Sādhanā (2022)47:168
https://doi.org/10.1007/s12046-022-01931-1

Challenges in making blockchain privacy compliant for the digital world: some measures

SMITA BANSOD[1,*] and LATA RAGHA[2]

[1]Department of Information Technology, Faculty, Shah & Anchor Engineering College, Research Scholar, Terna Engineering College, Mumbai University, Mumbai, India
[2]Department of Computer Engineering, Father Conceicao Rodrigues Institute of Technology, Vashi, Mumbai, India
e-mail: sakec.smitab@gmail.com; lata.ragha@fcrit.ac.in

MS received 5 June 2021; revised 21 April 2022; accepted 1 June 2022

Abstract. Due to the pandemic, most of the personal transactions relating to finance, commerce and healthcare services have gone online making privacy preservation a critical requirement. Consequently, privacy has been made a critical parameter in Data Protection Regulations leading to the search for such a privacy compliant system which is also resilient to attacks. A detailed analysis of the Blockchain technology, which is becoming popular for secure applications in the finance sector, indicates that there are several challenges relating to user identity, transaction linkability, crypto-keys management, data privacy, usability, interoperability, and post- quantum compliance of privacy regulations which need to be resolved before its widespread adoption. Being a decentralised system, there is a need to analyse the vulnerability to attacks of each layer in the Blockchain architecture. This paper discusses the development flow of some of the privacy enhancement mechanisms like ZKPs, SMPC, Ring signatures, Mixing, Homomorphic Encryption and quantum resilient computing, bringing out their features and lacunae. There is a detailed discussion of the privacy mechanisms adopted by blockchain platforms like ZCash, Zerocoin, Hyperledger, Wanchain, Coin Party, Monero, Cryptomate, MixCoin, Coinshuffle, PICNIC and New Hope. Every platform has some limitation or the other and it is essential that researchers come out with mitigation steps for the existing mechanisms and come up with improved new Privacy Enhancement Techniques. One such architecture using PET has been proposed.

Keywords. Privacy; blockchain; zero knowledge proof; ring signature; multiparty computation; mixing; homomorphic encryption; quantum computing; PET.

1. Introduction

Covid-19 pandemic forced the accelerated digitalization of many sectors, with large-scale adoption of contactless solutions and virtual collaboration tools. Digital era demanded systems with high performance, scalability, efficiency, reliability, compactness, and most importantly security. Individuals and businesses went after several new technologies such as Cloud, Virtualization, Quantum Computing, Automation and Artificial Intelligence to select systems that will meet the needs of the environment created by the new norms like e-Government policies, rules, and regulations. The enormous increase in online interactions between governments, businesses and individual citizens demanded a high level of protection and privacy of all data used in these interactions. Protection is how well the data is secured against attacks once it has already been gathered and so becomes the responsibility of the data gatherer. Privacy is the ability to safeguard the interests of the users by defining the process to handle the personal information collected from them. Any relaxation of privacy will infringe on the rights of the users to ensure that their personal data will never be misused, thereby violating the requirements of the legal regulations.

Since data protection and privacy are critical elements of any online interaction, Blockchain technology is considered to have the features to revolutionize the online interactions by bringing in transparency across all the users by revamping currently existing processes and bringing in efficiency and adding value.

Blockchain allows the transfer of digital assets in a decentralized fashion without the need for third parties. In Blockchain technology transactions are publicly available for reading but none can modify the transaction, once it is recorded, making the data which enters the system safe and secure. But there are many questions relating to Data Privacy that need to be analysed, discussed, debated and researched in order to provide convincing solutions complying with the

*For correspondence
Published online: 18 August 2022

Data Protection Regulations so that Blockchain technology could fit in as the preferred system. This paper discusses the features of Blockchain technology with a focus on the different mechanisms as well as platforms that need to be studied further to find acceptable solutions to the privacy preservation and security attack issues.

2. Motivation and contribution

The draft Personal Data Protection bill [1] is under the consideration of the Parliament of India. The draft proposes to mandate strict privacy requirements for personal data in respect of digital applications.

The expert committee set up to review the provisions of the draft bill has recommended that the digital economy should aim to benefit the citizens by strengthening the privacy, safety and security aspects of all the digital transactions. The user is expected to make more privacy-conscious decisions keeping in mind the need for close control of the transactions. There is a growing demand that data privacy should be given the status of a fundamental human right.

On reviewing the latest literature, it is apparent that there are several gaps in the present privacy, safety and security aspects of blockchain applications. These have been listed, analysed and a suitable privacy enhanced architecture has been recommended in this paper.

3. Brief background

3.1 *Privacy preservation*

(1) Data Privacy Personal Identification Information (PII) of any person is considered as very sensitive and so the individual concerned should have the right to decide as to the persons or entities who will have access to that information [2]. Data privacy preservation is meant to provide this feature without any comprise. Privacy should be protected in the sense that the personal data and its flow should not be observed by anyone and the owner must have the exclusive right to give or withdraw permission to other trusted parties to view that data and not disclose it to others.

(2) Requirements Privacy protection should be the most important requirement in the digital era. While developing an application or adapting a new technology, it is essential to follow the law of the land. Any violation of Data Privacy resulting in the use of an application should lead to punitive action on the owner of the application. Sensitive applications, like User identity management (location related), Patients' data (health record, medicines, state of mind, physical condition, behaviour pattern), Financial data, Educational data or any Business data should have special data privacy protection.

(3) Privacy protection Regulations - the Indian Scene: There are various laws relating to data privacy applicable to different countries like the General Data Protection Regulation (GDPR) in Europe, Freedom of Information Act 2000 (FIA) in the United States of America, Data Protection Act 1998 (DPA) in the UK, Personal Information Protection Act (PIP) in South Korea and the Personal Data Protection Act 2012 (PDPA) in Malaysia.

In India, Data Privacy is presently governed by the rules under the Information Technology Act, 2000. With the intention of bringing about a comprehensive overhaul of the existing data privacy regime, the Government proposed the Personal Data Protection Bill [1] in the year 2019, which is currently being examined by the Joint Parliamentary Committee and is expected to be presented before the Parliament very soon. The bill's preamble recognizes the need to develop the digital economy and digital governance with adequate protection of privacy of individuals. It affirms that the "right to privacy is a fundamental right" and seeks to enforce the privacy preservation in respect of overseas corporates as well who wish to do business with India.

Broadly the Bill aims to (i) provide for protection of the privacy of individuals relating to their personal data, (ii) specify the flow and usage of personal data, (iii) create a relationship of trust between persons and entities processing the personal data, (iv) protect the fundamental rights of individuals whose personal data are processed, (v) create a framework for organizational and technical measures in the processing of data, (vi) lay down the norms for social media intermediary and cross-border data transfer, (vii) fix accountability of entities processing personal data, and (viii) propose remedies for unauthorized and harmful data processing. It is expected that the Data Protection Authority will oversee the implementation of the provision of the Bill.

3.2 *Why Blockchain*

The global trend is to look at Blockchain Technology as the most suited one for ensuring Data Security and Privacy. The adverse effects due to the attacks are minimized to a large extent by the use of Blockchain technology and modern applications like Cryptocurrency, Finance, Healthcare, e-Governance, and many more, which have adopted Blockchain technology are reporting good results.

4. Basic terminologies

4.1 *Data security*

There is a need to protect the application from unauthorized access due to hacking. There is a list of attacks, services and mechanisms which are related to Data privacy preservation [3]. Privacy is classified as Content Privacy and Contextual Privacy. Further Contextual privacy is categorized into Anonymity and Pseudonymity. Based on these categories, there are several possible attacks on privacy namely, Brute Force, Timing attack, Latency attack,

Predecessor attack, Packet counting attack, Profiling attack, Disclosure attack, Message Tagging, Sting attack, Send 'n' seek attack, Active attack exploiting user reactions, Denial of Service attack, Flooding attack, Flow Marking attack, Clogging Attack and so on.

4.2 *Blockchain basics*

Blockchain is a duplicated digital ledger which is shared among the peers with the unique feature of immutability. Further, the transactional records, called "blocks" or distributed as a "chain" among the peers. This technology is becoming popular because it increases the trust amongst the users leading to reduced cost.

In 2009, Santoshi Nakamoto introduced Blockchain technology with Bitcoin application [4] as a peer to peer electronic cash system. It became very attractive for real time applications as a secure system with immunity to third-party interference and as an example of an open, or permissionless blockchain.

Blockchain is neither restricted to the application of bitcoin or cryptocurrency as in phase 1 nor to Ethereum as in phase 2. Today, blockchain is in phase 3, where the development of various new applications are in progress in different areas like Government, IOT, Artificial Intelligence and so on.

4.3 *Blockchain network and block structure*

Distributed nodes are connected with each other to form a mesh network. Every node having the copy of all the transacted data is known as full node or mining node. Some nodes function only as user nodes without having a copy of all the transactions and blocks. Each of these nodes have validated blocks, each block built as two parts and all these connected to form a chain as shown in figure 1.

Block Header entails (i) BlockID: unique sequential number. (ii) Parent Block Hash value: First block value. (iii) Transaction hash: root node value of all transactions in that block using Merkle hashing method. (iv) Number of transactions in that block. (v) Timestamp: Validation time value. (vi) Nonce: Random number calculated for validation of the block. (vii) n: Number of initial zeros in hash value of validated block. Transactions List consists of number of transactions in that particular block.

New data entered in Blockchain can never be erased and can only be updated by consensus between the participants in the system. A verifiable record of every transaction is retained in the system [5]. A summary of the basic features of this technology is given as:

(1) Distributed Database With the distributed database, there is no need for any intermediary to verify the records by any user as the complete history is available.

(2) Mesh connected network Each peer can communicate with another peer directly and broadcast the information to all nodes.

(3) Transparency The unique alpha-numeric address identifies each user or node and transactions take place between these with pseudonymous addresses. This will ensure anonymity of users and transactions if required.

(4) Irreversibility of Records The algorithms deployed in this technology enable the system to store all entered data without any provision for deletion or manipulation. This ensures that transactions can be audited but cannot be altered.

(5) Operational Logic The distributed ledger facilitates the programming of the system by setting up operational algorithms and business rules automatically to initiate transactions.

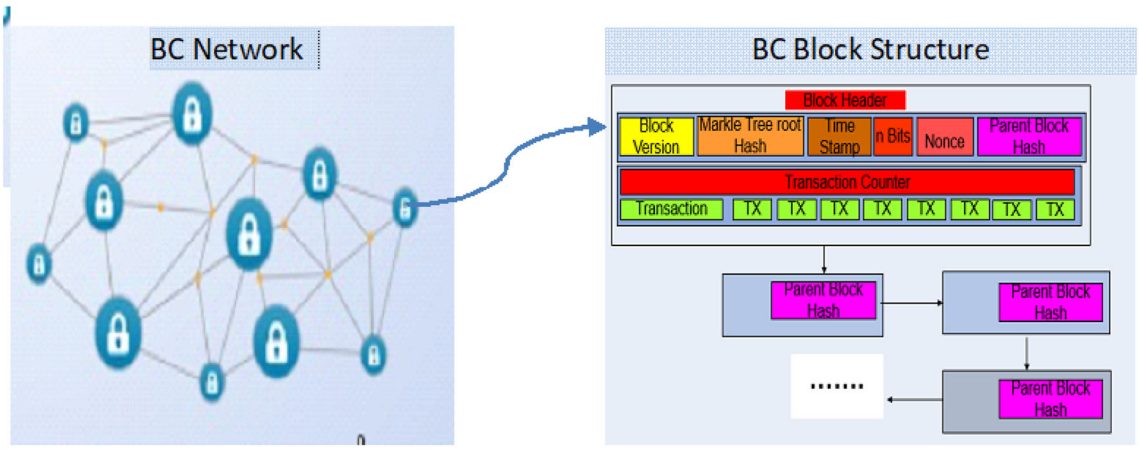

Figure 1. Blockchain network and block structure.

4.4 *Blockchain – not a panacea*

Notwithstanding all its merits, the Blockchain solutions are subject to certain limitations like scalability, response times, security threats and privacy issues which affect user identity, confidentiality and transparency on the ledger [6]. Further, Blockchain is not fully compliant with the GDPR. Attackers are known to track the record of transactions and succeed in tracing out the identity of transaction owner. Blockchain technology is vulnerable to other kinds of attacks, namely Cyber Crimes, Double spending, Privacy leakage in transaction, 51% attack on PoW, Private key security, Smart contract frauds, and Price manipulation operations [7].

Despite downsides, Blockchain technology presents some unique advantages which make this technology attractive for the digital era. Currently there is a lot of research and many experiments are under way in the area of Privacy preservation to find out situations where Blockchain technology adds the most value.

5. Issues in Blockchain relating to privacy preservation

The characteristics of Blockchain are decentralization, transparency, auditability, and persistency. The characteristics are attractive, but there are related side effects as mentioned in the paper [7]. Though there are various challenges, this paper discusses some of the issues connected with the privacy preservation and security attacks.

(a) Identification in a decentralized and persistent environment is a very difficult task. The security and risk management aspects need further study in Blockchain environment as suggested by NIST in white paper [8]. Fake identity, anonymous user and unauthorized entry may cause problems to identification of user and data. Hence if Blockchain-based identity is to become an ultimate architectural feature of tomorrow's web, then mitigation measures to overcome the risk of security and privacy are to be implemented.

(b) Transaction linkability and the related address tracing are generalized issues in Blockchain. Cryptocurrency has been suffering from analysis attack of wallet address, transaction coins and other related active attacks. Although Bitcoin is an old application, having been in use for over 11 years, these issues have not been fully resolved yet. Cryptocurrency applications ZCash and Monero are encountering attacks and are discovering the loopholes in the operations. It is found that in some cases the shielding address delinks the transparent address and also transparent address does not protect the value of transactions. Onion or Garlic cast routing is designed to be highly resistant to wide range of attacks while ensuring a high level of anonymity but these are still vulnerable to different types of attacks such as timing analysis.

(c) Key management or wallet management is another big challenge in Blockchain technology. Operations like generation of keys and exchange of keys are termed as Key management operations which has always been challenging for enterprises [9]. IT organizations face challenges like Scalability, Security and Availability when trying to control and manage the encryption keys. Mechanisms like the Public Key scheme [10] and the Ring Signature scheme [11] provide secure keys and mix them at random to provide anonymity to the user. Tricks like change of address by the user are also risky. There are chances that the transaction owner will be identified. In the process of managing the key, if the user forgets the key used, then Data recovery becomes a major issue. Even renowned applications like uPort have not yet resolved the challenges relating to the recovery of lost or stolen keys. The various issues related to different Key management methods and Recovery schemes are discussed in paper [12].

(d) Data privacy One of the features of Blockchain is permanency of all information entered into the systems. Manipulation of data is impossible in the distributed network as the validity is frequently verified. But Data Protection Regulation mandates that every user must have the right to erasure and the right to be forgotten. Everyone must have the right to be deleted from publicly accessible registers, databases, and so on. While persistency is considered as a security feature, Data Protection Laws look at this feature as an intrusion on privacy and user rights. However, papers [13, 14] discuss the feature of deleting data of a public-private Blockchain. On-chain data deletion is a complex task but off-chain data deletion can be relatively secure. Data privacy on network and storage need special attention. Data privacy should be protected in social media as well as other forms while using different data mining or big data analytics algorithms [15] .

(e) Usability A number of applications in several areas like e-Governance, Healthcare and Finance are being developed by adapting Blockchain technology [16]. The Blockchain technology is highly complex with different stakeholders for each application. While developers focus on the usability of the applications, the requirements of privacy should not be compromised. Applications like Smart Contracts are increasingly adopting Blockchain technology because it simplifies business and trade between both anonymous and identified parties, without compromising on authenticity and credibility. It is a challenging task to develop user friendly application modules while preserving privacy.

(f) Interoperability Any system for the future should be user friendly and capable of seamlessly operating with other systems which are already in operation with various applications as shown in figure 2. There should be no need for the already existing systems to shut down temporarily to install conversion interfaces for interoperability. Researchers are working on the interoperability issues of the different applications in a complex Blockchain

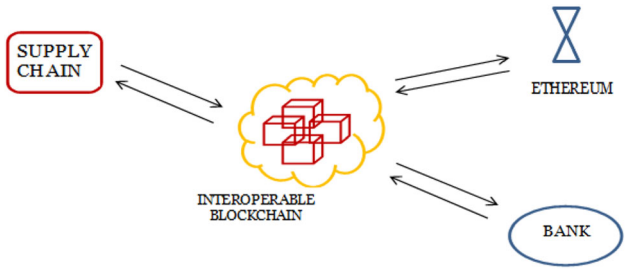

Figure 2. Example of interoperability.

environment, merging different modules using different Smart Contracts, Programming Languages and different platforms without data leaks. This is a challenging task for even experienced software engineers.

(g) Quantum Computing This is an upcoming field of research that uses quantum mechanics so that certain kinds of computations are performed more efficiently and much faster than a regular computer. It is feared that such computers pose a threat to the existing cyber security infrastructure. In particular, the quantum computer will destroy some of the cryptographic principles behind the Blockchain technology [17].

In traditional cryptography algorithms are generated to function as public and private keys to ensure authorized access. These two keys are governed by a complex mathematical relationship which is very difficult to hack with normal computational methods in real time. However, there is the possibility that the much faster quantum computers could be used to break the cryptographic keys. Such an attack is much worse than forging keys because this will affect the entire system. The algorithm proposed by Peter Shor has already threatened the hacking of asymmetric cryptography using a quantum computer. Another threat to hash value cryptography is the Grover's algorithm.

Research work on post quantum cryptography has come up with algorithms resistant to hacking using quantum computers. Tangle or Wanchain platforms are reported to produce crypto-algorithms resistant to quantum computing. Quantum resistant cryptography or Post Quantum Cryptography is an area that requires continuous research to remain ahead of the attackers.

(h) Compliance It may be seen from the above discussion that several features of Blockchain, which are termed as advantages of the technology, are known to be non-compliant with the provisions of the Personal Privacy Protection regulations. The rules and regulations [18] are quite firm on the rights of the user to be forgotten, privacy preservation, right to portability, conditions for consent and data protection.

6. Blockchain security

Although, Blockchain is becoming popular because of its novel features, being a distributed system with decentralized control, there is a need for careful scrutiny of the critical security aspects and authentication mechanisms Such a security analysis requires to be done at each layer of the Blockchain architecture. Unfortunately, there is no standardised model architecture, although many authors have discussed three, four or five layered network structure for Blockchain. The paper [19] mentions a four layered structure namely network, consensus, replicated state machine/ transaction and application layers with details of attacks and risk assessments of the model. However, the countermeasures discussed in the paper are not very effective. The other paper [20] has proposed an architecture with data layer, control layer and other layers as per the requirements of the OSI model. Literature reveals the various surface attacks on Blockchain with real time examples. The security analysis of each layer is discussed in the paragraphs below.

The Data layer in the Blockchain database holds the transaction data, hash values and wallet information in a distributed manner. The attacks on Block Data cited in the paper [21] are Malicious information attacks. Malicious information is written in the form of virus signatures, politically sensitive topics, and many more in the Blockchain database. The characteristic of persistency prevents the deletion of such malicious data from Blockchain once it is written in. It is believed that approximately 60 files contain illegal data on bitcoin Blockchain. While the application of signature and encryption methods as well as redactable Blockchain [22] algorithms like Chameleon hash functions could be applied to mitigate the adverse effects to some extent, there are chances that inappropriate content will remain in the layer and expose the users to risk.

The Network layer is the layer which is most vulnerable to attacks. Both, the Blockchain networks - the Private network and the Public network - have their own strengths and weaknesses. While access control, authorization and availability (in single network) are the strong points of the private network, its major weakness happens to be the interconnectivity issue. On the contrary, features like decentralization, availability, openness and low entry barrier are the strengths of the Public network while issues like authentication, efficiency and vulnerability to various attacks, are its weaknesses. Cybercriminals look for network vulnerabilities and exploit them with attacks like Man in middle (MIM), DNS, BGP hijacks, Spatial partitioning, Eclipse, Routing, Denial of Service on connectivity as well as local resources and Sybil. While validating the blocks, the Blockchain network generates the fork due to misalignment of different miners, which metamorphoses into Stale Blocks or Orphaned Blocks leading to Sybil or

selfish mining attacks by assigning several identifiers to the same node.

Consensus layer is the most important layer which validates the blocks through miners. Each new block added to the network should have the consensus agreement of all nodes in a distributed network. This function is achieved by the appropriate consensus algorithm for each application. The Permissionless blockchain makes use of consensus algorithms like PoW (Proof of Work), PoS (Proof of Stack), PoR (Proof of Reputation) and PoA (Proof of Authority). The Permissioned consensus protocols use Byzantine Fault Tolerant (BFT), PBET (Practical BFT) and Raft algorithms. The Consensus Layer protocols are vulnerable to generalized attacks like Majority attack or 51% attack, Double-spending attack, Finney attack, Time-Validation Attack, Block Withholding Attack by (selfish miner to create double spending attack), Classical block withholding attack to harm pool operator in PoW, Pool Specific Attack, Memory Pool (mempool) attack, Consensus delay attack, Timejacking Attack, Time validation attack, and Counter block withholding attack [19, 23]. Consensus Layer protocols are application based. For example, multiple BFT protocols are designed for the Consensus Layer to securely tolerate an optimal number of faults under different network settings. But each one of these protocols has some security loophole or the other, making it vulnerable to attacks like Feather Forking attack, Pool Specific Attack, Nothing-at-Stake attack, Grinding Attack, DOS on a Leader/Committee and Long-Range Attack/Stack bleeding attack.

Replicated State Machine Layer or Transaction layer is vulnerable to user identity, transaction data confidentiality, integrity, authentication, availability threats and related attacks. In addition, Smart-contract oriented bugs [7, 24] like Lack of privacy, Re-entrancy, Gasless send, Exception Syndrome, Programming, Stack overflow, Out of gas exception, Call to Unknown, Immutability, Rigorous and robust Compilation, also exist as vulnerabilities. The two languages used in Smart contracts are vulnerable to separate attacks. Turing-Complete Languages like Serpent and Solidity which provide arbitrary programming logic led to large surface attacks while Turing-Incomplete Languages like Pact and Scilla are designed with an emphasis on safety at the cost of expressiveness.

Application Layer threats are oriented to definite applications and are directly related to user interface. The well-known attack on Tokyo based MT GOX forced the exchange to file for bankruptcy in 2013 after hackers had

Table 1. Blockchain layers, vulnerability surfaces and related attacks.

Layers	Major surface	Attacks
Data layer	Transaction data, hash values and wallet information	Malicious use and insertion of illegal data
Network layer	Interconnectivity, authentication	Man In middle, DNS, BGP hijacks and spatial partitioning, Eclipse, Routing, DOS attacks on connectivity as well as local resources, Identity revealing attack due to sybil listeners
Consensus layer	Various upcoming consensus Algorithms and their properties	51%, double-spending, Finney, Time-Validation, Block Withholding, Feature forking, Pool Specific, mempool, consensus delay, Timejacking, time validation
Replicated state machine layer	Smart-contract, User identity, transaction data confidentiality, integrity, authentication and availability	Reentrancy, Lack of privacy, Immutability, Programming, Stack overflow, Exception Syndrome, Call to Unknown, Out of gas exception, Rigorous and robust Compilation, Gasless send.
Application layer	User interface, Software Client Vulnerabilities	Double spending, Wallet theft, Cryptotoken attack

illegally generated cryptocurrency for a very high value. Users generally face scalability and performance issues in Application layer in addition to crypto token attack and Wallet theft. Crypto token attack leads to double spending and affects the real values of currency. Software Client Vulnerabilities and Keylogger malicious software affect the security of wallet addresses and key thefts are made possible leading to wallet attack. The different languages used for Smart Contract and their related threads lead to attack on Blockchain.

Cryptojacking attack finds mention as the most significant attack in the various cyber security reports for the year 2018. The most common attack is to turn a website into your mining pool to steal the hash value. One report indicates that around 4000 websites were affected due to this attack.

Table 1 summarizes the vulnerabilities of the various layers to security attacks.

7. Mechanisms for privacy preservation

The vulnerability of Blockchain to various kinds of attacks has motivated researchers to come up with strategies and mechanisms to improve the cyber security aspects of Blockchain. Bug Bounty approach is quite popular in identifying the loopholes in the security of any system in order to design strategies to close the security gaps. Researchers from different applications (like healthcare, e-governance) and technical areas (like AI, Machine Learning, Big data, Data mining) continuously propose new privacy preservation techniques. Some of the techniques/ algorithms /protocols which enhance the privacy or anonymity are discussed.

Privacy Enhancement Techniques (PETs) PETs allow protecting the online user's identity, data and transactions. Hard and soft privacy technologies [25] both fall under the PETs which are used without risking the privacy and security of information. A mixing transaction privacy enhancement scheme [26] is constructed by using aggregate signature and group signature algorithms of a set of mixing peers. In addition, there are network privacy enhancement techniques such as Garlic and Onion Routings. The different combinations of the various PET schemes are discussed in the following paragraphs.

7.1 *ZKPs*

Zero Knowledge Proofs (ZKPs) is a cryptographic protocol by which one of the nodes (verifier) can verify the other's (prover's) accurate data, without disclosing any personal data for the verification purpose. Prover sends the secret embedded in the function f (like challenge) and Verifier verifies S without disclosing the secret as shown in figure 3.

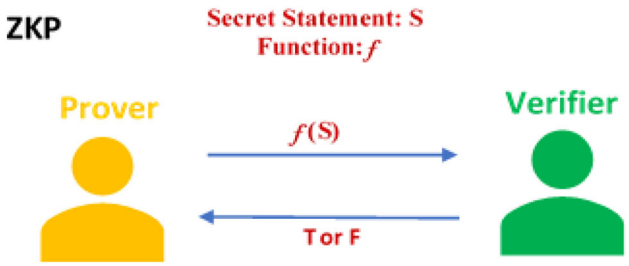

Figure 3. Fundamental flow of ZKP.

The Blockchain technology utilizes ZKP and related enhanced algorithms for improving the security. Table 2 gives a glance of the development of ZKP over the years.

ZKP is used for verification purpose without revealing the sensitive data. For example, bank verifies the income certificate for minimum amount which should satisfy through the certificate for loan purpose without revealing exact income. Authentication system can be built on ZKP without revealing information to verifier and others for authentication purpose. In ZKP mechanism, both prover and verifier should show honest behavior in order to maintain privacy. While achieving authentication, confidentiality of data should be ensured. Identity of the person can be kept secret, so anonymous transactions can happen and transactions and related attacks (wallet theft) can be prevented. ZCash, Hyperledger and other blockchain applications are using ZKP and enhanced versions to achieve privacy/anonymity.

7.2 *SMPC*

In Secure Multi Party Computation two or more parties of different data owners do not share their private data but agree to compute some joint function to ensure privacy (parties acquire only the output of the computation) and correctness (output of the computation is correct).

Suppose there are n parties P1, P2, ⋯, Pn and one of the party Pi knows only about his/her own secret input Xi. All the n parties jointly compute the function F such that

$$F(X1, X2, \cdots, Xn) = (Y1, Y2, \cdots, Yn)$$

where Pi only learns his/ her own output Yi. SMPC is shown in the figure 4.

SMPC must satisfy the following two parameters:

- Privacy: Participant Pj cannot get any other input Xi(j ≠ i).
- Consistency: Honest participants receive same output as Y1 = Y2 = ⋯ = Yn.

Shamir's Secret Sharing (SSS) MPC protocol is a basic protocol which was introduced in 1970. Secret(s) was shared with n parties with absence of some and without

Table 2. ZKP development flow.

Method	Year	References	Features	Lacunae
Zero-Knowledge Proofs	1987	[27]	At ½ probability, the protocol works perfectly	Few NP problems need to solve
ZK interactive proofs and arguments for languages in NP	1992	[28]	Efficiently checkable proofs for NP and speed up with 3 colorability	Slightly costly protocol
Succinct non-interactive adaptive argument of knowledge (SNARK).	2012	[29]	Efficient secured, protocol	Complex
Pinocchio	2013	[30]	In order to realize both asymptotic and concrete efficiency highly efficient cryptographic protocol employing quadratic programs is used	Requires support to enhance parallel execution for truly practical verifiable computing
Pairing-based Non-interactive Arguments	2016	[31]	Efficient use of arithmetic circuit satisfiability on NP-complete language with asymmetric pairings	Dynamic pairing but for higher values above 3 practically not confirmed
Scalable Transparent ARgument of Knowledge (ZK-STARK)	2018	[32]	Interactive Oracle Proofs (IOP) for error correcting codes and exponentially fast verification	Honesty of all parties is basic requirement to improve the trust among the parties

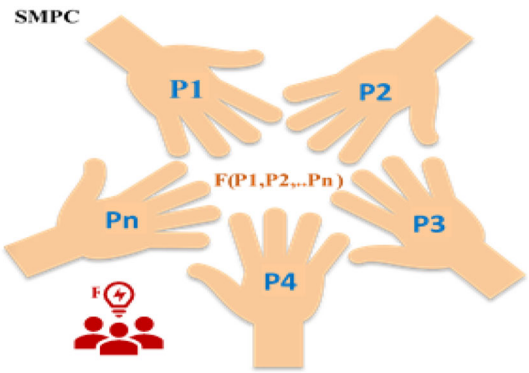

Figure 4. Fundamental flow of SMPC.

knowing the actual data. It is also known as (t+1) / n threshold value of Secret sharing as the secret which can be reconstructed by any subset of (t + 1) or more of the participants, but no subset of t or less participants can discover anything about it. One of the ways is to consider t as a polynomial and using Lagrange basic polynomials find out (t+1) degree value using addition, multiplication or multiplication with constant. Table 3 gives a glance of the development of SMPC over the years.

Practical implementation of SMPC protocol has been very slow although many schemes have been proposed [37]. Various techniques, such as, Shamir Secret Sharing, Honest-majority MPC with secret sharing (BGW protocol), Threshold cryptography, and Dishonest-majority MPC are being considered to address the secure Multi party communication issues. In the Honest majority assumption technique, more than 50% of the participants might be honest whereas Dishonest majority hypothesis considers that more than 50% participants might be dishonest. Yehuda Lindell continues to work in this field since 2004 and his projects and publications are mentioned in his webpage [38].

The Blockchain based SMPC framework called Homomorphism Encryption Technique was proposed in March 2020 [39]. This mechanism overcomes the single point failure, data integrity and Collusion attack (in semi honest model) problems. SMPC continues to be a theoretical concept to solve the Blockchain's consensus and smart contract problems. One example of Decentralized Finance (DeFi) applications is Wanchain which uses SMPC for privacy protection. It also enables interoperation with other Blockchain like etherium (in Wanchain 2.0) and Bitcoin (in Wanchain 3.0) [40].

Table 3. SMPC development flow.

Method	Year	References	Features	Lacunae
Shamir's Secret Sharing	1970	[33]	First secret sharing in multiple parties' algorithm	Single Points of Failure, Share Revocation, Lack of Implementation Standards, Auditability issue
Yao's Protocols for Secure Computations	1982	[34]	Garbled Circuits Protocol	Use for 2 parties, hence not suitable practically
GMW, CCD, BGW, BCC, CGMA, RB, GMR, GM	1980's to 90's	[35, 36]	Basic algorithms for recent MPC, rich theory	In the presence of a forceful adversary anonymity and user action may be denied.
Yehuda Lindell work	2004 till date	[37, 38]	Real time commercial project, real-life issues can be solved	Expert attention required to deploy this complex scheme
Block-SMPC	2020	[39]	Solution for single point of failure, data integrity, collusion attack	Real time experiment and analysis require

7.3 *Ring signatures*

It is a type of digital signature in which multiple parties come together and form a group and anyone from that group can sign the message using the key. Thus, someone from that group endorses the signed message. The fundamental process of ring signature is shown in figure 5. Ring signature is slightly different from group signature. Without additional setup one set of users can be used as a signing set. All ring members need to know about public key of each other rather than any other knowledge, permission or support to become a member of the ring. As Blockchain does not ensure privacy and anonymity, the various algorithms are proposed using ring signature concept.

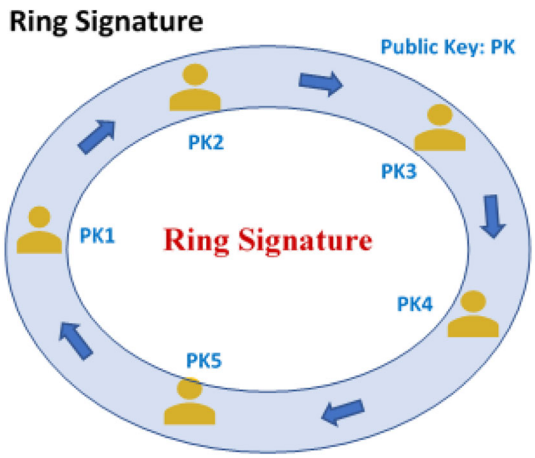

Figure 5. Fundamental process of ring signature.

After the Ring Signature scheme was invented by Ron Rivest, Adi Shamir, and Yael Tauman Kalai in 2001, a number of combinations of this scheme with or without Random Oracle have been published. The aggregate signature scheme with ring members scalable approach [41] and the Ring signature on the elliptic curve scheme [11] provide unconditional anonymity and protection from forging, although Elliptic curve is vulnerable to quantum computing. The Lattice-based Linkable Ring Signature with Co-Signing is mentioned in literature as post-quantum cryptographic mechanism. Other schemes like Universal ring signature [42], Identity-based threshold ring signature [43] and a few others are in conceptual stage. Table 4 gives a glance of the development of Ring Signature over the years.

7.4 *Mixing*

Mixing network address concept allows a group of distributed parties to post their messages without disclosing their identity keeping any other party blind in honest or dishonest majority conditions [47]. Linking of the user's address with the transaction is avoided as shown in figure 6.

Table 4. Ring Signature development flow.

Method	Year	References	Features	Lacunae
How to Leak a Secret	2001	[44]	Signer-ambiguous, no third-party involvement	Costly, not useful in the presence of strong adversary
Identity-based anonymous designated ring signatures	2006	[45]	Based on bilinear pairings and Random oracle	Need to improve efficiency
Linkable Ring Signature	2018	[46]	Lattice-based, protects electronic wallets	Complex

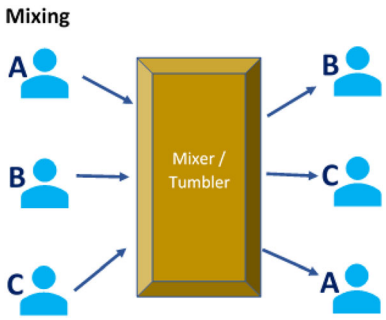

Figure 6. Fundamental process of mixing.

But if the centralized services are used, confidentiality of identity cannot be assured as the transactions are open to public verification.

The mixing process (also called obfuscate process) involves the mixing of the various senders' messages and transfer to various receivers in such a way that an attacker cannot interpret the relationship between senders and the target receivers, thereby protecting the identity. The mixing scheme in paper [48] provides privacy using signature protocol without involvement of third party and extra transaction fees. However, there is a need to reduce the mixing wait time in Blockchain technology. The various mixing schemes are to be made efficient and cost effective.

7.5 *Post quantum computing*

A quantum computer operates three million times faster than a traditional computer to solve problems. The fundamental process of post quantum computing is shown in figure 7. It has posed a threat to hack several of today's algorithms used in cryptography seriously impacting IT security. As discussed in section 5 *g* (Issues in Blockchain), Grover's algorithm and Shor's algorithm are the principal

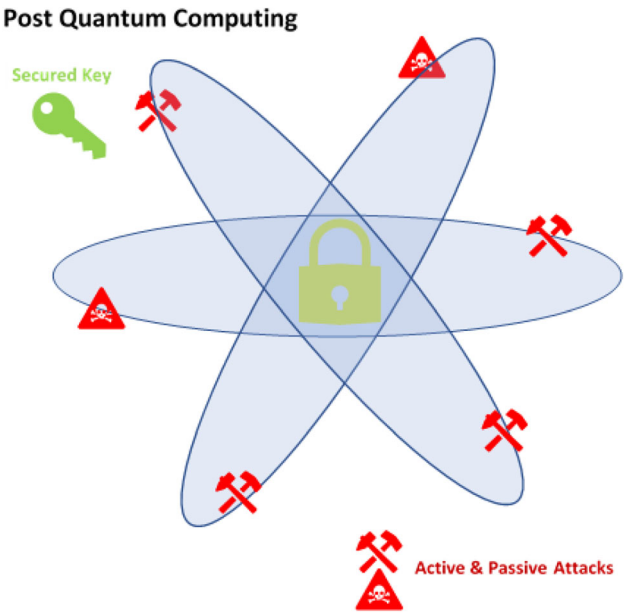

Figure 7. Fundamental post quantum computing.

threats due to quantum computing. On the other hand, encryption algorithms, like quantum key distribution (QKD), which are created using quantum computing, may provide strong security to Blockchain based applications.

Quantum resistant cryptography is a field of study where security is sought to be ensured in the context of quantum computers breaking the traditional cryptographic algorithms [17]. Of the various traditional cryptographic schemes that have been developed, like Hash based, Multivariate based and Code based algorithms, NIST claims that the Lattice based NTRU family of cryptographic algorithms is the most practical which is immune to quantum computer based attacks [49]. However, further studies are going on in the area of quantum resistance cryptography to address issues like speed of key generation, size of key and signature bits with a view to standardize quantum resistant protocols.

7.6 *Homomorphic encryption (HE)*

HE goes hand-in-hand with all the cryptography techniques. It can merge with all the techniques explained above to achieve the privacy objective. It is a special kind of encryption where the encrypted data is computed without decryption. Example is Google search. This term was first introduced by Ronald L. Rivest, Len Adleman and Michael L. Dertouzos in 1978 as a special encryption function called "privacy homomorphism" [50]. For privacy preservation in cloud storage and computation HE is more suitable for encrypting data. Traditional encryption procedure follows three steps, namely, key generation, encryption and decryption while HE has one more step, analysis/evaluation as shown in figure 8. HE is based on two major operations [51] namely (a) Multiplicative Homomorphic Operations: E(S1*S2) = E(S1) * E(S2) and (b) Additive Homomorphic Operations: (S1+S2) = (S1) + (S2) with the assumptions 'E' for Encryption and 'n' for a set of all possible messages where 'S1' and 'S2' are any two messages from 'n'. The fundamental process of Homomorphic Encryption is shown in figure 8.

HE is basically divided into three types[52].

(i) Partially homomorphic encryption (PHE)

It permits single operation, either addition or multiplication, which may be called any number of times. For example – RSA (1978), Goldwasser - Micali Cryptosystem (1982), Elgamal Algorithm (1985), Pallier Cryptosystem (1999).

(ii) Somewhat homomorphic encryption (SWHE)

It permits both addition and multiplication operations, but called only limited number of times. For example – SYY (2000), BGN (2005), IP (2009).

(iii) Fully homomorphic encryption (FHE)

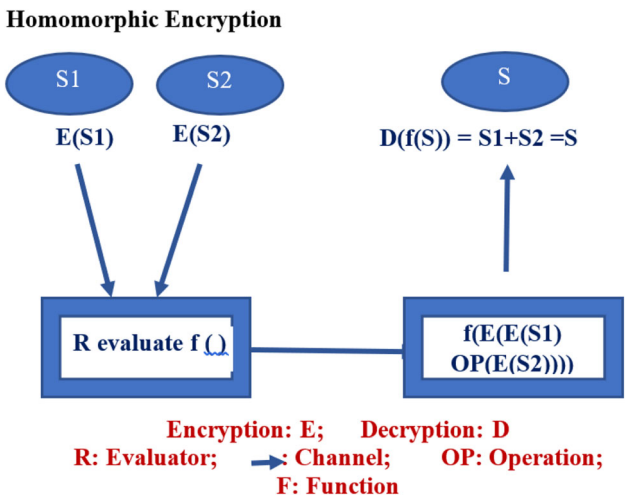

Figure 8. Fundamental process of homomorphic encryption.

It permits both addition and multiplication operations, but random number of times. For example – lattice-based (2009), integer based (2010), learning with error based (2011), NTRU type encryption schemes (2012), FHE based on Elliptic curve Cryptography (2016).

Some of the publicly available FHE implemented libraries are NTL, GM, FLINT, MPFR, MPIR, FFTW [53]. The implementation work of Modified Multi-Key FHE, SWHE using NTRU schemes is explained in paper [54]. Due to simplicity of this scheme, it is considered as an alternative to post quantum cryptography. Generalized analysis for any HE scheme is based on security, speed, and simplicity.

Homomorphic Secret Sharing (HSS) [55] is an algorithm in which the secret is encrypted via homomorphic encryption. This scheme, which is considered safe for multiparty computation, is based on the principle of multiplying a security threshold of ($t < m/2$) with two secrets. The other feature is the optimal compactness, which gives a single bit output.

8. Blockchain platforms/applications based on privacy mechanisms

8.1 *Zcash*

Zcash was launched in 2016 by the research scientists from UC Berkeley, John Hopkins, Technion and Tel Aviv universities with MIT in the lead. It is using zkSNARKs protocols and related versions as privacy preservation mechanism. Later, ZClassic split as fork of ZCash, with the intention to create a cryptocurrency focused on privacy preservation. ZCash employs a cryptographic tool called zk-SNARKs, which stands for Zero Knowledge Succinct Non-Interactive Argument of Knowledge. This tool allows two users to engage in transactions keeping their payment addresses anonymous by obfuscating the payment addresses of both parties and the amount involved in each transaction. This feature makes ZCash unique among the other cryptocurrencies. Anyone whose Zaddr has been shared with a third party is affected due to third party dishonesty. A "Sapling Wood-Chipper" attack in Zcash 2.x provides an inexpensive way to "fill all transactions on all blocks" and "prevent any actual transaction from occurring". ZCash makes use of bellman, a Rust-language library for implementation of zk-SNARKs. Before the Sapling upgradation, ZCash worked on Pinocchio protocol, and currently Jens Groth's zk-SNARK is in use. ZCash is vulnerable to any of the attacks like Sapling Wood-Chipper, Remote Side-Channel on Anonymous Transactions and Allowed Infinite Counterfeit [56]. These vulnerabilities were rectified by Sapling update and by adapting new protocols which avoided the related attacks.

8.2 *Zerocoin*

Zerocoin is the predecessor to ZCash but different from ZCash though the same team was working behind the development of Zerocoin. This was designed as an extension protocol to Bitcoin, but the proposal was abandoned. It works on the principle of mixing coins and Zero-knowledge Proofs to provide anonymity. In the year 2017, over a span of a few weeks, a manipulative coding attack created 370,000 fake ZCoin tokens leading to a loss of over $600000. At the device level, Zerocoin did not incorporate real-time tracking or fund transaction tracing.

8.3 *Hyperledger*

In 2015, the Linux Foundation started the creation of the Blockchain-based distributed ledgers, called the Hyperledger Project. This project had contributions from IBM, Data Asset, Intel, Sovrin and others leading to Hyperledger frameworks like Hyperledger Fabric and Sawtooth, and libraries like Hyperledger Ursa [57]. Also benchmark tools like Hyperledger Caliper and Hyperledger Indy were developed to disclose verification data selectively on the basis of need. Before the Hyperledger Indy version 1.12.4 became available, it was possible to make unauthorized alterations in the ledger because of the absence of signature verification. The updated transaction modifies the metadata because of improvement in Verisign and keys [58].

8.4 *Wanchain*

Wanchain supports cross-chain transactions between different Blockchain networks. It includes the following three mechanisms: (i) Threshold secret-sharing technology, (ii) Multi-party computing for the locked account management, and (iii) The ring signatures and one-time accounts-based privacy security system for smart contract token transactions [59]. Previous versions of Wanchain faced vulnerabilities of medium severity due to elliptic curve cryptography. There is no search to see if the public key point passed through the derived function which is on the secp256k1 curve. As a result, after performing a series of ECDH operations, the private key used in this implementation may get exposed leading to the recovery of the long-term private key provided by the library. On an elliptic curve, bit-length leakage during scalar multiplication is possible, which might enable functional recovery of the long-term private key which leads to timing attack [60]. So, this platform is resistant to quantum computing.

8.5 *CoinParty*

It is the combination of two existing components - threshold Elliptic curve Digital Signature algorithm and decryption mixnets. This makes for one-to-one transfers, raising the amount of confidentiality possible by orders of magnitude. Although, CoinParty is an improvement over CoinJoin which relies on shuffling of output addresses by a centralized service, it will not protect privacy from insiders. The anonymity is restricted to n members, plausible deniability is eliminated with increased transaction cost for wider mixing parties [61].

8.6 *Monero*

Monero is a cryptocurrency emphasizes on privacy. It was launched in 2014. It is a free, fast, private and secure open-source protocol that uses the CryptoNote application layer. Monero is the first cryptocurrency in which all users are automatically anonymous. Stealth Addresses, Ring Signatures, and RingCT are three main technologies that hide the sender, recipient, and the number of a transaction. One of the vulnerabilities is Cryptojacking [62] where rTorrent clients were accessible and deployment of cryptominers on them was possible without authentication. To avoid this, clients do not accept outside connection. Some more attacks mentioned in [63] as (i) Disproportionately Gaining Network Share, (ii) Injecting Peer Lists of Malicious Nodes, (iii) Block Height Mirroring, (iv) Spying on Transactions, (v) Wallet DoS via Block Height+2, (vi) Transaction DoS via Dropping Stem-Phase Transactions, (vii) Node DoS via out-of-memory crash. The mitigations are cited as Dandelion++ and/or Tor/i2p usage, or given in PR (Pull Request) numbers. Cascade effect attacks are avoided by increasing the minimum ring size of each input and enhancing the ring confidentiality of transactions.

8.7 *CryptoNote*

CryptoNote [64] is an application layer protocol designed to work with cryptocurrencies like Monero and DigitalNote. It uses Ring Signatures and One-time addresses for untraceable and unlinkable transactions. The closed set attack like brute force attack is explained in the paper "New Empirical Traceability Analysis of CryptoNote-Style Blockchains" by Zuoxia Yu and analysed using clustering method with the cascade attack. The "key image" used in CryptoNote coins that use the elliptic curve ed25519 can be altered in a unique way, enabling issue of double-spends. This has the potential to allow someone to generate an unlimited number of coins in a manner that is difficult to detect without first learning about the hack and writing a

code to detect it. The simple solution [65] to this problem is multiplying the key images by the curve order for accuracy and verifying that the result corresponds to the identity element.

8.8 *Mixcoin*

Mixcoin is bitcoin's first unified coin mixing device [64]. To maintain external anonymity, Mixcoin uses a central mixing server (or trusted third party) to mix transaction addresses and provide mixing services to users. As users' addresses can be hidden away from communicating directly, transaction content can be secured from the attackers. Third Party Server handles mixing process of internal and external users' addresses, hence there may be leakage of transaction amount and user privacy. Simple solutions attempted earlier have not been successful. Mixcoin adopted a reputation-based cryptographic accountability mechanism [66]. However, the transparency process would not be enough to eliminate the threat of third-party information leakage.

8.9 *CoinShuffle*

CoinShuffle's [67] decentralized scheme fully realizes internal unlinkability, which prevents users from causing loss of funds by combining them. This scheme is vulnerable to DOS attack because the coin mixing scheme allows the presence of all users at the same time. Larger the number of participants, higher is the connectivity charges, which could result in a situation where there are not enough users to join. The anonymity of CoinShuffle is dependent on the size of the anonymity collection, which is small, and it is therefore open to cross and sybil attacks [66]. CoinShuffle++ is the faster and better solution where it generates public and private key pairs with unique strings of numbers for mutual trust and secret sharing among only two participants.

8.10 *Microsoft Picnic*

The code name "Picnic" refers to a post-quantum digital signature algorithm [68]. Picnic was developed in cooperation with engineers and researchers from various esteemed universities. It uses ZKP and cryptographic hash and block methods to support hard problems and quantum resistance. Picnic improves the MPC protocol (LowMC) by reducing the signing time by making the signatures short [69]. Due to this modification, signing of messages and verification of the signatures are made several times faster while having the same signature size. TLS fortune attack due to quantum computing can be resolved by Picnic's quantum-resistant key exchange and signature algorithms.

8.11 *NewHope*

Erdem Alkim, Leo Ducas, Thomas Poppelmann, and Peter Schwabe developed NewHope [70], a key-agreement protocol designed to resist quantum machine attacks. NewHope is based on a difficult-to-solve mathematical problem known as Ring Learning With Errors (RLWE). It has been chosen as a round-two competitor in the NIST Post-Quantum Cryptography Standardization race. Now it is known as Google NewHope and available in the Canary version of Chrome which was awarded the 2016 Internet Defense Prize. In key reuse attack, the adversary creates a malformed key to start key exchange sessions to decode the signal variations [71]. The proposal of error-reconciliation mechanism on signal function using special lattice can prevent the key reuse attack. The 'NewHope IND-CCA KEM secure key encapsulation mechanism' would stop such an attack.

Table 5 summarizes the various Blockchain platforms/applications which may use one or more combinations of the privacy mechanisms. Although, these platforms are vulnerable to various attacks, there are mitigation measures to make these platforms/applications foolproof to attacks.

9. Limitations

The above analysis clearly shows the need for further study which is required to determine the relative strengths and disadvantages of the various PETs, create new PETs or enhance the efficacy of existing ones, and consider the challenges to PET deployment in the online marketplace. Individuals often need to be made aware of the role of PETs so that they can make an informed choice of the technique to be adopted in order to secure their information on the internet and benefit the most from these techniques. The high computational power and the low usability continue to be the major issues in this area making these techniques quite expensive. PET algorithms need to be protected from black market as these could become the root cause for Silk Road or Darknet market.

10. Proposed privacy enhanced architecture

Considering the various points that have emerged in the above discussions, a privacy enhanced architecture for the blockchain application is illustrated in figure 9. The Self-Sovereign Identity (SSI) concept used in this architecture enables individuals to retain control over their digital identities in all applications. The User is given credentials linked to the identity by the Issuer in a privacy preserving manner. The User is allowed access to all digital services (to go ahead with transactions) by the Service provider after the credentials presented by the User are verified without

Table 5. Blockchain platforms, Privacy mechanisms, Vulnerability and Mitigation.

Platform/application	Privacy mechanisms	Vulnerability	Mitigation
ZCash [72]	Zero-knowledge Proofs (ZK SNARKS)	Remote Side-Channel Attacks on Anonymous Transactions, sapling Wood-Chipper, Allowed Infinite Counterfeit	Sapling update and adapting Jens Groth's zk-SNARK
Hyperledger [57]	Zero-knowledge Proofs	Improper Verification of Cryptographic Signature	Update metadata associated with a DID
Zerocoin [73]	Zero-knowledge Proofs	Doble spending	Introduced Zcash
Wanchain [59]	SMPC, Ring signature, OTP	Timing Attack	Quantum resistant algorithms
CoinParty [61]	SMPC, Mixing	No Anonymity against insider	2/3 users should be honest
Monero [74]	Ring signature	Spying on Transactions, Cryptohajacking	Dandelion++ and/or Tor/i2p usage.
CryptoNote [64]	Ring Signature	Double-spends	Verify key image accuracy
Mixcoin [75]	Mixing	Privacy failure due to Trusted Third party	Reputation-based cryptographic accountability
CoinShuffle [67]	Decryption mix network	Cross attack, Sybil attack	Mutual secret sharing among 2 participants
Microsoft Picnic [68]	PKI, Post quantum	Attack on secret sharing and digital signature	LowMC Multiparty Computation Protocol
NewHope [70]	Post quantum Computing	Key Reuse Attack	IND-CCA KEM secure key encapsulation mechanisms

the need for any external administrative authority. User is provided Personally Identifiable Information (PII) by the government and then it is cryptographically secured on a blockchain using a hash function. This ensures that only the hash value is available to those who want to verify user's identity without having to check other personal information.

The cryptographically verifiable digital identity, which employs new standards such as Decentralized IDentifier (DID) and Verifiable Credentials (VC) based on blockchain/distributed ledger, is fully governed by its owner. The type of identity data is decided by the identity owner, who retains full control over its use as long as it is needed. The identity cannot be revoked, modified or removed by anyone else. Further, the User is permitted access to all operations related to the identity and personal data. The User can assign control of all such functions to others.

The architecture envisages the use of Zero knowledge proof, homomorphic encryption and PII certificate for privacy preservation of user's information in distributed form, so that a small portion of the needed information can be provided. The sequence of operations is discussed below:

(1) User sends Request to Issuer(E-Government) for DID.
(2) Issuer asks for PII which require to provide DID.

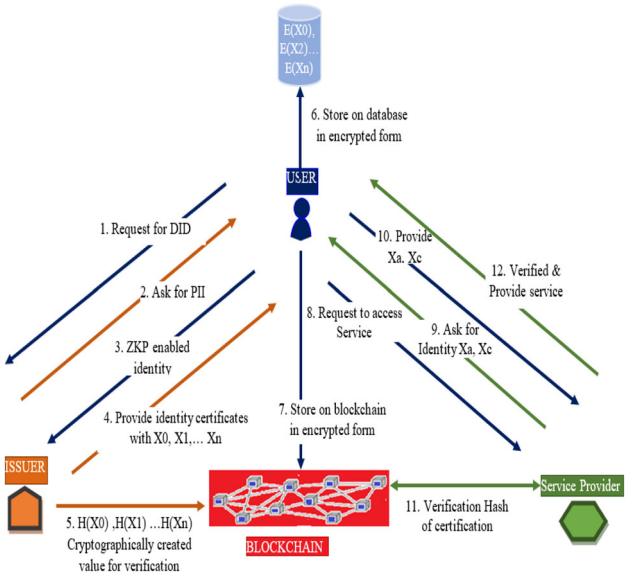

Figure 9. Proposed architecture.

(3) User provides only authenticated essential information i.e. ZKP enabled identity to issuer.
(4) Issuer provides identity certificates in the form of X0, X1,,,… Xn to User which is in segregated information format signed by Issuer.
(5) Also hash values H(X0), H(X1) …H(Xn) are generated by Issuer for verification purpose which can be stored on the blockchain.
(6) User stores the identity certificates on personal database in Symmetric homomorphic encrypted format.
(7) User also stores the encrypted form data on the blockchain.
(8) The User who has the Identity certificates, can request for services to the Service provider, as and when required.
(9) Service provider demands Identity data Xa, Xc or any other information.
(10) User provides required information as Xa, Xc.
(11) Service Provider verifies the Hash values and digital signature on the certification.
(12) On successful verification, Service Provider provides services to User.

It is accepted that the proposed architecture addresses many of the limitations of adapting blockchain technology for various applications. It is expected that this model will remove the privacy related limitations, particularly in the following applications: University certificates, Crowdfunding, Car rental system, Bug Bounty, Bank credit limit, Bidding, e-voting, etc.

11. Conclusion

This paper identified the technological requirements of data privacy and protection in general for the online transactions for the contactless working of today's digital world. The existing as well as the proposed Data protection regulations of various countries are emphasizing the importance of user privacy insisting that the users should have the basic right to delete and forget if they wish to. It is the basic requirement that a system in the digital era should be secure from attacks and measures to mitigate the vulnerability to attacks should be implemented. In this context, the suitability of Blockchain technology to meet the requirements of security and privacy was examined and the aspects which require further research and study in order to make Blockchain technology future proof have been analysed in detail. The use of Privacy Enhancing Techniques has been explained elaborately. The need for efficient crypto-privacy algorithms which will make Blockchain technology more effective and enable building of quantum resistant ledgers has been emphasized. It is believed that these measures will lead to more wide spread use of Blockchain in the digital world fully compliant with the privacy regulations. The proposed architecture in this paper takes into account the various shortcomings of the blockchain applications. As and when further limitations come to light, mitigation measures have to be applied to make blockchain technology a robust one.

References

[1] Prasad RS 2019 *The Personal Data Protection Bill*, 2019
[2] Cloudflare Team 2021 What is data privacy? https://www.cloudflare.com/learning/privacy/what-is-data-privacy/
[3] Boussada R, Elhdhili M and Saidane L 2016 A survey on privacy: Terminology, mechanisms and attacks. In: *IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco,* pp. 1–7
[4] Nakamoto S 2008 Bitcoin: A Peer-to-Peer Electronic Cash System, p. 9
[5] Mearian L 2017 Computerworld Apr 24, NEWS ANALYSIS FAQ: What is blockchain and how can it help business? *CSO from IDG Communications, INDIA*
[6] Ma Y, Sun Y, Lei Y, Qin N and Lu J 2020 A survey of blockchain technology on security, privacy, and trust in crowdsourcing services. *World Wide Web* 23–1: 393–419
[7] Bansod S and Ragha L 2020 Blockchain technology: applications and research challenges. In: *International Conference for Emerging Technology (INCET), Belgaum, India*, pp. 1–6

[8] Lesavre L 2020 A Taxonomic Approach to Understanding Emerging Blockchain Identity Management System *National Institute of Standards and Technology*
[9] Aarhus C CKMS 2015 Crypto Key Management System *Denmark: Cryptomathic. [Online]*. https://www.cryptomathic.com/products/key-management/crypto-key-management-system
[10] Wang R, He J, Liu C, Li Q, Tsai W and Deng E 2018 A privacy-aware PKI system based on permissioned blockchains. In: *IEEE 9th International Conference on Software Engineering and Service Science (ICSESS), Beijing China*, pp. 928–931
[11] Li X, Mei Y, Gong J, Xiang F and Sun Z 2020 A blockchain privacy protection scheme based on ring signature. *IEEE Access* 8: 76765–76772
[12] Eskandari S, Clark J, Barrera D and Stobert E 2015 A first look at the usability of bitcoin key management. In: *Proceedings 2015 Workshop on Usable Security*
[13] Lohwasser R 2019 Co-Founder & CEO, LITION, LITION_-WHITEPAPER 2019 *The Blockchain Standard Infrastructure for Business*
[14] Hillmann P, Knüpfer M, Heiland E and Karcher A 2021 Selective Deletion in a Blockchain arXiv:2101.05495
[15] Casino F, Dasaklis T and Patsakis C 2019 A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inf.* 36: 55–81
[16] Al-Jaroodi J and Mohamed N 2019 Blockchain in industries: a survey. *IEEE Access* 7: 36500–36515
[17] Rodenburg B 2017 Blockchain and Quantum Computing
[18] Sim W, Chua H and Tahir M 2019 Blockchain for identity management: the implications to personal data protection. In: *IEEE Conference on Application, Information and Network Security (AINS), Pulau Pinang, Malaysia*, pp. 30–35
[19] Homoliak I, Venugopalan S, Hum Q and Szalachowski P 2019 A security reference architecture for Blockchains. In: *IEEE International Conference on Blockchain (Blockchain), Atlanta, GA USA*, pp. 390–397
[20] Yang W, Aghasian E, Garg S, Herbert D, Disiuta L and Kang B 2019 A survey on blockchain-based internet service architecture: requirements, challenges, trends, and future. *IEEE Access* 7: 75845–75872
[21] Saad M, Spaulding J, Njilla L, Kamhoua C, Nyang D and Mohaisen 2019 Overview of attack surfaces in blockchain for distributed systems security 3: 51–66
[22] Ateniese G, Magri B, Venturi D and Andrade E 2017 Redactable blockchain – or – rewriting history in bitcoin and friends. In: *IEEE European Symposium on Security and Privacy (EuroS&P), Paris*, pp.111–126
[23] Wang H, Wang Y, Cao Z, Li Z and Xiong G 2019 An overview of blockchain security analysis. *Cyber Security, Singapore*, pp. 55–72
[24] Rouhani S and Deters F 2019 Security, performance, and applications of smart contracts: a systematic survey. *IEEE Access* 7: 50759–50779
[25] Deng M, Wuyts K, Scandariato R, Preneel B and Joosen B 2010 A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requir. Eng.* 16: 3–32
[26] Feng T, Chen X, Liu C and Feng X 2019 Research on privacy enhancement scheme of blockchain. *Trans. Secur. Priv.* 2–6
[27] Goldwasser S, Micali S and Rackoff C 1985 The knowledge complexity of interactive proof systems. *ACM*
[28] Kilian J 1992 A note on efficient zero-knowledge proofs and arguments (extended abstract). In: *Proceedings of the Twenty-Fourth Annual ACM Symposium on Theory of Computing- STOC '92, Victoria, British Columbia, Canada,* pp. 723–732
[29] Bitansky N, Canetti R, Chiesa A and Tromer E 2012 From extractable collision resistance to succinct non-interactive arguments of knowledge In: *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference on-ITCS 12, Cambridge, Massachusetts*, pp. 326–349
[30] Parno B, Howell J, Gentry C and Raykova M 2013 Pinocchio: nearly practical verifiable. In: *Computation IEEE Symposium on Security and Privacy, Berkeley, CA*, pp. 238–252
[31] Groth J 2016 On the size of pairing-based non-interactive arguments. In: *Advances in Cryptology – EUROCRYPT M. Fischlin and J.-S. Coron, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg,* 9666: 305–326
[32] Ben-Sasson E, Bentov I, Horesh Y, Riabzev M 2018 Scalable, transparent, and post-quantum secure computational integrity, p. 83
[33] Shamir A 1979 How to share a secret. *Commun ACM* 22–11: 612–613
[34] Yao A 1982 Protocols for Secure Computations *University of California Berkeley, California, IEEE*, p. 5
[35] Goldwasser S 1997 Multi party computations: past and present. In: *Proceedings of the sixteenth annual ACM symposium on Principles of distributed computing - PODC '97, Santa Barbara, California, United States*, pp. 1–6
[36] Evans D, Kolesnikov V and Rosulek M A 2018 Pragmatic Introduction to Secure Multi-Party Computation, p. 181
[37] Lindell Y 2021 Secure multiparty computation. *Commun. ACM* 64–1: 86–96
[38] Lindell Y 2018 Multi Party Computation Protocols *Website* https://cyber.biu.ac.il/grants/external-grants/
[39] Yang Y, Wei L, Wu J and Long C 2020 Block-SMPC: a blockchain-based secure multi-party computation for privacy-protected data sharing. In: *Proceedings of the 2020 The 2nd International Conference on Blockchain Technology, Hilo HI USA*, pp. 46–51
[40] Birch O 2018 https://medium.com/wanchain-foundation https://www.wanchain.org/. [Online]
[41] Qiao K, You W and Tang H 2019 A new privacy protection security scheme for blockchain. *J. Phys.: Conf. Ser.* 1237: 022025
[42] Tso R 2013 A new way to generate a ring: Universal ring signature. *Comput. Math. Appl.* 65–9: 1350–1359
[43] Deng L and Zeng J 2014 Two new identity-based threshold ring signature schemes. *Theor. Comput. Sci.* 535: 38–45
[44] Rivest R, Shamir A, Tauman Y 2001 How to leak a secret advances in cryptology. In: *ASIACRYPT 2001, C. Boyd, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg 2248:552–565*
[45] Chen Y, Susilo W and Mu Y 2006 Identity-based anonymous designated ring signatures. In: *Proceeding of the 2006 International Conference on Communications and Mobile Computing - IWCMC '06, Vancouver, British Columbia, Canada*, p. 189
[46] Torres W, Steinfeld R, Sakzad A and Kuchta V 2018 Post-quantum linkable ring signature enabling distributed

authorised ring confidential. In: *Transactions in Blockchain, ACISP-2018*, p. 45
[47] Zhang R, Xue R and Liu L 2019 Security and privacy on blockchain. *ACM Comput. Surv*. 52–3: 1–34
[48] Xiao R, Ren W, Zhu T, Choo K 2019 A mixing scheme using a decentralized signature protocol for privacy protection in bitcoin. *Blockchain IEEE Trans. Dependable and Secure Comput.*, pp. 1–1
[49] Fernandez T and Fraga P 2020 Towards post-quantum blockchain: a review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access* 8: 21091–21116
[50] Rivest R, Adleman L and Dertouzos M 1978 On data banks and privacy homomorphisms. *Foundations of secure computation*
[51] Sirajudeen Y and Anitha R 2018 Survey on Homomorphic Encryption International Conference for Phoenixes on Emerging Current Trends in Engineering and Management (PECTEAM 2018), Chennai, India
[52] Chaudhary P 2019 Analysis and comparison of various fully homomorphic encryption techniques. In: *International Conference on Computing, Power and Communication Technologies (GUCON)*, p. 5
[53] Acar A, Aksu H, Uluagac A and Conti M 2018 A survey on homomorphic encryption schemes: Theory and implementation. *ACM Comput. Surv*. 51–4: 1–35
[54] Che X, Zhou T, Li N, Zhou H, Chen Z and Yang X 2020 Modified multi-key fully homomorphic encryption based on NTRU cryptosystem without key-switching. *Tinshhua Sci. Technol.* 25–5: 564–578
[55] Boyle E, Gilboa N, Ishai Y and Tessaro S 2017 Foundations of Homomorphic Secret Sharing, p. 43
[56] Hackett R 2019 Zcash discloses vulnerability that could have allowed 'infinite counterfeit'. *Cryptocurrency The Ledger - Cybersecurity, Fortune*
[57] Blummer T, Bohan S, Bowman M, Cachin C, *et al.* 2018 HL_Whitepaper_Introduction to Hyperledger. *The Linux Foundation*
[58] NIST 2020 Information Technology Laboratory. *National Vulnerability Database CVE-2020-11093 Detail*
[59] Lu J, Yang B, Liang Z and Lu L 2017 Wanchain White paper *Wanchain Foundation Ltd*
[60] snyktest@3test/wanchain-asset-ledger@1.2.0. https://snyk.io/test/npm/@3test/wanchain-asset-ledger/1.2.0
[61] Ziegeldorf J, Grossmann F, Henze M, Inden N and Wehrle K 2015 CoinParty: secure multi-party mixing of bitcoins. In: *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy, San Antonio Texas USA*, pp. 75–86
[62] Nadeau M 2021 What is cryptojacking? How to prevent, detect, and recover from it
[63] Simmons S 2020 A Brief Breakdown of Monero's Ongoing Network Attacks *#Monero #Network #p2p*
[64] CryptoNote Technology CryptoNote - Create your own Cryptocurrency
[65] Luigi R 2017 Disclosure of a Major Bug in CryptoNote Based Currencies *MONARO* [Online]
[66] Wang D, Zhao J and Wang Y 2020 A survey on privacy protection of blockchain: the technology and application. *IEEE Access* 8: 108766–108781
[67] Ruffing T, Moreno P and Kate A 2014 CoinShuffle: practical decentralized coin mixing for bitcoin computer security. In: *ESORICS 2014 M. Kutyłowski and J. Vaidya, Eds. Cham: Springer International Publishing 8713:345–364*
[68] Chase M, Derler D, Goldfeder S and Katz J 2020 Picnic: *Microsoft Research Project*
[69] Kales D and Zaverucha G 2020 Improving the Performance of the Picnic Signature Scheme. *TCHES*, pp. 154–188
[70] Schwabe P 2017 NewHope Post-quantum key encapsulation *[Online]*
[71] Liu C, Zheng Z and Zou G 2018 Key reuse attack on NewHope key exchange protocol. In: *Information Security and Cryptology – ICISC 2018 K. Lee, Ed. Cham: Springer International Publishing* 11396:163–176
[72] The research scientists from MIT, Technion, Hopkins J, Aviv University, UC Berkeley 2016 Zcash *Electric Coin Company [Online]*
[73] Miers I 2013 Zerocoin Project http://zerocoin.org/
[74] Monero 2015 *MONERO A Private Digital Currency*
[75] Bonneau J, Narayanan A, Miller A, Clark J, Kroll J and Felten W 2014 Mixcoin: Anonymity for Bitcoin with accountable mixes *IACR Cryptology ePrint Archive, 2014:77*