Educational Administration: Theory and Practice
2024, 30(4), 7551-7557
ISSN: 2148-2403
https://kuey.net/

Research Article

Blockchain-Based Trust Mechanism For Empowering And Augmenting The Cloud

Vandana Rao*

*Research Scholar, Janardan Rai Nagar Rajasthan Vidyapeeth University in Udaipur, Rajasthan. Email ID: vandanak30k6@gmail.com

Citation: Vandana Rao, (2024), Blockchain-Based Trust Mechanism For Empowering And Augmenting The Cloud, *Educational Administration: Theory And Practice, 30(4), 7341-7346,* Doi: 10.53555/kuey.v30i4.2608

ARTICLE INFO

ABSTRACT

Cloud computing (CC) has become a revolutionary approach that provides the ability to scale, adapt, and save costs while managing computational resources. Nevertheless, worries over the protection, accuracy, and reliability of data in cloud services continue to exist. Conventional centralized methods of trust management frequently fail to adequately handle these challenges in a comprehensive manner. The primary obstacles encountered by conventional trust mechanisms in cloud environments, including vulnerabilities such as single points of failure, lack of transparency, and susceptibility to malicious assaults. Blockchain is an emerging and promising decentralized framework alongside distributed computing paradigm. Hence, blockchain technology (BCT) is highly appropriate for building a distributed alongside decentralized trust framework. The study examines the fundamental concepts and capabilities of BCT that allow it to be highly suitable for improving trust in CC. The features encompassed are decentralization, immutability, transparency, and cryptographic security. This study provides a detailed discussion of several consensus algorithms, smart contract frameworks, and distributed ledger technologies that are often used in trust mechanisms based on blockchain.

Keywords: Blockchain Technology; Cloud Computing; Trust Mechanism; Empowering; Augmenting

1. INTRODUCTION

In recent times, there has been a significant focus on BCT for its use in applications that demand decentralized and heightened security aspects. The rapid progress in the utilization of BCT is opening up opportunities for future generations and emerging sectors in commerce and finance. Blockchain is a decentralized, publicly accessible, and unchangeable database used to secure different transactions. This technology primarily depends on a peer-to-peer (P2P) system design wherein the transaction data is decentralized and not controlled by any centralized body. Aside from blockchain, another dominant technology in today's society is CC (Kowalski et al., 2021).

CC has attained noteworthy attention recently because to its infinite resource sharing and improved user experience. It is considered a prominent research topic in the field of IT, and its substantial commercial value is gradually becoming apparent. Nevertheless, CC systems have faced significant challenges in terms of trust and security. In 2016, Cloudflare, a prominent provider of cloud security services, disclosed a significant flaw in its software that led to the unauthorized exposure of sensitive data. This incident impacted a minimum of 2 million websites, including those of renowned internet companies like Uber alongside 1password. Failures within Microsoft Azure public cloud storage inside March 2017 disrupted cloud company operations for about 8 hours. A security breach occurred in June 2017at AWS, leading to the unauthorized disclosure of personal material belonging to 200 million registered voters in the United States (Trivedi et al., 2021).

A. Three Major Trust Risks in Cloud

- Control loss: Upon uploading their data, code, along with operating procedures to remote cloud servers, users surrender control over them.
- Lack of transparency: CC seems as a black box to customers who are unaware of its core working methods, which raises concerns regarding privacy handling.
- Insufficient security guarantee: While many cloud service providers claim to have Service Level Agreements (SLAs) that guarantee a certain level of service consistency, along with security, along with privacy, the specifications provided in these SLAs are often ambiguous and lacking in specificity.

BCT, as an up-and-coming decentralized framework alongside distributed computing paradigm, has garnered significant attention alongside experienced rapid development due to the increasing popularity of digital currency.

B. Benefits of Blockchain

- The upkeep of trust connections is not reliant on a 3rd-party center, yet the resilience of the system cannot be compromised by the actions of a few nodes.
- The working standards and data records are accessible, clear, and can be easily followed and traced.
- The chain data structure alongside consensus methods guarantee trust evidence's integrity, reliability, and security.

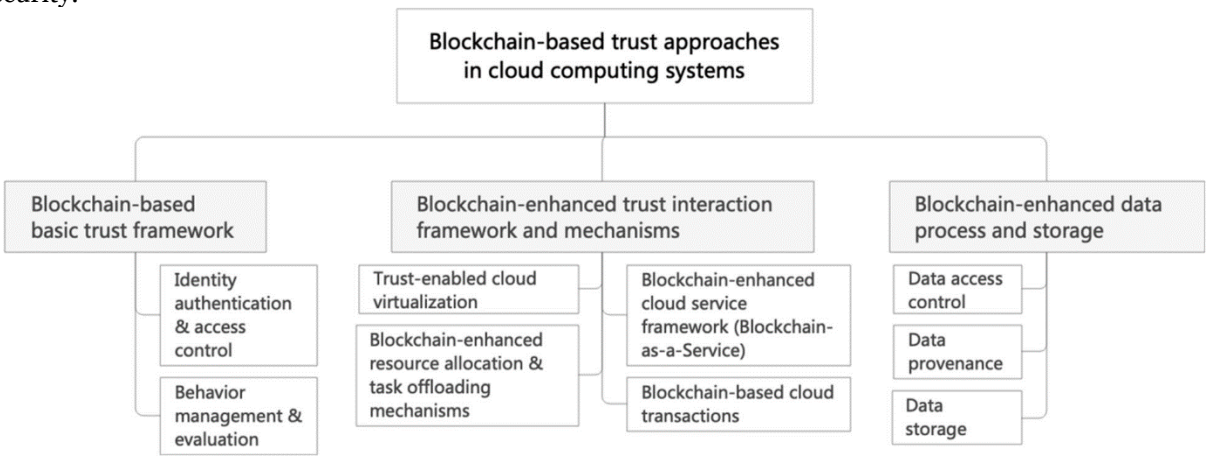


Figure 1: Blockchain-grounded trust tactics within CC systems (Yin et al., 2021)

Blockchain offers a novel approach to creating cloud trading environments that are enabled by trust. So far, a number of trust management methods based on blockchain were offered (Yin et al., 2021). Recent research has unequivocally demonstrated the significant benefits of blockchain-based systems. The primary aim of this study is

i) To extensive evaluation of trust mechanisms based on blockchain in a CC context.
ii) To explore the integration of BCT in various CC implementation modes, thereby pushing CC's boundaries.
iii) To identify those areas of research that have not yet been explored and propose potential avenues for future investigation in the field of trust management within CC using BCT.

2. LITERATURE REVIEW

Several surveys on trust mechanisms in CC settings have already been conducted.
Rawashdeh et al., (2018), presented a comprehensive overview of trust models that were previously used in cloud systems. Matin et al., (2018), have examined the most advanced trust evaluation skills within CC systems. BCT, specifically its application in E-currency, attracted considerable attention from scholars. Currently, there was a plethora of blockchain reviews available. Xiao, et al., (2020), specifically examined the distributed consensus system in blockchain. A comprehensive review on the integration of blockchain alongside ML in communication along with network systems was presented in Paper (Liu et al., 2020). Gai, et al., (2019), examined the infrastructure of cloud services based on BCT and performed a performance comparison from both software and hardware viewpoints. A study conducted by Yang et al., (2019), investigated blockchain's integration with edge computing. The study covered several aspects, including the concept, requirements, framework, and obstacles associated with this combination.
There is a scarcity of surveys or taxonomy that have specifically examined trust solutions based on blockchain in CC platforms. Thus, this study adopts a different viewpoint that not only improves upon prior studies but also concentrates on utilizing BCT to enable trust in managing services and resources in cloud systems.

3. RESEARCH CHALLENGES

- Most trust models happen to be centralized, while those declaring they are decentralized rely on 3rd-party certification center or even trust. This reliance on a 3rd-party introduces numerous security issues, including one failure point, overloading, alongside loss of credibility.
  The lack of accessibility and traceability of trust evidence restricts its availability to all parties, resulting in unconvincing and partially trusted trust evaluation outcomes.
- Unreliability of trust assessment outcomes: The current trust models have limited descriptive power, mostly relying on numerical score for trust data. This approach is inadequate for real-world applications, like E-commerce, where feedback from users often contains many data kinds, including both quantitative and textual information.

- Not as adaptable: The process of trust decision-making relies on subjective techniques, like expert scoring and the average approach. As a result, these models are subjective, lacking scientific rigor and malleability.

4. BLOCKCHAIN BASED TRUST MECHANISM

A. Blockchain-based cloud service framework

Service Level Agreements (SLAs) sometimes lack credibility and fail to be applied automatically as necessary in real-world scenarios. The Nash equilibrium game theory was utilized to facilitate negotiations between cloud providers and consumers, with the aim of minimizing gas usage. In the suggested architecture, observers were the regular nodes in the BC network, who earned revenues by overseeing cloud transactions. So, they facilitated transactions to occur according to the agreed terms and ensured that all parties fulfilled their financial responsibilities. The system consisted of two separate categories of intelligent agreements: the witness pool agreement along with the SLA agreement. Through transactions, clients alongside providers initially discussed utilisation specifics of the SLA. They then proceeded to randomly choose a specific number of witnesses by executing witness pool smart contract. Figure. 1 displays the specific information on the service engagement (Zhou et al., 2019).

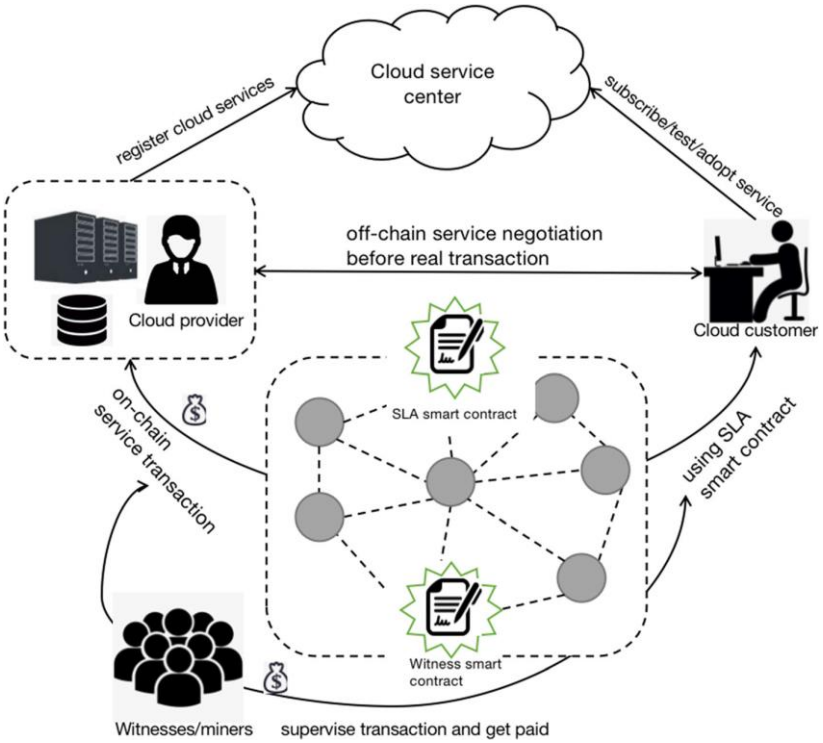


Figure 2: Witness-contained cloud service interaction protocol (Zhou et al., 2019)

The primary innovation of this research is the integration of BCT into cloud manufacturing, enabling decentralized interaction without requiring a trusted 3rd-party institution. Nevertheless, with the suggested system, there is a risk of private data being compromised in online settings. Additionally, it lacks the ability to rectify erroneous actions, and every function, including writing, requires payment.

B. Blockchain-based cloud transactions

CC happens to be a business model that offers IT services, with service transactions being its core operations. Clearly, a computing environment that is not trusted cannot provide a secure transaction. In order to securely and reliably implement and utilize software, introduced a Cleanroom Security Service Protocol (CSSP) (Zhou et al., 2017). This protocol is essentially a mutual agreement that operates within a consortium blockchain architecture, as seen in Figure 2. CSSP was primarily developed for the SaaS computing setting. The protocol was designed to safeguard the service provider along with the user. It utilized a consortium BC to minimize computational and processing burdens. Smart contracts were employed to accelerate the implementation along with execution of software. In the event of malicious behavior, immediate action could be taken.

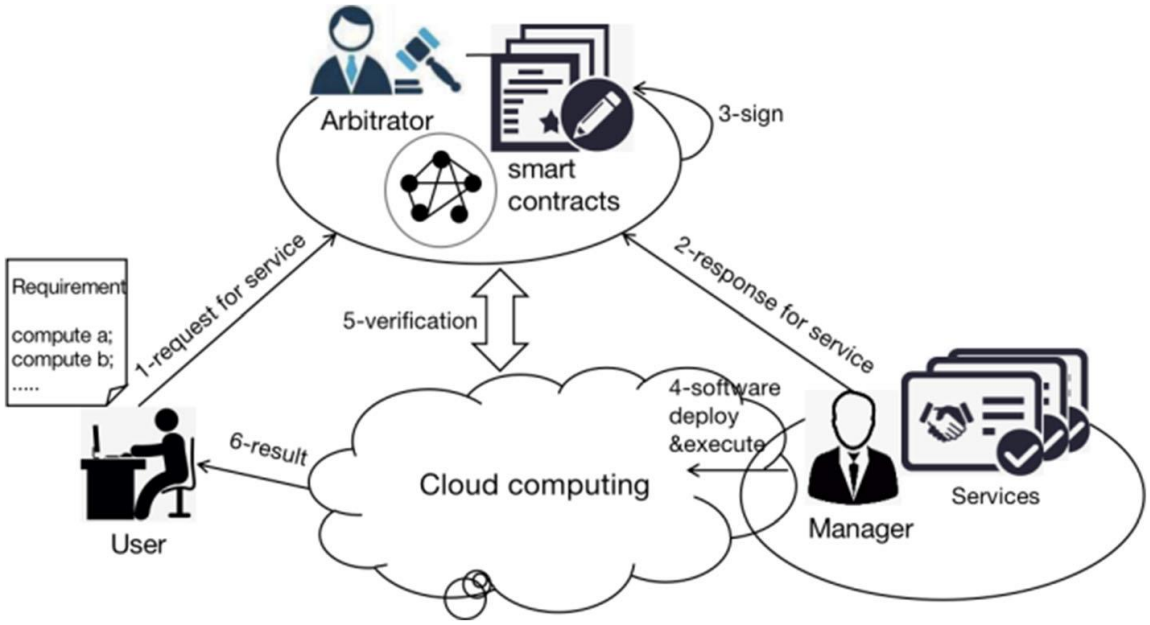


Figure 3: Main procedure in CSSP (Zhou et al., 2017)

a. Model's limitations

- The instructions did not provide a clear method for assessing nonquantitative characteristics, such as data integrity, within reputation computation model.
- The presentation as per the new calculation model's theoretical basis was omitted, and no information was provided on the utilization of the natural language interpretation approach for user feedback evaluation.

C. Blockchain-boosted resource distribution alongside task divesting mechanisms

BC is a highly efficient method for creating a distributed alongside decentralized system of trust. Nevertheless, the consensus mechanism's high energy consumption hinders its optimal performance in a cloud-edge service (hybrid) paradigm. Cloud mining, a method that incentivizes miners to acquire or lease resources from all cloud providers, has emerged as a potential resolution to the existing conflicts. To enhance the efficiency of blockchain applications that rely on cloud mining, employed game theory to manage the communication across cloud/edge providers alongside miners (Xiong et al., 2020). They successfully achieved distributed and rapid PoW by utilizing the ADMM algorithm. So, Figure 3 illustrates the process of offloading Proof of Work (PoW) computations to either cloud or even edge servers. This work stands out by adopting a unique approach compared to most blockchain-based applications. It focuses on examining the effective functioning of the BC consensus mechanism directly on terminal devices with limited resources. The resource competition alongside allocation issue in the scenario involving several suppliers and miners was resolved using the multi-follower multi-leader game theory.

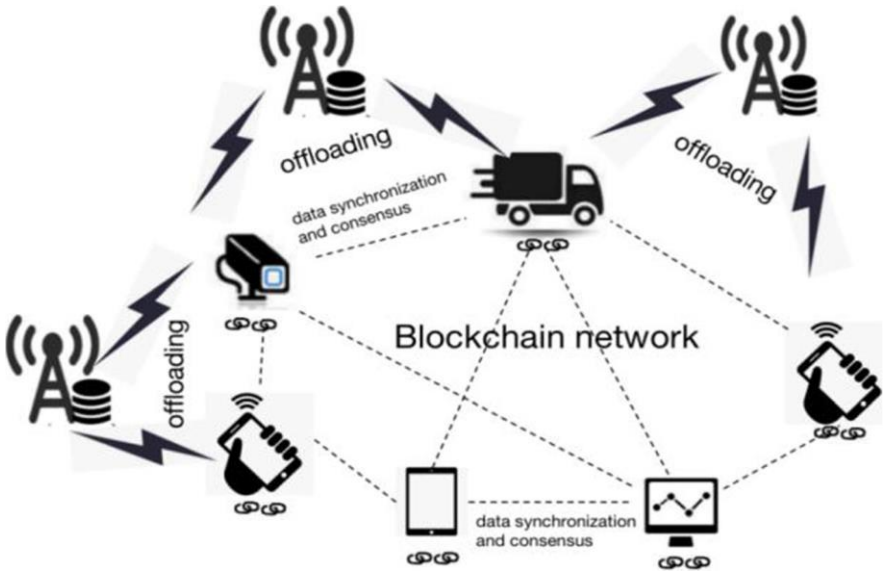


Figure 4: PoW offloading to cloud/edge servers (Xiong et al., 2020)

D. Trust-enhanced cloud virtualization

To address the possible risks in Docker Content Trust (DCT), this introduced a trust model called Decentralized Docker Trust (DDT) that is based on BCT. DDT has several benefits, such as mitigating the vulnerability to DoS attacks and providing digital signature verification services. The text provided conducted a comprehensive examination of the technical structure of Docker Content Trust, deliberated on the utility of Notary in Docker trust management, and highlighted two significant possible risks associated with DDT. The user developed an innovative Docker trust management framework and procedures using BCT. They provided a detailed explanation of how to deploy along with utilise this new model, and validated its effectiveness via prototype trials (Xu et al., 2018).

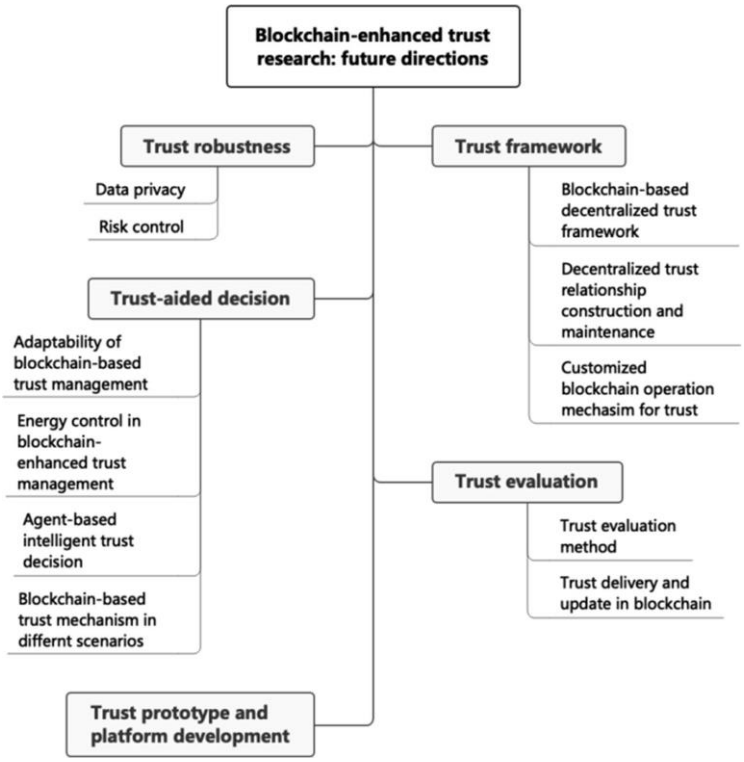
5. COMPARISON OF THE MODELS

Below is a concise description of the contrast of the linked works inside the framework and mechanisms of trust interaction increased by blockchain.

Author and Reference	Management mode	Application scenario	Performance test	Blockchain type	Main indicator
Yang et al., (2019)	Decentralized	Cloud transactions	Rinkeby (test net of Ethereum)	Ethereum	Feasibility
Zhou et al., (2019)	decentralized	Cloud security management	Case study, simulation	Ethereum	Integrity, availability
Xiong et al., (2020)	Centralized	JointCloud	Theoretical analysis	Not clear	credibility
Xu et al., (2018)	Semidecentralized	E-commerce	Real testbed	Consortium blockchain	credibility, latency, throughput
Gai et al., (2019)	decentralized	Cloud outsourcing	Simulation	Bitcoin	compatibility, robust, collision-resistance

6. FUTURE RESEARCH DIRECTIONS

Despite numerous researchers proposing techniques for trust management as per blockchain, significant disparities remain between theoretical concepts and their practical implementation. The future study directions are divided into four categories as per several trust research fields.



A. Blockchain-based decentralized trust framework (Xiong et al., 2020)

Blockchain is an inherent decentralized and peer-to-peer consensus architecture. CC systems have several building modes, along with the introduction of fog computing, alongside edge computing, along with IoT utilisations has increased the diversity of cloud implementation methods. Hence, it is imperative for a trust framework based on blockchain to contemplate how to adjust to various utilisation scenarios in the cloud and present a tailored and adaptable architecture for trust authentication (Xiong et al., 2020).

B. Trust evaluation

Blockchain is a decentralized system that enables the formation of comprehensive and verifiable transaction records between cloud entities. Nevertheless, it is necessary to employ specialized evaluation methodologies in order to calculate trust based on the original transaction records. Thus, it is imperative to discover an apt approach for gauging trust alongside examine the way to create a trust block based on trade account (Trivedi et al., 2021).

C. Trust-aided decision

A further concern is enhancing the flexibility of trust management based on BCT, hence achieving dynamic access control. One potential resolution is to construct a trust model that prioritizes human needs, allowing services to perceptively evaluate their security vulnerabilities and implement an appropriate security strategy based on the likelihood of an attack (Xiao et al., 2020).

D. Trust robustness

The matter of privacy is another significant concern that requires attention. BCT offers the benefits of data openness and traceability. However, it also exposes vulnerabilities to privacy breaches and the misuse of data. Future research should strive to achieve a harmonious equilibrium between transparency and user privacy (Yin et al., 2021).

7. CONCLUSION

This study presents a classification system and an evaluation of trust management methods that are based on BCT in CC platforms. The approaches can be categorized into three phases: a blockchain-grounded fundamental trust framework, a blockchain-boosted trust interaction framework alongside mechanisms, along with data management. Subsequently, it provides a thorough examination and juxtaposition of the current trust methods that rely on BCT. Blockchain framework enhances the efficiency alongside adaptiveness of trust-enabled CC. This framework combines cloud and edge computing and incorporates a double-BC grounded cloud transaction model.

REFERENCES

1. Gai K, Guo I, Zhu L, Yu S (2019) Blockchain Meets Cloud Computing: A Survey. IEEE Communications Survey Tutorials.
2. Kowalski, M., Lee, Z. W., & Chan, T. K. (2021). Blockchain technology and trust relationships in trade finance. Technological Forecasting and Social Change, 166, Article 120641.
3. Liu Y, Yu F, Li X, Ji H, Leung VM (2020) Blockchain and machine learning for Communications and networking systems. IEEE Commun Survey Tutorials 22(2):1392–1431.
4. Matin C, Navimipour J, Jafari N (2018) Cloud computing and trust evaluation: a systematic literature review of the state-of-the-art mechanisms. J Electrical Syst Information Technol 5(3):608–622.
5. Rawashdeh E, Abuqaddom I, Hudaib A (2018) Trust models for Services in Cloud Environment: a survey. In: In proceedings of 9th international conference on information and communication systems (ICICS), IEEE 2018, pp 175–180.
6. Trivedi, S., Mehta, K., & Sharma, R. (2021). Systematic literature review on application of blockchain technology in E-finance and financial services. Journal of Technology Management & Innovation, 16(3), 89-102.
7. Xiao Y, Zhang N, Lou W, Hou Y T (2020) A Survey of Distributed Consensus Protocols for Blockchain Networks, IEEE Communications Surveys & Tutorials, 22(2):1432–1465.
8. Xiong Z, Kang J, Niyato D, Wang P, Poor HV (2020) Cloud/edge computing Service Management in Blockchain Networks: multi-leader multi-follower game-based ADMM for pricing. IEEE Trans Serv Comput 13(2):356–367.
9. Xu Q, Jin C, Rasid M, Veeravalli B et al (2018) Blockchain-based decentralized content trust for docker images. Multimedia Tools Applications 77(14): 18223–18248.
10. Yang R, Yu F, Si P, Yang Z, Zhang Y (2019) Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges. IEEE Commun Survey Tutorials 21(2):1508–1532.
11. Yin Y, Li Y, Ye B, Liang T, Li Y (2021) A Blockchain-based incremental update supported data storage system for intelligent vehicles. IEEE Trans VehTechnol:1

12. Zhou H, Ouyang X, Ren Z, Su J, de Laat C, Zhao Z (2019) "a Blockchain based witness model for trustworthy cloud service level agreement enforcement," IEEE INFOCOM 2019 - IEEE conference on computer Communications. France, Paris, pp 1567–1575.
13. Zhou L, Cui T, Wang G et al (2017) Cssp: the consortium Blockchain model for improving the trustworthiness of network software services. In proceedings of 2017 IEEE international symposium on parallel and distributed processing with applications and 2017 IEEE international conference on ubiquitous computing and Communications (ISPA/IUCC). IEEE 2017:101–107.