A Survey on Security and Performance Optimization of Blockchain

Dongqing Li[1(✉)], Congfeng Jiang[1], Yin Liu[2], Linlin Tang[2], and Li Yan[2]

[1] College of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou 310018, China
{ldongqing,cjiang}@hdu.edu.cn
[2] Information and Telecommunications Company, State Grid Shandong Electric Power Company, Jinan 250000, China
5918874@qq.com, 6335875@qq.com, yanli@sd.sgcc.com.cn

Abstract. This paper investigates the security issues and performance optimization of the blockchain. Security has been a hot topic in blockchain technology. Stealing cryptocurrency and disclosing the privacy of transaction process have exposed the vulnerability of blockchain in different degrees. These vulnerabilities not only caused significant losses to the project team and users, but also raised doubts about the security of the blockchain. As a formalized contract in the code, smart contracts provide a more convenient method than traditional ones, while they increase the risk of blockchain. Moreover, secure transactions should resist external attacks and protect user privacy. In addition, the performance analysis of blockchain has also aroused great interest. Therefore, this paper summarizes the related work of blockchain performance analysis from the following three aspects to promote the further research of blockchain: simulation systems of blockchain, evaluation of blockchain network and optimization of blockchain application.

Keywords: Blockchain · Smart contract · Cryptocurrency · Privacy · Performance analysis

1 Introduction

Blockchain technology is rising, which attracts more people's interest because of its decentralization, tamper proof and anonymity. Blockchain is an encrypted, ordered, block-based and only additional data structure maintained by mutual distrust peers, which have the latest copy of the database. Blockchain perfectly solves the trust crisis in the information system. Blockchain can be divided into public blockchain, private blockchain and consortium blockchain, etc. Public blockchain is that anyone can participate in the system to read data, send confirmable transactions and compete for accounting. Public blockchain is generally considered to be completely decentralized, because no person or organization can control or tamper with data. Private blockchain means that its write permission

H. Gao et al. (Eds.): ChinaCom 2020, LNICST 352, pp. 101–111, 2021.
https://doi.org/10.1007/978-3-030-67720-6_7

is controlled by an organization or institution. Due to the limited participating nodes, private blockchain can often have extremely fast transaction speeds, better privacy protection and lower transaction costs. And Consortium blockchain is jointly managed by several institutions.

There are currently three stages in the development of blockchain technology. The first stage is the era of cryptocurrency such as Bitcoin. The second stage is the main innovation brought by Ethereum, that is, the emergence of smart contracts. Finally, the third stage is the gradual integration of blockchain technology into practical production. Smart contracts reduce other transaction costs related to the contract, but this also brings some problems, such as increased risk. The immutable feature makes it impossible to repair or update once an error occurs. In Ethereum, smart contracts are written using Solidity and then compiled into bytecode, which is executed by the Ethereum virtual machine (EVM). However, multiple vulnerabilities have been found in smart contracts such as solidity, which can make it easy for criminals to steal currency. What's worse, the blockchain is not completely anonymous, because every transaction on the blockchain is public. In other words, anyone can look up all transactions and balances for each public key. Although secret transaction can hide the transaction amount, the computation and communication costs are very high, and it is detrimental to the scalability of cryptocurrency. The traceability of cryptocurrency provides financial crime protection, but it shows that the cryptocurrency lacks confidentiality and anonymity. Therefore, the privacy protection mechanism of blockchain should strike a balance between anonymity and supervision, and achieve transparency and confidentiality at the same time.

In the design and deployment of the blockchain, it is infeasible or impractical to rely on experimentation or trial-and-error to find the best architecture, configuration, or parameters [1]. Fortunately, a simulation-based system allows designers and analysts to easily explore different configurations and their impact on the operation of the blockchain system, which enables researchers to find the optimal system configuration suitable for their goals. As we all know, there is no appropriate measurement standard for the performance of the blockchain [15], but many scholars conducted a lot of research on the performance of blockchain and obtained many useful conclusions. Some work has found some bottlenecks in the performance research of blockchain platform and optimized them. As an emerging technology, blockchain provides open, transparent, traceable, and immutable data protection measures. It guarantees the security and convenience of data usage through a unique encryption and sharing mechanism, and it can also reduce the cost of application and improving efficiency.

The rest of this article is organized as follows. Section 2 outlines the vulnerabilities of smart contracts and transaction security. Section 3 summarizes the simulation, performance evaluation and optimization techniques of the blockchain. Finally, Sect. 4 concludes this paper.

2 Security Issues

As the blockchain becomes more and more popular and valuable, the security issue of blockchain becomes much more prominent. In order to enhance the security of the blockchain, researchers have proposed various methods to help discover and prevent security issues before they cause losses. Blockchain security issues include financial fairness in the presence of fraud and suspension, as well as the cryptographic concepts of confidentiality and authenticity. This section will summarize the current security issues from three aspects: smart contracts, cryptocurrency and privacy security.

2.1 Smart Contract

A smart contract is a program that runs on the blockchain, usually using a high-level programming language called Solidity. Since the contracts stored in the ledger can only be publicly obtained and cannot be modified, the attacker can obtain financial profits from the contract through the vulnerability of the smart contract. The existing work mainly focuses on the research of Ethereum smart contract attacks, because Ethereum is the most famous and common smart contract framework today. Table 1 is a comparison of these jobs. For example, Atzei et al. [4] conducted an investigation on Ethereum smart contracts, and divided them into three classes according to the level of vulnerabilities: Solidity, EVM and Blockchain levels, which were further subdivided into 12 categories of vulnerabilities. Based on the vulnerability classification of Atzei, Cook et al. [10] proposed DappGuard that can protect smart contracts from known attacks and learn new attacks. But DappGuard is just a proof of concept based on development tools. Teether [16] can automatically create exploits by analyzing four key EVM instructions, namely CALL, SELFDESTRUCT, CALLCODE and DELEGATECALL. The first two instructions will cause a direct transfer, and the last two instructions can execute any Ethereum bytecode set by the attacker in the content of the contract. Teether identifies the path leading to the critical instruction and converts the path into a set of constraints. Then, by using the constraints to find the solution, the key transaction that triggered the vulnerability can be inferred. The solc-verify [13] is a source code level verification tool. In addition to the vulnerability analyses of smart contracts on the Ethereum platform, there are also analysis of other blockchain platforms. For example, Wang et al. [30] developed a highly automated formal validator VERISOL for Solidity in the Azure blockchain workbench, which guarantees the security of smart contracts.

2.2 Cryptocurrency

An attacker can exploit the client's insecure settings to attack the blockchain. Specifically, it is to obtain cryptocurrency by executing operations that go against the user's wishes, for example, transferring Bitcoin to the attacker's address. Cheng et al. [8] designed and implemented a system that could capture an

Table 1. Comparison of different methods of protecting smart contracts

Project	Work platform	Support language	Contributions
Atzei et al.	Ethereum	Solidity and EVM bytecode	Analysis of the security of Ethereum smart contracts
DappGuard	Ethereum	Solidity	Propose design solutions for real-time monitoring and protection systems
Teether	Ethereum	EVM bytecode	Automatically exploit contract vulnerabilities
Solc-verify	Ethereum	Boogie	Modular validator for implementing smart contracts
VERISOL	Azure	Solidity	Verify and find errors in smart contracts

attacker's actual malicious behavior in Ethereum, which could be an attack stealing Ether. To avoid the impact of vulnerabilities and protect cryptocurrencies from being stolen, a lot of studies analyzed the vulnerabilities in existing cryptocurrency wallets. Notary [3] is a system composed of both hardware and software architecture, which contains three domains: kernel domain, agent domain and communication domain. Notary's switch design based on separation and reset avoids security loopholes in cryptocurrency hardware wallets, thereby improving application security.

In order to track illegal cryptocurrency activities, DBSCAN clustering technology is applied to the content of fraud websites to find out the types of prepaid and phishing fraud, so as to further understand these cryptocurrency scams. Due to the transparency of the blockchain, it is easy to analyze illegal gains and find further links before activities. Phillips et al. [23] found five different types of fraud on more than 1000 websites.

2.3 Privacy and Security

In the early blockchain systems, such as Bitcoin, Ethereum and Hyperledger, the capital flow and transaction amount of all transactions are publicly disclosed on the blockchain, so as to reach a consensus quickly for each node. Parties can use pseudonym public key to protect their real identity and increase their anonymity; however, these blockchain systems can only provide simple unlinkability. Attackers can link to the user's real identity in the real world through big data analysis, address clustering and network analysis. In fact, the main resistance to the

widespread use of decentralized smart contracts and cryptocurrencies is the lack of privacy protection. Therefore, how to achieve a balance between anonymity and minimum regulation is still a challenge for blockchain.

In order to improve the privacy protection of blockchain system, some mixing technology-based solutions have been proposed, but malicious central mixing nodes will leak the privacy of participants and even steal digital assets. For protecting the privacy of participants, Valenta et al. [29] designed Blindcoin, which integrates blind signature into mixcoin. The central mixing node only provides mixing services, but cannot link the input and output of transactions. For preventing the central hybrid node from stealing participants' assets, CoinSwap [20] establishes a connection between the escrow transaction and the corresponding redemption ones through hashing lock, and the Mixcoin [6] uses signature-based accountability technology.

Encryption is the most common solution in privacy protection. A privacy data storage protocol is established based on ring signature on elliptic curve, and the complete anonymity of ring signature is used to ensure the data security and user identity privacy in blockchain applications [18]. However, kumaret et al. [17] emphasized that attackers can still link the transaction address to the real identity when the anonymous size set in the ring signature is small. In order to ensure its unlinkability, a large anonymous set can be selected, but this will significantly increase the storage cost of transactions. RingCT 2.0 [26]is a novel ring signature mechanism designed with an accumulator tool that balances efficiency and privacy issues in Monero.

3 Performance Evaluation and Optimization

For numerous practical reasons, such as multi-parameter and various consensus mechanisms, it's difficult to find the appropriate design and deployment for the blockchain. Simulation of blockchain system is a good choice, which can help designers optimize parameters and evaluate the performance of planned blockchain network by simulating a real operating environment. There is a lot of work to help us better plan and design a scalable, stable and flexible blockchain network. This section will summarize the current blockchain performance issues from three aspects: simulation, performance analysis and performance optimization.

3.1 Simulation

In order to promote the design and research of blockchain networks, many practical simulation tools have been proposed. Table 2 shows the different blockchain goals of the simulation system. For example, BlockSim [1] is a discrete event simulation framework that focuses on modeling methods in the Bitcoin blockchain through the proof-of-work protocol and the longest chain rule. The simulation framework proposed by Chitra et al. [9] is to use agent-based simulation in the

Table 2. Different blockchain goals of the simulation system

Model	Work	Contributions	Condition
BlockSim	Bitcoin	Explore different configurations and their effects on the behavior of blockchain systems through simulation-based models	Simulation
Agent-Based Simulations	Kadena's Chainweb	Evaluate blockchain protocol claims and measure network operations through agent-based adversarial simulation	Simulation
SimBlock	Bitcoin	Simulate a peer-to-peer network of a public blockchain composed of thousands of nodes, of which the parameters of the blockchain and its network can be flexibly configured	Simulation
BlockSIM	Ethereum or Hyperledger	Help blockchain architects better evaluate the performance of planned private blockchain networks and determine the optimal system parameters for their purposes through the run scenario	Simulation
BlockZoom	Blockchain application	Provide a reproducible environment for experimental distributed ledger technology and intelligent contract applications	Real

blockchain algorithm transaction protocol, which is applied to Kadena's Chainweb. This technology can effectively monitor and evaluate the risks in real-time blockchain systems. BlockSIM [22] can accurately model and test the stability time and transaction throughput of the blockchain under a given scenario. SimBlock [5] and BlockZoom [25] are systems for large-scale blockchain networks. Most of the test methods are implemented in a simulator or through a small local blockchain network, but BlockZoom can test the performance of the blockchain under a real scenario.

Table 3. Comparison of different blockchain performance analysis methods

Project	Goal	Scenario	Metrics
Blockchain-Enabled Wireless Internet of Things	Communication and security	Blockchain-enabled wireless IoT system	SINR, TDP transmission success rate, overall communication throughput and security
Scalable Access Management in IoT Using Blockchain	Scalability	Distributed IoT management system based on Ethereum	Throughput, latency and scalability
Blockchain in VANET	The impact of mobility	Vehicle Ad Hoc Network with Blockchain System	The probability of successfully adding a block to the chain, the stability of the rendezvous, and the number of blocks exchanged during the rendezvous
BLOCKBENCH	Data processing capability	Ethereum, Parity and Hyperledger Fabric	Throughput, latency, scalability, fault tolerance and safety indicators
DAGBENCH	Evaluate the performance of the DAG distributed ledger	IOTA, Byteball and Nano	Throughput, latency, scalability, success indicators, resource consumption, transaction data size, transaction fees

SINR: signalto-interference-plus-noise ratio; TDP: transaction data packet

3.2 Performance Analysis

Blockchain has characteristics like invariance and transparency, which means it has the potential to be a data processing platform. Therefore, BLOCKBENCH [11] conducted a comprehensive evaluation of Ethereum, Parity, and Hyperledger Fabric in order to understand the performance of a private blockchain with Turing-complete smart contracts on data processing workloads. The decentralized blockchain uses many encryption technologies to ensure that the data in the ledger cannot be tampered with. It not only provides a way to ensure data security for mutually untrusted nodes of the Internet of Things, but also reduces the high maintenance cost. Therefore, the blockchain can be used in the Internet of Things and vehicle ad hoc networks. However, the existing performance analysis for the blockchain cannot be directly applied to the performance analysis of the Internet of Things system or the vehicle ad-hoc network. Therefore, Sun

et al. [27] and Novo et al. [21] focus on the performance of the Internet of Things supporting the blockchain. Similarly, Kim et al. [15] studied the performance of the blockchain system in the vehicle ad-hoc network, because mobility will pose different challenges to the performance of the blockchain.

DAG develops rapidly by virtue of its scalability and resource efficiency. Directed acyclic graphs are block-free, just store transactions as vertices of the graph, so transactions can be processed immediately without waiting for block composition. Most of the current performance analysis methods are for the two representative blockchains, Bitcoin and Ethereum. DAGBENCH [12] is the first framework to comprehensively evaluate DAG distributed ledgers. Table 3 compares these performance analysis methods.

3.3 Performance Optimization

After Sun [27], Javaid [14] and others fully studied, blockchain system models and performance analysis, the performance is further optimized. For example, Sun et al. [27] proposed an algorithm based on performance analysis to optimize the deployment of communication nodes in a blockchain system to achieve maximum transaction throughput. The transaction flow in Hyperledger Fabric follows the execution-sequence-verification model, and many previous performance studies have emphasized that the verification phase is one of its main contributions to latency. Javaid et al. [14] and Thakkar et al. [28] analyzed the delay of Fabric, and then redesigned the verification or submission phase of Fabric.

Although blockchain has many advantages, it also has some obvious shortcomings. To resolve these shortcomings, scholars have put forward corresponding solutions. For example, Setty et al. [24] propose VOLT to improve the insufficient security, slow speed and high cost caused by mining of blockchain. The number of blockchains is constantly increasing, but they are all independent and unconnected. Moreover, the current cross-blockchain operation technology is very limited, which hinders asset transfer and data exchange between different blockchains. This brings challenges to both users and developers. Realizing the interoperability of the blockchain is a great advancement of the blockchain. Dextt [7] implements the interaction between blockchains, in which the deterministic cross-blockchain token transfer protocol is used to achieve the ultimate consistency of cross-blockchain token transfer. It is undeniable that the performance of the blockchain is limited by the global consensus demand. Most solutions assume that the blockchain is accessed synchronously, but Teechain [19] is the first secure payment network that proposes asynchronous blockchain access. Many blockchains are now subject to severe architectural constraints, because of not only the sequential execution of transactions to ensure consistency but also the confidentiality of data. OXII and ParBlockchain [2] are proposed to support distributed applications with conflicting workloads. OXII is a new permissioned blockchain sorting-execution paradigm. It first generates a dependency graph for transactions within a block, allowing parallel execution of non-conflicting transactions, and achieving higher concurrency. ParBlockchain

Table 4. Comparison of different blockchain performance analysis methods

Scenario	Contributions	Optimization design
Blockchain-enabled wireless IoT system [21]	Maximize transaction throughput and determine the best full-featured node deployment of the blockchain system	Design algorithm to find optimal FN density
Hyperledger Fabric [14]	Optimize the delay in the verification phase	Use chaincode caching and parallel database read and write
Hyperledger Fabric [28]	Optimize the delay of verification phase and submission phase	Use MSP cache, block parallel VSCC verification, CouchDB batch read/write during MVCC verification and submission
VOLT [24]	Realize a safe and resource-efficient blockchain network	Building blockchain service providers and Caesar consensus, etc.
Cross-blockchain [7]	Cross-blockchain token transfer	Witness contest, VETO transaction, etc.
Teechain [19]	Implement a payment network that uses asynchronous blockchain access operations and provides dynamic deposits	Dynamic deposits of treasury bonds, payment with asynchronous blockchain access and commission chain
ParBlockchain [2]	Handling workloads with conflicting transactions	Generate dependency graphs for transactions within the block, allowing parallel execution of non-conflicting transactions

is a permissioned blockchain specially designed for the OXII paradigm. Table 4 shows the methods of blockchain performance optimization by different studies.

4 Conclusion

In this survey paper, we analyzed the current research status of blockchain security and performance optimization. Firstly, the classification of blockchain security vulnerabilities and attack prevention technologies are analyzed, then the methods to protect user privacy in blockchain are discussed, and finally, the research on performance evaluation and optimization of blockchain is summarized. With the further development of blockchain, it will have more complete solutions and wider applications.

Acknowledgment. This work is supported by the National Natural Science Foundation of China (No. 61972118).

References

1. Alharby, M., van Moorsel, A.: BlockSim: a simulation framework for blockchain systems. ACM SIGMETRICS Perform. Eval. Rev. **46**(3), 135–138 (2019)
2. Amiri, M.J., Agrawal, D., El Abbadi, A.: ParBlockchain: leveraging transaction parallelism in permissioned blockchain systems. In: 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), pp. 1337–1347. IEEE (2019)
3. Athalye, A., Belay, A., Kaashoek, M.F., Morris, R., Zeldovich, N.: Notary: a device for secure transaction approval. In: Proceedings of the 27th ACM Symposium on Operating Systems Principles, pp. 97–113 (2019)
4. Atzei, N., Bartoletti, M., Cimoli, T.: A survey of attacks on ethereum smart contracts (SoK). In: Maffei, M., Ryan, M. (eds.) POST 2017. LNCS, vol. 10204, pp. 164–186. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-662-54455-6_8
5. Banno, R., Shudo, K.: Simulating a blockchain network with SimBlock. In: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 3–4. IEEE (2019)
6. Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J.A., Felten, E.W.: Mixcoin: anonymity for bitcoin with accountable mixes. In: Christin, N., Safavi-Naini, R. (eds.) FC 2014. LNCS, vol. 8437, pp. 486–504. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45472-5_31
7. Borkowski, M., Sigwart, M., Frauenthaler, P., Hukkinen, T., Schulte, S.: DeXTT: deterministic cross-blockchain token transfers. IEEE Access **7**, 111030–111042 (2019)
8. Cheng, Z., et al.: Towards a first step to understand the cryptocurrency stealing attack on ethereum. In: 22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019), pp. 47–60 (2019)
9. Chitra, T., Quaintance, M., Haber, S., Martino, W.: Agent-based simulations of blockchain protocols illustrated via kadena's chainweb. In: 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 386–395. IEEE (2019)
10. Cook, T., Latham, A., Lee, J.H.: DappGuard: active monitoring and defense for solidity smart contracts (2017). Accessed 18 July 2018
11. Dinh, T.T.A., Liu, R., Zhang, M., Chen, G., Ooi, B.C., Wang, J.: Untangling blockchain: a data processing view of blockchain systems. IEEE Trans. Knowl. Data Eng. **30**(7), 1366–1385 (2018)
12. Dong, Z., Zheng, E., Choon, Y., Zomaya, A.Y.: DAGBENCH: a performance evaluation framework for DAG distributed ledgers. In: 2019 IEEE 12th International Conference on Cloud Computing (CLOUD), pp. 264–271. IEEE (2019)
13. Hajdu, Á., Jovanović, D.: SOLC-VERIFY: a modular verifier for solidity smart contracts. In: Chakraborty, S., Navas, J.A. (eds.) VSTTE 2019. LNCS, vol. 12031, pp. 161–179. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-41600-3_11
14. Javaid, H., Hu, C., Brebner, G.: Optimizing validation phase of hyperledger fabric. In: 2019 IEEE 27th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), pp. 269–275. IEEE (2019)

15. Kim, S.: Impacts of mobility on performance of blockchain in VANET. IEEE Access **7**, 68646–68655 (2019)
16. Krupp, J., Rossow, C.: teEther: gnawing at ethereum to automatically exploit smart contracts. In: 27th USENIX Security Symposium (USENIX Security 2018), pp. 1317–1333 (2018)
17. Kumar, A., Fischer, C., Tople, S., Saxena, P.: A traceability analysis of Monero's blockchain. In: Foley, S.N., Gollmann, D., Snekkenes, E. (eds.) ESORICS 2017. LNCS, vol. 10493, pp. 153–173. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-66399-9_9
18. Li, X., Mei, Y., Gong, J., Xiang, F., Sun, Z.: A blockchain privacy protection scheme based on ring signature. IEEE Access **8**, 76765–76772 (2020)
19. Lind, J., Naor, O., Eyal, I., Kelbert, F., Sirer, E.G., Pietzuch, P.: Teechain: a secure payment network with asynchronous blockchain access. In: Proceedings of the 27th ACM Symposium on Operating Systems Principles, pp. 63–79 (2019)
20. Maxwell, G.: CoinSwap: transaction graph disjoint trustless trading, October 2013
21. Novo, O.: Scalable access management in IoT using blockchain: a performance evaluation. IEEE Internet Things J. **6**(3), 4694–4701 (2018)
22. Pandey, S., Ojha, G., Shrestha, B.: BlockSim: a practical simulation tool for optimal network design, stability and planning. In: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 133–137. IEEE (2019)
23. Phillips, R., Wilder, H.: Tracing cryptocurrency scams: clustering replicated advance-fee and phishing websites. arXiv e-prints (2020)
24. Setty, S., Basu, S., Zhou, L., Stephenson, J., Venkatesan, R.: Enabling secure and resource-efficient blockchain networks with volt. Technical report, MSR-TR-2017-38, Microsoft, August 2017. https://www.microsoft.com/en-us/research/publication/enabling-secure-resource-efficient-blockchain-networks-volt/
25. Shbair, W.M., Steichen, M., François, J., State, R.: BlockZoom: large-scale blockchain testbed. In: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 5–6. IEEE (2019)
26. Sun, S.-F., Au, M.H., Liu, J.K., Yuen, T.H.: RingCT 2.0: a compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency Monero. In: Foley, S.N., Gollmann, D., Snekkenes, E. (eds.) ESORICS 2017. LNCS, vol. 10493, pp. 456–474. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-66399-9_25
27. Sun, Y., Zhang, L., Feng, G., Yang, B., Cao, B., Imran, M.A.: Blockchain-enabled wireless Internet of Things: performance analysis and optimal communication node deployment. IEEE Internet Things J. **6**(3), 5791–5802 (2019)
28. Thakkar, P., Nathan, S., Viswanathan, B.: Performance benchmarking and optimizing hyperledger fabric blockchain platform. In: 2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), pp. 264–276. IEEE (2018)
29. Valenta, L., Rowan, B.: Blindcoin: blinded, accountable mixes for bitcoin. In: Brenner, M., Christin, N., Johnson, B., Rohloff, K. (eds.) FC 2015. LNCS, vol. 8976, pp. 112–126. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48051-9_9
30. Wang, Y., et al.: Formal specification and verification of smart contracts for azure blockchain. arXiv preprint arXiv:1812.08829 (2018)