identity proof is considered valid.

7.3. Comparison of ZK-SNARKs and ZK-STARKs for identity sharing on blockchain

As shown in Table 7, the two protocols can be compared as follows:

Table 7
Comparison of ZK-SNARKs and ZK-STARKs for identity sharing on blockchain.

Feature	ZK-SNARKs	ZK-STARKs
Privacy preservation	Yes	Yes
Efficiency	Good (small proofs)	Excellent (small proofs)
Security	Good	Excellent (no trusted setup)
Transparency	Moderate (depends on setup)	Excellent (transparent)
Selectivity	Yes	Yes
Trustless verification	No (requires a setup)	Yes
Adoption and standardization	Widely adopted, standardized	Less widespread, evolving

(1) **Privacy Preservation:** Both ZK-SNARKs and ZK-STARKs offer strong privacy preservation, allowing users to prove identity attributes without revealing sensitive data. This feature will remain critical in future blockchain applications, especially in privacy-sensitive sectors like healthcare and finance.
(2) **Efficiency:** ZK-STARKs have a clear advantage in terms of efficiency due to their smaller proofs and the elimination of the need for a trusted setup. This efficiency will become increasingly important as blockchain applications scale and demand faster and more cost-effective verification.
(3) **Security:** ZK-STARKs offer superior security by removing the reliance on a trusted setup. As blockchain technology evolves and quantum computing threats loom on the horizon, the elimination of the trusted setup will be a compelling reason to choose ZK-STARKs.
(4) **Transparency:** ZK-STARKs are transparent in their construction, making them highly suitable for public blockchains. Trust in the verification process is paramount, and transparency ensures that the proof generation process is verifiable and immune to tampering.
(5) **Selectivity:** Both ZK-SNARKs and ZK-STARKs support selective disclosure, allowing users to share specific identity attributes. This selective disclosure will continue to be essential for minimizing data exposure.
(6) **Trustless Verification:** ZK-STARKs enable trustless verification, meaning that anyone on the blockchain can independently verify identity proofs. This aligns with the decentralized nature of blockchain technology and reduces reliance on central authorities.
(7) **Adoption and Standardization:** ZK-SNARKs have a head start in terms of adoption and standardization. However, the field of zero-knowledge proofs is rapidly evolving, and ZK-STARKs are gaining attention for their security and efficiency benefits. As ZK-STARKs mature and gain wider acceptance, they are likely to become more accessible and standardized.

While ZK-SNARKs currently enjoy greater adoption, ZK-STARKs offer compelling advantages in terms of security, efficiency, and transparency. As blockchain technology continues to advance and address scalability and security challenges, ZK-STARKs are likely to play an increasingly prominent role in identity sharing and other privacy-sensitive applications on the blockchain. The choice between the two will depend on the specific requirements of each use case, with ZK-STARKs being favored for applications demanding higher security and efficiency.

8. Challenges, recommendations, & lessons learned

8.1. Blockchain challenges and recommendations

Blockchain technology, with its decentralized architecture, promises to revolutionize digital identity sharing by providing a secure and decentralized framework for managing personal data. However, the decentralized nature of blockchain presents certain challenges, especially regarding the efficient storage and management of user identities.

One significant challenge is the inherent limitation of storage capacity in blockchain networks. Since every node in a blockchain network maintains a copy of all transactions, the system's storage capacity is finite. As the volume of user data increases over time, this constraint becomes more apparent and can lead to scalability issues. Latency is another challenge associated with blockchain technology. The time it takes to add a new block to the blockchain, known as latency, is influenced by the consensus mechanism in use. The necessity for all network nodes to receive, verify, and include new transactions can introduce delays. This is particularly relevant for applications requiring rapid response times. Additionally, blockchain's immutability, while a strength, poses difficulties when updates or deletions of certain data elements are necessary. Once data is recorded on the blockchain, it becomes immutable, making it challenging to accommodate changes or deletions of mutable data, such as addresses or contact details.

To address these challenges, several strategic recommendations can be considered:

1. Off-Chain Data Storage: One potential solution involves storing only a hashed representation of the data directly on the blockchain, while the actual data is stored off-chain. This approach, as suggested by Tang et al. can significantly reduce on-chain data, alleviating storage concerns while preserving data integrity through hashing.

2. Sharding for Efficient Storage: Sharding, a technique that partitions data across multiple nodes, offers a promising approach to optimize storage within the blockchain. By distributing data in this manner, storage utilization is optimized, and scalability is enhanced.

3. Latency Mitigation Strategies: To address latency issues, various strategies can be explored. One approach is streamlining the consensus process by employing Byzantine fault-tolerant (BFT) protocols to select leader nodes, as highlighted by Xie et al. Another strategy involves adopting a sharding-based blockchain architecture, which separates consensus-related messages from block computation and dissemination. This separation can lead to reduced latency, as proposed by Wang et al.

By implementing these recommendations, the blockchain community can overcome the challenges related to decentralized storage, latency, and data modification. This proactive approach will pave the way for more efficient and agile digital identity frameworks, ensuring that blockchain continues to be a key enabler in the realm of secure and decentralized identity sharing.

8.2. ZKPs challenges and recommendations

In the realm of cryptographic proofs, zk-STARKs have emerged as a groundbreaking innovation, especially with their ability to operate without relying on a trusted third-party setup. This attribute makes them a compelling choice for applications such as identity sharing on blockchain platforms. Yet, like any nascent technology, they come with a set of challenges that need careful navigation.

The initial setup for zk-STARKs is notably more nuanced than for zk-SNARKs. It demands meticulous steps, from parameter configuration to the selection of domain-specific constraints. The very foundation of a zk-STARK system's security and efficiency rests on this setup. As such, navigating this intricate process necessitates a profound expertise in the field to ensure the system remains both robust and optimized. When

it comes to computational demands, zk-STARKs are notably resource-hungry, especially when juxtaposed with zk-SNARKs. Core processes intrinsic to zk-STARKs, such as polynomial evaluations and FFT operations, can elongate processing durations. In a high-velocity blockchain environment, where rapid transaction processing is the norm, this could pose potential scalability challenges. Another dimension to consider is the proof size. While zk-STARKs are adept at producing succinct proofs, they often exceed the compactness of proofs generated by zk-SNARKs. This disparity can exert pressure on a blockchain's storage and bandwidth capacities, especially if resources are at a premium. Time efficiency is another area where zk-STARKs face challenges. Their proving and verification processes tend to be more time-consuming than those of zk-SNARKs. Such delays can impact the dynamism of a blockchain system, especially in scenarios demanding instantaneous proof validations. Moreover, the design focus of zk-STARKs leans heavily towards algebraic computations. This specialization might curtail their versatility in more diverse computational scenarios, especially those that pivot around intricate logic or non-algebraic tasks. Considering the relative novelty of zk-STARKs compared to zk-SNARKs, the developmental ecosystem surrounding them is still in its formative stages. This embryonic state can present hurdles in implementation, given the potential scarcity of mature tools, libraries, and frameworks. Lastly, the world of zk-STARKs is in a state of flux, with research and development in full swing. While this promises a horizon of enhancements, it also implies that zk-STARKs are still on their journey towards achieving the rigorous standardization and vetting that zk-SNARKs have undergone. For pioneers looking to integrate zk-STARKs into blockchain systems, staying aligned with cutting-edge research and being agile in adopting emerging techniques is paramount.

However, it is essential to spotlight the transformative potential of ZKPs. They usher in a new era of identity sharing, where privacy and efficiency coalesce seamlessly. Their prowess in consolidating multiple proofs into a singular, streamlined proof is a game-changer, especially when the goal is to verify multifaceted identity attributes without unnecessary data disclosures.

Certain ZKPs, like zk-SNARKs, have the added advantage of being non-interactive, which trims down communication overheads and propels the verification process. This ensures a swift, yet private, validation of identity attributes. Furthermore, the parallel verification capabilities of ZKPs are a boon for systems that thrive on speed. Coupled with their ability to authenticate identity attributes without divulging the actual data, they strike a harmonious balance between privacy and storage optimization. The future of ZKPs is radiant with possibilities. As research forges ahead, we can anticipate a cascade of refined algorithms and optimization strategies. These advancements will further hone the efficiency of ZKPs, enabling seamless identity sharing with minimal computational strain. Their inherent feature of selective disclosure amplifies privacy, granting individuals autonomy over their identity disclosures. In the digital identity domain, ZKPs are promising. They encapsulate a harmonious blend of privacy and efficiency, positioning themselves as the vanguard for systems that champion both secure and scalable identity sharing.

8.3. Lessons learned

Throughout our survey and analysis of blockchain-based identity sharing with Zero-Knowledge Proofs (ZKPs), several important lessons have emerged. These lessons provide valuable insights for researchers, developers, and stakeholders in the field of digital identity and blockchain technology:

1. **Diverse Applications**: Blockchain-based identity sharing with ZKPs is a versatile technology with applications beyond digital identity. It can be applied in fields such as supply chain management, healthcare, finance, and more. Understanding its diverse applications is crucial for harnessing its full potential.

2. **Interdisciplinary Collaboration**: Successful implementation of blockchain-based identity solutions often requires collaboration between experts from multiple domains, including cryptography, cybersecurity, blockchain technology, and legal and regulatory compliance.

3. **Privacy by Design**: Privacy should be an inherent part of the design and development process. Incorporating privacy-enhancing technologies like ZKPs from the outset ensures that identity sharing systems are robust and user-centric.

4. **Regulatory Awareness**: Compliance with legal and regulatory frameworks, such as GDPR and HIPAA, is essential. Understanding the legal implications and ensuring alignment with regulations is paramount for any identity sharing system.

5. **Usability Matters**: User experience plays a pivotal role in the adoption of blockchain-based identity solutions. User-friendly interfaces and seamless interactions are crucial to gaining user trust and acceptance.

6. **Security and Scalability Balancing Act**: Achieving a balance between security and scalability is an ongoing challenge. Solutions should be designed with both aspects in mind, ensuring that security is not compromised as the system scales.

7. **Standardization and Interoperability**: Establishing industry standards and ensuring interoperability between different blockchain networks and identity systems is essential. Standardization promotes adoption and fosters a more cohesive ecosystem.

8. **Community Engagement**: Engaging with the broader blockchain and identity-sharing community is valuable for sharing knowledge, best practices, and lessons learned. Collaboration accelerates innovation in the field.

9. **Continuous Adaptation**: The landscape of blockchain technology and identity sharing is dynamic. Stakeholders must stay informed about emerging trends, research, and advancements to adapt and evolve their solutions.

10. **Ethical Considerations**: As identity sharing systems collect and manage sensitive user data, ethical considerations should be at the forefront. Transparency, consent, and data ownership are ethical principles that should guide system design.

These lessons reflect the multidimensional nature of blockchain-based identity sharing with ZKPs. Embracing these lessons can pave the way for more robust, secure, and user-centric identity sharing systems in the future.

9. Conclusion

Recent data breaches have raised serious concerns for using the present centralized identity sharing approach, which requires users to share their true identity information or documents to obtain services. Such a centralized system produces a vulnerable architecture, which frequently leads to identity theft and other cybercrimes. Blockchain has the potential to substantially revolutionize identity sharing through decentralized mechanisms. However, the inherent transparency of blockchain exposes it to vulnerabilities in user identity sharing, especially leading to privacy concerns. This paper provided a comprehensive overview of current blockchain technology and extensively analyzed the application of zero-knowledge proof technology to preserve user identity privacy. Key concepts related to blockchain technology and zero-knowledge proof methods are highlighted and the use of ZKP in blockchain-based identity sharing techniques is critically analyzed. The article also provided a critical reflection of existing literature employing ZKP-based identity sharing techniques using blockchains. Finally, critical research challenges and their possible solutions along with future research issues are presented to inspire researchers and practitioners to focus their efforts on developing innovative solutions that can unlock the full potential of blockchain technology in the realm of identity sharing while upholding user privacy.

CRediT authorship contribution statement

Lu Zhou: Conceptualization, Methodology, Writing – original draft, Writing – review & editing. **Abebe Diro:** Conceptualization, Funding acquisition, Methodology, Project administration, Resources, Supervision, Writing – original draft, Writing – review & editing. **Akanksha Saini:** Funding acquisition, Methodology, Resources, Supervision, Writing – original draft, Writing – review & editing. **Shahriar Kaisar:** Funding acquisition, Methodology, Resources, Supervision, Writing – original draft, Writing – review & editing. **Pham Cong Hiep:** Funding acquisition, Methodology, Resources, Writing – original draft, Writing – review & editing.

Declaration of competing interest

The authors declare no conflict of interest.

Data availability

No data was used for the research described in the article.

Acknowledgment

This research was supported by College of Business and Law Melbourne Vietnam Collaborative Project Support Scheme, RMIT University, Australia.

References

[1] Ning H, Zhen Z, Shi F, Daneshmand M. A survey of identity modeling and identity addressing in internet of things. IEEE Internet Things J 2020;7(6):4697–710.
[2] Wang C, Yang B, Cui J, Wang C. Fusing behavioral projection models for identity theft detection in online social networks. IEEE Trans Comput Social Syst 2019;6(4):637–48.
[3] Alkhadra R, Abuzaid J, AlShammari M, Mohammad N. Solar winds hack: In-depth analysis and countermeasures. In: 2021 12th International conference on computing communication and networking technologies (ICCCNT). IEEE; 2021, p. 1–7.
[4] Pitney AM, Penrod S, Foraker M, Bhunia S. A systematic review of 2021 microsoft exchange data breach exploiting multiple vulnerabilities. In: 2022 7th International conference on smart and sustainable technologies (splitech). IEEE; 2022, p. 1–6.
[5] Becker M. "Here's a bandaid"– musings on the T-mobile data breach and what we need to do next.
[6] Roy G. Criticality of E-privacy and data leakage amid the pandemic: Privacy-preserving techniques and frameworks. In: Machine learning and data analytics for predicting, managing, and monitoring disease. IGI Global; 2021, p. 183–9.
[7] Wang J, Huang J, Kong L, Chen G, Zhou D, Rodrigues JJC. A privacy-preserving vehicular data sharing framework atop multi-sharding blockchain. In: 2021 IEEE global communications conference (GLOBECOM). 2021, p. 1–6.
[8] Sun X, Yu FR, Zhang P, Sun Z, Xie W, Peng X. A survey on zero-knowledge proof in blockchain. IEEE Netw 2021;35(4):198–205.
[9] Partala J, Nguyen TH, Pirttikangas S. Non-interactive zero-knowledge for blockchain: A survey. IEEE Access 2020;8:227945–61.
[10] Liu Y, He D, Obaidat MS, Kumar N, Khan MK, Choo K-KR. Blockchain-based identity management systems: A review. J Netw Comput Appl 2020;166:102731.
[11] Soltani R, Nguyen UT, An A. A survey of self-sovereign identity ecosystem. Secur Commun Netw 2021;2021:1–26.
[12] Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. SIGCOMM Comput Commun Rev 2004;34(2):39–53.
[13] Toosi AN, Calheiros RN, Buyya R. Interconnected cloud computing environments: Challenges, taxonomy, and survey. ACM Comput Surv 2014;47(1):1–47.
[14] Badirova A, Dabbaghi S, Moghaddam FF, Wieder P, Yahyapour R. A survey on identity and access management for cross-domain dynamic users: Issues, solutions, and challenges. IEEE Access 2023.
[15] Pöhn D, Hommel W. New directions and challenges within identity and access management. IEEE Commun Stand Mag 2023;7(2):84–90.
[16] Zaghloul E, Li T, Mutka MW, Ren J. Bitcoin and blockchain: Security and privacy. IEEE Internet Things J 2020;7(10):10288–313.
[17] Zou W, Lo D, Kochhar PS, Le X-BD, Xia X, Feng Y, Chen Z, Xu B. Smart contract development: Challenges and opportunities. IEEE Trans Softw Eng 2021;47(10):2084–106.
[18] Chen J, Xia X, Lo D, Grundy J, Luo X, Chen T. Defining smart contract defects on ethereum. IEEE Trans Softw Eng 2022;48(1):327–45.
[19] Wang S, Ouyang L, Yuan Y, Ni X, Han X, Wang F-Y. Blockchain-enabled smart contracts: Architecture, applications, and future trends. IEEE Trans Syst Man Cybern: Syst 2019;49(11):2266–77.
[20] Rahman MU. Scalable role-based access control using the eos blockchain. 2020, arXiv.
[21] Kondratiuk D, Seijas PL, Nemish A, Thompson S. Standardized crypto-loans on the cardano blockchain. In: Financial cryptography and data security. FC 2021 international workshops: CoDecFin, DeFi, VOTING, and WTSC, Virtual event, March 5, 2021, revised selected papers. Springer; 2021, p. 579–94.
[22] Zhang P, Wang L, Wang W, Fu K, Wang J. A blockchain system based on quantum-resistant digital signature. Secur Commun Netw 2021;2021:1–13.
[23] Belotti M, Božić N, Pujolle G, Secci S. A vademecum on blockchain technologies: When, which, and how. IEEE Commun Surv Tutor 2019;21(4):3796–838.
[24] Yue K, Zhang Y, Chen Y, Li Y, Zhao L, Rong C, Chen L. A survey of decentralizing applications via blockchain: The 5G and beyond perspective. IEEE Commun Surv Tutor 2021;23(4):2191–217.
[25] Satoshi N. Bitcoin: A peer-to-peer electronic cash system. 2008, (accessed 28 April 2023). [Online]. Available: https://bitcoin.org/bitcoin.pdf.
[26] Daniel L. Transactions as proof-of-stake. 2013, (accessed 28 April 2023). [Online]. Available: https://cryptochainuni.com/wp-content/uploads/Invictus-Innovations-Transactions-As-Proof-Of-Stake.pdf.
[27] Castro M, Liskov B. Practical byzantine fault tolerance. In: OsDI, Vol. 99. 1999, p. 173–86.
[28] Daniel L. Delegated proof-of-stake white paper. 2014.
[29] Zheng Z, Xie S, Dai H-N, Chen W, Chen X, Weng J, Imran M. An overview on smart contracts: Challenges, advances and platforms. Future Gener Comput Syst 2020;105:475–91.
[30] Lim SY, Fotsing PT, Almasri A, Musa O, Kiah MLM, Ang TF, Ismail R. Blockchain technology the identity management and authentication service disruptor: a survey. Int J Adv Sci, Eng Inf Technol 2018;8(4–2):1735–45.
[31] Bao H, Ren B, Li B, Kong Q. BBNP: A blockchain-based novel paradigm for fair and secure smart grid communications. IEEE Internet Things J 2022;9(15):12984–96.
[32] Baza M, Lasla N, Mahmoud MMEA, Srivastava G, Abdallah M. B-Ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain. IEEE Trans Netw Sci Eng 2021;8(2):1214–29.
[33] Kumar P, Kumar R, Gupta GP, Tripathi R. A distributed framework for detecting DDoS attacks in smart contract-based blockchain-IoT systems by leveraging fog computing. Trans Emerg Telecommun Technol 2021;32(6).
[34] Tran D. Data breaches affecting millions of Australians are on the rise, information commissioner says. 2023, https://www.abc.net.au/news/2023-03-01/data-breaches-revealed-by-australian-information-commissioner/102039710, accessed 10 May 2023.
[35] Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Integration of blockchain and cloud of things: Architecture, applications and challenges. IEEE Commun Surv Tutor 2020;22(4):2521–49.
[36] Wang C, Wang S, Cheng X, He Y, Xiao K, Fan S. A privacy and efficiency-oriented data sharing mechanism for IoTs. IEEE Trans Big Data 2023;9(1):174–85.
[37] Fiat A, Shamir A. How to prove yourself: Practical solutions to identification and signature problems. In: Advances in cryptology — CRYPTO' 86. Springer Berlin Heidelberg; 1987, p. 186–94.
[38] Bai T, Hu Y, He J, Fan H, An Z. Health-zkIDM: A healthcare identity system based on fabric blockchain and zero-knowledge proof. Sensors 2022;22(20).
[39] Partala J, Nguyen TH, Pirttikangas S. Non-interactive zero-knowledge for blockchain: A survey. IEEE Access 2020;8:227945–61.
[40] Ben Sasson E, Chiesa A, Garman C, Green M, Miers I, Tromer E, Virza M. Zerocash: Decentralized anonymous payments from bitcoin. In: 2014 IEEE symposium on security and privacy. 2014, p. 459–74.
[41] Rondelet A, Zajac M. ZETH: On integrating zerocash on ethereum. 2019, [Online]. Available: https://arxiv.org/abs/1904.00905.
[42] Ben-Sasson E, Chiesa A, Tromer E, Virza M. Succinct non-interactive zero knowledge for a von Neumann architecture. In: 23rd {USENIX} security symposium ({USENIX} security 14). 2014, p. 781–96.
[43] ElSheikh M, Youssef AM. Dispute-free scalable open vote network using zk-SNARKs. 2022, arXiv.
[44] Lee J, Choi J, Oh H, Kim J. Privacy-preserving identity management system. Cryptology ePrint Archive; 2021.
[45] Ben-Sasson E, Bentov I, Horesh Y, Riabzev M. Scalable, transparent, and post-quantum secure computational integrity. Cryptology ePrint Archive; 2018.
[46] Xie J, Tang H, Huang T, Yu FR, Xie R, Liu J, Liu Y. A survey of blockchain technology applied to smart cities: Research issues and challenges. IEEE Commun Surv Tutor 2019;21(3):2794–830.
[47] Guan Z, Wan Z, Yang Y, Zhou Y, Huang B. BlockMaze: An efficient privacy-preserving account-model blockchain based on zk-SNARKs. IEEE Trans Dependable Secure Comput 2022;19(3):1446–63.
[48] Song Z, Wang G, Yu Y, Chen T, et al. Digital identity verification and management system of blockchain-based verifiable certificate with the privacy protection of identity and behavior. Secur Commun Netw 2022;2022.

[49] Miers I, Garman C, Green M, Rubin AD. Zerocoin: Anonymous distributed E-cash from bitcoin. In: 2013 IEEE symposium on security and privacy. 2013, p. 397–411.
[50] Duffield E, Diaz D. Dash: A privacy-centric cryptocurrency. 2015, (accessed 28 April 2023). [Online]. Available: https://github.com/dashpay/dash/wiki/Whitepaper.
[51] Xu L, Shah N, Chen L, Diallo N, Gao Z, Lu Y, Shi W. Enabling the sharing economy: Privacy respecting contract based on public blockchain. In: Proceedings of the ACM workshop on blockchain, cryptocurrencies and contracts. 2017, p. 15–21.
[52] Hou D, Zhang J, Huang S, Peng Z, Ma J, Zhu X. Privacy-preserving energy trading using blockchain and zero knowledge proof. In: 2022 IEEE international conference on blockchain (blockchain). 2022, p. 412–8.
[53] Zhang Y. Increasing cyber defense in the music education sector using blockchain zero-knowledge proof identification. Comput Intell Neurosci 2022;2022.
[54] Yuan K, Yingjie Y, Tong X, Wenchao Z, Sufang Z, Chunfu J. Privacy-protection scheme of a credit-investigation system based on blockchain. Entropy 2021;23(12).
[55] Song L, Ju X, Zhu Z, Li M. An access control model for the internet of things based on zero-knowledge token and blockchain. EURASIP J Wireless Commun Networking 2021;2021(1).
[56] Liu Z, Hu C, Xia H, Xiang T, Wang B, Chen J. SPDTS: a differential privacy-based blockchain scheme for secure power data trading. IEEE Trans Netw Serv Manage 2022.
[57] Ren Z, Zha X, Zhang K, Liu J, Zhao H. Lightweight protection of user identity privacy based on zero-knowledge proof. In: 2019 IEEE International conference on system, man and cybernetics (SMC). 2019, p. 2549–54.
[58] Al-Aswad H, Hasan H, Elmedany W, Ali M, Balakrishna C. Towards a blockchain-based zero-knowledge model for secure data sharing and access. In: 2019 7th International conference on future internet of things and cloud workshops (FiCloudW). 2019, p. 76–81.
[59] Jo U, Oktian YE, Kim D, Oh S, Lee H, Kim H. A zero-knowledge-range-proof-based privacy-preserving blockchain platform for COVID-19 contact tracing. In: 2022 International conference on platform technology and service (PlatCon). 2022, p. 53–8.
[60] Yang X, Li W. A zero-knowledge-proof-based digital identity management scheme in blockchain. Comput Secur 2020;99:102050.
[61] Zheng H, You L, Hu G. A novel insurance claim blockchain scheme based on zero-knowledge proof technology. Comput Commun 2022;195:207–16.
[62] Rasheed A, Mahapatra RN, Varol C, Narashimha K. Exploiting zero knowledge proof and blockchains towards the enforcement of anonymity, data integrity and privacy (ADIP) in the IoT. IEEE Trans Emerging Top Comput 2022;10(3):1476–91.
[63] Namazi M, Ross D, Zhu X, Ayday E. zkFaith: Soonami's zero-knowledge identity protocol. 2022, arXiv.
[64] Tomaz AEB, Do Nascimento JC, Hafid AS, De Souza JN. Preserving privacy in mobile health systems using non-interactive zero-knowledge proof and blockchain. IEEE Access 2020;8:204441–58.
[65] Pop CD, Antal M, Cioara T, Anghel I, Salomie I. Blockchain and demand response: Zero-knowledge proofs for energy transactions privacy. Sensors 2020;20(19):5678.
[66] Li W, Guo H, Nejad M, Shen C-C. Privacy-preserving traffic management: A blockchain and zero-knowledge proof inspired approach. IEEE Access 2020;8:181733–43.
[67] Jeong S, Ahn B. Implementation of real estate contract system using zero knowledge proof algorithm based blockchain. J Supercomput 2021;77(10):11881–93.
[68] Gai K, Tang H, Li G, Xie T, Wang S, Zhu L, Choo K-KR. Blockchain-based privacy-preserving positioning data sharing for IoT-enabled maritime transportation systems. IEEE Trans Intell Transp Syst 2022;24(2):2344–58.
[69] Wang C, Wang S, Cheng X, He Y, Xiao K, Fan S. A privacy and efficiency-oriented data sharing mechanism for IoTs. IEEE Trans Big Data 2023;9(1):174–85.