Journal of Physics: Conference Series

Decentralized Digital Certificate Revocation System Based on Blockchain

Decentralized Digital Certificate Revocation System Based on Blockchain

Aisong Zhang[1] and Xinxin Ma[1]

[1] School of Software, Beihang University, No.37 Xueyuan Road, Haidian 100191, China
E-mail: zhangaisongbuaa@163.com

Abstract. Current digital certification revocation systems are insufficient in the application scenario of multiple certification authorities (CAs), and it leads to a lack of mutual trust, access stability, and timeliness of data synchronization between CAs. We propose a decentralized digital certificate revocation system based on consortium blockchain technology with a secret sharing scheme. It can invalidate the digital certificate in special cases to protect the user's information and property security. Based on the characteristics of the decentralized consensus mechanism, consortium blockchain technology is the core technology of the system. The scheme achieves collaborative management of digital certificate revocation lists (CRLs) by multiple CAs, and introduces secret sharing scheme, further safeguarding the reliability of the maintenance process, and then the online certificate status protocol (OCSP) can be developed based on this system. This system is security, effective, and cannot be tampered. Compared with the traditional revocation scheme, it achieves trusted and reliable CRL system above multiple CAs, which can provide new ideas for the way of digital certificate revocation and expand the application range of blockchain technology.

1. Introduction

Digital certificate, a certificate that identifies the identity of the parties involved in a communication over the Internet, is a digital signature of a certificate authority (CA) that contains public key owner information and a public key that can be used to verify the identity of the communicating entity over the Internet Identity. When verifying the certificate, the user only needs to decrypt the signature with the provided public key, and then compares the result with the Hash operation on the plain text. If the result is consistent, the certificate can be proved that the certificate has not been tampered with or fraudulently used. Digital certificates can be widely used in electronic and e-commerce related activities, and can be used in the security mechanism of online payment, online shopping, online subscription, and access to secure sites and so on.

In some circumstances, digital certificates may sometimes be revoked earlier than the expiration date. When the subscriber's personal identity information changes, or the subscriber's private key is lost, leaked or suspected of being leaked, the certificate subscriber shall promptly withdraw the certificate request from the CA, and the CA shall put the certificate into the publicly released certificate revocation list in time. The revocation of the certificate also indicates the end of the life of the certificate. In addition, if the private key is accidentally leaked, other users who have obtained the private key to sign various electronic documents or protocols may imitate the digital signature. In this way, unpredictable results such as the loss of economic property may be caused. When these accidents occur, the continued use of traditional digital certificates may have a more serious impact. Thus, when verifying the validity of a certificate, we should verify whether it has been revoked or not through its CRL or OCSP server.

However, different CAs might sign the certificates, and many organizations all have their own CAs, in which case a single CA maintains a related CRL. It complicates the certificate verifier's work because one has to query to different CRL servers when verifying certificates from different CAs. What's more, it requires all CRL servers should be online all time, and the work pressure of these CRL servers might be unbalanced in different periods of time, which would cause data traffic blocked and access denied.

In this paper, we propose a decentralized digital certificate revocation system based on blockchain technology, which can be used to unite all CAs to maintain a trusted CRL whose security is based on the consensus mechanism. The system uses consortium blockchain as the core technology. Based on the characteristics of its decentralized consensus mechanism, it achieves the collaborative management of CRL for multiple CAs and introduces the secret sharing scheme to further ensure the reliability of the maintenance process.

The rest of this paper is organized as follows. Section 2 provides our Contributions. Section 3 provides the related work. Section 4 presents the innovation points and the specific process of the scheme. Section 5 provides a security analysis of this scheme. Finally, Section 6 concludes this paper.

2. Our Contributions

We propose a decentralized certificate revocation system based on blockchain technology. Our contribution can be summarized as follows.

Firstly, combining blockchain technology with digital certificate revocation mechanism and using blockchain as the core technology, the proposed scheme is optimized to be a consortium blockchain revocation mechanism with distributed consensus, strong enforceability and low fault tolerance in the untrusted multiple CAs circumstance.

Secondly, the scheme adopts a penalty mechanism different from the incentive mechanism of bitcoin, which implies that nodes in the blockchain in the system are honest. Therefore, all nodes have a consensus that the system should be stable and secure, improving security.

Thirdly, considering the need of many CA organizations to jointly maintain and update the digital certificate revocation list, this scheme creatively selects the consortium chain and introduces a secret sharing scheme to improve the fault tolerance and further safeguard the maintenance process security.

Finally, based on this scheme, OCSP system can also constructed to make it trusted above multiple CAs. In addition, as a new decentralized transaction management technology, blockchain has a wide range of application prospects. This article is not only limited to the traditional Internet finance, but also applies blockchain technology to the establishment of digital certificate revocation mechanism. The future of other regulatory system operation and maintenance programs provide a new idea.

3. Related Work

Recently, there have been many certificate revocation mechanisms proposed, which can be divided into two categories: non-voting-based mechanism and voting-based mechanism [1]. In the non-voting-based mechanism, Clulow et al. proposed a suicide method to revoke certificate by the node once it recognizes the certificate is malicious, in which the certificates of the accuser and the accused node would be revoked [2]. Liu et al. proposed the revocation method based on cluster, whose security depends on reliability and trustworthiness of the cluster head [3]. In the voting-based mechanism, Luo et al. proposed the scheme to achieve that the node is recognized as a malicious node if there are m/N nodes' accusations, which will cost a long time to finish the revocation [4]. Then Chaib et al. proposed a more efficient revocation method by assigning nodes different accusation weight [5].

The blockchain technology is widely used with the proposal of bitcoin [6] and can realize the non-temperable information record in the decentralized network. Each block contains the transactions having occurred since the last block, and a hash of the previous block in the sequence that identifies the predecessor uniquely [7], and the owner using ECDSA signs all transactions. Nodes on receiving a transaction will verify its validity and send it to all neighbours. In addition, when facing several different blockchains, nodes will adopt only one, which is the longest or the most consistent with its knowledge, as the valid blockchain and broadcast this one to its neighbours. Bitcoin nodes compete with each other to compute SHA-256 with assigned number of 0 in front of the hash result to get the reward. Besides, all nodes cannot forge a transaction as long as the underlying public/private key cryptosystem is secure [8]. Therefore, combined with blockchain technology, security research and security application also came into being [9]. For example, blockchain is used to realize privacy protection [10], and blockchain is used to implement smart contract [11].

4. Scheme Implementation

4.1. Innovation Points

4.1.1. Blacklist. Different from the incentive mechanism of bitcoin, we use the penalty mechanism in our scheme. We assume that there would not be all CAs refusing to generate a new block at the same time. In each block, the miner will assign cannum miners, who are the miners for the next block, and the number of revocations in the current block sorts them. In order to penalize a CA that refuses to post a new block or writes information that has been written to a digital certificate revocation list, the miners will create a blacklist containing the former candidate in the new block. All CAs will refuse to add its revocation information the CA is in blacklist now, unless it applies for recovery and verification after blacklistnum blocks. The probability of assuming that all cannum candidates will become offline during the same period or refuse to release a new block will be negligible. This rule will apply to cannum candidates and will be reorganized if an incident such as a refusal to release a new block or an error occurs. In addition, all spoofed CAs will be added to the blacklist with blacklistnum indicating the number of blocks in the blacklist that the penalized CA is in. Moreover, in this way, the error probability of the mechanism can be reduced.

4.1.2. System Structure. As shown in Figure 1, the CA that contains the hash value of the previous block creates the new block. All records received by this CA will be wrote in the block, including public key update, public session key, digital certificate revocation list information, and verification digital signature of share of this CA. The work CA will collect the newly released digital certificate revocation list information for each CA and generate new blocks to complete the update of the list information at any time. Blacklists of spoofed CAs in the latest blacknum are also included in the block. In order to reduce the size of the block, all the CAs will be hashed in the Merkle tree and the root is contained in the block. As a result, obsolete records will be discarded.

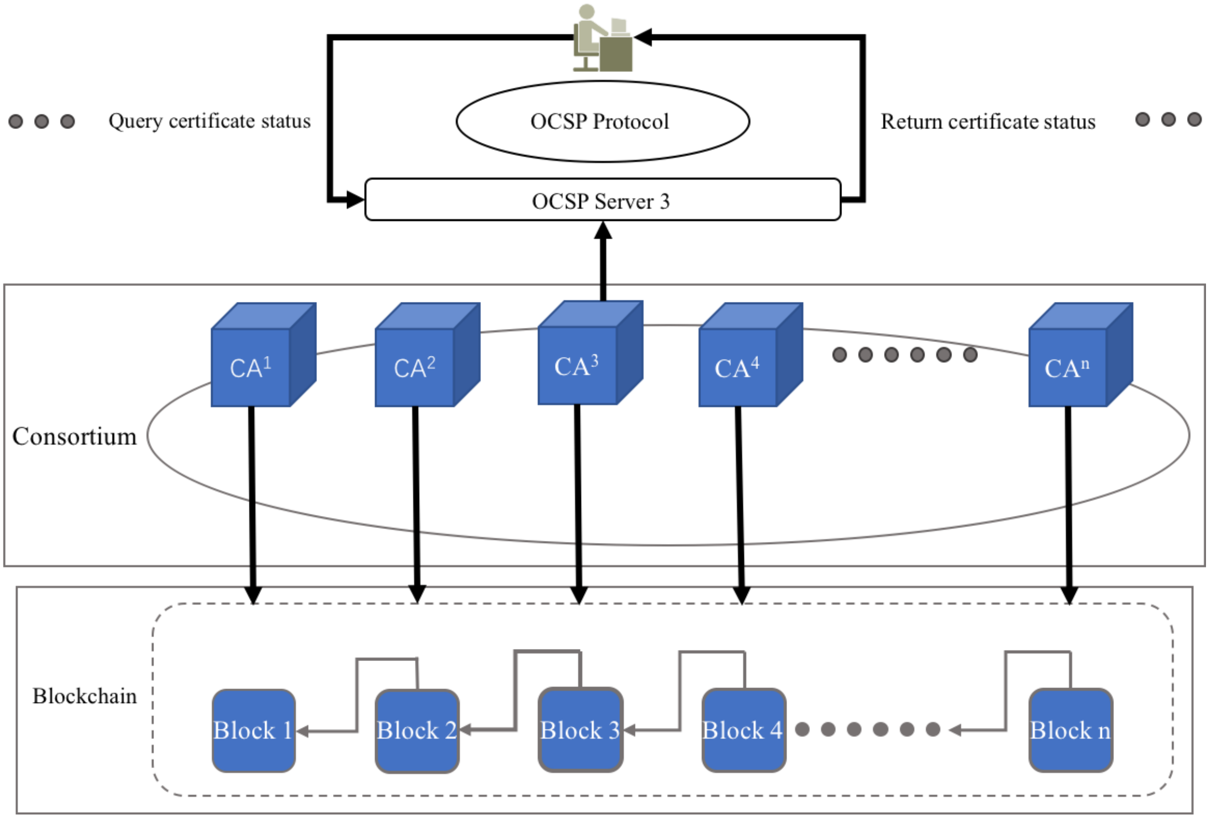
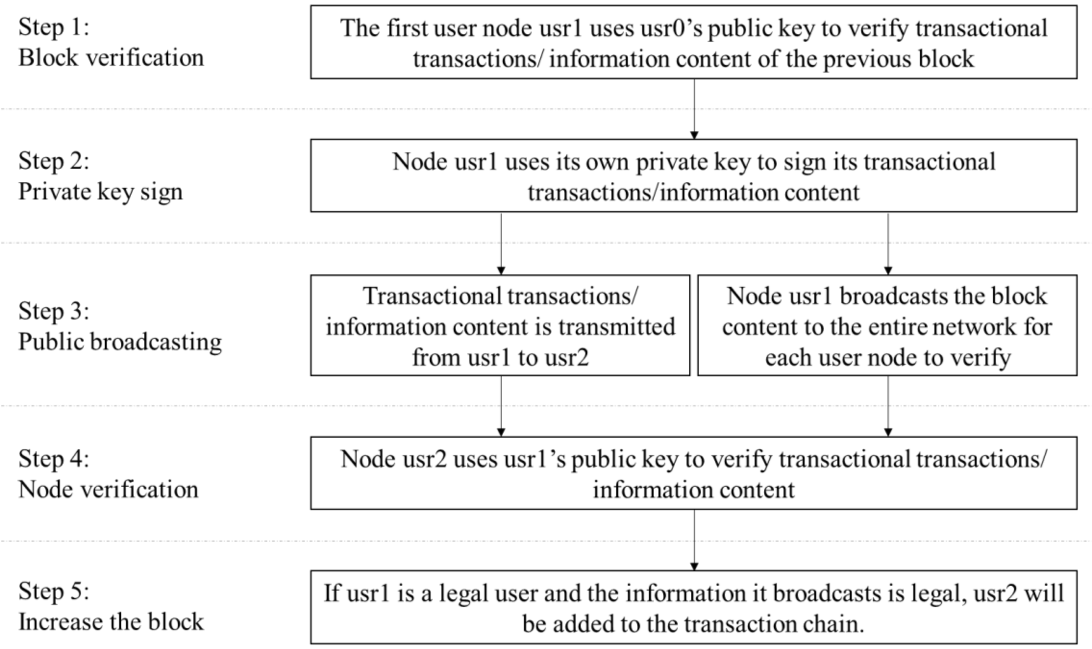


Figure 1. System architecture diagram

4.2. *Specific Process*

As shown in Figure 2, the general process steps of blockchain are as follows.



Step 1:
Block verification

The first user node usr1 uses usr0's public key to verify transactional transactions/ information content of the previous block

Step 2:
Private key sign

Node usr1 uses its own private key to sign its transactional transactions/information content

Step 3:
Public broadcasting

Transactional transactions/ information content is transmitted from usr1 to usr2

Node usr1 broadcasts the block content to the entire network for each user node to verify

Step 4:
Node verification

Node usr2 uses usr1's public key to verify transactional transactions/ information content

Step 5:
Increase the block

If usr1 is a legal user and the information it broadcasts is legal, usr2 will be added to the transaction chain.

Figure 2. The general process of blockchain

Step 1: The first user of the blockchain is node usr1, which uses the public key of usr0 to verify the information content of the previous block.

Step 2: Node usr1 usr1 uses its own private key to sign its transactional transactions/information content.

Step 3: Transactional transactions/ information content is transmitted from usr1 to usr2, and Node usr1 broadcasts the block content to the entire network for each user node to verify.

Step 4: Node usr2 uses usr1's public key to verify transactional transactions/ information content.

Step 5: If Step 4 passes the verification, it indicates that the node usr1 is a legal user and the information it broadcasts is legal, and then can be saved in the block chain. At this time, the node usr2 is also added to the transaction chain.

Here, we combined CRL digital certificate revocation mechanism with the consortium blockchain consensus mechanism to design the scheme. Consortium blockchain consensus mechanism can establish a digital certificate revocation list chain, which is jointly maintained by the consortium members. Consortium members control its writing and confirmation rights. Therefore, members will restrict each other and cooperate with each other. Based on the traditional blockchain workflow, we propose a blockchain-based digital certificate revocation scheme by adding new revocation certificate blocks and new parameter blocks Blacklist block, Candidates block, Merkle Hash Tree block.

As shown in Figure 3, specific process steps of the scheme are as follows:

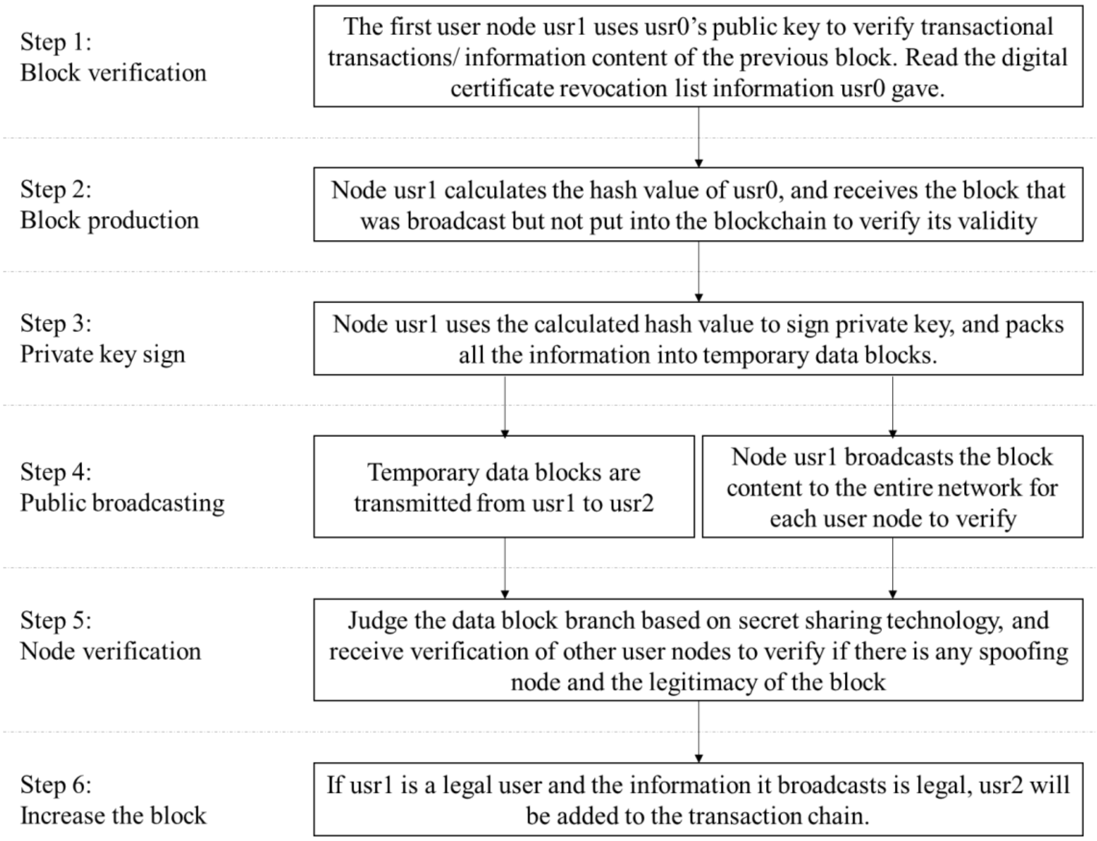

Step 1:
Block verification
The first user node usr1 uses usr0's public key to verify transactional transactions/ information content of the previous block. Read the digital certificate revocation list information usr0 gave.
Step 2:
Block production
Node usr1 calculates the hash value of usr0, and receives the block that was broadcast but not put into the blockchain to verify its validity
Step 3:
Private key sign
Node usr1 uses the calculated hash value to sign private key, and packs all the information into temporary data blocks.
Step 4:
Public broadcasting
Temporary data blocks are transmitted from usr1 to usr2
Node usr1 broadcasts the block content to the entire network for each user node to verify
Step 5:
Node verification
Judge the data block branch based on secret sharing technology, and receive verification of other user nodes to verify if there is any spoofing node and the legitimacy of the block
Step 6:
Increase the block
If usr1 is a legal user and the information it broadcasts is legal, usr2 will be added to the transaction chain.

Figure 3. The process of digital certificate revocation system scheme.

Step 1: The first user of the blockchain is node usr1, which uses the public key of usr0 to verify the information content of the previous block and reads the digital certificate revocation list information given by usr0. Moreover, the digital certificate revocation list information refers to the original digital certificate revocation list information generated in the blockchain originally given.

Step 2: Node usr1 calculates the hash value of the last data block (i.e., node usr0) and checks the validity of the block that was broadcast but not placed in the blockchain. Here, hash value calculation is a hash of the last data block in the created data chain

Step 3: The node usr1 signs the calculated hash value in a private key and packs all the information into a temporary data block. In addition, private key signature refers to usr1, which is the current node's private key for digital signature.

Step 4: While the temporary data block is transmitted from node usr1 to node usr2, the block contents are broadcasted for the entire network to facilitate verification by each user node, where broadcasting refers to the temporary data block sent to the entire network.

Step 5: Data block branch judgment, receiving verification of other user nodes, checking whether there is a deceiving node and the legitimacy of the block. When at least M of N nodes (M≤N, and cannot be too small) confirm that the operation is legal and provide a digital signature share, the verification digital signature can be decrypted so that the legitimacy is verified. Here, the node verification includes the following aspects: the legitimacy of the preamble node, the digital certificate revocation list information in the data block (no spoofing) and the situation of duplicate processing (the blockchain data exists in the form of transaction list, so this situation also called duplicate payment or double consumption problems)

Step 6: If node usr1 is a valid node and generates a valid block, add this block in the blockchain to update the list of revoked digital certificates. On the contrary, if the result of the test is that the node usr1 is a spoofing node, the penalty mechanism is implemented and added to the blacklist block of the blacklist, and the outdated information is discarded.

5. Security and Efficiency Analysis

In this system, digital signatures are used to ensure that the records are broadcasted by the exact CA. Different from the incentive mechanism in Bitcoin, we take the punishment measures, which means that the assigned miner would be put into the blacklist and be isolated in case it refused to generate a new block, to ensure the miners assigned would not strike. We assuming that more than half of the CAs are truthful, and it has a negligible probability that all assigned miners in candidate list would refuse to generate a new block. Because all honest CAs have the consensus that the system should be stable and secure to revoke their certificates, and they know if all miners' strike, it will cost more energy to re-organize the system. In addition, this system uses current mainstream cryptographic algorithm. Therefore, our scheme can guarantee the security of the system.

The number of CAs in the alliance chain is limited, so the data transmission is faster and the delay is lower. In addition, with the black list mechanism, nodes do not need to perform energy-intensive computing tasks for mining. So, this scheme can also improve efficiency.

6. Conclusion

In this paper, we proposed a digital certificate revocation scheme based on blockchain, which adopts consortium blockchain as the core technology. Based on the characteristics of its decentralized consensus mechanism, the scheme is able to make different CA form the consortium to manage the blockchain. Each CA runs a node so that multiple CA's collaborative management of CRL can be achieved. In order to ensure the reliability of the maintenance process, it introduces the secret sharing program to constraint the power between CAs. Compared with the traditional revocation scheme, our scheme is more superior and reliable. In addition, it reduces the burden of maintenance while protecting the security of the entire mechanism.

7. References

[1] Xu, H. and Wang, R. and Jia, Z., A lightweight certificate revocation scheme for hybrid mobile ad hoc networks, International Journal of Security and Its Applications, SERSC 2016, vol. 10, No. 1 (2016), pp.287-302.

[2] J. Clulow, and T. Moore, "Suicide for the common good: a new strategy for credential revocation in self-organizing systems", Sigops Oper. syst.rev, vol. 40, (2006), pp. 18-21.

[3] W. Liu, H. Nishiyama, N. Ansari, J. Yang, and N. Kato, "Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks", IEEE Transactions on Parallel & Distributed Systems, vol. 24, no. 2, (2013), pp. 239-249.

[4] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "URSA: Ubiquitous and Roubust Access Control for Mobile Ad Hoc Networks", IEEE/ACM Transactions on Networking, vol. 12, no. 6, (2004), pp. 1049 - 1063.

[5] N. Chaib, N. Lagraa, M. Yagoubi, and A. Lakas, "Unthresholded adaptive revocation technique in mobile ad hoc networks", Proceedings of Acm Symposium on Qos and Security for Wireless and Mobile Networks, Paphos, Cyprus, (2012) October 21-25.

[6] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Consulted, 2008.

[7] Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in bitcoin," in Financial Cryptography and Data Security - 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26-30, 2015, Revised Selected Papers, ser. Lecture Notes in Computer Science, R. B ̈ohme and T. Okamoto, Eds., vol. 8975. Springer, 2015, pp. 507 – 527.

[8] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in 13th IEEE International Conference on Peerto-Peer Computing, IEEE P2P 2013, Trento, Italy, September 9-11, 2013, Proceedings. IEEE, 2013, pp. 1–10.

[9] J. A. Garay, A. Kiayias, and N. Leonardos, The bitcoin backbone protocol: Analysis and applications, in Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, So_a, Bulgaria, April 26-30, 2015, Proceedings, Part II, ser. Lecture Notes in Computer Science, E. Oswald and M. Fischlin, Eds., vol. 9057. Springer, 2015, pp. 281-310.

[10] G. Zyskind, O. Nathan, and A. Pentland, Decentralizing privacy: Using blockchain to protect personal data, in 2015 IEEE Symposium on Security and Privacy Workshops, SPW 2015, San Jose, CA, USA, May 21-22, 2015. IEEE Computer Society, 2015, pp. 180-184.

[11] A. E. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, in IEEE Symposium on Security and Privacy, SP 2016, San Jose, CA, USA, May 22-26, 2016. IEEE Computer Society, 2016, pp. 839-858.