Enhanced Privacy Protection in Blockchain Using SGX and Sidechains

M. Mohideen Abdulkader, S. Ganesh Kumar

Enhanced Privacy Protection in Blockchain using SGX and Sidechains

Mohideen AbdulKader M[1], S. Ganesh Kumar [2]
[1]SRM Institute of Science and Technology
[1] mm4123@srmist.edu.in
[2]SRM Institute of Science and Technology
[2]ganeshk1@srmist.edu.in

Abstract. Blockchain is a peer to peer network that is decentralized in nature. It has immutable and persistent property which make this technology more secured. Blockchain is not only suited for crypto currencies but also used for many applications like identity protection, smart contracts, health care, online polling system and much more. In addition, blockchain network holds a distributed ledger which makes all data available to every node in the network. Due to this, security and privacy protection becomes a major concern in blockchain technology. Some of existing solutions to blockchain privacy issues are homomorphice encryption, zero knowledge proofs, ring signature and multiparty computations. Though existing privacy preservation mechanisms secures the blockchain network from privacy leakage. It has limitations when implemented in large scale applications. In this paper, a three layered protection scheme is proposed to enhance the privacy of blockchain technology. This idea of three layered protection integrates randomized address generation, content erasure mechanism and IntelSGX together and forms a secure architecture. It will enhance the security and privacy of blockchain network to a greater extent.

Keywords: Blockchain Privacy, Randomized Address Generation, Cryptography, Content Erasure Mechanism, Blockchain Security, Anonymity, Distributed Ledger Technology.

1 Introduction

Blockchain is a decentralized network and append only digital distributed ledger technology. Blockchain network is secured by cryptographic algorithms which enables transfer of digital assets between the nodes. With the use of blockchain application Bitcoin was the first digital cryptocurrency built over it which was introduced by Satosi Nakamoto in 2008. Bitcoin is an open source application that allows any number of users to join the network. By joining the blockchain network these nodes can make transactions of digital currency among them [31]. Based on the characteristics and usage blockchain can be categorized into public

and private blockchain. Even though blockchain is considered as one of the secure technology there exists some privacy concerns that needs to be addressed.

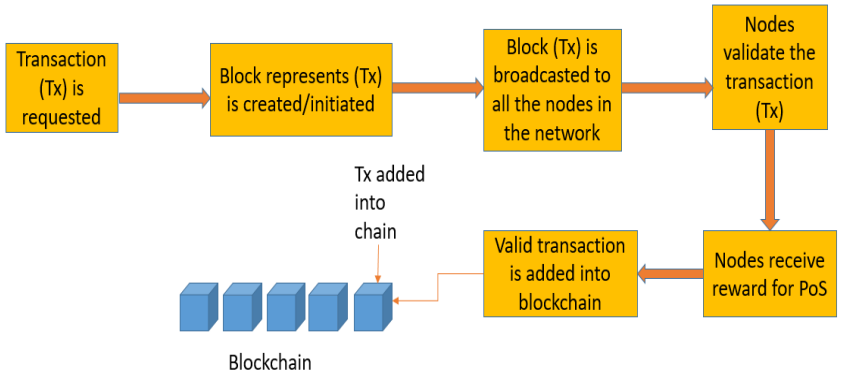

Fig. 1. Blockchain Transaction Architecture

The above figure represents the transaction that happens in a blockchain network. Initially a transaction Tx is requested in the blockchain network. Block representing the requested transaction Tx are created. This created block is broadcasted to all the participants in the network. All the nodes validate the transaction in the network by undergoing consensus mechanisms. If the transaction Tx becomes valid in it is added as a block in the blockchain. Blockchain can be classified majorly into public and private based on their characteristics and usage. Public blockchain is an open source network where any users can join that as a participant node. It have permission less access to the network and uses proof of work or proof of stake consensus mechanisms to validate the transactions. Whereas, private blockchain restrict access to only authorized users. Identity of the user is known in the private blockchain. Most private blockchain network uses proof of authority as consensus mechanisms to validate the transactions. Both public and private blockchain network holds a distributed ledger where all the information related to the transactions are stored which are visible to all other participants of the network. This makes the technology prune to security and privacy attacks [30]. In this paper, privacy challenges faced by the blockchain are analyzed based on which a three layer protection mechanism is proposed. It integrates three major methods such as randomized addressing scheme, content erasure mechanism and IntelSGX together to improve the security and privacy issues on blockchain network.

2 Security and Privacy Issues on Blockchain

Blockchain faces some major security and privacy related issues which are set backs the growth of this technology which are described as follows.

2.1 Transaction and identity privacy issue

Transaction related information and data are stored in the distributed ledger of the blockchain which is visible to all other nodes in the network. This scenario leads to privacy issues. An attacker node can make use of transaction graph analysis to identify and extract the transaction information from the ledger [1]. Sensitive information such as user identity and information on transaction amount can be extracted out by this technique. Even though anonymous address was assigned to the users, an attacker can trace all the transactions happening between the nodes from which original identity of the users can be extracted [29].

2.2 Data integrity issue

It means the risk that the distributed ledger of the blockchain is fraudulently tampered. This issue is more prominent for blockchain that deals with minimal transaction and uses chains of smaller storage size. When blockchain network uses a smaller number of nodes then it is prone to 51% attack [20]. Where, most of the nodes in the network together attacks the genuine user to tamper the data.

2.3 Data confidentiality issue

It means the risk that sensitive information are exposed to all participants in the blockchain network. Anonymous address can be assigned to the users in the blockchain to avoid the leakage of user identity information [21]. Even then, in the case of private and permissioned blockchain achieving user anonymity is quite difficult.

2.4 Issue on availability

It means the risk that participants cannot access blockchain network due to Denial of Service (DoS) attack. Availability issue depends on the number of nodes and transactions happening in that blockchain network. Private chains are generally smaller in size and easily disrupted by traditional Denial of Service (DoS) attack [22]. In addition, blockchain also faces interoperability risks when two different blockchain network need to operate together.

3 Privacy preservation mechanisms and its limitations

3.1 Bitcoin privacy by mixing services

Mixing mechanisms are mainly implemented on bitcoin applications to improve the privacy. This mechanism was proposed by Chaum and it is used in bitcoin transactions [2]. Bitcoin transaction means that two users in a blockchain network transfers a digital currency between them without the use of any central server node [6]. Unlike normal transaction bitcoin does not use any central server node. Between two transacting node an intermediate node is added in this technique. Initially, the sender node sends the transaction amount in form of bitcoins to the intermediate node. Intermediate node collects the bitcoins sent from different sender nodes [5]. Collected bitcoins are then transferred to the respective receiver node. By this method, the sender and receiver of the transaction are kept anonymous [3]. An attacker node cannot identify the exact details of the transactions happened in the network. This bitcoin mixing services are of two types such as mixing with central node and mixing without a central node [4].

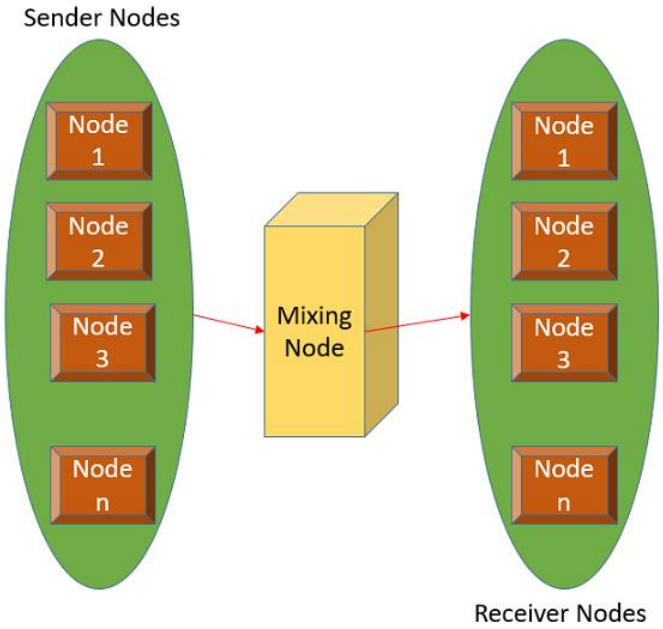

Fig. 2. Bitcoin mixing services (Source: D.Ron et al, 2013)

3.2 Privacy by zero knowledge proof mechanism

Zero knowledge proof mechanism is one of the widely used technique in block-chain network to improve the privacy which is proposed by Goldwasser et al [10]. In this technique, in order to make a transaction the sender node need to prove a statement to be true to the recipient node. If the statement is proved then it can initiate the transaction. In addition, while proving the statement no additional information should be revealed to the recipient. Transactions will be performed only after successful verification of the proof by the recipient. There are two types of zero knowledge proofs that is interactive and non-interactive zero knowledge proof mechanisms. In both the mechanisms it is difficult for the attacker to extract out the sensitive information. Interactive zero knowledge proof allows two way communication between the sender and receiver. Whereas, in non-interactive method there is no two way communication between the sender and recipient nodes.

3.3 Privacy by signature scheme

Digital signature scheme named as ring signature is proposed by Rivest et al. In this mechanism, n number of nodes form a group called as a ring. In this ring, n number of transactions happen within the ring nodes. After a successful transaction within the ring group that transaction is added as a block in the blockchain network. In ring signature scheme there is no trusted third party node. Transactions are processed in a decentralized way without the use of central or third party node [3]. In this technique, when the transaction is initiated sender signs the transaction. Sender uses its private key to sign the transaction which is initiated and it is broadcasted to all other nodes in the ring group. In the recepient end, after verifying the transaction the recepient node can identify the signer is present in the ring group or not. If it's a valid sign then transaction is processed else transaction is declined. By this way, only authorized nodes can process the transaction and unauthorized users are restricted [14]. When number of nodes in the ring increases then computation also increase in a proportional which leads to computational errors [26].

3.4 Privacy by homomorphic encryption technique

In this mechanism, computations are performed on the already encrypted cipher text which is called as homomorphic encryption. Initially, the given plaintext A is encrypted into cipher text f(A). In cipher text f(A) some computations are performed which gives the computed cipher text f(B). Now the decryption of computed cipher text f(B) gives the output plain text A which is same as the input.

Sender node sends the transaction in this way so that the receiver node gets only the final output after decryption. Sensitive information are not disclosed to any other node in the network [23]. Rivest et al proposed this mechanism which is majorly used in many blockchain network. Implementation of homomorphic encryption in blockchain network improved the privacy drastically but significantly failed for large scale blockchain applications [28].

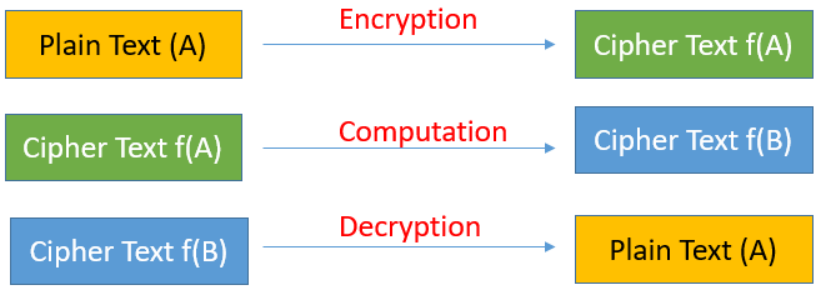

Fig. 3. Privacy by Homomorphic Encryption

3.5 Privacy by multi-party computation

In this mechanism, computations are performed by multiple nodes together without revealing their original identities. Multi-party computations are majorly used by blockchain smart contracts as it involves multiple nodes to sign a contract. It does not involve any third party node and is completely performs the computations in a decentralized way [25]. The major highlight of this technique is that sensitive data are divided into multiple segments. Each segments of sensitive data are distributed and stored in different nodes of the blockchain network. It enhances the privacy and security of the sensitive information to a greater extent [31].

4 Limitations of existing blockchain privacy mechanisms

Existing mechanisms such us bitcoin mixing services, signature scheme, multi-party computation, zero knowledge proofs and homomorphic encryption are widely used in many potential blockchain application [16]. These mechanisms

delivered a considerable protection to sensitive transactional data. Even then it has several limitations which was discussed in the below table. Based on this, new methodology for privacy preservation on blockchain is proposed.

Table 1. Limitations of existing privacy mechanisms

S. No	Privacy Mechanism	Applications	Limitations
1	Mixing Services	Mixcoin Blindcoin CoinShuffle Tumblebit	1. Prone to Denial of Service (DoS) attack. 2. Third Party Node (TTP) may disclose sensitive information
2	Zero Knowledge Proof	Zerocoin Zerocash	1. High cost for computing the proof. 2. Usage of storage space is very high.
3	Homomorphic Encryption	Confidential Transaction Paillier Encryption	1. Consumption of memory space and time complexity is very high.
4	Ring Signature	CryptoNote Monero	1. Scalability is poor. 2. Not feasible when the participants are increasing.
5	Multipart Computation	Millionaire Problem	1. High computation costs between the parties involved 2. Computation overhead and not suitable for large scale applications

Above mentioned mechanisms achieves privacy in blockchain network [7]. Moreover, these mechanisms pocess certain limitations which affects the growth rate of blockchain technology [8]. One major limitation is the use of third party node in mixing services which leads to Denial of Service (DoS) attacks [9]. Performance and efficiency of existing mechanisms need to be improved. In addition, almost all existing mechanisms affects with high computational and storage overhead. So building a large scale application with blockchain is quite difficult with these issues. Hence we propose a three layered protection scheme by integrating random address generation, content erasure mechanism and IntelSGX to overcome the limitations and to develop a highly efficient and secured privacy preserved blockchain network.

Implementing of the proposed privacy preserving scheme may bring drastic improvement in terms of efficiency, performance and security [17].

5 Proposed method for privacy enhancement

Here we propose a three layered protection scheme for privacy enhancement on blockchain network. The below mentioned figure represents the architecture of our proposed three layered protection scheme.

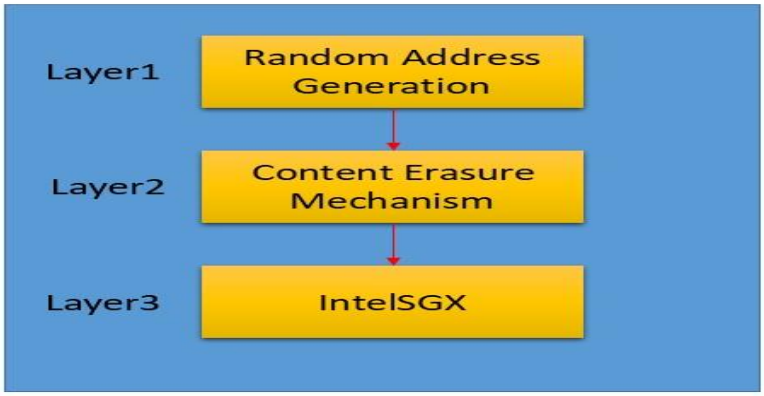

Fig. 4. Three Layered Protection Architecture

5.1 Layer 1: Random address generation

This is the first layer of the proposed scheme. Whenever a transaction Tx is requested on blockchain network. Sender node initiates the transaction Tx and sends the request to the receiver node and the recepient node accepts the transaction [12]. Many privacy mechanisms are used in between to make the user anonymized. Here in our scheme both sender and receiver which is already assigned with an anonymous address is again randomized [13]. Every time when the sender node initiates the transaction Tx, Ty and so on random address is assigned to both the sender node and reciever node. For every transaction an unique address is assigned and this is an one time unique address assigned for that particular transaction. This technique gives a complete anonymity to the sender and reciever noodes.

5.2 Layer 2: Content erasure mechanism

Transacting nodes are assigned with random address and the transaction are initiated. Transaction are carried out between the sender and the receiver. Once the transaction Tx is completed all the sensitive information stored on-chain are moved to off-chain storage [24]. Content erasure mechanism are used by which only hash pointers are made available on-chain. All the sensitive information related to the current transaction are moved to sidechains or off-chain storage. Other participants in the network will have access only to hash pointer where detailed information are kept hidden.

5.3 Layer 3: IntelSGX

Transaction information are moved from distributed ledger to the off-chain storage system. In off-chain storage these data need to be secured for which IntelSGX is used in third layer. Therefore, sensitive transaction data moved to sidechains or off-chain are secured using software guard extension (IntelSGX). SGX can be used to store the sensitive data by creating a secure storage space called enclave [11]. Only authorized users have access to enclave which is completely secured and free from attacker node [15]. Transaction information can be segregated into sensitive and non-sensitive information then sensitive information is moved to the enclaves of IntelSGX. It increases the privacy and security of the data by delivering more secured space that restricts disclosure of sensitive information. Integrating SGX improves security of transaction processing, consensus and smart contracts in blockchain technology.

Integration of this three layered protection scheme improves the privacy on blockchain to a greater extent. In addition, we use privacy preserving proof of stake concensus mechanism for validation of transactions [27]. Inclusion of this concensus mechanism improves the validation time without data explotation. By this way privacy preserving mechanisms are included at different levels of a blockchain transaction. Complete user anonymity and highly efficient data privacy can be acheieved.

7 Conclusion

Blockchain is a highly anticipated technology that are implemented to build many applications such as electronic voting, supply chain and identity preservation. Security and privacy issues in the blockchain restricts the growth rate of this

technology to a greater extent [18]. In this paper, we analysed the existing security and privacy privacy challenges of blockchain technology. Major issues on the existing mechanisms are addressed. In addition, a three layered protection scheme is also proposed for developing a highly efficient privacy preserving mechanisms. Existing privacy mechanisms of blockchain are prone to several limitations such us computation overhead, storage overhead and performance degradation [19]. Building up three layered protection may solve the existing limitations but the implementation feasibility of the proposed scheme need to be analyzed. Implementation and performance of the proposed scheme in large scale applications is the other major direction for the researchers to address.

References

1. D. Ron and A. Shamir, ‘‘Quantitative analysis of the full bitcoin transaction graph,’’ in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, vol. 7859, Nov. 2013, pp. 6–24, doi: 10.1007/978-3-642-39884-1_2.
2. L. Valentaand, B. Rowan,”Blindcoin: Blinded, accountable mixes for bitcoin” in International Conference on Financial Cryptography and Data Security,pp. 112-126, Springer, 2015.
3. Z. Wang, J. Liu, Z. Zhang, and H. Yu, ‘‘Full anonymous blockchain based on aggregate signature and confidential transaction,’’ *J. Com- put. Res. Develop.*, vol. 55, no. 10, pp. 2185–2198, Oct. 2018, doi: 10.7544/issn1000-1239.2018.20180430.
4. L. Valenta and B. Rowan, ‘‘Blindcoin: Blinded, accountable mixes for bitcoin,’’ in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2015, pp. 112–126.
5. E. B. Sasson, A.Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, “ Zerocash: Decentralized anonymous payments from bitcoin,“ in IEEE Symposium on Security and Privacy, pp.459-474, 2014.
6. “Dash is digital cash.” https://www.dash.org//.
7. G. Dong, Y. Chen, J. Fan, Y. Hao, and F. Li, ‘‘Research on privacy protection strategies in blockchain application,’’ *Comput. Sci.*, vol. 46, no. 5, pp. 29–35, May 2019, doi: 10.11896/j.issn.1002- 137X.2019.05.004.
8. Z. Liu, D. Wang, and B. Wang, ‘‘Privacy preserving technology in blockchain,’’ *Comput. Eng. Des.*, vol. 40, no. 6, pp. 1567–1573, Jun. 2019, doi: 10.16208/j.issn1000-7024.2019.06.012.
9. E. Heilman, L. Alshenibr, F. Baldimisti, A. Scafuro, and S. Goldberg, “Tumblebit: An untrusted bitcoin compatible anonymous payment hub,” in Proc, NDSS, 2017, pp.1_15.
10. S. Goldwasser, S. Micali, and C. Rackoff, ‘‘The knowledge complexity of interactive proof systems,’’ *SIAM J. Comput.*, vol. 18, no. 1, pp. 186–208, Feb. 1989, doi: 10.1137./0218012.
11. H. G. Zhang, ``Research and development of trusted computing in China," in *Proc. 3rd Asia_Paci_c Trusted Infrastruct. Technol. Conf. (APTC)*. New York, NY, USA: IEEE Computer Society, 2008, pp. 1_3.
12. U. Rajput, F. Abbas, R. Hussain, H. Eun, and H. Oh, ‘‘A simple yet efficient approach to combat transaction malleability in bitcoin,’’ in *Proc. Int. Workshop Inf. Secur. Appl.* Cham, Switzerland: Springer, 2015, pp. 27–37.

13. N. Van Saberhagen, Cryptonote v2.0, https://static.coinpaprika.com/storage/cdn/whitepapers/1611.pdf(2013).
14. D. L. Chaum, ‘‘Untraceable electronic mail, return addresses, and digital pseudonyms,’’ *Commun. ACM*, vol. 24, no. 2, pp. 84–90, Feb. 1981, doi: 10.1145/358549.358563.
15. N. Zhenyu, Z. Fengwei, and S. Weisong, ‘‘A study of using TEE on edge computing,’’ *J. Comput. Res. Develop.*, vol. 56, no. 7, pp. 1441– 1453, Jan. 2019.
16. X. Li, Y.Niu, L. Wei, C. Zhang, and N. Yu, ‘‘Overview on privacy pro- tection in bitcoin,’’ *J. Cryptol. Res.*, vol. 6, no. 2, pp. 133–149, Apr. 2019, doi: 10.13868/j.cnki.jcr.000290.
17. J.Bonneau, A.Narayanan, A.Miller, J.Clark, A.Kroll and E.W. Felten, “ Mixcoin: Anonymity for bitcoin with accountable mixes,” in International Conference on Financial Cryptography and Data Security, pp.486-504, Springer, 2014.
18. Sivaganesan, D. "Smart Contract Based Industrial Data Preservation on Block Chain." Journal of Ubiquitous Computing and Communication Technologies (UCCT) 2, no. 01 (2020): 39-47.
19. Wang, Haoxiang. "IoT based Clinical Sensor Data Management and Transfer using Blockchain Technology." Journal of ISMAC 2, no. 03 (2020): 154-159.
20. J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, ‘‘Mixcoin: Anonymity for bitcoin with accountable mixes,’’ in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, in Lecture Notes in Computer Science, 2014, pp. 486–504.
21. Miers, C.Garman, M.Green, and A.D.Rubin, “Zerocoin: Anonymous distributed e-cash from bitcoin,” *IEEE Symposium on Security and Privacy*, pp.397–411, 2013.
22. M. Fleder, M. S. Kester, and S. Pillai, ‘‘Bitcoin transaction graph analysis,’’ Feb. 2015, *arXiv:1502.01657*. [Online]. Available: https://arxiv.org/abs/1502.01657
23. T. Ruffing, P. Monero – Sanchez, and A.Kate, “CoinShuffle: Practical decentralized coin mixing for bitcoin”, in European Symposium on Research in Computer Security, pp.345-364, 2014.
24. J. Wang, C.-Y. Fan, Y.-Q. Cheng, B. Zhao, T. Wei, F. Yan, H.-G. Zhang, and J. Ma, ‘‘Analysis and research on SGX technology,’’ *J. Softw.*, vol. 29, no. 9, pp. 2778–2798, Sep. 2018, doi: 10.13328/j.cnki.jos.005594.
25. P.Todd. Stealth Addresses. Accessed: Jan. 6, 2014. [online]. Available: https: //lists.linuxfoundation.org/pipermail/bitcoin-dev2014- January/004020.html.
26. S. Hu, C. Cai, Q. Wang, C. Wang, X. Luo, and K. Ren, ‘‘Searching an encrypted cloud meets blockchain: A decentralized, reliable and fair realization,’’ in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Honolulu, HI, USA, Apr. 2018, pp. 792–800, doi: 10.1109/INFO- COM.2018.8485890.
27. R. L. Rivest, A. Shamir, and Y. Tauman, ‘‘How to leak a secret,’’ in *Proc. 7th Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, 2001, pp. 552– 565.
28. D. Chaum and V. H. Eugène, ‘‘Group signatures,’’ in *Advances in Cryptol- ogy*. Berlin, Germany: Springer, 1991, pp. 257–265.
29. R. L. Rivest, L. Adleman, and M. L. Dertouzos, ‘‘On data banks and privacy homomorphisms,’’ *Found. Secure Comput.*, vol. 4, no. 11, pp. 169–180, Jan. 1978.
30. R. Tso, Z.-Y. Liu, and J.-H. Hsiao, ‘‘Distributed E-voting and E- bidding systems based on smart contract,’’ *Electronics*, vol.8, no.4, p. 422, Apr. 2019, doi: 10.3390/electronics8040422.
31. T. Wang, ‘‘A review of the study of secure multi-party computation,’’ *Cyberspace Secur.*, vol. 5, no. 5, pp. 41–44, May 2014.