A Survey of Privacy Concerns in Blockchains and Information Retrieval

Archana Chhabra [a], Rahul Saha [b], Gulshan Kumar [c], Tai Hoon Kim [d]

[a] *School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India*
[b] *School of Computer Science and Engineering ,Lovely Professional University, Phagwara, Punjab, India*
[c] *School of Computer Science and Engineering,Lovely Professional University, Phagwara, Punjab, India*
[d] *Glocal Campus, Konkuk University, 268 Chungwon-daero Chungju-si Chungcheongbuk-do, 27478, South Korea*

Abstract

With the increase in population the number of internet users has also increased over the years, protecting the privacy of user data has become an important issue. To maintain the privacy of ones' information many techniques are there but, each of them has one or the other loophole. Moreover, the emerging cross-chain technology to provide interoperability is another part of concern for blockchains. In this paper, the concept of security and privacy is studied in relation to blockchain technology and how the blockchain network is more secure as compared to other networks. Also, the survey has been done on the advancement of blockchain in different applications such as e-commerce, health care, etc. and techniques based on private information retrieval to maintain privacy of data has also been studied. Further, the analysis has been done to conjugate the blockchain and private information retrieval to provide better security and privacy to the internet users.

Keywords

Privacy, Security, Blockchain, PIR, survey

1. Introduction

In this era of technological revolution, the blockchain is considered to be the new concept after the internet since 2008, when it was first introduced by the researcher who implemented the concept of the digital currency known as bitcoin. With time various cryptocurrencies came into existence such as Ethereum which introduces smart contracts, but, the blockchain is emerging as one of the most promising and innovative techniques of cyber-security. It provides a secure, transparent, and distributed framework for sharing, exchanging, and integrating the information among several users and third parties. The idea behind building blockchain was aiming at a network without any control of the central body. The blockchain uses the consensus protocol to ensure the integrity of the data stored in the system. For instance, one may assumes it an easy task to steal something from a box kept at an isolated place instead stealing something from a box kept in open under many eyes. Thus, the blockchain can be considered as a public ledger in which all committed transactions are stored in the list of blocks open to all and where new blocks can be appended whenever required. The fundamental characteristics of the blockchain are shown in Figure 1.

Algorithms, Computing and Mathematics Conference, August 19 – 20, 2021, Chennai, India.
EMAIL: rsahaaot@gmail.com (Rahul Saha)
ORCID: 0000-0003-3921-9512 (Rahul Saha)

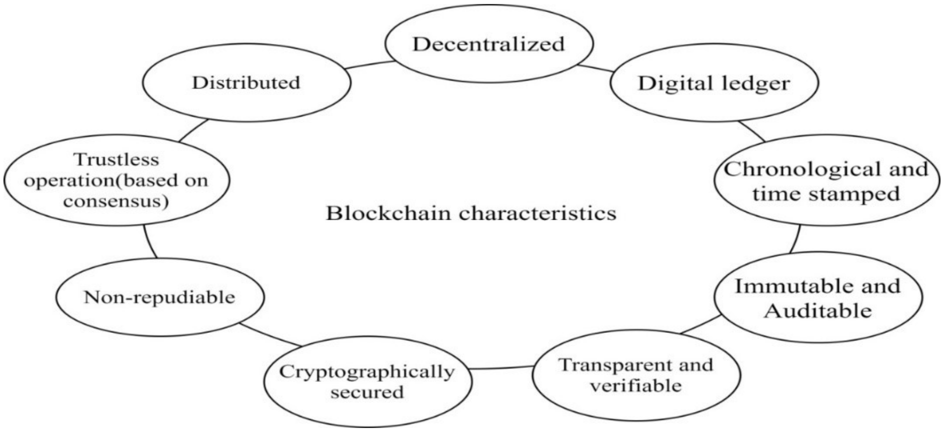
Decentralized
Digital ledger
Chronological and time stamped
Immutable and Auditable
Transparent and verifiable
Cryptographically secured
Non-repudiable
Trustless operation(based on consensus)
Distributed
Blockchain characteristics

Figure 1: Characteristics of Blockchain

1.1. Motivation behind Blockchain

Blockchain is an innovation to the financial transactions which are based on the involvement of trusted third-party between the buyer and the seller such as e-bay/amazon, etc. that provides a trusted platform for both the users. But trusting someone always remains an issue in the world of the internet. Therefore, the blockchain network aimed to overcome this issue by providing a data structure to store and retrieves data in a secure, distributed, and decentralized way. These features made the blockchain network popular and gain acceptance in various domains over internet such as healthcare, IoT, supply chain management, e-commerce, etc. It has been observed that transparency, openness, and decentralization are the biggest motivating factors that lead to the development and success of blockchain technology by overcoming the problem of a single point of system failure which is very common in centralized systems. Moreover, the blockchain facilitates immutability of records which ensure the integrity of data even in the case of public ledgers [1].

Though the blockchain has great potential to become a new engine over internet to conduct digital commerce and share our personal data and life events in different domains but there are some serious challenges in implementing blockchain. Firstly, it suffers from scalability problem as it cannot handle large number of daily transactions in banking sector because it requires many updates in the single transaction to complete which is not allowed by blockchain as the records once written in the chain of blocks cannot be altered. To make any changes new blocks should be added which in turn further needs to be verified and validated. This will not only decrease the transaction speed but also increases the cost of the transaction. It could be handled with storage optimization and increasing the block size but, then there will always be a trade-off between block size and optimization. Secondly, initial cost of implementing blockchain network is quite high. Moreover, it may also suffer from privacy leakage in spite of the fact that user are using their public and private keys. In this paper, we discuss the major advantages of using blockchain in each application of digital world despite having certain challenges. Also, we shed some light on benefits of using blockchain in conjunction with private information retrieval schemes in contrast to the existing solutions and how privacy can be maintained in a better way over the internet.

1.2. What is Blockchain?

A blockchain consists of blocks connected in a chronological order. Each block in the chain contains data to share or transact, hash of that data, and the previous hash which is open and accessible by all on the network as shown in Figure 2. One of the biggest advantages of blockchain is that it is decentralized and distributed in nature which makes it more secure. It uses a peer-to-peer network (decentralized) for managing the chain rather than the centralized network. Therefore it is open and public to anyone to join the chain [2]. The blocks in blockchain are connected to each other in a chronological order. From this architectural point of view, we can list some basic properties of blockchain:

1. Blocks can store any type of data.
2. Ensures data integrity.
3. Append-only.
4. Specific communication protocol is used because of decentralized network.
5. Uses a consensus algorithm, like proof-of-work, which reduces the chance of malicious node to enter.

For example, if the blockchain is about bitcoins it will contain data for transactions, information about receiver and sender, and the number of bitcoins present in the network. Each block contains a hash value which is verified and if there is any change in the hash value then it means the hash does not belong to that block. Moreover, each block also contains the hash of the previous block which facilitates the connectivity of blocks to each other. Once a transaction is added to the block of a chain it cannot be altered or tempered, hence, provides more security. Thus, a blockchain provides a secure way of transaction among any two peers in an open network which could be verified if required.

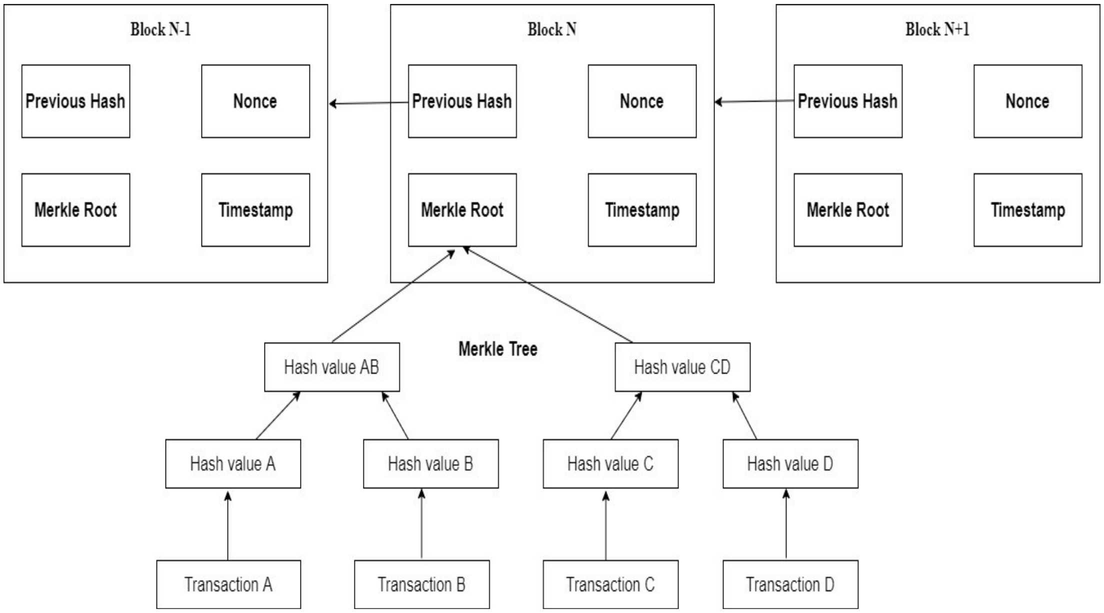

Figure 2: Structure of blockchain

1.3. History and Evolution of Blockchain

Blockchain technology is based on the concept of decentralized and distributed computing. Blockchain is not a new term rather it was practiced first in the 1990s to stop tampering with documents by a group of researchers. But it got fame in the year 2009 when it was used and implemented by Santoshi Nakamoto to create digital cryptocurrency also known as bitcoin [3]. The invention of bitcoin as blockchain helped in overcoming the problem of double-spending over the internet without any intervention of a trusted third party.

After bitcoin, the fame of blockchain on the internet keeps growing on in the form of cryptocurrency as an application of cash till 2012, but sooner people started using digital currency as a secure way for transferring payment electronically in the form of smart contracts by 2013. Before this many people believe that bitcoin and blockchain are similar terms. But after 2014 the research has been made that blockchain can also be used for different applications such as health care systems, supply chain management, e-voting, IoT, and many more. Nowadays, more work is being done on blockchain in different fields which deals with the privacy of information retrieval over the network globally [4] [5]. The Figure 3 below show the growth in blockchain technology over the years.

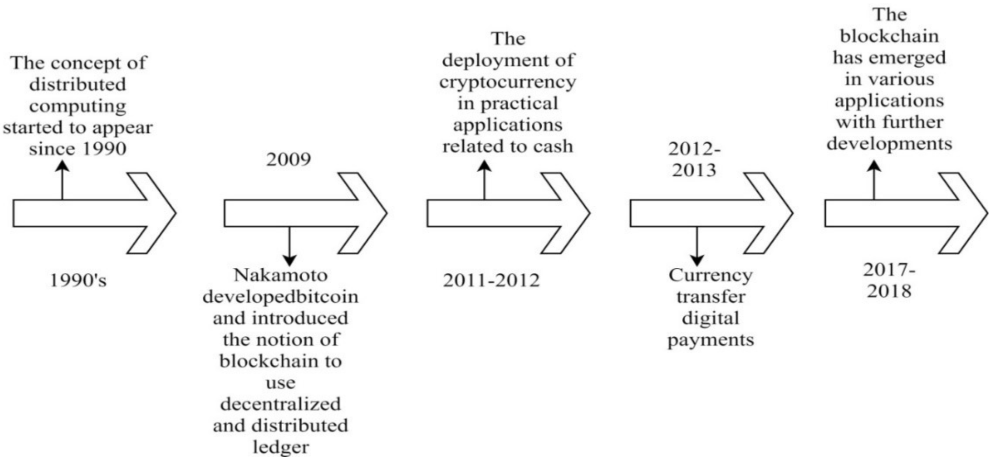
The concept of distributed computing started to appear since 1990
1990's
2009
Nakamoto developedbitcoin and introduced the notion of blockchain to use decentralized and distributed ledger
The deployment of cryptocurrency in practical applications related to cash
2011-2012
2012-2013
Currency transfer digital payments
The blockchain has emerged in various applications with further developments
2017-2018

Figure 3: History of Blockchain

Another new addition in this blockchain development is Cross Chain [6]. The blockchain alone cannot provide the features such as interoperability among different connected entities on the network [7] [8]. Cross chain attempts to solve all this issue [9]. One excellent example of a blockchain project which is trying to explore cross chain transactions through banking services in cross-border networks is Ripple [10]. Secondly, Polkadot allows the transfer of smart contract data through various blockchains [11]. Futher, the Blocknet are currently working on creating a decentralized exchange all in the effort of enhancing interchange communication [12]. Aion online is another blockchain project that deals with scalability and interoperability issues of blockchains. It is also coming up as a standard protocol used by various blockchains [13]. All these projects of Cross Chains are in infancy stage and needs rigorous feasibility studies in corresponding to standalone blockchains. However, they possess benefits of scalability, interoperability and more decentralization and also leave behind various research questions.

1.4. Types of Blockchain

Blockchain networks are broadly classified into three type's namely public blockchain, private blockchain and consortium blockchain [14].

1. Public blockchain: In this type of blockchain there is no restriction on access by anyone. Therefore, it is also known as a permissionless blockchain. Anybody having an internet connection and wish to communicate can become a participant of the network by following the consensus protocol (set of rules). Whenever a new node joins the network all the previous chain history is shared with that node. It is extremely secure because of its redundant nature [15]. Moreover, the public system facilitates anonymity and transparency of data on the network. The most common example of public blockchain technology is Bitcoin and Ethereum blockchain.
2. Private blockchain: A private blockchain is based on permission. One can only join the network after getting an invitation request from the administrator. It is controlled by authorized users. Therefore provides more privacy as compared to public blockchain and is more adaptable by government and private sector companies because a central authority is required to govern which

makes the network more secure, faster, and more efficient. But it has one downside also they do not follow the concept of decentralization in contrast to public blockchain [16].

3. Consortium blockchain: It is also known as a hybrid blockchain because it is a mixture of both private and public blockchain networks. Hence it provides the advantages of both the networks that are it is partly centralized as it is not completely controlled by one organization rather it is ruled by a dedicated group of people such as board members and also partly decentralized because each node is given the right to make choice for their data or transaction to be kept open or private in advance. Hence it plays a vital role in increasing the efficiency and transactional privacy of the network [15].

1.5. Contribution and Organization

Blockchain is gaining popularity in various application domains. The transparency and decentralization of blockchains are no doubt the advantages of this technology; the privacy concerns are still an open question for blockchains. Therefore, we survey all the existing literature that is connected with privacy issues or privacy solutions in blockchains or related applications. This survey also covers the ways related to information retrieval with privacy preservation which is a good candidate for blockchains for privacy issues of open and immutable transactions. This survey will be helpful for the privacy researchers; blockchain researchers to develop privacy assured applications. The major contribution of this survey is as follows:

1. We survey the privacy-based blockchain literature. To the best of our knowledge, this survey is the first of its kind in this direction.
2. We categorize the blockchain privacy solutions based on applications.
3. We also consider the privacy information retrieval problems and solutions which is another novelty of this survey.

The rest of this paper is organized as follows. Section II explains privacy perspectives. Section III describes the literature work related to the importance of maintaining privacy using blockchain in different fields. Section IV provides the analysis of the literature and limelight the problems that persist related to privacy that can be worked upon. Further, Section V concludes the paper by discussing the latest trend in technology and gives the outcome of the research work.

2. Privacy Perspectives

Privacy is the state of being free from public scrutiny or from having your secrets or personal information shared. When you have your own room that no one enters and you can keep all of your things there away from the eyes of others, this is an example of a situation where you have privacy. Privacy has a quite long history it has its origin since ancient times. The protection of privacy from the technical aspect is also very important because today with the advancement in science and technology dependency of people on laptops, mobiles, desktop, etc for socializing themselves is highly increased. Daniel Solove has defined privacy [17] as involving the right of mandating personal privacy concerning storing, re-purposing, provision to third parties, and displaying of information pertaining to oneself via the internet.

Privacy of an individual could belong to financial privacy, internet privacy, medical privacy, sexual privacy, and political privacy. Every individual wants their personal information is not to be shared or used by others to avoid themselves from discrimination, personal embarrassment, or damage to one's professional reputation [18].

2.1. Privacy Parameters

There are following ways to assure privacy of an individual:

1. Identifiability: It is defined as the extent to which a person's identity can be identified directly or indirectly. The linking of information to a particular data set refers to a person's identity [18].
2. Anonymity: It means hiding the real identity of the person due to which he will be non-identifiable, unreachable, or untrackable by others. It is a technique by which one can feel free to do whatever he wants by hiding himself. But on the darker side, it could also be misused by an individual to lie easily to others [18].
3. Pseudonymity: It is derived from the word 'pseudonym' meaning 'false name', which allows a person to use other names instead of using his real identity to communicate with others. Pseudonymity has become essential on the internet on computer networks and also it is used in conjunction with other features of privacy. A digital pseudonym consists of a bit of string that is unique as Id and is used to authenticate the person and his data [18].
4. Unlinkability: It is a state of the system in which it is very difficult for the attacker or observer to detect whether the two sets of data are related to each other or not. Unlinkability ensures that a user may make multiple uses of resources or services without others being able to link these uses together [19].
5. Unobservability: It is the property of privacy that makes an intruder unable to observe the information being shared on the network indistinguishable. It means the attacker can notice who is sending messages and who is receiving nut cannot relate who is sending data to whom. Unobservabilty is considered as a desirable property in steganographic systems [19].
6. Transparency: It is the ability to easily access and work with data no matter where the data is located or what kind of application has created the data. It also ensures that the data being reported is accurate and is coming from an authorized source which builds the interest and trust of people communicating over network [18].
7. Intervenability: It is the ability which allows an individual to raise a complaint whenever he feels his privacy is harmed by someone [19]. For data controllers, intervenability allows them to have efficient means to control their data processors as well as the respective IT systems to prevent undesired effects. Examples for such means may be the ability to stop a running process to avoid further harm or allow investigation, to ensure secure erasure of data including data items stored on backup media, and manually overruling of automated decisions or applying breaking glass policies.

2.2. Privacy Methods

For protecting an individual's personal information certain security measures are to be taken so that the privacy of the data could be assured. To maintain the privacy of information it is very important to determine what kind of data is collected (e.g. medical, financial or personal), where and how it is to be gathered, who can access it, and so on. To protect the systems from data privacy breach following measures can be taken [20] [21]:

1. Change management: People must keep on updating their information frequently on the internet specifically social media sites so that their information cannot be tracked easily by a malicious user.
2. Data loss prevention: It helps in monitoring and protecting the data in motion on the network, data in storage, and also the data in use in end devices. Moreover, it also helps to block attacks, privilege abuse, and unauthorized access, malicious web request, and unusual activities to prevent data theft.

3. Data masking: It helps in anonymizes data by encrypting or hashing, perturbation, and generalization. Also, it facilitates data pseudonymization by replacing sensitive information with realistic fictional data which helps in maintaining operational and statistical accuracy of information.
4. Data Protection: It ensures the integrity and confidentiality of data by controlling change reconciliation, data across borders, query whitelisting, etc.
5. Ethical walls: It creates a boundary between business groups to comply with M and A requirements, government clearance, etc.
6. Information auditing and archiving: It provides monitoring of data by law and contractual regulations. Whenever there is unauthorized access or change made to the data it activates warning triggers. Further, it creates an audit trail for forensic visibility.
7. User rights management and tracking: It keeps a track of end-user web application by mapping it with the shared database/application and finally to the data accessed. Also, it identifies excessive, inappropriate, and unused privileges.

2.3. Privacy requirements in Blockchain

To protect the privacy in blockchain-based applications two requirements have to be fulfilled that is the links between transactions should not be visible or discoverable and the content of transactions is only disclosed to the peers involved. These requirements could be set easily in case of private/permissioned blockchain by keeping the transaction transparent to all. But, in case of public blockchain everyone has access to the network with no restrictions so the privacy requirements should be considered on the basis of following two factors:

1. Identity Privacy: It is the property which allows an individual to hide his real identity from others on the network. But, even if a user apply random addresses (or pseudonyms) while making transactions in blockchain network, they have only limited identity privacy because an adversary who is observing the unencrypted network and traversal through the public blockchain, may discovers who is using the network and for what purpose by utilizing certain behavioral analysis strategies such as Anti-Money Laundering (AML) regulation [22] and Know Your Customer (KYC) policy [23].
2. Transaction Privacy: This property allows a user to provide restrictive access to his transactional details such as amount or the transaction pattern could only be accessed by specific users on the network instead being visible to all in public blockchain network. For example, in electrical health record management or big data's anonymous authentication and authorization, users do not want to disclose their sensitive information to all which raised a need for higher levels of privacy to build an individual's trust in the application.

2.4. Privacy threats for Blockchain

The protection of privacy is a critical issue in blockchain network because of its transparent and publicly available nature one can easily make privacy breach while observing the network communication. This section covers certain major privacy attacks that could be made in blockchain.

1. Privacy Leakage: This attack is mainly caused by reuse of addresses by the users in the network. Public address of each peer is open to all in the network which could easily be traced by any adversary via internet. Though, the peers are allowed to use different pseudonyms for different transactions to hide their real identities but the adversary can link it to the actual user as all the transactional details related to a node is visible to all the peers which is a major drawback of blockchain [24].

2. Selfish mining: In this, the selfish miners keep the mined blocks with themselves as secret blocks rather broadcasting it on the network and continue doing this until their chain of secret blocks become bigger than the actual public chain. The blocks generated by other miners are thus pruned /ignored and are not considered for reward. So, selfish miners tend to get more revenue. Therefore, the rational miners would be attracted to the selfish pool and want to join it which makes the selfish miner power more than 51 percent quickly and increases the chances of attack in the network [24].
3. Sybil attack: It is a kind of cyber-attack in which the adversaries try to create multiple fake identities to gain large number of influencing nodes in the network. As per the PoW consensus more than 50 percent power is required to gain control on the network, so the adversary try to make as much fake identities as it can to rule the network and intrude personal information of the users. This attack may further leads to strong privacy leakage if the blockchain network is compromised [25].
4. Linking attack: These attacks are more common in blockchain-based IoT's. For instance, an anonymized data collected from two separate transactions which contains records of an individual can be linked together using certain algorithms to fetch the details of the user maliciously and it could happen because of the distributed nature of the blockchain network. Thus, the anonymized data is not 100 percent private, so to maintain the privacy strong privacy-protection methods are to be applied [26].
5. Transactional fingerprints: It is another threat to the anonymity of transactions. It could be possible if one could gain access to any of the six mentioned aspects of the transaction namely, Random time-interval (RTI), hour of day (HOD), time of hour (TOH), time of day (TOD), coin flow (CF), and input/output balance (IOB). The extra knowledge about any of these may lead to de-anonymize a user [27].
6. Distributed denial of service: In this attack a dishonest miner node may uses the large number of peers in the network to send a lot requests to the victim node such as invalid transaction, invalid blocks and so on in order to disrupt the victim's transaction to complete [28].

3. Related work on privacy

In the field of computing, blockchain technology is the biggest innovation of the 21st century which has shown major advances in many fields from financial to manufacturing as well as education and medical. It is still unknown to many but the concept was there in existence since the 1990s and gained popularity a few years back.

In early 1991 the famous scientists Stuart Haber and W. Scott Stornetta discovered the term blockchain, which consists of a secured cryptographic chain of blocks containing documents whose timestamps, could not be tampered with by anyone. After a year in 1992, the system was upgraded by incorporating the concept of Merkle trees to improve efficiency by providing support for a large number of documents in one block. The major change to the blockchain technique was made in the year 2008 by Santoshi Nakamoto who worked as a team and invented Bitcoin-a digital ledger application also known as cryptocurrency. Also, he published the first paper on Bitcoin technology in 2009, in which he provided details about building trust in digital cash and the importance of decentralization in computing [29].

The blockchain is a peer-to-peer distributed network that is secured and used to record transactions on a number of computers. It is transparent to all the connected nodes which enable all to access the shared content over the network. It provides a secure way for people to make any kind of transactions without the involvement of a trusted third party.

Many people have the misconception that Bitcoin and blockchain can be used interchangeably but the fact is- Bitcoin is the first application of blockchain technology that came into existence in 2008. After digital cash with the advancement in technology, blockchain has gain popularity in other applications such as smart contracts, real estate, etc by the end of the year 2015. The Most common application during that period is the innovation of Ethereum which differs from Bitcoin as it provides the feature to record other assets such as slogans and contracts in addition to timestamp. Ethereum was officially launched by Buterin in 2015 and given great competition to the Bitcoin technique and gain popularity in the space of cryptocurrency. Also in 2015, the concept of Hyperledger connecting digital ledger was come into existence by LINUX foundation under the leadership of Brian Behlendorf which seeks for the collaborative development of distributed ledgers. Its main focus is to improve the reliability and performance of the current system to support global business transactions.

Blockchain does not stop rising after Ethereum and Bitcoin rather it has now gained popularity in many fields including finance, insurance, medical, education, and so on. In recent years, many large enterprises and government agencies are exploring blockchain technology applications to achieve wonders in this era of the digital world. No doubt blockchain is now into every field but it still has many loopholes in each application area which is to be addressed.

Potential applications of blockchain can be categorized as shown:

1. Blockchain in Finance: Blockchain was primarily designed for Bitcoin which is the most commonly known digital currency based on the concept of decentralization. Other than Bitcoin, it was later used for Ethereum, Peercoin, Altercoin, etc. [30]. Blockchain fulfills the necessary security and privacy aspects of financial transactions between users so the concept of bitcoin is adopted worldwide. Blockchain provides full confidentiality of the data being transact as it uses encryption algorithms to gain access to the data. Further by mixing certain hashing techniques at different levels of a transaction, provides data integrity that is once the data is written no one on the network can change it. Also, it facilitates a non-repudiation feature by recording the time and information of each transaction made between different users on the network.
2. Blockchain in healthcare: Maintaining health record manually is a very time consuming and tedious task. To overcome this, many hospitals are now opting for online healthcare systems provided publicly by some authorized organizations over the globe. These organizations guarantee the security and privacy of an individual's health record shared on the network. The blockchain technique for storing the health information of people works differently from the Bitcoin concept as it is not to be accessed by all on the network, so there must be some central body to govern all the data stored [31]. To provide better security services data should be collected in a repository which could also be termed as data lakes. And to fetch data from that lake one must be an authorized user of it. Also, to maintain the privacy of information each individual or owner of the data must be given the authority to share his/ her information with whom they want and not to be accessed by anyone who is part of the network. All these measures are provided by blockchain technology so it is fruitful to use this technology worldwide. Moreover, as blockchain networks are distributed in nature so it also provides the built-in feature of fault-tolerance across the network.
3. Blockchain in IoT: IoT is an interface that allows the nodes to connect and communicate to transfer data over the network without any intervention of human to human or human to computer interaction [32] [33]. Nodes could be any device, person, object, animal, etc. Using blockchain in conjunction with IoT storage of data and accessing it a much simpler task from any remote location while also ensuring security and privacy of user's information in the network. For example, while creating an online account for accessing any application an individual has to go through a long sequence of steps that are asked by the service provider to be fulfilled before utilizing their services. Also, it asks for a certain set of questions to be answered such as What's your pet's name? so that in case of verification of account because of forgot password or any other issue it can guarantee a privacy check to the account holder by asking such questions. As

the internet is growing day by day so the demand for secure IoT is also increasing which could be provided with the help of Blockchain. The Major use of Blockchain-based IoT is in building smart contracts, RFID, Digital wallets, and so on. The biggest challenge of implementing blockchain in IoT is the scalability of the network because, with an increase in the number of computing devices, request-response time will also increase.

4. Blockchain in other domains: In addition to the above-mentioned application areas of blockchain, it could also be developed or used for security and privacy of other domains such as defense, supply chain management, automobile industry, education, and government. Despite many advantageous features, blockchain technology still takes 10 to 15 more years for establishing its roots in these fields.

The increase in digitization of personal information and internet technologies poses several challenges to consumer's private information being shared on the network. Moreover, the consumers are a great source of providing data for web blogs and social networking sites so their private information is more vulnerable on the internet. Therefore, privacy has always been a great topic to research for scholars for many years. However, recently the research is more influenced by the threats to privacy and the ways to overcome them. Further in this paper, privacy issues of blockchain technology in different areas are discussed from the year 2015 till now. The literature is divided based on different application areas of blockchain.

3.1. Privacy of Blockchain in financial market

After the innovation of bitcoin and its alternative cryptocurrencies such as Ethereum, Litecoin, Primecoin financial services have affected for nearly a decade. Since then the banking industry is widely affected by economic transformation, internet development, and financial innovations. Therefore, the banking industry requires an urgent change and also needs to seek new growth of avenues. This change could only be made possible with the adoption of blockchain technology in the financial sector which has given a new direction to the finance market by inventing FinTech in 2016 [34]. Mu Qi-Guo in 2016 has put light on the fact that blockchain will fundamentally revolutionize the existing operational models of finance and economy which might further lead to great technological innovations in the field of FinTech. In this paper, the author has discussed all the possible changes that could be made to the existing financial market in collaboration with blockchain technology highlighting all the benefits and challenges in the field.

Further, the new studies made by IBM have found that blockchain solutions are being adopted worldwide. The survey data clear that 15 percent of banks and 14 percent of financial institutions intend to implement blockchain commercially on large scale by 2017 [35].

Moreover, the survey results of another research known as "Blockchain Rewires Financial Markets: Trailblazers take the lead", has taken a sample of 200 financial institutions from all over the globe and concluded that 7 on the count of 10 financial companies are focusing on integrating blockchain technology for assuring the following four areas namely, clearing and settlement of transactions, wholesale payments, issuance of debt and equity, reference data. All this is made possible because the blockchain promises a transparent, secure, and reliable platform to each participating entity in the network.

Quan Khanh Nguyen in 2016 has studied the financial crisis in the banking economy and how they have been overcome with the adoption of blockchain technology in the financial sector. It has made the management of money by consumers very easy by providing relevant applications for smartphones, laptops, and tablets and blessed the world of digitization to achieve wonders. The author concluded that blockchain opens a new era of opportunities where the nature of business among people will transform from competition to cooperation [36].

3.2. Privacy of Blockchain in E-commerce

Xinping Min et al. in 2016 have studied the comparison between permissioned blockchain framework (PBF) and bitcoin –derived blockchain in E-commerce and suggested the improvement in terms of throughput, latency, and capacity. The author analyzed the pros and cons of both the techniques and designed the permissioned blockchain framework to support the instant transaction and dynamic block size in e-commerce. His framework is based upon peer inner blockchain Protocol (PIBP) provide better throughput and overcome latency issue. Moreover, to prevent a dishonest peer to enter a network to assure high credibility of transaction author used a permissioned trusted trading Network (PTTN) [37].

Yukin Xu and Xinping Min et al. in 2017 have derived a new consensus mechanism to provide better credibility in comparison to previously existing consensus algorithms. The authors presented E-commerce blockchain consensus mechanisms (EBCM) which do not work on the principle of computing power and token rather works in a similar level of security and credibility as Nakamoto's consensus. EBCM is capable to achieve high throughput in a real-time transaction. The author compares the EBCM with Bitcoin to justify better throughput and latency. And finally, the author concludes that EBCM is best suited to deal with the low credibility of transactions as it helps in building a safe and public autonomous transaction network [38].

Yi-Hui Chen et al. in 2018 have applied the blockchain technique on one of the most used applications of e-commerce over the internet is E-Auction which suffers from trust issues on the intermediary between the buyer and the seller. And secondly, costs high to pay the trusted third party. The author applied a decentralized peer to peer blockchain technique to resolve both the issues mentioned. The peer to peer access structure guarantees the trusted communication from one point to another by authenticating themselves before transferring the data. And the decentralization feature cuts own the cost of a centralized trusted party. For this, the smart contract is created which hides the bidding cost from the lead bidder. To assure these certain rules are created and as a smart deal which cannot be opened before the deadline. In this paper, the author provides a mechanism based on blockchain for E-auction which deals with confidentiality, non-repudiation, and tamper-proofing of the bid [39].

C.Liu et al. in 2018 have developed a normalized autonomous transaction system based on blockchain facilitating IoT-based e-commerce. The author designed a three-layer NormaChain sharding blockchain network that works to increase the efficiency of the transaction and also the scalability of the system. Moreover, the author also uses the decentralized public-key encryption scheme (PEKS) to guarantee illegal and unwanted user access to avoid crime transactions. Moreover, it also protects from ciphertext attacks as stealing of secret keys is not possible which guarantees legitimate privacy to the user [40].

Y.Jiang et al. in 2019 have proposed a blockchain-based e-commerce system for preserving privacy while shopping online. The author derived a protocol that prevents the user from any kind of identity threat such as address or contact number, etc. The author uses blockchain technology to protect user's information by implementing private smart contracts which act as a bridge between the buyer and the seller at the time of transaction and hides the personal details of the user. Also, the author used the zero-knowledge proof algorithm called zk-SNARKs which create and issue shield token to generate proof of ownership among the users [41].

Table 1 shows the research gap in the area of maintaining privacy in e-commerce using blockchain.

Table 1: Privacy of Blockchain in E-commerce

Ref-no	Year	Contribution	Privacy Parameter	Blockchain type	Research gap
37	2016	Peer inner blockchain protocol for trusted transaction	Identifiabliblity and unlinkability	Private/permissioned blockchain	Storage of transactions and blocks
38	2017	E-commerce blockchain consensus mechanism	Identifiability, credibility and unobservability	Consortium Blockchain	Storage of transaction and blocks, Data consistency
39	2018	Blockchain based Smart Contract for Bidding System	Anonymity, unlinkability and unobservability	Consortium blockchain	Complex Architecture and Implementation cost
40	2018	Normachain	Anonymity, unlinkability and unobservability	Consortium blockchain	Trasaction handling
41	2019	Blockchain-based e-commerce system	Anonymity and pseudonymity	Public/permission-less blockchain	Scalability

3.3. Privacy of Blockchain in healthcare

Xiao Yue et al., in 2016 built an application named Healthcare Data Gateway (HDG) is a blockchain-based framework that allows patients to own, control, and share their information securely without hampering their privacy. Two protocols are used in the model to safeguard patient's data, first is Indicator-centric schema (ICS) which helps patients to organize all kinds of personal health records easily and the second is secure multi-party computing (MPC) which protects the patient information from an untrusted third party to access. The author designed three-layer architecture to build his mobile app for supporting the mentioned features and making it easy for an individual to install it on their phone and can access it from anywhere. The HDG supports anonymization, secure communication, and data backup and recovery [42].

Xueping Liang et al., in 2017 discussed the privacy and security issues in the existing electronic health care mobile applications and tried to cover some of them in a better way by proposing a new framework that integrates the feature of decentralized and permissioned blockchain to preserve the individual's identity by allowing him to manage his data manually as the data is shared and synchronized via the cloud with the healthcare providers and health insurance companies. The author also worked on improving the scalability and performance by adopting a tree-based data processing algorithm to handle large sets of data at the same time. The author developed a mobile app works on hyper ledger fabric blockchain technology which validates the nodes on the network to assure the privacy of the healthcare system that is between the end-user and the cloud [43].

Christian Esposito et al., in 2018 put the limelight on the limitations to the existing cryptographic framework used to address security and privacy in cloud-based health care systems and also suggested better solutions to overcome the current issues to host and share data within the cloud. Manual maintenance of health records has become a hectic job that everybody is bored off. Therefore, certain techniques have been designed to store the medical records and personal health data of an individual on an electronic platform which has various drawbacks such as identity theft for personal benefits, etc are mentioned in this paper. The author proposed a conceptual blockchain-based health care ecosystem to provide better security and privacy for sharing data within the cloud. This system facilitates the following four benefits as described in the paper that there is no requirement of the third party to sign the agreement which protects the system from a single point of failure. Secondly, each patient is allowed to access and control their details. Thirdly, medical history is recorded as a chain of blocks that is consistent, accurate, complete, and timely distributed among all on the network. Lastly, in case any changes made to the data on blockchain will be visible to all patients or members on the network. But on the darker side, the author also mentioned some of the challenges that have to be considered while its practical implementation such as the data on the blockchain is immutable that is the data once added cannot be altered or removed, it should be dealt with in while implementing [44].

Table 2 describes the gap in the area of health-care implementation using Blockchain.

Table 2: Privacy of Blockchain in Healthcare

Ref-no	Year	Contribution	Privacy Parameter	Blockchain type	Research gap
42	2016	Build an app HDG using blockchain	Identifiabliblity and unlinkability	Private/permissioned blockchain	High computational cost and scalability
43	2017	Blockchain for data sharing and collaboration-a mobile application	Identifiability, unlinkability and pseudonymity	Private/Permissioned Blockchain	Access control and large database
44	2018	A conceptual blockchain-based to protect health data stored in a cloud	Identifiability, Anonymityand unlinkability	Consortium blockchain	Complex Architecture and Implementation cost

3.4. Privacy of blockchain in supply chain management

Feng Tiang et al., in 2016 studied the agri-food supply logistics in China and find out the problems that persist in the existing logistics pattern of the market which is traceability of the product supplied. To overcome these issues the author discussed the advantages and disadvantages of RFID and blockchain technology and discovered how it can benefit the supply of the food chain market in China. The author developed a conceptual framework to design an agri-food supply chain traceable system which helps in enhancing food safety, quality and also helps in reducing the loss incurred during the logistics process. And finally, compare the results with the traditional food chain system and proves it better in terms of monitoring and tracing of food quality and safety from the farm to the fork [45].

In comparison to the above-mentioned conceptual framework Miguel Pincheira et al., in 2018 has practically implemented a system for agri-food supply chain management with some changes and analyzed the performance of the system on different factors. The authors designed and deployed a system called 'AgriBlockIot' based on decentralized blockchain and integrated it with IoT sensor devices for better results. This system assures the transparent and auditable asset traceability of the food along the whole supply chain from production to consumption. The author implemented the system on two different blockchains that is Ethereum and hyper ledger sawtooth and compares the results of both the techniques based on latency, CPU, and network usage, and also lime lighted its pros and cons. The author concluded that the performance of hyper ledger system is better than that of one implemented with Ethereum but in certain scenarios, it is better to use Ethereum technique instead of the hyper ledger. He discovered it is more convenient to use Ethereum blockchain with IoT device in case of more scalability and reliability is needed, otherwise, it is better to use hyper ledger blockchain because it is considered as a mature implementation at the level of Ethereum [46].

Yash Madhwal and Peter B. Panfilov, in 2017 has mentioned the importance of SCM in the aviation industry and discussed the loopholes in the existing supply chain of spare parts of the aircraft's globally. The author showcases the use of blockchain in managing the inventory of aircrafts spare parts and also monitoring its performance and usage. This will help in achieving a transparent network for the supply of different parts and reduce the risk of black marketing the product. The author concluded that these new data-driven distributed techniques will help the SCM managers to analyze the supply, demand, and source of availability of the parts and also protect them from any illegal access [47].

Table 3 highlights the gaps in the field of maintaining privacy in supply chain management using Blockchain.

Table 3: Privacy of Blockchain in Supply Chain Management

Ref-no	Year	Contribution	Privacy Parameter	Blockchain type	Research gap
45	2016	RFID and blockchain-based agri-food chain	Traceability and authenticity	Public/permission-less blockchain	High implementation cost, Storage and synchronization
46	2018	AgriBlockIoT	Transparency and traceability	Public/Permission-less Blockchain	Single language used for smart contracts and Computation

					cost
47	2017	Blockchain-based SCM for spare parts of an aircraft	Transparency and availability	Public/Permission-less Blockchain	Authentication of spare parts, RFID tags and smart contracts can be used for better results

3.5. Privacy of Blockchain in IoT

Ali Dorri et al., in 2017 has proposed an optimized blockchain for IoT systems to provide better security and privacy in IoT devices connected over the network. Though the blockchain technique is expensive and suffers from high overlay bandwidth and delays which does not complement IoT devices, they suggested a lightweight blockchain-based architecture in conjunction with IoT which provides most of the security and privacy features of IoT devices at low overhead and delay. To examine his idea he tried to implement it on a smart home but can also be applied to other IoT applications. The author followed a three-tier hierarchical structure to provide optimize resource usage and also increase the scalability of the network but still has to work upon consensus for better results [48].

Moreover, Ali Dorri et al., later in 2017 has proposed a better or modified lightweight scalable (LSB) blockchain framework to assure security and privacy in IoT devices. In this paper, the author tried to overcome certain drawbacks of IoT systems such as limited resource consumption, centralization, and lack of privacy. The author proposed a comprehensive tired LSB framework that will meet all the major requirements of the IoT devices and applications. Also, the blockchain technology will help in preserving the security and privacy of the network. The architecture works on the principle of lightweight consensus algorithm which proved better in terms of latency, overhead, and scalability [49].

Yogachandran Rahulamathavan et al., in 2017 have developed an IoT ecosystem based on blockchain using the Attribute-based encryption (ABE) technique for maintaining privacy in the network. The author sheds light on basic properties provided by blockchain such as data integrity, non-repudiation but he also mentioned that confidentiality and privacy are the two major issues that are still to be overcome in a better while appending blockchain to IoT. This novel architecture provides both confidentiality and access control and also identified as an effective technique for data communication in decentralized networks. The ABE algorithm provides end-to-end privacy in the ecosystem because only the trusted miners in the network can decrypt the encrypted data by the sender [50].

Lizing Zhou et al., in 2018 has proposed a novel system to provide better security and privacy features for IoT applications called 'Beekeeper' which involves the concept of threshold servers and homomorphic computation on the data stored in blockchain. The author used Ethereum blockchain and threshold secure multi-party protocol to perform computations (TSMPC) on the server's data. The system allows any node to become a leader if it desires to be. Moreover, the homomorphic computation helps the server to process user's data easily without learning anything from it. The performance of the Beekeeper system can be increased rapidly as it allows or attracts external computing devices to join the network. Further, it also protects from any malicious node to enter as TSMPC helps in verifying the threshold number of its servers is active or not. Therefore, the proposed model guarantees the decentralization, confidentiality, anonymity, homomorphic threshold, and credibility of the transaction [51].

Md. Abdur Rahman et al., in 2019 has designed and implemented a Mobile edge computing (MEC) framework based upon blockchain and IoT for facilitating secure sharing economic services in smart cities. The author worked upon one of the major issues faced by the sharing economy that is the management of the unique identity and verification of each stakeholder securely and anonymously. The author mentioned the pros and cons of using cognitive edge computing with blockchain to support the sharing economy application of IoT and come up with an architecture that supports decentralization on and off storage blockchain, identity management, and smart contract services to transact the data [52].

Abdallah Zoubir Ourad et al., in 2018, have discussed how the use of blockchain technology in conjunction with IoT provides better access and authentication of user data on the network. The authors reviews the basic IoT authentication model and also the blockchain-based authentication model and based on their pros and cons a new architecture is using Ethereum smart contracts to address the challenges in the existing model [53].

Nachiket Tapas et al., in 2018 has proposed an enhanced model based upon blockchain to overcome the drawbacks of existing IoT cloud-based data storage applications. The author implemented his model using smart contracts over Ethereum platform. It mainly focuses on providing better access control and audit operations over the network. The author took into consideration the concept of a smart city to prove his idea as smart cities are well suited for research in multiple areas nowadays. The author highlighted that the infrastructure of smart cities can be viewed as a heterogeneous network of cyber resources that leads to deal with the problem of access control, authorization, and delegation of IoT-cloud resources [54].

Table 4 shows the research gap in the area of IoT using blockchain technology.

Table 4: Privacy of Blockchain in IoT

Ref-no	Year	Contribution	Privacy Parameter	Blockchain type	Research gap
48	2017	Optimized Blockchain for IoT	Anonymity and unlinkabilty	Public/permission-less blockchain	Overhead and overlay can be improved
49	2017	Blockchain-based smart home framework	Identifiability, anonymity and unlinkabilty	Consortium blockchain	Computation and implementation cost is high
50	2017	IoT ecosystem using ABE technique	Anonymity, unlinkability and unobservability	Private/Permissioned Blockchain	Scalability and computational cost
51	2018	IoT system based on TSMPC protocol	Anonymity, unlinkability and	Public/permission-less blockchain	Scalability

			unobservability		
52	2019	MEC-based economy system	Identifability and anonymity	Private/Permissioned blockchain	System can be further tested for sharing economies at a large scale
53	2018	Oauth implementation via smart contract	Identifability, anonymity and unobservability	Public/permission-less blockchain	Consumption(gas) cost and scalability can be improved
54	2018	IoT system for Cloud Authorization and Delegation	Anonymity and unlinkabiltiy	Public/permission-less blockchain	Usage of Smart contracts for SmartMEEcosystem

3.6. Privacy preserving strategies for blockchain

Undoubtedly, the blockchain technology has achieved milestone in a diversity of applications over internet assuring better privacy and security in contrast to the various other centralized and distributed techniques but it is still vulnerable to certain privacy attacks because of its openness and transparency among all the peers in the network. Therefore, surveys has been conducted which highlights the available techniques used for enhancing privacy of blockchain in a diversity of applications.

Qu Feng et al., in 2019 has studied the weaknesses of existing wireless communication channel for VANETs (Vehicular ad-hoc Network) and come up with a novel framework based on blockchain technology known as BPAS (Blockchain-assisted Privacy-preserving Authentication System) which facilitates the auto authentication of the vehicles while preserving the privacy at same time. The authors uses hyperledger fabric platform for deploying the framework and evaluating the results to verify. To hide the real identity of the vehicle owner and providing the traceability of the vehicle at the same time is a tedious task which is successfully achieved by the authors with this architecture. The various algorithms are used namely, fuzzy extractor which will enhance the security at the time of authenticating the vehicle, ABE (Attribute-based Encryption to ensure the privacy of user, and blockchain and smart contracts which will help in maintaining access controls and provides ABIs (application binary interfaces) which supports inserting, uploading and revoking of public keys with respect to the vehicles [55].

Aiqing Zhang and Xiadong Lin, in 2018 has made a review on critical issues that persists in the existing EHRs and analyzed that in the recent years blockchain has provided quite promising solutions in this field of health-care to achieve privacy of patient data sharing on the network. The authors proposed a framework based on blockchain for preserving privacy while diagnosis of a patient. Two blockchains were used namely, private and consortium blockchain; the private blockchain is used to store the actual PHI (personal health information) of the patient which is encrypted while consortium blockchain keeps the records of the PHIs indexes. The BSPP (blockchain-based secure and privacy-preserving PHI) protocol was implemented on JUICE and the performance of the architecture is evaluated in terms of privacy and security [56].

Mengmeng Yang et al., in 2018 conducted a survey in the field of IoT applications that is crowdsensing. The crowdsensing is a technique which enables the people with mobile devices to travel to specific locations and collect data to submit it back to the requesters and earn reward in return. The authors analyzed that the existing system suffers with a problem of privacy infringement and therefore, proposed a novel solution based on blockchain to address the privacy issues. The framework is designed in such a way that it overcomes the problem that is caused by the transparency property of blockchain that is user's real identity cannot be disclosed by linking to his payment transactional history. Moreover, the system also facilitates the location privacy to the workers in the crowdsensing system without the involvement of any third party. To implement the proposed architecture the authors used a combination of public and private blockchain in their model [57].

Yiming Wu et al., in 2019 has identified that task matching is a very critical issue in crowdsensing application of IoT. Thus, they proposed a blockchain-based privacy-preserving task matching (BPTM) system to resolve the privacy and reliability related issues in the existing solutions. The authors highlighted that identity anonymity is a very sensitive issue in crowdsensing application; therefore, it is to be handle with care, otherwise, in case if the workers identity is disclosed and distributed publically then it may lead to many malicious things. A searchable encryption technique is used to achieve the privacy-preserving in task matching to protect requirements of the task and preferences of the worker's. Also, the concept of encrypted index is used to provide matching services. The combination of smart contract with searchable encryption guarantees the identity anonymity and reliability of the system without any involvement of third party [58].

Chao Lin et al., in 2020 have proposed a blockchain-based conditional privacy-preserving authentication (BCPPA) protocol for VANETs. The authors shed light on the drawbacks on the existing solutions based on blockchain, PKI (private key integration) protocols, or ID-based protocols. The authors stated that somehow or the other these protocols lacks in guarantying the privacy such as key/certificate preloading and revocation, intraceability or frequent interactions in the VANETs. Therefore, the authors designed a novel framework by combining blockchain and PKI-based technique to address the mentioned challenges. Moreover, the framework also resolves the escrow problem and provides periodically updated private information which means it works well with realistic on-board units (OBUs) [59].

Webin Jhang et al., in 2018 have built up a naïve blockchain-based voting protocol which not only preserves end-to-end privacy in the system but also provides mechanism for detectability and correctability against cheating. The authors conducted a research on existing online platforms for voting that are centralized and even those which are based on blockchain suffers from certain confidentiality and privacy breach issues. Therefore, they designed a new receipt-free, easily verifiable and privacy-preserving peer voting protocol that helps the existing peer on the networks to vote without any interference of third-party for identifying the voters or tallying the votes [60].

Wenbo Jiang et al., in 2019 have discussed the privacy and security problems that currently exist in various public key infrastructures (PKI) IoT applications based on centralized networks such as single point of failure, privacy breach and so on. The authors also studied the various blockchain-based solutions which are decentralized in nature and have desirable properties such as cryptography, immutable records, etc. are proved to be a great solution for developing blockchain-based PKIs which are well suitable for many IoT applications but it does not behave well in handling thin-clients. The thin-clients are those who have limited storage on their device and hence cannot keep a copy of complete database. To deal with this problem a naïve framework is designed known as privacy-preserving thin-client authentication scheme (PTAS) based on blockchain in collaboration with private information retrieval (PIR) protocols. It will allow the thin-clients to act normally as full nodes and identity of the user that who is authenticating with the thin-client will be hidden among k indistinguishable identities because of PIR technique [61].

Ashutosh Dhar Dwivedi et al., in 2019 has discussed the shortcomings in the field of maintain health-care records over internet. The authors studied the existing techniques such as RPM (remote patient monitoring) and many other based on IoT and blockchain; but they stated that each of these suffers from certain privacy issues in one way or the other. Moreover, the authors also highlighted that implementing the blockchain in its actual could be disadvantageous as it demands high computational cost, high bandwidth and large computational power; thus, are not suitable for most resource-constrained IoT devices. To resolve these issues, the authors come up with a novel framework which works on the concept of modified blockchain in which they have eliminated the concept of PoW making it suitable for IoT devices. They used a combination of light-weight digital signature which provides tamper-proofing of the documents, ring signature which allows a signer to sign a message anonymously making it impossible for others to guess who has signed the message except the actual signer and lastly the concept of double encryption of data using lightweight encryption and public encryption schemes. Using these techniques together the author's guarantees the privacy and anonymity of user's data in small IoT devices for health-care [62].

The Table 5 below describes the various strategies that are provided by different authors to preserve privacy in blockchain network.

Table 5: Privacy preserving strategies for Blockchain

Ref-no	Year	Framework/ Architecture	Privacy Parameter	Application area
55	2019	BPAS	Unlinkability, Traceability and identifiability	VANETS
56	2018	BSPP	Anonymity and identifiability	Healthcare
57	2018	Blockchain-based privacy preserving crowdsensing system	Anonymity, Unlinkability, and Transparency	Crowdsensing
58	2019	BPTM	Identity anonymity , Unlinkability, and User privacy	Crowdsensing
59	2020	BCPPA	Unlinkability and 51 percent attack	VANETS
60	2018	Blockchain-based privacy preserving voting framework	Privacy to voter, detection and correction against cheating	Online Voting
61	2019	PTAS	Privacy to user and data	Thin-clients

62	2018	Cluster-based blockchain	Anonymity of user data	Healthcare

3.7. Privacy Information Retrieval

In cryptography, private information retrieval (PIR) is a protocol that allows a user to retrieve an ith bit of the information from the n bit database server without revealing which data is retrieved. This can be done in two ways, first by using information-theoretic PIR and second, by using computational PIR.

Information-theoretic PIR based on replication of server allows the user to access the complete database to fetch the queried information which not only helps in leaking the other information to the user rather also reduces the communication efficiency between the client and the server.

On the other hand, computational PIR based on the single server uses cryptographic algorithms to maintain the privacy of the data needed by the client while communicating with a server which leads to computational overhead. Therefore, a survey has been done which discusses the various ways of assuring the privacy of data using PIR schemes.

Ali khoshgozara et al., in 2009 has discussed all the existing solutions to maintain the privacy of location using PIR schemes and proposed a new technique that is best among all to guarantee the location privacy of the user. The authors developed a scalable private information retrieval information approach to location privacy known as SPIRAL. It overcomes the issue that exists in previously existing techniques that blur the user's location when the spatial distance is extended and also suffers from revealing the user's identity to others in the nearby region. The SPIRAL assures privacy which is invariant to the total number of users, size of the enclosed region, and querying pattern of the user. It provides a blind evaluation of the queries in the range [63].

Wesam Al Amiri et al., in 2019 has proposed a system for smart parking for drivers in crowded cities where parking is a major issue because of traffic congestion and air pollution. In contrast to the existing systems, he built a system using the concept of consortium blockchain in conjunction with PIR. It allows the driver to search for the nearest available parking lot which is provided by the blockchain and without sharing his location with anyone which is provided by PIR. He implemented his work using a python charm cryptographic library that runs on Raspberry Pi 3 devices. Moreover, his work was also financially supported by a central body known as NSF grant [64].

Li weng et al., in 2015 proposed a new PCBIR protocol over existing schemes for protecting privacy in large content-based information systems. The author designed a framework that provides a double layer of protection. Firstly, it uses robust has values for queries which prevent from disclosing original content and features. Second, the client can further reduce some bits to increase the ambiguity in the server which makes it difficult to understand by the server what kind of information the client wants. The authors tested the proposed work on different sizes of the dataset and experimented with it on Matlab and get the desired results which proved that the system can be used for any CBIR system. The author also proposed a k diversity privacy-preserving scheme for the system under which a device can make a policy depending upon its capability because a stronger policy will not only increase the load on the server rather it will also increase the cost of bandwidth and data processing. This is very useful for heterogeneous systems [65].

Razane Tajeddine et al., in 2017 have studied all the techniques suitable for colluded databases and find out certain problems such as download cost, the capacity of a query, and so on. Thus, the author comes up with a naïve solution that employs an extended t-PIR scheme for a minimal of t server may collude, for any given pattern of the query. The author experimented with some special collusion patterns and proves that the retrieval rate is significantly high. The proposed work of coded data with arbitrary collusion pattern works well when the size of t (a subset of the server) is less [66].

Karam Banawan et al., in 2019 has discussed the problem regarding PIR through wiretaps and provided a better solution that provides both security and privacy to the user trying to retrieve the information. The authors designed an algorithm based on the asymmetric key generation which maximizes the retrieval rate and also helps the client to retrieve the mth message privately from the N copies of the database without leaking any information to the eavesdropper in the communication channel. It focuses on the two major problems of the PIR, first is to protect the identity of the desired data from the public databases and second is protecting the requested message from the external eavesdrop(wiretap) observing the communication. In this paper, to overcome the problem mentioned above the authors implemented the secrecy constraint in conjunction with the usual privacy constraint in which a secret key is generated for each database with the artificial noise vector using an MDS code [67].

Iordanis Kerenidis et al., in 2004 developed a Quantum symmetric privacy information retrieval (QSPIR) in comparison to the previously existing PIR and SPIR schemes for protecting the privacy of data as well as the user without shared randomness among the servers which is not possible in any of the existing SPIR models. The different datasets are tried and tested by the authors to prove that QPIR requires less communication than the best known classical PIR schemes. A review is made by the authors on the existing SPIR models in the quantum world, where users and servers have quantum computers and can communicate qubits to retrieve information [68].

Terence H. Chan et al., in 2015 proposed a new PIR scheme for coded data storage on the servers over the existing schemes which are based on uncoded data storage. The author experiments with his proposed work using MDS codes for storing the data and guarantees the error-free and private retrieval of information to the user. The author also shows in his results that the coded PIR technique provides the optimal trade-off between retrieval cost and storage cost in comparison to the existing schemes which does not give the best results when the data size is large [69].

Hsuan-Yin Lin et al., in 2019 have studied the trade-offs that can be achieved if some information leakage is allowed as demanded by the user while retrieving data from the server using PIR protocols. HE named his work as weakly-private information retrieval (WPIR) as it allows to leak some identity of the data being retrieved as asked by the client and also compares the other two parameters that are upload cost and access complexity with the existing PIR schemes. To achieve WPIR the author partitioned the complete database into n equal parts and allowed leakage of particular part on demand. Under WPIR the authors proposed two schemes; first, one assures the minimum upload and downloads cost of the data, and another works upon privacy factor. The authors' work has proved that relaxing the perfect privacy factor not only improves the download and upload cost but also gives a higher access rate [70].

Kaihua Qin et al., in 2019 have worked upon the privacy of lightweight bitcoin transactions and came up with the drawback that a large bandwidth is required if privacy is to be assured using simple payment verification (SPV) protocol. Moreover, if bloom filters are used for the transaction then privacy cannot be guaranteed. Thus, the authors come up with a naïve solution in which they have used SPV protocol in conjunction with the PIR scheme which not only reduces the bandwidth rather it also decreased the latency factor and guarantees privacy to the user [71].

Jayneel Vora et al., in 2018 have put a limelight on the issues in the existing electronic health records (EHRs) and proposed a blockchain-based framework for Securing Electronic Health Records known as BHEEM. The existing EHRs schemes are unable to guarantee security to the patient's data and these are unable to maintain the balance between providing data to patients, providers, and third-party access. Therefore, the author introduced a new concept of BHEEM which overcomes the existing issues and also helps in maintaining the security and privacy of EHRs. Moreover, the authors have shown that the framework is highly scalable [72].

Table 6 describes the research gap in the field of maintaining privacy of data using PIR.

Table 6: Privacy Information Retrieval

Ref-no.	Year	Architecture/ Framework	Privacy Parameter	Blockchain type	Research gap
63	2009	Scalable PIR for location privacy	Anonymity	NA	Not suitable for large subset of database server
64	2019	Blockchain based PIR	Anonymity and unlinkability	Consortium blockchain	Not feasible for mobile application
65	2015	Robust hash algorithm for preserving content-based privacy	Privacy of person and data	NA	Does not work if client and server has different architecture
66	2017	PIR scheme on coded data for arbitrary collusion patterns	Privacy of data	NA	Not suitable when colluding sets are large in number
67	2019	PIR through wiretap channel II	Identifiability and unlinkability	NA	Can be experimented further in the presence of Byzantine adversaries
68	2004	Quantum computing to maintain PIR	Privacy of person and data	NA	Communication complexity needs to be improved
69	2015	PIR scheme for coded data	Privacy of data	NA	Work well for fixed storage size

70	2019	Weakly PIR	Information leakage	NA	Privacy of data is compromised
71	2019	SPV based PIR protocol for lightweight Bitcoin	Privacy of user	Public/ permission-less blockchain	Downloading bandwidth can be improved further
72	2018	Blockchain based framework for EHRs	Identifiability and unlinkability	Private/ prmissioned blockchain	More execution time and large computational power

4. Open Research Problem

The main objective of this paper is to study the existing PIR and blockchain schemes that are used by many researchers to guarantee privacy in different domains over the internet and highlight the gaps in the literature work. After reviewing all the above-mentioned papers it has been observed that PIR is of two types, namely, information-theoretic PIR and computational PIR. Both types have their pros and cons, so it completely depends on the user which type of PIR he wants to depend upon the nature of the information. Moreover, it is also analyzed that if blockchain and PIR if applied together than privacy of data and user can be handled in a more convenient manner.

From the review made in section III, we have observed some open research opportunities in the direction of blockchain privacy and PIR.

1. Though the blockchain networks have gained popularity in different domains over internet but it still faces some challenges because of it open to all and transparent feature.
2. The problem of linkability of transactional data which may help a dishonest node to use it for its own benefits.
3. Also in case of public blockchain the anonymity of peers could also be disadvantageous and may lead to malicious attacks.
4. The problem in retrieving data if a subset of the database server is large in number because it leads to complex computation as the data being queried has to be searched on more than one database server.
5. Downloading bandwidth is low in most of the solutions that are only based upon informational PIR because it sends a copy of the entire database to the client when a request is made by him.
6. Computational cost is higher because in the case of computational PIR many complex algorithms are used which increases the transaction's complexity rate with a polynomial value.
7. Storage or caching of data is a big issue because upon requesting the ith bit from the database the whole database is sent to maintain the privacy of data.
8. More execution time is needed for computation in the case of computational PIR which increases the access time cost.
9. In many PIR models, adversaries may attack while communication is done because it mainly focuses on protecting the privacy of data.

It has been observed that both blockchain and PIR are applicable individually for different applications to maintain privacy in their ways but, they still face certain challenges despite having various advantages and their unique features. The diagram below in Figure 4 highlights the major characteristics of blockchain and PIR and also focus on common features that could be advantageous to guarantee privacy in various applications. Moreover, in case of cross chains when multiple blockchains integrate to provide interoperability the privacy concerns are also high. For example, if a blockchain application is developed to trace the supply of vaccinations in countries and another blockchain is introduced to collect the COVID patients and their vaccination process and they are connected, in that case the privacy levels are also different and PIR can help in processing the information.

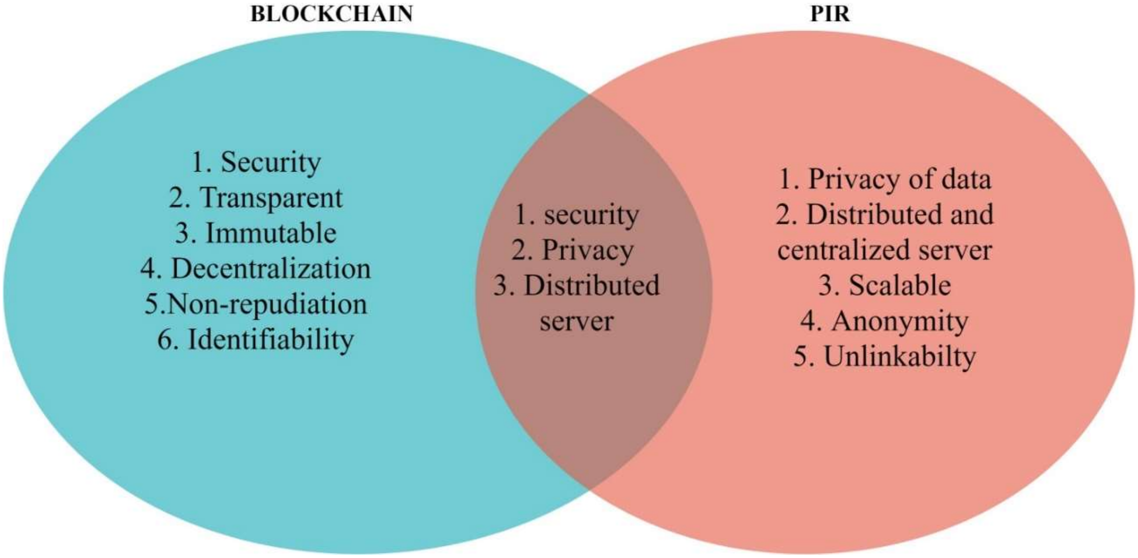

Figure 4: Blockchain and PIR

To tackle all the above-mentioned issues it is advisable to use blockchain in conjunction with PIR to assure privacy and security in various domains applicable to all decentralized and distributed system based applications of IoT, SCM, healthcare, finance, e-commerce, etc. It is a fact that both blockchain and PIR schemes have their advantages and disadvantages but if these two are implemented together can bring a major change in the history of technological advancement. For instance, their merger can lead to the development of a prototype which supports non anonymous user to make unlinked transactions providing privacy to both user's identity and the information being shared or retrieved. And to prove this, the results of this new prototype can be compared with the existing blockchain-based protocols.

5. Conclusion

In this paper, we have discussed privacy in different aspects specifically concerning blockchain and PIR. Blockchains are the main focus in this survey where we review the various blockchain applications that deal with different privacy parameters. Moreover, we also discuss the PIR concept and review the existing literature based on the same. The main idea behind this survey is to focus on the collaboration aspect of blockchains and PIRs as they are two different parts; however, they both are having the potentials to be conjugated. The research problems identified during the study opens up various important directions of blockchains and PIR handshaking.

6. Acknowledgement

I would like to thank Dr. Rahul Saha, Gulshan Kumar and Tai Hun Kim for their expertise and assistance throughout all aspects of our study and for their help in writing the manuscript.

7. References

[1] C. Komalavalli, Deepika Saxena, Chetna Laroiya, Chapter 14 - Overview of Blockchain Technology Concepts, Editor(s): Saravanan Krishnan, Valentina E. Balas, E. Golden Julie, Y. Harold Robinson, S. Balaji, Raghvendra Kumar, Handbook of Research on Blockchain Technology, Academic Press, 2020, Pages 349-371, ISBN 9780128198162, https://doi.org/10.1016/B978-0-12-819816-2.00014-9.

[2] Khan, M.A., Salah, K.: IoT security: review, blockchain solutions, and open challenges. Futur. Gener. Comput. Syst. 82, 395–411 (2018).

[3] Banafa, A.: IoT and blockchain convergence: benefits and challenges. IEEE Internet of Things (2017)

[4] R. Chatterjee and R. Chatterjee, "An Overview of the Emerging Technology: Blockchain," 2017 3rd International Conference on Computational Intelligence and Networks (CINE), Odisha, 2017, pp. 126-127, doi: 10.1109/CINE.2017.33.

[5] C. Komalavalli, Deepika Saxena, Chetna Laroiya,Chapter 14 - Overview of Blockchain Technology Concepts, Editor(s): Saravanan Krishnan, Valentina E. Balas, E. Golden Julie, Y. Harold Robinson, S. Balaji, Raghvendra Kumar, Handbook of Research on Blockchain Technology,,2020,Pages 349-371, ISBN 9780128198162, https://doi.org/10.1016/B978-0-12-819816-2.00014-9.

[6] Hong Su, Bing Guo, Yan Shen, Tao Li, Strongly Connected Topology Model and Confirmation-based Propagation Method for Cross-chain Interaction, available at: https://arxiv.org/pdf/2102.09237.pdf.

[7] L. Cao and B. Song, Blockchain cross-chain protocol and platform research and development, 2021 International Conference on Electronics, Circuits and Information Engineering (ECIE), 2021, pp. 264-269.

[8] N. Shadab, F. Houshmand and M. Lesani, Cross-chain Transactions, 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2020, pp. 1-9.

[9] S. Lin, Y. Kong and S. Nie, Overview of Block Chain Cross Chain Technology, 2021 13th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), 2021, pp. 357-360.

[10] Soravis Srinawakoon, Ripple-Backed Cross-Chain DeFi Platform Kava Integrates Band Protocol for Decentralized Oracle Support, available at: https://medium.com/bandprotocol/ripple-backed-cross-chain-defi-platform-kava-integrates-band-protocol-for-decentralized-oracle-2b29a7b50ae5.

[11] Gavin Wood, Polkadot: Vision for a Heterogeneous Multi-chain Framework, available at: https://polkadot.network/PolkaDotPaper.pdf, accessed on: 01-01-2021.

[12] Arlyn Culwick, Dan Metcalf, The Blocknet Design Specification, available at: https://blocknet.co/whitepaper/Blocknet_Whitepaper.pdf, accessed on: 01-01-2021.

[13] Aion: The Open Application Network, available at: https://aion.theoan.com/\#whitepapers, accessed on: 01-01-2021.

[14] A SURVEY ON SECURITY AND PRIVACY ISSUES OF BLOCKCHAIN TECHNOLOGY Archana Prashanth Joshi, Meng Han and Yan Wang Kennesaw State University, Marietta, GA 30060, USA doi:10.3934/mfc.2018007 Volume 1, Number 2, May 2018 pp. 121-147.

[15] 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 Software Architecture (ICSA), 2017 IEEE International Conference on, IEEE, 2017, 243252.

[16] Zheng, Z., Xie, S., Dai, H-N., Chen, X. and Wang, H. (2018) ‘Blockchain challenges and opportunities: a survey’,Int. J. Web and Grid Services, Vol. 14, No. 4, pp.352–375. [8] The meaning and value of privacy Daniel J. Solove.

[17] Dawood, Hamza S.. "Book Notes: Understanding Privacy, by Daniel J. Solove." Osgoode Hall Law Journal 47.4 (2009) : 819-820. http://digitalcommons.osgoode.yorku.ca/ohlj/vol47/iss4/8.

[18] Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management–A Consolidated Proposal for Terminology January 2007 Andreas Pfitzmann.

[19] A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity ManagementJanuary 2010A Pfitzmann.

[20] https://www.imperva.com/learn/data-security/data-privacy

[21] Information Fusion Volume 13, Issue 4, October 2012, Pages 235-244 Information fusion in data privacy: A survey GuillermoNavarro-ArribasaVicençTorra

[22] Schott, P.A., 2006. Reference Guide to Anti-money Laundering and Combating the Financing of Terrorism. World Bank Publications. Send shared. https://blockchain.info/de/wallet/send-shared. J. Siim, "Proof-of-stake".

[23] Gill, M., Taylor, G., 2004. Preventing money laundering or obstructing business? financial companies' perspectives on know your customerprocedures. Br. J. Criminol. 44 (4), 582–594.

[24] J.R. Douceur, The Sybil Attack in International Workshop on Peer-to-Peer Systems, Springer, 2002, pp. 251–260.

[25] G. Danezis, Statistical disclosure attacks, in: IFIP International Information Security Conference, Springer, 2003, pp. 421–426.

[26] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in bitcoin," in International Conference on Financial Cryptography and Data Security, pp. 34–51, Springer, 2013.

[27] M. Vasek, M. Thornton, and T. Moore, "Empirical analysis of denialof- service attacks in the Bitcoin ecosystem," in International conference on financial cryptography and data security. Springer, Berlin, Heidelberg, 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 International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2014, pp. 72-86.

[29] Gwyneth Iredaleon, History Of Blockchain Technology: A Detailed Guide, available at: https://101blockchains.com/history-of-blockchain-timeline/, accessed on: Jan, 2021.

[30] G. Wood, Ethereum: A secure decentralised generalised transaction ledger, Ethereum Project Yellow Paper, 151, 2014, 1-32.

[31] L. A. Linn and M. B. Koo, Blockchain for health data and its potential use in health it and health care related research, in ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST, 2016.

[32] F. Chen, P. Deng, J. Wan, D. Zhang, A. V. Vasilakos and X. Rong, Data mining for the internet of things: Literature review and challenges, International Journal of Distributed Sensor Networks, 11 (2015), 431047.

[33] A. Dorri, S. S. Kanhere and R. Jurdak, Blockchain in internet of things: challenges and solutions, arXiv preprint, arXiv:1608.05187.

[34] Guo and Liang Financial Innovation (2016) 2:24 DOI 10.1186/s40854-016-0034-9, Blockchain application and outlook in the banking industry.

[35] https://equensworldline.com/en/home/blog/2017/may-17/20170519-blockchain-will-lead-the-revolution-in-the-banking-sector.html

[36] Blockchain – A Financial Technology For Future Sustainable Development Quoc Khanh Nguyen.

[37] X. Min, Q. Li, L. Liu and L. Cui, "A Permissioned Blockchain Framework for Supporting Instant Transaction and Dynamic Block Size," 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, 2016, pp. 90-96, doi: 10.1109/TrustCom.2016.0050.

[38] Xu Y., Li Q., Min X., Cui L., Xiao Z., Kong L. (2017) E-commerce Blockchain Consensus Mechanism for Supporting High-Throughput and Real-Time Transaction. In: Wang S., Zhou A. (eds) Collaborate Computing: Networking, Applications and Worksharing. CollaborateCom 2016. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 201. Springer, Cham

[39] Y. Chen, S. Chen and I. Lin, "Blockchain based smart contract for bidding system," 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, 2018, pp. 208-211, doi: 10.1109/ICASI.2018.8394569.

[40] 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," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4680-4693, June 2019, doi: 10.1109/JIOT.2018.2877634.

[41] Y. Jiang, C. Wang, Y. Wang and L. Gao, "A Privacy-Preserving E-Commerce System Based on the Blockchain Technology," 2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE), Hangzhou, China, 2019, pp. 50-55, doi: 10.1109/IWBOSE.2019.8666470.

[42] Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. J Med Syst. 2016;40(10):218. doi:10.1007/s10916-016-0574-6

[43] X. Liang, J. Zhao, S. Shetty, J. Liu and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, 2017, pp. 1-5, doi: 10.1109/PIMRC.2017.8292361

[44] C. Esposito, A. De Santis, G. Tortora, H. Chang and K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?," in IEEE Cloud Computing, vol. 5, no. 1, pp. 31-37, Jan./Feb. 2018, doi: 10.1109/MCC.2018.011791712.

[45] Feng Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," 2016 13th International Conference on Service Systems and Service Management (ICSSSM), Kunming, 2016, pp. 1-6, doi: 10.1109/ICSSSM.2016.7538424.

[46] M. P. Caro, M. S. Ali, M. Vecchio and R. Giaffreda, "Blockchain-based traceability in Agri-Food supply chain management: A practical implementation," 2018 IoT Vertical and Topical Summit on Agriculture - Tuscany (IOT Tuscany), Tuscany, 2018, pp. 1-4, doi: 10.1109/IOT-TUSCANY.2018.8373021.

[47] Madhwal, Yash \& Panfilov, Peter (2017). Blockchain And Supply Chain Management: Aircrafts' Parts' Business Case, Proceedings of the 28th DAAAM International Symposium, pp.1051-1056, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-11-2, ISSN 1726-9679, Vienna, Austria DOI: 10.2507/28th.daaam.proceedings.146

[48] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, 2017, pp. 618-623, doi: 10.1109/PERCOMW.2017.7917634.

[49] Ali Dorri, Salil S. Kanhere, Raja Jurdak, Praveen Gauravaram, LSB: A Lightweight Scalable Blockchain for IoT security and anonymity, Journal of Parallel and Distributed Computing, Volume 134, 2019, Pages 180-197, ISSN 0743-7315, https://doi.org/10.1016/j.jpdc.2019.08.005.

[50] Y. Rahulamathavan, R. C. -. Phan, M. Rajarajan, S. Misra and A. Kondoz, "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption," 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Bhubaneswar, 2017, pp. 1-6, doi: 10.1109/ANTS.2017.8384164.

[51] L. Zhou, L. Wang, Y. Sun and P. Lv, "BeeKeeper: A Blockchain-Based IoT System With Secure Storage and Homomorphic Computation," in IEEE Access, vol. 6, pp. 43472-43488, 2018, doi: 10.1109/ACCESS.2018.2847632.

[52] 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," in IEEE Access, vol. 7, pp. 18611-18621, 2019, doi: 10.1109/ACCESS.2019.2896065.

[53] Ourad A.Z., Belgacem B., Salah K. (2018) Using Blockchain for IOT Access Control and Authentication Management. In: Georgakopoulos D., Zhang LJ. (eds) Internet of Things – ICIOT

2018. ICIOT 2018. Lecture Notes in Computer Science, vol 10972. Springer, Cham. https://doi.org/10.1007/978-3-319-94370-1_11

[54] N. Tapas, G. Merlino and F. Longo, "Blockchain-Based IoT-Cloud Authorization and Delegation," 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina, 2018, pp. 411-416, doi: 10.1109/SMARTCOMP.2018.00038.

[55] Q. Feng, D. He, S. Zeadally and K. Liang, "BPAS: Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular Ad Hoc Networks," in IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4146-4155, June 2020, doi: 10.1109/TII.2019.2948053.

[56] Zhang, A., Lin, X. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. J Med Syst 42, 140 (2018). https://doi.org/10.1007/s10916-018-0995-5

[57] Mengmeng Yang, Tianqing Zhu, Kaitai Liang, Wanlei Zhou, Robert H. Deng, A blockchain-based location privacy-preserving crowdsensing system, Future Generation Computer Systems, Volume 94, 2019, Pages 408-418, ISSN 0167-739X, https://doi.org/10.1016/j.future.2018.11.046.

[58] Y. Wu, S. Tang, B. Zhao and Z. Peng, "BPTM: Blockchain-Based Privacy-Preserving Task Matching in Crowdsourcing," in IEEE Access, vol. 7, pp. 45605-45617, 2019, doi: 10.1109/ACCESS.2019.2908265.

[59] 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," in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2020.3002096.

[60] W. Zhang et al., "A Privacy-Preserving Voting Protocol on Blockchain," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2018, pp. 401-408, doi: 10.1109/CLOUD.2018.00057.

[61] Wenbo Jiang, Hongwei Li, Guowen Xu, Mi Wen, Guishan Dong, Xiaodong Lin, PTAS: Privacy-preserving Thin-client Authentication Scheme in blockchain-based PKI, Future Generation Computer Systems, Volume 96, 2019, Pages 185-195, ISSN 0167-739X, https://doi.org/10.1016/j.future.2019.01.026.

[62] Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. Sensors 2019, 19, 326. https://doi.org/10.3390/s19020326

[63] A. Khoshgozaran, H. Shirani-Mehr and C. Shahabi, "SPIRAL: A Scalable Private Information Retrieval Approach to Location Privacy," 2008 Ninth International Conference on Mobile Data Management Workshops, MDMW, Beijing, 2008, pp. 55-62, doi: 10.1109/MDMW.2008.23.

[64] W. A. Amiri, M. Baza, K. Banawan, M. Mahmoud, W. Alasmary and K. Akkaya, "Privacy-Preserving Smart Parking System Using Blockchain and Private Information Retrieval," 2019 International Conference on Smart Applications, Communications and Networking (SmartNets), Sharm El Sheik, Egypt, 2019, pp. 1-6, doi: 10.1109/SmartNets48225.2019.9069783.

[65] L. Weng, L. Amsaleg, A. Morton and S. Marchand-Maillet, "A Privacy-Preserving Framework for Large-Scale Content-Based Information Retrieval," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, pp. 152-167, Jan. 2015, doi: 10.1109/TIFS.2014.2365998.

[66] 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," 2017 IEEE International Symposium on Information Theory (ISIT), Aachen, 2017, pp. 1908-1912, doi: 10.1109/ISIT.2017.8006861.

[67] K. Banawan and S. Ulukus, "Private Information Retrieval Through Wiretap Channel II: Privacy Meets Security," in IEEE Transactions on Information Theory, vol. 66, no. 7, pp. 4129-4149, July 2020, doi: 10.1109/TIT.2020.2977058.

[68] Iordanis Kerenidis, Ronald de Wolf, Quantum symmetrically-private information retrieval, Information Processing Letters, Volume 90, Issue 3, 2004, Pages 109-114, ISSN 0020-0190, https://doi.org/10.1016/j.ipl.2004.02.003.

[69] T. H. Chan, S. Ho and H. Yamamoto, "Private information retrieval for coded storage," 2015 IEEE International Symposium on Information Theory (ISIT), Hong Kong, 2015, pp. 2842-2846, doi: 10.1109/ISIT.2015.7282975.

[70] R. Zhou, T. Guo and C. Tian, "Weakly Private Information Retrieval Under the Maximal Leakage Metric," 2020 IEEE International Symposium on Information Theory (ISIT), Los Angeles, CA, USA, 2020, pp. 1089-1094, doi: 10.1109/ISIT44484.2020.9174334.

[71] K. Qin, H. Hadass, A. Gervais and J. Reardon, "Applying Private Information Retrieval to Lightweight Bitcoin Clients," 2019 Crypto Valley Conference on Blockchain Technology (CVCBT), Rotkreuz, Switzerland, 2019, pp. 60-72, doi: 10.1109/CVCBT.2019.00012.

[72] J. Vora et al., "BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records," 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 2018, pp. 1-6, doi: 10.1109/GLOCOMW.2018.8644088.