Research And Analysis of Cryptographic Methods Based on Blockchain

Rongxi Wei *

College of Computer Science and Technology, Xinjiang University, Urumqi, 830000, China

* Corresponding Author Email: 20211305228@stu.xju.edu.cn

Abstract. This paper systematically reviews the research foundation, core technologies, and practical applications of cryptography in the blockchain field. Algorithms, and data immutability relies on cryptographic hash functions and Merkle tree structure; the balance between transparency and privacy in block chain relies on the encryption technique of zero-knowledge proofs, ring signature, homomorphic encryption. Therefore, every part of block chain is based on cryptography; without the mathematical guarantee of cryptography, the trust decentralized by block chain is meaningless. The security of block chain mainly relies on the encryption techniques such as hash functions, digital signatures and encryption algorithms, and traditional cryptographic methods will have vulnerabilities when facing quantum computing, because quantum computer may be used to break currently commonly used algorithms such as RSA, ECC eventually. This "security paradox" requires us to pay more attention to block chain technologies, because block chain technology needs to advance in tandem with cryptography. Traditional blockchain technologies can't be used indefinitely. Against this background, researching block chain －based crypto is of great theoretical significance and practical value: on the one hand, researching on new cryptographic methods applicable to block chain can extend the area of cryptosystems and give people a new way of solving the security problems in block chain; on the other hand, we should not neglect the possibility of breaking the block chain by combining quantum computing with cryptanalysis research.

Keywords: Blockchain; Cryptographic technologies; Privacy.

1. Introduction

Block chain empowers the digital economy and supports global cooperation. It is not just a technology but also a new collaboration paradigm: reducing enterprise collaboration costs, enhancing data value, enabling individuals to control their data sovereignty and enjoy inclusive services, and building a trustworthy social system that drives the upgrade of the digital economy. When discussing block chain, one cannot overlook cryptography. From a technical perspective, block chain's decentralized identity verification relies on asymmetric encryption algorithms, and data immutability relies on cryptographic hash functions and Merkle tree structures. besides that, the transparency/privacy depends on zero-knowledge-proof (ZKP), ring signature, homomorphic encryption and so on. Thus, all block chain relies on cryptography for its functionality, trust decentralized by block chain is meaningless unless crypto math guarantees that are offered by cryptography. Security of block chain mostly also depends on cryptography like hash function, digital signatures, encryption and so on. In general case, traditional cryptography methods show vulnerability to be conquered under the high-computing power of quantum computers because quantum computer inevitably breaks those public-use algorithms like RSA.ECC etc. Which thus raises this "security paradox, and confront it requires urgent researching of block chain-based cryptographic method from both theoretical perspective and techniques challenge. One aspect, researches concerning cryptography can apply to block chain expands cryptography's scope itself as it provides new visions for dealing with security issues raised by block chain. On the other aspect, the trust mechanisms of distributed architectures heavily rely on cryptography; on the other hand, technological advances present entirely new challenges to existing cryptographic methods. Against this backdrop, researching block chain-based cryptographic methods holds significant theoretical and practical importance. From a theoretical standpoint, exploring new cryptographic methods suitable

for block chain can expand the scope of cryptography and offer new approaches to solving security issues in block chain. From a practical aspect, designing security and efficiency protocols and algorithms to provide a strong guarantee of the real world's use of block chain technology and more suitable fields of application in an important position. Domestically and abroad Scholars and institutions from various countries have realized the significance of the problem and conducted relevant research. Overseas Firstly, there are some basic cryptographic technologies suitable for block chain, such as the SHA series of hash algorithms, elliptic curve cryptography algorithms of Bitcoin, etc., and the related research work on privacy protection, such as zero-knowledge proofs, ring signature and so on. China's "Chain" is at the forefront in the world with Changan Chain, AntChain and Tencent TrustedChain development platform to support high throughput (for example, Changan Chain supports 100 000 tps) cross institutional cooperation. For example, according to the Ministry of Industry and Information Technology "block chain industry report", consortium block chain technology for domestic government services, the number of scenes applied to supply chains and other areas ranks first in the world [1]. Especially in terms of cryptographic techniques innovation, for instance, from Tsinghua University: a Tsinghua Univeristy team proposed a series of work on Qubit Blockchain (Tsinghua Univeristy), the design of the "quantum resilience blockchain - ZK-Pf Privacy Auth Frmework (QBc-zk pa framework)", which designed a hybrid cryptographic technique combining post quantum cryptosystems and zero knowledge proof, supported IoT scenario and realized approximate 98% protective effect on privacy data, through put reaches 700 t/s [2]. The team from Chinese Academy of Sciences, the Energy Blockchain Cross-chain Tech designed and realized through blockchain energy market across chain, and its multi-level collaborative supervision architecture could solve cross-chain data security problem, applied to the State Grid Pilot distributed Power transactions project [3]. While that, another Peking University team from School of Computer Science, Peking University designed Weak Consensus Algoti, Sphinx, and the design increased the transaction throughput of block chain about 43k tps (node number 8), this design decreases the consistency guaranteed strictly level by loosen it suitably applications whose guarantee consensus levels doesn't need be extremely high e.g. certificate store, 10 times faster than Ethereum’s Geth client average transaction TPS reachs 4k or 5k leve [4]. Globally, Solana uses "Proof of History "+"Proof of Stake ("PoH"+"PoS") hybrid consensus scheme to increase the throughput about 60,000 TP per second, during the fourth quarter of the year 2024 it exceeds surpassed ETH exceeded it became DEX top trading pairs chain (shares around 30%+). Layer 2 keeps innovate, Base everyday transaction reached avg 7.2 million, accounting for 48.3% of the total transactions of the top ten Layer 2 solutions [5]. The privacy public chain Partisia Blockchain combines Multi-Party Computation (MPC) with zero-knowledge proofs (ZK) and launched "MPC-as-a-Service", meeting EU GDPR compliance requirements in scenarios such as medical data sharing and spectrum auctions, achieving a 99.7% success rate in transactional privacy protection [6]. The international team developed the "Ownership Transfer and Execution Protocol (OTEx)", which enables cross-chain asset transfer through gateways and auxiliary blockchains and has been successfully validated on the Ethereum test net. The International Organization for Standardization (ISO) released the "Blockchain and Distributed Ledger Technology - Cross-Chain Interoperability Framework," defining a seven-layer protocol stack for cross-chain communication to promote seamless interaction between different public and consortium blockchains. JPMorgan launched "JPM Coin" for cross-border payment settlement, reducing transaction time from 3 days to seconds. Decentraland's virtual land transaction volume exceeded $1 billion, allowing users to verify digital assets via blockchain [7]. NBA Top Shot achieved cumulative sales of over $2 billion, converting players' highlight moments into NFT products. The US MedRec platform uses blockchain to enable cross-hospital sharing of patient records and combines zero-knowledge proofs to protect privacy, piloted at Harvard University-affiliated hospitals, improving data access efficiency by 40%. In summary, the concept of block chain technology has become relatively stable. The current focus of research is on large-scale application. Domestically, consortium block chains empower the real economy, while internationally, the focus is on innovation in public block chains and expansion of financial markets, covering payment settlement, digital asset

verification, and sharing of medical records. One first discusses the research background, clarifies the significance of the study, and reviews the current state of research both domestically and internationally, laying the foundation for subsequent research; Chapter Two delves deeper into the technical aspects, specifically introducing the technical characteristics and architecture of blockchain, while also explaining the traditional cryptographic methods involved, as well as blockchain privacy enhancement, thus constructing a solid technical theoretical framework; Chapter Three focuses on practical applications, exploring new applications of cryptography in the blockchain field and conducting comparative analysis for selection; Chapter Four summarizes the research findings, presents research conclusions, and offers a research outlook, guiding researchers in the related fields toward future research directions. Purpose of the article to systematically review the research foundation (background, significance, current status) in the blockchain field, core technologies (technical characteristics, architecture, cryptographic methods, etc.), and practical applications (new cryptographic applications and selection), as well as summarize research findings and clarify future research directions, providing researchers in the intersection of blockchain and cryptography with a comprehensive and organized reference to help grasp the research trends in the field. Significance of the article from a theoretical perspective, this paper elucidates the technical characteristics of blockchain, traditional cryptographic methods, privacy enhancement, and the foundations of post-quantum cryptography.

2. Research on Cryptography Foundation

Next, the applications of cryptography in blockchain will be demonstrated through SHA-256 and SM3, as well as the associated properties of one-wayness, avalanche effect, collision resistance, and fixed output length. SHA-256 is an internationally recognized cryptographic algorithm developed by the National Institute of Standards and Technology (NIST) in the United States, based on the Merkle-Damgård construction. SM3 is developed by the State Cryptography Administration of China, borrowing the design ideas of SHA-256, optimizing the message expansion algorithm, and its security conforms to Chinese national cryptographic standards. It is a mandatory cryptographic algorithm for critical information infrastructure, government systems, and the financial sector in China [8].

2.1. Related Concept

2.1.1 One-wayness

One-wayness: Prevents attackers from reversing sensitive data (such as passwords or transaction information) from the hash value, which is fundamental for privacy protection and data tampering prevention (Table 1).

Table 1. Applications of One-WaynessAgainst

Data tampering	Make reverse modification of the hash chain extremely costly and imtamable
Consensus competition	Allow mechanisms such as PoW to only try and error in the right direction, ensuring fairness
Privacy Protection	Make the address, transaction data, and certificate content cannot be reverse cracked, to achieve identity and data isolation
On efficiency balance	*Make it possible to verify light nodes and store evidence on the chain, reducing the operation and storage costs of blockchain*

2.1.2 Avalanche Effect

Avalanche Effect: Ensures that minor changes in input are quickly detectable, preventing attackers from creating false data with the same hash by "fine-tuning the input (Table 2).

Table 2. Applications of Avalanche EffectFor Data Identification

Tampering	*Make "hidden tampering" impossible, any small change will trigger a global hash change, which will be detected by the whole network in real time*
Consensus mechanisms	*Ensure that the Nonce attempt of PoW is completely random, eliminate "computing power cheating", and ensure the fairness of consensus*
Validation efficiency	*Merkle tree and on-chain evidence verification do not need to traverse the full amount of data, but can quickly determine the integrity through the top layer hash, reducing the operating cost*

2.1.3 Collision Resistance

Collision Resistance: Prevents hash collision attacks (Table 3).

Table 3. Applications of Collision Resistance

Data labeling	*Ensure that the hash value of block, transaction, address and certificate storage "only corresponds to the input data", and avoid the confusion of identification caused by "diferfent data sharing the same hash"*
Security	*Prevent malicious behaviors such as fake blocks, transaction replacement, double-spending attack and address confusion to maintain the imtamability of blockchain and asset security*
Consensus and law	*The "only valid block" principle that* guarantee*s PoW consensus, and the "original data uniqueness" on-chain ev*idence, make the *consensus* mechanism of blockch*a*in and *the* value of legal evidence valid

2.1.4 Fixed Output Length

Fixed Output Length: Both SHA-256 and SM3 output 256 bits, facilitating storage, transmission, and verification (Table 4).

Table 4. Applications of Fixed Output Length

Standardization of structures	*The format of core data such as block header, Merkle tree and address is unified to avoid format confusion caused by differences in input data size and ensure seamless coordination among nodes on the whole network*
Optimize efficiency	*Significantly reduce the storage/transfer costs of light nodes, simplify the logic of Merkle verification and consensus judgment, and enable the blockchain to run efficiently on all kinds of devices from servers to mobile phones*
Ecological compatibility	*Provide a unified hash/address format standard for wallet, exchange, browser and other ecological tools to reduce development adaptation costs and improve user experience*

2.2. Crytographic Foundation

Currently, blockchain privacy-enhancing technologies are primarily based on cryptographic innovations and can be divided into three categories: "transaction privacy protection," "identity privacy protection," and "data privacy protection." The core logic, representative projects, and applicable scenarios of each category differ significantly

Hiding "who transferred how much to whom" This technology is at the core of privacy enhancement, focusing on preventing the leakage of transaction participants (addresses) and transaction amounts. As shown in figure 1, the mainstream solutions include coin mixing protocols, ring signatures, and zero-knowledge proofs. Coin Mixing Protocol Principle: Combine transactions from multiple users to obscure the correlation of fund flows: when User A transfers to B and User C transfers to D, the transactions are merged into a single multi-input, multi-output transaction, making it impossible for outsiders to distinguish which input corresponds to which output [9]. Example: Bitcoin Mixer, Wasabi Wallet Advantages: Simple implementation, strong compatibility (no need to

modify the blockchain base layer), low computational cost. Limitations: Privacy strength depends on the number of participants in the mix; requires trust in the coin mixing service provider.

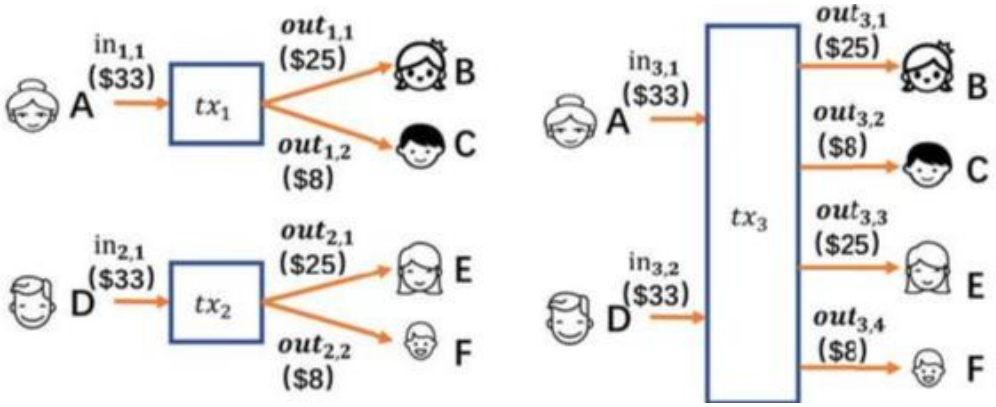

Fig. 1 Flow chart of currency mixing protocol

Randomly select multiple "decoy addresses" from the blockchain's historical address pool and combine them with the user's real address to form a "signing ring" (figure 2). After signing, outsiders cannot determine "which address is the true transaction initiator." At the same time, transaction amounts are hidden through a commitment scheme. Example: Monero, Grin Advantages: Fully decentralized (no need to trust a third party), high privacy strength (unable to locate the real address), fast transaction verification.

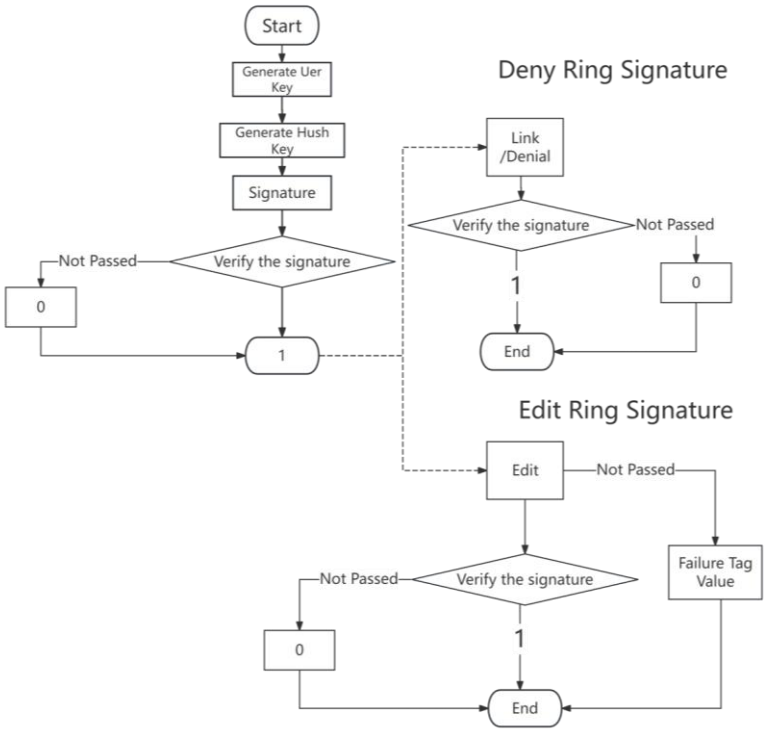

Fig. 2 Flow chart of ring signature

As shown in figure 3, the prover (transaction initiator) proves to the verifier (node) that the transaction is valid (e.g., sufficient balance, no double-spending) without disclosing transaction addresses or amounts. The verifier only needs to validate the proof without knowing the specific details [10]. Example: Zcash, ZkSync Advantages: Extremely high privacy strength (can hide addresses, amounts, and transaction existence), supports selective disclosure (information can be revealed to regulators if compliance is required).

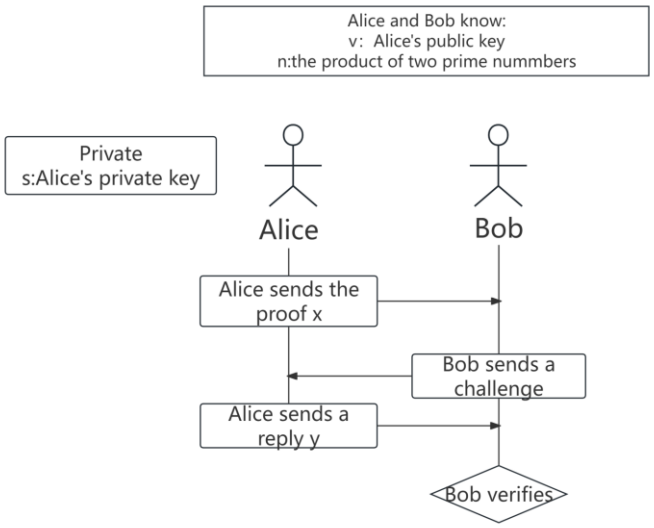

Fig. 3 Flow chart of Zero-Knowledge Proof

3. Research on New Technologies

Cryptography's new applications in the blockchain field, along with comparative analysis for selection comparison and decision suggestion (Table 5).

Table 5. Selection and Decision

Technological dimension	*Postquantum cryptography*	*zero-knowledge proof*	*Secure multi-party computing*	*Homomorphic Encryption*
Rank of Security	*2*	*3*	*4*	*1*
Rank of computing pow	*3*	*2*	*1*	*4*
Compliance	*Complies with the NIST Post-Quantum Standard (2030)*	*Support GDPR data minimization principle*	*Interagency data sharing regulations must be met*	*It needs to be compatible with encrypted data storage compliance*
Typical Scenario	*Asset storage, cross-border payments*	*Financial transactions, medical data sharing*	*Supply chain finance, joint AI training*	*Big data analysis, AI model training*
Representative Project	*BITCOIN. Project Eleven*	*zkSync. Zcash*	*AntChain. ConsenSys OP-Chain*	*Zama. Partisia block chain*

Recommendations: - Short-term needs: Prioritize zero-knowledge proofs (e.g., zkSync) or SMPC (e.g., AntChain) for a balance of privacy and efficiency. - Long-term needs: post-quantum cryptography (e.g., Dilithium3) and homomorphic encryption (e.g., Zama's CBP) should be planned in advance to address quantum computing threats and sensitive data processing. - Hybrid solution:

Combine multiple technologies (e.g., zero-knowledge proof + SMPC) to achieve the optimal balance of "privacy-efficiency-compliance" in complex scenarios such as supply chain finance. In the future, with continuous optimization of hardware acceleration technologies (e.g., FPGA, ASIC) and cryptographic algorithms (e.g., Halo2, PlonK), cryptography will upgrade blockchain from a "trust machine" to a "privacy machine," enabling large-scale applications in finance, healthcare, government, and other fields.

4. Conclusion

Research purpose to elaborate research background (background, importance, current status) in blockchain field, core technologies (technical characteristics, framework, algorithmic cryptography, etc.), practical application scenarios (new application of cryptographic technology and selection criteria) and summarize research results and clarify research directions, providing a relatively systematic and complete introduction and reference to relevant researchers at the intersection of blockchain and cryptography so that they can better understand research situation and direction in this field; Research Outlook Provide practical references for subsequent relevant researchers. Significance of Article Through an analysis on theory, it clarifies technical characteristics of blockchain, traditional cryptographic methods, privacy enhancement and basic content of post-quantum cryptography technology and focuses on research progress of blockchain integration with cryptography, thus covering background and theoretical significance, researching framework, practical scenario and future direction with systematic exposition and analysis. After the study, this article derives three core conclusions: (1) Cryptography is fundamental corner stone of trust mechanism of blockchain. Classic cryptographic algorithms (SHA-256, SM3) and their corresponding algorithmal properties (one-wayness, avalanche effect, randomness and so on) directly determine blockchain's characteristics, such as its "immutable", “fairness" among consensus party, and basic data privacy protection. Taking one-wayness as example, if one wants reverse-cracked any transaction data, which cannot be achieved theoretically and time complexity for it is extremely higher; meanwhile, if using a certain change quantity in original block information to generate one-bit quantity variation within hash value, avalanche effect ensures the whole blockchain can achieve real-time response to whether the original data has been changed, these mathematical properties guarantee the whole security properties under distributed environment are ensured with mathematical theoretical and security guarantees from cryptography technologies. Without mathematics guarantees from cryptography technology, decentralized trust mode of blockchain has no actual values. blockchain privacy-enhancing techniques (PECT), driven by cryptocurrency cryptography technology innovation, form a diverse protection system. Transaction private technologies (such as Zcash’s zero-knowledge proof technique, Monero’s ring signature method) can conceal both fund flow and identities. Identity privacy technologies (stealth address, DID identity system of Hyperledger network), disconnected people's own real identity information from blockchain′ s identity address or account numbers. Data privacy and information protecting (e.g., Homomorphic Encryption (HE) encryption by Zama, secure multiparty computation-based encryption and key exchange techniques (SMPC / SMPKE) proposed by American blockchain company Coinbase) solving problems about sensitive information leakage within blockchain smart contracts and on-chain storage. All kinds have different target and situations, providing flexible tools for various application scenarios for privacy needs when promoting blockchain technologies widely in finance, health care and government. (2) Emerging cryptographic techniques addressing different challenges. According to Table 2 and comparison mentioned in the manuscript, homomorphic encryption has best security grade level but heavy computational overhead, while SMPC balances well efficiency; (3) Emerging cryptographic techniques have clear applications to some existing technical bottlenecks in blockchain. For instance, quantum－insensitive post－quantum cryptography mainly for data processing at present. With further exploration in this study, the future application direction about emerging cryptographic techniques is clearly clarified in related cases like financial system and complexity,

suitable for cross-institution collaboration; Zero-Knowledge Proof, focused on the balance of privacy-efficiency, applicable for short-term practicality needs; post-quantum cryptography (e.g., Dilithium3), essential for protecting long-term resistance against quantum computing threats. Other combinations (Zero-Knowledge Proof + SMPC) also provide optimal trade-offs (efficiency and security) for more complicated circumstances like Supply Chain Finance. Meanwhile, we have seen diversified researches and usages across China and other countries as reflected below. China is focusing on developing "consortium blockchains" to assist the real economy with high throughput solutions by Changan Chain, State Grid based Energy Chains, etc. International efforts highlight breakthroughs of public chains' practicality (e.g., DEX led Solana vs Uniswap), speed-up with Layer 2 via Optimism or Base and privacy compliance (e.g., GDPR aligned blockchain Partisia's solution), which enrich the Blockchain-cryptography ecology and accelerate technological maturity. Looking forward, with hardware optimization (FPGA, ASIC), algorithm optimization (Halo2, PlonK), Cryptography could evolve the current blockchain into a new trend from a "Trust Machine" to a "Privacy Machine". The future trends are optimized algorithms of fully homomorphic encryption to accommodate more complex Smart Contract demands; the next phase of Quantum-resistant development with post-quantum Cryptography integration into already issued Public-blockchain chains including Bitcoin, Ethereum and other private chains; development of hybrid solutions to enable balanced applications between different technologies that need to fulfill the demand of regulatory compliances regarding the privacy-efficiency trade-off, etc. These will contribute Blockchain's large-scale applications in critical sectors such as cross-border payments, digital sharing including Health-care data among medical facilities and Digital Government, thereby benefiting the overall growth of world Digital Economies.

References

[1] Sartaj A, Shubham K A, Shobhit G et al. Study of Cryptographic Techniques Adopted in Blockchain. IEEE Xplore, 2024.

[2] Laith H J, Anshoo M, Sanjeev K J et al. Analysing Blockchain-Based Cryptography: Enhancing Security, Transparency, and Practical Implementations. IEEE Xplore, 2024.

[3] Hadi G, Jorge G, Edmundo M et al. Post-Quantum Blockchain Security for the Internet of Things: Survey and Research Directions. IEEE Xplore, 2024.

[4] Wang Y, Ismail E S. A Review on the Advances, Applications, and Future Prospects of Post-Quantum Cryptography in Blockchain and IoT. IEEE Xplore, 2025.

[5] Manh B D, Nguyen C H, Hoang D T et al. Privacy-Preserving Cyberattack Detection in Blockchain-Based IoT Systems Using AI and Homomorphic Encryption. arXiv, 2025.

[6] Blass E, Kerschbaum F. BOREALIS: Building Block for Sealed Bid Auctions on Blockchains. ACM Digital Library, 2020.

[7] Chaudhary A. zkFi: Privacy-Preserving and Regulation Compliant Transactions using Zero Knowledge Proofs. ResearchGate, 2023.

[8] Garay J, Kiayias A, Leonardos N. The Bitcoin Backbone Protocol: Analysis and Applications Eurocrypt, 2020.

[9] Chen N Y. Scalable Blockchain Architectures for Enhancing Integrity and Privacy in Vehicular Ad-hoc NetworksPhD Thesis. University of Nottingham Ningbo China, 2025.

[10] Chhetri G, Somvanshi S, Hebli P et al. Post-Quantum Cryptography and Quantum-Safe Security: A Comprehensive Survey. arXiv, 2025.