Blockchain Cryptography and Security Mechanisms

Mubarak Wumbei Salifu
224047655

Abstract **-** This study covers blockchain technology's concept, architecture, applications, cryptography, security and privacy issues. Blockchain technology was introduced by Satoshi Nakamoto as Bitcoin's foundation. The study examines blockchain's data, consensus, network, and application layers. Smart contract execution, decentralized networking, and transaction verification are enabled by each layer. The study further highlights blockchain's built-in security features including digital signatures, cryptographic hashes, and consensus methods like Practical Byzantine Fault Tolerance and Proof of Work, which guarantee data integrity and prevent 51 percent attacks. To balance transparency and secrecy, differential privacy, zero-knowledge proofs, and pseudonymization are utilized. Despite interoperability issues, legal ambiguity, and quantum computing concerns, the study explores innovative approaches to integrate blockchain into secure systems including smart surveillance, international e-commerce, and IoT frameworks.

I. CONCEPT OF BLOCKCHAIN TECHNOLOGY

The foundational technology, often known as Blockchain in contemporary times, was initially put forth in 2008 by an individual using the pseudonym Satoshi Nakamoto, who introduced the first application of Blockchain, and whose actual identity still remains undisclosed [1]. The concept of blockchain was initially established as the foundational technology of a decentralized peer-to-peer electronic cash system, commonly known as Bitcoin [2]. This technology is the first cryptocurrency to be developed using the blockchain concept. In the subsequent five-year period, Vitalik Buterin introduced a novel blockchain-based system named Ethereum [3]. The underlying concept of this technology aims to augment the capabilities of Bitcoin by creating a blockchain that incorporates a comprehensive Turing-complete programming language. The utilization of this blockchain technology has become widespread on a global scale, serving as a foundation for decentralized applications. In recent years, there has been a noticeable increase in the use of blockchain-based solutions by several industries, including FinTech and retail [4]. With the increasing understanding and widespread adoption of blockchain technology, its applications have extended beyond the realms of payment processing and money transmission to encompass diverse domains such as data sharing, item tracking, supply chain monitoring, power systems, and even digital voting [5], [6]. This trend can be attributed to the emergence and expansion of cryptocurrencies such as Bitcoin and Ethereum [7]. Blockchain can be considered as a distributed and decentralized ledger comprising a progressively elongated series of documents, referred to as blocks, which are sequentially linked together and managed by a peer-to-peer network [6]. [8] defined blockchain as a technology that employs cryptographic techniques to guarantee secure transmission and access, while also enabling data consistency, resistance to tampering, and the capacity to track information. [9] also defined blockchain as a linear and immutable data structure composed of interconnected blocks, wherein each block encapsulates a collection of transactions that undergo validation through cryptographic protocols. The data contained within the blocks remains unaltered and immutable. In another definition, [10] stated that blockchain is a platform that maintains digital information and records in a decentralized manner (i.e., distributed ledger technology), which is known for its safe and verifiable bookkeeping capabilities, as well as its capacity to be audited effectively.

[11] asserts that blockchain's data storage mechanism employs an encrypted structure that can be represented graphically or in a tree-like format, consisting of interconnected basic blocks, which are logically linked together using pointers. The underlying structure of blockchain is rooted in a decentralized and distributed computing framework that operates on a peer-to-peer network prioritizing the establishment of trust and value over the mere transmission of information [12]. [13] added that a blockchain facilitates a decentralized framework for the documentation of non-changeable transactions, ensuring that no singular institution or entity possesses authority over the data. The objective is accomplished through the implementation of a distributed consensus process, which yields data that is immutable in nature. When discussing the purpose of blockchain-based systems, [14] made a point that the aim is to establish trust inside a specific system not by completely eliminating trust, but by enhancing the level of confidence among participants, hence indirectly minimizing the reliance on trust. In this vein, Diallo et al. (2022) argued that blockchain can be understood as history of transactions, serving as a repository for entities engaged in interactions that do not fully trust each other. The blockchain is a data structure consisting of a series of blocks that are interconnected [16]. Typically, a block within a blockchain consists of two primary components: transactional data and metadata [11], [16]. The metadata of a block generally includes various components such as a timestamp, a hash value representing the current block, and a hash value representing the prior block [10], [16]. In addition, each block comprises a collection of transactions, and each block is connected to its preceding block through a cryptographic reference, commonly referred to as a hash [11], [17]. The

computation of hash values uses a one-way function that possesses strong cryptographic properties [16]. This feature enables the interconnection of blocks to establish a sequential database. The transactions included within a block are condensed into a singular hash value which will be subsequently incorporated into the subsequent block, so establishing a hash chain that upholds the immutability of the ledger [18]. The inherent characteristics of blockchains lead to the detection of any alterations made to the data by other members in the network, as the hash of the subsequent block would not align with the data on the modified block [16].

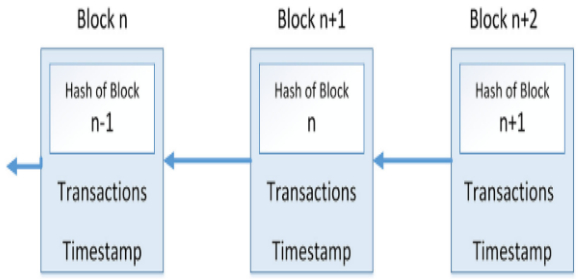

Figure 1:Blockchain Structure. Adopted from Sadu et al. (2021)

Block n is the present block under consideration. The block consists of a collection of transactions, accompanied by a timestamp indicating the moment of their inclusion in the chain, and the cryptographic hash value of the preceding block (n-1). This establishes a secure connection to the preceding block. The n+1 refers to the subsequent block in the chain, immediately following block n. Like how block n contains the hash of block n-1, block n+1 will contain the hash of block n. This mechanism guarantees that each block is cryptographically linked to its preceding block. Furthermore, given the value of n+2, this represents the subsequent block in the series following block n+1. The chain will be extended by including the hash of block n+1. This particular block will possess its own set of transactions and timestamp, and it will ultimately be followed by a following block that makes reference to its hash value.

II. LAYERS OF BLOCKCHAIN

A. Data Layer

Transactions, blocks, the Hash function, the Merkle tree, and the digital signature all make up this layer [19]–[22]. The notion of blockchain involves the utilization of a digital ledger consisting of a sequential arrangement of factual information, commonly known as blocks, that are interconnected [23], [24]. The process commences with the primary block, commonly known as the "genesis block," and extends as successive blocks are verified and added [25]. Each block contains many transactions involving the transfer or receipt of digital currency. Additionally, it is characterized by a unique code, known as a hash, which serves to establish its connection to the previous block, thereby forming a chain [26]. The security of this blockchain is guaranteed by its immutability, as any attached data becomes unalterable. A typical block comprises two fundamental elements, namely the transaction data and a header [27]. Transactions take place when an individual employs their private key, which functions as a secure digital signature, to provide authorization for a particular action, such as the transfer of digital money or the validation of a digital contract (Liu et al., 2017). The block header is composed of two essential elements: the hash of the previous block, which establishes a linkage between them, and a unique code called the Merkle tree root, which offers a succinct representation of all the transactions included in the block [23]. The process of incorporating a new block into the blockchain involves the utilization of a mechanism called consensus, which facilitates the attainment of a collective consensus regarding the attributes of the new block, such as its unique hash value [29], [30]. The hash value must adhere to established criteria. Furthermore, it records the exact time at which the block was created. After the block is formed, it is disseminated via a peer-to-peer (P2P) network [31].

The process of adding a block to the blockchain is dependent on achieving consensus within the network regarding its legitimacy. This framework offers a decentralized structure wherein no solitary entity holds authoritative power, and all individuals adopt fair and equal roles [30]. Furthermore, each block is equipped with its own unique digital signature and timestamp, so guaranteeing the integrity, transparency, and permanence of the blockchain. The data layer also includes the Merkle tree. The Merkle tree is a technique utilized to provide a concise representation of the entirety of transactions included within a block on the blockchain [32], [33]. The operational mechanism involves the generation of digital fingerprints, also known as hashes, for each individual transaction [34]. These hashes are then paired and combined. Subsequently, the aforementioned pairs are subjected to a hashing algorithm, and this iterative procedure persists until a solitary hash value is obtained, encapsulating the entirety of the transactions [35], [36].

The final hash, commonly referred to as the Merkle root, is retained within the header of the block [37]. The utility of this approach lies in its ability to streamline the verification process for a specific transaction. Rather than examining every transaction present on the blockchain, only those that contribute to the formation of the Merkle root necessitate scrutiny [38].In the event of any modification to a transaction, the corresponding alteration in the Merkle root would serve as an indicator of the change that has taken place [39].

The implementation of this mechanism enhances the security of the blockchain system and facilitates the streamlined verification process of transactions encapsulated within a block. Furthermore, the digital signature that forms part of the data layer is an established and reliable technique used to authenticate and ensure the integrity of digital content [40]. Public key cryptography is employed in this system, utilizing two distinct keys: a public key, which can be disseminated to others, and a private key, which is safeguarded by the owner in confidentiality [41], [42]. The public key serves the purpose of verifying a signature or encrypting a message, whereas the private key is utilized for generating a signature or decrypting a message [43]. Within the realm of blockchain technology, the public key functions as a designated identifier for individuals to receive digital currencies, while the private key grants exclusive access and control over this currency [44]. Maintaining the confidentiality of the private key is of utmost importance as it governs the authorization to access the digital assets [45].

B. Consensus Layer

Within a blockchain network, the absence of a centralized authority is evident, as there is no entity responsible for overseeing transactions or safeguarding against unauthorized manipulation of data by malicious actors [46]. In order to mitigate fraudulent activities, such as the double spending of digital currency, it is imperative to ensure the verification of each block of transactions [47]. Consensus algorithms are employed to accomplish this task through the implementation of specific rules. The utilization of these algorithms facilitates consensus among the computers within the network on the authenticity and reliability of transactions, hence obviating the necessity for mutual trust [48], [49]. Technologies applied in the consensus layer includes the Practical Byzantine Fault Tolerance (pBFT), Proof of Elapsed Time (PoET), Leased Proof of Stake, Delegated Proofof Stake (DPoS), Proof of Bandwidth, Proof of Authority and Proof of Authentication [50]–[56].

C. Network Layer

The network layer inside the blockchain architecture, commonly referred to as the peer-to-peer (P2P) network, facilitates intercommunication among the many nodes, or computers, comprising the blockchain system [57]. The network facilitates the ability of each node to locate and establish connections with other nodes, enabling the sharing of the most recent blocks and ensuring the synchronization and up-to-date state of the blockchain [58]. In a peer-to-peer (P2P) network, the distribution of tasks is decentralized over multiple computers. This facilitates the effective execution of transactions and the administration of the blockchain. The network consists of two primary categories of nodes, namely full nodes and light nodes. Full nodes play a crucial role in the blockchain ecosystem as they undertake the task of verifying and validating transactions and blocks in accordance with the established rules of the blockchain [59]. Ensuring network reliability is of utmost importance. Light nodes, on the other hand, primarily focus on facilitating transactions and transmitting them to full nodes for verification [60]. The storage of the entire blockchain is not undertaken; rather, only the most crucial components, such as headers or keys, are retained [61].

D. Application Layer

The blockchain application layer encompasses several components such as smart contracts, chaincode, and decentralized applications (dApps) [62], [63]. The aforementioned layer consists of two distinct sub-layers, namely the presentation layer and the execution layer [63]. The presentation layer encompasses several components such as scripts, application programming interfaces (APIs), and the user interface (UI) [64]. These tools facilitate the integration between the application layer and the blockchain network. The execution layer encompasses smart contracts, chaincode, and the fundamental regulations that govern their operation [14]. The presentation layer is responsible for transmitting instructions to the execution layer, which in turn executes transactions [14], [63]. For instance, in the Hyperledger Fabric (HF) framework, instructions are transmitted to chaincode, while in the Ethereum Virtual Machine (EVM), they are directed to smart contracts.

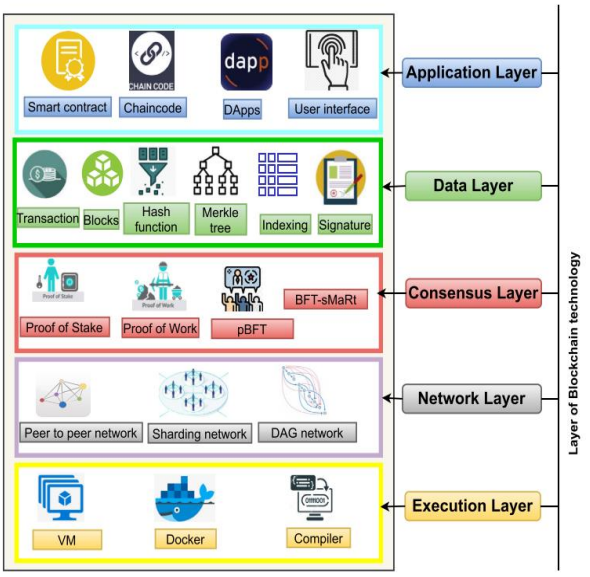

Figure 2:Blockchain Structure. Adopted from [14]

III. BLOCKCHAIN SECURITY

[65] investigated the utilization of blockchain technology to augment the security and efficacy of cross-border electronic commerce. This article examines the challenges associated

with existing e-commerce systems, with a specific focus on document recording, authorization procedures, record sharing effectiveness, and identity verification. The solution being presented utilizes the combination of asymmetric encryption technology and blockchain to establish a system that enables traceability of cross-border e-commerce records, ensures immutability of data, and simplifies the process of identity verification. This technique employs file synchronization contracts and authorization contracts that leverage the unalterable modification capacity of blockchain and asymmetric encryption to safeguard the confidentiality of customers' cross-border e-commerce data.

[66] introduced an innovative strategy for augmenting the security and effectiveness of online document verification by leveraging blockchain technology. The study examined the increasing demand for robust and effective verification and authentication methods for digital documents, which has become increasingly prominent due to the transition towards digitization. The authors present a theoretical framework for a self-sovereign identity (SSI) model that combines blockchain technology and cryptography. [67] introduced an innovative strategy for safeguarding privacy to enhance the security of blockchain technology. This concept incorporates trusted execution environments (TEE) within permissioned blockchain systems. The paper emphasizes several key security elements, namely transparency, anti-interference, traceability, decentralization, and verification. These attributes serve to guarantee the dependability of data on the blockchain through its public nature, hence facilitating consensus and upholding the consistency of the global state.

[68] emphasized the significance of blockchain's distributed ledger in ensuring immutability, a critical aspect for enhancing security in the context of the Internet of Things (IoT). The article highlights the primary security attributes of blockchain, which encompass its decentralized structure that eliminates any singular point of vulnerability, as well as the distinctive linkage of blocks through digital signatures, rendering any modifications to records infeasible without impacting the entirety of the chain. The additional security measures employed in this context encompass the utilization of cryptographic techniques for the purpose of information exchange, as well as the implementation of secure hashing algorithms (SHA) and elliptic curve digital signature algorithms (ECDSA). [69] introduced a novel system that effectively combines the functionalities of email and blockchain technology to facilitate the secure transmission of official documents. The study highlights the primary security attributes of blockchain, notably its decentralized architecture that mitigates the vulnerability of individual nodes and strengthens the overall resilience of the system. The utilization of blockchain technology guarantees the maintenance of safe and transparent record-keeping for document exchanges, owing to its inherent attributes of integrity, reliability, traceability, and non-repudiation. To incorporate these security measures, the system utilizes a consortium blockchain, which securely retains all transferred logs, receipts, and user registration information in a consistent and auditable manner. The system incorporates smart contracts that encompass many functionalities.

[70] explored the creation and implementation of a management platform that is specifically designed to increase the security and integrity of blockchain networks. The primary objective of the platform was to mitigate the prevalent issues of unauthorized data transmission and hostile cyber-attacks within blockchain networks, thereby addressing the substantial obstacles they present to their overall ecological security. The paper highlighted the fundamental security attributes of blockchain, which encompass its decentralized structure that mitigates the risk of individual node failures and bolsters the overall resilience of the system. [71] presented a security management scheme that utilizes blockchain technology. The scheme is specifically tailored to address the requirements of collecting, storing, and accessing telemetry data in optical networks. The proposed system utilized smart contracts on the Ethereum blockchain, in conjunction with the InterPlanetary File System (IPFS), to augment the security of telemetry data in terms of its collection, storage, and accessibility. The blockchain system incorporates security measures in the form of two smart contracts, namely the Data Collection Smart Contract (DCSC) and the Data Management Smart Contract (DMSC).

[72] examined the potential of utilizing blockchain technology, namely Hyperledger Fabric, to enhance the security aspects of the Internet of Things (IoT). The study delves into the topic of a blockchain-based IoT security authentication system. The primary security feature under discussion is the IoT-chain, which is a security authentication system that incorporates blockchain technology to facilitate dynamic administration of security certification in the context of the Internet of Things (IoT). The system consists of three types of chain codes: the access code, which serves as the main program responsible for user safety authentication; the device code, which enables the retrieval of the URL of resource data generated by storage devices; and the policy code, which presents access control strategies for administrator users. The process of implementing IoT-chain encompasses multiple stages. Firstly, a device resource sharing model is established, which links IoT device data with matching URLs. Additionally, the proposal introduces a distributed architectural system that facilitates the administration of access privileges and augments the security of device resources. The structure demonstrates a proficient approach in tackling the obstacles presented by conventional

centralized security authentication methods, which encounter difficulties in providing adequate security authentication within the contemporary Internet of Things (IoT) landscape.

[71] presented a security management scheme that utilizes blockchain technology. The scheme is specifically tailored to address the requirements of collecting, storing, and accessing telemetry data in optical networks. The proposed system utilized smart contracts on the Ethereum blockchain, in conjunction with the InterPlanetary File System (IPFS), to augment the security of telemetry data in terms of its collection, storage, and accessibility. The blockchain system incorporates security measures in the form of two smart contracts, namely the Data Collection Smart Contract (DCSC) and the Data Management Smart Contract (DMSC). The responsibility of DCSC encompasses the authentication of identification during the process of data collecting, with a specific focus on maintaining the integrity of telemetry subscription information. The Data Management and Security Center (DMSC) is responsible for the secure storage of data and the implementation of established security access control protocols for data retrieval. This methodology effectively tackles the difficulties linked to centralized storage, including the potential vulnerability of a sole point of failure and the manipulation of data. [73] investigated the utilization of blockchain technology in combination with Elliptic Curve Diffie-Hellman to bolster the security measures of instant messaging programs. The primary objective was to ensure that the communication transmitted via these applications remains exclusively accessible to the designated receivers, hence offering a heightened level of security compared to conventional encryption techniques. This strategy capitalizes on the decentralized characteristics of blockchain technology, which guarantees the preservation of data integrity and security. The utilization of robust encryption and hashing methods renders the data highly resistant to hacking or destruction. The application described in the paper utilizes the Ethereum blockchain and Solidity smart contracts for the purpose of overseeing user registration, login, friend management, and encrypted messaging. The method facilitates direct communication between users, enabling them to exchange messages without the need for any intermediary entities. This characteristic aligns with the fundamental principle of End-to-End Encryption.

[74] examined the security implications of utilizing blockchain technology inside the realm of digital currency transactions. The central focus of this work revolves around the utilization of the Practical Byzantine Fault Tolerance (PBFT) algorithm within the context of blockchain technology, with the aim of augmenting the level of data security, specifically in relation to transactions using digital currencies. The intrinsic characteristics of blockchain, such as unforgeability, traceability, openness, and transparency, establish a robust basis of trust, which is essential for the functioning of digital money. Nevertheless, the transparency of blockchain data may provide security vulnerabilities, particularly in the context of digital currency transactions. In order to tackle this issue, the study proposed the utilization of the Practical Byzantine Fault Tolerance (PBFT) consensus method in conjunction with the incorporation of support for various channels into alliance blockchain super ledgers. This methodology guarantees the protection of data privacy throughout the transmission of digital currency by facilitating the mutual separation of data across distinct channels. The implementation of Practical Byzantine Fault Tolerance (PBFT) in blockchain entails the partitioning of nodes into two distinct categories: accounting nodes and common nodes. Furthermore, this study examines the utilization of encryption methods, encompassing both symmetric and asymmetric approaches, for the purpose of safeguarding digital currency data.

[75] centers on the augmentation of blockchain security by means of incorporating machine learning (ML) methodologies and Software Defined Networking (SDN). The paper provides an overview of the vulnerabilities of blockchain technology to cyberattacks, despite its strong security and dependability features. The authors suggest employing machine learning techniques in combination with software-defined networking (SDN) to identify and mitigate security breaches in blockchain networks. The primary security aspect examined in the study is the use of an anomaly-based detection method. This method involves the utilization of an encoder-decoder model that has been trained on blockchain activity. Its purpose is to discover a typical pattern that may suggest the presence of potential attacks. The approach demonstrates proficiency in identifying zero-day attacks that exploit undisclosed vulnerabilities, owing to its capacity to identify deviations from typical network patterns. The execution of this security methodology entails the utilization of a blockchain framework on the Ethereum platform, wherein several smart contracts are put on the chain to oversee tasks such as verification and tracing. The framework's machine learning component employs unsupervised learning techniques, mostly due to the infrequency of attack occurrences and the absence of labeled data.

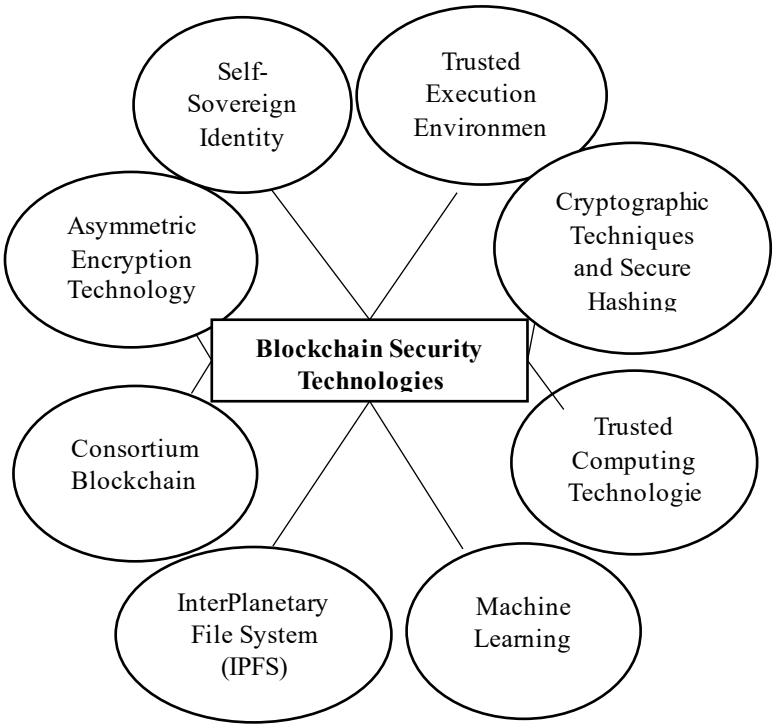

Figure 3: Technologies of Blockchain Security. Source: Author's construct

Figure 3 centers on "Blockchain Security Technologies," illustrating several blockchain security solutions. It comprises of Trusted Execution Environments, which protect sensitive data processing, and the Self-Sovereign Identity (SSI) concept, which gives people authority over their identity data. While trustworthy system behaviors are provided by Trusted Computing Technologies, data integrity and secrecy are guaranteed by Cryptographic Techniques and Secure Hashing Algorithm. Through anomaly detection and predictive analysis, machine learning improves security; decentralized storage and data sharing are made possible via the InterPlanetary File System (IPFS). Because only authorized participants can access consortium blockchains, security and privacy are improved, and Asymmetric Encryption Technology uses public and private key pairs to secure transactions and communications. These elements taken together guarantee the reliability and security of blockchain systems.

IV. BLOCKCHAIN PRIVACY

[76] presented a thorough examination of blockchain security and privacy with an emphasis on its intrinsic qualities, weaknesses, and solutions. The study emphasises how blockchain is both a groundbreaking decentralized ledger technology and a system with privacy issues. Advanced cryptographic solutions that address privacy concerns include consensus algorithms like Proof of Work and Byzantine fault-tolerant mechanisms, hash-chained storage that uses hash pointers and Merkle trees, and privacy-enhancing technologies like anonymous signatures, secure multi-party computation (SMPC), and non-interactive zero-knowledge proofs (NIZK). Along with highlighting the significance of privacy features like anonymity, unlikability, and data confidentiality for strong blockchain systems, the authors also compare blockchain transaction models, highlighting Ethereum's account-based system for balance simplicity and Bitcoin's UTXO model for unlikability.

[77] suggested a lightweight blockchain-based framework dubbed Lib-Pri as a privacy-preserving solution for smart surveillance systems. The project integrates blockchain, smart contracts, object identification, and edge computing technologies to solve privacy issues related to widespread video monitoring. The Lib-Pri system uses privacy-preserving smart contracts and a private, permissioned blockchain to establish and enforce access rights. By using off-chain storage for sensitive data and real-time privacy enforcement at the edge through smart cameras, it guarantees safe video access and storage. [78] addresses the privacy hazards associated with decentralized and transparent systems, examines privacy-preserving techniques in blockchain technology. The study draws attention to how blockchain is being used in industries like healthcare, education, and banking while highlighting how vulnerable user and transactional data are to inference attacks on public ledgers. Among the privacy methods covered are attribute-based signatures, zero-knowledge proofs, secure multi-party computing, anonymization, and differential privacy. The authors stress how crucial it is to incorporate privacy-preserving features like pseudonymization and smart contract-based access control to safeguard private information while keeping the integrity of the blockchain. According to the study's findings, allowing user-defined access and anonymizing data are two of the best practices; scalability and application-specific solutions should be the main goals of future research. [79] offered a thorough examination of blockchain technology's privacy and security risks.

It examines the decentralized, unchangeable nature of blockchain technology and its uses in a range of industries, including supply chains, healthcare, and banking. The authors stress how crucial privacy-preserving tools like consensus processes, smart contracts, and cryptographic algorithms are to protecting private information and facilitating open transactions.

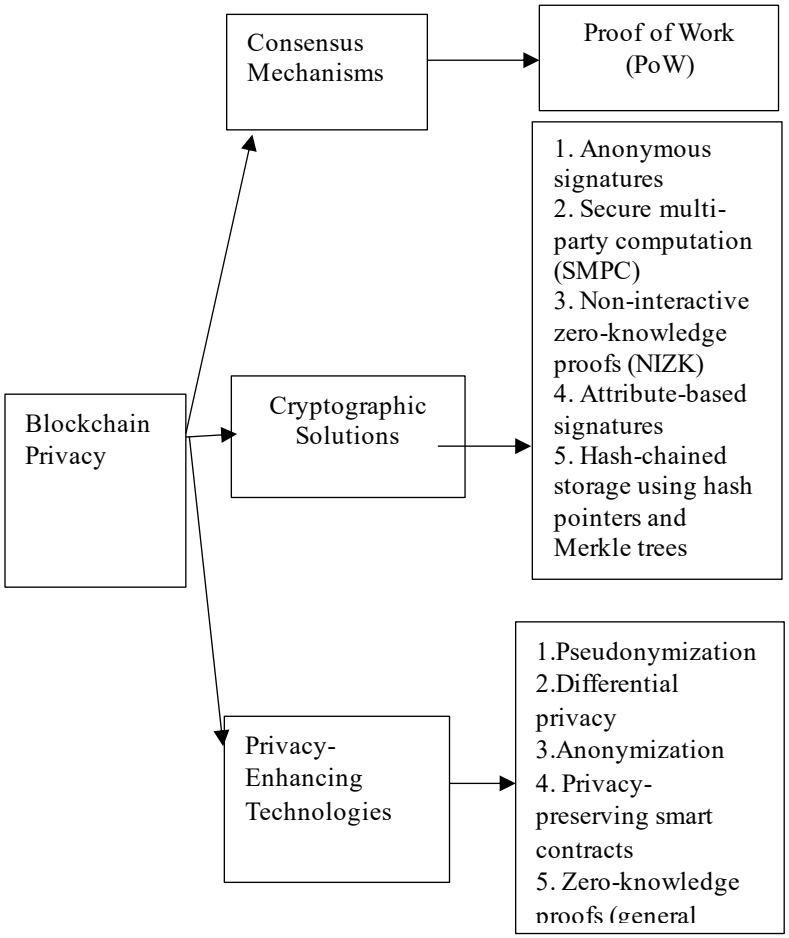

Figure 4: Blockchain Privacy. Source: Author's construct

V. TYPES OF PRIVACY IN BLOCKCHAIN

Sowmiya & Poovammal (2020) identified two categories of privacy in blockchain. They are identity and data privacy.

A. Identity Privacy

The distinct blockchain address of the specific node that completed the transaction is used to identify transactions on the blockchain network. To protect the user's privacy, the node's identity is kept a mystery. When it comes to user identity privacy, security and privacy always intersect. By examining the connections between the transactions that a certain user makes, the attacker can determine the individual's attributes. For instance, common traits such as location, sex, age range, etc. It is crucial to keep personal information hidden from other network users. Blockchain technology's privacy-preserving identity management approaches might help achieve this.

B. Data Privacy

Any node on the blockchain may access the data as it is kept in the global ledger. Every transaction recorded on the blockchain could conceal important personal data. Encrypting the transaction prior to outsourcing is the conventional technique for preventing data manipulation. The validator must confirm the transaction's legitimacy without revealing any important information if every transaction is encrypted and sent to the ledger. Certain protocols, cryptographic algorithms, and privacy-preserving techniques must be modified to get around this obstacle.

VI. BLOCKCHAIN SECURITY AND PRIVACY ISSUES

[79] highlighted critical flaws in blockchain security and privacy. The authors argued that issues are brought on by network latency and transaction handling capacity limitations, data privacy hazards resulting from blockchain's openness, and consensus mechanism flaws such vulnerability to majority (51%) assaults are among the main dangers. The findings of the study further argued that despite their benefits, smart contracts are vulnerable to code errors that hackers might take advantage of. Integration across networks is made more difficult by interoperability problems brought on by the absence of common protocols. The study also indicated that while permission blockchains are vulnerable to centralization flaws that might lead to single points of failure, regulatory uncertainties present compliance problems. Furthermore, the resilience of existing cryptographic methods is called into question by the imminence of quantum computing.

[76] also examined security and privacy issues with blockchain. In the study, major concerns were identified, such as the need for strong cryptographic techniques to prevent data tampering, the vulnerability of decentralized consensus to majority (51%) assaults, and the inherent hazards of pseudonymity, which might enable malevolent actors to conceal their identity. The paper also highlights the limits of attaining complete consistency across distributed ledgers and the double-spending issue in bitcoin systems. The authors also drew attention to the difficulties with confidentiality and unlikability in transactions, since statistical analysis may be able to deduce or link sensitive user data. These flaws according to the study highlight the necessity of stronger consensus algorithms and improved privacy-preserving strategies to strengthen blockchain's security and privacy architecture.

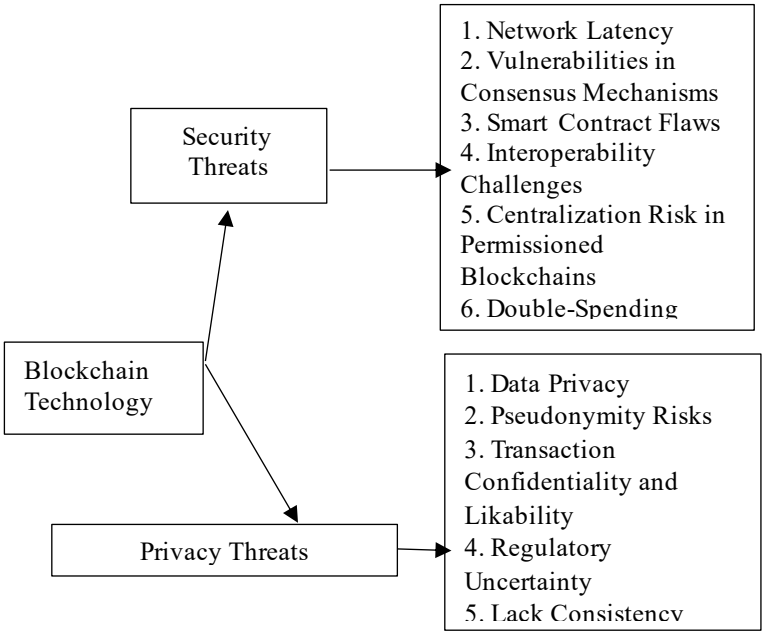

Figure 5: Blockchain Privacy and Security Issues. Source: Author's construct

VII. CRYPTOGRAPHY

Cryptography, meaning "secret writing," protects data secrecy, integrity, authentication, and non-repudiation [80]. This concept uses ways to turn plain text into ciphertext that only authorized parties may decrypt with a key. Cryptography protects data against illegal access [81]. For encryption and decryption, algorithms and keys are used. There are symmetric and asymmetric encryption methods [82]. Traditional symmetric encryption uses the same key for encryption and decryption, requiring secure key sharing [83]. Instead, asymmetric encryption protects communication without key exchange using a public key for encryption and a private key for decryption [84]. New cryptographic approaches like Public Key Infrastructure (PKI) ease secure key exchange [83], [84]. Public keys can be freely shared for secure stranger conversation. Businesses provide their public keys to encrypt sensitive data like credit card details. Digital signatures, another cryptography breakthrough, validate sender identity and content integrity to ensure digital communication validity. For data integrity, cryptographic systems use hash functions, which create a fixed-size output from an arbitrary input. Strong algorithms like Rivest Shamir Adleman (RSA) [85], Advanced Encryption Standard (AES) [86], and Elliptic Curve Cryptography (ECC) [87] address current security challenges.

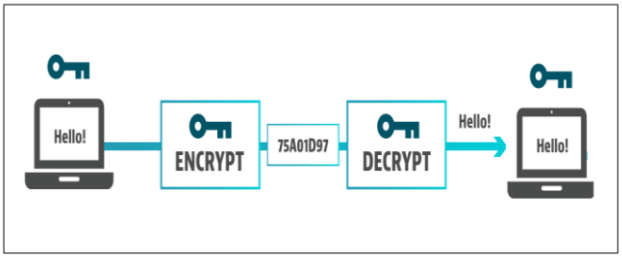

Figure 6: Concept of Blockchain Cryptography. Source: [80]

VIII. CRYPTOGRAPHY MEASURES IN SOLVING SECURITY AND PRIVACY ISSUES IN BLOCKCHAIN

A. *Public and Private Key Cryptography*

Blockchain security relies on asymmetric cryptography, which employs public and private keys [86]. Every user has a hidden private key and a public key. Signing transactions with the sender's private key ensures their legitimacy. The public key lets third parties verify the signature without the private key. This approach prevents tampering and unwanted access by restricting transaction initiation to the genuine owner.

B. *Hash Functions*

Blockchain data accuracy depends on hash functions [88]. Their output is a random, fixed-length string of characters. A blockchain chain is formed when each block hashes the previous one. Any data change would modify a block's hash, invalidating subsequent blocks and notifying the network of probable manipulation. After recording, this structure prevents covert data changes.

C. *Zero-Knowledge Proofs*

With zero knowledge proof, one person can prove a claim is true without revealing further facts [89]. ZKPs validate blockchain transactions without exposing transaction details, improving privacy. ZKPs allow shielded transactions in cryptocurrencies like Zcash, protecting transaction amounts and participants.

D. *Ring Signatures*

Ring signatures allow group members to sign communications anonymously(Liu et al., 2020). By concealing transaction sources, this strategy promotes privacy. Ring signatures safeguard Monero's anonymity by preventing transaction identification.

E. *Homomorphic Encryption*

Homomorphic encryption allows computations on encrypted data without decrypting it, resulting in an encrypted output that matches plaintext operations [91].

This enables blockchain smart contracts and transactions while protecting data.

References

[1] V. Stallone, M. Wetzels, and M. Klaas, "Applications of Blockchain Technology in marketing — A systematic review of marketing technology companies," *Blockchain Res. Appl.*, vol. 2, no. 3, p. 100023, 2021, doi: 10.1016/j.bcra.2021.100023.

[2] A. Sadu, A. Jindal, G. Lipari, F. Ponci, and A. Monti, "Resilient design of distribution grid automation system against cyber-physical attacks using blockchain and smart contract," *Blockchain Res. Appl.*, vol. 2, no. 1, p. 100010, 2021, doi: 10.1016/j.bcra.2021.100010.

[3] A. Laurent, L. Brotcorne, and B. Fortz, "Transaction fees optimization in the Ethereum blockchain," *Blockchain Res. Appl.*, vol. 3, no. 3, p. 100074, 2022, doi: 10.1016/j.bcra.2022.100074.

[4] M. Mazzoni, A. Corradi, and V. Di, "Performance evaluation of permissioned blockchains for fi nancial applications : The ConsenSys Quorum case study," *Blockchain Res. Appl.*, vol. 3, no. 1, p. 100026, 2022, doi: 10.1016/j.bcra.2021.100026.

[5] L. Mosley, H. Pham, X. Guo, Y. Bansal, E. Hare, and N. Antony, "Towards a systematic understanding of blockchain governance in proposal voting: A dash case study," *Blockchain Res. Appl.*, vol. 3, no. 3, p. 100085, 2022, doi: 10.1016/j.bcra.2022.100085.

[6] A. Sarfaraz, R. K. Chakrabortty, and D. L. Essam, "The implications of blockchain-coordinated information sharing within a supply chain: A simulation study," *Blockchain Res. Appl.*, vol. 4, no. 1, p. 100110, 2023, doi: 10.1016/j.bcra.2022.100110.

[7] L. Hang and D. Kim, "Optimal blockchain network construction methodology based on analysis of con fi gurable components for enhancing Hyperledger Fabric performance," *Blockchain Res. Appl.*, vol. 2, no. 1, p. 100009, 2021, doi: 10.1016/j.bcra.2021.100009.

[8] H. Chen, X. Luo, L. Shi, Y. Cao, and Y. Zhang, "Security challenges and defense approaches for blockchain-based services from a full-stack architecture perspective," *Blockchain Res. Appl.*, vol. 4, no. 3, p. 100135, 2023, doi: 10.1016/j.bcra.2023.100135.

[9] S. Mojtaba, H. Bamakan, A. Babaei, and P. Babaei, "Blockchain technology forecasting by patent analytics and text mining," *Blockchain Res. Appl.*, vol. 2, no. 2, p. 100019, 2021, doi: 10.1016/j.bcra.2021.100019.

[10] K. Hunt, A. Narayanan, and J. Zhuang, "Blockchain in humanitarian operations management: A review of research and practice," *Socioecon. Plann. Sci.*, vol. 80, no. October 2021, p. 101175, 2022, doi: 10.1016/j.seps.2021.101175.

[11] X. Xu, Y. Guo, and Y. Guo, "Fog-enabled private blockchain-based identity authentication scheme for smart home," *Comput. Commun.*, vol. 205, no. April, pp. 58–68, 2023, doi: 10.1016/j.comcom.2023.04.005.

[12] M. Antwi, A. Adnane, F. Ahmad, R. Hussain, M. H. ur Rehman, and C. A. Kerrache, "The case of HyperLedger Fabric as a blockchain solution for healthcare applications," *Blockchain Res. Appl.*, vol. 2, no. 1, p. 100012, 2021, doi: 10.1016/j.bcra.2021.100012.

[13] S. Krishnakumar, I. Taylor, J. Nabrzyski, and I. Barclay, "Verifiable Badging System for scientific data reproducibility," *Blockchain Res. Appl.*, vol. 2, 2021, doi: 10.1016/j.bcra.2021.100015.

[14] A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in IoT : challenges and solutions," *Blockchain Res. Appl.*, vol. 2, no. 2, p. 100006, 2021, doi: 10.1016/j.bcra.2021.100006.

[15] E. hacen Diallo, O. Dib, and K. Al Agha, "A scalable blockchain-based scheme for traffic-related data sharing in VANETs," *Blockchain Res. Appl.*, vol. 3, no. 3, p. 100087, 2022, doi: 10.1016/j.bcra.2022.100087.

[16] R. Belen-Saglam, E. Altuncu, Y. Lu, and S. Li, "A systematic literature review of the tension between the GDPR and public blockchain systems," *Blockchain Res. Appl.*, vol. 4, no. 2, p. 100129, 2023, doi: 10.1016/j.bcra.2023.100129.

[17] I. Merrell, "Blockchain for decentralised rural development and governance," *Blockchain Res. Appl.*, vol. 3, no. 3, p. 100086, 2022, doi: 10.1016/j.bcra.2022.100086.

[18] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain Res. Appl.*, vol. 3, no. 2, p. 100067, 2022, doi: 10.1016/j.bcra.2022.100067.

[19] D. López and B. Farooq, "A multi-layered

blockchain framework for smart mobility data-markets," *Transp. Res. Part C Emerg. Technol.*, vol. 111, pp. 588–615, 2020, doi: 10.1016/j.trc.2020.01.002.

[20] Y. Yuan and F. Y. Wang, "Blockchain and Cryptocurrencies: Model, Techniques, and Applications," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 48, no. 9, pp. 1421–1428, 2018, doi: 10.1109/TSMC.2018.2854904.

[21] P. Wang and S. Qiao, "Emerging Applications of Blockchain Technology on a Virtual Platform for English Teaching and Learning," *Wirel. Commun. Mob. Comput.*, 2020, doi: 10.1155/2020/6623466.

[22] Y. Xinyi, Z. Yi, and Y. He, "Technical Characteristics and Model of Blockchain," in *2018 10th International Conference on Communication Software and Networks, ICCSN 2018*, 2018, pp. 562–566. doi: 10.1109/ICCSN.2018.8488289.

[23] P. C. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, "Blockchain data-based cloud data integrity protection mechanism," *Futur. Gener. Comput. Syst.*, vol. 102, pp. 902–911, 2020, doi: 10.1016/j.future.2019.09.028.

[24] E. Bandara *et al.*, "Mystiko - Blockchain Meets Big Data," *Proc. - 2018 IEEE Int. Conf. Big Data, Big Data 2018*, pp. 3024–3032, 2018, doi: 10.1109/BigData.2018.8622341.

[25] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, 2018, doi: 10.1109/TKDE.2017.2781227.

[26] Y. Ren, Y. Liu, S. Ji, A. K. Sangaiah, and J. Wang, "Incentive Mechanism of Data Storage Based on Blockchain for Wireless Sensor Networks," *Mob. Inf. Syst.*, 2018, doi: 10.1155/2018/6874158.

[27] W. Gao, W. G. Hatcher, and W. Yu, "A survey of blockchain: Techniques, applications, and challenges," *Proc. - Int. Conf. Comput. Commun. Networks, ICCCN*, no. i, pp. 1–11, 2018, doi: 10.1109/ICCCN.2018.8487348.

[28] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain Based Data Integrity Service Framework for IoT Data," *Proc. - 2017 IEEE 24th Int. Conf. Web Serv. ICWS 2017*, pp. 468–475, 2017, doi: 10.1109/ICWS.2017.54.

[29] Z. Wang, Y. Tian, and J. Zhu, "Data Sharing and Tracing Scheme Based on Blockchain," *8th Int. Conf. Logist. Informatics Serv. Sci. LISS 2018 - Proceeding*, no. 61662009, pp. 1–6, 2018, doi: 10.1109/LISS.2018.8593225.

[30] L. Guo, H. Xie, and Y. Li, "Data encryption based blockchain and privacy preserving mechanisms towards big data," *J. Vis. Commun. Image Represent.*, vol. 70, 2020, doi: 10.1016/j.jvcir.2019.102741.

[31] Y. Chen, H. Li, K. Li, and J. Zhang, "An improved P2P file system scheme based on IPFS and Blockchain," *Proc. - 2017 IEEE Int. Conf. Big Data, Big Data 2017*, 2017, doi: 10.1109/BigData.2017.8258226.

[32] J. Kan and K. S. Kim, "MTFS: Merkle-Tree-Based File System," in *ICBC 2019 - IEEE International Conference on Blockchain and Cryptocurrency*, 2019, pp. 43–47. doi: 10.1109/BLOC.2019.8751389.

[33] D. M. Nguyen, Q. H. Luu, N. Huynh-Tuong, and H. A. Pham, "MB-PBA: Leveraging Merkle Tree and Blockchain to Enhance User Profile-based Authentication in E-Learning Systems," in *Proceedings - 2019 19th International Symposium on Communications and Information Technologies, ISCIT 2019*, 2019, pp. 392–397. doi: 10.1109/ISCIT.2019.8905114.

[34] A. P. Mohan, M. R. Asfak, and A. Gladston, "Merkle Tree and Blockchain-Based Cloud Data Auditing," *Int. J. Cloud Appl. Comput.*, vol. 10, no. 3, pp. 54–66, 2020, doi: 10.4018/IJCAC.2020070103.

[35] D. Lee and N. Park, "Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree," *Multimed. Tools Appl.*, vol. 80, no. 26–27, pp. 34517–34534, 2021, doi: 10.1007/s11042-020-08776-y.

[36] H. Zhu, Y. Guo, and L. Zhang, "An improved convolution Merkle tree-based blockchain electronic medical record secure storage scheme," *J. Inf. Secur. Appl.*, vol. 61, no. August, 2021, doi: 10.1016/j.jisa.2021.102952.

[37] C. Castellon, S. Roy, P. Kreidl, A. Dutta, and L. Boloni, "Energy Efficient Merkle Trees for Blockchains," in *Proceedings - 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2021*, 2021, pp. 1093–1099. doi: 10.1109/TrustCom53373.2021.00149.

[38] A. Mizrahi, N. Koren, and O. Rottenstreich, "Optimizing Merkle Proof Size for Blockchain Transactions," in *2021 International Conference on*

COMmunication Systems and NETworkS, COMSNETS 2021, 2021, vol. 2061, no. Section VI, pp. 299–307. doi: 10.1109/COMSNETS51098.2021.9352820.

[39] J. Chen, Z. Lv, and H. Song, "Design of personnel big data management system based on blockchain," *Futur. Gener. Comput. Syst.*, vol. 101, pp. 1122–1129, 2019, doi: 10.1016/j.future.2019.07.037.

[40] X. Zou and P. Zeng, "A New Digital Signature Primitive and Its Application in Blockchain," *IEEE Access*, vol. 11, no. June, pp. 54607–54615, 2023, doi: 10.1109/ACCESS.2023.3280638.

[41] A. Mehbodniya, J. L. Webber, R. Neware, F. Arslan, R. V. Pamba, and M. Shabaz, "Modified Lamport Merkle Digital Signature blockchain framework for authentication of internet of things healthcare data," *Expert Syst.*, vol. 39, no. 10, 2022, doi: 10.1111/exsy.12978.

[42] S. Singh, N. K. Rajput, V. K. Rathi, H. M. Pandey, A. K. Jaiswal, and P. Tiwari, "Securing Blockchain Transactions Using Quantum Teleportation and Quantum Digital Signature," *Neural Process. Lett.*, vol. 55, no. 4, pp. 3827–3842, 2023, doi: 10.1007/s11063-020-10272-1.

[43] S. J. Basha, V. S. Veesam, T. Ammannamma, S. Navudu, and M. V. V. S. Subrahmanyam, "Security enhancement of digital signatures for blockchain using EdDSA algorithm," in *Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV 2021*, 2021, no. Icicv, pp. 274–278. doi: 10.1109/ICICV50876.2021.9388411.

[44] M. Yusup, D. Cahvadi, E. Febriyanto, Mardiana, and F. Budiarty, "The Impact of Socio- Economic in Digital Signature Using Blockchain Application," in *2020 8th International Conference on Cyber and IT Service Management, CITSM 2020*, 2020, pp. 19–24. doi: 10.1109/CITSM50537.2020.9268893.

[45] V. Bralić, H. Stančić, and M. Stengård, "A blockchain approach to digital archiving: digital signature certification chain preservation," *Rec. Manag. J.*, vol. 30, no. 3, pp. 345–362, 2020, doi: 10.1108/RMJ-08-2019-0043.

[46] Y. Hao, Y. Li, X. Dong, L. Fang, and P. Chen, "Performance Analysis of Consensus Algorithm in Private Blockchain," *IEEE Intell. Veh. Symp. Proc.*, vol. 2018-June, no. Iv, pp. 280–285, 2018, doi: 10.1109/IVS.2018.8500557.

[47] N. Chaudhry and M. M. Yousaf, "Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities," in *ICOSST 2018 - 2018 International Conference on Open Source Systems and Technologies, Proceedings*, 2019, pp. 54–63. doi: 10.1109/ICOSST.2018.8632190.

[48] M. Kaur and S. Gupta, "Blockchain Consensus Protocols: State-of-the-art and Future Directions," in *Proceedings of International Conference on Technological Advancements and Innovations, ICTAI 2021*, 2021, pp. 446–453. doi: 10.1109/ICTAI53825.2021.9673260.

[49] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, and M. A. Imran, "A Scalable Multi-Layer PBFT Consensus for Blockchain," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 5, pp. 1146–1160, 2021, doi: 10.1109/TPDS.2020.3042392.

[50] D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos, and G. Das, "Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems," *2019 IEEE Int. Conf. Consum. Electron. ICCE 2019*, pp. 1–5, 2019, doi: 10.1109/ICCE.2019.8662009.

[51] X. Xu, D. Zhu, X. Yang, S. Wang, L. Qi, and W. Dou, "Concurrent Practical Byzantine Fault Tolerance for Integration of Blockchain and Supply Chain," *ACM Trans. Internet Technol.*, vol. 21, no. 1, pp. 1–17, 2021, doi: 10.1145/3395331.

[52] O. Onireti, L. Zhang, and M. A. Imran, "On the viable area of wireless practical byzantine fault tolerance (PBFT) blockchain networks," in *2019 IEEE Global Communications Conference, GLOBECOM 2019 - Proceedings*, 2019, pp. 1–6. doi: 10.1109/GLOBECOM38437.2019.9013778.

[53] A. Pal and K. Kant, "DC-PoET: Proof-of-Elapsed-Time Consensus with Distributed Coordination for Blockchain Networks," in *2021 IFIP Networking Conference, IFIP Networking 2021*, 2021, pp. 1–9. doi: 10.23919/IFIPNetworking52078.2021.9472787.

[54] D. Tosh, S. Shetty, P. Foytik, C. Kamhoua, and L. Njilla, "CloudPoS: A Proof-of-Stake Consensus Design for Blockchain Integrated Cloud," in *IEEE International Conference on Cloud Computing, CLOUD*, 2018, pp. 302–309. doi: 10.1109/CLOUD.2018.00045.

[55] B. M. Yakubu, M. M. Ahmad, A. B. Sulaiman, A. S. Kazaure, M. I. Khan, and N. Javaid, "Blockchain based smart marketplace for secure internet bandwidth trading," in *2021 1st International Conference on Multidisciplinary Engineering and*

Applied Science, ICMEAS 2021, 2021, pp. 1–6. doi: 10.1109/ICMEAS52683.2021.9692424.

[56] N. Al Asad, M. T. Elahi, A. Al Hasan, and M. A. Yousuf, "Permission-based blockchain with proof of authority for secured healthcare data sharing," in *2020 2nd International Conference on Advanced Information and Communication Technology, ICAICT 2020*, 2020, pp. 35–40. doi: 10.1109/ICAICT51780.2020.9333488.

[57] Q. Dai, B. Zhang, and S. Dong, "A DDoS-Attack Detection Method Oriented to the Blockchain Network Layer," *Secur. Commun. Networks*, 2022, doi: 10.1155/2022/5692820.

[58] S. Guo, X. Hu, S. Guo, and X. Qiu, "Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System," *IEEE Trans. Ind. Informatics*, vol. 16, no. 3, pp. 1972–1983, 2020, doi: 10.1109/TII.2019.2938001.

[59] T. Neudecker and H. Hartenstein, "Network layer aspects of permissionless blockchains," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 1, pp. 838–857, 2019, doi: 10.1109/COMST.2018.2852480.

[60] D. Fu and L. Fang, "Blockchain-based trusted computing in social network," in *2016 2nd IEEE International Conference on Computer and Communications, ICCC 2016 - Proceedings*, 2017, pp. 19–22. doi: 10.1109/CompComm.2016.7924656.

[61] S. Guo, X. Hu, Z. Zhou, X. Wang, F. Qi, and L. Gao, "Trust access authentication in vehicular network based on blockchain," *China Commun.*, vol. 16, no. 6, pp. 18–30, 2019, doi: 10.23919/j.cc.2019.06.002.

[62] F. Glaser, F. Hawlitschek, and B. Notheisen, "Business Transformation through Blockchain," in *Business Transformation through Blockchain*, 2019, pp. 121–143. doi: 10.1007/978-3-319-98911-2.

[63] Y. Qian *et al.*, "Towards decentralized IoT security enhancement: A blockchain approach," *Comput. Electr. Eng.*, vol. 72, pp. 266–273, 2018, doi: 10.1016/j.compeleceng.2018.08.021.

[64] Z. Li, J. Hao, J. Liu, H. Wang, and M. Xian, "An IoT-Applicable Access Control Model under Double-Layer Blockchain," *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 68, no. 6, pp. 2102–2106, 2021, doi: 10.1109/TCSII.2020.3045031.

[65] Z. Hongmei, "A Cross-Border E-Commerce Approach Based on Blockchain Technology," *Mob. Inf. Syst.*, 2021, doi: 10.1155/2021/2006082.

[66] A. Satybaldy, A. Subedi, and M. Nowostawski, "A Framework for Online Document Verification Using Self-Sovereign Identity Technology," *Sensors*, vol. 22, no. 21, 2022, doi: 10.3390/s22218408.

[67] R. Zhou and Z. Lin, "A Privacy Protection Scheme for Permissioned Blockchain Based on Trusted Execution Environment," *Proc. - 2022 Int. Conf. Blockchain Technol. Inf. Secur. ICBCTIS 2022*, pp. 1–4, 2022, doi: 10.1109/ICBCTIS55569.2022.00012.

[68] A. K. Yadav and V. P. Vishwakarma, "Adoptation of Blockchain of Things(BCOT): Oppurtunities & Challenges," in *2022 IEEE International Conference on Blockchain and Distributed Systems Security, ICBDS 2022*, 2022, pp. 1–5. doi: 10.1109/ICBDS53701.2022.9935985.

[69] C. M. Chiu, F. M. Hsu, M. H. Shen, and C. M. Lin, "An Architecture for Electronic Exchange of Official Document Based on Email and Blockchain," *J. Internet Technol.*, vol. 24, no. 2, pp. 333–344, 2023, doi: 10.53106/160792642023032402012.

[70] X. Wang, A. Badshah, S. Tu, and M. Waqas, "Blockchain-Based Security Management Platform," in *Proceedings - 2021 2nd Asia Symposium on Signal Processing, ASSP 2021*, 2021, pp. 118–121. doi: 10.1109/ASSP54407.2021.00026.

[71] H. Zhu *et al.*, "Blockchain-enabled Data Security Management for Optical Network Telemetry," in *2023 21st International Conference on Optical Communications and Networks (ICOCN)*, 2023, pp. 1–3. doi: 10.1109/icocn59242.2023.10236015.

[72] Z. Gong-Guo and Z. Wan, "Blockchain-based IoT security authentication system," in *Proceedings - 2021 International Conference on Computer, Blockchain and Financial Development, CBFD 2021*, 2021, pp. 415–418. doi: 10.1109/CBFD52659.2021.00090.

[73] P. Pansara, R. Patel, K. Shah, R. Jhaveri, and V. Parmar, "Chat Application Security: Implementing Blockchain-based End-to-End Encryption," in *Proceedings of the 17th INDIACom; 2023 10th International Conference on Computing for Sustainable Global Development, INDIACom 2023*, 2023, pp. 496–500.

[74] M. Xie, Z. Liao, and L. Huang, "Data Security Based on Blockchain Digital Currency," in

Proceedings - 2020 3rd International Conference on Smart BlockChain, SmartBlock 2020, 2020, pp. 5–10. doi: 10.1109/SmartBlock52591.2020.00009.

[75] S. Gaba, I. Budhiraja, A. Makkar, and D. Garg, "Machine Learning for Detecting Security Attacks on Blockchain using Software Defined Networking," in *2022 IEEE International Conference on Communications Workshops, ICC Workshops 2022*, 2022, pp. 260–264. doi: 10.1109/ICCWorkshops53468.2022.9814656.

[76] R. Zhang, R. Xue, and L. Liu, "Security and Privacy on Blockchain Applications," *Explor. Blockchain Appl. Manag. Perspect.*, vol. 52, no. 3, pp. 63–75, 2019, doi: 10.1201/9781003389552-5.

[77] A. Fitwi, Y. Chen, and S. Zhu, "A lightweight blockchain-based privacy protection for smart surveillance at the edge," in *Proceedings - 2019 2nd IEEE International Conference on Blockchain, Blockchain 2019*, 2019, pp. 552–555. doi: 10.1109/Blockchain.2019.00080.

[78] B. Sowmiya and E. Poovammal, "Methods and techniques for privacy preserving in blockchain," in *Proceedings of the 3rd International Conference on Intelligent Sustainable Systems, ICISS 2020*, 2020, pp. 1346–1351. doi: 10.1109/ICISS49785.2020.9316115.

[79] K. Sharma, N. Kumar, and R. K. Kaushal, "Privacy and Security in Blockchain: A Comprehensive Analysis of Techniques and Threats," in *2023 IEEE International Conference on Blockchain and Distributed Systems Security, ICBDS 2023*, 2023, pp. 1–6. doi: 10.1109/ICBDS58040.2023.10346542.

[80] A. M. Qadir and N. Varol, "A review paper on cryptography," in *7th International Symposium on Digital Forensics and Security, ISDFS 2019*, 2019, pp. 1–6. doi: 10.1109/ISDFS.2019.8757514.

[81] S. K. Routray, M. K. Jha, L. Sharma, R. Nyamangoudar, A. Javali, and S. Sarkar, "Quantum cryptography for IoT: APerspective," 2017. doi: 10.1109/ICIOTA.2017.8073638.

[82] V. Padamvathi, B. V. Vardhan, and A. V. N. Krishna, "Quantum Cryptography and Quantum Key Distribution Protocols: A Survey," in *Proceedings - 6th International Advanced Computing Conference, IACC 2016*, 2016, pp. 556–562. doi: 10.1109/IACC.2016.109.

[83] M. Moizuddin, J. Winston, and M. Qayyum, "A comprehensive survey: Quantum cryptography," in *2017 2nd International Conference on Anti-Cyber Crimes, ICACC 2017*, 2017, pp. 98–102. doi: 10.1109/Anti-Cybercrime.2017.7905271.

[84] I. Giroti and M. Malhotra, "Quantum Cryptography: A Pathway to Secure Communication," in *6th IEEE International Conference on Computational System and Information Technology for Sustainable Solutions, CSITSS 2022*, 2022, pp. 1–6. doi: 10.1109/CSITSS57437.2022.10026388.

[85] W. W. Widiyanto, D. Iskandar, S. Wulandari, E. Susena, and E. Susanto, "Implementation Security Digital Signature Using Rivest Shamir Adleman (RSA) Algorithm As A Letter Validation And Distribution Validation System," in *2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC)*, 2022, pp. 599–605. doi: 10.1109/IIHC55949.2022.10060839.

[86] F. M. Kaffah, Y. A. Gerhana, I. M. Huda, A. Rahman, K. Manaf, and B. Subaeki, "E-Mail message encryption using advanced encryption standard (AES) and huffman compression engineering," 2020. doi: 10.1109/ICWT50448.2020.9243651.

[87] P. More, S. Sakhare, and P. Sawane, "Implementation and Analysis of ECC (Elliptic Curve Cryptography) Security Routing Protocol in NS2," in *2023 3rd Asian Conference on Innovation in Technology, ASIANCON 2023*, 2023, pp. 1–5. doi: 10.1109/ASIANCON58793.2023.10270716.

[88] S. K. Sinha and D. Mukhopadhyay, "Time Efficient Hash Key Generation For Blockchain Enabled Framework," *IEEE Access*, no. November, pp. 155867–155884, 2024, doi: 10.1109/ACCESS.2024.3478845.

[89] D. Capko, S. Vukmirovic, and N. Nedic, "State of the Art of Zero-Knowledge Proofs in Blockchain," in *2022 30th Telecommunications Forum, TELFOR 2022 - Proceedings*, 2022, pp. 2022–2025. doi: 10.1109/TELFOR56187.2022.9983760.

[90] X. Liu, M. Zhang, Y. Zheng, and Y. Yang, "A linkable Ring Signature Electronic Cash Scheme Based on Blockchain," in *Proceedings - 2020 3rd International Conference on Smart BlockChain, SmartBlock 2020*, 2020, vol. 1, pp. 163–166. doi: 10.1109/SmartBlock52591.2020.00037.

[91] J. Ryu, K. Kim, and D. Won, "A Study on Partially Homomorphic Encryption," in *Proceedings of the 2023 17th International Conference on Ubiquitous Information Management and Communication, IMCOM 2023*, 2023, no. 2, pp. 1–4. doi:

10.1109/IMCOM56909.2023.10035630.