IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 2 February 2024, accepted 24 February 2024, date of publication 26 February 2024, date of current version 5 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3370857

SURVEY

Navigating the Maze: Exploring Blockchain Privacy and Its Information Retrieval

ARCHANA CHHABRA[1], **RAHUL SAHA**[1], **(Member, IEEE), GULSHAN KUMAR**[1], **(Senior Member, IEEE), AND TAI-HOON KIM**[2], **(Member, IEEE)**

[1]School of Computer Science and Engineering, Lovely Professional University, Phagwara 144001, India
[2]School of Electrical and Computer Engineering, Chonnam National University, Yeosu Campus, Yeosu, Jeollanam 59626, Republic of Korea

Corresponding authors: Tai-Hoon Kim (taihoonn@chonnam.ac.kr) and Rahul Saha (rsahaaot@gmail.com)

ABSTRACT Blockchain networks provide a reliable and secure mode of communication due to their decentralized and distributed nature. The emergence of amalgamated blockchain-based internet-of-things (IoT) systems has generated a huge amount of data to be online. Though blockchains show potential for ensuring transparency, traceability, and immutable records, the privacy of online data in blockchains becomes a question. The privacy of blockchain transactions is at stake as various privacy breaching methods are used by attackers such as linking the transactions, deanonymization, etc. However, the benefits of blockchain make the technology a dominator in the present and future technological paradigms. The other side of the coin deals with privacy information retrieval (PIR), which is necessary to retrieve private information from servers without much revealing. However, the conjunction of blockchain privacy and PIR is very critical and an important aspect of blockchain solutions. In this present survey, we pioneer in analyzing the privacy factors of existing blockchain solutions. We discuss the privacy parameters and important privacy enhancement techniques for blockchains comprehensively. We show the applicability of privacy in various domains including e-commerce, supply chain, healthcare, and IoT. We also discuss PIR-related issues and solutions in the existing literature. We highlight open research problems and discuss the benefits of collaborating with PIR and blockchain systems to improve privacy in blockchains. Our survey is beneficial for academia and industries to be aware of the present status of privacy solutions in blockchains and to address the identified loopholes to make the systems better.

INDEX TERMS Blockchain, information, privacy, retrieval, security, survey.

I. INTRODUCTION

Currently, after the development of Bitcoin, the blockchain is transforming the technology industry and trending in the digital world [3]. It gained popularity in the financial market (cryptocurrency) because of its unique traits such as distributed ledger, consensus mechanism, selection of public and private participation of the nodes, and transaction immutability. With the advancement in technology, blockchain keeps on expanding its roots in different applications namely supply chain, education, healthcare, IoT, and many more after the invention of hyperledger and ethereum [4], [5].

With time the blockchain keeps on rising and ensures a private and secure way of communication among peers in contrast to the centralized systems. For example, it makes it more difficult for a malevolent user to steal data that is publicly available and subsequently steal it from a private central network. The primary goal of blockchain networks is to create decentralization, which solves the centralized system's trust and failure problems. The development and evolution of this revolutionary technology over time are described below covering all five generations, each of which brought new features and capabilities [97], [98] as shown in Figure 1.

- *Blockchain 1.0 (Bitcoin)*:
  - Bitcoin, created by an anonymous entity known as Santoshi Nakamoto, introduced the world to blockchain technology in 2008.
  - Blockchain 1.0 was primarily focused on digital currency and peer-to-peer transactions. It utilized

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

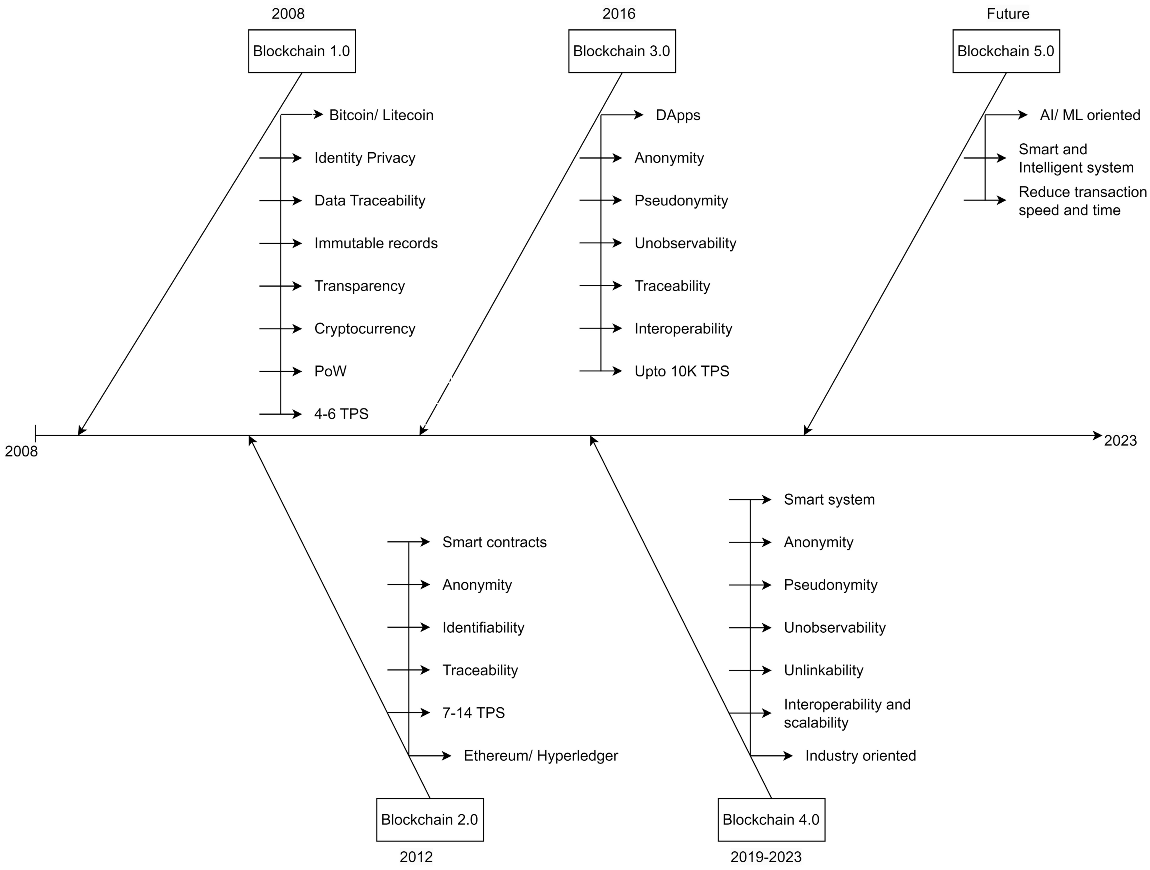

FIGURE 1. Privacy-oriented evolution of Blockchain.

a proof-of-work (PoW) consensus mechanism for security.
  - This generation established the concept of decentralized and trustless transactions.

- *Blockchain 2.0 (Ethereum)*:
  - Ethereum, created by Vitalik Buterin and launched in 2012, was a significant step forward in blockchain technology.
  - Blockchain 2.0 introduced the concept of smart contracts, which are self-executing contracts with predefined rules and conditions.
  - It used the ethereum virtual machine (EVM) to run decentralized applications (DApps).
  - Ethereum popularized the use of initial coin offerings (ICOs) to fund blockchain projects.
- *Blockchain 3.0 (Scalability and Interoperability)*:
  - This generation of blockchain technology aimed to address the scalability and interoperability issues faced by earlier blockchains.
  - Projects like EOS, Cardano, and Polkadot emerged to improve transaction throughput, reduce latency, and enhance compatibility between different blockchains.
  - Proof-of-stake (PoS) and delegated PoS (DPoS) consensus mechanisms gained popularity for their energy efficiency and scalability.
- *Blockchain 4.0 (Integration of Advanced Technologies)*:
  - Blockchain 4.0 represents the integration of advanced technologies such as artificial intelligence (AI), IoT, and big data into the blockchain ecosystem.
  - It seeks to enable decentralized applications to interact with real-world data and systems.
  - Projects like IOTA (for IoT integration) and Chainlink (for smart contract oracles) are examples of Blockchain 4.0 initiatives.
- *Blockchain 5.0 (The future)*:
  - Blockchain 5.0 is a concept still in its infancy, aiming to bring about the vision of Web 3.0, a decentralized and user-centric internet.
  - It seeks to integrate blockchain, decentralized finance (DeFi), non-fungible tokens (NFTs), and other technologies to create a more user-friendly and functional internet.
  - Concepts like decentralized autonomous organizations (DAOs), self-sovereign identity, and

decentralized storage are key components of this generation.

A. FUNDAMENTALS OF BLOCKCHAIN

A blockchain is a decentralized peer-to-peer network. It enables any node to issue a block or transaction after validating it in accordance with [2]. Transactions in the blockchain are validated independently by peers, timestamped, and then added to the ledger. As a result, once data is added, it cannot be easily changed. The blockchain nodes are linked to one another and share basic attributes such as:

- Any kind of data can be stored.
- Assures integrity of data.
- Append-only
- A specific protocol is used for communication.
- Consensus mechanisms namely proof-of-work and proof-of-stake are used to reduce the chance of malicious nodes to enter.

The blockchain network can be classified into three types: public blockchain, private blockchain, and consortium blockchain [14].

- *Public blockchain*: It is available to all networks, and anyone can join. There is no single authority in charge of the peers. Because of this openness, it is sometimes referred to as permissionless blockchain [15]. To get an incentive to behave properly, any node that wishes to join must adopt a consensus procedure such as proof-of-work or proof-of-stake and possess digital money. The most common examples of public blockchains are Bitcoin and Ethereum.
- *Private blockchain*: It is governed by a single authority, and joining the network requires permission. It is permissible for a single authority to establish the rules for network membership [16]. It can be used by educational institutions or private organizations–for example, multichain applications.
- *Consortium blockchain*: It combines private and public blockchains. It enables a pre-selected group of nodes to control the network and provide the consensus mechanism for others to join. It is not open to all, and each participant has equal rights. Without a doubt, it is less decentralized than public blockchain but more performant. Every participating node is pre-verified, and if it is suspected of being harmful by other nodes, it is removed from the network [15]. Consortium blockchains include Hperledger, Corda, and Quorum.

B. BLOCKCHAIN PRIVACY ATTRIBUTES

The applications that require sharing of sensitive information; data privacy, and user privacy need the utmost care. Blockchain technology has revolutionized the industry by ensuring the privacy of an individual. It facilitates various privacy parameters in comparison to the centralized systems as described below:

- *Identifiability*: A user who registers the network is provided a set of unique keys through which he is identified in case found malicious [18].
- *Anonymity/Pseudonimty*: A person's real identity is hidden from others on the network. A user uses his alias/pseudonym such that other peers cannot track the real identity of the user and are unable to fetch his sensitive details. On the other side, this property can also be misused by a malicious peer [18].
- *Transparency*: Blockchain serves as a transparent channel for all participants. Everyone on the network has access to the ledger details. This privacy feature can be abused by a malicious peer because sensitive information is available to all, posing a risk [19].
- *Immutable records*: Records that have been written and added to the blockchain cannot be changed or removed. This aids in the auditing and verification of records following a user denial [19].

The above-mentioned privacy parameters differentiate the blockchain from other centralized systems. The centralized systems do not provide a transparent medium for communication. Moreover, these systems are not good at guaranteeing user and data privacy as any adversary can easily track the user's real identity and can use it maliciously, in case, the trusted third party is compromised. Next, the blockchain supports the immutability of records, thus, no one can deny data generation and cannot alter the records. This helps in easily verifying and auditing the source of information if required.

Blockchain is primarily famous for financial applications such as Bitcoin, and cryptocurrency as it saves time and reduces the need for third-party dependency. Since 2016, after Ethereum came into the picture, blockchain gained popularity in multiple domains such as healthcare, IoT, supply chain, and many more. Later, another new addition called Cross-chain [6] is added to the blockchain development. Cross-chain provides interoperability of value and information among blockchains [7], [8]. The standalone blockchain is unable to provide the full feasibility or benefits of blockchains. Cross-chain solves the above-mentioned issues [9]. For example, Ripple which is a blockchain project helps in cross-chain and cross-border banking services [10]. Polkadot is used to promote the transfer of smart contracts through different blockchain [11]. Similarly, Blocknet is trying to create a decentralized environment to enhance the exchange of sensitive information [12]. Aion is another online platform based on cross-chain that deals with interoperability and scalability issues of blockchain [13].

C. MOTIVATION AND CONTRIBUTION

Blockchain-based frameworks are widely accepted and deployed to address the challenges of centralized system failure, privacy, reliability, and scalability that happen with IoT ecosystems. Furthermore, blockchain promotes transparency, openness, and immutable records, allowing users to quickly trace data and give a reliable mechanism to detect data leakage or manipulation if any exists. The existing IoT models have less computational and storage capacity and lack interoperability. For these reasons, blockchain-based

IoTs have gained popularity and facilitate data integrity, peer-to-peer trust, and many more [1].

In recent years, blockchain has achieved a milestone as it provides a distributed and decentralized secure, transparent, and open environment for communication. However, it is vulnerable to various privacy challenges. For instance, leakage of transaction privacy is a big issue in public blockchain. This is proved in the recursive calling attack on smart contracts in June 2016. During this attack by the criminals approximately sixty million dollars were stolen. Moreover, blockchain is vulnerable to privacy leakage even though the user is using their asymmetric key pairs, i.e., public and private keys. This occurs because IoT networks retain and upload sensitive user information. When such a vast volume of IoT data is uploaded to a blockchain, it becomes vulnerable to transaction linkage attacks and traffic correlation problems [79] to some extent or totally (depending on needs). Much existing research has proven that blockchain transactions can be linked to retrieve the user's information. For example, in smart healthcare systems [80], this type of attack can track patients' and hospitals' identities, as well as users' locations [81], [82].

Blockchain is adopted in a diversity of applications these days but privacy is still an open question. Thus, we study and analyze the existing privacy works in blockchain and highlight the gap in them. In addition to blockchain, we also discuss how PIR provides privacy to the user and its data. Further, we will figure out whether PIR and blockchain can be conjugated or not. If so, then we discuss how it could enhance privacy in blockchain-based applications. This survey is beneficial for researchers and academicians to get a thorough idea of the existing challenges of blockchain in different domains and the ways to handle these challenges. Here, we mention the major contribution of our survey:

- *Comprehensive review*: Our study explores the privacy challenges of blockchain-based systems in depth and highlights gaps in the literature. This will aid in assessing the privacy limitations that must be met while developing blockchain applications.
- *Prevention techniques*: We identify different privacy-preserving strategies used in blockchain-based applications. This provides an excellent chance for academicians to devise unsophisticated answers to blockchain privacy challenges.
- *Information retrieval*: We analyze the Privacy Information Retrieval (PIR) problems and solutions in conjunction with blockchain. It opens a new direction for the readers to construct the blockchain-based framework ensuring privacy and PIR.

D. MATERIALS AND METHODS

A methodical way to assess and measure the patterns, impact, and influence of scholarly publications usually books, essays, and other academic works is called bibliometric analysis. In the subject of scientometrics, which measures the production and impact of scientific research, it is an invaluable instrument. Through the identification of terms and subjects that are becoming more popular within an area, it might highlight new research trends. Funding organizations, policymakers, and researchers can all benefit from this knowledge. To study the versatility of blockchain and understand the privacy concerns of blockchain in different applications we explore various databases. We mainly searched the papers from Science Direct, IEEE Xplore, Elsevier, Web of Science, Springer, and ACM Digital Library. The keywords we use for our research are blockchain in different domains such as healthcare, IoT, SCM, and e-commerce. Next, we search related to privacy threats, and privacy concerns in blockchain. Further, we search for existing privacy-preserving techniques for blockchain and the ways to conjugate PIR and blockchain systems. Our research will open a gateway for academicians and researchers to think about merging the blockchain and PIR to improve the privacy of decentralized systems.

E. PAPER ORGANIZATION

The remainder of this work is structured as follows. The section II discusses privacy concerns in the blockchain. We present the literature work connected to the combination of blockchain privacy and its accompanying applications in Section III, alerting the discovered gaps and scope of improvement. Section IV examines existing privacy-preserving approaches for blockchain-based applications. Section V provides the survey related to the PIR techniques and identifies the benefits of collaborating with the blockchain. Further, section VII discusses some open research gaps related to blockchain privacy identified in the literature, and section VI compares the existing survey related to privacy in blockchain. Finally, Section VIII concludes the paper. We provide Figure 2 for the clarity of the information flow in our presented survey.

II. PRIVACY CONCERNS IN BLOCKCHAIN

Privacy is defined as the right of an individual to draw a thin line for others to protect their sensitive information not to be disclosed [17]. Privacy is the key aspect of blockchain as it provides the cryptography key for secure communication between peers on the network. This key is formed by a combination of random strings of numbers which is nearly impossible for anyone to guess. However, the openness and transparency of blockchain are concerning matters when question comes to individual privacy. The data shared by users on the blockchain network is easily accessible to all peers and can be exploited maliciously by a dishonest peer. Thus, it causes certain privacy attacks in blockchain-based applications. These threats are discussed in the following subsection.

A. PRIVACY THREATS IN BLOCKCHAIN

The blockchain provides a decentralized and distributed environment to store, share, and access data without any need for a trusted third party. However, the blockchain stores the data in an open environment which could be

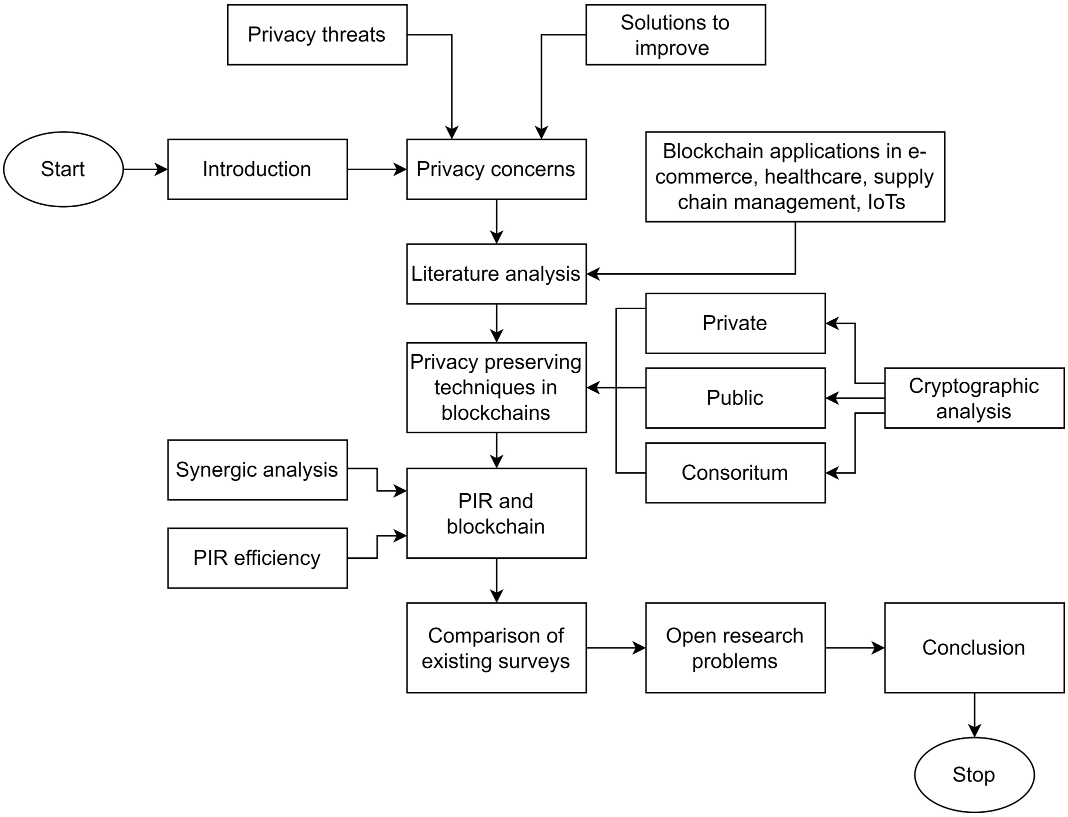

FIGURE 2. Flowchart to represent information flow in our present survey.

disadvantageous for applications that involve the storage of personal information such as banking, and e-health. Ensuring privacy in such applications is a great urge. The blockchain system must ensure two main properties to guarantee privacy. To begin with, various transactions by a single user cannot be linked in any way. Second, the data kept on the blockchain should not be open to the public and freely accessible to all [18], [19]. The failure of the above properties leads to the following privacy attacks [21], [22], [23], [24], [25], [26], [27], [28], [29]:

- *Transaction privacy leakage*: This type of attack is caused by linking the transaction details/behavior to a particular user and gathering his personal information. It could be done in the following ways:
  - Blockchain transactions are often pseudonymous, which means that they are linked to cryptographic addresses rather than real-world identities. However, if someone manages to link a real identity to an address, they can trace all transactions associated with it, compromising privacy.
  - Reusing addresses in transactions can lead to privacy risks. When an address is reused, it becomes easier to trace the flow of funds, potentially exposing transactional history.
  - A malicious node can track the same public address used for multiple transactions by the user.
  - When a user makes a Bitcoin payment, the service provider can link the user's true identity, which can then be utilized for criminal purposes.
  - Continuously observing the transaction graph pattern makes it feasible for an intruder to relate the different addresses to the same user to steal his real identity.
- *Identity privacy leakage*: The blockchain allows the use of pseudonyms to hide real identities to facilitate user anonymity. However, it could be disadvantageous because some malicious peers can join the network by hiding their actual identities for fraudulent attacks.
- *Malicious smart contracts*: Smart contracts run automatically whenever a node wants to join the network. Smart contracts can be vulnerable as they may contain any malicious code stored on the blockchain network.

We use Table 1 to summarize the blockchain elements, which can be the target of the attackers for the above-mentioned attacks.

B. SOLUTIONS TO IMPROVE THE PRIVACY OF DATA

To overcome the aforementioned privacy issues we suggest certain solutions to enhance privacy in blockchain-based applications [20]:

- To protect the user's identity before uploading it to the blockchain network, hard cryptographic techniques

TABLE 1. Attack elements in blockchain transactions and its mitigation procedure.

Element	Attack	Risk	Mitigation
Public addresses	Links public addresses to real-world identities	If an individual's identity can be associated with their public address, all transactions associated with that address become linked to them	Use of privacy-focused cryptocurrencies or techniques like coin mixing or ring signatures to obfuscate the linkage between addresses and real-world identities
Transaction graph	Analyzes the transaction graph to infer relationships between different addresses	Inferred connections from the analysis may reveal the flow of funds and potentially link addresses together	Confidential Transactions or zk-SNARKs to obfuscate transaction details and amounts
Metadata	Extracts metadata from transactions or associated communications	Additional data like timestamps, IP addresses, or transaction types may reveal sensitive information	Additional privacy layers or cryptographic methods for metadata protection
Smart contracts	Exploiting code-based vulnerabilities in smart contracts to reveal information	Errors in smart contracts or malicious smart contract codes leak information about transactions	Security audits on smart contracts with privacy assurance
Transaction mixing or CoinJoin services	Compromising the integrity of mixing services	If the mixing service is not trustable, it might keep logs or collude with attackers, compromising user privacy	Use reputable and privacy-focused mixing services, or employ alternative privacy-enhancing techniques
Network-level analysis	Monitors network traffic to trace transactions	Analyzing data packets on the network layer can potentially reveal transaction-related information	Employ techniques like VPNs or use privacy-focused blockchain networks with additional network-level privacy measures

such as ring signatures, homomorphic encryption, and zero-knowledge proof can be used to protect the real identity of the user. These techniques make it impossible for malicious peers to link different wallets/IP addresses to the same user. As users utilize pseudonyms to join, each user's identity should be confirmed and authenticated ahead of time. Certain procedures, such as know your customer (KYC) and anti-money laundering (AML), can be implemented to accomplish this.

- The mechanism like public key encryption-based keyword search (PEKS) can be used before uploading the real data on the blockchain network. It helps in hiding the actual data of the user by encrypting it and creates secure searchable indexes on the blockchain to be searched using keywords.
- The transactions executed by the peers on the blockchain are visible to all keeping it a fair and transparent medium for communication. However, it gives a bright opportunity to the malicious nodes to observe the transaction behavior (transaction graph) to link it to the particular user and steal his details. It can be prevented by using homomorphic encryption techniques like private information retrieval (PIR). It allows the anonymous user to query the blockchain without disclosing his real identity and the data he is looking for to anyone on the network.

III. LITERATURE ON BLOCKCHAIN PRIVACY

In 2008, the blockchain was initially used for deploying the cryptocurrency named Bitcoin [30]. With the advancement in the digital world over the years blockchain gained popularity in different domains such as EHealth, IoT, education, and many more by the end of 2015. During this period the biggest achievement of blockchain was the Ethereum platform for making distributed applications (dAPPs). Another milestone in the same year is the launch of hyperledger fabric which is a LINUX foundation [31]. Both these blockchain platforms are very useful and provide different characteristics for constructing decentralized architectures. Further, it helps increase the reliability and performance of business transactions all around the globe.

The blockchain keeps on rising with the technological revolution and has established roots in a diversity of application areas. For example, IoT, smart city, education, supply chain, healthcare, and many more [32]. This section studies the existing blockchain efforts in several sectors. We do this by analyzing the privacy criteria provided by various existing solutions and highlighting the shortcomings in them. Furthermore, we discuss the privacy-preserving approaches utilized to protect the user's identity and data. In the following subsections, we will look at how blockchain is being used in various applications such as e-commerce, supply chain management, IoT, and healthcare.

A. BLOCKCHAIN-BASED E-COMMERCE SYSTEMS

The study in [33] compares and contrasts the permissioned blockchain framework (PBF) with the blockchains utilized in Bitcoin e-commerce. According to the authors, after assessing the benefits and drawbacks of both approaches, the permissioned blockchain framework allows instant transactions and variable block sizes in e-commerce. In terms

TABLE 2. Blockchain privacy in E-commerce.

Ref.	Year	Contribution	Privacy Parameter	Blockchain Type	Research Gap
[33]	2016	Blockchain-based peer inner protocol for trusted transaction	Identifiability and pseudonymity	Private and permissioned blockchain	Not suitable for large data storage
[34]	2017	E-commerce blockchain consensus mechanism	Identifiability, credibility and unobservability	Consortium blockchain	Does not guarantee consistent data
[35]	2018	Bidding system	Anonymity and unobservability	Consortium blockchain	High implementation cost because of complex architecture
[36]	2018	Normachain, a blockchain-based IoT system for e-commerce	Anonymity and unobservability	Consortium blockchain	Transaction privacy at risk
[37]	2019	Blockchain-based architecture for trading	Anonymity and pseudonymity	Public blockchain	Interoperability and Scalability

of throughput and latency, the suggested model is more effective. Designated in [34] is another permissioned trusted trading network (PTTN). Any dishonest node is forbidden from entering the network. When a dishonest peer attempts to join a network, this ensures the transaction's high credibility by giving high credibility to the transactions.

A blockchain network is made for the e-auction application of online commerce [35]. It explicitly addresses the problems with centralized systems' lack of trust. It lowers the price given to the trustworthy middleman who stands between the customer and the supplier. The author of this work developed a smart contract that specifies the guidelines for placing a bid and that is not made public before the deadline. The systems aid in keeping the bid private, non-repudiable, and tamper-proof. Furthermore, the work in [36] describes the construction of a three-layered NormaChain sharding blockchain network. The blockchain network is more effective and scalable because of this system. Additionally, to combat fraudulent transactions, the authors adopt a PEKS mechanism to block unauthorized access to the network. A blockchain-based online buying strategy that protects anonymity is proposed in the study [37]. To shield the user from any identity-based threats, such as those based on address or phone number, the framework is built using a private smart contract. When a transaction is being completed, the system serves as a conduit between the buyer and the seller while keeping the user's personal information hidden. To build shield tokens that users may use to prove their ownership, the zk-snarks concept is used. The research gaps related to blockchain in e-commerce are mentioned in Table 2.

B. BLOCKCHAIN-BASED HEALTHCARE SYSTEMS

A healthcare data gateway (HDG) is suggested in [38]. With the help of this blockchain-based architecture, patients may safely grant ownership, control, and permission to share their data without jeopardizing its privacy features. Two protocols are used: secure multi-party computing (SMPC) and indicator-centric schema (ICS). In addition to protecting the patient's private information from unauthorized outside access, it assists patients in properly arranging their health records with a minimum of complexity. The authors created a mobile application of their concept, which makes it simple for a person to download on their phone and access from any location [39]. Further, a fresh permission-based blockchain structure is suggested in [40]. It safeguards the user's identity by granting him the ability to control and share his data in the cloud, as well as sync it with healthcare providers. To validate network nodes and maintain end-user privacy, a mobile application based on the hyperledger fabric blockchain is also deployed.

The work in [41] has created a concept blockchain-based healthcare ecosystem. It solves privacy problems in the existing cryptography architecture for cloud-based healthcare systems. The suggested work was significant and provided numerous advantages. To begin with, it eliminates the requirement for a third party to sign the agreement, protecting the system from a single point of failure. Second, everyone has access to and control over their personal information. The medical records are then kept in a chain of blocks that are distributed over the network in a consistent, accurate, comprehensive, and timely manner. Finally, any changes to the data are visible to all network nodes. A blockchain-based BCHealth platform for IoT healthcare is also proposed [42]. It provides restricted access to network-stored user-sensitive data. The concept is realized by the use of two distinct chains, one for maintaining access controls and the other for data transfers. As a result, patients can connect with healthcare practitioners in secret. Another safe healthcare system for remote patient monitoring, intended to detect chronic conditions such as diabetes, is created [43]. The system employs blockchain and proxy re-encryption techniques to ensure the confidentiality and privacy of healthcare data. cite49 also created a blockchain-based healthcare system for IoT devices. It enables users to conceal their identities while transmitting encrypted health-related data from their devices. Furthermore, the proposed protocol is built on zk-SNARK, the DHKE algorithm, and digital signatures to enable anonymous authentication and secure data-sharing communication channels between users and healthcare service providers. A blockchain-based distributed application (DA) framework that protects privacy is put forth [44].

TABLE 3. Blockchain privacy in healthcare.

Ref.	Year	Contribution	Privacy Parameter	Blockchain Type	Research Gap
[38]	2016	Blockchain-based application development	Identifiability and pseudonymity	Private blockchain	High computational cost and less scalable
[39]	2017	Blockchain-based mobile application for sharing healthcare data	Identifiability, anonymity and credibility	Private blockchain	Not suitable for large database and less accessible
[40]	2018	Blockchain-based security provisions for healthcare clouds	Anonymity and unobservability	Consortium blockchain	Voluminous data can't be stored
[41]	2021	BCHealth for secure interaction with healthcare service providers	Transparency and identifiability	Public blockchain	Cluster management and load balancing
[42]	2022	Blockchain-based model for remote patient monitoring	Privacy and secure data access	Public blockchain	Computational cost is high
[43]	2022	Blockchain architecture for IoT healthcare using zk-SNARK	Anonymity and data security	Public blockchain	Not beneficial for smartphone users and High computation time
[44]	2023	IoT-based blockchain system for medical certificates	Authorized access	Private blockchain	Applicable for medical certificates only

TABLE 4. Blockchain privacy in supply chain management.

Ref.	Year	Contribution	Privacy Parameter	Blockchain Type	Research Gap
[45]	2016	Agri-food supply chain traceability with RFID and blockchain	Traceability and authenticity	Public blockchain	High implementation cost, storage and synchronization
[46]	2017	aircraft spare parts management	Transparency and availability	Public blockchain	Authentication of spare parts, RFID tags, and smart contracts can be used for better results
[47]	2018	AgriBlockIoT, a agri-food traceability solution	Transparency and traceability	Public blockchain	Single language used for smart contracts and computation cost
[48]	2022	TPPSUPPLY framework	Anonymity, transparency and traceability	Private blockchain	Limited space and applicable for lightweight nodes
[49]	2023	Blockchain-based framework for SCM using PCGSO	Privacy, transparency and authorised data access	Consortium blockchain	Limited storage space

Healthcare certificates can be created and maintained with the help of this framework. To develop and issue medical certifications, it connects the blockchain network to system objects including medical facilities, verifiers, doctors, and conventional authorities. Fraud and unauthorized access to medical records are also prevented. Table 3 mentions the gap in the blockchain-based healthcare systems.

C. BLOCKCHAIN-BASED SUPPLY CHAIN MANAGEMENT SYSTEMS

The study in [45] proposed and designed a traceable system for agri-food supply. It improves food safety and quality control while lowering logistics losses. When it comes to tracking and monitoring the quality and safety of food from farm to fork, the system excels. AgriBlockIoT, another agri-food supply architecture, is being implemented in [46]. From manufacturing to consumption, it delivers food transparency and auditable asset traceability along the whole supply chain. Ethereum and hyperledger saw-tooth blockchains are utilized for this purpose. The outcomes of both systems are compared in terms of latency, CPU, and network utilization. The authors discovered that the hyperledger system outperforms Ethereum. A traceable and privacy-preserving blockchain system architecture for supply chain (TPPSUPPLY) is another project being worked on in [47]. Blockchain-based smart contracts that are both on-chain and off-chain enable privacy, traceability, and transparency while promoting anonymity. The framework enables anonymous users to submit requests for any type of items, from food supply to pharmaceutical supply, and securely track them without the need for a third-party middleman.

The study in [48] explores the gaps in the current global supply chain for airplane replacement components and discusses the significance of SCM in the aviation industry. The protocol handles the inventory of aircraft spare parts and analyzes overall performance and utilization. The architecture promotes transparency in the supply of various items, reducing the possibility of black marketing. This style of design helps SCM managers analyze the availability of

TABLE 5. Blockchain privacy in IoT.

Ref.	Year	Contribution	Privacy Parameter	Blockchain Type	Research Gap
[50]	2019	Optimized blockchain for IoT	Identifiability and anonymity	Public blockchain	Overhead in overlay can be improved
[51]	2017	Blockchain-based smart home framework	identifiability, anonymity and unobservability	Consortium blockchain	High implementation and computational cost
[52]	2017	Blockchain-based IoT ecosystem using Attribute-based encryption (ABE) technique	Anonymity and transparency	Private blockchain	Scalability and computational cost
[53]	2018	A Blockchain-based IoT system based on Threshold secure multi-party computing (TSMPC) protocol	Anonymity and unobservability	Public blockchain	Scalability
[54]	2019	MEC-based sharing economy system, which leverages the Blockchain on-chain and off-chain framework to store immutable ledgers	Anonymity and identifiability	Private blockchain	System can be further tested for sharing economies at a large scale
[55]	2018	Oauth implementation via smart contract	Anonymity, identifiability and unobservability	Public blockchain	Consumption(gas) cost and scalability
[56]	2018	Blockchain-based IoT-Cloud Authorization and Delegation	Anonymity and pseudonymity	Public blockchain	Usage of Smart contracts for SmartMEEcosystem
[57]	2020	Blockchain-based framework for remote data integrity check	Privacy, traceability and data integrity	Public blockchain	Limited storage space and less scalability
[58]	2022	BPRPDS architecture	Anonymity and unforgeability	Private blockchain	Only licensed user can join the network, high implementation cost

parts and their sources of supply, demand, and supply, while also safeguarding them from unwanted access. Further, the work in [49] suggests a blockchain solution for supply chain management of logistical data that protects user privacy. It employs the perceptive craving game search optimization (PCGSO) technique to build the best key for data sanitization, ensuring logistics data privacy. Table 4 describes the gaps in blockchain-based SCM applications.

D. BLOCKCHAIN-BASED IOT SYSTEMS

The study in [50] provided a lightweight blockchain-based architecture for IoT devices to enhance security and privacy in IoT applications. This architecture works well with minimum overhead and latency. The model is used to demonstrate the performance of a smart house. The architecture is divided into three layers to optimize resource utilization and scalability. To improve security and privacy in IoT networks, [51] suggests an additional modified lightweight scalable (LSB) blockchain. The design tackles IoT applications' drawbacks, including limited resource consumption, centralization, and a lack of privacy. It is utilized to satisfy all fundamental needs for IoT-based systems. The lightweight consensus algorithm, distributed trust, distributed throughput management, and transaction traffic separation from data flow are all used. The newly proposed design outperforms the old framework in terms of latency, overhead, and scalability, the authors found after running simulations and comparing the findings to the old framework. Furthermore, an attribute-based encryption (ABE) technique is utilized in [52] to increase the privacy of IoT-based applications. This method ensures both confidentiality and access control. It has proved to be a successful data communication technology in decentralized networks. Because only trustworthy miners can decode the data, this technique ensures end-to-end anonymity.

A simple framework called 'Beekeeper' is used in [53]. To increase the security and privacy of IoT-based applications, it makes use of threshold servers and homomorphic computation. The server's data is processed using the Ethereum blockchain and the threshold secure multi-party protocol (TSMPC). It enables any node that satisfies the requirements to take the lead in the network. Furthermore, a homomorphic technique allows the user to conceal his data from unauthorized access. It prevents any rogue node from joining the network since the TSMPC protocol verifies the number of server answers active at the time. Thus, the proposed model guarantees the decentralization, confidentiality, anonymity, homomorphic threshold, and reliability of the transaction. The work in [54] also suggests an MEC infrastructure for IoT systems based on blockchain technology. It addresses the major issue of sharing economic services in smart cities and provides a secure environment. It manages each stakeholder's identification verification anonymously. As a result, it supports decentralization, on-chain and off-chain data storage, identity management, and smart contract services to facilitate secure transactions. Furthermore, the suggested IoT solution [55] employs Ethereum smart contracts to ensure the following features, namely accountability, integrity, and traceability with tamper-proofing of records.

The study in [56] proposed an improved model based on blockchain. It employs Ethereum smart contracts to address the shortcomings of conventional cloud-based data storage in IoT applications. It ensures network access control and audit operations. The concept has been implemented for smart city IoT applications and is well-suited for other domains. The study emphasizes a heterogeneous approach to smart city infrastructure to handle the issue of access control, permission, and delegation of IoT-cloud resources. A blockchain-based privacy-preserving technique for remote data integrity checks in IoT devices is also introduced in [57]. Since the paradigm does not rely on a third party for data integrity checks, it is suitable for database management application systems. The suggested approach gives users complete authority to track unauthorized auditing transactions. Moreover, a privacy-preserving and rewarding private data-sharing method based on blockchain technology is presented and implemented in [58] for IoT-based applications. It employs a ring signature to protect the user's true identity from other network users. The technology permits the development of anonymous tokens for the exchange of data among users. Table 5 mentions the research gap in blockchain-based IoT applications.

IV. PRIVACY PRESERVING TECHNIQUES IN BLOCKCHAIN

In this section, we go over the approaches and privacy protection strategies utilized to improve privacy in blockchain-based apps. We study various existing techniques and categorize them according to the protection of data privacy, transaction, or identity privacy, and key-based or data storage protection mechanisms [96]. The taxonomical diagram of these strategies is shown in Figure 3.

A. PRIVATE BLOCKCHAIN

The work in [59] presents a simplistic blockchain-based framework called blockchain-assisted privacy-preserving authentication system (BPAS) for vehicular ad-hoc networks (VANETs) to solve the drawbacks of earlier centralized VANETs. It aids with the auto-authentication of automobiles while also providing privacy. A hyperledger fabric is utilized to design the architecture, and the results are assessed to ensure the system's performance. It permits the car owner to conceal his or her true identity and can be traced if necessary. To accomplish this, many algorithms are utilized, such as fuzzy extractor to improve security when authenticating the car, ABE to secure user privacy, and smart contracts to ensure data access control. Furthermore, application binary interfaces (ABIs) are employed to make it easier to insert, upload, and revoke public keys associated with automobiles. Another blockchain-based conditional privacy-preserving authentication (BCPPA) mechanism is described in [63]. It shows the shortcomings of current blockchain-based, PKI-based, or ID-based protocol-based solutions. It mentions that these protocols run into privacy problems because of frequent interactions in VANETs, in-trackability, and key/certificate preloading and revocation. The suggested approach combines the PKI protocol with blockchain to address the aforementioned problems. The technology also resolves the escrow issue and provides private information that is frequently updated, suggesting that it works well with realistic on-board units (OBUs). A blockchain-based recommendation system has also been developed by the authors in [67] to protect user privacy when storing and disseminating massive amounts of data online. Three major processes are used to construct the system. The first step is to use local sensitive hashing (LSH) to cluster the data. Following that, a local differential to privacy technique is used to safeguard the user's identity and data, which is done at the user level. Finally, interplanetary file system (IPFS) storage is used to store vast amounts of data. It assigns each user a unique hash key to access the stored data.

B. PUBLIC BLOCKCHAIN

A significant obstacle to the use of IoT for crowd sensing is task matching. Reference [62] suggests a blockchain-based privacy-preserving task matching (BPTM) system as a result. It helps to resolve the privacy and dependability problems with the earlier options. Identity anonymity is another key issue with these systems. As a result, there is cause for concern since if personal information is released, it could be used maliciously. Instead, the authors propose a task-matching searchable encryption system. The encrypted index is also stored on a blockchain-based platform to offer matching services. A combination of smart contracts and searchable encryption is used to protect user privacy and boost system performance. The work in [64] also uses a basic voting system based on a blockchain. It provides a technique to stop cheating through the use of detectability and correctability procedures and ensures end-to-end privacy in the system. The authors identified loopholes in existing systems that compromise secrecy and privacy and developed a novel peer-voting protocol that is receipt-free, easily verifiable, and privacy-preserving. It enables network nodes to vote without interference from outside parties in identifying voters or tallying ballots. The work in [65] covers the numerous privacy issues in public key infrastructure (PKI)-based IoT applications. It also examines existing blockchain-based PKI schemes and concludes that they are not suitable for thin clients. Because of limited storage, thin clients cannot download the complete blockchain data. As a result, a naive privacy-preserving thin-client authentication scheme (PTAS) is proposed and built, which is based on blockchain and PKI in conjunction with PIR. It allows thin clients to function like complete nodes while keeping the identity of the user authenticating with the thin client concealed. Furthermore, the authors proposed the $(m-1)$

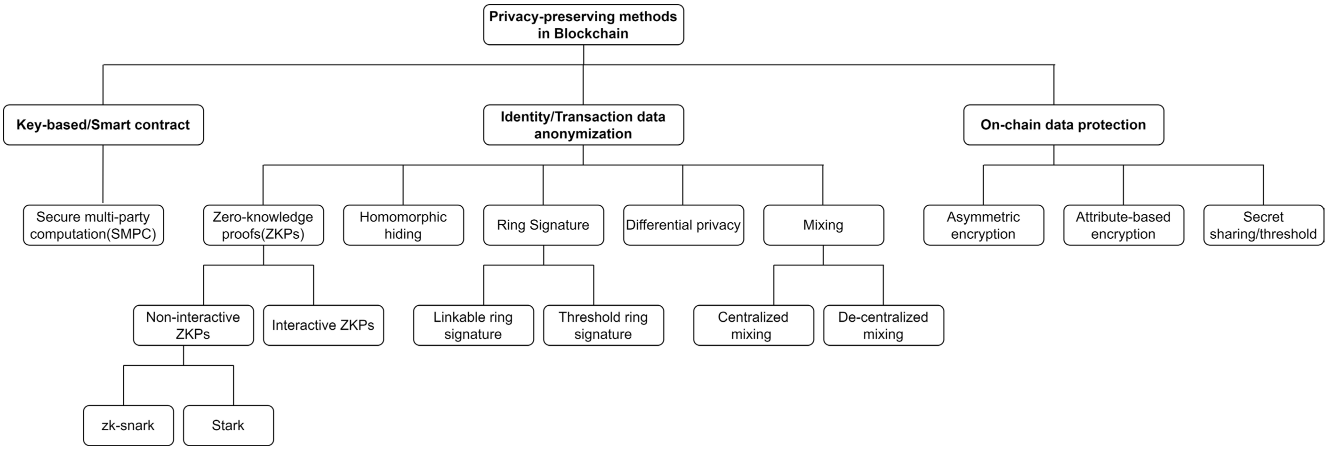

FIGURE 3. Taxonomical view of privacy-preserving methods.

private PTAS concept, which indicates that even if $(m-1)$ full node users colluded, they did not receive any benefit. Under [100], a naive federated learning strategy is proposed to address privacy leaks and trust concerns. A Privacy-Preserving Trust Management Architecture (PPTMA) based on blockchain was implemented by the authors. PPTMA uses federated learning to develop a trust model tailored to the specifics of each collaborative task. Device privacy is protected throughout the trust assessment process by utilizing a method similar to Differential Privacy (DP). Further, to improve the accuracy of trust computing, a game theory-based incentive mechanism is also suggested to incentivize the IOT device to proactively and truthfully transmit the trust data to the blockchain. At last, a parallel consensus protocol accelerates the consensus process by realizing an assembly line.

C. CONSORTIUM BLOCKCHAIN

In the study [60], existing EHR issues are recognized, and blockchain options for patient data protection are investigated. A new framework is created by combining two blockchains: private and consortium. Personal health information (PHI) is encrypted and stored on a private chain, while indexes of this data are saved on a consortium blockchain. The architecture's performance is examined in terms of privacy and security, yielding superior results than the techniques. Furthermore, in [61] a survey is carried out in one of the IoT-based applications known as crowdsensing. It notes that the current system has a problem with privacy invasion and hence proposes a new approach. The framework is designed to handle the problem of related transactions, and by linking to the user's financial transaction history, the system makes sure that the user's genuine identity is kept a secret. The crowdsensing system also enhances the location privacy of the employees. Another simplistic technique based on the idea of a modified blockchain is proposed in the paper in [66]. Instead of PoW consensus, this uses a combination of lightweight digital signatures. It protects documents from tampering. The ring signature is then used, which enables an anonymous signer to sign a message. Because of this, a malicious node can't ascertain and identify the message's signer, save for the actual signer. Furthermore, it encrypts the data twice utilizing public and lightweight encryption methods to enhance user privacy and anonymity in EHealth. The authors in [68] have created a Privchain concept based on blockchain and AI for supply chain components. Moreover, it permits dealing with data storage offline, minimizing processing overhead. A naive privacy-preserving framework is deployed for secure data exchange in intelligent transportation systems (ITS) in [69]. It introduces the concept of bloom filters to select the low-frequency data from multiple keywords given as input to search the database. It reduces the computational cost of the entire system. Another cutting-edge blockchain technology that provides integrity to medical records and helps to ensure authentication is used to securely store health data in the cloud. Here, an enhanced blowfish model that ensures authentication features is used to install blockchain with the best encryption possible. Additionally, a novel method known as Elephant Herding Optimization with Opposition-based Learning (EHO-OBL) generates keys in the best possible way. Thus, the created approach preserves the integrity of the data, and finally, the superiority of the presented approach is demonstrated concerning multiple metrics [99]. Table 6 mentions the various techniques to enhance privacy in blockchain networks.

Cryptograhic analysis: From Figure 3, we observe that several cryptographic techniques are used in blockchain components such as smart contracts, transaction identities, and on-chain data protection. We all know that blockchain transactions are too complex and create computational overhead by default. Therefore, it is necessary to analyze how the mentioned cryptographic solutions are feasible in blockchain transactions with complexities in the threshold.

- Secure MPC in blockchains allows confidential computations without revealing individual data, ensuring privacy and shared private keys for resilience against single points of failure. It guarantees Byzantine fault tolerance, even in the presence of malicious actors. However, challenges include computational and communication overhead, potentially slowing transactions. The complexity of cryptographic protocols makes implementation and auditing challenging, and larger transaction sizes may impact storage and bandwidth requirements.

- Zero-knowledge proofs (ZKPs) enhance privacy in blockchain transactions by allowing one party to prove knowledge of certain information without revealing the information itself. ZKPs ensure confidentiality while validating transactions, offering robust privacy protection. Implementing ZKPs in blockchain transactions can introduce computational overhead, potentially impacting transaction processing times. Transaction verification using ZKPs can be resource-intensive, affecting scalability in large-scale blockchain networks.
- Homomorphic encryption enhances blockchain privacy by allowing computations on encrypted data without decryption. It enables confidential transactions, securing sensitive information from exposure. Key management and the complexity of homomorphic encryption methods may pose implementation challenges. The resource-intensive nature of homomorphic encryption could impact scalability in large-scale blockchain networks.
- Ring signatures enhance blockchain privacy by allowing a user to sign a transaction on behalf of a group, obfuscating the actual signer. This ensures transaction unlinkability and enhances confidentiality on the blockchain. Ring signatures may introduce larger transaction sizes, impacting storage and bandwidth requirements. While offering privacy, they do not provide sender or receiver anonymity within the ring, and the level of privacy achieved depends on the size and composition of the ring.
- Differential privacy in blockchain safeguards individual user data, bolstering privacy. It allows statistical analysis without revealing specific contributions, balancing transparency and confidentiality. Implementing differential privacy introduces complexity and potential trade-offs in accuracy. Achieving optimal privacy levels may require careful parameter tuning, and improper configuration could impact the quality of analytics and overall system performance.
- Mixing methods enhance privacy in blockchain by obfuscating transaction traces. Mixing may face scalability challenges, and the effectiveness relies on the adoption rate. It doesn't offer complete anonymity, and the mixing process may introduce delays in transaction confirmation.
- Even though asymmetric encryption methods are superior in terms of security parameters, such methods may introduce computational overhead, impacting transaction processing times. Besides, key management complexities and potential vulnerabilities in key exchange processes can pose security challenges.
- In the case of attribute-based encryption, complexity in managing attributes and keys may pose challenges. Additionally, the system's scalability and the potential for misuse or misconfiguration can impact its effectiveness in certain scenarios.
- Secret sharing threshold in blockchain enhances security by distributing sensitive information among participants, preventing single points of failure. However, implementation complexity and the need for secure key management may present challenges. The overhead in communication and computation could affect transaction efficiency in certain scenarios.

Cryptographic methods enhance blockchain privacy enabling confidential transactions. However, challenges arise from computational overhead, communication complexity, and implementation intricacies. Therefore, a balance between robust privacy measures and transaction efficiency remains crucial in optimizing the synergy between cryptographic techniques and blockchain for enhanced privacy preservation.

V. PRIVACY INFORMATION RETRIEVAL AND BLOCKCHAIN

PIR is a technique that guarantees privacy to the user and the data accessed by him. It allows a user to search a bit of information stored in multiple database servers without revealing his identity and not disclosing the data he is looking for. PIR is applicable in different domains like finance, healthcare, and trade to fetch data without leaking any information during retrieval [70]. For instance, a person who wishes to invest in the stock market has to download the relevant database to gather the facts without disclosing his piece of information to anyone so that potential investment can be made. The PIR is broadly classified as information-theoretic PIR (ITPIR) and computational PIR (CPIR). ITPIR consists of multiple database servers. Each server contains a replica of information that can be accessed by a user. The user gets a separate response to his query from each server without losing his credentials and identifies the correct response on his own. On the other side, CPIR is a single server database model based on cryptographic algorithms. It guarantees user and data privacy but puts additional computation overhead in contrast to ITPIR where the database server may collude [71]. Therefore, in this section, we emphasize light on how PIR is beneficial in blockchain scenarios by discussing some of the existing works.

A framework is designed by the authors in [72] to provide a double layer of protection for large content-based information systems. The first layer uses robust hash values to put the query and prevent the original data to disclosed. The second layer enables the client to further lower some bits to raise ambiguity in the server, making it difficult for a malicious

TABLE 6. Privacy-preserving techniques for blockchain.

Ref.	Year	Contribution	Privacy Parameter	Application Area	Technique
[59]	2019	BPAS framework	Identifiability and Traceability	VANETs	Attribute-based encryption
[60]	2018	BSPP architecture	Identifiability, anonymity, and unobservability	Healthcare	Public key infrastructure
[61]	2018	Blockchain-based privacy preserving crowd sensing system	Anonymity, unlinkability, and transparency	Crowd sensing	Ring signature
[62]	2019	BPTM system model	User and data privacy	Crowd sensing	Public key cryptography
[63]	2020	BCPPA framework	Anonymity and identifiability	VANETs	Public key infrastructure
[64]	2018	Blockchain-base privacy-preserving framework for voting	Anonymity, identifiability, and unobservability	E-voting	zk-snarks and homomorphic encryption
[65]	2019	PTAS architecture	User and data privacy	Thin-clients	Public key infrastructure
[66]	2019	Light-weight and cluster-based blockchain	Anonymity of user data	Healthcare	Mixing services
[67]	2021	Blockchain-based recommendation system	Data access, and privacy	Big data	Differential privacy
[68]	2022	Blockchain and artificial intelligence-based model:Privchain	Location and data privacy	Supply chain	zk-snarks and homomorphic encryption
[69]	2023	Blockchain-based Intelligent transportation systems using bloom filters	Data privacy	Transportation	Bloom filters and PEKS technique
[99]	2024	Blockchain-based Elephant Herding Optimization with Opposition-based Learning model	Data integrity and authentication	Medical record storage on cloud	EHO-OBL
[100]	2024	Blockchain-based federated learning model (PPTMA)	Privacy leakage and trust	Indutrial IoT	Differential privacy and federated learning

server to comprehend what kind of information the client is seeking. Further, to maintain the privacy of lightweight Bitcoin transactions large bandwidth is required using a simple payment verification (SPV) protocol. Moreover, the existing studies prove that the usage of bloom filters does not guarantee transaction privacy. Thus, the work in [73] proposes a naive solution that conjugates SPV and PIR techniques. It not only cuts bandwidth, but it also minimizes latency and protects the user's privacy. Furthermore, according to the work in [74], traffic congestion is one of the key concerns with smart parking systems for vehicles in congested locations. Therefore, a new system is deployed by collaborating consortium blockchain and PIR. The drivers can easily search for the nearest available parking lot without sharing their location with anyone. The system behaves efficiently in terms of hiding the location details of the drivers. Another blockchain-based smart parking system with privacy protection and reputation management is suggested in study [75]. During information retrieval, a PIR approach is also used to offer the driver location privacy. The authors employ a commitment strategy to ensure fair parking charges and to prevent parking lot owners from inappropriately manipulating their rates. Further, in [76] an architecture based on consortium blockchain and PIR using ring signature is deployed. This scheme improves the multiple transaction modes and ensures privacy for the smart parking system. Based on these research solutions we can say that PIR and blockchain together can do wonders to enhance privacy in different domains as both techniques complement each other.

A. SYNERGY BETWEEN PIR AND BLOCKCHAIN

The efficiency and application of PIR in blockchain within distribution environments hold significant promise for enhancing data privacy and security. PIR, a cryptographic technique, enables a user to retrieve specific information from a database without disclosing the queried data to the database owner. In the context of blockchain in distribution environments, PIR can be instrumental in preserving confidentiality while facilitating secure and decentralized data access. This technology finds application in scenarios where sensitive information needs to be accessed or verified within a distributed network without compromising the integrity of the underlying blockchain [77], [78]. By integrating PIR into blockchain systems, organizations can achieve a balance between data privacy and transparency, fostering a more secure and efficient distributed environment for diverse applications such as supply chain management, logistics, and decentralized finance (DeFi). The implementation of PIR in blockchain contributes to a robust framework that safeguards sensitive information, thereby advancing the overall security and trustworthiness of distributed systems in various industries. Thus, PIR and blockchain complement each other and provide the following benefits for distributed and decentralized networks.

- *Enhanced Privacy*: Distributed applications may benefit from increased privacy when PIR and a blockchain are combined. Enhancing data privacy, users can retrieve data from a distributed blockchain-based database while hiding their unique search terms.
- *Immutable records*: A blockchain can be used to store the PIR-retrieved data, guaranteeing its integrity and immutability. Applications that need a history of data access that is auditable and unchangeable will find this to be extremely helpful.
- *Secure data sharing*: When PIR and blockchain are combined, safe data exchange can be made possible in ations where several parties need to view and update data while protecting confidential information.

B. TECHNIQUES FOR PIR EFFICIENCY

As we know blockchain is transparent and PIR ensures the privacy of retrieved information. Thus, PIR in blockchain for distributed environments requires a synergical balance between preserving user privacy and ensuring the efficiency and scalability of information retrieval operations. We list the available techniques, which are employable in PIR to enhance its efficiency in the context of blockchain in distributed environments.

- *Optimized PIR protocols*: Researchers and developers can design and implement PIR protocols that are optimized for the specific characteristics of blockchain networks. These protocols should minimize computational and communication overhead while providing strong privacy guarantees.
- *Parallelization*: Leveraging parallel processing can significantly improve the efficiency of PIR operations in a distributed environment. This involves dividing tasks into smaller sub-tasks that can be processed simultaneously by different nodes in the network.
- *Caching mechanisms*: Implementing caching mechanisms can reduce redundant PIR queries by storing and reusing previously retrieved information. This can be particularly useful in scenarios where multiple users query similar or identical data.
- *Batch processing*: Aggregating multiple PIR requests into batches can reduce the overall communication overhead. This approach allows nodes to process multiple requests in a single round, improving efficiency, especially in networks with latency constraints.
- *Homomorphic encryption*: Homomorphic encryption allows computations to be performed on encrypted data without decrypting it. Applying homomorphic encryption to PIR operations can enhance privacy without sacrificing efficiency, as computations can be conducted on encrypted data directly.
- *Privacy-focused blockchain*: Integrating privacy features directly into the design of the blockchain enhances the efficiency of PIR. Such features include privacy-focused consensus algorithms and/or cryptographic techniques reducing the need for extensive privacy-preserving computations.
- *Selective disclosure*: Implementing selective disclosure mechanisms allows users to reveal only the necessary information, reducing the amount of data transferred and processed during PIR operations. Besides, selective disclosure can be connected with granular control (exercising precise and detailed control over the sharing and disclosure of personal information), and contextual relevance (context-based information sharing) to enhance the functions of PIR.
- *Off-chain solutions*: Off-chain solutions, such as sidechains or layer-2 scaling solutions, can be employed to move certain PIR operations off the main blockchain, reducing congestion and improving overall efficiency.

Efficiency in PIR within blockchain's distributed environments is a challenge that requires careful consideration of trade-offs between privacy, computational complexity, and network overhead. The selection of techniques depends on a use case, desired privacy levels, and the unique characteristics of the distributed environment. Researchers and practitioners employ rigorous experimental evaluations and simulations to identify the optimal combination of privacy-preserving methods for specific contexts.

VI. COMPARATIVE DISCUSSION

In this section, we first make a comparative discussion of the available privacy-preserving architectures, which are in real-time use and we identify the pros and cons. Further, we move ahead with the existing surveys of privacy-preserving blockchains to make our present survey stand out from all.

A. REAL-TIME PRIVACY-PRESERVING BLOCKCHAIN ARCHITECTURES

Zcash's architecture relies on zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs) [83]. When users transact, this protocol enables the verification of the transaction's validity without revealing details. Zcash utilizes two types of addresses: transparent (similar to Bitcoin) and shielded (leveraging zk-SNARKs for enhanced privacy). Monero's blockchain architecture employs ring signatures for transaction privacy, ensuring unlinkability and untraceability [84]. Ring Confidential Transactions (RingCT) further obscures transaction amounts. Stealth addresses enhance recipient anonymity, generating unique addresses for each transaction. Monero's dynamic block size and regular hard forks optimize scalability and resist centralization. Enigma's blockchain architecture integrates a second-layer protocol for privacy, using secure multi-party computation (SMPC) [85]. The protocol enables decentralized applications (DApps) to process private data without exposing it on the blockchain. Enigma's "secret contracts" execute computations off-chain, preserving confidentiality. The network relies on a dual-token system, with ENG tokens for governance and fees and secret (SCRT) tokens for privacy-preserving computations. Bulletproofs is a cryptographic construction used in blockchain architectures to provide efficient and compact zero-knowledge proofs [86]. It enables confidential transactions with reduced computational and storage requirements. By verifying the validity of a transaction without exposing details, Bulletproofs enhances privacy on the blockchain. Notably, it mitigates the size scalability issues associated with traditional cryptographic constructions, making it a valuable tool for blockchain projects aiming to implement confidential and efficient transactions without compromising on security. Mimblewimble is a privacy-focused blockchain architecture that enhances confidentiality and scalability [87]. It achieves this by employing transaction aggregation and cut-through, reducing data size. Mimblewimble eliminates the need to store the entire transaction history on the blockchain, enhancing privacy. The protocol incorporates confidential transactions, obscuring amounts and ensuring unlinkability. Mimblewimble's lightweight design and emphasis on privacy make it an attractive solution for users seeking confidential and scalable transactions on the blockchain. Quorum is a permissioned blockchain platform developed by JPMorgan Chase [88]. It incorporates a privacy-focused consensus algorithm called Constellation, ensuring confidential transactions within a network. Quorum employs private smart contracts (Quorum Chaincode) to enable secure and selective sharing of transaction details. The platform allows for controlled transparency, enhancing privacy for enterprise applications. While offering decentralized features, Quorum maintains a focus on meeting the specific privacy and scalability requirements of financial institutions and enterprises, making it a suitable choice for permissioned blockchain networks with confidential transaction needs. R3 Corda is a distributed ledger platform designed for enterprise use [89]. Its architecture prioritizes privacy by adopting a ''need-to-know'' approach, sharing transaction data only with relevant parties. Corda's unique design allows for the creation of interoperable and secure smart contracts. With a focus on financial services, Corda enables direct transactions between parties, enhancing efficiency and reducing reconciliation efforts. Its permissioned network structure and emphasis on privacy make Corda suitable for diverse applications in industries where secure and confidential transactions are crucial, particularly within the context of financial services and business-to-business interactions.

B. COMPARISON OF SURVEYS

In [90], the authors provide a survey regarding the importance of security and privacy measures in the blockchain. It demonstrates numerous approaches that can be used for architectures built on blockchains, including mixing, anonymous signatures, encryption, non-interactive zero-knowledge proof, and more. In essence, it gives a general notion of the role that security and privacy play in the blockchain. The authors in [91] also discuss several privacy concerns and privacy-related blockchain challenges. It also draws attention to the cryptographic defenses that are already in place, such as transaction preservation and anonymity. Various privacy protection major techniques such as rind signature, mixing, homomorphic encryption, and son are discussed in [92]. It also provides a comparative analysis of privacy protection from the aspect of technical characteristics and anonymity. The survey in [93] focuses on different shortcomings in the blockchain network about the algorithms used. It also demonstrates various use cases for blockchain which study data provenance and ownership in conjunction with security.

The authors explore various security and privacy vulnerabilities in blockchain in [94]. It also focuses on the current methods for securing the system's privacy and makes fresh recommendations for enhancing blockchain privacy. Moreover, the work in [95] presents various privacy issues in blockchain-based frameworks such as transaction linkability, and user identity. It covers current privacy-preserving blockchain systems for use in e-health, cryptocurrencies, smart cities, and cooperative ITS. A recent study [96] on privacy-preserving discusses the existing privacy-preserving strategies thoroughly and mentions the gaps related to interoperability in blockchain-based applications. It suggests different ways to improve interoperability like hash-locking, sidechains/relays, and notary schemes. Our study examines the privacy viewpoints, parameters, and issues in comparison to the existing surveys. It also examines alternative privacy-preserving strategies for these applications and highlights the significance of blockchain in diverse applications. It also emphasizes the function of a PIR-based system in protecting user and data privacy. Further, it sheds light on how blockchain and PIR work together to enhance the privacy of blockchain-based systems. The existing survey is compared in Table 8, which also explains how our study differs from theirs.

VII. OPEN RESEARCH PROBLEMS

Our research's main objective is to draw attention to the privacy challenges currently faced by blockchain applications as well as the solutions used to get around these problems. Our survey explores several existing works related to privacy of the blockchain-based systems and highlights the existing privacy challenges. We also study the existing privacy-preserving strategies for guaranteeing privacy in blockchain applications. Our survey also studies the role of PIR in achieving privacy. Moreover, it calls into consideration whether blockchain and PIR ought to be coupled to enhance user and data privacy in blockchain-based systems. As a result, we present some research questions that shed light on the future of blockchain and PIR collaboration.

- **RQ-1: How can PIR be effectively integrated into blockchain to enhance privacy in decentralized applications?**
  To integrate PIR into blockchain for enhanced privacy in decentralized applications, smart contracts must be adapted to incorporate PIR protocols like Homomorphic

TABLE 7. Blockchain-based privacy-preserving architectures.

Name	Ref.	Pros	Cons
Zcash	[83]	Implements zero-knowledge proofs (zk-SNARKs) for transaction privacy, Offers selective transparency, allowing users to disclose transaction details if needed	zk-SNARKs can be computationally expensive, Initial setup and trust assumptions during the setup ceremony
Monero	[84]	Uses ring signatures and confidential transactions for enhanced privacy, providing unlinkability and untraceability of transactions.	Larger transaction sizes compared to other cryptocurrencies, limited scalability due to the increased computational requirements
Enigma	[85]	Implements a second-layer protocol for privacy using secure multi-party computation (SMPC), and supports decentralized applications (DApps) with private data.	Complexity in implementing and auditing SMPC protocols, potential performance overhead due to additional computation.
Bulletproofs	[86]	Efficient zero-knowledge proof system, enhancing privacy without sacrificing scalability, can be integrated into various blockchain platforms	Requires some computation, although less than some alternatives, adoption challenges due to the need for network-wide upgrades
Mimble-Wimble	[87]	Provides strong privacy through transaction aggregation and cut-through, lightweight and scalable compared to traditional blockchain architectures	Limited scripting capabilities, impacting smart contract functionality, relatively smaller user base and ecosystem
Quorum	[88]	Implements a privacy-focused consensus algorithm (Constellation), supports private transactions through the use of private smart contracts (Quorum Chaincode)	Limited adoption outside the financial industry, the complexity of setting up and managing a Quorum network
R3 Corda	[89]	Designed for privacy in enterprise scenarios, implements a "need-to-know" approach, only sharing transaction details with relevant parties	Centralized to a certain extent, with permissioned networks, limited use cases beyond specific industries

TABLE 8. Comparative analysis of the survey.

Ref.	Year	Contribution
[90]	2019	Studies the privacy issues and describes different privacy techniques
[91]	2019	Highlights the privacy issues and privacy threats and various cryptographic defense mechanisms for maintaining privacy
[92]	2020	Provides a comparative survey on major privacy protection techniques such as ring signature, homomorphic encryption, and so on
[93]	2022	Discuss the privacy aspects and highlight the loopholes in the existing solutions
[94]	2019	Describes the security and privacy attacks in blockchain and suggests new ways to improve privacy
[95]	2019	Highlight the various privacy issues specifically and survey the existing privacy-preserving solutions in different applications
[96]	2023	Study the existing literature and provide ways to improve the interoperability in blockchain-based systems while ensuring the privacy
Current Study	2023	Describes the need for privacy aspects and mentions the privacy threats. It also discusses the privacy-preserving schemes for blockchain in different applications and identifies the gap in the literature. Moreover, it emphasizes how privacy can be achieved through PIR mentioning its pros and cons. Further, it opens the way for the merger of blockchain and PIR to improve the privacy of the system with better efficiency.

Encryption or Oblivious Transfer. Decentralized storage solutions such as IPFS should be utilized to store sensitive data off-chain, with on-chain references maintained through secure mappings. Access control mechanisms within smart contracts must regulate user permissions for querying and retrieving specific data. Techniques like confidential transactions and zero-knowledge proofs should be implemented to obfuscate transaction details and enable secure data proofs.

- **RQ-2: Is anonymity advantageous for the integration of blockchains and PIR?**
  Anonymity is advantageous for integrating blockchains and PIR as it enhances user privacy through techniques like ring signatures and stealth addresses. These measures obfuscate transaction details, dissociating identities from blockchain activities. While providing increased confidentiality, it is crucial to strike a balance between anonymity and regulatory compliance, necessitating continuous research in privacy-preserving technologies for blockchain systems. Quantum-resistant cryptographic techniques might become essential to thwart potential threats posed by quantum computing to the privacy and security of blockchain and PIR systems. Moreover, AI-driven privacy-preserving algorithms may be leveraged to dynamically adapt privacy measures based on user preferences and evolving regulatory landscapes, ensuring a cutting-edge and adaptive approach to privacy in decentralized environments.
- **RQ-3: Can blockchain transactions be protected from linking attacks?**
  The literature work shows that the existing blockchain-based framework uses cryptographic mechanisms like zero-knowledge proofs, privacy wallets, and mixing techniques to protect the system from privacy leakage. Though these strategies can enhance privacy and make it more difficult to link transactions, the strategies do not provide an absolute solution to

provide transaction anonymity. Determined adversaries with sufficient resources may still find ways to link the transactions to reveal their identities based on time-based analysis of the transaction graphs and infer knowledge about value transfers. Users should consider their threat model and the specific blockchain they are using when deciding which privacy-enhancing techniques to employ. Thus, a model that provides non-linkable transactions in a blockchain environment to protect the data from a dishonest peer is suggested.

- **RQ-4: How to hide transactional data from unwanted disclosure in blockchain?**
  The existing blockchain solutions describe certain ways to protect transactional data like avoiding sharing personal information in transaction metadata and using strong passwords, two-factor authentication, and secure storage solutions for the protection of private keys. However, complete transactional data privacy is difficult to achieve specifically in public/permissionless blockchains due to their design principles of transparency and immutability. Determined adversaries with sufficient resources can de-anonymize users.
- **RQ-5: How to reduce the bandwidth in blockchain systems while applying PIR for data access?**
  In this regard, employing CPIR while committing transactions can be helpful because it eliminates the need to download the entire database. Leveraging efficient compression algorithms can further decrease the size of data payloads without compromising information integrity. The use of selective data retrieval mechanisms in PIR ensures that only relevant information is transmitted, reducing unnecessary data transfer. Off-chain storage solutions like IPFS can be employed to store large datasets, reducing the on-chain data footprint and associated bandwidth demands. Continuous research into lightweight PIR techniques and network optimization strategies contributes to further bandwidth reduction in blockchain systems.
- **RQ-6: What are the potential privacy challenges in the convergence of PIR and blockchain, and how can they be mitigated?**
  Privacy challenges in merging PIR and blockchain include potential scalability issues, as cryptographic computations in PIR can be resource-intensive. To mitigate this, optimizations such as parallelization and off-chain computation can enhance scalability. Another challenge is ensuring user anonymity, which can be addressed through the use of privacy-focused consensus mechanisms like privacy-preserving proof-of-stake. Balancing transparency with privacy poses a challenge, and the integration of confidential transactions and zero-knowledge proofs can strike this balance effectively. Lastly, robust security audits and continuous monitoring are critical to identifying and addressing vulnerabilities, ensuring a resilient and private PIR-blockchain convergence.
- **RQ-7: How to deal with deanonymization attack in blockchain?**
  To mitigate deanonymization attacks in blockchain and PIR-based data access, privacy-centric techniques like ring signatures and confidential transactions can be employed to obfuscate transaction details and sender/receiver identities. Implementing advanced cryptographic primitives, such as zero-knowledge proofs, enhances the unlinkability of user activities on the blockchain. Implementing decoy transactions and mixing services further complicates attempts to deanonymize users by introducing uncertainty about the true origin of transactions. Regularly updating privacy protocols and staying abreast of emerging cryptographic advancements can fortify defense against deanonymization attacks, ensuring a resilient and privacy-preserving blockchain ecosystem.
- **RQ-8: How can the decentralized nature of blockchain be leveraged to enhance the privacy guarantees provided by PIR?**
  Leveraging the decentralized nature of blockchain to enhance privacy guarantees in PIR involves distributing data across nodes, minimizing the risk of a single point of failure. PIR queries can be processed across the network, ensuring that no single node possesses complete information. Decentralized consensus mechanisms, such as proof-of-stake or sharding, can further disperse the responsibility of PIR processing, enhancing overall privacy. Smart contracts can facilitate secure and privacy-preserving data sharing, and the immutability of the blockchain ensures that once data is stored, it remains tamper-resistant, contributing to the integrity of PIR processes. Continuous improvement in decentralized architectures can optimize PIR for enhanced privacy in blockchain environments.
- **RQ-9: What impact does the integration of PIR and blockchain have on the performance and latency of data retrieval in decentralized applications?**
  The integration of PIR and blockchain can impact the performance and latency of data retrieval in decentralized applications. PIR protocols, while enhancing privacy, may introduce computational overhead. Optimizations, such as parallelization and off-chain computation, can mitigate these issues. Furthermore, leveraging efficient consensus mechanisms and decentralized storage solutions, like IPFS, can contribute to improved performance. Consideration of factors like network latency and transaction throughput is crucial in designing PIR-blockchain integration that strikes a balance between enhanced privacy and acceptable performance levels. Continuous testing and optimization are essential to fine-tune the system for optimal decentralized application performance.
- **RQ-10: How can PIR and blockchain be applied to secure identity management in decentralized**

systems?
The integration of PIR and blockchain in decentralized systems offers a robust solution for secure identity management. Blockchain's decentralized ledger ensures tamper-resistant storage of identity data, reducing the risk of unauthorized alterations. PIR protocols enable users to selectively disclose identity attributes during verification, enhancing privacy. Smart contracts can be employed to manage decentralized identity issuance and verification, ensuring transparency and security. Zero-knowledge proofs, when integrated, allow users to prove possession of certain identity attributes without revealing sensitive information. Decentralized identifiers (DIDs) can be linked to off-chain identity data, fostering a secure and privacy-centric identity management system. Continuous advancements in cryptographic techniques and blockchain governance contribute to the ongoing enhancement of secure identity management in decentralized ecosystems

- **RQ-11: What role can zero-knowledge proofs play in combining PIR and blockchain for improved privacy?**
  Zero-knowledge proofs play a crucial role in combining PIR and blockchain, enhancing privacy by allowing one party to prove knowledge of certain information to another without revealing the information itself. In the context of PIR, zero-knowledge proofs enable a user to prove the validity of their query response without disclosing the specific data queried. This ensures data confidentiality while allowing verifiable transactions on the blockchain. The implementation of techniques like zk-SNARKs (zero-knowledge succinct non-interactive arguments of knowledge) in smart contracts facilitates efficient and succinct proofs, minimizing computational overhead. The integration of zero-knowledge proofs in blockchain-PIR systems provides a powerful tool for privacy-preserving transactions, identity verification, and confidential data sharing in decentralized applications. Continuous research and refinement of zero-knowledge proof techniques contribute to the ongoing evolution of privacy-enhanced blockchain ecosystems.
- **RQ-12: In what ways can PIR and blockchain be utilized for confidential and auditable transactions in decentralized financial systems?**
  In decentralized financial systems, PIR and blockchain can be employed for confidential and auditable transactions. Smart contracts can utilize PIR to selectively retrieve and process financial transaction details while maintaining user privacy. Blockchain's transparency ensures auditable transactions, and the integration of privacy-preserving techniques, such as confidential transactions, enables secure financial interactions without exposing sensitive information. This approach combines the benefits of privacy and auditability, crucial for fostering trust in decentralized financial ecosystems.
- **RQ-13: What are the potential trade-offs between privacy and transparency when implementing PIR in a decentralized blockchain setting?**
  Implementing PIR in a decentralized blockchain setting involves navigating potential trade-offs between privacy and transparency. While PIR enhances privacy by allowing users to retrieve specific information without revealing the queried data, it may introduce computational overhead, impacting transaction speed. Striking a balance requires optimizing PIR protocols to mitigate latency concerns without compromising privacy. The choice of cryptographic primitives, such as zero-knowledge proofs, can influence the trade-off, as they enable verifiability without full disclosure. Decentralized systems must carefully design access controls and user permissions to manage the tension between data confidentiality and blockchain's inherent transparency. Continuous research and development in PIR techniques aim to minimize these trade-offs, advancing privacy in decentralized blockchain environments.
- **RQ-14: How can the combination of PIR and blockchain be extended to secure data sharing and collaboration in decentralized networks and federated or collaborative environments?**
  The combination of PIR and blockchain can be extended to secure data sharing and collaboration in decentralized networks and collaborative environments. Smart contracts can facilitate PIR-based access controls, allowing selective data retrieval and sharing while preserving privacy. Utilizing DIDs and verifiable credentials ensures secure and privacy-preserving user authentication within collaborative environments. Off-chain storage solutions, such as interplanetary file systems (IPFS), enhance data scalability and accessibility while maintaining the integrity of shared information on the blockchain. Employing zero-knowledge proofs enables users to prove ownership or knowledge of certain data without disclosing the actual content, fostering secure collaboration in federated settings. Continuous advancements in cryptographic techniques and decentralized governance models contribute to the ongoing improvement of secure data sharing and collaboration in decentralized and federated environments.
- **RQ-16: How can the integration of PIR and blockchain enhance user privacy by mitigating the risks associated with on-chain data leakage?**
  The integration of PIR and blockchain enhances user privacy by mitigating risks associated with on-chain data leakage. PIR protocols allow users to query data without revealing the specific information being accessed, preventing the exposure of sensitive details on the blockchain. Off-chain storage solutions, such as IPFS, can be employed to store confidential information, reducing the reliance on on-chain data storage. Smart contracts can manage access controls, ensuring that

only authorized parties can retrieve specific information, thus minimizing the risk of unauthorized on-chain data access. Continuous advancements in cryptographic techniques and decentralized governance models contribute to the ongoing improvement of user privacy and the prevention of on-chain data leakage.

- **RQ-17: How can the transparency of blockchain be maintained while still preserving the privacy of sensitive transaction details using PIR?**
  Maintaining the transparency of blockchain while preserving the privacy of sensitive transaction details using PIR involves employing cryptographic techniques such as zero-knowledge proofs. Zero-knowledge proofs enable a prover to demonstrate the validity of a statement without revealing specific details, allowing for transparent verification without exposing sensitive information. PIR protocols, integrated into smart contracts, enable users to selectively retrieve transaction details without disclosing the entire transaction history. Confidential transactions, a cryptographic technique, further enhances privacy by obfuscating the transaction amounts while preserving the integrity of the blockchain. This combination ensures that while the blockchain remains transparent, the privacy of sensitive transaction details is maintained, striking a balance between openness and confidentiality. Continuous refinement of cryptographic protocols and governance models contributes to the ongoing evolution of this transparent yet privacy-preserving approach in blockchain systems.
- **RQ-18: How can PIR and blockchain collaboratively contribute to data minimization strategies in decentralized systems, reducing the exposure of unnecessary information?**
  PIR and blockchain collaboratively contribute to data minimization by using selective or minimal disclosure. PIR protocols enable users to query specific data points without revealing the entire dataset, ensuring minimal exposure. Smart contracts enforce access controls leading to the least privilege. The decentralized and transparent nature of blockchain ensures that only authorized entities have access to the required data, reducing exposure to unnecessary information.
- **RQ-19: What cryptographic techniques can be employed to secure PIR within a blockchain, ensuring that user data remains confidential in a decentralized setting?**
  To secure PIR within a blockchain and ensure user data confidentiality in a decentralized setting, cryptographic techniques such as Homomorphic Encryption and Oblivious Transfer can be employed. Homomorphic Encryption allows computations on encrypted data, ensuring the privacy of user queries during PIR operations. Oblivious Transfer enables users to retrieve information without revealing their specific choice, contributing to confidential data access in decentralized applications.

The blockchain and PIR both provide privacy in their own way but have certain drawbacks. We observe that both techniques have many common characteristics such as distributed database, security, and privacy. Furthermore, the cross-chain solutions in blockchain give rise to privacy challenges on the other hand provide interoperability. For instance, if a blockchain application is to be deployed to manage and track the supply of vaccinations all around the globe and another blockchain keeps the record of the COVID patients with their vaccination check. If we connect these two chains, then privacy has to be taken care of at various levels. This can be achieved with the help of PIR. Our study analyzes several privacy issues and clarifies how blockchain and PIR can be used to ensure privacy and security in several applications including including IoT, SCM, healthcare, finance, e-commerce, and others. our review of the existing investigations applies to all decentralized and distributed system-based applications. PIR schemes and blockchain both undoubtedly have benefits and drawbacks, but combining both strategies could be advantageous and mark a new turning point in the history of the technological revolution. This partnership enables the creation of a system that encourages non-anonymous users to broadcast anonymous transactions to the blockchain network.

Another important fact to notice is that, in all the probable solutions suggested in the above-mentioned research problems, cryptographic methods are important. However, as we have discussed earlier in Section IV, cryptographic methods can pose challenges to blockchain transactions with increased complexity, reduced throughput, reduced scalability, and increased transaction finality time. Thus, we need a careful balance between the two contradictory parameters of cryptography for privacy preservation and the performance of blockchains. Employing lightweight cryptographic algorithms, optimizing key management, and exploring innovations like post-quantum cryptography can enhance transaction speed. Batch processing, where multiple transactions are grouped for simultaneous cryptographic operations, reduces overhead. Implementing parallelization for cryptographic tasks and leveraging hardware acceleration, such as secure enclaves, further boosts efficiency. Continuous research and development are essential to identify new cryptographic techniques that can enhance security without compromising the scalability and speed of blockchain networks.

VIII. CONCLUSION

Our survey mentions the existing privacy concerns in blockchain applications. It also examines the practices now in use to improve privacy in blockchain-based systems. Our review's main objective is to identify privacy needs that have not been fully satisfied by state-of-the-art blockchain technologies and notify the future designs and developments of privacy-ensured decentralized applications. We also talk about the PIR concept and go over the available literature on it. This will help researchers and academicians figure out the loopholes in the existing techniques and come up with new solutions to improve privacy in blockchain applications. Further, we discuss how the collaboration of blockchain and PIR could be beneficial as both are completely different from each other. The open research problems highlight how both techniques could be clubbed to achieve the required privacy parameters namely, user and transaction anonymity and unlinkability of transactions in blockchain applications.

REFERENCES

[1] C. Komalavalli, D. Saxena, and C. Laroiya, ''Overview of blockchain technology concepts,'' in *Handbook of Research on Blockchain Technology*. New York, NY, USA: Academic, 2020, pp. 349–371.

[2] M. A. Khan and K. Salah, ''IoT security: Review, blockchain solutions, and open challenges,'' *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[3] B. Ahmed, ''IoT and blockchain convergence: Benefits and challenges,'' *IEEE Internet Things J.*, vol. 9, pp. 1–10, 2017.

[4] R. Chatterjee and R. Chatterjee, ''An overview of the emerging technology: Blockchain,'' in *Proc. 3rd Int. Conf. Comput. Intell. Netw. (CINE)*, Oct. 2017, pp. 126–127.

[5] S. Hong, ''Strongly connected topology model and confirmation-based propagation method for cross-chain interaction,'' 2015, *arXiv:2102.09237*.

[6] L. Cao and B. Song, ''Blockchain cross-chain protocol and platform research and development,'' in *Proc. Int. Conf. Electron., Circuits Inf. Eng. (ECIE)*, Jan. 2021, pp. 264–269.

[7] N. Shadab, F. Houshmand, and M. Lesani, ''Cross-chain transactions,'' in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2020, pp. 1–9.

[8] S. Lin, Y. Kong, and S. Nie, ''Overview of blockchain cross-chain technology,'' in *Proc. 13th Int. Conf. Measuring Technol. Mechatronics Automat. (ICMTMA)*, Jan. 2021, pp. 357–360.

[9] S. Srinawakoon. *Ripple-Backed Cross-Chain DeFi Platform Kava Integrates Band Protocol for Decentralized Oracle Support*. Accessed: Jan. 1, 2021. [Online]. Available: https://medium.com/bandprotocol/ripple-backed-cross-chain-defi-platform-kava-integrates-band-protocol-for-decentralized-oracle-2b29a7b50ae5

[10] G. Wood. *Polkadot: Vision for a Heterogeneous Multi-Chain Framework*. Accessed: Jan. 1, 2021. [Online]. Available:https://polkadot.network/PolkaDotPaper.pdf

[11] A. Culwick and D. Metcalf. *The Blocknet Design Specification*. Accessed: Jan. 1, 2021. [Online]. Available: https://blocknet.co/whitepaper/Blocknet Whitepaper.pdf

[12] *Aion: The Open Application Network*. Accessed: Jan. 1, 2021. [Online]. Available: https://aion.theoan.com/whitepapers

[13] A. P. Joshi, M. Han, and Y. Wang, ''A survey on security and privacy issues of blockchain technology,'' *Math. Found. Comput.*, vol. 1, no. 2, pp. 121–147, 2018.

[14] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, and P. Rimba, ''A taxonomy of blockchain-based systems for architecture design,'' in *Proc. IEEE Int. Conf. Softw. Archit. (ICSA)*, Apr. 2017, pp. 243–252.

[15] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, ''Blockchain challenges and opportunities: A survey,'' *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[16] H. S. Dawood, ''Book notes: Understanding privacy, by daniel J. Solove,'' *Osgoode Hall Law J.*, vol. 47, no. 4, pp. 819–820, Oct. 2009.

[17] A. Pfitzmann and M. Hansen, ''A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management,'' Tech. Rep., 2010, pp. 1–96.

[18] N. Gupta, ''A deep dive into security and privacy issues of blockchain technologies,'' in *Handbook of Research on Blockchain Technology*. New York, NY, USA: Academic, 2020, pp. 95–112.

[19] Amlegals Legal Strategies. *Data Privacy Issues in Blockchain*. Accessed: Sep. 20, 2023. [Online]. Available: https://amlegals.com/data-privacy-issues-in-blockchain

[20] G. Navarro-Arribas and V. Torra, ''Information fusion in data privacy: A survey,'' *Inf. Fusion*, vol. 13, no. 4, pp. 235–244, Oct. 2012.

[21] P. A. Schott, *A Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism*. Washington, DC, USA: World Bank Publications, 2006.

[22] M. Gill, ''Preventing money laundering or obstructing business: Financial companies' perspectives on 'know your customer' procedures,'' *Brit. J. Criminol.*, vol. 44, no. 4, pp. 582–594, Jul. 2004.

[23] R. Douceur, ''The Sybil attack,'' in *Proc. 1st Int. Workshop Peer Peer Syst.*, 2002, pp. 251–260.

[24] G. Danezis and A. Serjantov, ''Statistical disclosure or intersection attacks on anonymity systems,'' in *Proc. Int. Workshop Inf. Hiding*. Cham, Switzerland: Springer, 2004, pp. 293–308.

[25] Y. Gao, J. Shi, X. Wang, R. Shi, Z. Yin, and Y. Yang, ''Practical deanonymization attack in Ethereum based on P2P network analysis,'' in *Proc. IEEE Int. Conf. Parallel Distrib. Process. With Appl., Big Data Cloud Comput., Sustain. Comput. Commun., Social Comput. Netw. (ISPA/BDCloud/SocialCom/SustainCom)*, Sep. 2021, pp. 1402–1409.

[26] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, ''Evaluating user privacy in Bitcoin, financial cryptography and data security,'' in *Proc. 17th Int. Conf.* Cham, Switzerland: Springer, 2013, pp. 34–51.

[27] M. Vasek, M. Thornton, and T. Moore, ''Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem,'' in *Financial Cryptography and Data Security*. Cham, Switzerland: Springer, 2014, pp. 57–71.

[28] B. Johnson, A. Laszka, J. Grossklags, M. Vasek, and T. Moore, ''Game-theoretic analysis of DDoS attacks against Bitcoin mining pools,'' in *Financial Cryptography and Data Security*. Cham, Switzerland: Springer, 2014, pp. 72–86.

[29] K. Abouelmehdi, A. Beni-Hssane, H. Khaloufi, and M. Saadi, ''Big data security and privacy in healthcare: A review,'' *Proc. Comput. Sci.*, vol. 113, pp. 73–80, Jan. 2017.

[30] S. Milton, ''Data privacy vs. data security,'' in *Global Business Leadership Development for the Fourth Industrial Revolution*. Hershey, PA, USA: IGI Global, 2021, pp. 209–235.

[31] G. Wood, *Ethereum: A Secure Decentralized Generalized Transaction Ledger*, vol. 151. Zug, Switzerland: Ethereum Project Yellow Paper, 2014, pp. 1–32.

[32] L. A. Linn and M. B. Koo, ''Blockchain for health data and its potential use in health it and healthcare-related research,'' in *Proc. ONC/INST*, 2016, pp. 1–10.

[33] X. Min, Q. Li, L. Liu, and L. Cui, ''A permissioned blockchain framework for supporting instant transaction and dynamic block size,'' in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Aug. 2016, pp. 90–96.

[34] Y. Xu, Q. Li, X. Min, L. Cui, Z. Xiao, and L. Kong, ''E-commerce blockchain consensus mechanism for supporting high-throughput and real-time transactions, Networking, Applications, and Worksharing,'' in *Proc. 12th Int. Conf. Comput. Netw., Appl., Worksharing* Cham, Switzerland: Springer, 2016, pp. 490–496.

[35] Y.-H. Chen, S.-H. Chen, and I.-C. Lin, ''Blockchain based smart contract for bidding system,'' in *Proc. IEEE Int. Conf. Appl. Syst. Invention (ICASI)*, Apr. 2018, pp. 208–211.

[36] C. Liu, Y. Xiao, V. Javangula, Q. Hu, S. Wang, and X. Cheng, ''NormaChain: A blockchain-based normalized autonomous transaction settlement system for IoT-based e-commerce,'' *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4680–4693, Jun. 2019.

[37] Y. Jiang, C. Wang, Y. Wang, and L. Gao, ''A privacy-preserving e-commerce system based on the blockchain technology,'' in *Proc. IEEE Int. Workshop Blockchain Oriented Softw. Eng. (IWBOSE)*, Feb. 2019, pp. 50–55.

[38] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, ''Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control,'' *J. Med. Syst.*, vol. 40, no. 10, pp. 1–8, Oct. 2016.

[39] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, ''Integrating blockchain for data sharing and collaboration in mobile healthcare applications,'' in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Oct. 2017, pp. 1–5.

[40] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K. R. Choo, ''Blockchain: A panacea for healthcare cloud-based data security and privacy?'' *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan. 2018.

[41] K. M. Hossein, M. E. Esmaeili, T. Dargahi, A. Khonsari, and M. Conti, "BCHealth: A novel blockchain-based privacy-preserving architecture for IoT healthcare applications," *Comput. Commun.*, vol. 180, pp. 31–47, Dec. 2021.

[42] K. Azbeg, O. Ouchetto, and S. J. Andaloussi, "Access control and privacy-preserving blockchain-based system for diseases management," *IEEE Trans. Computat. Social Syst.*, vol. 10, no. 4, pp. 1515–1527, Aug. 2023.

[43] D. A. Luong and J. H. Park, "Privacy-preserving blockchain-based healthcare system for IoT devices using Zk-SNARK," *IEEE Access*, vol. 10, pp. 55739–55752, 2022.

[44] P. Sharma, S. Namasudra, N. Chilamkurti, B.-G. Kim, and R. Gonzalez Crespo, "Blockchain-based privacy preservation for IoT-enabled healthcare system," *ACM Trans. Sensor Netw.*, vol. 19, no. 3, pp. 1–17, Aug. 2023.

[45] F. Tian, "An Agri-food supply chain traceability system for China based on RFID & blockchain technology," in *Proc. 13th Int. Conf. Service Syst. Service Manage. (ICSSSM)*, Jun. 2016, pp. 1–6.

[46] Y. Madhwal and P. B. Panfilov, "Blockchain and supply chain management: Aircrafts parts business case," in *28th Annals DAAAM Int. Symp.*, 2017, pp. 1051–1056.

[47] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, "Blockchain-based traceability in Agri-food supply chain management: A practical implementation," in *Proc. IoT Vertical Topical Summit Agricult. Tuscany (IoT Tuscany)*, May 2018, pp. 1–4.

[48] B. Bura, S. Topal, and U. Nuriyev, "TPPSUPPLY: A traceable and privacy-preserving blockchain system architecture for the supply chain," *J. Inf. Secur. Appl.*, vol. 66, pp. 103–116, May 2022.

[49] B. Aljabhan and M. A. Obaidat, "Privacy-preserving blockchain framework for supply chain management: Perceptive craving game search optimization (PCGSO)," *Sustainability*, vol. 15, no. 8, p. 6905, Apr. 2023.

[50] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A lightweight scalable blockchain for IoT security and anonymity," *J. Parallel Distrib. Comput.*, vol. 134, pp. 180–197, Dec. 2019.

[51] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623.

[52] Y. Rahulamathavan, R. C. Phan, M. Rajarajan, S. Misra, and A. Kondoz, "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Dec. 2017, pp. 1–6.

[53] L. Zhou, L. Wang, Y. Sun, and P. Lv, "BeeKeeper: A blockchain-based IoT system with secure storage and homomorphic computation," *IEEE Access*, vol. 6, pp. 43472–43488, 2018.

[54] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, "Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city," *IEEE Access*, vol. 7, pp. 18611–18621, 2019.

[55] A. Z. Ourad, B. Belgacem, and K. Salah, "Using blockchain for IoT access control and authentication management," in *Proc. 3rd Int. Conf. Internet Things (ICIOT)*, 2018, pp. 150–164.

[56] N. Tapas, G. Merlino, and F. Longo, "Blockchain-based IoT-cloud authorization and delegation," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Jun. 2018, pp. 411–416.

[57] Q. Zhao, S. Chen, Z. Liu, T. Baker, and Y. Zhang, "Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems," *Inf. Process. Manage.*, vol. 57, no. 6, Nov. 2020, Art. no. 102355.

[58] T. Li, H. Wang, D. He, and J. Yu, "Blockchain-based privacy-preserving and rewarding private data sharing for IoT," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 15138–15149, Aug. 2022.

[59] Y. Wu, S. Tang, B. Zhao, and Z. Peng, "BPTM: Blockchain-based privacy-preserving task matching in crowdsourcing," *IEEE Access*, vol. 7, pp. 45605–45617, 2019.

[60] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-Health systems via consortium blockchain," *J. Med. Syst.*, vol. 42, no. 8, pp. 1–18, Aug. 2018.

[61] M. Yang, T. Zhu, K. Liang, W. Zhou, and R. H. Deng, "A blockchain-based location privacy-preserving crowdsensing system," *Future Gener. Comput. Syst.*, vol. 94, pp. 408–418, May 2019.

[62] Q. Feng, D. He, S. Zeadally, and K. Liang, "BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4146–4155, Jun. 2020.

[63] C. Lin, D. He, X. Huang, N. Kumar, and K. R. Choo, "BCPPA: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 12, pp. 7408–7420, Dec. 2021.

[64] W. Zhang, Y. Yuan, Y. Hu, S. Huang, S. Cao, A. Chopra, and S. Huang, "A privacy-preserving voting protocol on blockchain," in *Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD)*, Jul. 2018, pp. 401–408.

[65] W. Jiang, H. Li, G. Xu, M. Wen, G. Dong, and X. Lin, "PTAS: Privacy-preserving thin-client authentication scheme in blockchain-based PKI," *Future Gener. Comput. Syst.*, vol. 96, pp. 185–195, Jul. 2019.

[66] A. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, Jan. 2019.

[67] L. Lin, Y. Tian, and Y. Liu, "A blockchain-based privacy-preserving recommendation mechanism," in *Proc. IEEE 5th Int. Conf. Cryptography, Secur. Privacy (CSP)*, Jan. 2021, pp. 74–78.

[68] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "PrivChain: Provenance and privacy preservation in blockchain enabled supply chains," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Aug. 2022, pp. 157–166.

[69] S. Jiang, J. Cao, H. Wu, K. Chen, and X. Liu, "Privacy-preserving and efficient data sharing for blockchain-based intelligent transportation systems," *Inf. Sci.*, vol. 635, pp. 72–85, Jul. 2023.

[70] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin, "Protecting data privacy in private information retrieval schemes," *J. Comput. Syst. Sci.*, vol. 60, no. 3, pp. 592–629, Jun. 2000.

[71] S. Vithana, Z. Wang, and S. Ulukus, "Private information retrieval and its applications: An introduction, open problems, future directions," Tech. Rep., 2023, pp. 1–13.

[72] L. Weng, L. Amsaleg, A. Morton, and S. Marchand-Maillet, "A privacy-preserving framework for large-scale content-based information retrieval," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 152–167, Jan. 2015.

[73] R. Tajeddine, O. W. Gnilke, D. Karpuk, R. Freij-Hollanti, C. Hollanti, and S. E. Rouayheb, "Private information retrieval schemes for coded data with arbitrary collusion patterns," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2017, pp. 1908–1912.

[74] K. Banawan and S. Ulukus, "Private information retrieval through wiretap channel II: Privacy meets security," *IEEE Trans. Inf. Theory*, vol. 66, no. 7, pp. 4129–4149, Jul. 2020.

[75] I. Kerenidis and R. de Wolf, "Quantum symmetrically-private information retrieval," *Inf. Process. Lett.*, vol. 90, no. 3, pp. 109–114, May 2004.

[76] T. H. Chan, S.-W. Ho, and H. Yamamoto, "Private information retrieval for coded storage," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2015, pp. 2842–2846.

[77] R. Zhou, T. Guo, and C. Tian, "Weakly private information retrieval under the maximal leakage metric," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2020, pp. 1089–1094.

[78] K. Qin, H. Hadass, A. Gervais, and J. Reardon, "Applying private information retrieval to lightweight Bitcoin clients," in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, Jun. 2019, pp. 60–72.

[79] J. Vora, A. Nayyar, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and J. J. P. C. Rodrigues, "BHEEM: A blockchain-based framework for securing electronic health records," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2018, pp. 1–6.

[80] M. M. Badr, W. A. Amiri, M. M. Fouda, M. M. E. A. Mahmoud, A. J. Aljohani, and W. Alasmary, "Smart parking system with privacy preservation and reputation management using blockchain," *IEEE Access*, vol. 8, pp. 150823–150843, 2020.

[81] S. Singh, D. Satish, and S. R. Lakshmi, "Ring signature and improved multi-transaction mode consortium blockchain-based private information retrieval for privacy-preserving smart parking system," *Int. J. Commun. Syst.*, vol. 34, no. 14, p. 911, Sep. 2021.

[82] A. Johnson, C. Wacek, R. Jansen, M. Sherr, and P. Syverson, "Users get routed: Traffic correlation on tor by realistic adversaries," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2013, pp. 337–348.

[83] Z. Zhang, W. Li, H. Liu, and J. Liu, "A refined analysis of zcash anonymity," *IEEE Access*, vol. 8, pp. 31845–31853, 2020.

[84] M. Möser, K. Soska, E. Heilman, K. Lee, H. Heffan, S. Srivastava, K. Hogan, J. Hennessey, A. Miller, A. Narayanan, and N. Christin, "An empirical analysis of traceability in the Monero blockchain," *Proc. Privacy Enhancing Technol.*, vol. 2018, no. 3, pp. 143–163, Jun. 2018.

[85] G. Zyskind, O. Nathan, and A. Pentland. (2015). *Enigma: Decentralized Computation Platform with Guaranteed Privacy*. Accessed: Dec. 12, 2023. [Online]. Available: http://livinglab.mit.edu/wp-content/uploads/2016/01/enigma_full.pdf

[86] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Short proofs for confidential transactions and more," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2018, pp. 315–334.

[87] C. Lin, D. He, X. Huang, X. Xie, and K. R. Choo, "PPChain: A privacy-preserving permissioned blockchain architecture for cryptocurrency and other regulated applications," *IEEE Syst. J.*, vol. 15, no. 3, pp. 4367–4378, Sep. 2021.

[88] M. Mazzoni, A. Corradi, and V. Di Nicola, "Performance evaluation of permissioned blockchains for financial applications: The ConsenSys quorum case study," *Blockchain, Res. Appl.*, vol. 3, no. 1, Mar. 2022, Art. no. 100026.

[89] R. G. Brown. (2018). *The Corda Platform: An Introduction*. Accessed: Dec. 12, 2023. [Online]. Available: https://www.corda.net/content/corda-platform-whitepaper.pdf

[90] Q. Feng, "A survey on privacy protection in the blockchain system," *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, Jan. 2019.

[91] D. Wang, J. Zhao, and Y. Wang, "A survey on privacy protection of blockchain: The technology and application," *IEEE Access*, vol. 8, pp. 108766–108781, 2020.

[92] T. T. Huynh, T. D. Nguyen, and H. Tan, "A survey on security and privacy issues of blockchain technology," in *Proc. Int. Conf. Syst. Sci. Eng. (ICSSE)*, Jul. 2019, pp. 362–367.

[93] M. T. Mahmood, O. N. Ucan, and A. A. Ibrahim, "A survey on privacy and policy aspects of blockchain technology," in *Proc. Int. Conf. Eng. MIS (ICEMIS)*, Jul. 2022, pp. 1–11.

[94] J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. Torres Moreno, and A. Skarmeta, "Privacy-preserving solutions for blockchain: Review and challenges," *IEEE Access*, vol. 7, pp. 164908–164940, 2019.

[95] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Comput. Surv.*, vol. 52, no. 3, pp. 1–34, 2019.

[96] R. Yin, Z. Yan, X. Liang, H. Xie, and Z. Wan, "A survey on privacy preservation techniques for blockchain interoperability," *J. Syst. Archit.*, vol. 140, Jul. 2023, Art. no. 102892.

[97] T.-M. Choi and T. Siqin, "Blockchain in logistics and production from blockchain 1.0 to blockchain 5.0: An intra-inter-organizational framework," *Transp. Res. E, Logistics Transp. Rev.*, vol. 160, Apr. 2022, Art. no. 102653.

[98] S. Tanwar, "Blockchain revolution from 1.0 to 5.0: Technological perspective," in *Blockchain Technology*. Springer, 2022, pp. 43–61.

[99] G. Verma, "Blockchain-based privacy preservation framework for healthcare data in cloud environment," *J. Experim. Theor. Artif. Intell.*, vol. 36, no. 1, pp. 147–160, Jan. 2024.

[100] X. Wu, Y. Liu, J. Tian, and Y. Li, "Privacy-preserving trust management method based on blockchain for cross-domain industrial IoT," *Knowl.-Based Syst.*, vol. 283, Jan. 2024, Art. no. 111166.

ARCHANA CHHABRA is currently pursuing the Ph.D. degree with Lovely Professional University, Punjab, India. Her research interests include blockchain, intrusion detection, and artificial intelligence.

RAHUL SAHA (Member, IEEE) received the Ph.D. degree in cryptography from Lovely Professional University, Punjab, India. He is currently a Professor with Lovely Professional University. Previously, he was a Postdoctoral Researcher with the University of Padova, Italy. He has authored and coauthored more than 50 publications in various international journals and conferences. His research interests include network security, cryptography, blockchain, DLTs, and IoT security.

GULSHAN KUMAR (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from Lovely Professional University, Punjab, India, in 2017. He is currently a Postdoctoral Researcher with the University of Padova, Italy; and an Associate Professor with Lovely Professional University. His current research interests include cyber-physical systems, blockchain, edge and cloud computing, wireless sensor networks, and optimization techniques.

TAI-HOON KIM (Member, IEEE) received the B.E. and M.E. degrees from Sungkyunkwan University, South Korea, and the Ph.D. degree from the University of Bristol, U.K., and the University of Tasmania, Hobart, TAS, Australia. He is currently affiliated with the School of Electrical and Computer Engineering, Chonnam National University, Republic of Korea. His main research interests include security engineering for IT products, IT systems, development processes, and operational environments.