Theory and Practice of Science and Technology
2025, VOL. 6, NO. 7, 168-172
DOI: 10.47297/taposatWSP2633-456932.20250607

Research on Technologies of Blockchain and Their Cross-Domain Applications: Systematic Exploration Based on Zero-Knowledge Proof and Regulatory Requirements

Jinhua Zhou

Beijing Normal - Hong Kong Baptist University, College of Science and Technology, Zhuhai, Guangdong, 519087, China

ABSTRACT

Blockchain technology has garnered widespread attention across various sectors such as finance, healthcare, and government services due to its decentralized, tamper-resistant, and traceable nature. However, the conflict between privacy protection and regulatory compliance has emerged as a key barrier to its further development. Zero-Knowledge Proof (ZKP), as a next-generation privacy-enhancing technology, offers unique advantages in achieving "verifiability without disclosure." This paper systematically reviews the core technologies of blockchain and existing privacy protection methods, providing an in-depth comparison of mainstream ZKP protocols (e.g., zk-SNARK, zk-STARK, and PLONK) in terms of efficiency, security, and generality. It highlights how ZKP has become a technological pillar for privacy-compliant blockchain systems. The paper then explores practical application models of ZKP in cross-domain scenarios such as healthcare, finance, e-government, and supply chains, and further analyzes potential mechanisms through which ZKP can fulfill regulatory requirements such as AML, KYC, and auditing while preserving privacy. Finally, it discusses current technical bottlenecks and future development trends, including the integration of ZKP with AI, secure hardware, and post-quantum cryptography, as well as strategic frameworks for building a scalable and regulation-friendly blockchain ecosystem.

KEYWORDS

Blockchain; Privacy protection; Practical application models; Regulatory requirements; Development trends

1 Overview of zero-knowledge proof technology and protocol comparison

1.1 Theoretical origins and engineering evolution of zero-knowledge proofs

Zero-Knowledge Proof (ZKP) is one of the fundamental tools in modern cryptography, first proposed by Goldwasser, Micali, and Rackoff in 1985. Its core idea is to allow a prover to convince a verifier of the truth of a statement without revealing any additional information. A standard ZKP system must satisfy three fundamental properties: completeness, zero-knowledge, and soundness . ZKP protocols typically rely on the verifier making random challenges, requiring multiple rounds of interaction between the prover and verifier. The prover must first provide a commitment and then respond to the verifier ' s challenge based on a random value. If the statement is true, the prover can consistently pass the challenges; otherwise, they can only pass individual rounds with a certain probability. The verifier accepts the proof only when the probability of correctness becomes sufficiently high, yet learns nothing about the statement itself from the commitments or responses.

1.2 Structure principles and comparisons of mainstream zkp protocols

1.2.1 Zk-SNARK: succinct non-interactive zero-knowledge proof of knowledge

Zk-SNARK (Zero-Knowledge Succinct Non-interactive Argument of Knowledge) was first proposed by Bitansky et al. in 2012, with its theoretical foundation traceable back to the definition and expansion of interactive zero-knowledge proofs by Goldwasser et al. in the 1980s . With the deepening of research in computational complexity theory, algebraic geometry coding, and homomorphic encryption, zk-SNARK has gradually evolved into a practical non-interactive zero-knowledge proof system applicable to NP languages. This protocol uses structural encoding (such as QAP) to transform computations into verifiable constraint systems and employs bilinear pairings to construct a succinct knowledge argument. Its core lies in generating a public reference string (CRS) through a one-time.

1.2.2 Zk-STARK: scalable transparent zero-knowledge proof

To address the inherent limitations of zk-SNARK in terms of trusted setup and quantum resistance, Ben-Sasson et al. proposed the zk-STARK (Zero-Knowledge Scalable Transparent Argument of Knowledge) protocol in 2018 based on the ZKPCP theory. This protocol abandons pairing encryption and instead relies on collision-resistant hash functions, Merkle tree commitments, and the IOP (Interactive Oracle Proof) model. By abstracting the prover's behavior into an algebraic intermediate representation (AIR), it achieves a fully trustless, quantum-safe, and highly scalable zero-knowledge proof

system.

1.2.3 Plonk: a simple protocol for general updateable reference strings

Between the excellent efficiency of zk-SNARK and the security and transparency of zk-STARK, Gabizon et al. proposed the PLONK (Permutations over Lagrange-bases for Oecumenical Noninteractive Arguments of Knowledge) protocol in 2019. Its core design concept is to establish a universal proof system that supports any circuit structure, while improving construction efficiency and maintaining a reasonable security boundary. PLONK adopts polynomial constraint expressions based on Lagrange interpolation bases and a permutation verification mechanism at the technical level. It achieves compatibility and reusability for different circuits through structured reference string (SRS) referencing.

In practical applications, PLONK has been widely adopted by multiple ZK-Rollup and privacy computing projects. For example, the Aztec protocol uses PLONK to build an optional auditing-based privacy payment mechanism, and the Mina protocol uses PLONK to achieve chain-wide SNARK compression, keeping the block size stable at the several KB range. Looking forward to the future, PLONK will become the basic module of large-scale recursive ZKP systems, helping to build a modular, plug-and-play, and regulatory-compatible ZKP ecosystem.

These three mainstream protocols demonstrate a clear evolutionary trajectory of ZKP technology from theoretical research to industrial application and then towards general modularization. zk-SNARK, with its superior performance, has become the mainstay for privacy currencies and on-chain rapid verification, suitable for practical deployment and on-chain validation. zk-STARK, with its fully transparent and quantum-resistant advantages, is oriented towards future infrastructure construction, suitable for long-term deployment and high-security scenarios. PLONK, on the other hand, strikes a balance between universality and recursive capabilities, offering both scalability and engineering friendliness, and has become a widely adopted new trend in recent years. Together, they support the technical foundation for building the next-generation "verifiable but not revealing" privacy blockchain systems.

2 Cross-domain applications of zkp in blockchain systems: integration and advantages

Zero-Knowledge Proofs (ZKPs) offer a robust cryptographic foundation for achieving both privacy preservation and regulatory compliance, making them particularly valuable in sensitive and data-intensive sectors. This section explores how ZKP-enhanced blockchain systems are being integrated across key domains—healthcare, financial services, e-government, and supply chain management—and analyzes the technical and institutional advantages enabled by such deployments.

2.1 Healthcare and medical data sharing

The healthcare sector demands stringent privacy safeguards due to the highly sensitive nature of patient data. Traditional centralized medical record systems are vulnerable to data breaches, misuse, and lack of interoperability. ZKP-enabled blockchain systems can address these challenges by ensuring confidential sharing and verifiable integrity of medical records.

For instance, ZKPs can allow hospitals, insurers, and research institutions to verify patient eligibility or diagnosis results without revealing the underlying data. Patients retain sovereignty over their data while enabling cross-institutional collaboration. Furthermore, ZKP protocols such as zk-SNARK or PLONK can be embedded into electronic health record (EHR) platforms to guarantee data integrity and auditability without sacrificing confidentiality. This architecture facilitates GDPR-compliant healthcare data management and supports the development of patient-centered data ecosystems.

2.2 Financial services and regulatory technology (regtech)

In the financial sector, ZKPs serve as a transformative solution to the long-standing dilemma between privacy and compliance. Blockchain-based financial systems can leverage ZKPs to enable anonymous yet auditable transactions, particularly in areas such as Know Your Customer (KYC), Anti-Money Laundering (AML), and secure digital identity verification.

For example, a user can prove their creditworthiness or residency without disclosing their full financial history or identity credentials. Banks and regulatory authorities benefit from selective disclosure and verifiable compliance proofs, reducing the need for full data exposure. Emerging financial applications—such as decentralized exchanges (DEXs) and privacy-preserving stablecoins—are increasingly adopting ZKP-based modules to ensure user confidentiality while remaining audit-friendly. Moreover, recursive ZKP systems offer potential in real-time financial auditing and risk monitoring.

2.3 E-government and digital public services

Governments worldwide are exploring blockchain to improve transparency, traceability, and efficiency in public service delivery. However, public blockchain systems raise concerns over excessive data exposure. ZKP integration allows governments to maintain transparent logic with hidden inputs, thereby striking a balance between openness and privacy.

Typical use cases include anonymous voting systems, where ZKPs enable individuals to prove voting eligibility and correct vote casting without revealing their identity or vote content. In social welfare distribution, ZKPs can prevent fraud by verifying recipient eligibility without exposing personal data. Additionally, public procurement, land registry, and tax declaration systems can employ ZKPs to verify correctness and legitimacy without revealing sensitive underlying records. This fosters public trust and strengthens institutional accountability.

2.4 Supply chain management and intelligent manufacturing

Modern supply chains span multiple stakeholders across regions and regulatory jurisdictions, demanding traceability, confidentiality, and tamper-resistance. Blockchain ensures immutable tracking, but often conflicts with business confidentiality needs. ZKPs provide a secure bridge, enabling proof of origin, compliance, or quality assurance without disclosing proprietary logistics or pricing information.

For instance, manufacturers can prove that materials comply with environmental or labor standards without revealing supplier identities. Retailers can validate product authenticity to consumers while protecting commercial secrets. In intelligent manufacturing, ZKP can be combined with IoT devices and smart contracts to verify machine states, production milestones, or energy usage in a privacy-preserving manner. This is especially valuable in Industry 4.0 scenarios, where secure data sharing across trust boundaries is critical.

3 Regulatability and compliance challenges: how zkpbalancesprivacy and oversight

3.1 Regulatory priorities: anti-money laundering (AML), know your Customer (KYC), and auditability

With the rapid development of blockchain technology, various decentralized applications are flourishing in multiple fields such as finance, healthcare, and government affairs. However, the privacy protection feature of decentralized systems and traditional regulatory mechanisms are increasingly in conflict, especially in the financial sector, where the balance between privacy protection and regulatory compliance has become a key issue. Specifically, the following are the main areas of compliance that regulatory authorities focus on:

Anti-Money Laundering (AML) requires financial institutions to identify, report, and prevent money laundering through appropriate review and monitoring measures. In blockchain applications, due to anonymity and decentralization, illegal fund flows are difficult to track and can easily become breeding grounds for criminal activities. Regulatory authorities need to review transactions to ensure the legitimacy of the source of funds, but at the same time, personal privacy protection should not be overly infringed upon.

Know Your Customer (KYC) is a key procedure used by financial institutions to identify the identities of their customers. In traditional banking, customer identities are verified through documents and facial recognition, but in decentralized finance (DeFi) platforms, anonymous transactions and decentralized identities make KYC more complex. To comply with KYC requirements, financial institutions need to effectively collect user information to ensure that each transaction is backed by a legitimate identity and prevent false identities and tax evasion.

3.2 How to achieve "controlled transparency" or "authorized disclosure" while protecting privacy in ZKP

In the context of the continuous expansion of practical applications of blockchain systems, the structural contradiction between privacy protection and compliance regulation has become increasingly prominent. Especially in high-sensitive fields such as finance, healthcare, and government affairs, users not only want to keep their identities, transactions, and behaviors anonymous, but also need to meet regulatory requirements such as anti-money laundering (AML), customer due diligence (KYC), auditing, and accountability. The traditional blockchain architecture is either completely transparent (sacrificing privacy) or completely anonymous (blocking the regulatory path). Zero-knowledge proof (ZKP), as a "verifiable yet non-disclosable" cryptographic technology, provides a new solution to this contradiction.

ZKP is building a legal and compliant privacy foundation for blockchain systems through mechanisms such as "controlled transparency" and "authorized disclosure". In the "controlled transparency" aspect, the regulatory window mechanism allows users to disclose partial information (such as transaction amounts and sources of funds) to the regulatory authorities under authorization, without exposing the complete transaction structure. Zcash has implemented this mechanism based on zk-SNARK, and users can generate authorization proofs through local wallets, supporting the

coexistence of on-chain privacy and regulatory compliance. Systems like zk-Ledger also adopt similar designs, becoming a new paradigm for privacy compliance governance.

4 Future development trends: research directions and technological integration of the next generation high-efficiency ZKP protocol

As the application of blockchain expands in various fields, zero-knowledge proof (ZKP), as a key technology for privacy protection and data verification, is facing multiple challenges such as improving efficiency, enhancing scalability, and integrating with other cutting-edge technologies. In the future, the development of ZKP protocols will gradually incorporate areas like artificial intelligence (AI), secure hardware, and quantum resistance technology to meet the increasingly complex requirements for privacy protection and compliance regulation. The following will detail these future development trends and possible technological integration directions.

Although current ZKP protocols (such as zk-SNARK, zk-STARK, PLONK, etc.) have made significant progress in privacy protection and data verification, there is still considerable room for improvement in terms of computational efficiency, verification time, and protocol universality. The main research directions in the future focus on the following aspects:

4.1 The integration of ZKP with cutting-edge technologies

The future development of ZKP technology will not only focus on improving the protocol itself, but also involve deep integration with other cutting-edge technologies, mainly including artificial intelligence (AI), secure hardware, and quantum-resistant technologies, etc. The application of AI technology in blockchain is increasingly widespread, especially in smart contracts, data processing, and pattern recognition.]In the future, the integration of ZKP with AI will help automate the generation of ZKP, and AI algorithms can be used to automatically generate and verify ZKP proofs, especially when dealing with massive data, AI can optimize the proof generation process, reducing manual intervention and time costs; it is also beneficial for the optimization of smart contracts, where ZKP can protect the data privacy of smart contracts, and AI can provide optimization algorithms for the execution of smart contracts, combined with ZKP to improve the execution efficiency of smart contracts.

4.2 Build a blockchain ecosystem that is compatible with both privacy protection and regulatory compliance

With the continuous development of ZKP technology, how to build a blockchain ecosystem that is both privacy-protected and compliant with regulations will be the focus of future research .The goal of this ecosystem is to ensure that the blockchain can meet the privacy protection requirements of various industries while also meeting the requirements of anti-money laundering (AML), customer due diligence (KYC), and audit compliance laws and regulations. ZKP introduces the concept of controlled transparency in the blockchain, that is, while protecting user privacy, it allows compliant parties (such as regulatory agencies, auditing institutions) to access certain data under specific conditions. This mechanism not only resolves the contradiction between "privacy protection and regulatory compliance" but also ensures the verifiability and auditability of data, achieving a transparent but controlled data sharing model. For example, the "regulatory window" technology: in platforms such as Zcash and zkLedger, using ZKP proofs can verify the legality of transactions without exposing the specific transaction amount or the transaction parties .

Nowadays, the emergence of multiple blockchain platforms has led to cross-chain interoperability becoming another direction of blockchain technology development. How to ensure the privacy of cross-chain transactions while meeting the compliance requirements of each chain will be the core challenge in the design of future blockchain privacy protection architectures. Cross-chain privacy protection: ZKP can provide privacy protection for cross-chain transactions, ensuring the consistency and security of cross-chain data while ensuring that the privacy of both transaction parties is not disclosed. For example, blockchain networks such as Polkadot and Cosmos have been exploring cross-chain privacy protection solutions based on ZKP. ZKP will play a more important role in the global blockchain ecosystem. In the future, ZKP technology will further enhance the privacy compliance of blockchain, enabling its wide application in more industries and promoting the global and compliant development of blockchain technology.

5 Conclusion

This article explores the significant utility of zero-knowledge proof technology in improving the privacy, scalability, storage capacity, and verification capabilities of blockchain from multiple aspects. IZero-knowledge proof has formed a

relatively mature system over the past 30 years. In the design of blockchain systems, the problems that the system needs to improve or the features that need to be implemented are transformed into a specific provable problem, then from the proof problem to the engineering algorithm implementation approach, and finally transformed into a certain property or function that the blockchain can achieve. Each step requires comprehensive consideration of whether zero-knowledge proof can provide these characteristics without sacrificing decentralization, security, and scalability. Particularly, as a new network ecosystem infrastructure, blockchain requires extensive privacy security, high computing capabilities for interconnection and interoperability, and global verifiability and regulatory support. All of these require the participation of privacy computing, especially zero-knowledge proof. This is also the trend and advantage of zero-knowledge proof in the future development of blockchain. Several existing cases of zero-knowledge proof applications in blockchain have shown that as long as zero-knowledge proof is properly utilized, it can greatly improve the performance of blockchain in application scenarios. This emerging Internet technology can also demonstrate increasingly important value.

References

[1] Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof- systems [C]//STOC '85: Proceedings ofthe Seventeenth Annual ACM Symposium on Theory of Computing. New York: ACM,1985: 291- 304.

[2] Furer M,Goldreich O,Mansour Y,et al. On completeness and soundness in interactive proof systems[J]. Advances inComputing Research: A Research Annual,1989, 5: 429- 442.

[3] Ben- Or M, Goldreich O, Goldwasser S, et al. Everything provable is provable in zero- knowledge [C]//Advances in Cryp-tology- CRYPTO '88. Berlin: Springer,1988: 37- 56.

[4] Shamir A. IP = PSPACE [J]. Journal of the ACM,1992, 39(4): 869- 877.

[5] Blum M, Feldman P, Micali S. Non- interactive zero- knowledge and its applications[C]//STOC '88: Proceedings of theTwentieth Annual ACM Symposium on Theory of Computing. New York: ACM,1988: 103-112.

[6] Blum M,De Santis A,Micali S,et al. Noninteractive zero- knowledge[J]. SIAM Journal on Computing,1991,20 (6):1084- 1118.

[7] Fiat A,Shamir A. How to prove yourself: Practical solutions to identification and signature problems[C]//Advances inCryptology- CRYPTO '86. Berlin: Springer,1987: 186- 194.

[8] Goldwasser S,Tauman Y. On the (in)security of the Fiat- Shamir paradigm [C]//FOCS '03: Proceedings of the 44th Annu-al IEEE Symposium on Foundations of Computer Science. Piscataway: IEEE,2003: 102- 115.

[9] Fortnow L. The complexity of perfect zero- knowledge [C]//STOC '87: Proceedings of the Nineteenth Annual ACM Symposi-um on Theory of Computing. New York: ACM,1987: 204- 209.

[10] Groth J. Short pairing- based non- interactive zero- knowledge arguments[C]// Advances in Cryptology- ASIACRYPT ' 10.Berlin: Springer, 2010: 321- 340.

[11] Groth J. On the size of pairing- based non- interactive arguments[C]//Advances in Cryptology- EUROCRYPT '16. Berlin:3Springer, 2016: 305- 326.

[12] Bitansky N, Canetti R, Chiesa A, et al. From extractable collision resistance to succinct non- interactive arguments ofknowledge, and back again [C]// ITCS '12: Proceedings of the 3rd Innovations in TheoreticalComputer Science Confer-ence. New York: ACM,2012: 326- 349.

[13] Parno B, Howell J, Gentry C, et al. Pinocchio: Nearly practical verifiable computation [C]//2013 IEEE Symposium on Se-curity and Privacy. Piscataway: IEEE,2013: 238- 252.

[14] Groth J,Kohlweiss M,Maller M,et al. Updatable and universal common reference strings with applications to zk- SNARKs[C]//Advances in Cryptology- CRYPTO '18. Berlin: Springer,2018: 698- 728.

[15] Maller M,Bowe S,Kohlweiss M,et al. Sonic: Zero- knowledge SNARKs from linear- size universal and updatable structuredreference strings [C]//CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Secu-rity. New York: ACM,2019: 2111-2128.

[16] The halo2 book [EB / OL]. [2022- 10- 01]. https://zcash. github. io / halo2 / .

[17] Ben- Sasson E, Bentov I, Horesh Y, et al. Scalable zero knowledge with no trusted setup[C]//Advances in Cryptology-CRYPTO '19. Berlin: Springer,2019: 701- 732.