A Systematic Review on ZKP Algorithms for Blockchain: Methods, Use-cases and Challenges

K. Usha
Department of Banking Technology,
Pondicherry University,
Pondicherry

T. Thenmozhi
Department of Computer Science and Engineering,
KGiSL Institute of Technology,
Tamil Nadu, India

M. Preyadarssini
Tata Consultancy Services,
Sverige AB, Mäster
Samuelsgatan 42, 111 57
Stockholm, Sweden

ABSTRACT

Recent technological advancements have brought the complete business world into the digital space, which uses various technologies such as the Internet of Things, Decentralized ledger technology, and Artificial Intelligence. In this digital space, user authentication plays a crucial role. Verifying the user's identity with selective information disclosure is an efficient way of authentication. Moreover, the identity management of all the entities in the digital space requires a decentralized environment with the lowest level of vulnerabilities. In addition, most business processes in the digital space operate on a public medium prone to attacks, data bleach, etc., and also carry sensitive private information. Hence, digital business space must provide the functionality of security and privacy-preserving information transactions. Furthermore, certain transactional information needs user identity protection as a part of security measures, also known as anonymity. The cryptographic ZKP approach is one of the effective ways to implement the concepts mentioned earlier. ZKP is a verification technique where the identity credentials of a person or entity are verified with selective information disclosure or, in other words, without revealing private information. ZKP can be used to efficiently implement secure information exchange and anonymous identity verification. This paper reviews ZKP models/algorithms proposed in the literature for the various use cases, such as authentication, identity management, security, privacy, and anonymity in a centralized and decentralized environment. Further, this paper analyses the proposed ZKP models for Blockchain in the literature and its various possible applications. Finally, this paper analyses the limitations and challenges of ZKP models.

General Terms

ZKP, Blockchain

Keywords

Authentication, Identity management; Security; Privacy, Anonymity

1. INTRODUCTION

Zero-knowledge proof is a cryptographic model in which the confirmer can verify the claimant by implementing a sequence of stereotyped actions and gets convinced that the claimant has secret information without disclosing any private or other information, including the claimant's data and the confirmer's data [1]. The most significant advantages of ZKP models are i) Implementing ZKP is more straightforward than other cryptographic algorithms since it doesn't require any complicated public key-private key pair. ii) Also, repeated execution of the ZKP model/algorithm will not provide any hint for intruders for more information. The most significant features of ZKP algorithms are i) Inclusiveness/Completeness – assures that confirmation concerning verification is complete and that the claim may proceed with the further process. ii) Reliability/Trustworthiness – In another way, it is known as soundness, which promises that the verified transaction is entirely genuine and not fraudulent. iii) Zero-Knowledge Criteria - ensures zero access to the highly sensitive credentials of both claim and confirmers [2]. Blockchain is one of the implementations of distributed ledger technology, in which the storage of transactional information in a distributed database runs on a peer-to-peer network [3]. Cryptographic algorithms ensure the security of the ledger data. The ledger has unique characteristics such as an append-only format, immutability, and updatable-ness via consensus with peer nodes. Blockchain applications [4] are widespread in real-time use cases such as cryptocurrency payment and transaction, finance, digital education and governance, healthcare, etc., and they also solve security issues when operating the Internet of Things and artificial intelligence-based applications [5]. Despite the widespread applications of blockchain technology, specific problems related to privacy, anonymity, and security need to be solved.

1.1 Review of existing study works

The study presented in this reference paper [6] analyses various models, such as hash-based, signature-based, and ZKP models, for selective disclosure of digital identity. This study categorizes various models and compares them. The application of the selective disclosure models considered in this study is anonymity and, to some extent, privacy. The study describes [7] the various ZKP algorithms for privacy preservation implemented in Blockchain. This paper also describes the current state of the art of ZKP in Blockchain and its future direction. This review paper [8] analyses ZKP models for authentication and architecture for IoT applications. This paper also analyses the advantages and limitations of ZKP models for authentication in IoT applications. The reference review paper [9] analyses the ZKP methods used for security and privacy in corporate blockchain networks. The comparative studies of ZKP methods with other privacy preservation methods also portray these models' issues and challenges [10]. This paper comprehensively surveys ZKP methods for blockchain-based identity management. This paper also presents the challenges and future directions.

1.2 Gap analysis and need for this study

Some existing studies focus on a broader perspective of selective disclosure models, but their applications are confined to privacy preservation and anonymity. Further, few other studies have explored the ZKP integration with Blockchain to solve the application's privacy issues. Some papers analyze the implementation of ZKP models for decentralized identity management and present their evaluations. In addition, review ZKP models for specific applications such as the Internet of Things, etc. This study exclusively reviews ZKP models, which are considered more advantageous than all other selective disclosure models. This study also aims to analyze ZKP models for various use cases such as identity management, authentication, security, privacy preservation, and anonymity. This study analyzes ZKP integrated with Blockchain models for multiple applications. This proposed study also discusses the issues related to blockchain implementations, which can be solved using ZKP models.

1.3 Objectives of this study

This paper reviews ZKP models for various use cases such as identity management, access control, authentication, security, privacy, and anonymity. Further, this study extends the scope of the study to interpret the significance of ZKP models in a Blockchain environment. Furthermore, this paper reviews various applications of ZKP models and ZKP models integrated with Blockchain. Finally, it presents the challenges and future directions of implementing ZKP methods and their applications.

- To conduct a comprehensive survey of existing literature that explores how ZKP aids in digital identity management, authenticating information, securing information, privacy-preservation of data, and anonymity.
- To perform a deeper analysis of ZKP models integrated with Blockchain and its applications
- To understand the importance of ZKP models in blockchain implementations, privacy related to identity, transactions, and smart contracts is also analyzed according to the type of Blockchain – private, public, and consortium [9].
- To analyze the shortcomings and outline the challenges in ZKP model implementations.

1.4 Review Methodology

The following topics are considered for this review article: ZKP, ZKP models, ZKP integration with Blockchain Technology, ZKP use cases – implementation of access control, anonymously authenticating information, anonymous identity management, security and privacy preservation of information. The research objectives are framed with the fundamental analysis of the searched content. Works of literature from the databases i) ACM, ii)IEEE, iii) Scopus, iv) Springer, v) Web of Science, vi) Taylor and Francis, and vii) Willey based on the topics, content, and concepts related to the framed objectives were taken. Further, by removing duplicates from the results obtained by the search, manual examination of the abstract and full article to categorize the ZKP model, ZKP use cases, and ZKP+Blockchain applications. Finally, the report is prepared by classifying and analyzing the ZKP models and applications.

1.5 Organization of this paper

The organization of the paper is given as follows. Section 2 describes the Zero Knowledge Proof concept and its evolution, the types of ZKP models, and its features. Section 3 discusses blockchain concepts and their evolution, block verification and block appending processes, different types of Blockchain, smart contracts, consensus algorithms, and generic use cases. This section also discusses issues with blockchain implementations. Moreover, section 4 illustrates ZKP algorithmic models – ZK-SNARKS, ZK-STARKS, Bulletproof, and interactive ZKP. Further, section 5 describes a systematic review of ZKP model use cases – security and privacy preservation, multifactor authentication, anonymity, identity management, and use cases of ZKP models in blockchain implementations. Furthermore, section 6 portrays challenges in the implementation of ZKP models. Finally, section 7 concludes the review paper.

2. ZERO KNOWLEDGE PROOF

Zero-knowledge proof is a cryptographic model in which the confirmer can verify the claimant by implementing a sequence of stereotyped actions and gets convinced that the claimant has secret information without disclosing any private or other information, including the claimant's data and the confirmer's data. ZKP is a cryptographic technique that helps authenticate information without revealing both claimant and confirmer privacy-preservation details. ZKP plays a significant role in anonymous identity management, mutually anonymous authentication, access control, securing private information, and securing transactional information. This approach is beneficial in scenarios where anonymity, security, and privacy are preponderant. Use cases in which these performance characteristics are predominant are identity management, access control, authentication, and back-and-forth transacting information [11].

Generally, these algorithms are mathematically based and are resistant to attacks. Information shared for authentication, access control, and identity management is invulnerable (i.e.) protected against intruders' access/manipulation. ZKP algorithms have recently evolved into post-quantum cryptographic-based algorithms that are quantum-resistant. ZKP allows user to hide their privacy-sensitive information and allows their identity-based information for security and privacy reasons. ZKP helps user anonymity for identity management, anonymous authentication, securing private information with selective disclosure, etc. The evolution of ZKP models is shown in the table 1 below. The table portrays the various models of ZKP algorithms from its evolution three decades ago to now. The table shows that the ZKP methods evolved as generic methods and underwent a lot more transitions, and now there are lattice-based and quantum-resistant algorithm models. ZKP models aid in achieving a balance between confidentiality and transparency of the information. ZKP allows a claimant to claim the identity or authenticity of the information without revealing it directly. The claimant can create proof that does not indicate their private data and cannot be inferred from the evidence [12].

2.1 Types of ZKP models

The ZKP model works in two ways: i) Interactive ZKP and ii) Non-interactive ZKP models. In the interactive ZKP model, the claimant and the confirmer establish synchronized communication for authenticating/identity verification. During communication, the claimant produces proof based on basic information without disclosing critical credentials. Confirmer witnesses the evidence and sends back a set of challenges in the sequence of interactions to that claimant for further responses [13]. This type of interaction goes for multiple rounds until the confirmer produces the results, as illustrated in Figure 1. For example, consider a mobile voting system in which voters' age has been verified for checking voting eligibility, with mathematical variations of numbers verified instead of getting direct age information from the claimant.

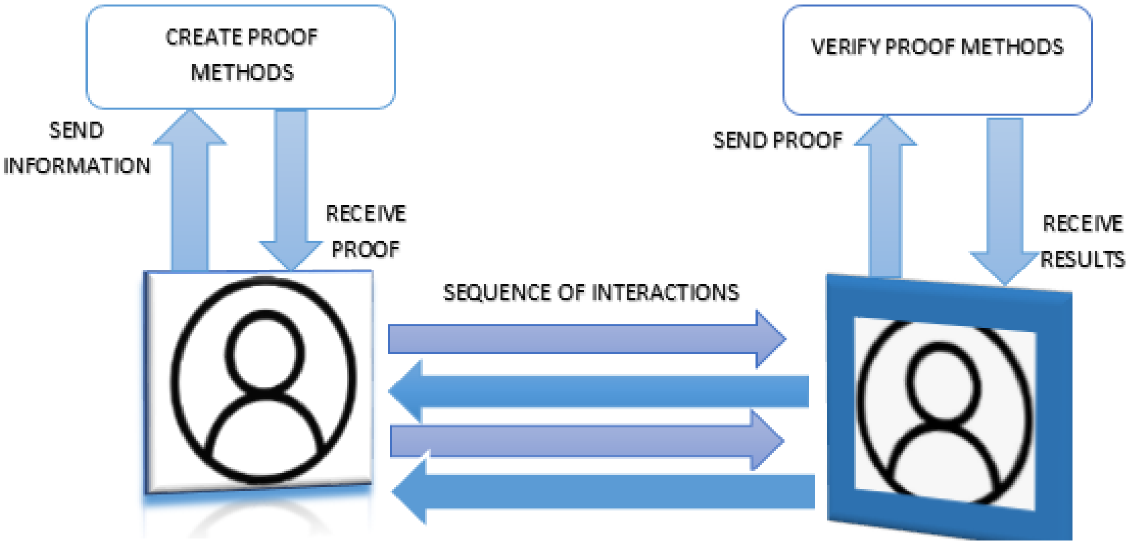

Figure 1. Illustration of Interactive Zero Knowledge Proof

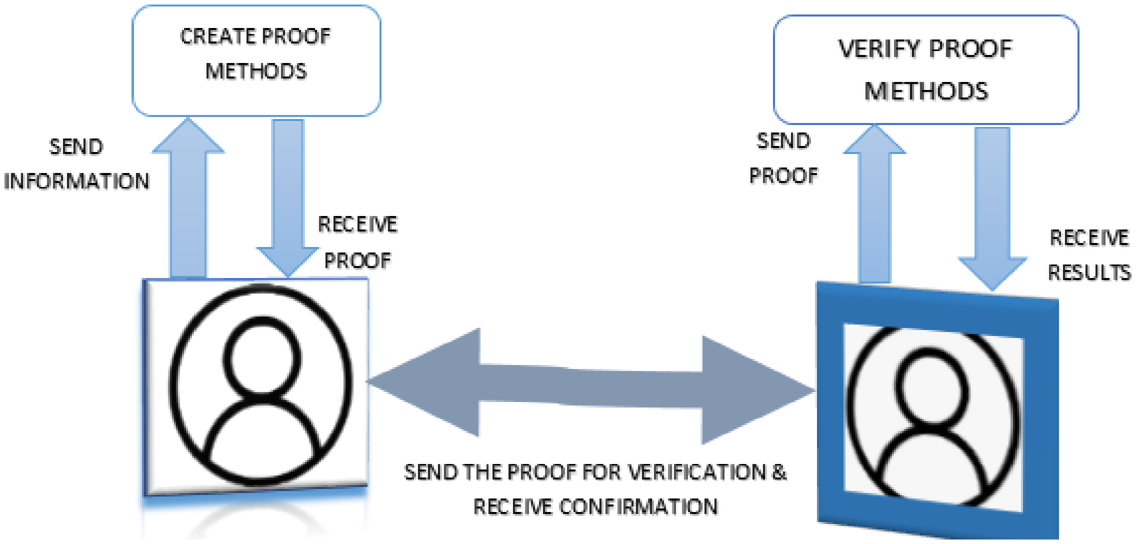

Figure 2. Illustration of Non-Interactive Zero Knowledge Proof

Table 1 Evolution of ZKP

S. No	Year	References	Description
1	1985	Gold-Wasser, Micali, Rackoff [14]	Generic ZKP
2	1987	Santis [15]	Non-interactive ZKP (first algorithm)
3	1988	Gennaro et al. [17]	Efficient NZKP using quasi-safe prime product
4	1988	Gennaro et al. [17]	Efficient NZKP using quasi-safe prime products
5	1989	Schnorr [18]	ZKP in an interactive mode – Signature scheme based on discrete logarithmic problems
6	2006	Persiano et al. [19]	Double round NIZKP
7	2008	Peikert [20]	NIZKP- Lattice cryptography
8	2009	Xagawa and Tanaka K [21]	NTRU (Quantum resistance ZKP) (first algorithm)
9	2013	Xie et al.[22]	ZKP for Ring LWE
10	2015	Cabaracas [23]	Post-quantum commitment scheme for ZKP using lattice problem
11	2016	Martin Fernandez [24]	NIZKP FOR authentication
13	2019	Alshameri and Kumar [26]	NIZKP with a fully homomorphic commitment scheme
14	2022	Lyubashevskey [27]	Lattice-based ZKP scheme (Generic Module LWE)

In the Non-interactive model, there is no synchronized communication setup. The claimant will generate the proof by selectively disclosing information and sending it to the confirmer for verification. There are neither multiple rounds of interactions nor back-and-forth communication. This model works in scenarios where synchronization is impossible, as illustrated in Figure 2. For example, suppose the claimant wants to prove they are an authorized citizen of a particular country. In that case, they can send the details related to the set of country names or continents to which the country belongs to the confirmer without revealing the actual information.

3. BLOCKCHAIN

Blockchain is a distributed database operated on a peer-to-peer network, and Blocks store transactional information [28]. Blocks are linked using hash pointers to form a blockchain structure. Blockchain technology emerged by integrating three main concepts of computer science: i) data structure - block storage and linking blocks with hash pointers, similar to a linked list data structure in which nodes store data and a simple pointer connects nodes. ii) Database – Storage of data similar to that of a traditional database, which is in a table format, and CRUD operations are possibly done by the centralized authority. In contrast, the Blockchain's storage format is blocks, and Read and Write is consensus with other participants. iii) Network – Peer-to-peer network. All participants are equal. In contrast, traditional database storage operates on the client-server network in which the server stores and operates on data. Cryptographic concepts play a crucial role in securing the data stored in the Blockchain and the overall implementation of the Blockchain, creation of hash pointers, and data encryption with public-key infrastructure and digital signature, etc.

3.1 Evolution of Blockchain

Technically, Blockchain is defined as follows: Blockchain is a distributed ledger shared on a peer-to-peer network. Blockchain uses cryptographic algorithms for secured information storage and transactions. The characteristic features of Blockchain are that it is an append-only ledger that is immutable and updatable via consensus algorithms. Generally, it helps to keep records in a shared, distributed, and secured way. It is more beneficial in terms of transparency. Every system user holds a copy of the documents to view, and updates are possible via agreement among other users. The following table defines the evolution of Blockchain Technology. Initially, Blockchain started with cryptocurrency transactions and payments. It further grew in implementing distributed applications (Dapps) and deploying digital services offered by the government, financial institutions, and other business organizations using smart contracts. Furthermore, it recently emerged as the backbone architecture for building digital infrastructure.

Table 2 Evolution of Blockchain

S. No	References	Year	Description
1	[29]-[31]	2009-2011	Cryptocurrencies
2	[32]-[34]	2012-2017	DApps
3	[35]-[37]	2008-2022	Digital Services
4	[38]-[40]	2022 and beyond	Digital Intelligence infrastructure.

The significant aspect of Blockchain technology is disintermediation. Transacting information for various applications eliminates the need for intermediaries, a predominant entity in traditional systems. Blockchain is among the distributed ledger technologies; the others are tree structure and directed acyclic graphs (DAGs). The transactional information is stored in blocks linked by cryptographic algorithms. Blockchain simulates linked list data structure in which pointers are chained as hash pointers, and nodes are represented as Blocks. Block information can be categorized as Blockhead and Block body. Blockhead consists of i) Block hash, ii) Time stamp linked with transactional information, iii) Hash value of the previous block, iv) Nonce - a randomly generated number, and iv) Merkle tree root value. The following figure 3 illustrates the Block Structure in a Blockchain.

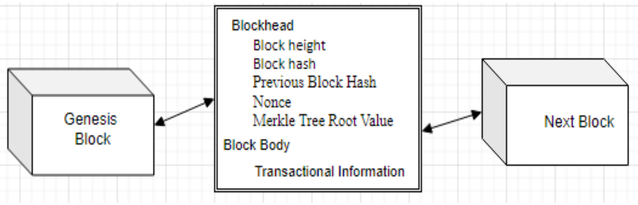

Figure 3. Illustration of Generic Structure of Block in a Blockchain

The block body consists of a list of transactional information. A blockchain block is addressed by its hash value, which is represented as block hash. The block's position in the Blockchain is defined in the block as block height value. In any Blockchain-based application, when a user wants to perform operations, it becomes a request from the user side. It generates new transactions in their application and broadcasts the network's transaction information. This transaction will become a part of an unverified and unmined pool of transactions with the nodes. The nodes will collect such transactions and select a specific set of transactions for mining. Mining here means verifying the transaction information and manipulating the hash values of the transactions to find the block address (block hash value) so that these transactions can be added to the block. Once the hash value is found, it will be announced in the network along with the public key for others to verify and approve. Once all other nodes have been verified, a consensus is reached on appending it to the proposed Blockchain [41]. The following Figure 4 illustrates the blockchain verification and block appending process.

The consensus algorithms play a crucial role in the implementation of Blockchain Technology. All the peers in the network verify and validate transactional information in the absence of centralized nodes. The consensus algorithm provides instructions for creating the block with an agreed set of transactions and appending the block in the Blockchain with an agreement with other nodes.

3.2 Types of Blockchain

System architectures can be categorized into centralized, decentralized, and distributed. A centralized system has a single point of authority that controls all the other nodes for accessing and sharing the information.

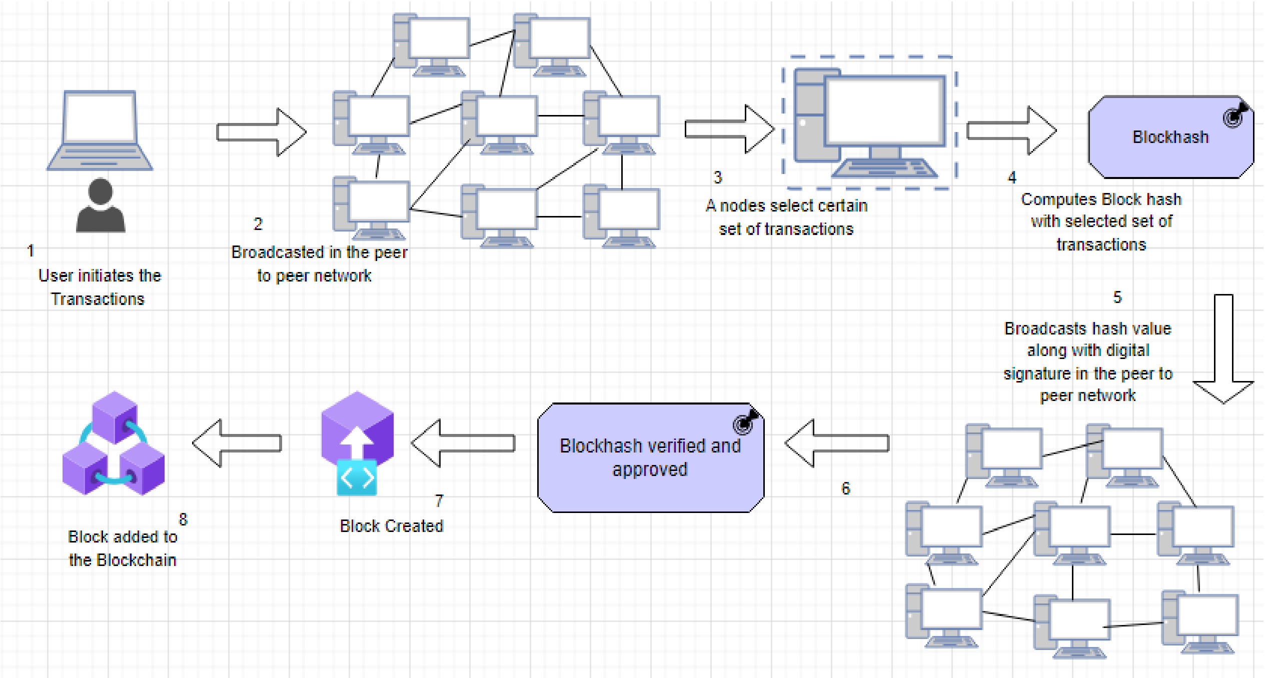
1
User initiates the Transactions
2
Broadcasted in the peer to peer network
3
A nodes select certain set of transactions
Blockhash
4
Computes Block hash with selected set of transactions
5
Broadcasts hash value along with digital signature in the peer to peer network
6
Blockhash verified and approved
7
Block Created
8
Block added to the Blockchain

Figure 4. Illustrates the blockchain verification and block appending process.

For example, Client-server architecture and example application is TCP/IP (Transmission control protocol/Internet Protocol). In contrast, the decentralized system architecture has no central authority to control accessing and sharing information. All nodes are equal and run independently and simultaneously for processing. For example, a peer-to-peer network and an example application is Blockchain [42]. In distributed system architecture, the computations are distributed among the nodes for processing. This concept of distributed processing may be included in peer-to-peer or client-server systems architecture. For example, N-trier computing systems and example applications are cluster, fog, and grid computing. The systems can be designed using hybridization of any of these architectures mentioned above. For example, Web service systems were implemented by combining centralized and distributed architecture. Similarly, cryptocurrency systems (Bitcoin, Ethereum) were implemented using a decentralized and distributed architecture. As discussed earlier, Blockchain runs on a peer-to-peer network. It distributes the ledger information over the peer-to-peer network for verification and validation, avoiding the need for intermediation. This process's three primary access control operations are viewing, sharing, and updating the information. The blockchain system can be categorized into public, private, consortium, and hybrid based on the permissions given for these access privileges [43].

3.2.1 Public Blockchain

Public Blockchain is permissionless, in which any node can join the network without taking permission required by any other node, and exiting from the network at any time is also possible. This concept of joining and leaving without other participants' permission forms peer-to-peer in which all participating nodes are equal. Every node processes the information with the help of a shared copy of the distributed ledger. The transactional information is verified and validated by all the nodes in the network. This process makes the nature of the Blockchain a trustless system, processing without intermediation. Even though the ledger information is given as public, it is secured by cryptographic algorithms. Selecting the node to perform the mining process, which computes the hash value of the block and appends it to the Blockchain, is done by consensus algorithms. In this process, sharing the Blockchain with all the peer nodes and allowing them to exercise their access privileges results in a trilemma trade-off in achieving distribution, decentralization, and privacy preservation.

3.2.2 Private Blockchain

A peer-to-peer network formed for sharing and managing information in a closed environment or enterprise is known as a private blockchain, which falls under the category of private Blockchain. This system will store and share enterprise information with blockchain users. The enterprise information stored will be secured and immutable. This private Blockchain also enables internal information transactions among enterprises. Information management within the organizational enterprise can be implemented using a private blockchain, which eases the execution of business processes. The reliability of the business process system can be improved by implementing private Blockchain in the business enterprise. This private blockchain design introduces the trade-off through several factors, such as decentralization, identity management, access control, and anonymity. Building a private blockchain is done in two ways: i) using Hyberledger and ii) building on a public Ethereum network.

3.2.3 Consortium Blockchain

In consortium blockchain, the peer-to-peer group is formed among the nodes present in the consortium or federation. For example, in the supply chain management application, the participants of this applications are from different organizations. Hence, there is a need to design a system that accommodates the participants from other enterprises while access privileges are restricted to specific nodes in the consortium network. In this approach, all the participating nodes are in the same virtual network, or individual virtual networks are integrated into the consortium blockchain. This implementation also has a trade-off with decentralization, privacy, and anonymity [44].

3.3. Consensus Algorithms

Initially, the development of Blockchain-based implementations, Proof of Work, Proof of Stake, and Proof of Byzantine Fault Tolerance were proposed and used. Later, many other algorithms were developed and used. There are three categories of the proposed consensus algorithms. The categorization employs a concept in which agreement with the nodes is arrived at. The first category is a work-proof-based consensus mechanism, in which a miner node is selected based on the computational power of the nodes. The evaluation of the computational power of the node is done by solving a complex problem. The computational power of the node is directly proportional to the complex work of finding the address of the new block and appending it to the Blockchain. A few examples of this mechanism are PoW, DPPoW, etc. The second category of consensus algorithm is capability-based consensus mechanisms, in which miner nodes are selected using their capability. The capability can be defined by criteria such as service to the community, number of cryptocurrencies being held, and trust established in the network by the node—examples: PoS, DPoS, PoET, PoA, etc. The final category of the consensus mechanism is the Voting-based mechanism. In this mechanism, the mining node is elected to generate a block and append it to the Blockchain [44]. This mechanism avoids unnecessary wastage of computational mechanisms, which happens with work-proof mechanisms. This mechanism also handles Byzantine attacks. Examples are BFT, PBFT, DBFT, etc. Among the above three, the voting-based mechanism is considered more advantageous since i) it handles Byzantine, ii) it provides a high level of decentralized compared to other mechanisms, iii) it is prone to attacks/vulnerability of less than 33% compared to other mechanisms. iv) Produces high throughput and consumes low energy and resources. v) Scalability achieved is comparatively low and can be sorted out through other mechanisms.

3.4 Smart Contracts

Smart contracts are decentralized programs that contain business logic; to execute them, they comprise limited data. Business logic in smart contracts is defined to check the conditions set for the business process to execute automatically. Generally, smart contracts don't need only a blockchain environment; it is an electronic transaction protocol that executes the terms and conditions of the contract. It enables the business's standard contractual conditions to be verified electronically without needing trusted intermediaries. Also, these smart contracts can mitigate malicious and inadvertent transactions [45]. In other words, a smart contract is a secure and auto-executable program comprised of agreement business aspects that are self-running, enforceable, and unstoppable. Some of the features of smart contracts are secured implementation of business logic, auto executable, enforceable, unstoppable, transparent, and unalliable coding. It gets executed based on the data available. One smart contract can be called another smart contract for the execution of business logic. Ethereum smart contracts proposed by Vitalik Butsin in 2014 [46] are one example of a smart contract, which can be created using solidity programming language to build distributed applications. Auto-execution, auto-verifiability, and tamper resistance are features of Ethereum smart contracts.

3.5 Generic Use-cases of Blockchain

Blockchain technology is considered one of the emerging, also known as disruptive technologies, since it has replaced the centralized system. The existing centralized system is limited in establishing Trust as an external factor. In contrast, Trust is an in-build factor in a decentralized environment and is the most significant entity for any system. Building intelligent systems requires Trust as an internal factor to achieve data security and integrity. Moreover, traditional systems are a more time-consuming, costly, and complex process (in terms of risk) since achieving security and establishing Trust is complex. In Blockchain technology-based implementation, the trust factor of the system comes within the system, which can also be known as a trust-less system, as establishing Trust in the system process should be a transparent mechanism. Blockchain system design enhances Trust within the system processes of a specific domain. Blockchain provides a reliable vision of shared, distributed transactions and eradicates the single-point failure of centralized systems. Blockchain technology combines significant concepts like cryptographic techniques, peer-to-peer networking technology, and tamper-evident distributed ledger technology, including fault tolerance, immutability, provenance, and auditability [47]. Blockchain use cases are widespread in various domains: Cryptocurrency, finance and payments, education, health, manufacturing, supply chain, energy, agriculture, etc. Blockchain can be further integrated with proficient technologies [48] such as the Internet of Things, AI, Big data, etc.

3.6 Issues with Blockchain

Transaction information stored in the Blockchain is distributed/shared in the peer-to-peer network, which may be publicly available with all nodes if the blockchain implementation is public. The public nature of the Blockchain will allow any time entry/exit of the nodes. Hence, a malicious node can get added to the network, a data leak may happen, and the system's privacy may fail, leading to the attack of genuine users of the system. Moreover, encryption technology may still pose a threat to tracking related transactions to get the identity. Furthermore, the development of quantum computing has put all cryptographic systems under threat. There is a need to store and share the selective information and update the Blocking Technology implementation with quantum resistance and selective information disclosure algorithms. Blockchain technology implementation is expected to handle the contradiction between security and privacy, which means information systems, services, or any other digital infrastructure should support security aspects without leaking the privacy information in serving mechanisms.

4. DESCRIPTION OF ZKP ALGORITHMS

4.1 ZK-SNARKS – Zero-Knowledge Succinct Non-interactive Argument of Knowledge

This ZKP (non-interactive) model is applied in various applications, including Blockchain. ZK-SNARKs model helps the claimant show the confirmer how to authenticate the information without revealing additional information. ZK-SNARKs are mainly used in scenarios where privacy is a significant factor. ZKP algorithms can be applied in the real world, such as confidentiality and preserving privacy in cryptocurrency transactions, such as ZCASH, decentralized, identity management, secure mobile and remote voting systems, etc. The main features of ZK-SNARKs are their non-interactive nature, compact proof generation, and complex cryptographic algorithms for key generations as security features [49].

Table 3 Comparison of Non-interactive ZKP algorithms

Concepts	ZK-SNARK	ZK-STARK	BULLETPROOF
Size of the proof	Small proof	Large-proof, linear, and quadratic size growth	Small proof and Dynamic proof without compromising security.
Speed	Comparatively faster	Fastest	Slowest
Applications	Used in applications where there is limited storage space. E.g., Blockchain. It is also suitable for limited network transfer speed, E.g., Internet of Things.	Used in applications in which proof size plays a significant role, E.g., Data center management, Cloud computing, Machine Learning, etc.	Used in applications with high-level computing environments, where one claimant creates a proof, many confirmers verify the proof—for example, Blockchain.
Environment	Trusted Setup	A trusted environment is not required.	A trusted environment is not required.

The processes involved in ZK-SNARKs are given as follows. The initial step is to derive public parameters from secret parameters, referred to as standard reference strings. The second step is generating the claimant's and the confirmer's keys. The claimant will generate proofs using the claimant's key, whereas the confirmer's key is used to verify the proof. The elliptic curve cryptography technique is used for cryptographic keys. In the third step, the proof is generated with the following information: i) claimant's key, (ck), ii) generic statement, z iii) private information as a. Proof generated in this step has a relationship among standard reference parameters, generic statement (x) and private information (a). The final proof verification step is done using the confirmer's key, generic statement (x), and proof sent by the claimant. This step verifies that the determined proof is valid.

4.1.2 ZK-STARK - Zero-Knowledge Scalable Transparent Argument of Knowledge

The ZK-STARK method generates proof for the claimant in the same way as ZK-SNARKS and the same for verifying the proof. However, unlike ZK-SNARK, ZK-STARK uses hash function rather than elliptic curve cryptography to generate proof primitives. Hash functions resist quantum attacks, whereas elliptic curve cryptography is more vulnerable to quantum attacks [50]. Implementing ZK-SNARK is possible only with a reliable environmental setup, whereas implementing ZK-STARK is not required.

4.1.3 Bulletproof

The bulletproof algorithm generates proofs for verification like the other two algorithms, ZK-SNARKS and ZK-STARKS. Bulletproof are small-sized proofs in a predefined range that generate standard reference strings and are implemented in a trusted setup. Bulletproof is vulnerable to quantum attacks and finds its use-case anonymously authenticating people. Bulletproof produces fewer commitments and verifies the inner proof to implement unlinkability with source identity. Table 3 illustrates the comparative analysis of Non-interactive ZKP algorithms [51].

4.2 Interactive ZKP

In an interactive model of the ZKP algorithm, the claimant and confirmer will be in synchronous online communication for several sounds of messaging [52]. The steps for the interactive ZKP algorithm are given as follows:

Step 1: The Claimant generates proof known as commitment and sends it to confirmer.

Step 2: The confirmer generates a challenge question on receiving the commitment for verification.

Step 3: The Claimant responds to the challenge with the commitment and generic information.

Step 4: The steps above are repeated until the confirmer accepts the commitment and verifies it as genuine.

5. SYSTEMATIC REVIEW OF USE-CASES OF ZKP MODELS

5.1 Security and Privacy

Abhijeet R. Raipurkar et al. [53] present a Blockchain-based solution model for identity management. Self-sovereign identity is used in decentralized identity management. ZKP-based verification for the claimed identity is done to ensure security and privacy in decentralized identity management. The results of the proposed models prove that the third-party system can efficiently verify the claims through a public network. The proposed system is implemented using PolygonID, Metamask, and ReactJS. Results show that ZKP efficiently manages remote identity, improving user privacy and security. Po-wen Chi et al. [54] have proposed a novel scheme known as blockchain-designated verifier proof (BDVP), which addresses the 'collision problem,' i.e., verifier sharing of the public key to the third party to prove the identity, and solves the problem of when verifier tries to send proofs with all its generated computational transcripts to the third party to proof prover's identity. The proposed technique is analyzed for quantum resistance and compared to other existing ZKP schemes/modules for Blockchain. Results show that BDVP is an efficient technique for privacy-preserving the prover when the implementation is done through Blockchain. Ya-chai Tsai et al. [55] analyze ZKRP (Zero-Knowledge Range Proof) implementation for Bank payments with Blockchain. The proposed ZKRP algorithms pose non-interactive and range flexibility features. Performance evaluation is done by comparing it with other NIZKP algorithms, and results show that the proposed one is more flexible and applicable for Dapps. Max Kobelt et al. [56], the authors have compared various ZKP implementations and designed benchmarking algorithms that aid decision-making. It has two implementations, one proving knowledge of hash preimage using MIMC EdDSA Signature Verification. Chunjie Guo et al. [57] proposed a new scheme, BioAu-SVM+ZKP, allowing users to authenticate themselves to third-party applications without disclosing biometric template-related information. ZKP algorithms produce the evidence utilizing polynomial commitment. Here, SVM is used to classify fingerprints. The efficiency of the proposed algorithms is evaluated by conducting experiments with the reasonable. The efficiency of the proposed algorithms is evaluated by conducting experiments with a reasonable-sized dataset. Gulshan Kumar et al. [58] propose a blockchain-based framework, referred to as BRON, that manages the organization's human resources information globally without any privacy leakage. ZKP algorithms in this paper are used for global verification and data retrieval for various processes in this application without affecting the privacy of the users' data. BRON inculcates ZKP Algorithms for anonymously authenticating the information. BRON uses Proof of Authority as a consensus algorithm and smart contracts for the auto-incentive process. Results show that implementation of the framework produces good throughput and less latency than centralized HRM systems. Prabhat Kumar et al. [59] proposed a blockchain-based healthcare system framework. This framework also includes IoT and Deep learning approaches.

ZKP algorithms were used to achieve secure data transmission and data integrity. The results show that the proposed framework efficiently and effectively secures data transmission. Hamza Baniata et al. [60] propose a fog-enabled blockchain-based credential management framework called PriFoB. The proposed framework in this paper adopts a permissionless blockchain, and a generic model of ZKP is used to enhance privacy. Zilin Liu et al. [61] implement a generalized blockchain-based data-sharing protocol in which data privacy is preserved through ZKP algorithms. Yang Lin et al. [62] propose architecture using Blockchain and ZKP for privacy preservation in advertising information systems. Jiahui Huang et al. [63] utilize a one-way hash-based function for ZKP and ZK-SNARKS for privacy preservation in digital asset transfers. The proposed method in this paper is referred to as ZKchain. Tao Feng, Puyang, et al. [64] have proposed a blockchain-based framework for data privacy, security, and availability using ZKP and smart contracts and secured data-sharing transactions in cloud services. Jialin Zhu et al. [65] analyze privacy-preservation mechanisms for digital certificate management. Junbeom Park and Seongjn Chang [66] have proposed a frame for smart homes using Blockchain, IoT, and ZKP. In this work, ZKP is used to safeguard the public keys of the homework. Xheya Xia et al. [67] propose an efficient anonymous authentication and key agreement scheme with privacy-preserving for smart cities. Sai Kiran Deveraselti et al. [68] propose a ZKP-based data privacy and identity anonymity protocol for data transfer in peer-to-peer networks. Xiao Xu [69] proposes a novel information system based on ZK-SNARKS for managing information on students with disability. Verifying students with a disability using the proposed system is effectively done using ZKP models. This paper also analyses the significance of ZKP models in educational systems. Honglei Li and Weilian Xue [70] propose an e-auction scheme without intermediatory. The system is constructed using Blockchain Technology. Smart Contract technology and a Non-interactive ZKP model are implemented using a bulletproof algorithm. The results show the efficiency of the proposed e-auction scheme regarding privacy preservation, security, and reliability. Yangzhou Cao et al. [71] propose a dual blockchain framework for privacy preservation in vaccine passport systems. This system uses public Blockchain to maintain the supply chain of vaccines and adopts consortium blockchain for verifying and validating passport information using ZKP.

5.2 Multifactor Authentication

Quan Nguyen et al. [72] propose a framework to authenticate users when they want to access their application through a website (third-party system), unreliable device, and network by adding another layer of security, which is known as two-factor authentication. ZKP implements completeness and zero knowledge for the user by allowing them to produce proof of the login credentials. The paper concludes that the proposed framework mitigates hardware keyloggers, software keyloggers, and shoulder surfing attacks. Md. Onais Ahmed et al. [73] analyze the importance of multifactor authentication in securing information in smart city networks. Initially, it illustrates the security and privacy threats of implementing a smart city. The author proposes a new blockchain-based multifactor framework named "BAuth –ZKP" for a security smart city where transactions are verified through ZKP. The proposed MFA mechanism uses a commitment scheme and character count ZKP technique. Saba Khanum and Kurram Mustafa [74] propose an encryption scheme that is a hybridization blind and ring signature process using lattice cryptography. The encrypted data is stored in the block since the blockchain network nodes verify it. The verification scheme employed in the nodes is based on ZKP and is also used to authenticate information and avoid unauthorized data access changes. Dongmeihi et al. [75] proposed reliable medical data and healthcare sharing using Blockchain and ZKP. This smart contract and ZKP model automatically verify and authenticate information without leaks. Chinjie Guo et al. [76] proposed a privacy preservation scheme for fingerprint biometric templates using NIZKP. ZP-SNARKS is in a NIZKP model in which the claimant generates proof with the help of secret and generic information. The proposed system prepares the proof with the length of constants, reducing time and space complexity. Yudai Xue and Jinsong wang [77] propose a blockchain system for implementing traceability in Business applications to enhance cooperation among business entities. Traceable information is authenticated using Blockchain and zero-knowledge proof method for privacy-preserving. Transparency and reliability during the traceability process are achieved using smart contracts. Firas Hamila et al. [78] propose a non-interactive zero-knowledge proof model by transforming an interactive protocol. The transformed protocol is used in a two-factor authentication scheme of an IoT application.

5.2 Anonymity

Samia Boutalbi et al. [79] proposed a protocol to handle communication and information exchange among wireless devices in IoT networks in an anonymous way. The protocol is implemented through Blockchain and ZKP. Results obtained after the simulation depicted lower energy consumption and reduced communication costs. EunSeong Boo [80] proposes a framework using Blockchain for payments with a lightning concept. In this, anonymity in payments was achieved through ZKP. The LiteZKP concept is implemented using the Merkle tree to manage the computational complexity. The performance of LiteZKP is analyzed by implementing it in a device with limited configuration. The results show that LiteZKP outperforms up to 50% of the traditional blockchain implementations. Lasse Herkind et al. [81] proposed a blockchain-based cash flow management architecture. ZKP algorithms such as ZK-SNARKS and Bulletproof ensured privacy-based verification and anonymity for confidential transactions. Richard Banach [82] proposes a punishment-not-rewarding mechanism for Blockchain network participation for those dealing with services related to blockchain maintenance. Privacy and efficiency become trade-offs when implementing a punishment mechanism; privacy concerns are trade-off entities. ZKP's ZK-SNARKS algorithm addresses this trade-off. Yachao Huo [83] proposes a protocol in which two parties can compute or process together to achieve functionality in a circuit application while maintaining. Their inputs are private using ZKP. This proposed solution is also resilient to quantum. Jin Cheng Ma and Fe Li [84] propose a methodology combining ZKP and encryption model to protect the privacy of both parties involved in cross-border trade and maintain confidentiality in transaction amount and anonymity.

5.4 Identity Management

Marrico Barros et al. [85] propose a model to authenticate vaccinated people for different pathogens without revealing their identity. The self-solvenier identity model has been used for identity management, and ZKP algorithms play a role in ensuring the privacy of the shared health credential. Canling Wang et al. [86] A trust-based authorized access control scheme using the Blockchain and ZKP model has been proposed. Smart contracts were used to automatize trust verification and active access permissions by ensuring user privacy. The performance evaluation shows that the proposed scheme is more secure, reliable, and efficient than existing access control mechanisms. Sid El Kafhali [87] analyses blockchain-based voting systems and discusses privacy preservation and identity management methods. ZKSMP (Zero Knowledge set membership proof) code verifies the voter's identity without revealing private data. Munivel and Kannammal [88] have proposed a solution to mitigate phishing attacks in mobile applications. The confirmer verifies the user's identity using a based authentication protocol, where the actual password is not sent to the verifier. Results show the proposed scheme effectively mitigates phishing attacks in mobile applications using cloud computing. Zhiming Song et al. [89] propose a digital identity verification and management using Blockchain Technology, SSI, and ZKP.

In this model, a non-interactive ZKP algorithmic model, ZK-SNARKS, is used. ZK-SNARKS uses the quadratic arithmetic technique on an elliptic curve to generate a proof. The same is verified by the confirmer efficiently and effectively. Ying Zhang [90] proposed a blockchain technology and smart contracts-based framework to reserve rights for methods and innovations produced in the music education process. Jie Li et al. [91] present a privacy-preserving authentication scheme for the Internet of Vehicles. ZKP models were for decentralized identity management. Here, the implementation of the Blockchain enhances the efficiency of the authentication process. The following figure 5 illustrates the percentage of research works reviewed in various use cases of ZKP.

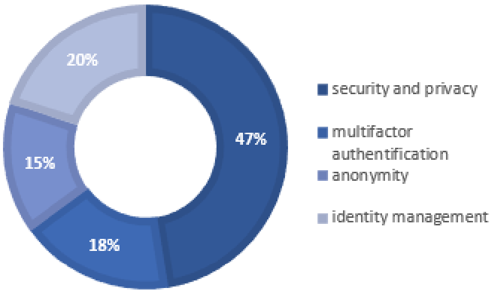

Figure 5. Illustration of Percentage of research works reviewed in various use cases of ZKP

5.5 Uses of ZKP Models in Blockchain Implementations

Blockchain-based implementations suffer from security and privacy issues and anonymous authentication. ZKP models play a significant role in preserving privacy and implementing anonymity with blockchain systems. Authors of this paper [92] propose the ZKP model combined with ring signatures for privacy preservation in healthcare systems implemented using Blockchain. Further, Xijian Xu et al. [93] propose ZKP mechanisms based on Pederson Commitments, which generate verifiable proofs to protect sensitive information during a trading phase of the payment system implemented using Blockchain. The implementation of ZKP is done by using the steps of processing ZK-SNARKS. Javier Jose Diaz Rivera et al. [94] propose a zero-trust architecture, a distributed authentication mechanism that utilizes Blockchain for multifactor authentication. In this architecture, ZKP models are used to handle blockchain privacy issues that arise with Blockchain. The authors of this paper [95] propose a privacy-preserving authentication scheme that uses Blockchain in payment systems. Privacy-preservation of sensitive user data is achieved using zero-knowledge proofs. Smart contracts were used to process the fund flow among the merchants. Duc Anh Luong and Joug Hwan Park [96] in their work, propose identity management for anonymous authenticating users implemented using Blockchain. In this work, user authentication is done without revealing their real identities using a zero-knowledge proof model known as ZK-SNARKS—this model also hybrids with other techniques, such as Shamir's secret sharing.

6. CHALLENGES IN THE IMPLEMENTATION OF ZKP MODELS

ZKP algorithms are more flexible and reliable to be implemented for real-world problems. Quantum threats need to be considered when implementing ZKP algorithms. Few research papers have discussed quantum attacks and post-quantum cryptographic solutions. According to the analysis in the research papers, even during quantum attacks, the confirmer's privacy is preserved, and this property is very suitable for blockchain implementations. More advanced potential ZKP algorithms must be constructed while considering the quantum resistance property. Further, ZKP algorithms in Blockchain debilitate its scalability, decreasing its applications' broadness. This property is mainly affected when the implementation platform has limited resources like IoT. Privacy and usability should be balanced and managed effectively, especially in applications like finance, health care, etc. The massive deployment of blockchain systems with privacy preservations must solve interoperability aspects. In general, the optimization of ZKP algorithms to strengthen the proof can be done with various methods to improve the efficiency and applications of the model. For example, Bugs in generated proofs are possible, which makes any imposter produce false proof, and the confirmer may also verify and give positive results. Similar challenges generate proof and solve challenges posted by the confirmer to the claimant [R36]. Lattice-based cryptography can be used to construct the ZKP algorithm—optimizations concerning the reduction in proof generation time. ZKP provides higher privacy and security than other methods. ZKP, combined with blockchain implementations, provides resilience against various attacks, such as denial of service (attack against availability) and modification (attack against confidentiality). ZKP integrated with Blockchain for privacy preservation reduces the cost of computations and communications.

7. CONCLUSION

In digitizing business or digital transformation, various implementations like user authentication, identity management, security and privacy-preservation of the data, and anonymity play a crucial role. Also, digital business transformation is achieved through blockchain technology, which has the property of openness and transparency but suffers from privacy issues. This paper thoroughly studies the use cases of ZKP models and their effectiveness in achieving anonymous authentication, decentralized identity management, security, and privacy preservation. Further, the paper introduces Blockchain, its types, features, and issues related to privacy. Furthermore, it shows how the ZKP model solves the privacy-related problems with Blockchain. Finally, this paper presents the analysis of ZKP algorithms and research areas. The future scope of this study could be extended by reviewing and analyzing blockchain integration with various other cutting-edge technologies to achieve data security and privacy solutions, which may result in practical application and facilitate a smooth business continuation process.

8. ACKNOWLEDGMENT

This research was not funded by any grant.

9. CONFLICTS OF INTEREST

The authors have no conflicts of interest to declare.

7. REFERENCES

[1] Mohameden Dieye. Pierre Valiorgue. Jean-Patrick Gelas. El-Hacen Diallo. Parisa Ghodous. Frédérique Biennier. Éric Peyrol. 2023. A Self-Sovereign Identity Based on Zero-Knowledge Proof and Blockchain. IEEE Access. Volume 11. 2023. DOI: 10.1109/ACCESS.2023.3268768

[2] Yinjie Gong, Yifei Jin, Yuchan Li, Ziyi Liu, Zhiyi Zhu. 2022. Analysis and comparison of the main zero-knowledge proof scheme. International Conference on Big Data, Information and Computer Network. IEEE Xplore. DOI 10.1109/BDICN55575.2022.00074

[3] Imran Bashir, Mastering Blockchain Second Edition, 2018 Packt Publishing

[4] Olusogo Popoolaa. Marcos Rodriguesb. Jims Marchanga. Alex Shenfieldb. Augustine Ikpehaib. Jumoke Popoolaa. 2024. A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & Blockchain: Problems, challenges, and solutions. Blockchain: Research and Applications. Volume 5. 100178.

[5] Ibrar Yaqoob. Khaled Salah. Mueen Uddin. Raja Jayaraman. Mohammed Omar. and Muhammad Imran. 2020. Blockchain for Digital Twins: Recent Advances and Future Research Challenges. IEEE Network 2020. DOI: 10.1109/MNET.001.1900661

[6] Seila Berciroric Ramic, Ehlimana Cogo, Irfan Prazina, Emir Cogo, Muhamed Turkanvic, Razija Turcinhozic, Mulahasanovic, Sasa Mrdovic. Selective Disclosure of Information. ICT EXPRESS – (ARTICLE IN PRESS)

[7] Xiaoqiang Sun, F. Richard Yu, Peng Zhang, Zhiwei Sun, Weixin Xie, and Xiang Peng. 2021. A Survey on Zero-Knowledge Proof in Blockchain. IEEE Network July/ August 2021. DOI: 10.1109/MNET.011.2000473

[8] Zhigang Chen, Yuting Jiang, Xinxia Song and Liqun Chen. 2023. A Survey on Zero-Knowledge Authentication for Internet of Things. Electronics 2023, 12, 1145. https://doi.org/10.3390/electronics12051145

[9] Anatoly Konkin · Sergey Zapechnikov. 2023. Zero-knowledge proof and ZK-SNARK for private blockchains. Journal of Computer Virology and Hacking Techniques (2023) 19:443–449 https://doi.org/10.1007/s11416-023-00466-1

[10] Luzhon, Abebe, Diro, Akansha Saini, Shahriar Kaisar, Pham Cong Heip. 2024. Leveraging Zero Knowledge Proofs For Blockchain Based Identity Management: A Survey of Advancements, Challenges, and Opportunities. Journal of Information Security and applications 80 (2024) 103678.

[11] Raul Ramos Fernandez. 2024. Evaluation of trust service and software product regimes for zero-Knowledge proof development under eIDAS 2.0, Computer law and security review, Volume 53, July 2024, 105968.

[12] Vid Keršič. Sašo Karakatič. Muhamed Turkanović. 2024. On-chain zero-knowledge machine learning: An overview and comparison. Journal of King Saud University - Computer and Information Sciences. Volume 1. 102207

[13] Ikram Nur Muharam. Iis P. Tussyadiah. Albert Nsom Kimbu. 2024. Decentralising Airbnb: Testing the acceptability of blockchain-based sharing economy systems. Tourism Management. Volume. 102. 104871.

[14] Goldwasser, S. Micali, S and Rackoff. C. 1985. The knowledge complexity of interactive proof-systems. In Proc. 17th Annu. ACM Symp. Theory Comput.(STOC).NewYork, NY, USA: Association for Computing Machinery, pp. 291–304, DOI: 10.1145/22145.22178.

[15] DeSantis A., Micali S., and Persiano G. 1988 Non-interactive zero-knowledge proof systems. In Advances in Cryptology (CRYPTO). C. Pomerance. Ed. Berlin, Germany: Springer, pp. 52–72.

[16] Goldreich O. and Kushilevitz. E. 1988 A perfect zero-knowledge proof for a problem equivalent to discrete logarithm. In Advances in Cryptology (CRYPTO) (Lecture Notes in Computer Science). Springer. Vol. 403. pp. 57–70. DOI: 10.1007/0-387-34799-2_5.

[17] Gennaro R. Micciancio D. and Rabin T. 1998. An efficient non-interactive statistical zero-knowledge proof system for quasi-safe prime products. Cryptol. ePrint Arch., Tech. Rep. 1998/008, 1998. https://eprint.iacr.org/1998/008

[18] Schnorr C. P. 1990. Efficient identification and signatures for smart cards. Advances in Cryptology(CRYPTO). G.Brassard, Ed. NewYork, NY, USA: Springer. 1990. pp. 239–252.

[19] Persiano G. and Visconti I. 2006. On non-interactive zero-knowledge proofs of knowledge in the shared random string model. in Mathematical Foundations of Computer Science, R. Královič and P. Urzyczyn, Eds. Berlin, Germany: Springer. pp. 753–764.

[20] Peikert. C. and Vaikuntanathan. V. 2008 Non-interactive statistical zero-knowledge proofs for lattice problems. In Advances in Cryptology (CRYPTO). D.Wagner.Ed.Berlin. Germany: Springer. pp. 536–553.

[21] Xagawa K and Tanaka K. 2009. Zero-knowledge protocols for NTRU: Application to identification and proof of plaintext knowledge. in Provable Security, J. Pieprzyk and F. Zhang, Eds. Berlin, Germany: Springer. pp. 198–213.

[22] Xie. X. Xue R. and Wang M. 2013. Zero-knowledge proofs from ring-LWE. In Cryptology and Network Security, M. Abdalla, C. Nita-Rotaru, and R. Dahab, Eds. Cham, Switzerland: Springer. pp. 57–73.

[23] Cabarcas. D. Demirel. D. Göpfert. F. Lancrenon. J. and Wunderer T. 2015. An unconditionally hiding and long-term binding post-quantum commitment scheme. Cryptol. ePrint Arch., Tech. Rep. 2015/628, 2015. https://eprint.iacr.org/2015/6282

[24] Martín-Fernández. F. Caballero-Gil. P. and Caballero-Gil C. 2016. Authentication based on non-interactive zero-knowledge proofs for the Internet of Things. Sensors. Vol.16. No.1. pp. 75.

[25] Baum. C. Damgård. I. Lyubashevsky V. Oechsner. S. and Peikert C. 2018. More efficient commitments from structured lattice assumptions. In Security and Cryptography for Networks (Lecture Notes in Computer Science), Vol.11035, D.Catalanoand R.D.Prisco, Eds. Amalfi, S A, Italy: Springer. Sep. pp. 368–385.

[26] Alshameri H.M. and Kumar P. 2019. An efficient zero-knowledge proof based identification scheme for securing software defined network. Scalable Comput., Pract. Exper. Vol. 20. No. 1. pp. 181–189.

[27] Lyubashevsky. V. Nguyen N. K. and Plançon M. 2022. Lattice-based zero knowledge proofs and applications: Shorter, simpler, and more general. IACR Cryptol. ePrint Arch., Tech. Rep. 284/2022, 2022.

[28] Li peng. Wei Feng. Zheng Yau Yafeng Li. Xiakang Zhou. Shohei Shimizu. 2021. Privacy preservation in Blockchain: A survey. Digital Communication and Network. Volume 7. pp.295-307.

[29] Ju-Chun Yen. Tawei Wang. 2021. Stock price relevance of voluntary disclosures about blockchain technology and cryptocurrencies. International Journal of Accounting Information Systems Volume 40. March 2021. 100499

[30] Ujkan Q. Bajra. Ermir Rogova. Sefer Avdiaj. 2024. Cryptocurrency blockchain and its carbon footprint: Anticipating future challenges. Technology in Society. Volume 77. June 2024, 102571.

[31] Lingyue Zhang. Zongyang Zhang. Tianyu Li. Shancheng Zhang. 2024. A consensus-based solution for cryptocurrency arbitrage bots in intelligent Blockchain. Digital Communications and Networks(DCN). Under Press.

[32] Jiawei Zheng. Xuewen Dong. Wei Tong. Qihang Liu. Xinghui Zhu. 2019. Blockchain-based secure digital asset exchange scheme with QoS-aware incentive mechanism. 2019 IEEE 20th International Conference on High-Performance Switching and Routing (HPSR). IEEE Xplore.

[33] Muhammad Shoaib Farooq. Usman Iftikhar. Adel Khelifi. 2022. A Framework to Make Voting System Transparent Using Blockchain Technology. IEEE Access. Volume 11. 59959-69. DOI: 10.1109/ACCESS.2022.3180168

[34] Shaoliang Peng. Xing Hu. Jinglin Zhang. Xiaolan Xie. Chengnian Long. Zhihui Tian. Hongbo Jiang. 2020. An Efficient Double-Layer Blockchain Method for Vaccine Production Supervision. IEEE Transactions on Nanobioscience, VOL. 19, NO. 3, JULY 2020.

[35] Isabel Román-Martínez. Jorge calvillo-arbizu. Vicente J. Mayor-Gallego. Germán Madinabeitia-Luque. Antonio J. Estepa-Alonso. Rafael M. Estepa-Alonso. 2023 Blockchain-Based Service-Oriented Architecture for Consent Management, Access Control, and Auditing. IEEE Access. Volume 11. 2023.

[36] Weiqi Dai. Chunkai Dai. Kim-Kwang Raymond Choo. Changze Cui. Deiqing Zou. Hai Jin. 2020 SDTE: A Secure Blockchain-Based Data Trading Ecosystem. IEEE Transactions on Information Forensics and Security, VOL. 15, 2020.

[37] Olusogo Popoolaa. Marcos Rodriguesb. Jims Marchanga. Alex Shenfieldb, Augustine Ikpehaib. Jumoke Popoolaa. 2024. A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & Blockchain: Problems, challenges, and solutions. Blockchain: Research and Applications. Volume 5. 2024. 100178.

[38] Weilin Zheng. Zibin zheng. Xiangping Chen. Kemian Dai. Peishan Li. Renfei Che 2019 NutBaaS: A Blockchain-as-a-Service Platform. IEEE Access. Volume 7. 2019. 134423-433.

[39] Chia-Huag Liao. Xue-Qin Guan. Jen-Hao Cheng. Shyan-Ming Yuan. 2022. Blockchain-based identity management and access control framework for open banking ecosystem. Future generation computing systems. 2022. Volume 135, pp. 450-466.

[40] Yi Gong. Boyuan Yu. Lei Yang. Fanke Meng. Lei Liu et al. 2024. Toward next-generation networks: A blockchain-based approach for core network architecture and roaming identity verification. S2352-8648(24)00099-3, Digital Communications and Networks. Doi: https://doi.org/10.1016/j.dcan.2024.08.008.

[41] Jorge Bernal Bernabe. Jose Luis Canovas. Jose l. Hernandez-ramos. Rafael Torres Moreno. And Antonio Skarmeta. 2019. Privacy-Preserving Solutions for Blockchain: Review and Challenges. IEEE ACCESS. Volume 7. 164909-940. 2019.

[42] Ansif Arooj. Muhammad Shoaib Farooq. Tariq Umer. 2022. Unfolding the blockchain era: Timeline, evolution, types, and real-world applications. Journal of Network and Computer Applications. Volume 207. 103511

[43] Ka Ching Chan. Xujuan Zhou. Raj Gururajan. Xiong Zhou. Mustafa Ally. Michael Garinder. 2019 Integration of Blockchains with Management Information Systems. International Conference on Mechatronics, Robotics and Systems Engineering (MoRSE) 4-6 December 2019, Bali, Indonesia

[44] Bahareh Lashkari. Petr Musilek 2021. A Comprehensive Review of Blockchain Consensus Mechanisms. IEEE Access. vol. 9, pp. 43620-43652, doi: 10.1109/ACCESS.2021.3065880

[45] Ahmed Kosba. Andrew Miller. Elaine Shi. Zikai Wen. Charalampos Papamanthou. 2016. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. 2016 IEEE Symposium on Security and Privacy. IEEE Computer Society. DOI 10.1109/SP.2016.55

[46] Vitalik Butterin. 2014 Ethereum White Paper: A next-generation smart contract and Decentralized application platform.

[47] Nitin Upadhyay. 2024. Business models for the Blockchain: An empirical analysis. Digital Business. 2024. Volume 4. Issue 2. 100082.

[48] Salman Saleem Virani. 2024. Blockchain end-user adoption and societal challenges: Exploring privacy, rights, and security dimensions. IET Blockchain. Willey Publications. 2024. Volume 1. pp. 1–15.

[49] Abla Smahi. Hui Li. Yong Yang. Xin Yang. Ping Lu. Yong Zhong. Caifu Liu. 2023. BV-ICVs: A privacy-preserving and verifiable federated learning framework for V2X environments using Blockchain and zkSNARKs. Journal of King Saud University – Computer and Information Sciences Volume. 35 (2023) 101542.

[50] Bjorn Oude Roelink Mohammed El-Hajj Dipti Sarmah, 2024. Systematic review: Comparing zk-SNARK, zk-STARK, and bulletproof protocol for privacy-preserving authentication, SecurityPrivacy, pp. 1-50, Wiley, https://doi.org/10.1002/spy2.401.

[51] Mohammed El-Hajj and Bjorn Onde Roelink. 2024. Evaluating Efficiency of ZK-SNARK, ZK-STARK, and Bulletproof in Real-world Scenarios: A Benchmark Study. Information. Volume 15. 463.

[52] Suhui Liu. Liquan Chen. Hongtao Yu. Shang Gao. Huiyu Fang. 2023. BP-AKAA: Blockchain-enforced Privacy-preserving Authentication and Key Agreement and Access Control for IIoT. Journal of Information Security and Applications. Volume 73. March 2023. 103443

[53] Abhijeet R. Sheryas Bobde. Anurag Tripahi. Mohit Sahu. 2023. Digital Identity System using Blockchain based Self Sovereign Identity and Zero Knowledge Proof. 21st OITS International Conference on Information Technology. (OCIT 2023). IEEE Xplore. DOI: 10.1109/OCIT 59427. 2023. 10430981.

[54] Po-Wen Chi. Yun-Hsiu Lu. and Albert Guan. 2023 A Privacy-Preserving Zero-Knowledge Proof for Blockchain. Volume 11. Pp. 85108-117 IEEE access 2023. DOI: 10.1109/ACCESS.2023.3302691

[55] Ya-Che Tsai. Raylin Tso. Zi- Yuan Liu, Kung Chen. 2019. An Improved Non-Interactive Zero-Knowledge Range Proof for Decentralized Applications. IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON). DOI 10.1109/DAPPCON.2019.00025

[56] Max Kobelt. Michael Sober. Stefan Schulte. 2023. A Benchmark for Different Implementations of Zero-Knowledge Proof Systems. IEEE International Conference on Blockchain (Blockchain). IEEE Access. pp. 33-40. DOI 10.1109/Blockchain60715.2023.00015

[57] Chunjie Guo. Lin You. Xinggyu Li. Gengram Hu. Shengguo Wang. Chengfang Cao. 2024. A novel biometric authentication scheme with privacy protection based on SVM and ZKP. Computer & Security. Elsevier. (144) 103995.

[58] Gulsan Kumar. Rahul Saha, Manish Gupta, Taithoon Kim. 2024 BRON: A Blockchained framework for privacy information retrieval in human resource management. Heilyon 10 e33393.

[59] Prabhat Kumar. Randhir Kumar. Govind P. Gupta C. Rakesh Tripathic. Alireza Jolfaeid. Najmul Islame A.K.M. 2023. A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system. Journal of Parallel and Distributed Computing. Elsevier. Vol. 172. pp. 69-93.

[60] Hamza Banita. Attila Kertesz. 2022. PriFoB: a Privacy-aware Fog-enhanced blockchain based system for Global Accreditation and Credential Verification. Journal of Network and Computer Applications. Vol. 205. (2022) 103440.

[61] Zilin Liu. Anjia Yang. Huang Zeng. Changkun Jiang. and Li Ma. A. 2023. Generalized Blockchain-Based Government Data Sharing Protocol. Hindawi Security and Communication Networks Vol. 2023, Article ID 9998433, 9 pages https://doi.org/10.1155/2023/9998433.

[62] Yangzhou Cao. Jiageng Chen and Yajun Cao. 2022. Blockchain-Based Privacy-Preserving Vaccine Passport System, Hindawi Security and Communication Networks Volume 2022, Article ID 4769187, 16 pages https://doi.org/10.1155/2022/4769187

[63] Jiahui Huang. Teng Huang. Huanchun Wei. Jiehua Zhang. Hongyang Yan. Duncan S.Wong. HaiboHu. 2024. zkChain: A privacy-preserving model based on zk-SNARKs and hash chain for efficient transfer of assets. Trans Emerging Tel Tech. 2024. 35. e4709. https://doi.org/10.1002/ett.4709

[64] Tao Feng. Pu Yang. Chunyan Liu. Junli Fang. and Rong Ma. 2022. Blockchain Data Privacy Protection and Sharing Scheme Based on Zero-Knowledge Proof. Hindawi Wireless Communications and Mobile Computing, Article ID 1040662, 11 pages https://doi.org/10.1155/2022/1040662

[65] Jialin Zhu. Wenlong Feng. Wang Zhong. Mengxing Huang. and Siling Feng. 2023. Research on Privacy Protection of Technology Service Transactions Based on Blockchain and Zero-Knowledge Proof. Hindawi Wireless Communications and Mobile Computing, Article ID 6196872, 7 pages https://doi.org/10.1155/2023/6196872

[66] Junbeom Park and Seongju Chang. 2023. Secure device control scheme with Blockchain in a smart home. Measurement and Control. 2023. Vol. 56(3-4) pp. 546–557.

[67] Xueya Xia. Sai Ji Pandi Vijaya kumar. Jian Shen. and Joel. Rodrigues J. P. C. 2021. An efficient anonymous authentication and key agreement scheme with privacy-preserving for smart cities. International Journal of Distributed Sensor Networks.Vol. 17(6)

[68] Sai Kiran Deverasetti. Anjila Neupane. Indranil Roy. Reshmi Mitra and Bidyut Gupta. 2024. Establishing Trust using Zero Knowledge Succinct Proof in Peer-to-peer Data Transfer. Proceedings of 36th International Conference on Computer Applications in Industry and Engineering. EPiC Series in Computing Volume 97. pp. 91–100.

[69] Xiao Xu. 2024. Zero-knowledge proofs in education: a pathway to disability inclusion and equitable learning opportunities. Smart Learning Environments https://doi.org/10.1186/s40561-024-00294-w

[70] Honglei Li and Weilian Xue. 2021. A Blockchain-Based Sealed-Bid e-Auction Scheme with Smart Contract and Zero-Knowledge Proof. Hindawi Security and Communication Networks Volume 2021. Article ID 5523394, 10 pages https://doi.org/10.1155/2021/5523394

[71] Yangzhou Cao,Jiageng Chen and Yajun Cao, Blockchain-Based Privacy-Preserving Vaccine Passport System, Hindawi Security and Communication Networks, Article ID 4769187, 16 pages https://doi.org/10.1155/2022/4769187

[72] Quan Nguyen. Mikhail Rudoy. Arjun Srinivasan. 2014. Two Factor Zero Knowledge Proof Authentication System. 6.857 Spring 2014 Project.

[73] Md. Onais Ahmad. Gautami Tripathi. Farheen Siddiqui. Mohammad Afshar Alam. Mohd Abdul Ahad. Mohd Majid Akhtar. and Gabriella Casalino. 2023. BAuth-ZKP—A Blockchain-Based Multifactor Authentication Mechanism for Securing Smart Cities. Sensors. Vol 23. 2757. https://doi.org/10.3390/s23052757

[74] Saba Khanum, Khurram Mustafa. 2023. A lattice-based blind ring signature scheme for sensitive data protection in blockchain applications. Concurrency Computat Pract

Exper. 35. e7835. 14 pages. https://doi.org/10.1002/cpe.7835

[75] Dongmei Li. Xiaohui Ke. Xiaomei Zhang. Yujin Zhang. 2024. A trusted and regulated data trading scheme based on Blockchain and zero-knowledge proof, IET Blockchain. 1–13, Willey Publications.

[76] Chunjie Guo. Lin You. Xingyu Li. Gengram Hu. Shenggguo Wang. Chengtang Cao. 2024. A Novel biometric authentication scheme with privacy protection based on SVM and ZKP. Computers and security, Vol. 144, 103995.

[77] Yudai Xue and Jinsong Wang. 2022. Design of a Blockchain-Based Traceability System with a Privacy-Preserving Scheme of Zero-Knowledge Proof. Hindawi Security and Communication Networks, Article ID 5842371, 12 pages https://doi.org/10.1155/2022/5842371

[78] Firas Hamila. Mohammad Hamad. Daniel Costa Salgado. Sebastian Steinhorst. 2024. Enhancing security in Fiat–Shamir transformation-based non-interactive zero-knowledge protocols for IoT authentication, International Journal of Information Security. Vol. 23. pp. 1131–1148 https://doi.org/10.1007/s10207-023-00779-8

[79] Samia Boutalbi. Julio C´esar P´erez Carc´ıa. Abderrahim Benslimane. 2021. Blockchain-based secure Handover for IoT using Zero-Knowledge Proof protocol. GLOBECOM 2021 – IEEE Global Communication Conference. IEEE Xplore. 2021. DOI: 10.11091/GLOBECOM 46510.9685733.

[80] EunSeong Boo. Joongheon Kim. and JeongGil Ko. 2022. LiteZKP: Lightening Zero-Knowledge Proof-Based Blockchains for IoT and Edge Platforms. IEEE SYSTEMS JOURNAL. MARCH 2022. VOL. 16, NO. 1.

[81] Lasse Herskind. Alberto Giaretta. Michele De Donno. NicolaDragoni. 2019. BitFlow: Enabling real-time cash-flow evaluations through Blockchain, Concurrency Computat Pract Exper. 2019. Vol 32. e5333. John Wiley & Sons, Ltd.

[82] Richard Banach. 2021. Blockchain applications beyond the cryptocurrency casino: The Punishment not Reward blockchain architecture, Concurrency Computatation Pract Exper. John Wiley & Sons, 2021. Vol. 33. e5749 pp. 1-23 https://doi.org/10.1002/cpe.5749

[83] YachaoHuo. ZongquZhao. Panke Qin Shujing. Wang Chengfu Zheng. 2024 Post-quantum secure two-party computing protocols against malicious adversaries, Concurrency Computat Pract Exper. John Wiley & Sons Ltd 2024. Vol. 36. e7923. pp. 1of14 https://doi.org/10.1002/cpe.7923

[84] Jiahui Huang. TengHuang. HuanchunWei. JiehuaZhang. HongyangYan. DuncanS.Wong. HaiboHu. 2024. zkChain: A privacy-preserving model based on zk-SNARKs and hashchain for efficient transfer of assets, TransEmergingTelTech. John Wiley & Sons, Ltd. Vol. 35. e4709. 11 pages. https://doi.org/10.1002/ett.4709

[85] Mauricio de. Vasconcelos Barros. Frederico. Schardong. Ricardo Felipe Custódio. 2022. Leveraging Self-Sovereign Identity, Blockchain, and Zero-Knowledge Proof to Build a Privacy-Preserving Vaccination Pass. arXiv:2202.09207v1

[86] Canling Wang,Wei Wu, Fulong Chen ,Hong Shu,2 Ji Zhang, Yuxuan Zhang,Taochun Wang, Dong Xie,1and Chuanxin Zhao, 2024. A Blockchain-Based Trustworthy Access Control Scheme for Medical Data Sharing, Hindawi IET Information Security. Article ID 5559522, 16 pages https://doi.org/10.1049/2024/5559522

[87] Said El Kafhali, 2024. Blockchain-Based Electronic Voting System: Significance and Requirements, Hindawi Mathematical Problems in Engineering. Article ID 5591147, 17 pages https://doi.org/10.1155/2024/5591147

[88] Munivel E and Kannammal A, 2019. New Authentication Scheme to Secure against the Phishing Attack in the Mobile Cloud Computing, Hindawi Security and Communication Networks. Article ID 5141395, 11 pages https://doi.org/10.1155/2019/5141395

[89] Zhiming Song , Guiwen Wang, Yimin Yu,and Taowei Chen, 2022. Digital Identity Verification and Management System of Blockchain-Based Verifiable Certificate with the Privacy Protection of Identity and Behavior, Hindawi Security and Communication Networks, Article ID 6800938, 24 pages https://doi.org/10.1155/2022/6800938

[90] Ying Zhang, 2022. Increasing Cyber Defense in the Music Education Sector Using Blockchain Zero-Knowledge Proof Identification, Hindawi Computational Intelligence and Neuroscience, Article ID 9922167, 7 pages https://doi.org/10.1155/2022/9922167

[91] Jie Li, Yuanyuan Lin, Yibing Li, Yan Zhuang and Yangjie Cao, 2024. BPA: A Novel Blockchain-Based Privacy-Preserving Authentication Scheme for the Internet of Vehicles, Electronics 13, 1901. https://doi.org/10.3390/electronics13101901

[92] Maryam Nasr Esfahani, Behrouz Shahgholi Ghahfarokhi. Shahram Etemadi Borujeni. 2024. Blockchain-based end-to-end privacy-preserving scheme for IoT-based healthcare systems. Springer. Volume 80, pages 2067–2127.

[93] Xijian Xu. Jun Wu. 2024. Bridging Economic Model and Blockchain: ZKP Empowered Privacy Preservation payment channel with intermediatory Pricing. International Wireless Communications and Mobile computing, (IWCMC). IEEE Xplore. DOI: 10.1109/IWCMC 61514.2024.10592598.

[94] Javier Jose Diaz Rivera, Afaq Muhammad, Wang-Cheol Song. 2024. Securing digital identity in the Zero trust Architecture, A Blockchain approach to privacy-focussed multifactor authentication. IEEE Communication Society. Volume 5. pp. 1-24.

[95] Devishree Naidu, Bhusan Wanjari, Rohit Bhojwani, Saurabh Suchak, Rahul Baser, Niranjan Kumar Ray. 2023. Efficient Smart contract for Privacy Preserving Authentication in Blockchain using Zero Knowledge Proof. 21st PITS International Conference on Information Technology. IEEE Xplore. DOI:10:1109/OCIT 59427.2023/10430710.

[96] DUC ANH LUONG AND JONG HWAN PARK. 2022. Privacy-Preserving Identity Management System on Blockchain Using Zk-SNARK. IEEE Access. Volume 11. DOI: 10.1109/ACCESS.2022.3233828.