Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Security and Privacy Preserving Solution for Blockchain: Reviews and Challenges

R. Rajakarthik[1], Sumalatha V[2], R Rajalingam[3]

[1]Research Scholar, Department of Computer Applications, Vels University Chennai, India
[2]Associate Professor, Department of Computer Applications, Vels University,Chennai, India
[3]Assistant Professor, Department of Artificial Intelligence, Jeppiaar Engineering College, Chennai, India.
Email: rajakarthikmca@gmail.com

A block of transactions is a collection of recorded transactions. Each block is linked together using cryptography and includes transaction data, a timestamp, and a cryptographic hash of the block before it. This is based on distributed ledger technology and can be used with a variety of Internet-based interactive systems, including the Internet of Things, Identity Management, and Supply Chain Management. However, some privacy issues make it difficult to use in practise. This study aims to explore current security risks and privacy concerns related to the blockchain. We have talked about the present privacy-preserving cryptographic defence methods as well as the advantages and disadvantages of the cryptographic defence mechanisms utilised in the current real-world applications.

Keywords: blockchain, cryptography, cryptocurrency, privacy.

1. Introduction

Blockchain is a revolutionary advancement in decentralised information technology that ushers in a new era. In 2009, Satoshi Nakamoto posted the initial Bitcoin [1] technical specification and proof of concept (POC) on a mailing list for cryptography. The first and biggest cryptocurrency, Bitcoin continues to be the market leader in terms of trading volume and economic worth. As of Dec 2023, the market value [2] of Bitcoins was over $820 billion, and Ethereum is a decentralised open-source blockchain with smart contract features with a market valuation of $276 billion. Ethereum is the second-largest cryptocurrency and enjoys a very strong and dominant position in the cryptocurrency market after Bitcoin. The potential uses of Blockchain extend far beyond cryptocurrencies and there have been numerous improvements in developments, new test cases and applications as the technology has recently

gained more popularity, There are countless possible uses of blockchain technology including Cryptocurrency, Real estate management, Digital certificate management, E-Voting, IoT device management and security, Supply Chain, Payment Security Management, Cross Border Trade, Electronic Health Record Management, Decentralised Finance (DeFi) and many more. Although cryptocurrency applications are the most popular usage of blockchain, there are other uses as well, making it appealing for Internet of Things environments with decentralised topologies and numerous Internet-enabled devices. Data synchronisation and device management automation in IoT devices can be made simpler and faster by leveraging the blockchain (described in [3], [4], and [5]). The tracking and tracing of the products in supply chain management system can also be improved by blockchain([6], [7], [8]). Additionally, the decentralised nature of blockchain might naturally lessen the load on centralised servers that manage identification or Public Key Infrastructure(PKI) management system([9], [10],[11], [12]).Blockchain Technology will be an effective abstraction for the creation of distributed systems, but when deciding how to safeguard user's interests, it's important to take into account privacy issues including the revealing of genuine user names and transaction amounts. For instance, in the blockchain network, if the transactions and conversation between Purchasers and Vendors are not secured properly, it may result in the disclosure of crucial trade secrets of the suppliers and purchasers. Adoption of blockchain technology in supply chain management (SCM) systems is severely constrained because it is possible to determine the prices of goods from different suppliers by looking at transaction records when the blockchain is integrated with supply chain management system. As a result, suppliers will have less incentive to use this blockchain-based system. The aforementioned signs suggest that a comprehensive study and evaluation of blockchain privacy preservation is required.

2. Security Threats for Blockchain Technology

Blockchain technology generates a tamper-proof immutable ledger of transactions, but blockchain networks are still susceptible to fraud and cyberattacks. A number of hacks and frauds have been successful over the years because of recognised weaknesses in the blockchain technology. Examples include Sybil attacks, Phishing attacks, 51Pecent attacks and Routing attacks, which pose a danger to blockchains in four different ways.

A. Phishing attacks

Phishing is an effort to get a user's login credentials using fraud. Wallet key owners get emails from scammers that seem to be coming from a reputable source. The emails contain fake hyperlinks that request user's login information. If a user's login credentials or other sensitive information is compromised, both the end user and the blockchain network could suffer losses.

B. Routing attacks

Real-time, huge data transfers are necessary for blockchains. Data transfers to internet service providers(ISP's) can be intercepted by hackers. Routing attacks generally hide the danger from blockchain participants, making everything appear to be normal. However, behind the scenes, thieves have taken money or private information.

C. Sybil attacks

The primary objective of this attack is to overload the blockchain network and bring down the system by creating and using several bogus network identities. Sybil, a popular literature character name, has been identified as having a multiple identity disorder.

D. 51percent attack

It is also called as majority attack, a gang of miners or an entity will take complete control of more than 50percent of the blockchain hashing power. Though it is difficult on larger network, it is very much feasible in smaller networks which require less hashing power to defeat the majority of nodes.

3. Privacy-Preserving Solutions for Blockchain

In order to improve the anonymity of blockchain technology and also to protect user identity privacy and transaction data privacy, many researchers have come up with many blockchain privacy protection solutions. Mixing services, ring signatures, and non-interactive zero-knowledge proofs are three approaches commonly used in blockchain to maintain anonymity.

A. Mixing services

It's important to note that Bitcoin does not truly ensure anonymity because transactions employ pseudonymous addresses, which frequently makes it possible to connect one

user's transactions to another. Furthermore, in fig.1, all of the user's transactions might be made public if even one of those transactions is connected to his identity. In order to conceal their ownership, in fig.2, mixing services will accept the user coins and exchange them at random for other coin users. It is also known as laundries or tumblers. By severing the connections between addresses, mixing services enhances anonymity. No one is aware of the precise location of any given group of coins since the sources and destinations of the coins are separated. Coins from one user are exchanged at random with coins from another user is called mixing. As a result, their ownership of the coins is concealed from the spectator. Before the transactions are registered in the ledger, a mixing service is used to conceal the connections between the senders and recipients of such transactions. These mixing services do not offer any security against coin theft.

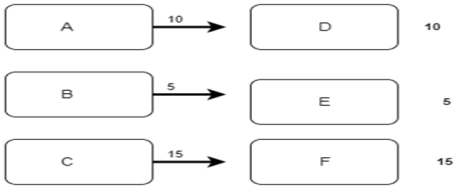

Fig. 1. Normal Transaction

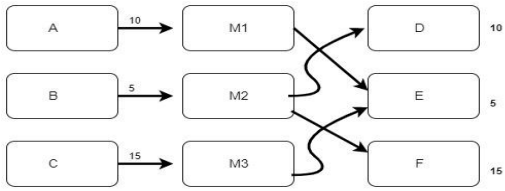

Fig.2.Transaction on Mixing Services

B. CoinJoin

If user A pays ten rupees in cash to user B, B does not know where the money came from. Later if user B gives to user C, C will not be able to figure out that user A was once owned it. But transactions in cryptocurrency are completely different and it is made of inputs and outputs.

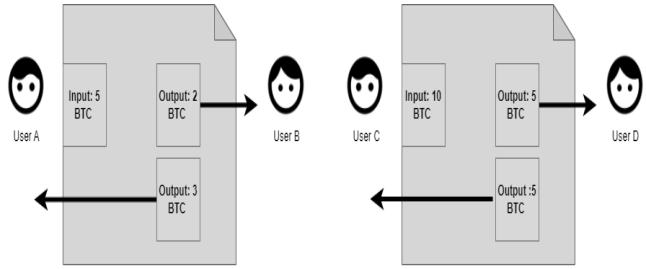

Fig. 2. A Two Different Simple Transaction

In fig-3, User A has 5 bit coins in his wallet and want to send 2 bitcoins to User B, and User C has 10 bitcoins in her wallet and wants to send 5 Bitcoins to User D. User A creates a transaction with 5 BTC UTXO (unspent transaction output) as an input and 2 BTC will be sent to user B's address as an output and the balance 3 BTC will be returned to user A's address, similarly user C creates a transaction with 10 BTC UTXO (unspent transaction output) as an input and 5 BTC will be sent to user D's address as an output and the balance 5 BTC will be returned to user C's address. It is basically like writing the details of the transaction amount and name of the participants in the bill register, the history of the transaction is not hidden and visible to everyone. As a substitute for traditional bitcoin transaction anonymization, CoinJoin [14] was put forth in 2013. It is driven by the concept of shared payment. With CoinJoin process, in fig-4, all the transactions are clubbed and executed as single transaction. The ledger will show that bit coins were paid from A and C addresses to B and D addresses. The addresses of A and C is concealed and not visible to everyone.

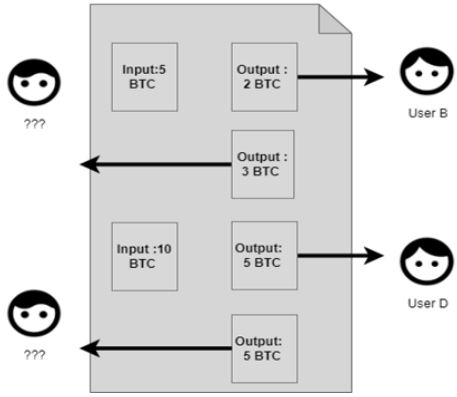

Fig. 3. A CoinJoin Transaction

There are various service providers in CoinJoin market who performs the mixing services and they charge fee for each transaction. Apart from above, user can also generate coinjoin transaction with discussing other users and make a combined payment, But it requires technical background to perform the transaction.To overcome these problems, Tim Ruffing introduced the CoinShuffle concept [15] in 2014, which further evolves the Coin-Join idea and promotes anonymity by eliminating the need for a third party to scramble transactions. CoinShuffle is a completely decentralized coin mixing protocol with anti-theft security.

C. Ring Signature

The algorithm of the ring signature is basically a kind of digital signature scheme, Any member of a group with access to the same set of keys can use the ring signature and the same was formalised by Rivest, Shamir, and Tauman[16].

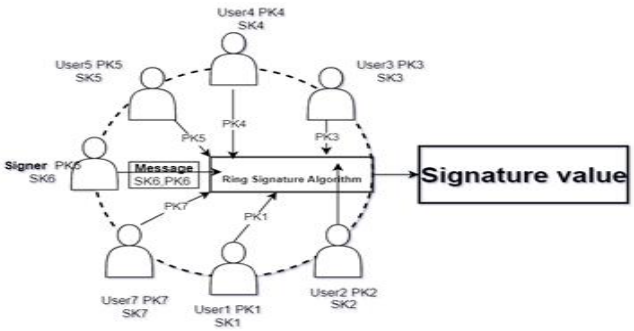

Fig. 4. Ring signature creation process

The signature contains only ring members. In this, the signer will randomly choose the public keys from multiple ring members, then combines their public and private keys and random numbers to complete the signature. The verifier of the signature will only verify that the signature comes from this signature group, but does not know the actual original signer who signed the signature. In fig.5, in the ring signature creation process, Signer chooses a group of selected participants including him and creates a ring like User1,User2…User7. Each and every participant will have the public and private key. The signer signs the message with his

own private key (SK6) and all the public keys PK1, PK2,…., PK7 of the ring members. In fig-6, The verifier will be able to know someone from the group has signed the message but he does not know who is the original signer. Therefore, this signature provides complete confidentiality and anonymity.

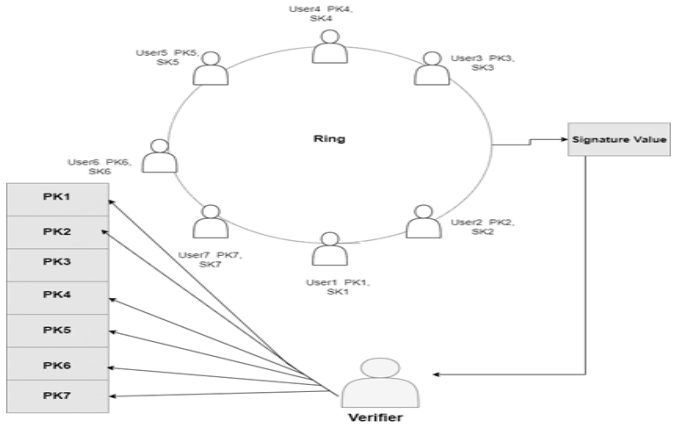

Fig. 5. Signature verification process

The ring signature algorithm must satisfy the below mentioned properties,

1. Unconditional Anonymity: The attacker will not be able to determine which member of the ring generated the signature.

2. Correctness: Everyone must confirm the signature.

3. Unforgeability: No one else in the ring could replicate the genuine signer's signature. Even if an attacker received a legitimate signature, he cannot create a fake signature for the message. In situations where the signer's identity must be protected, especially anonymous authentication in the cryptocurrency[18] and in the ad hoc group [17] , the ring signature has a number of uses. For the first time, by using the ring signature, CryptoNote[18] has concealed the source of the transaction. CryptoNote can safeguard the identity anonymity of both the payer and the payee's transactions. A transaction in CryptoNote is signed and confirmed via ring signature, and the verifiers may only confirm that the signer is a member of a particular user-set and cannot determine the signer's true identity. It can generate two distinct one-time private and public key pairs for its payee using a combination of random numbers generated by the payer and the payee's public address. For each transaction, a payer generates a one-time key, and the payee is the only one who can get their hands on the accompanying private key. The beneficiary's address becomes invisible to outsiders thanks to CryptoNote's achievement that no one can tell if two transactions are made to the same recipient. It uses traceable ring signatures [19] to track the sender who attempts to sign twice on several transactions to spend the same currency in order to inhibit double-spending attacks brought on by unidentifiable payers. Numerous Cryptocurrencies were created based on a similar concept and were inspired by CryptoNote, with Monero[20] being the most well-known.

D. Zero knowledge proof

It is an encryption technic which was coined by Goldwasser[21] in early 1980's. Prover and

verifier are the two parties involved in zero-knowledge proofs. The prover states his proof is true, without sharing any "knowledge" outside the statement, and the verifier must accept this assertion[24].Zero-knowledge protocols employes algorithms which takes any data as input and it gives result as either "true" or "false". A zero-knowledge protocol needs to fulfill the conditions mentioned below:

1) Completeness: If the given input is authentic, the zero-knowledge protocol consistently returns "true". Therefore, the proof will be accepted if the underlying claim is accurate, the prover and verifier are sincere.

2) Soundness: The zero-knowledge protocol cannot be logically tricked into returning "true" if the given input is flawed. This means that a dishonest prover cannot trick a sincere verifier into believing a bogus claim to be true.

3) Zero knowledge: The verifier should have zero knowledge of the claim and learns whether the claim is true or untrue, the verifier cannot derive the contents of the statement from the proof.

The structure of the zero-knowledge proof consists of three components: Witness, Challenge, and Response. The prover and the verifier are the two primary roles in zero-knowledge proofs. In fig-7, here Prover is called as A and the verifier is called as B, A must provide evidence that he are aware of the secret and the B must be able to confirm whether the A is telling truth or not.

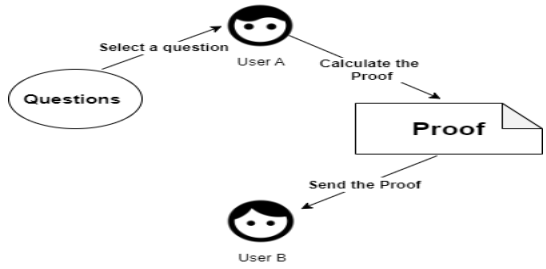

Fig. 6. Witness

in fig-7, the objective of the user A is to prove that he is aware of some secret information. Here the secret information is nothing but is a proof for the witness. A presumes that the witness is aware of the evidence, it creates a series of questions which can only be addressed by a party who have the access to the information. So, user A selects a question at random, determines the answer, and then sends it to User B to begin the verification process.

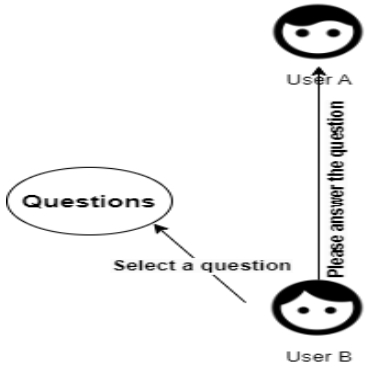

Fig. 7. Challenge

In fig-8, user B selects some more new set of questions, and asks the user A to answer.

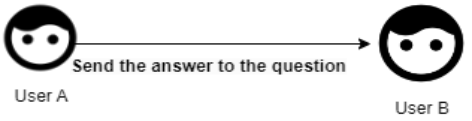

Fig. 8. Response

in fig-9, User A receives the query, determines the response, and gives it back to user B. based on the response from A, user B can determine whether A has the access to the witness or not. B again chooses additional inquiries to ensure that A is not just guessing and arriving at the correct answers only based on assumptions. Over the course of a number of iterations of this conversation, which continues until B is satisfied, the possibility of A inventing knowledge of the witness substantially lowers.

E. Non-interactive zero-knowledge proof

Although groundbreaking, interactive proving was only marginally useful because it required both parties to be present and engage in frequent interaction. Even if the verifier had full faith on the veracity of the prover, the proof would not be available for independent verification because it would need new messages between the verifier and the prover to compute a new proof. To overcome this problem, Non-Interactive Zero-Knowledge Proofs[24] involving a shared key between the prover and the verifier was introduced by Manuel Blum, Paul Feldman, and Silvio Micali. This gives the prover the ability to show their knowledge of something without actually disclosing it. In contrast to interactive proofs, non-interactive proofs simply required the transmission of one piece of information amongst the prover and the verifier. To generate a zero-knowledge proof, the prover feeds the secret data to a particular algorithm. The verifier receives this evidence and will use different algorithm to confirm that the prover is aware of the confidential information. Once the proof is accessible to anyone to verify, it decreases the communication amongst the prover and verifier.

The new ZKP-based protocol called zk-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) has the following extra features:

1. Succinct: The first important feature is, the size of proof is small and due the reduction of proof size, the verification process completes in some milliseconds.

2. Non-Interactive: The proof transcript is only one message from the prover to the verifier, thus there are no rounds of back-and-forth communication necessary.

3. Argument of knowledge: Prover should be with high computational power to verify the wrong statement.

zk-SNARK protocol consists of 1) Key generator-(G), 2) Proving key (pk), 3) Verification key (vk) and 4) Secret parameter (λ).

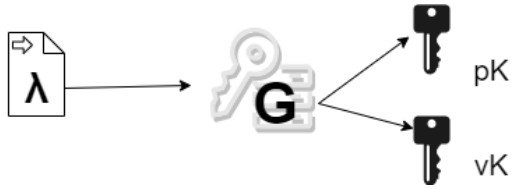

Fig. 9. Key generation process

In fig-10, first the key generator has to create two keys pk(proving key) and vk(verification key). The input to the key generator is secret parameter (λ).

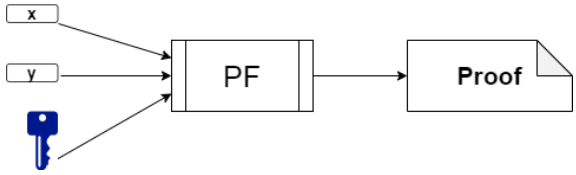

Fig. 10. Proof generation process

In fig-11, A proof is produced with the key pk and with additional inputs x(common) and w(private), proof = PF(pk, x, y).

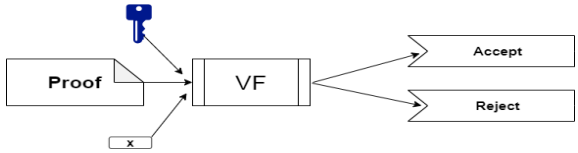

Fig. 11. Evaluation of proof

In fig-12,the verifier function(VF) takes proof as a input along with verifier key and private input, after completing the evalution process it gives result as to accept or reject. Verification= VF(vk, x, prf).

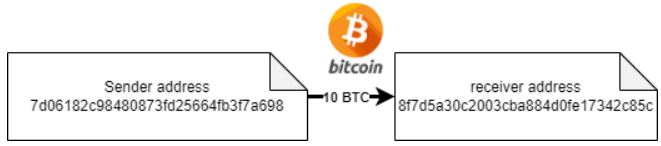

Fig. 12. Transaction without zk-SNARK

Using zk-SNARK protocol, in fig-13, The sender and receiver addresses are visible to everyone and it is visible to the public.

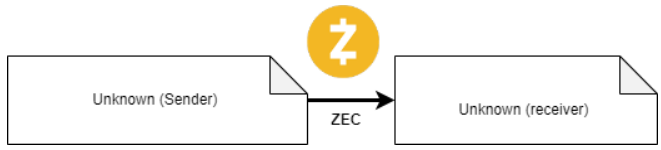

Fig. 14. Transaction with zk-SNARK

In fig-14, The sender and receiver addresses are not visible to everyone. Bitcoin transaction are fully transparent. Everyone can use the Bitcoin block explorer to check the transaction that has been sent from once BTC address to another BTC address. But in Zcash transactions can be private only if the user chooses z-address. A special view can provide selective transparency. Blockchain privacy is significantly increased by zero knowledge proof technology. This verification method will not reveal any other information about the message other than the truth of the statement. Numerous examples have demonstrated the value of zero knowledge proof in blockchain and cryptography. Many issues will be efficiently resolved if messages can be verified using zero knowledge proof. The most well-known, Zerocoin is designed with strong cryptographic technic along with zero-knowledge proofs to construct a currency pool which can be accessed by all over the world, from this currency pool, participants can easily transact enormous amount of coins without the need of third party. It is a Bitcoin expansion that provides dependable promises of anonymity which was proposed by Miers[25]. It does not rely on central banks or digital signatures to validate currencies, this feature prevents from double spending and also prevents transaction graph analysis. Zerocoin verifies the authenticity of currencies by demonstrating with zero knowledge that they are listed on an open list of reliable coins

Zerocash [26] offers even greater anonymity because it never makes public any information that connects the origin and destination of transactions. In contrast to Zerocoin, which only concealed a payment's origin and not its destination or quantity, Zerocash conceals both transaction amounts and user coin values.

Table 1. Security and Privacy Techniques Merits and Demerits

Privacy Technique	Applications	Type of Privacy	Merits	Demerits
Mixing	Bitcoin	User identity	1.Improved protection from hackers. 2.An extra layer of protection. 3.Hides the origin of the fund. 4.It is hard for hackers to trace where they come from.	1.The centralized mixing services introduce a single point of trust and failure, the service provider knows everything about the mixed transactions, and this will lead to trace or even steal coins. 2.Fee is charged for mixing by the service provide. 3. There will be delay in transactions.
Ring signature	Monero, CryptoNote	User Identity	1.No need trusted setup. 2. Internal unlink ability.	1.High cost and proof scalability. 2.The size of the transactions are very large which will rapidly increase the storage space in the whole blockchain records. 3.Keeping ring size small (i.e. more number of participants) will reduce the anonymity set size which will lead to increasing the risk of deanonymization.
Zero-Knowledge	ZeroCoin, Zerocash	Both User Identity and	1.Hides both transaction and identity details.	1.The major problem is, it requires trusted setup.

Proof		Transaction	2.Prevents transaction graph analysis.	2.In case if it is broken, adversaries can secretly mint coin.

4. Conclusion

The advantages and disadvantages of each security and privacy solution are listed in Table-1. We would like to stress the following three elements in order to accomplish security and privacy in a complicated blockchain system that must satisfy various security and privacy criteria with acceptable qualities:

1. The privacy and security of a blockchain cannot be ensured by a single technology. Therefore, it's crucial to select the appropriate solutions depending on the application environment.

2. When a new technology is incorporated into a huge, complicated system that already exists, it invariably leads to new problems or new types of attacks. These demands paying close attention to risk factors and potential harms of incorporating certain security and privacy strategies into blockchains and that is error-free or flawless in all ways.

3. Security, privacy and efficiency are continuously in competition with one another. As opposed to conventional data structures, we should promote the idea that blockchain technology can offer greater advantages. We list the typical attack vectors against blockchain in this study. We examine the solutions that are already in place to solve security and privacy concerns with blockchain technology.

References

1. "Bitcoin." https://bitcoin.org/en/.Accessed on 28-Dec-2023
2. https://coinmarketcap.com.Accessed on 30-Dec-2023.
3. S. Huh, S. Cho, and S. Kim, "Managing iot devices using blockchain platform," in Advanced Communication Technology (ICACT), 2017 19th International Conference on, pp. 464–467, IEEE,
4. A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: challenges and solutions," arXiv preprint arXiv:1608.05187,2016.
5. M. Conoscenti, A. Vetr ` o, and J. C. De Martin, "Blockchain for the internet of things: A systematic literature review," 2016.
6. H. M. Kim and M. Laskowski, "Towards an ontology-driven blockchain design for supply chain provenance," 2016.
7. K. Korpela, J. Hallikas, and T. Dahlberg, "Digital supply chain transformation toward blockchain integration," in Proceedings of the 50th Hawaii International Conference on System Sciences, 2017.
8. S. A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," 2016.
9. M. Ali, J. C. Nelson, R. Shea, and M. J. Freedman, "Blockstack: A global naming and storage system secured by blockchains.," in USENIX Annual Technical Conference, pp. 181–194, 2016.
10. C. Fromknecht, D. Velicanu, and S. Yakoubov, "A decentralized public key infrastructure with identity retention.," IACR Cryptology ePrint Archive, vol. 2014, p. 803, 2014.

11. A. Ebrahimi, “Identity management service using a blockchain providing certifying transactions between devices,” Aug. 1 2017.US Patent 9,722,790.
12. B. Qin, J. Huang, Q. Wang, X. Luo, B. Liang, and W. Shi, “Cecoin: A decentralized pki mitigating mitm attacks,” Future Generation Computer Systems, 2017.
13. Rui zhang , Rui xue and Ling liu, “Security and Privacy on Blockchain”
14. G. Maxwell, “Coinjoin: Bitcoin privacy for the real world,” accessed from https://bitcointalk.org/index.php?topic=279249.0.
15. Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate. [n.d.]. CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin. 345–364.
16. R. Rivest, A. Shamir, and Y. Tauman, “How to leak a secret,”Advances in CryptologyASIACRYPT 2001, pp. 552–565, 2001.
17. E. Bresson, J. Stern, M. Szydlo, Threshold ring signatures and applications to ad-hoc groups, in: Annual International Cryptology Conference, Springer, 2002, pp. 465–480.
18. N. van Saberhagen, “Cryptonote v 2. 0,” 2013.
19. E. Fujisaki, K. Suzuki, Traceable ring signature, in: International Workshop on Public Key Cryptography, Springer, 2007, pp. 181–200.
20. S.Noether, Ring signature confidential transactions for monero, IACR Cryptology ePrint Archive 2015 (2015) 1098.
21. S.Goldwasser, S.Micali, and C. Rackoff, “Knowledge complexity of interactive proof systems,” SIAM Journal on Computing,vol. 18, no. 1, pp. 186–208, 1989.
22. https://blockchainhub.net/blog/infographics/zcash-explained/ Accessed on 1stApril-23
23. https://www.altoros.com/blog/securing-a-blockchain-with-a-noninteractive-zero-knowledge-proof Accessed on 1stApril-23
24. M. Blum, P. Feldman, and S. Micali, “Non-interactive zeroknowledge and its applications,” in Proceedings of the twentieth annual ACM symposium on Theory of computing, pp. 103–112, ACM,1988.
25. I. Miers, C. Garman, M. Green, and A. D. Rubin, “Zerocoin: Anonymous distributed e-cash from bitcoin,” in SP ’13.
26. Zerocash: Decentralized Anonymous Payments from Bitcoin, Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, Madars Virza,2014 IEEE Symposium on Security and Privacy
27. S. Noether, A. Mackenzie, et al., “Ring confidential transactions,” Ledger, vol. 1, pp. 1–18, 2016.
28. S.-F. Sun, M. H. Au, J. K. Liu, and T. H. Yuen, “Ringct 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero,” in European Symposium on Research in Computer Security, pp. 456–474, Springer,2017.
29. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,”2008.
30. Zero-knowledge proof. Available at: https://z.cash/technology/zksnarks/ (30 march 2023).
31. https://blockchainhub.net/blog/infographics/ zcash-explained/ (30 march 2023).
32. R. C. Merkle, ``Protocols for public key cryptosystems," in Proc. IEEE Symp. Secur. Privacy, Apr. 1980, p. 122.
33. M. Bartoletti and L. Pompianu, ``An empirical analysis of smart contracts: Platforms, applications, and design patterns," in Proc. Int. Conf. Financial Cryptogr. Data Secur. Cham, Switzerland: Springer, 2017, pp. 494-509.
34. Z. Zheng, S. Xie, H. Dai, and H. Wang, ``An overview of blockchain technology: Architecture, consensus, and future trends," in Proc. IEEE Int. Congr. Big Data, Big Data Congr., Honolulu, HI, USA, Jun. 2017,pp. 557- 564.
35. D. Recordon and D. Reed, ``OpenID 2.0: A platform for user-centric identity management," in Proc. 2nd ACM Workshop Digit. Identity Manage., 2006, pp. 11-16.