Towards Understanding the Application Areas of Zero Knowledge Proof: A Comprehensive Analysis

Laura Atmanavičiūtė[1], Saulius Masteika[2]

[1]PhD student, Vilnius University, Kaunas Faculty, Institute of Social Sciences and Applied Informatics, 8 Muitinės St., Kaunas, LT-44280, Lithuania, laura.atmaviciute@knf.vu.lt
[2]Professor, Vilnius University, Kaunas Faculty, Institute of Social Sciences and Applied Informatics, 8 Muitinės St., Kaunas, LT-44280, Lithuania, saulius.masteika@knf.vu.lt

Abstract. As privacy and security concerns increase, Zero Knowledge Proof (ZKP) technology offers a promising solution for secure digital verification. ZKP addresses key privacy and security challenges across individual, business, and public sectors by enabling data protection without revealing sensitive information. The aim of this study is to analyse ZKP's application areas by reviewing current literature and case studies, examining its strengths, limitations, and potential risks. Findings highlight the capability of ZKP to enhance privacy, security, and verification processes across various fields, including blockchain technology, identity authentication, secure data sharing, and digital voting systems. The paper provides a balanced perspective on ZKP's benefits and challenges, including computational complexity and scalability issues. By suggesting practical use cases, this work aims to contribute to a deeper understanding of how ZKP technology can support innovation across various industries while addressing critical privacy and security needs.

Key words: zero knowledge proof, ZKP, blockchain, data privacy, digital identity.

Introduction

Relevance of the article

As digital interactions across the world expand, privacy and security challenges become increasingly critical, driving the need for innovative solutions to protect sensitive information. Among the technologies emerging to address these concerns, Zero Knowledge Proof (ZKP) offers a unique approach that enables secure verification without revealing sensitive data. It is particularly significant for organizations managing sensitive data and complying with data protection regulations. Although ZKP is built on a strong theoretical foundation, its practical application is still in its early stages, with challenges such as scalability and computational efficiency limiting its broader implementation. The exploration of this technology not only advances scientific understanding but also holds great potential for solutions in different fields, such as blockchain, identity verification, and secure communication.

Problem investigation level

In authentication systems, ZKPs are recognised for enhancing security by allowing user verification without exposing sensitive data, as demonstrated by Jaafar and Samsudin (2010). Similarly, noninteractive ZKPs have been explored to improve efficiency in cryptographic operations like key exchanges and secure communications (Wu, & Wang, 2014). In blockchain technology, ZKPs have shown promise in balancing privacy and transparency, notably in applications such as tax document validation and anonymous cryptocurrency transactions (Sasson et al., 2014). ZKPs have also been applied to secure voting systems, providing solutions for voter anonymity while maintaining election integrity (Neziri et al., 2022), and in physical security scenarios like nuclear warhead verification (Philippe et al., 2016). While research on ZKPs has addressed critical privacy and security challenges, significant gaps remain in fully exploring their potential and limitations.

Scientific problem

What are the key application areas of ZKPs, and what are the current challenges and opportunities in their practical implementation across these areas? Can ZKPs, successfully applied in cryptocurrencies, also be used in other fields such as social sciences, healthcare, education, and related areas?

Object of the article is the application areas of ZKP.

https://doi.org/10.15388/Gronskis.2025.1

***Aim of the article* is** to analyse ZKP's application areas by summarising current literature and case studies.

***Objectives of the article*:**

1. To examine the foundations of ZKPs and their role in addressing privacy and security concerns.
2. To apply SWOT analysis for ZKPs, highlighting its strengths and weaknesses.
3. To analyse application areas of ZKPs and identify priority fields.

***Methods of the article*:** This study employs a review of the literature and case studies to explore the foundations and advancements of ZKPs. SWOT analysis is applied to highlight its strengths, weaknesses, opportunities, and threats across applications. Case studies are analysed to evaluate their benefits and challenges.

1. The foundations and concepts of Zero-Knowledge Proofs

1.1. Introduction to Zero-Knowledge Proofs

ZKPs are cryptographic protocols that enable a prover to demonstrate the truth of a statement to a verifier without revealing any additional information. Introduced by Goldwasser, Micali, and Rackoff in 1985, ZKPs have become a cornerstone of modern cryptography, offering robust privacy and security across a range of applications (Groth, 2010; Fisch et al., 2014).

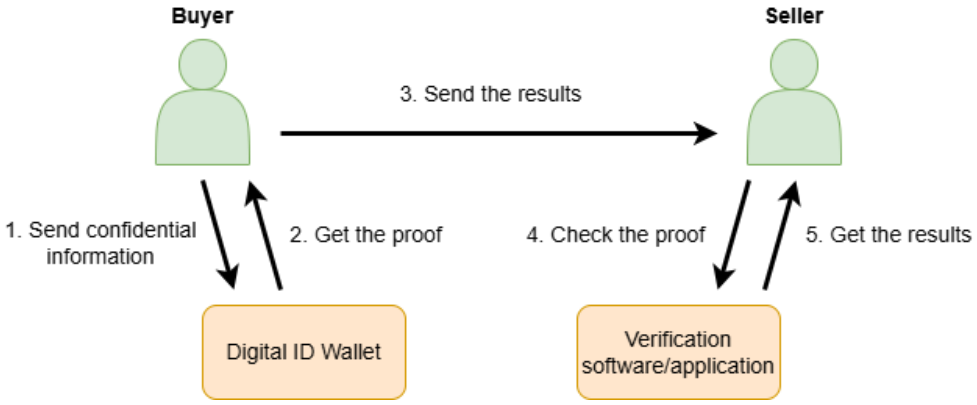
The fundamental properties of ZKPs can be categorised into three key attributes: completeness, soundness, and zero-knowledge. These properties ensure that ZKPs can be reliably used in scenarios requiring both security and privacy.

1. Completeness ensures that an honest prover can always convince an honest verifier of the truth of a statement if the prover possesses the correct information. This property guarantees that the protocol functions as intended under normal circumstances (Robert et al., 2020; Groth, 2010).
2. Soundness ensures that no cheating prover can convince the verifier of a false statement, except with negligible probability. This property is essential for maintaining the integrity of the proof system, as it prevents dishonest behaviour from succeeding (Backes, & Unruh, 2010; Escala, & Groth, 2014).
3. The zero-knowledge property is the most defining characteristic of ZKPs. It ensures that the verifier learns nothing beyond the validity of the statement. This attribute is vital for preserving privacy, as it allows the prover to demonstrate knowledge of a secret without disclosing any information about the secret itself. Applications of this property include secure authentication protocols and privacy-preserving transactions in cryptocurrencies like Zcash (Li et al., 2010; Gabay et al., 2019; Sasson et al., 2014).

These properties ensure privacy and trust of the protocol. To address different practical use cases' needs, researchers have developed distinct types of ZKPs, each optimised for specific applications and constraints. ZKPs are generally categorised into interactive ZKPs, and non-interactive ZKPs (NIZKs).

Interactive ZKPs involve a back-and-forth communication process between the prover and the verifier. For instance, the Schnorr protocol relies on iterative challenges, making it suitable for secure authentication where dynamic exchanges enhance proof integrity (Yue, 2023). In contrast, NIZKs eliminate the need for interaction by enabling the prover to generate a single proof that can be verified independently. This is often achieved using cryptographic hash functions or the Fiat-Shamir heuristic, which streamlines the process and reduces communication overhead (Blum et al., 2019). NIZKs are widely used in scenarios requiring efficiency, such as blockchain systems and cryptocurrencies. For example, Zcash employs zk-SNARKs to ensure transaction privacy while maintaining computational efficiency (Sasson et al., 2014; Bünz et al., 2018).

Figure 1 illustrates an example of an NIZK. In this scenario, the buyer transmits confidential data to a digital identity wallet, which generates a proof. This proof is subsequently forwarded to the seller's verification software, where it is validated, ensuring the authenticity of the data without disclosing the underlying information.



Source: created by the authors.

Fig. 1. Zero Knowledge Proof in retail

1.2. Cryptographic foundations and recent innovations

ZKPs rely on mathematical principles and computational hardness assumptions, such as the discrete logarithm problem (DLP) and the difficulty of factoring large integers. These foundations secure ZKP systems by making it infeasible to derive secrets from public data (Bellizia et al., 2021), (Roy, 2018). Commitment schemes, essential to ZKPs, ensure binding (preventing alteration) and hiding (concealing values until revealed), enabling applications like secure voting and authentication (Escala & Groth, 2014; Benhamouda et al., 2015). While more rigorous mathematical details may be essential for specialised applications, this section focuses primarily on conceptual and practical aspects relevant to privacy and security.

Advanced techniques like elliptic curve cryptography (ECC) enhance ZKP efficiency, offering strong security with smaller key sizes and faster computations (Damgård et al., 2012). Recent innovations such as zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) and zk-STARKs (Scalable Transparent Arguments of Knowledge) have transformed ZKP applicability.

Zk-SNARKs are lightweight, producing compact proofs independent of the complexity of computations. They are well-suited for blockchain applications, where minimising on-chain data is crucial (Chen et al., 2022). Their non-interactive nature simplifies verification by eliminating the need for back-and-forth communication between the prover and verifier, reducing computational overhead in decentralized systems (Ben-Sasson et al., 2015). However, zk-SNARKs require a trusted setup phase, introducing potential vulnerabilities if the setup process is compromised.

Zk-STARKs address this limitation by eliminating the need for trusted setups. Instead, they employ collision-resistant hash functions, enhancing transparency and security (Thibault et al., 2022). Zk-STARKs are highly scalable, handling large computations efficiently without increasing proof size or verification time, and are considered resilient to quantum attacks due to their independence from elliptic curve cryptography (Thibault et al., 2022). These features make zk-STARKs particularly suitable for high-throughput applications, such as decentralised finance and privacy-preserving smart contracts.

Both zk-SNARKs and zk-STARKs support private transactions, enabling user anonymity while maintaining blockchain integrity. Their ability to reduce computational demands facilitates faster and more cost-effective blockchain operations (Bespalov et al., 2021).

2. SWOT analysis and application areas of Zero-Knowledge Proofs

This section combines a SWOT analysis with an integrated discussion of the key application areas of ZKPs, providing a comprehensive view of the strengths, weaknesses, opportunities, and threats related to this technology. The analysis demonstrates how each SWOT factor is displayed in different contexts.

2.1. SWOT analysis

ZKPs, like all technologies, come with both strengths and weaknesses. Therefore, a SWOT analysis is applied to examine these factors, offering a clearer understanding of the potential impact of ZKPs on privacy, security, and emerging applications, while also addressing the challenges they face.

ZKPs excel in privacy preservation by allowing users to prove knowledge or identity without revealing sensitive information (Dieye et al., 2023). They also enhance security, as users can prove possession of a secret without exposing it, which is essential in financial transactions and access control (Park & Chang, 2022). In practice, the privacy-enhancing features of ZKPs benefit numerous application areas: for instance, healthcare platforms can safeguard patient records, and financial services can verify transactions without disclosing sensitive details. Non-interactive ZKPs (NIZKPs) further improve efficiency by reducing communication rounds, making them ideal for IoT and other high-latency environments (Wu & Wang, 2014).

ZKPs are also robust against spoofing attacks, ensuring the authenticity of users and data (Tangka et al., 2022). Their flexibility allows integration in various fields, such as secure blockchain transactions and privacy-preserving systems (Dieye et al., 2023). Finally, they foster trust in decentralized applications by enabling secure verification without revealing private data (Tangka et al., 2022).

Despite their advantages, ZKPs face complexity and high computational overhead, which can be prohibitive in resource-constrained environments like IoT (Gabay et al., 2019). This complexity primarily stems from the advanced cryptographic operations required to generate and verify proofs, demanding significant processing power, specialised expertise, and carefully chosen parameters. In large-scale or time-sensitive contexts such as payment networks or supply chain tracking, these computational demands can increase costs and reduce performance, creating further risks for deployment. In domains such as healthcare or regulated finance, where compliance and resource constraints intersect, even minor misconfigurations can undermine both security and performance. As a result, adopting ZKPs often involves specialised training, robust testing, and ongoing maintenance to mitigate these risks.

They also require a trusted setup for certain variants like zk-SNARKs, posing a risk if the setup is compromised (Banerjee, 2020). ZKPs rely on security assumptions, such as the hardness of computational problems, which may be threatened by advances in quantum computing (Broadbent et al., 2020). Furthermore, ZKPs may not be expressive enough to handle more complex assertions (Li et al., 2010), and traditional models with multiple interactions can introduce latency issues (Groth, 2010). Finally, their implementation complexity requires careful design to prevent vulnerabilities (Backes & Unruh, 2010). In domains such as healthcare or regulated finance, where compliance and resource constraints intersect, even minor misconfigurations can undermine both security and performance. Thus, adopting ZKPs often involves specialised training, robust testing, and ongoing maintenance to mitigate these risks.

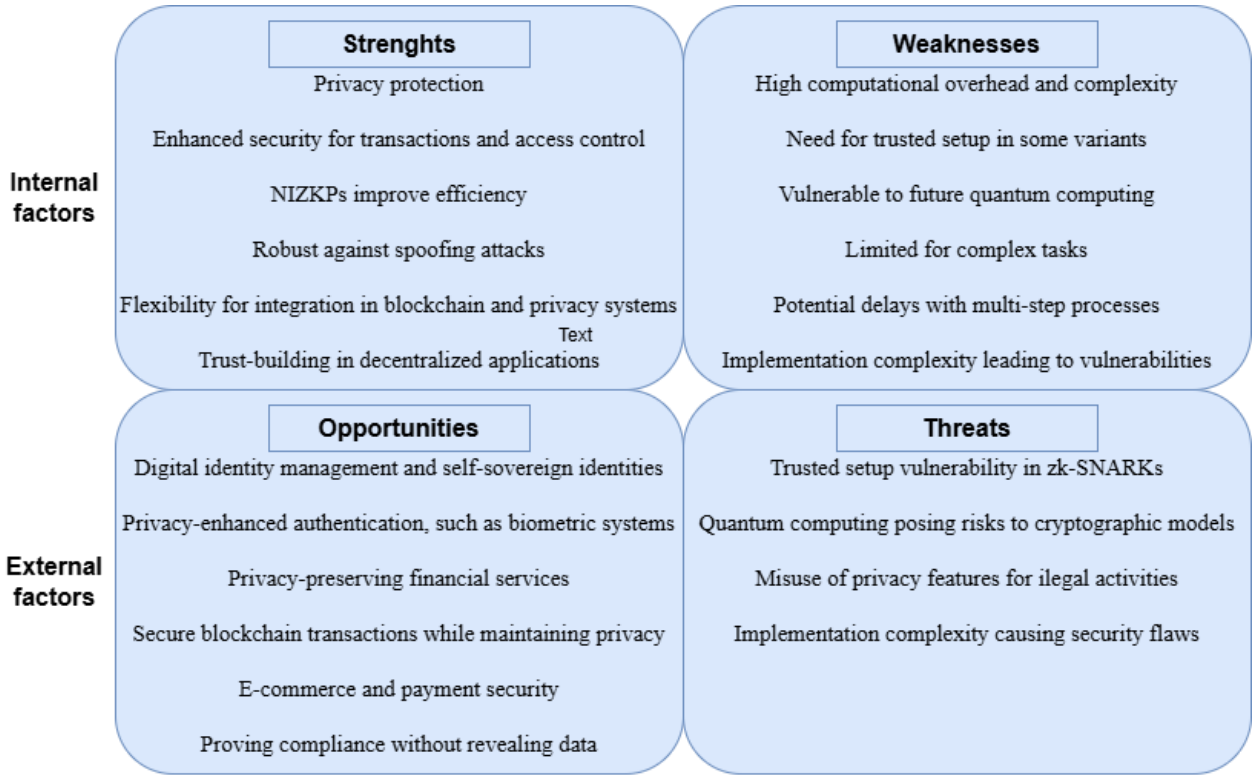
ZKPs offer significant potential in digital identity management, enabling self-sovereign identities without exposing sensitive data (Dieye et al., 2023). They can enhance authentication by providing private proofs, as in biometric systems (Guo et al., 2022). In financial services, ZKPs enable privacy-preserving credit checks or transaction verification, allowing institutions to confirm creditworthiness without disclosing full financial histories (Yuan et al., 2021).

They are also pivotal for secure blockchain transactions, enabling privacy while maintaining transparency (Bai et al., 2022). In e-commerce and payment security, ZKPs ensure confidentiality during digital transactions (Broadbent et al., 2020), and organisations can use them for regulatory compliance by proving adherence to regulations without revealing sensitive data (Takaragi et al., 2020). Supply chain management is another growing area: ZKPs can enhance trust, traceability, and product authenticity while safeguarding competitive or proprietary information.

A major threat to ZKPs is the trusted setup vulnerability, particularly in zk-SNARKs, where a compromised setup can expose the system to attack (Broadbent et al., 2020). Advances in quantum computing threaten the security assumptions underlying ZKPs, as quantum algorithms

could potentially break current cryptographic models (Broadbent et al., 2020). ZKPs also have a potential for misuse, as their privacy-enhancing capabilities can be exploited for illicit activities (Tangka et al., 2022). Lastly, implementation complexity remains a barrier, as flawed deployments can lead to security vulnerabilities (Backes & Unruh, 2010). Complexity risks vary across sectors: in IoT, low-power devices may struggle with intense cryptographic computations; in enterprise systems, integrating ZKPs with legacy software may require major architectural changes (Hamadeh & Tyagi, 2021).

The SWOT analysis of ZKPs revealed that this protocol has various potential applications, but also has its challenges, as shown in Fig. 2.



Source: created by the authors.

Fig. 2. SWOT analysis of ZKPs

2.2. Application areas and case studies

This subsection delves deeper into how ZKPs have been adopted in practice across multiple domains. It shows how the strengths, weaknesses, opportunities, and threats discussed in the SWOT analysis occur in practice, highlighting both the benefits and the challenges faced in actual application areas.

One of the earliest and most impactful uses of ZKPs has been in **cryptocurrencies**. Zcash, one of the most well-known cryptocurrencies, launched in 2016, uses zk-SNARKs to enable transactions without revealing sensitive details like the sender, receiver, or amount (Banerjee et al., 2020), (Zhang et al., 2020). This approach ensures confidentiality while maintaining transaction validity, exemplifying the role of ZKPs in cryptocurrency privacy (Biryukov & Feher, 2019).

ZKPs also play a vital role in **digital identity systems**. Decentralized identity platforms, such as Microsoft ION, implement selective proof-sharing mechanisms (DIF, 2024). Self-sovereign identity systems allow users to control and selectively disclose their personal data (Dieye et al., 2023). Guo et al. (2022) proposed a zk-SNARK-based biometric identification system, ensuring user authentication without exposing sensitive biometric information. These solutions demonstrate the privacy advantages of ZKPs in real-world contexts, but they also underscore the complexity challenge that arises when integrating with legacy identification systems.

In **healthcare**, ZKPs facilitate secure identity management and data sharing. The Health-zkIDM system integrates blockchain and ZKPs to protect medical records and identity verification (Bai et al., 2022). Similarly, ZKPs in financial services enable privacy-preserving creditworthiness verification, enhancing user privacy during financial transactions (Yuan et al., 2021). Such deployments demonstrate the opportunity to maintain patient confidentiality but also reveal potential weaknesses if cryptographic overhead strains medical IT systems with limited resources.

ZKPs also enhance privacy-preserving **voting systems**. Miao (2023) proposed a voting system ensuring voter eligibility and ballot secrecy. Protocols like DEMOS-2 and mix-nets provide cryptographic guarantees for vote secrecy and verifiability without compromising privacy (Kiayias et al., 2015), (Buchmann et al., 2013). Locher and Haenni (2015) further enhanced online voting systems with ZKP-based anonymity and result integrity. The ability to prove voter authenticity without revealing personal data exemplifies the technology's strengths, while complexities, such as usability and large-scale deployment, can pose a threat to reliability.

In **supply chain management**, ZKPs have been utilized to enhance privacy while ensuring traceability and authenticity. Multi-chain frameworks and zk-SNARK-based protocols verify product authenticity and ensure secure ownership transfers without revealing sensitive data (Zhang et al., 2023), (Vijayalakshmi et al., 2022). Applications like PrivChain address food fraud and enhance trust in supply chain transactions (Malik et al., 2021). This combines the opportunity to maintain proprietary data secrecy with the threat of implementation errors in complex cross-border supply networks.

In **Internet of Things (IoT) security**, ZKPs improve authentication and data integrity. ZK-rollups enable efficient batch verification while maintaining confidentiality (Xin et al., 2023). Electric vehicle authentication and IoT fog computing frameworks use ZKPs to ensure secure, resource-efficient operations (Gabay et al., 2019), (VG, 2024). Privacy-preserving data provenance models further enhance IoT network security (Hamadeh & Tyagi, 2021). However, high computational costs on low-power IoT devices demonstrate the weaknesses related to ZKP complexity.

Overall, ZKPs demonstrate significant potential across diverse fields by enhancing privacy and security while enabling verification without revealing sensitive information. As highlighted in the SWOT analysis, their success hinges on addressing complexities, preparing for emerging cryptographic threats, and leveraging new opportunities (such as scalable proof systems) in real-world implementations. In digital identity, they address critical privacy challenges, such as age and credential verification, proof of identity, passwordless authentication, ownership and income verification, and secure transactions. These capabilities highlight their promise for privacy-preserving digital identity solutions. Future work will be focused on identifying the most suitable proof systems for practical deployment in real-world digital identity applications.

Conclusions

1. The theoretical analysis confirms that ZKPs significantly enhance digital privacy and security, especially in scenarios requiring confidential verification. The study confirms that ZKPs are well-suited for applications where confidential verification is critical. The study shows that non-interactive approaches, like zk-SNARKs and zk-STARKs, effectively address scalability and computational efficiency, making them promising for blockchain and DeFi implementations. Additionally, zk-STARKs incorporate quantum-resistant properties, strengthening their capacity to secure future-proof privacy solutions. This underscores ZKPs growing importance as a foundation for privacy-preserving systems across diverse sectors.
2. The SWOT analysis highlights ZKPs' strengths in privacy preservation and data security, demonstrating particularly effective integration within digital identity and blockchain environments. However, the weaknesses – such as high computational costs, trusted setup vulnerabilities, and emerging quantum threats – remain serious challenges. Despite these obstacles, the analysis indicates significant opportunities for ZKPs in areas like privacy-preserving financial services and regulatory compliance, provided that careful design and

robust implementation minimize potential risks.

3. Based on the case studies and literature review, digital identity stands out as the most critical application domain for ZKPs, driven by escalating demands for secure, private authentication methods. The ability to prove credentials or transaction validity without divulging sensitive information positions ZKPs as a transformative solution for identity verification. While cryptocurrency, voting systems, and supply chain management also present notable opportunities, digital identity emerges as the top priority for advancing ZKP research and deployments, reflecting the urgent need for strong privacy protection in contemporary identity systems.

References

1. Backes, M., & Unruh, D. (2010). Computational Soundness of Symbolic Zero-Knowledge Proofs*. *Journal of Computer Security*, *18*(6), 1077–1155. Retrieved from https://doi.org/10.3233/jcs-2009-0392.
2. Bai, T., Hu, Y., He, J., Fan, H., & An, Z. (2022). Health-zkIDM: A Healthcare Identity System Based on Fabric *Blockchain and Zero-Knowledge Proof. Sensors*, *22*(20), 7716. Retrieved from https://doi.org/10.3390/s22207716.
3. Banerjee, A., Clear, M., & Tewari, H. (2020). Demystifying the Role of zk-SNARKs in Zcash. Retrieved from https://doi.org/10.48550/arxiv.2008.00881.
4. Bellizia, D., Mrabet, N.E., Fournaris, A.P., Pontié, S., Regazzoni, F., Standaert, F.X., … Valea, E. (2021). Post-Quantum Cryptography: Challenges and Opportunities for Robust and Secure HW Design. *2021 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, 1–6. Retrieved from https://doi.org/10.1109/dft52944.2021.9568301.
5. Benhamouda, F., Krenn, S., Lyubashevsky, V., & Pietrzak, K. (2015). Efficient Zero-Knowledge Proofs for Commitments from Learning with Errors over Rings. *Lecture Notes in Computer Science*, 305–325. Retrieved from https://doi.org/10.1007/978-3-319-24174-6_16.
6. Ben-Sasson, E., Chiesa, A., Green, M., Tromer, E., & Virza, M. (2015). Secure Sampling of Public Parameters for Succinct Zero Knowledge Proofs. 287–304. Retrieved from https://doi.org/10.1109/sp.2015.25.
7. Bespalov, Y., Garoffolo, A., Kovalchuk, L., Nelasa, H., & Oliynykov, R. (2021). Probability Models of Distributed Proof Generation for zk-SNARK-Based Blockchains. *Mathematics*, *9*(23), 3016. Retrieved from https://doi.org/10.3390/math9233016.
8. Biryukov, A., & Feher, D. (2019). Privacy and Linkability of Mining in Zcash. Retrieved from https://doi.org/10.1109/cns.2019.8802711.
9. Blum, M., Feldman, P., & Micali, S. (2019). Non-Interactive Zero-Knowledge and Its Applications. *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*. Retrieved from https://doi.org/10.1145/3335741.3335757.
10. Broadbent, A., Ji, Z., Song, F., & Watrous, J. (2020). Zero-Knowledge Proof Systems for QMA. *SIAM Journal on Computing*, *49*(2), 245–283. Retrieved from https://doi.org/10.1137/18m1193530.
11. Buchmann, J., Demirel, D., & Graaf, J.V.D. (2013). Towards a Publicly-Verifiable Mix-Net Providing Everlasting Privacy. *Financial Cryptography and Data Security*, 197–204. Retrieved from https://doi.org/10.1007/978-3-642-39884-1_16.
12. Bünz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., & Maxwell, G. (2018). Bulletproofs: Short Proofs for Confidential Transactions and More. *2018 IEEE Symposium on Security and Privacy (SP)*, 315–334. Retrieved from https://doi.org/10.1109/sp.2018.00020.
13. Chen, T., Lu, H., Kunpittaya, T., & Luo, A. (2022). A Review of zk-SNARKs. Retrieved from https://doi.org/10.48550/arxiv.2202.06877.
14. Dieye, M., Valiorgue, P., Gelas, J., Diallo, E., Ghodous, P., Biennier, F., … Peyrol, E. (2023). A Self-Sovereign Identity Based on Zero-Knowledge Proof and Blockchain. *IEEE Access*, *11*, 49445–49455. Retrieved from https://doi.org/10.1109/access.2023.3268768.
15. DIF, Decentralized Identity Foundation. (2024). ION: A Decentralized Identifier Implementation. *GitHub*. Retrieved from https://github.com/decentralized-identity/ion.
16. Escala, A., & Groth, J. (2014). Fine-Tuning Groth-Sahai Proofs. *Public-Key Cryptography – PKC 2014*, 630–649. Retrieved from https://doi.org/10.1007/978-3-642-54631-0_36.
17. Fisch, B., Freund, D., & Naor, M. (2014). Physical Zero-Knowledge Proofs of Physical Properties. *Advances in Cryptology – CRYPTO 2014*, 313–336. Retrieved from https://doi.org/10.1007/978-3-662-44381-1_18.
18. Gabay, D., Cebe, M., & Akkaya, K. (2019). On the Overhead of Using Zero-Knowledge Proofs for Electric Vehicle Authentication. *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. Retrieved from https://doi.org/10.1145/3317549.3326325.
19. Groth, J. (2010). Short Non-Interactive Zero-Knowledge Proofs. *Advances in Cryptology – ASIACRYPT 2010*, 341–358. Retrieved from https://doi.org/10.1007/978-3-642-17373-8_20.
20. Guo, C., You, L., & Hu, G. (2022). A Novel Biometric Identification Scheme Based on Zero-Knowledge Succinct Noninteractive Argument of Knowledge. *Security and Communication Networks*, *2022*, 1–13. Retrieved from https://doi.org/10.1155/2022/2791058.

21. Hamadeh, H., & Tyagi, A.K. (2021). An FPGA Implementation of Privacy Preserving Data Provenance Model Based on PUF for Secure Internet of Things. *SN Computer Science, 2*(2). Retrieved from https://doi.org/10.1007/s42979-020-00428-0.
22. Jaafar, A. M., & Samsudin, A. (2010). Visual Zero-Knowledge Proof of Identity Scheme: A New Approach. *2010 Second International Conference on Computer Research and Development*. Retrieved from https://doi.org/10.1109/iccrd.2010.38.
23. Kiayias, A., Zacharias, T., & Zhang, B. (2015). DEMOS-2: Scalable E2E Verifiable Elections without Random Oracles. *In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. Retrieved from https://doi.org/10.1145/2810103.2813727.
24. Li, H., Xu, H., Li, B., & Feng, D. (2010). On Constant-Round Zero-Knowledge Proofs of Knowledge for NP-Relations. *Science China Information Sciences, 53*(4), 788–799. Retrieved from https://doi.org/10.1007/s11432-010-0071-3.
25. Locher, P., & Haenni, R. (2015). Verifiable Internet Elections with Everlasting Privacy and Minimal Trust. 74–91. Retrieved from https://doi.org/10.1007/978-3-319-22270-7_5.
26. Malik, S.A., Dedeoglu, V., Kanhere, S.S., & Jurdak, R. (2021). PrivChain: Provenance and Privacy Preservation in Blockchain enabled Supply Chains. Retrieved from https://doi.org/10.48550/arxiv.2104.13964.
27. Miao, Y. (2023). Secure and Privacy-Preserving Voting System Using Zero-Knowledge Proofs. *Applied and Computational Engineering, 8*(1), 328–333. Retrieved from https://doi.org/10.54254/2755-2721/8/20230181.
28. Neziri, V., Shabani, I., Dervishi, R., & Rexha, B. (2022). Assuring Anonymity and Privacy in Electronic Voting with Distributed Technologies Based on Blockchain. *Applied Sciences. 12*. 5477. Retrieved from https://doi.org/10.3390/app12115477.
29. Park, J., & Chang, S.H. (2022). Secure Device Control Scheme with Blockchain in a Smart Home. *Measurement and Control, 56*(3–4), 546–557. Retrieved from https://doi.org/10.1177/00202940221105855.
30. Philippe, S., Goldston, R., Glaser, A., & d'Errico F. (2016). A Physical Zero-Knowledge Object-Comparison System for Nuclear Warhead Verification. *Nat Commun 7*, 12890. Retrieved from https://doi.org/10.1038/ncomms12890.
31. Robert, L., Miyahara, D., Lafourcade, P., & Mizuki, T. (2020). Physical Zero-Knowledge Proof for Suguru Puzzle. *Lecture Notes in Computer Science*, 235–247. Retrieved from https://doi.org/10.1007/978-3-030-64348-5_19.
32. Roy, P. (2018). On the Abundance of Large Primes with Small B-Smooth Values for p-1: An Aspect of Integer Factorization. *International Journal on Computer Science and Engineering, 10*(1), 7–13. Retrieved from https://doi.org/10.21817/ijcse/2018/v10i1/181001006.
33. Sasson, E.B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin. *2014 IEEE Symposium on Security and Privacy*. Retrieved from https://doi.org/10.1109/sp.2014.36.
34. Tangka, G.M.W., Delviolin, E.O., & Chou, H. (2022). Zero-Knowledge Proof Application in Ecommerce Payment. *Indonesian Scholars Scientific Summit Taiwan Proceeding, 4*, 69–75. Retrieved from https://doi.org/10.52162/4.2022162.
35. Thibault, L.T., Sarry, T., & Hafid, A. (2022). Blockchain Scaling Using Rollups: A Comprehensive Survey. *IEEE Access, 10*, 93039–93054. Retrieved from https://doi.org/10.1109/access.2022.3200051.
36. VG, P., Babu, B.R., & Pydala, B. (2024). BlockFog: A Blockchain-based Framework for Intrusion Defense in IOT Fog Computing. *Scalable Computing: Practice and Experience, 25*(3), 1950–1962. Retrieved from https://doi.org/10.12694/scpe.v25i3.2686.
37. Vijayalakshmi, M., Shalinie, S. M., Yang, M. H., Lai, S., & Luo, J. (2022). A Blockchain-Based Secure Radio Frequency Identification Ownership Transfer Protocol. *Security and Communication Networks*, 2022, 1–12. Retrieved from https://doi.org/10.1155/2022/9377818.
38. Wu, H., & Wang, F. (2014). A Survey of Noninteractive Zero Knowledge Proof System and Its Applications. *The Scientific World Journal*, 2014, 1–7. Retrieved from https://doi.org/10.1155/2014/560484.
39. Xin, L., Zhang, Y., Huang, C., Xing, B., Chen, L., Hu, D., … Chen, Y. (2023). An Access Control System Based on Blockchain with Zero-Knowledge Rollups in High-Traffic IoT Environments. *Sensors, 23*(7), 3443. Retrieved from https://doi.org/10.3390/s23073443.
40. Yuan, K., Yan, Y., Xiao, T., Zhang, W., Zhou, S., & Jia, C. (2021). Privacy-Protection Scheme of a Credit-Investigation System Based on Blockchain. *Entropy, 23*(12), 1657. https://doi.org/10.3390/e23121657.
41. Yue, M. (2023). Examining Schnorrs Protocol in the Context of Zero-Knowledge Proofs. *Theoretical and Natural Science, 14*(1), 27–32. Retrieved from https://doi.org/10.54254/2753-8818/14/20240870.
42. Zhang, B., Xu, J., Wang, X., Zhao, Z., Chen, S., & Zhang, X. (2023). Research on the Construction of Grain Food Multi-Chain Blockchain Based on Zero-Knowledge Proof. *Foods, 12*(8), 1600. Retrieved from https://doi.org/10.3390/foods12081600.
43. Zhang, Z., Li, W., Liu, H., & Liu, J. (2020). A Refined Analysis of Zcash Anonymity. *IEEE Access, 8*, 31845–31853. Retrieved from https://doi.org/10.1109/access.2020.2973291