Li et al. Journal of Cloud Computing: Advances, Systems and Applications (2021) 10:35
https://doi.org/10.1186/s13677-021-00247-5

Journal of Cloud Computing: Advances, Systems and Applications

RESEARCH Open Access

Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions

Wenjuan Li[1,2*], Jiyi Wu[2], Jian Cao[3], Nan Chen[1,2], Qifei Zhang[4] and Rajkumar Buyya[5]

Abstract

Through virtualization and resource integration, cloud computing has expanded its service area and offers a better user experience than the traditional platforms, along with its business operation model bringing huge economic and social benefits. However, a large amount of evidence shows that cloud computing is facing with serious security and trust crisis, and building a trust-enabled transaction environment has become its key factor. The traditional cloud trust model usually adopts a centralized architecture, which causes large management overhead, network congestion and even single point of failure. Furthermore, due to a lack of transparency and traceability, trust evaluation results cannot be fully recognized by all participants. Blockchain is a new and promising decentralized framework and distributed computing paradigm. Its unique features in operating rules and traceability of records ensure the integrity, undeniability and security of the transaction data. Therefore, blockchain is very suitable for constructing a distributed and decentralized trust architecture. This paper carries out a comprehensive survey on blockchain-based trust approaches in cloud computing systems. Based on a novel cloud-edge trust management framework and a double-blockchain structure based cloud transaction model, it identifies the open challenges and gives directions for future research in this field.

Keywords: Decentralized trust management, Blockchain technology, Cloud computing, Distributed ledger

Introduction

With the unlimited extension of resource sharing and a better user experience, cloud computing has become one of the hottest IT research issues in recent years and its huge commercial value is gradually emerging [1, 2]. However, cloud computing systems have encountered serious trust and security problems. For example, in 2016, Cloudflare, a well-known cloud security service provider revealed that a critical bug in its software had resulted in privacy data leakage, affecting at least 2 million websites, including services from many well-known Internet companies such as Uber and 1password. In March 2017, failures in Microsoft Azure public cloud storage affected related cloud business for more than 8 h. In June 2017, a security breach in Amazon Web Services resulted in the exposure of personal information of 200 million US voters. According to a survey conducted by Fujitsu, up to 88% of cloud customers are worried about data security issues and want to know what is happening on the physical servers.

In general, there are three major trust risks in cloud computing platform.

- Loss of control. Cloud users lose control of their own data, code and running process once submitting them to remote cloud servers.
- Lack of transparency. Not knowing the internal operation mechanisms, cloud computing is just like a black box to its users, raising their concern about privacy manipulation.

* Correspondence: liellie@163.com
[1]Qianjiang College, Hangzhou Normal University, Hangzhou 310018, China
[2]Artificial Intelligence Association of Zhejiang Province, Hangzhou 310036, China
Full list of author information is available at the end of the article

- Lack of a clear security assurance. Although most cloud service providers declare their Service Level Agreements (SLAs), trying to offer a certain degree of commitment to service reliability, security and privacy, the descriptions on SLAs are always vague and abstract.

Many scholars have embarked on trust-related research. For example, Li et al. introduced a novel trust approach which was enable to evaluate and predict users' cognitive behaviors [3]. In [4, 5], trust models combined with evolutionary algorithms were introduced, as were a number of valuable strategies to improve the efficiency of service management [6–10]. However, the traditional trust model usually relies on a centralized third-party trust management center, which may lead to delay, congestion and even single point of failure. In addition, in a centralized trust framework, since the evidence of trust is not open to all users, trust evaluation results are not fully trusted by all participants.

Being an emerging decentralized framework and a distributed computing paradigm, blockchain technology has received widespread attention, and its application has shown a blowout development with the popularity of digital cryptocurrencies. Blockchain is based on a decentralization P2P architecture, where all the nodes are equal and no control center exists. The benefits are:

- maintenance of trust relationships no longer depends on a third-party center, and the damage from a few nodes isn't able to destroy the robustness of the system,
- the operating rules and data records are open, transparent and traceable,
- and the chain data structure and the consensus mechanisms ensures the integrity, credibility and security of trust evidence.

Obviously, the decentralization feature of blockchain is particularly suitable for constructing a new distributed and decentralized trust model. Blockchain provides a new way to achieve trust-enabled cloud trading environments. To date, several blockchain-based trust management approaches have been put forward [11]. These new studies have proved the overwhelming advantage of blockchain-based schemes. For instance, the blockchain-based detection algorithm improved the accuracy by 5% to 15% [12]. The rewards of NFV (distributed network function virtualization) in MEC environments were increased to $6 \sim 7$ times using blockchain-enhanced method [13]. When processing large-capacity data requests, the delay of the blockchain-based method is only 1/5 of that of the traditional ones [14].

The most representative 35 articles were selected in this paper. These valuable methods are analyzed, classified, and compared. At present, blockchain-based trust management still faces huge challenges, such as trust relationship construction and maintenance, efficient trust evaluation methods, effectively response to attacks, unacceptable delay in real-time transactions, etc. For the benefit of future research, this paper suggests the possible future research directions.

Our contributions

The major contributions of this paper are listed below:

- It conducts a comprehensive review of blockchain-based trust approaches in cloud computing environment.
- It expands the boundaries of cloud computing to analyze the application of blockchain in the different implementation modes of cloud, including P2P, IoT, edge computing, etc., proposes a taxonomy of blockchain-based schemes and gives an in-depth analysis of the current approaches.
- It proposes a novel cloud-edge hybrid framework and a double-blockchain based transaction model for the flexible trust management.
- It identifies research gaps and suggests future research directions in blockchain-based trust management in cloud computing.

Related surveys

There are already some surveys on trust schemes in cloud computing environments. A. Horvath III et al. [15] explored the issues of consumer trust in cloud computing systems to help service providers improve their behaviors. S. Harbajanka and P. Saxena [16] conducted a review on trust approaches in cloud computing by pointing out the pros and cos of the related researches. E. Rawashdeh et al. [17] gave a detailed introduction on current trust models in cloud systems. J. Huang and D. Nicol [18] undertook a survey on the existing trust mechanisms and pointed out their limitations. T. Noor et al. [19] presented an overview of trust management in cloud services and discussed the open issues. M. Monir, et al. [20] presented a survey of trust solutions in cloud computing to measure the performance of service providers. M. Chandni et al. [21] discussed the possible attacks on cloud systems and then provided an overview of the existing trust-based techniques. J. Lansing and A. Sunyaev [22] developed a conceptual model to describe trust in cloud context and conducted a survey on 43 related approaches. C. Matin et al. [23, 24] analyzed the state-of-the-art trust evaluation methods in cloud computing systems. S. Deshpande and R. Ingle [25] presented a taxonomy and classification of trust models and

trust assessment methods in cloud paradigm. In order to help cloud users choose trustworthy service providers, M. Alhanahnah et al. [26] carried out a survey on the taxonomy of trust factors and evaluation methods. Mainly from the perspective of the sharing economy, F. Hawlitschek et al. [27] discussed the potential for using blockchain technology to construct trust-free systems. In order to exploit the function of trust in decision making, paper [28] discussed the concept, assessment, construction, and the application of trust. J. Granatyr et al. [29] carried out a review on trust and reputation methods for the Multi-Agent Systems (MASs).

With the emergence of the blockchain technology, especially its popularity in E-currency, it has attracted great attention from researchers. Currently, we can also find many blockchain reviews. For example, Y. Xiao, et al. [30] focuses on the distributed consensus protocol in blockchain. Paper [31] can be seen as a blockchain manual, which helps users to decide whether, which type and how to use blockchain. M. Ali, et al. [32] analyzed the applications of blockchain in IoT systems. Paper [33] provided a comprehensive survey on the combination research of blockchain and machine learning in communication and network systems. K. Gai, et al. [34] discussed the blockchain based cloud service infrastructure and compared the performance from both software and hardware perspectives. M. Saad, et al. [35] gave a comprehensive discussion on attacks of blockchain and the existing solutions. Paper [36] made a survey on the combination research of blockchain and edge computing, including the concept, requirements, framework and challenges.

However, to the best of our knowledge, still very few surveys or taxonomy have focused on blockchain-based trust solutions in cloud computing systems. Therefore, this paper chooses another perspective, which not only enhances the previous surveys, but also focuses on the blockchain-based approach for trust-enabled service/resource management in cloud systems. It identifies the current technical challenges and suggests directions for future research in applying blockchain technology to construct trust-enabled interactions in cloud computing systems.

Article structure

The rest of this paper is organized as follows. Section 2 gives a brief introduction on trust-related research in cloud and blockchain technology. Section 3 explains the methodology applied to find the related articles. The review and a comparison of blockchain-based trust approaches in cloud computing systems is presented in Section 4. Section 5 gives a novel cloud-edge hybrid trust management framework and a double-blockchain based cloud transaction model. Open challenges and future research directions are discussed in Section 6. And conclusions are given in Section 7.

Trust researches in cloud computing systems

Trust research classification

The concept of trust originated from sociology, and gradually extended its boundaries to areas of management, economics, and computer science. In 1996, M. Blaze et al. [37] first introduced trust mechanisms to cope with Internet security issues. Trust management provides a novel solution to solve security problems in heterogeneous, open, distributed and dynamically changing network environments. Figure 1 shows the shows the research scope of trust.

The first branch is the fundamental part of trust research, and the core is to study the concept of trust and its classification based on specific attributes. As shown in Fig. 1, trust can be divided into the following categories based on different classification methods [9].

- direct trust, indirect (recommendation) trust, and integrated trust (according to trust acquisition method)
- identity trust and behavior trust (according to the basis of identification) [38]
- function trust and experience trust (according to the timing of the occurrence of trust)
- objective trust and subjective trust (according to the representation of trust)
- intra-domain trust and inter-domain trust (according to trust relationship).

The second research branch is trust model, the core of which is the modeling, evaluating and management method of trust in order to support trust-enabled platform or trading environments. According to the trust management mode, a trust model can be divided into a centralized model or a decentralized model. In a centralized trust model, a central trust server is responsible for collecting, evaluating, and saving trust evidence of all parties, who is assumed to be fully credible and never be compromised. Taobao and eBay [39] are the typical centralized trust models. However, using a centralized trust model may bring about abnormal latency, blocking, and even a single point of failure, thus degrading cloud service QoS. Therefore, other researchers preferred a decentralized trust framework. For example, EigenTrust [40] and PeerTrust [41] are the well-known distributed trust models.

According to the trust evaluation method, trust models can be divided into the following different types.

- network topology-based model
- statistical-based model

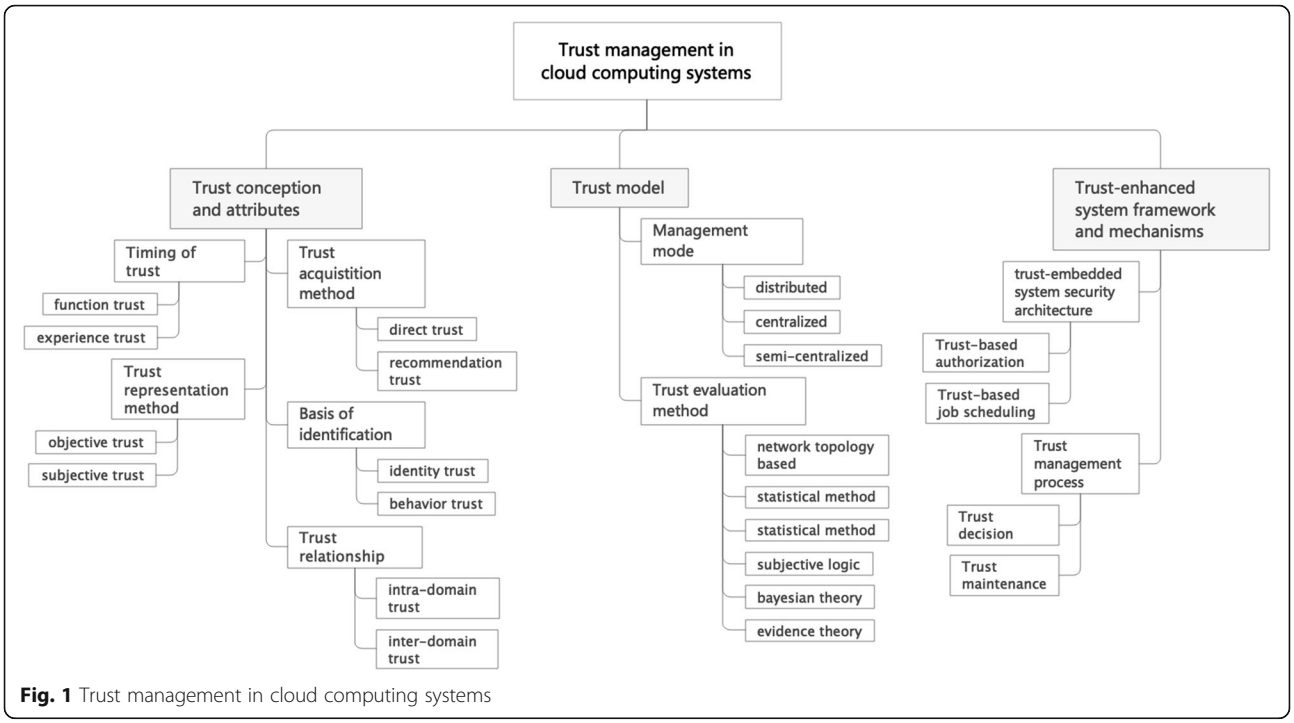

Fig. 1 Trust management in cloud computing systems

- fuzzy logic-based model
- subjective logic-based model
- Bayesian theory-based model
- evidence theory-based model

The last research branch is trust-enhanced system framework and mechanisms. By adding a trust management layer to the top of the traditional cloud security model, a trust-enabled system security framework is implemented. Trust mechanisms provide possible protection for cloud interconnection and interaction. Trust-based authorization and job scheduling are the typical research issues [42]. Trust-based mechanisms mainly include the design of trust decision and the efficient maintenance of trust.

Recent research results

In recent years, trust-enabled cloud service management strategies have been intensively studied. For example, in order to improve the performance of service matching, Li et al. designed a cloud service brokering model based

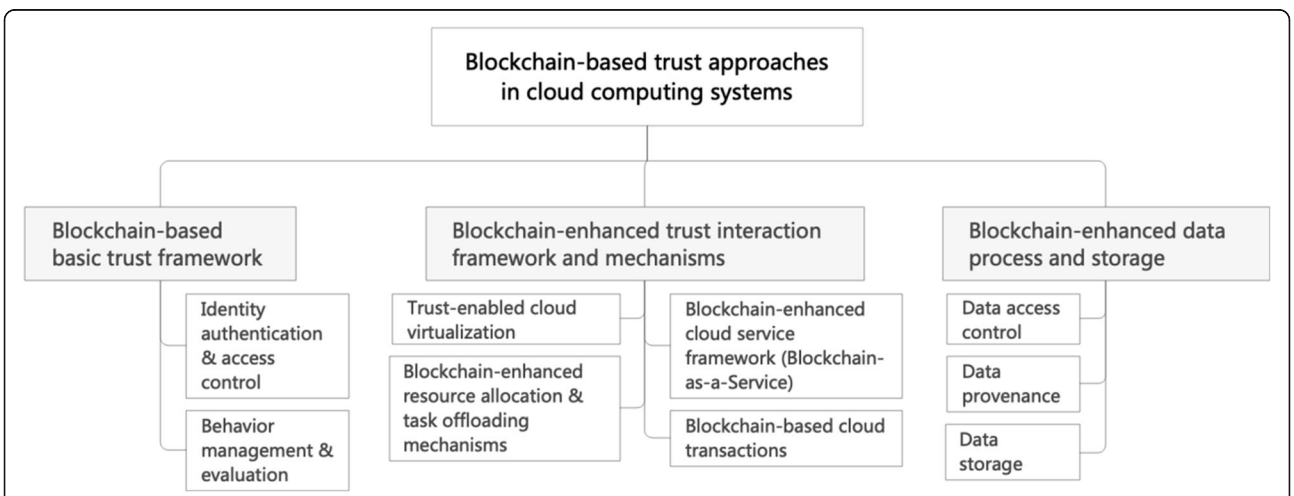

Fig. 2 Phases of blockchain-based trust approaches in cloud computing systems

on trust [43]. Mrabet et al. [44] put forward a new trust evaluation model named T-broker. AbdAllah et al. [45] designed TRUST-CAP, a trust-based cloud application protocol. Singh et al. [46] introduced a collaborative trust calculation scheme based on fuzzy logic. Nagarajan et al. [47] also presented a similar trust evaluation model. For the safety and efficiency of cloud duplication, Zahra et al. [48] proposed a novel encryption protocol named LEVEL. Zhang et al. [49] proposed a domain-based trust scheme for public clouds. Yefeng and Durresi [50] designed a three-level trust management framework to prevent cloud vendors and customers from being affected by potential attacks. Felipe and Fiorese [51] introduced a reputation framework combining both the objective and subjective trust indicators for cloud. Zhu et al. [52] introduced a novel trust calculation model named ATRCM for the CC-WSN integration platform. For the security of IaaS Cloud Computing systems, Kashif et al. [53] designed a new distributed trust framework. To help users avoid trading with malicious services, Hu et al. [54] put forward a cloud service interaction model based on trust and spanning tree. Wang et al. [55] proposed a trust and preference aware service selecting model called CC-PSM, for the safe and effective cloud transactions. Meng et al. [56] introduced a two-layer service searching protocol for users to find the most credible and cost-effective service. Yan et al. [57] designed a trust-enabled cloud service framework. For Service-Oriented Computing (SOC) environments, Hang et al. [58] put forward two set of service/resource selection methods based on a distributed trust model. The trust and QoS aware service selection or composition approaches were proposed in Paper [59–63].

Research challenges

At present, the research of trust-based approaches in cloud computing still faces huge challenges in theory and implementation.

- Most trust models are centralized, and even those that claim to be decentralized models still need a third-party trust or certification center, which may result in many security risks such as single point of failure, over-load and credibility loss, etc.
- Trust evidence is not open to all participants and not traceable, so trust evaluation results are not convincing nor are they fully trusted.
- Inaccuracy of trust evaluation results. The existing trust models lack a sufficient description capability (trust data mostly in the form of numerical scoring), which is insufficient in real applications, such as E-Commerce, where people's feedback often includes multiple data types such as numeric and characters.
- Less adaptive. Trust decision-making uses subjective methods, such as expert scoring and the averaging method, which makes the models subjective and lack scientific and adaptability. Trust models are not robust enough to deal with malicious attacks (collusion), especially malicious recommendations.
- Huge management overhead. It limits trust solutions in a large-scale network applications.
- Lack prototype and platform. Performance tests of trust models are mostly achieved by some simulation experiments, needing further evaluation.

Literature selection methodology

This section explains how we selected the surveyed papers.

Search method

We searched for relevant literature in the mainstream academic databases, namely ACM Digital Library, IEEEXplore, Elsevier, Springer, Wiley online database and CNKI of China.

We used a two-stage literature search method. In the first stage, the words "trust", "blockchain" and "cloud computing" were used to search the titles, key words and abstracts of research papers. As in some manuscripts, trust is equivalent to "reputation", we also used "reputation", "blockchain" and "cloud computing" to find more related articles.

Even after doing so, not many more articles were found. As there are many practical forms of cloud computing, such as P2P, wireless cloud, cloud IoT integration, etc., in the second phase, we adjusted the search strategy and only used the keywords "trust" and "blockchain". In this way, we retrieved many more articles, which we manually filtered to select the most relevant articles.

Outcome

Finally, we selected 35 research papers focusing on blockchain-based trust approaches for cloud computing systems. 57% of the articles were published in journals, and 43% were published in the proceedings of international conferences.

Phases, taxonomy and review of Blockchain-based trust approaches

In this section, we provides a comprehensive review on the blockchain-based trust approaches for credible interactions in cloud computing environments.

Our basis for document classification is the basic research taxonomy of trust and the blockchain methods in the different fields of trust-based cloud computing applications. Thus, the related solutions are classified into three categories: blockchain-based basic trust

framework, blockchain-enhanced trust interaction framework and mechanisms, and blockchain-enhanced cloud data management, as illustrated in Fig. 2.

The basic trust framework contains two sub research modules: 1) identity authentication & access control, 2) behavior management & evaluation. The blockchain-enhanced trust interaction framework and mechanisms include four sub research modules: 1) blockchain-enhanced cloud service framework (Blockchain-as-a-Service), 2) blockchain-based cloud transactions, 3) blockchain-enhanced resource allocation and task offloading, and 4) trust-enabled cloud virtualization. And the blockchain-enhaced data management mainly has three sub research areas: 1) data access model, 2) data provenance, and 3) data storage. In the following part, we will introduce the research progress in the mentioned areas.

Blockchain-based basic trust framework

The traditional trust frameworks always adopt a centralized model, with the center node suffering from a huge burden of computing and processing overhead, which may easily leads to possible failures such as single point failure and malicious fraud, and cannot adapt well to a real-time application scenario. And because the trust evidence is only visible to the center, trust evaluations are not fully recognized.

The natural decentralization feature of blockchain can decentralize the process of trust authentication, thereby overcoming the above problems caused by centralization.

Identity authentication and access control

Identity management is the fundamental part of trust-based cloud computing. Identity authentication ensures that the participants of cloud markets, including service providers and customers, are authenticated legitimate nodes. The traditional identity management method usually requires a third-party management center, which may lead to security risks, such as the excessive authority of the certification center and single point of failure. In large distributed systems, identity federation is another choice to overcome security and trust problems across multiple domains, however, it increases the complexity of system design and operation.

N. Alexopoulos et al. [64] investigated the possibility of using open distributed ledgers like blockchain technology to develop an authentication model for trust management (TM) systems. Based on blockchain framework and graph theory, they proposed an abstract authentication model and explored how blockchain could help participants mitigate attacks against them. They proved that by implanting trust-related information in a encrypted blockchain architecture, five prevalent attacks could be successfully alleviated.

The main contributions of the paper are as follows.

- It discussed the possibility of blockchain technology in building a decentralized trust model, and analyzed robustness of blockchain-enhanced TM systems when faced with different kinds of attacks.
- It clarified whether blockchain technology could improve or enhance the security of a genetic TM system.

For the effective trust governance of cloud computing systems, K. Bendiab et al. [65] proposed a novel identity management model based on blockchain technology. The proposed model enabled service venders to effectively manage their trust behaviors and relationships with customers or other providers in a distributed, decentralized and dynamic manner. The core idea is credible inter-domain trust management using blockchain network. The model covered the definition and computation method of three important factors of trust, namely user credibility, authentication and satisfaction. Figure 3 shows the architecture of the proposed blockchain-based identity authentication system.

The contributions of the paper are as follows.

- It analyzed and explained the limitation of identity federation in trust management.
- It introduced the implementation mechanism of blockchain in building identity management and designed a cross-domain authentication procedure, taking into account the dual role of CSP (as service provider and recommender).

The limitations are as follows.

- It only cared about the protection of CSP and their resources, while ignoring the security and privacy requirements of users,
- It is only a theoretical model which has not been implemented in a real cloud system.

Due to the resource restriction in IoT systems, peer authentication and trust management are not well implemented. A. Moinet et al. [66] designed a novel security model called the Blockchain Authentication and Trust Module (BATM) to enhance the credibility and validity of authentication in sensor networks.

The main contributions of the paper include:

- it pointed out the limitations of current work in balancing data-related mechanisms, including the

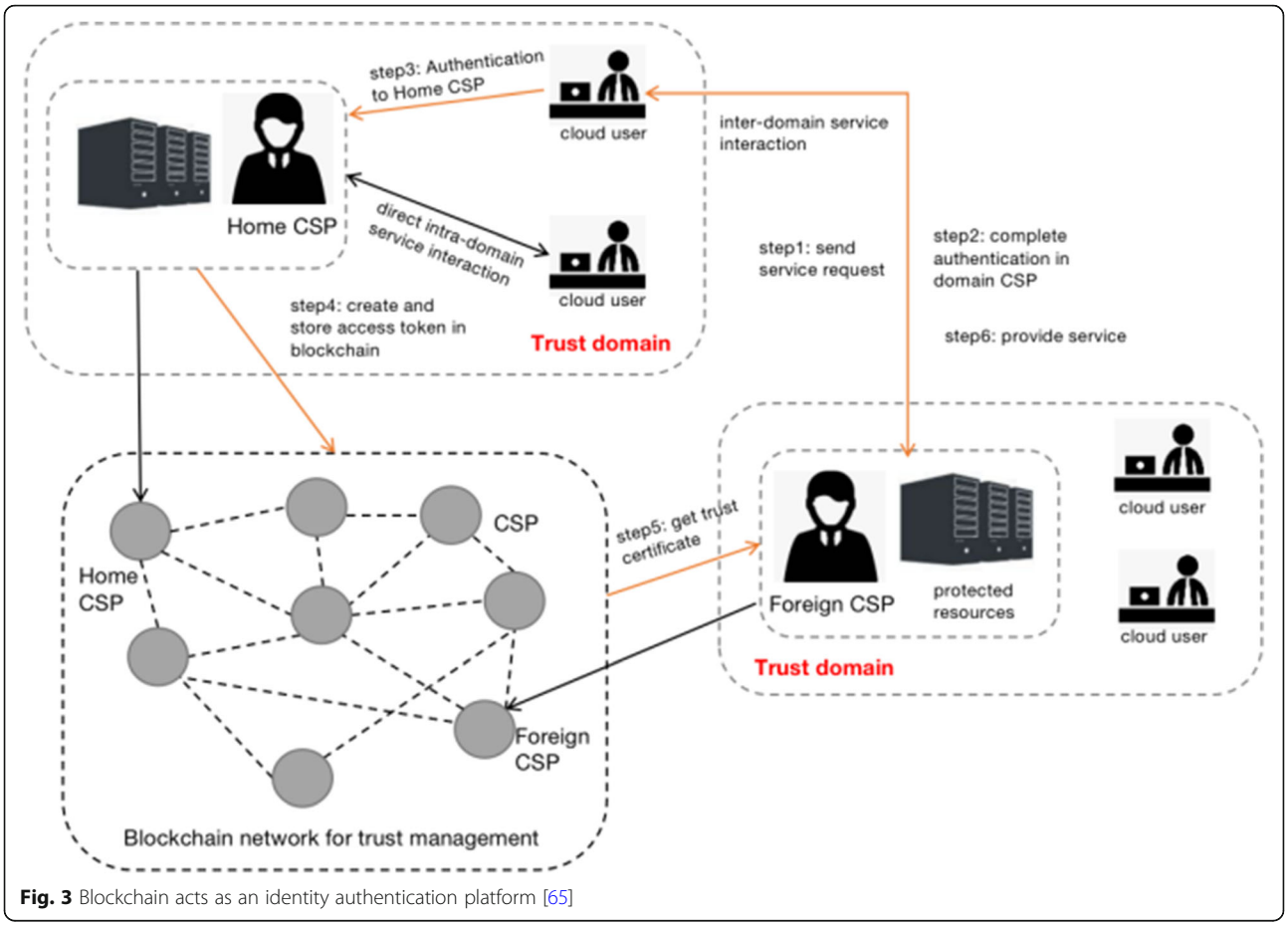

Fig. 3 Blockchain acts as an identity authentication platform [65]

protection of data security and privacy, node authentication and trust management,

- it proposed to use a blockchain-based data structure to store distributed authentication and trust information, and it introduced a human-like knowledge-based trust model.

However, it overlooked the choice of the related system parameters, and it only provided theoretical arguments without details on the actual implementation.

Based on blockchain techniques, Y. Liu et al. [67] designed a decentralized identity management system. The system contained two kernel parts, identity authentication and reputation/behavior management. In the proposed framework, the former was achieved by binding the customer's personal information with a specific public address, and reputation was represented by tokens. The most prominent contribution lies in the innovation of the blockchain implementation mechanisms, including the introduction of the incentive tasks (the participants can earn RpCoin by exposing malicious users), and the introduction of the fluctuation factor to better characterize the activity of system nodes and changes in their credibility.

These manuscripts demonstrate the possibility and potential use of blockchain technique in identity management to enhance the security and privacy of cloud systems. However, each approach was specifically designed for a specific environment and most papers only designed theoretical models and did not detail the implementation in a real system.

Behavior management and evaluation

Behavior trust is another key factor in assessing and predicting the credibility of entities' behaviors. S. Nayak et al. [68] utilized smart contracts to propose Saranyu, a trust model for the efficient resource management in cloud computing systems. Saranyu was designed to deliver four types of services, including identity management, authentication, authorization, and charging. The first two services were handled by public-private key pairs. Authorization was achieved by a smart contract. Charging was realized through the payment gateways according to service or resource usage.

Saranyu can be defined as some kind of the distributed application based on Web3 Java Script library. Tenants and users create their accounts through Saranyu DApp to obtain services and profits fairly through the

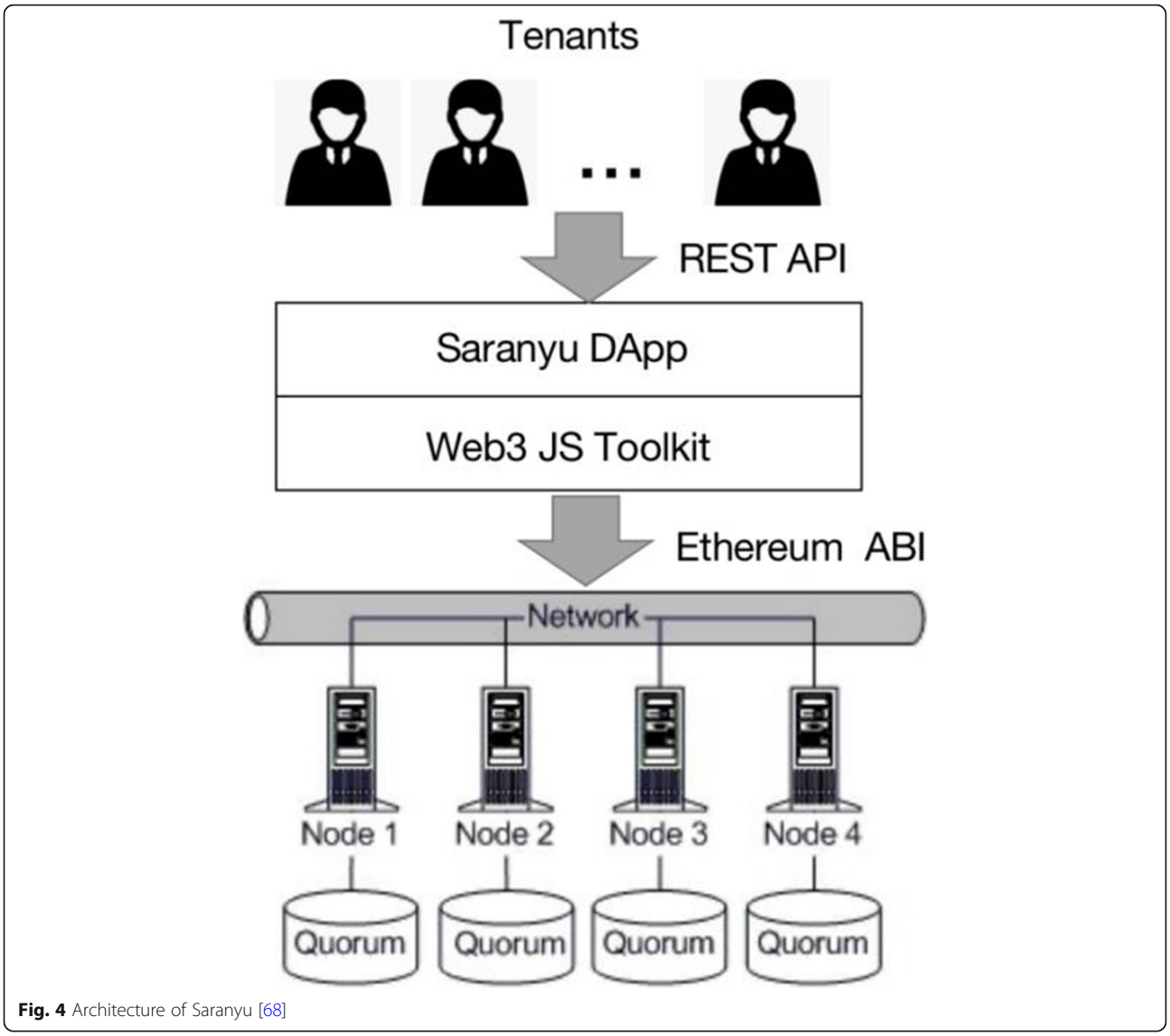

Fig. 4 Architecture of Saranyu [68]

operation of the platform. Figure 4 shows the architecture of Saranyu.

The contributions of the paper are:

- it used the smart contracts to realize a variety of services, including service management and tenant management, which could ensure the fairness of transactions to a certain degree,
- and it was a novel blockchain-based distributed App that combined open source Quorum and smart contracts.

The limitation of the work is that it can only be implemented in a licensed distributed ledger, in which only entities with legal credentials are allowed to participate. Also, the App had still been under development without a performance test in a large-scaled application environment.

For effective data credibility assessment in vehicular networks, Yang et al. [69] proposed a blockchain-based reputation system. The model comprises four types of entities: TA (Trusted Authority), OV (Ordinary Vehicle), MV (Malicious Vehicle), and the miners. TA is responsible for vehicle registration and capacity proof, OV broadcasts and receives messages and performs simple trust evaluation. Miners are elected from the OV and are responsible for generating blocks, and verifying and broadcasting certified blocks.

The focus of the paper was to analyze and implement data credibility. And the main processes include: data reliability assessment, information source rating (1 or – 1), miner selection (capability proof), blocks generation and verification, distributed consensus, and reputation calculation.

However, it was not really a decentralized scheme because TA participates in registration and distribution of key pairs, and the framework and implementation steps are not very clear.

Comparison of the models

The summary of the comparison between the related works in the blockchain-based basic trust framework is given in Tables 1, 2, and 3.

Table 2 Comparison of performance test

Reference	Effectiveness	Trust accuracy	Security/ Privacy
[65]	√		
[66]			√
[67]	√	√	
[68]		√	√
[64]			√
[69]	√		

Blockchain-enhanced trust interaction framework and mechanisms

Blockchain-based cloud service framework (Blockchain-as-a-service)

In practical applications, the Service Level Agreements (SLAs) sometimes are not credible and automatically executed as required. To this end, H. Zhou, et al. [70] added a new role "witness"to the traditional SLA service model to detect service violations and thus ensure the credibility. The Nash equilibrium theory of game theory was also used to help cloud providers and users negotiate and reduce the gas consumption.

In the proposed model, witnesses were the ordinary nodes in blockchain network, who gained profits by supervising cloud transactions. They helped the transactions proceed as agreed and forced all the parties to fulfill their money obligations. The system contained two types of smart contracts, including the witness pool contract and the SLA contract. During the transactions, customers and providers first negotiated the implementation details of SLA (including service duration, service fees, service compensation and witnesses to be co-employed, etc), and then randomly selected a certain number of witnesses through the execution of the witness pool smart contract. The details of the service interaction are shown in Fig. 5. This is one of the earliest documents that convert the problem of trust management into economics. However, it just used the theoretical methods for demonstration, which is difficult to prove its efficiency in the real transactions.

In response to the severe security issues faced by traditional centralized cloud computing architectures, P. Fernando, et al. [71] proposed a hybrid cloud service architecture based on blockchain and SDN. The proposed architecture contained a blockchain security management layer and a multi-controller SDN network layer. The latter contained an edge computing sub-layer and a P2P network routing sub-layer, as shown in Fig. 6.

The main contributions of this paper are as follows.

- It proposed a novel cloud computing service architecture based on an add-in blockchain security and autonomous management layer,
- It designed a blockchain-based bandwidth provision protocol to strengthen end-to-end connectivity, and the performance of the new model was verified by bandwidth occupancy rate, resource availability, and packet loss rate.

However, it can only be used in a relatively limited application scenario (bandwidth provision), and the author only provided a case study to prove the efficiency of the model.

In the era of Industry 4.0, cloud manufacturing has become a key technology for the globalization and intelligent development of manufacturing. Paper [72] introduced a blockchain-based decentralized cloud manufacturing model, and through the smart contracts, named blockchain-based DCMApp, it implemented an interaction agreement between resource providers and customers. DCMApp was different in a hybrid architecture as shown in Fig. 7. Most user data was stored locally, and only a small amount of important data was backed up on the blockchain network to reduce overhead.

The main contribution of the work is that it introduced blockchain technology into cloud manufacturing to realize the decentralized interaction without a third-

Table 1 Comparison of the applied methodology

Reference	Management mode	Application scenario	Performance test	Blockchain type	Main indicator
[64]	decentralized	TM systems	Theoretical analysis	Public blockchain	Trust assessment, security
[65]	decentralized	IaaS cloud federation	Theoretical analysis	Public blockchain	credibility, authentication, satisfaction
[66]	decentralized	Sensor networks	Simulation	Bitcoin	adaptive,reliability
[67]	decentralized	Identity management systems	Simulation,case study	Ethereum	feasibility
[68]	Semi-decentralized	Cloud tenant	Theoretical analysis	Public blockchain	distributed, completed
[69]	Semi-decentralized	Vehicular Networks	Simulation	Not clear	message accuracy

Table 3 Comparison of main contributions

Reference	Target & contribution	Improvement in Blockchain	Solution to attack
[65]	A graph theory model to build a trust network for authentication, and an open distributed ledgers to secure TM systems [65]	A graph theoretic model for consensus	Stealthy target attack, double registration attack, stale information attack, DoS attack, censorship attack
[66]	A blockchain-based trust model to help CSPs to autonomously manage trust [66]	the combination of proof-of-eligibility and proof-of-stake	/
[67]	Decentralized authentication and trust management for WSN	/	/
[68]	Identity management system based on blockchain	voting mechanism and reputation task, Incentive task (RpCoin reward and punishment)	/
[64]	Use blockchain to manage accounts in the datacenters of clouds [64]	Saranyu Manager, Tenant contract, Delegation contract	/
[69]	A blockchain based reputation system for data credibility in vehicle networks [69]	/	Fake messaging

party trust entity. However, in the proposed scheme, the private data might be exposed in the Internet environments, it could not correct the wrong operations, and all operations, even the write operation, need payment.

L. Xie et al. [12] proposed a semi-decentralized trust model based on blockchain technology for the vehicular IoT environment in SDN-enabled 5G-VANETs. The proposed scheme also used a joint Proof-of-Work and Proof-of-Stake mechanism to elect suitable miners and eliminate malicious traffic broadcasting. Based on a centralized controlled authentication mechanism and a decentralized trust management framework, it set up a semi-centralized trust model for road condition management.

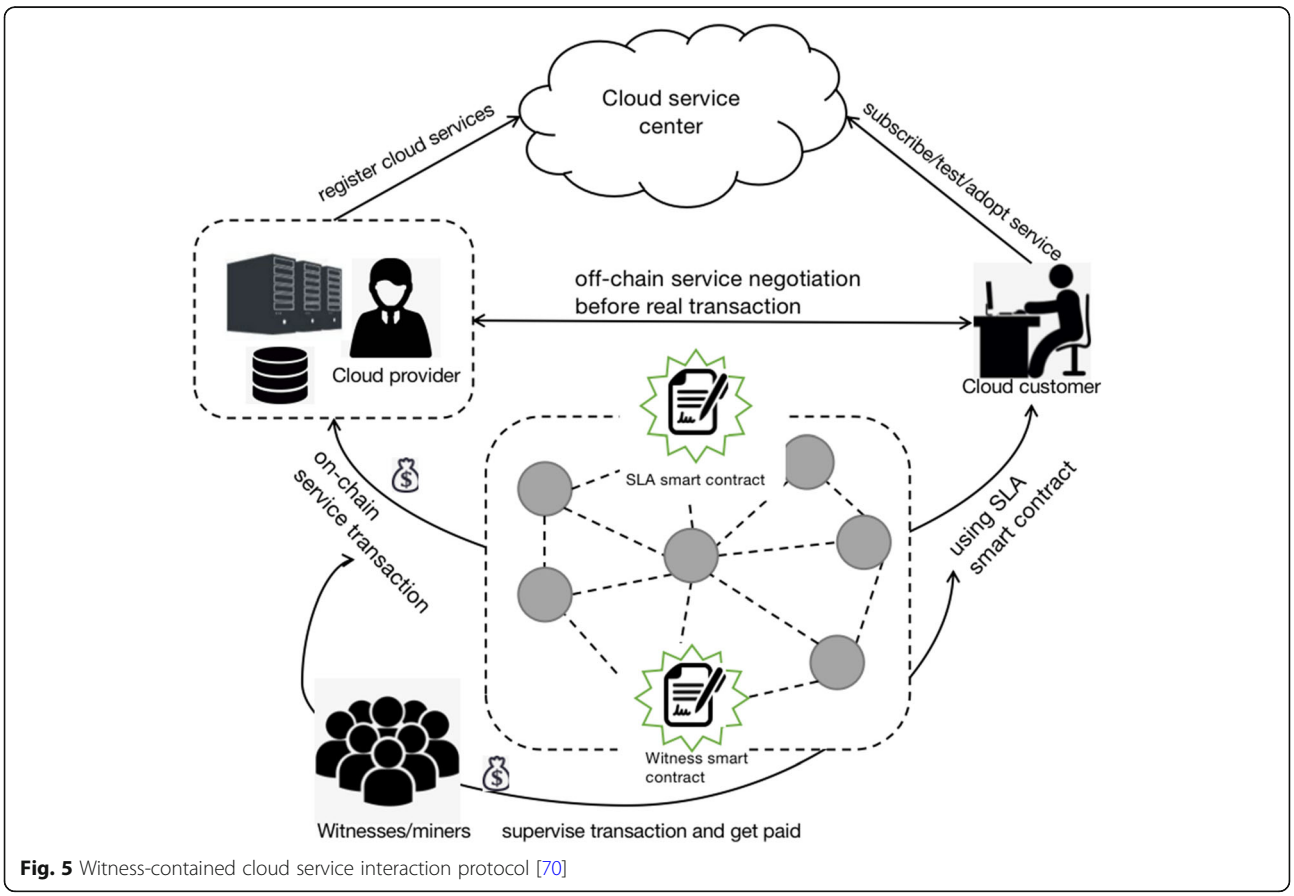

Fig. 5 Witness-contained cloud service interaction protocol [70]

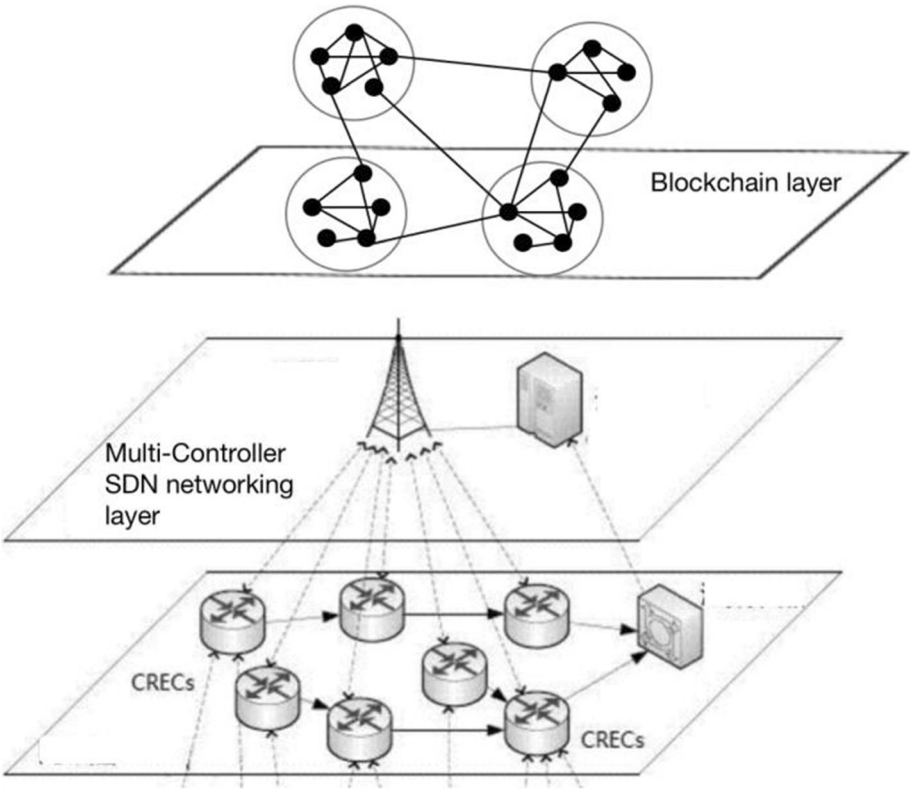

Fig. 6 Hybrid cloud service architecture based on blockchain and SDN [71]

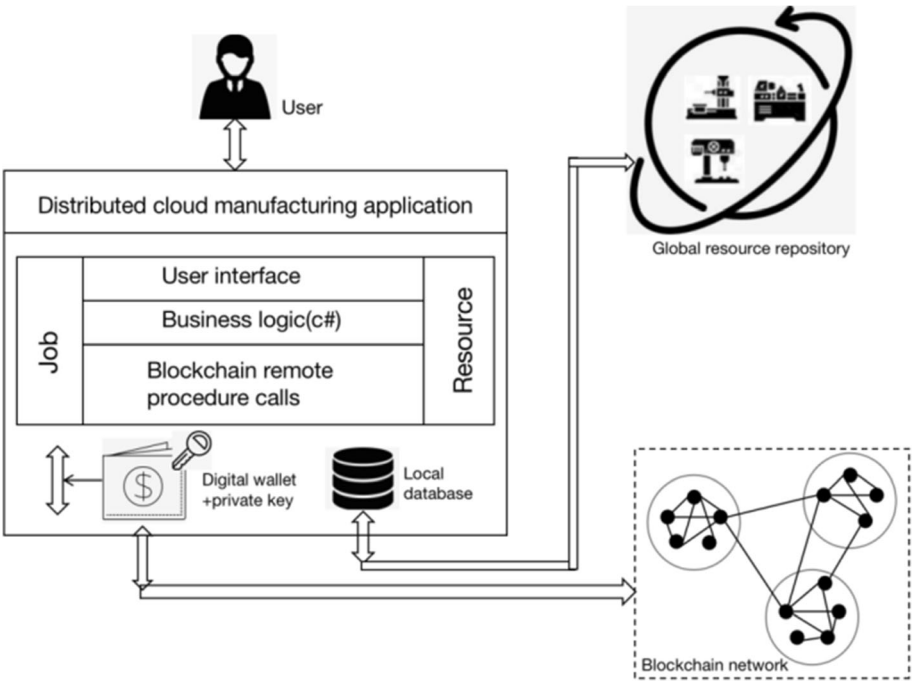

Fig. 7 Hybrid cloud manufacturing architecture extended version of [72]

The contributions of the paper are:

- it integrated the entities in the VANETs into the blockchain based P2P framework, achieving instant broadcasting of road information and direct and timely interaction between vehicles,
- distance was treated as the weight in evaluating the reputation and the credibility of messages, and the reputation of the RSUs is used to select suitable miners, ensuring the credibility of the data block.

However, it was not a fully decentralized model since TA was still required for registration, and the computation and consensus overhead is huge.

Blockchain-based cloud transactions

Cloud computing is a kind of business mode that provides IT services, thus service transactions are its kernel affairs. Obviously, an untrusted computing environment cannot ensure a safe transaction. To deploy and use software in a secure and tamper-resistant manner, Zhou et al. [73] proposed a Cleanroom Security Service Protocol (CSSP), which is actually a bilateral agreement based on a consortium blockchain framework, show in Fig. 8. CSSP was mainly designed for the SaaS computing environment.

The main contributions are:

- it was a bilateral protocol to protect both service provider and user, and it chose consortium blockchain to reduce the computation and process overhead,
- and it used the smart contracts to speed up the implementation and execution of software, and once malicious behavior is found, it could take action immediately.

However, the detection platform designed in the literature is relatively small, and only the traditional network models without trust and security mechanisms were compared.

Aiming at building a new cloud ecosystem, F. Ye et al. [74] introduced a new paradigm named JointCloud (Joint Cloud computing) and a novel dynamic and customized trust framework named DC-RSF. The core of DC-RSF is a customized model for credibility control named CDCM. CDCM can evaluate the credibility of a cloud service provider by the integration of service requirements and credential attributes. DC-RSF also contains a blockchain module, which is able to prevent trust data from being maliciously tampered with.

The contributions of the paper are as follows.

- It proposed a blockchain-based model for the credibility evaluation of providers in the JointCloud environment, ensuring the data security and non-tampered of the reputation data.
- The reputation evaluation model for cloud providers took into account both user-specific service requirements and the six service provision attributes, and it designed the reward and punishment mechanisms to encourage honest behavior and punish malicious behavior.
- It provided customized reputation services, which could adjust the weight of the reputation vector according to the preference of different users for different service attributes, and it recommended the use of the natural language interpretation

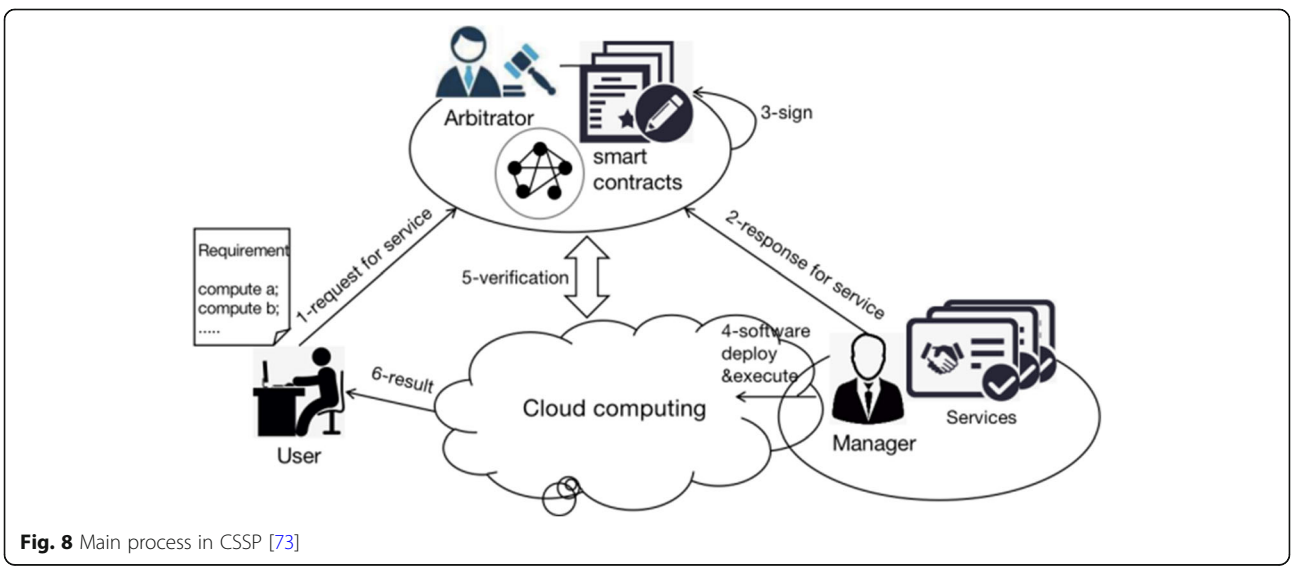

Fig. 8 Main process in CSSP [73]

technology to rate user feedback, thus realizing the dynamic evolution of the reputation model.

The limitations of the model are:

- it did not make clear how to evaluate non-quantitative indicators like data integrity in the reputation computation model,
- it skipped the demonstration on the theoretical basis of the new calculation model, with no details were given on how to use the natural language interpretation method for user feedback analysis,
- it did not describe how to implement the credit data framework based on blockchain, and it could not cope with the malicious users, since DC-RSF could only evaluate the credibility of service providers.

Most blockchain-based solutions have a fatal limitation in efficiency, which restricts them from being widely used. In order to create a safer and efficient cloud E-commerce system, Xie et al. [75] proposed a trusted framework named ETTF. By utilizing a peer blockchain protocol (PBP), ETTF supports large-scale real-time transactions. The ETTF model contained three kinds of peers, including gp (the global blockchain generation peer), vp (the global blockchain validation peer), and op (the ordinary peer), and two different protocols, PBP and E-commence Consensus Algorithm (ECA). By dividing the network into several sub-groups, ETTF can guarantee the credibility of most cloud instant transactions and achieves a much higher throughput along with lower latency compared to Bitcoin.

The contributions of the paper are:

- it tried to construct a credible E-Commence environment and payed attention to the latency and throughput issues in the instant transactions when using blockchain,
- and it designed a new peer-blockchain protocol, and by dividing the sub-committee, it reduced the time delay.

However, there is no clear description on how to deploy the blockchain-based framework.

Cloud outsourcing is an emerging cloud-based service outsourcing mode. In order to ensure the security and achieve fair payment in cloud outsourcing, Y. Zhang et al. [76] introduced a novel framework named BPay. Based on blockchain technology, BPay realized the strong fairness and compatibility by a special verification protocol and a top-down inspection method.

In BPay, the payment of the outsourcing service was divided into four phases, including service execution, service checking, payment and compensation. Figure 9 shows the life cycle of a typical outsourcing service in BPay.

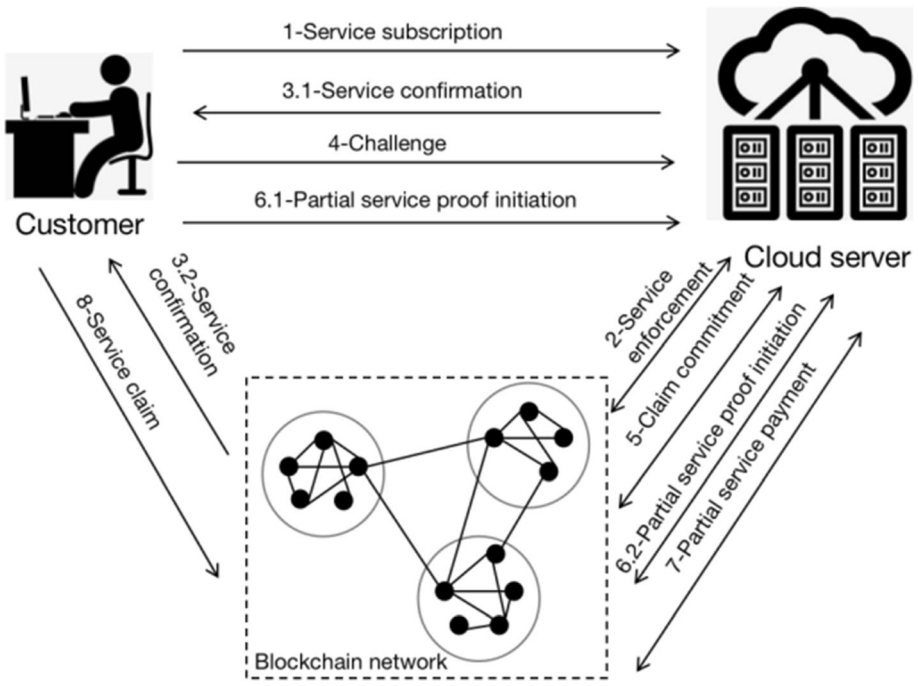

Fig. 9 Life cycle of a typical outsourcing service in BPay [76]

The main contributions are:

- it introduced blockchain technology into the field of outsourcing service payment, focusing on the issue of fair payment (covering the dual perspective of users and providers) to ensure the data integrity and the normal deployment and execution of services,
- and it designed a special transaction form named "deposit transaction" to constrain the behavior of provider and client in the payment, which was able to better protected the interests of both providers and users to some extent.

However, the interactions of BPay is quite complicated, which may affect its timeliness when used in the complex cloud outsourcing applications.

Blockchain-enhanced resource allocation and task offloading mechanisms

Blockchain is an effective way to construct a distributed and decentralized trust framework. However, the consensus mechanism requires a lot of energy consumption, preventing it from the best effect in a hybrid cloud-edge service model. Cloud mining, which encourages miners to purchase or rent resources from cloud providers, has become one of the possible solutions to the contradictions. In order to optimize the performance of blockchain applications based on cloud mining, Z. Xiong, et al. [77] used game theory to handle the interaction between cloud/edge providers and miners, and achieve distributed and fast proof of work through the Alternating Direction Method of Multipliers (ADMM) algorithm.

Figure 10 shows the PoW offloading to cloud or edge servers. The feature of this work is that it chose a different perspective from most blockchain-based applications to study how the blockchain consensus mechanism worked efficiently on resource-constrained terminal devices. And it used the multi-leader multi-follower game theory to solve the resource competition and allocation problem in the multi-providers and multi-miners scenario. However, the model only focused on the profit problem of task execution, and since the scale of test nodes is relatively small, its effectiveness in a real system cannot be confirmed.

Paper [78] also focused on the transactions between miners and cloud/edge providers. It proposed a market model for computing resource allocation, and achieved the optimization of wealth distribution through the auction model. The paper mainly considered two auction scenarios: fix resource for miners from providers, and miners freely compete resources. The feature of this work is that it considered the marketability of resource allocation and focused on the balance of distribution and maximization of benefits. Figure 11 shows the blockchain-based cloud-edge business ecosystem. Similarly, Paper [79] proposed a lightweight model for resource-constrained miners to offload computing tasks to cloud or edge, and a two-stage Stackelberg game to maximize and balance the benefits of cloud providers and miners.

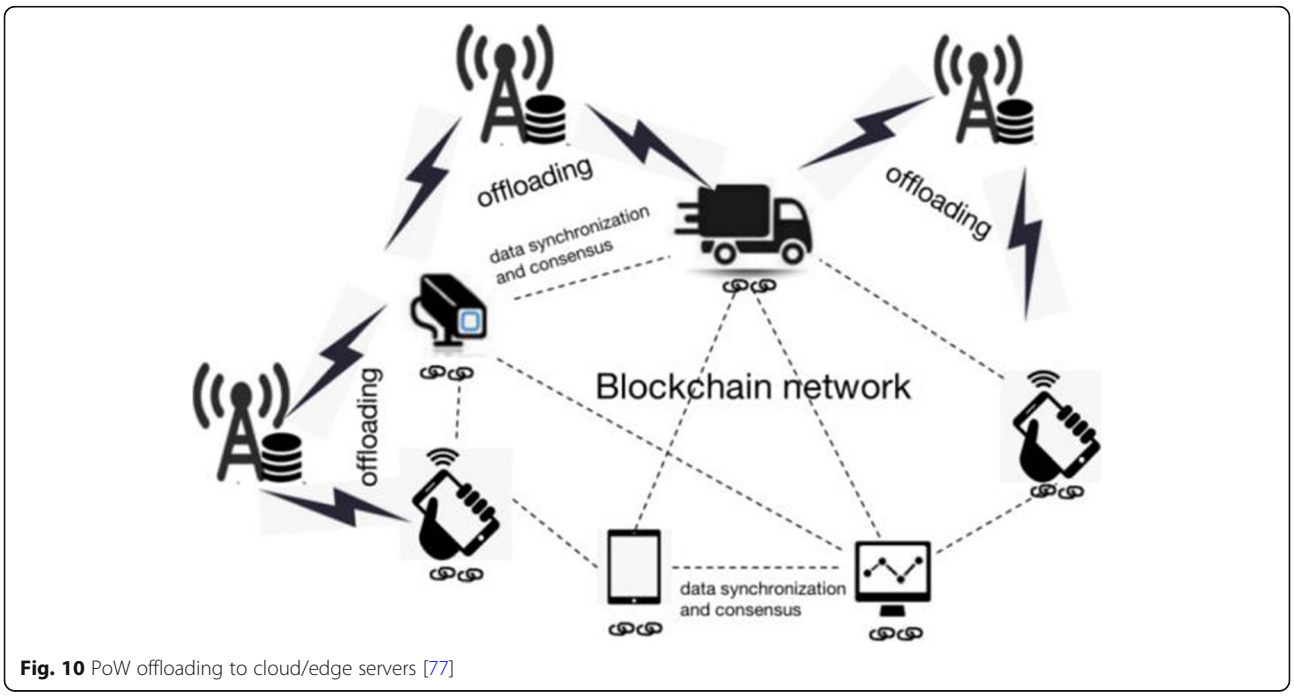

Fig. 10 PoW offloading to cloud/edge servers [77]

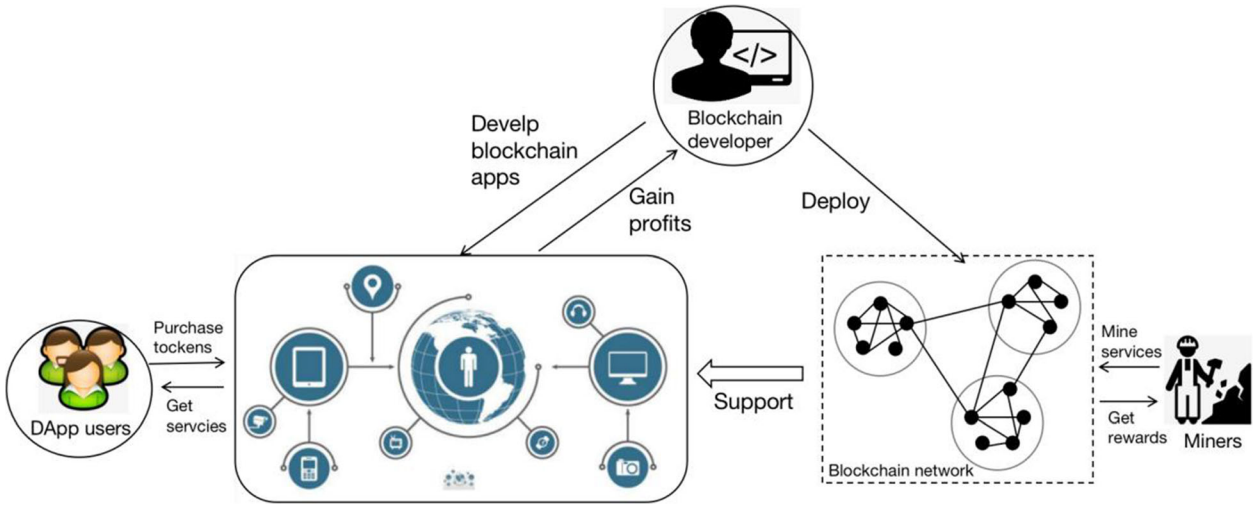

Fig. 11 Blockchain-based cloud-edge business ecosystem [78]

These two models both focused on how to help miners work effectively in a resource-constrained environment, and both adopted an economical method (game theory) for pricing when miners purchased resources, but they lacked the possible security and credibility analysis of their models.

Network function virtualization is a key technology of mobile edge computing. In order to improve the efficiency of resource allocation, X. Fu, et al. [13] proposed a blockchain-based network service virtualization framework to support anonymous login and virtual resource management strategies. This paper treated resource scheduling as a multi-objective optimization problem, while taking into account the requirements of service delay and operation overhead.

The main contributions of this paper are as follows.

- It introduced blockchain technology to enhance the credibility of resource allocation and proposed a distributed consensus mechanism to simplify the information collection and synchronization in the NFV-based edge computing systems.
- It treated the resource scheduling problem as a multi-objective optimization problem, which covered both the traditional system performance factors and trust factors and the trust mechanism covered both the credibility of blockchain nodes and the NFV-based MANO system.

Trust-enhanced cloud virtualization

Today Docker has become the most popular virtualization tool, because it greatly improves resource utilization of operating systems without much additional overhead. Authentication is critical for cloud users to determine whether an image is malicious or not. However, Notary the current authenticity solution of Docker is not strong enough to deal with attacks.

In order to cope with the potential threats in Docker Content Trust (DCT), Q. Xu et al. [80] proposed a blockchain-based trust model named Decentralized Docker Trust (DDT). The advantages of DDT include: it reduced the risk of DoS attacks, and it provided the digital signature verification services.

The contributions of the paper are as follows.

- It in-depth analyzed the technical architecture of Docker Content Trust, discussed whether Notary is useful in Docker trust management, and pointed out two major potential threats of DDT.
- It designed a novel blockchain-based Docker trust management framework and mechanisms, explained in detail how to deploy and implement the new model, and verified the model through prototype experiments.

However, the paper only conducts a prototype system and verifies the efficiency of the model by simulation experiments.

Comparison of the models

The summary of the comparison between the related works in the blockchain-enhanced trust interaction framework and mechanisms is given in Tables 4, 5 and 6.

Data management

Data access model

Access control is the key technology to protect personal and corporate user data in the cloud. However, the centralized access control strategies generally have

Table 4 Comparison of the applied methodology

Reference	Management mode	Application scenario	Performance test	Blockchain type	Main indicator
[70]	decentralized	Cloud transactions	Rinkeby (test net of Ethereum)	Ethereum	feasibility
[71]	decentralized	Cloud security management	Case study, simulation	Ethereum	integrity, availability
[72]	Semi-decentralized	Cloud manufacturing	Real testbed	Ethereum	applicability, reliability
[12]	Semi-decentralized	SDN-enabled 5G-VANETs	Simulation,Theoretical analysis	Not clear	security, privacy
[73]	decentralized	Cloud transactions	Real testbed	Consortium blockchain	security, tamper-resistant, effectiveness, efficiency
[74]	centralized	JointCloud	Theoretical analysis	Not clear	credibility
[75]	Semi-decentralized	E-commerce	Real testbed	Consortium blockchain	credibility, latency, throughput
[76]	decentralized	Cloud outsourcing	Simulation	Bitcoin	compatibility, robust, collision-resistance
[77]	Semi-decentralized	Cloud mining	Theoretical analysis, simulation	Public blockchain	convergence, profits
[78]	decentralized	Cloud trading	Simulation	Public blockchain	social welfare
[79]	decentralized	Cloud mining	Real testbed, simulation	Ethereum	distribution equilibrium
[13]	decentralized	Edge computing	Simulation	Not clear	trust, rewards
[80]	decentralized	Docker images	Prototype	Bitcoin	scalability, efficiency

risks of privacy leakage or hacker attack risks. Therefore, C. YANG,et al. [14] proposed a blockchain-based access control framework, named AuthPrivacyChain. AuthPrivacyChain used the addresses of entities in blockchain as the unique IDs, and designed related identity authentication and access control mechanisms. By utilizing the decentralized nature of blockchain, it realized the distributed and decentralized cloud access control framework, improving the privacy and security of data applications. Figure 12 shows the main authentication process of AuthPrivacyChain.

The main contributions of this paper are:

- it designed a decentralized identity management framework based on blockchain to implement the related strategies like data access control and authorization,

Table 5 Comparison of performance test

Reference	Efficiency	Overhead	Effectiveness	Trust accuracy	Throughput	Security/ Privacy
[70]		√				
[71]			√			
[72]		√	√			√
[12]	√	√	√		√	
[73]	√			√	√	
[74]	√					√
[75]	√				√	
[76]	√	√	√			
[77]	√					
[78]	√			√		
[79]	√					
[13]						√
[80]	√	√		√		√

Table 6 Comparison of main contributions

Reference	Target & contribution	Improvement in Blockchain	Solution to attack
[70]	Ensure the enforcement of cloud service SLA through blockchain technology	Witness-pool smart contract, specific-SLA smart contract	/
[71]	Blockchain and SDN hybrid architecture to enhance the integrity of cloud resource management	/	Malicious Hosts abusing the cloud platform
[72]	hybrid blockchain-based cloud manufacturing platform	Resource smart contract (RSC), Job smart contract (JSC)	Single point of failure
[12]	Blockchain-based security framework to solve privacy and security issues in the transportation system as well as in SDN-enabled 5G-VANET [12]	Combination of proof-of-work and proof-of-stake	Privacy leakage, Malicious traffic broadcasting
[73]	Design a Cleanroom Security Service Protocol (CSSP) to secure software deployment and usage based on a consortium blockchain framework [73]	/	/
[74]	Design a dynamic and customized reputation system framework to manage the reputation of cloud providers using blockchain to prevent the malicious tampering [74]	/	/
[75]	Secure E-commerce transactions based on ETTF, a decentralized trusted trading framework	Peer blockchain protocol (PBP) and ECA: E-commence consensus algorithm	
[76]	Fair payment framework for cloud outsourcing services	/	/
[77]	Use game theory to improve the performance of cloud mining	/	/
[78]	Design an auction-based market model to maximize the profits of provider and miner in cloud mining	/	/
[79]	The pricing scheme in cloud mining to reach the Stakelberg equilibrium	/	/
[13]	Blockchain-based NFV framework for resource allocation in MEC	Blockchain-based NFV framework for resource allocation in MEC	/
[80]	Blockchain-based decentralized Docker trust model	Carbonchain library	Dos Attack

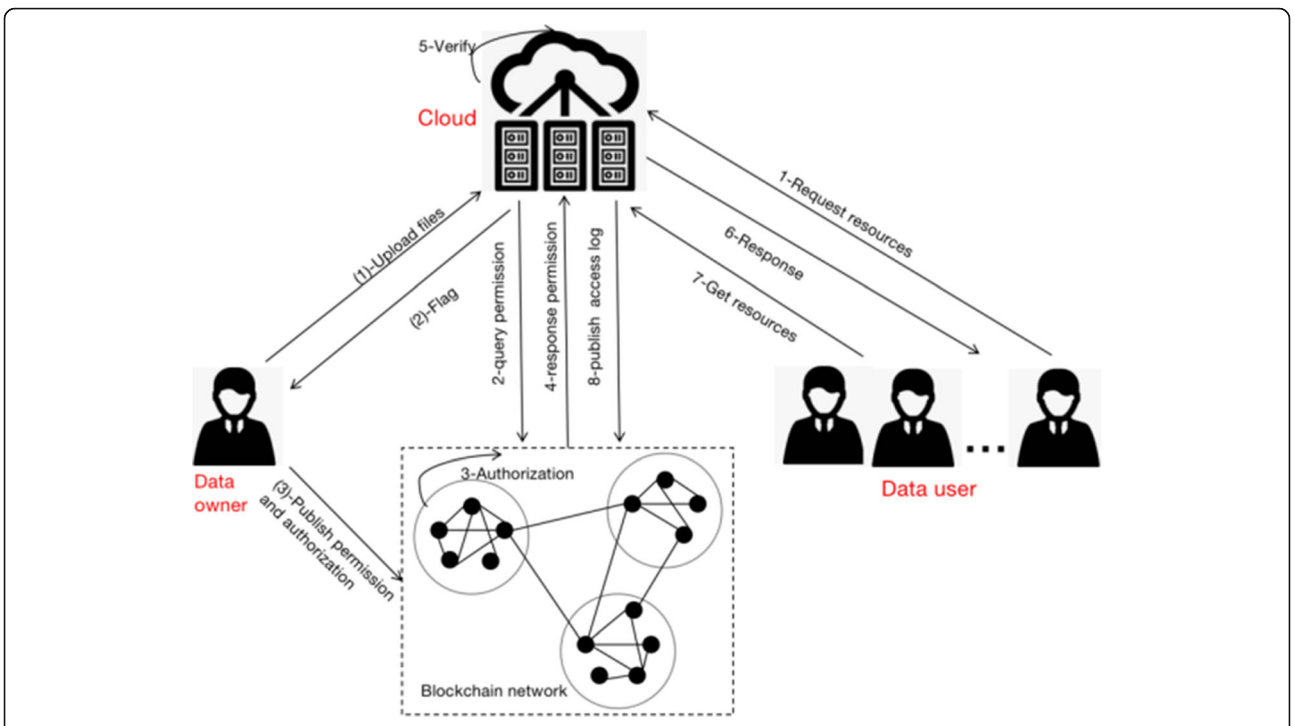

Fig. 12 Main authentication process of AuthPrivacyChain [14]

- and it enhanced the privacy protect of user data, which can effectively resist the internal and external attacks.

However, this paper only conducted the limited performance tests and compared with two basic models.

In order to reduce the misuse and abuse of IoT devices, K. Kataoka et al. [81] proposed a trust management method by integrating blockchain and SDN (Software-Define Networking). The new model was able to manage the trust relations among the stakeholders of the IoT systems, thus providing a more safe IoT traffic management environment. The authors verified the model by time, duration and cost. Figure 13 shows the trust-enhanced routing under the integration of blockchain and SDN.

The contributions of the paper include:

- it helped cloud user to identify the credibility of IoT services at the edge computing level, thus avoiding incredible data flow, and it proposed a 2-step protect process and trust-based interactions, which enabled participants to perceive and interact, achieving a whitelist-like similar effect,
- it integrated blockchain with SDN and adopted a dual software node structure along with two types of data structures (service profile and device profile) to deploy and implement trust, realizing the identification of software and hardware, and it proposed a new consensus mechanism of proof-of-concept.

However, the management overhead of the model was huge and the scheme had not been deployed in a real system.

S. Tuli et al. [82] proposed FogBus an IoT-Fog/Edge-Cloud integration framework to achieve a more efficient IoT deployment and resource management. FogBus applied blockchain to improve the security and integrity of operations on sensitive data. Compared with the existing related frameworks, FogBus was lightweight, responding quickly and was capable of controlling fog/edge and IoT devices. However, the embedded blockchain mechanism still needed improvement, especially the time latency and consensus mechanisms.

The contribution of the paper lies in that it introduced in detail the necessity and requirements of the IoT-Edge-Cloud hybrid computing framework, and it discussed the software & hardware design and implementation of the new model. Unfortunately, it does not elaborate on how to deploy blockchain in the model.

D. Medhane, et al. [83] proposed a distributed security framework based on blockchain, cloud computing, edge computing and SDN for the next generation IoT applications, which could be used to detect and avoid security attacks. The advantage of the hybrid service framework is that it was able discover attacks against identification quickly, as shown in Fig. 14.

J. Lee, et al. [84] proposed a blockchain-based distributed IoT security framework that integrated IoT, fog computing and cloud computing, and it designed a delay-aware construction algorithm DATC to reduce mobile application delay and triangular routing problems. The advantage of this paper is that the consensus mechanism used a RSA-based EPID scheme and a delay aware tree to evaluate the service delay. The author believed that they were the first work in blockchain technology to consider node mobility and network delay. However, it only evaluated the performance (service delay) of the model with the random method.

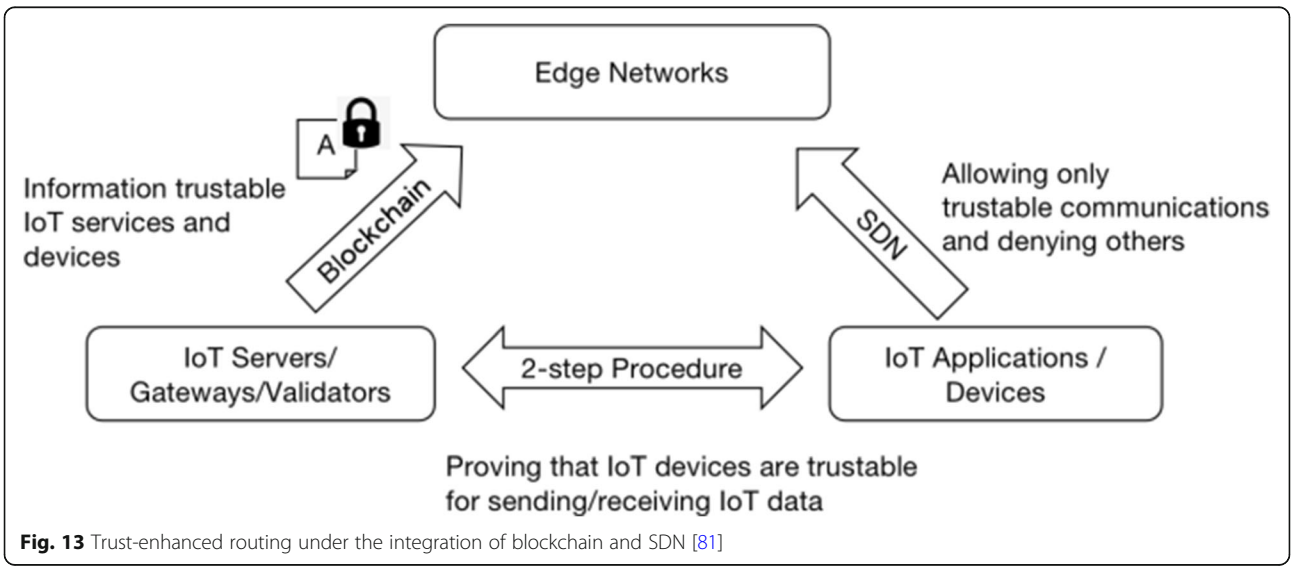

Fig. 13 Trust-enhanced routing under the integration of blockchain and SDN [81]

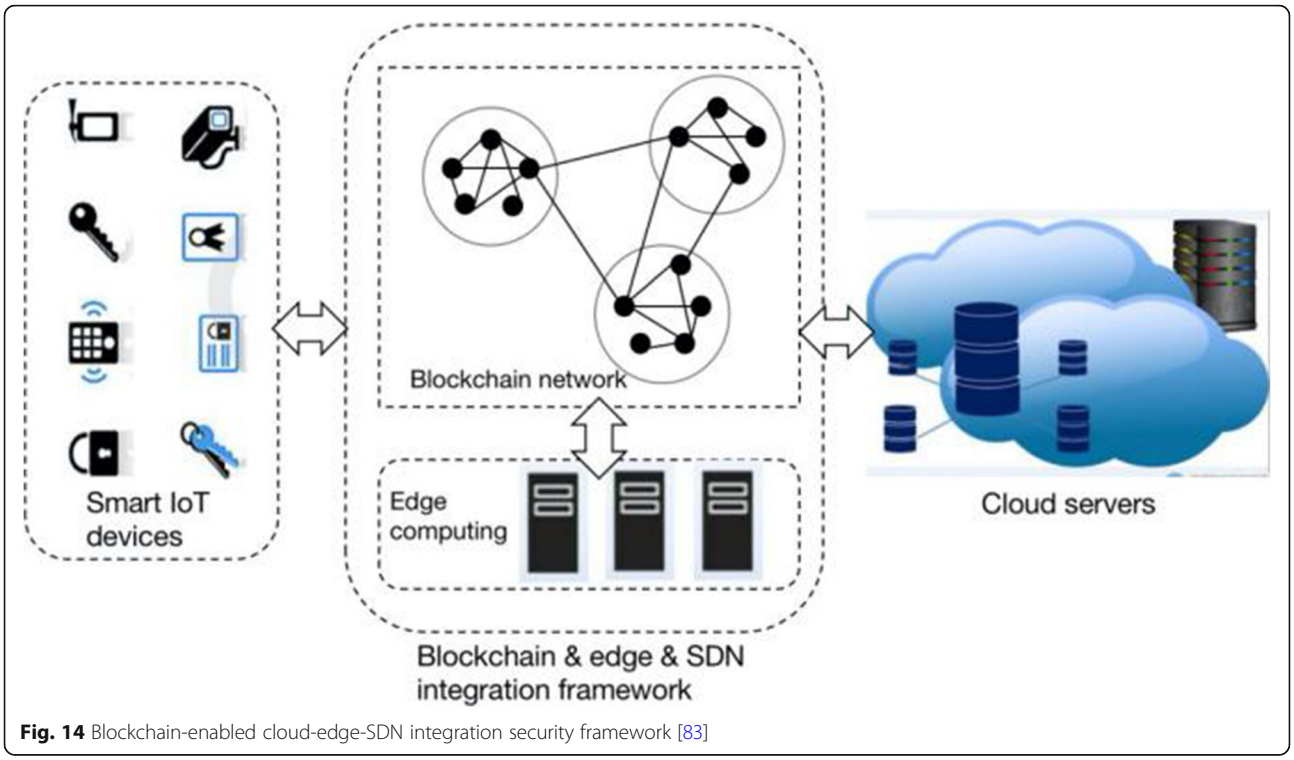

Fig. 14 Blockchain-enabled cloud-edge-SDN integration security framework [83]

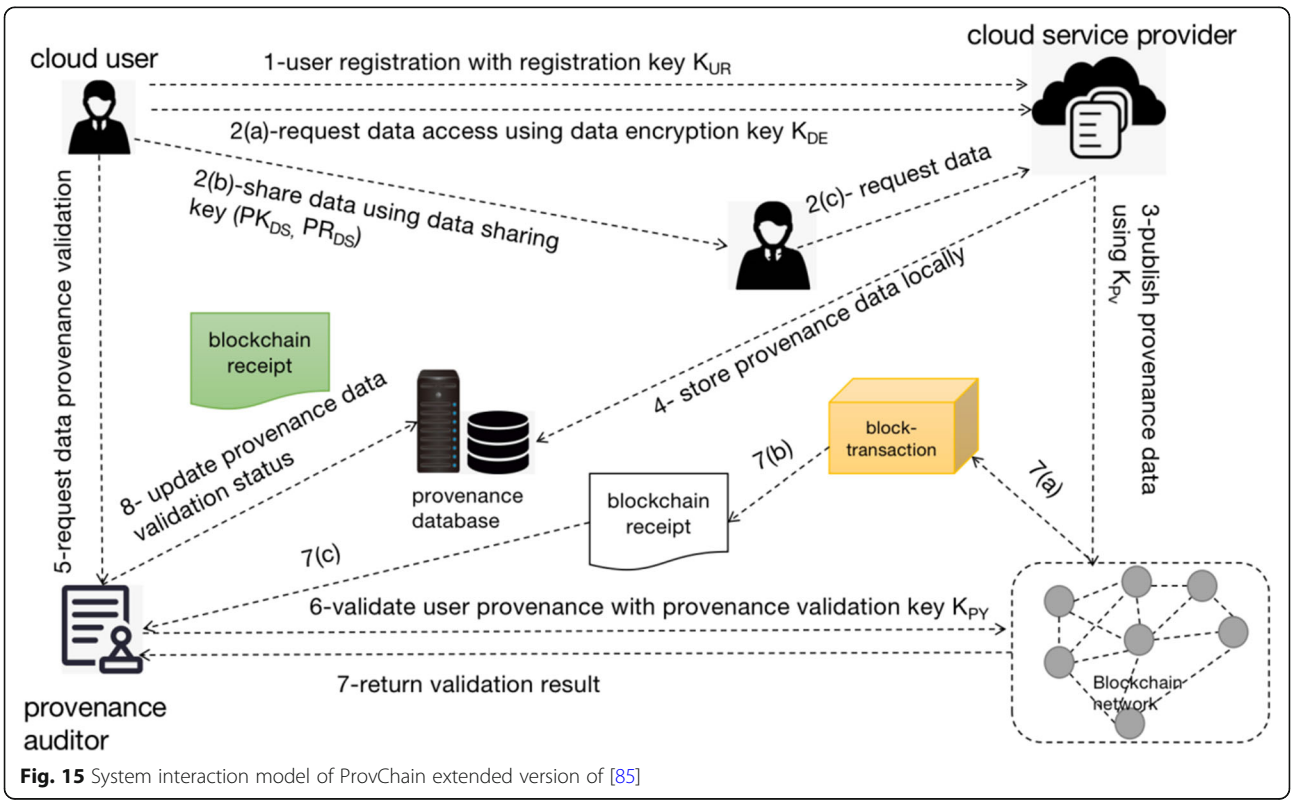

Fig. 15 System interaction model of ProvChain extended version of [85]

Data provenance

Data provenance records the history of a data object, which is essential for traceability, auditability, accountability, and privacy protection in cloud. However, the state-of-the-art research on data provenance is often too complex and lacks effectiveness. Based on the blockchain technique, X. Liang et al. [85] proposed a decentralized data provenance architecture named ProvChain for cloud. ProvChain stores the provenance data in blockchain to make data operation transparent and traceable, thereafter establishing a trustworthy relationship among entities in cloud markets.

Figure 15 shows the system interaction model of ProvChain. In the proposed platform, regardless of the operation storing, sharing or obtaining data, it was recorded as a transaction in the blockchain network, and also the provenance data was stored in the provenance database.

The contributions of the paper include:

- it proposed a data provenance architecture which was able to record and audit the data manipulation history in cloud data storage, and it adopted a three-layered implementation architecture to realize a complete life-time data protection,
- and data security was guaranteed by data encryption and the multi-key measures (registration key, data encryption key, data sharing key, data source key).

However, in the scheme, only the data of one single cloud provider could be authenticated, while the verification of cross-cloud, multi-clouds or federated clouds was not achieved, and the interoperability, data sharing and management in a multi-cloud environment was not handled well.

Currently, cloud computing is meeting the era of Internet of Everything (IoE), where massive amounts of data are generated in cloud systems. How to ensure data reliability and traceability has become a significant

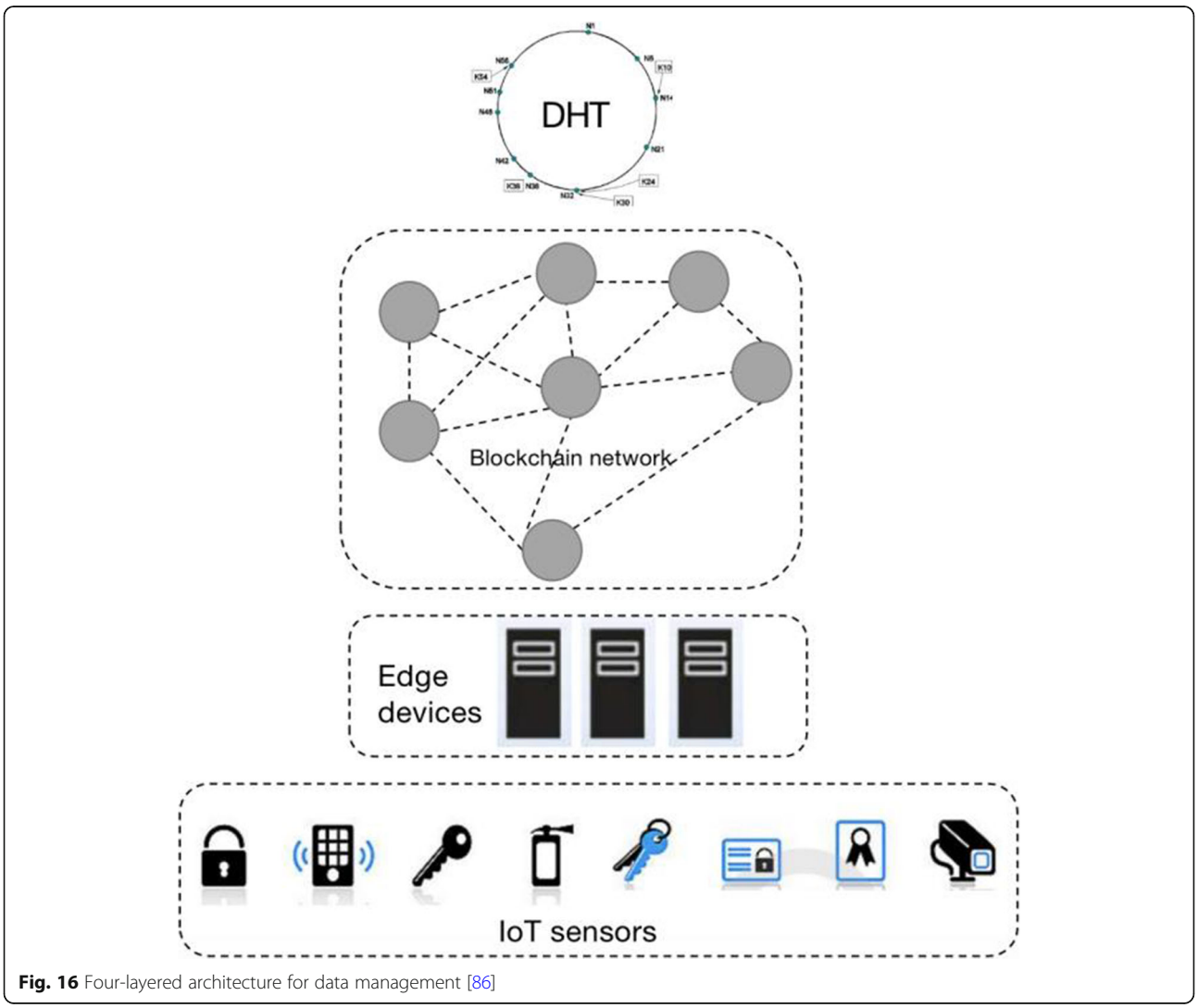

Fig. 16 Four-layered architecture for data management [86]

challenge. To improve the security and accountability of IoT storage platform, R. Li et al. [86] designed a distributed data storage model based on blockchain technology. Edge devices were added to help IoT devices perform encryption and decryption operations. Blockchain plays a role in this paper as a third-party trust authentication authority. Figure 16 shows the four-layered architecture of the model, in which numerous IoT sensors gather data to the edge devices, while edge writes the data into blockchain layer as transactions, and finally records it to the DHT network. The security of the model including protocol security, privacy, traceability and statistics are theoretically proven.

The main contributions of the paper include:

- it designed a decentralized IoT data management, storage, and privacy protection framework, and proposed an IoT & edge hybrid computing architecture to improve the computing power of IoT devices,
- it introduced a blockchain-based certificateless encryption method to achieve the certification and auditing, and it created the unique types of transactions, like data storage services and data access services.

However, the ID-based access control in this scheme cannot be applied to a more complex authorization scenario, and only the theoretical model is provided.

In order to protect the life cycle security of IoT data, H. Shafagh et al. [87] presented a data storage and sharing model based on blockchain.

The main contributions of the work are: it considered the life cycle security of IoT data, and it set up a grading policy to secure data management system, including three different levels.

However, it did not elaborate on how to implement the consensus and incentive mechanisms of blockchain, and the performance analysis was only theoretically carried out, without the experimental design.

B. Yu et al. [88] investigated the security and data privacy problems in IoT networks and designed a blockchain-based decentralized trust model for secure data management in IoT trading. Through a case study of a wearable device, the feasibility of blockchain for trust-enabled IoT trading was made evident. In addition, this work gave a brief introduction on the challenges for future research in building a trustworthy trading platform for IoT ecosystems.

The contributions of the paper are:

- it provided a detailed analysis of the trust crisis in the IoT ecosystem and discusses the advantages of using blockchain to construct a distributed trust framework,
- it illustrated the implementation of a blockchain-based IoT trust platform using a case study of data traceability of wearable medical devices, and it identified the prospects of future research in this field.

However, the framework of the blockchain-based IoT commodity was only theoretically defined and explained by the case study.

Vehicle Edge Computing enhances the computing power of traditional VANETs, however with many new challenges, particularly serious security and trust risks. Based on blockchain technique, Yang et al. [89] proposed a distributed and decentralized trust management model for vehicular networks, as shown in Fig. 17. By utilizing the Bayesian Inference Model, vehicles were able to validate the messages received from their neighborhoods. In the proposed model, RSUs were responsible for evaluating the trust of the message to the related vehicles. They loaded the trust data into a "block" and tried to add the block to the trust chain. To help RSUs reach consensus, the paper designed a new consensus mechanism of joint Proof-of-Work and Proof-of-Stake. Two kinds of attack sources were considered in the model: attacks from malicious vehicles including message spoofing attacks, bad mouthing and ballot stuffing attacks, and attacks from compromised RSUs.

The authors of the paper believed that an excellent trust model must incorporate the features of decentralization, tamper-proofing, consistency, timeliness, and availability, and they proved that blockchain technology was able to achieve these goals.

The highlights of the paper are:

- it designed a blockchain-based distributed reputation management scheme for vehicular networks, and it proposed a hybrid consensus mechanism that combines Proof-of-Work and Proof-of-Stake to update trust,
- and the evaluation of message credibility takes into account a variety of factors like distance.

However, the performance of the model was verified only on the simulation platform MATLAB.

Data storage

Data storage is an important type of cloud services. In view of the data application security, privacy leakage and trust crisis, as well as the performance bottleneck and single point of failure in the centralized data management center, researchers have proposed many distributed and blockchain-based schemes.

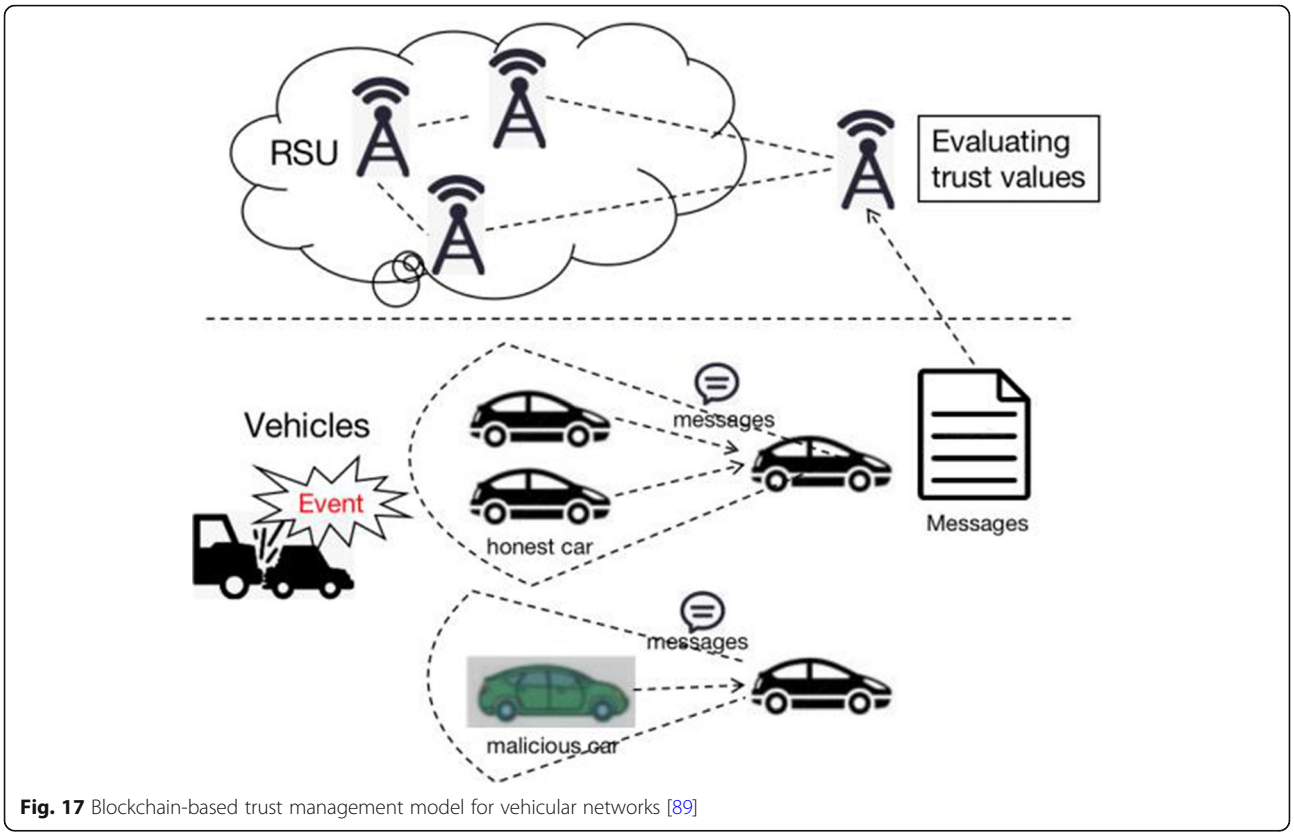

Fig. 17 Blockchain-based trust management model for vehicular networks [89]

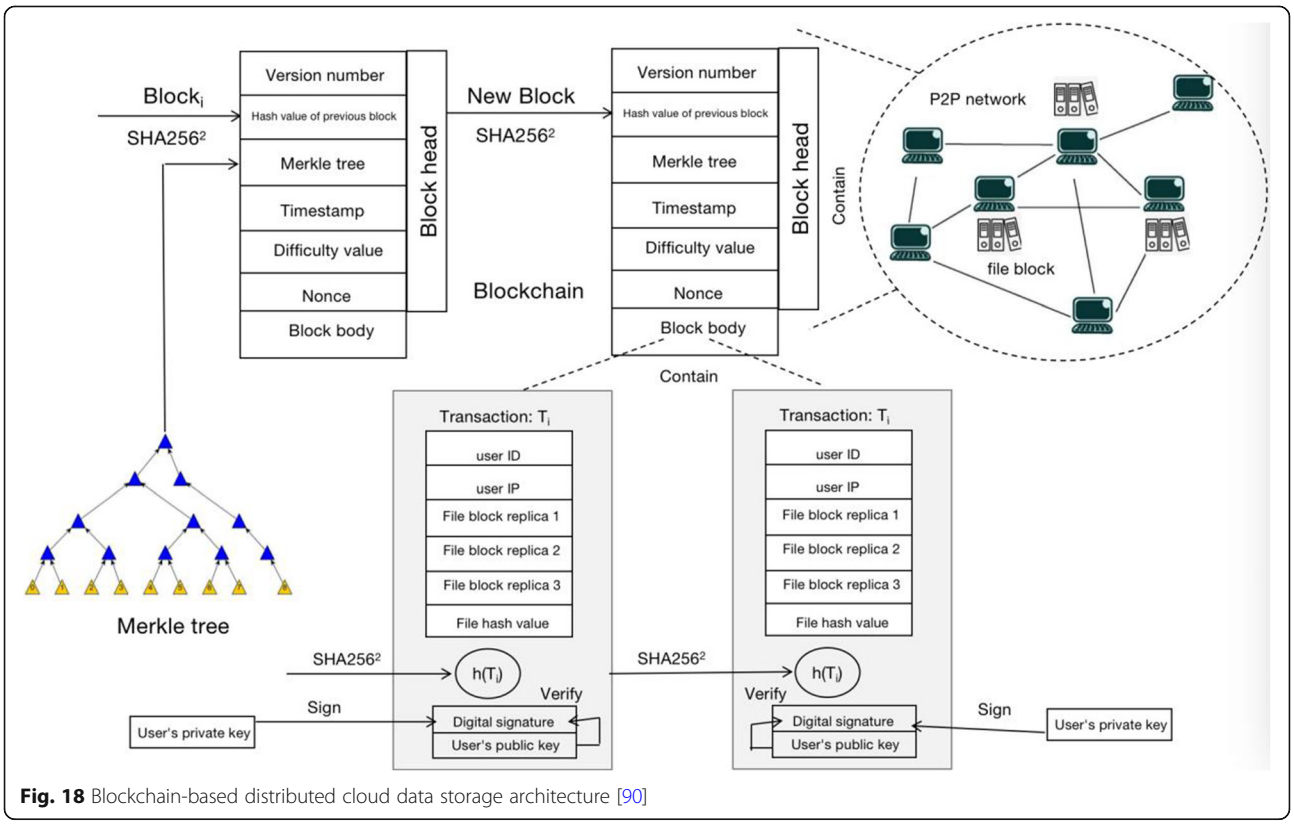

Fig. 18 Blockchain-based distributed cloud data storage architecture [90]

J. Li, et al. [90] proposed a blockchain-based distributed cloud storage security architecture, and designed a customized genetic algorithm to deal with the problem of copy distribution, thus to improve the performance and security of storage management. In the proposed architecture, the user files were divided into equal-length file blocks, and then encrypted, digitally signed and stored in the P2P network, shown in Fig. 18. The blockchain-based transactions were also designed, including user renting cloud storage or renting their own free space. The storage-related operations to each file block were recorded carefully in the body of each block in a safe, orderly and traceable manner.

The advantages of the model are as follows.

- It gave a comprehensive and detailed discussion on how to decide the number of copies in a distributed storage system.
- It used a generic algorithm to solve the problem of copy replacement between multiple users and multiple data centers, and it maintained the file loss rate and transmission delay in a very low level.

In order to improve the security and effectiveness of data sharing, the fairness of data distribution, and protect the profits of data owner in a multi-cloud environment, Paper [91] proposed a novel architecture based on blockchain technology, as shown in Fig. 19. The architecture contained four parts: cloud users, the data service agent (a third-party agency), the blockchain network, and data owners. The users sent data sharing request through the service agent, and obtained the corresponding data service after identity authentication and permission evaluation on blockchain. All data manipulation behaviors were recorded in the blockchain network.

The main contribution of the paper include:

- it proposed a data sharing business model based on blockchain for multi-cloud environment to protect data security and privacy,
- and it built a dynamic and fair data sharing and incentive mechanism by using the Shapley value.

However, it is not a completely decentralized trust mdoel, since the deployment of the model still relied on a credible third party agency.

The "one-bit-return" protocol is usually adopted in traditional cloud storage model for data deleting, which may easily lead to the unreliable deletion results. And other deletion strategies also have disadvantages such as non-verifiable deletion results, requires a trust third party for verification and low efficiency. To this end, C. Yang, et al. [92] put forward a blockchain-based data deletion scheme to improve the verifiability, efficiency and transparency. Figure 20 shows the basic steps in data storage. All data/file operations are recorded through the blockchain to ensure that the deletion of data on the server is honest. However, this method can only be used in the limited application of credible file deletion.

The traditional file timestamp strategy requires a credible third-party service provider (TSP), which may easily lead to reliability and single point of failure risks, along with the huge communication cost. Therefore, Paper [93] proposed a blockchain-based precise time stamping scheme for outsourcing data called Chronos+. In Chronos+, both storage and timestamp services were provided by cloud service providers to ensure the accuracy, security, scalability and effectiveness of file storage services.

The main contributions of this work are:

- it offered a detailed analysis on the timestamp required outsourcing file protection strategy, and pointed out the potential risks,
- and it proposed a batchable and customized time-stamping solution based on Ethereum, which could ensure the accuracy, security and scalability of cloud storage.

L. Zhu, et al. [94] designed a data management model for cloud computing systems using blockchain

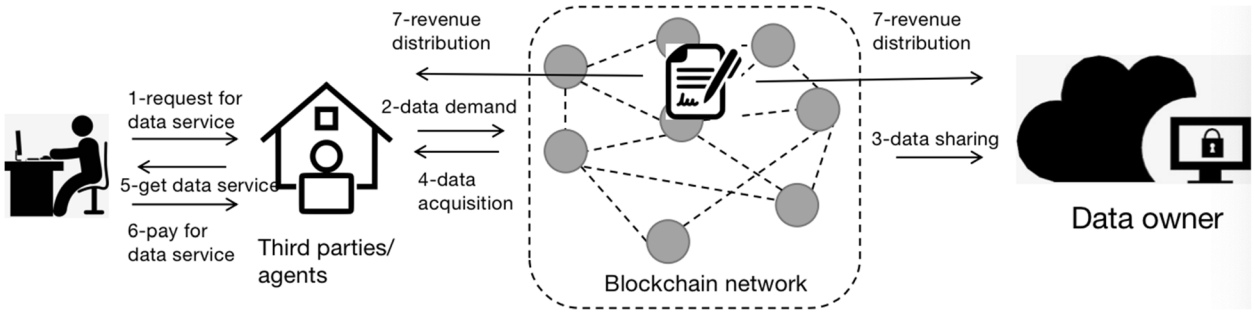

Fig. 19 Data sharing architecture for cloud data sharing [91]

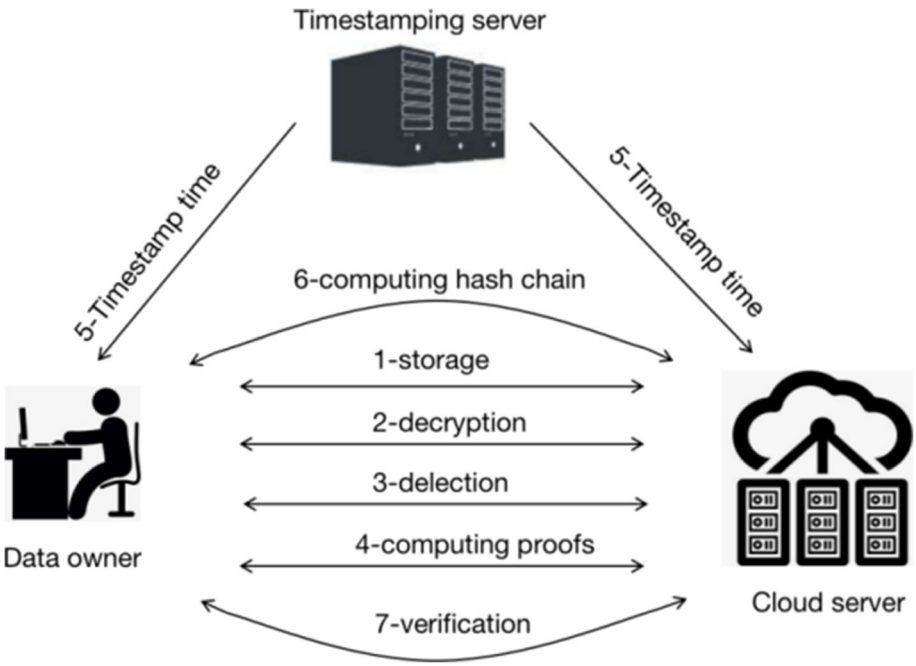

Fig. 20 Basic steps in data deletion [92]

distributed consensus mechanism and a third-party trust center. The uniqueness of this work is that it used both the ordinary voting nodes and the higher-level third-party trust authorities for transaction verification, which can be seen as a compromise strategy of blockchain and the traditional centralized architecture. The model improved the efficiency of consensus and dispute handling. However, it is not a completely decentralized and self-management and evolutionary trust model.

To enhance the security of data storage and sharing in VECONs, J. Kang et al. [95] established a distributed data management system based on the consortium blockchain framework and designed a series of smart contracts to achieve security, efficiency and privacy in data sharing and storage. In addition, they developed a three-weight subjective logic- based reputation model to improve the credibility of data.

The contributions of the paper include:

- it analyzed the possible reasons causing the RSUs to be compromised, and then proposed a two-blockchain frameworks (data storage blockchain and data sharing blockchain) to ensure the security of mobile data management,
- it proposed a new consensus mechanism of Proof-of-Storage, and a reputation evaluation model based on subjective logic for the high efficient and automatic data management without the need for authorization and authentication in second-hand data sharing.

The limitation of the model is that it does not explain how to determine the configuration of the related parameters, such as the setting of trust threshold, which has a great impact on whether the malicious vehicles can be effectively captured.

Comparison of the models

The summary of the comparison between the related works in the cloud data management is given in Tables 7, 8 and 9.

Summary of the comparison

In this section, we concludes the comparison of the blockchain-based trust management approaches in cloud computing systems.

These 35 blockchain-based trust management approaches are the research results of the last 3 years, showing that the blockchain-based scheme is very new and represents the latest trend in building decentralized and distributed trust. From the perspective of country distribution, 18 came from China, 5 from the United States, 4 from Singapore, and the rest came from 8 different countries (Australia, Germany, India, Argentina, Netherlands, Algeria, Switzerland and France), indicating that the scheme has been widely recognized by different research institutions of the world. Academics from China, the United States, and Singapore focus more on this method. From the perspective of areas of interest, the researchers from China focus on blockchain-based basic trust frameworks, and blockchain-based cloud

Table 7 Comparison of the applied methodology

Reference	Management mode	Application scenario	Performance test	Blockchain type	Main indicator
[14]	decentralized	Cloud access control framework	prototype, simulation	Public blockchain	decentralized, confidentiality
[81]	decentralized	IoT traffic management	Real testbed	Both Public and private blockchain	credibility, scalability, authenticity
[82]	Semi-decentralized	IoT & Fog &Cloud integration framework	Prototype	Not clear	light-weight, efficiency, energy consumption
[83]	decentralized	Security framework for IoT platform	Simulation	Not clear	energy consumption, throughput, latency
[84]	Semi-decentralized	IoT data management	Simulation	Not clear	data confidentiality, integrity, availability
[85]	Semi-decentralized	Data provenance architecture for cloud systems	Simulation	Private blockchain	data provenance, privacy, availability
[86]	Semi-decentralized	IoT data storage and protection	Theoretical analysis	Not clear	security, privacy, traceability, accountability
[87]	decentralized	Auditable IoT data storage and sharing	Theoretical analysis	Bitcoin	decentralized, distributed, resilient, auditable traceability
[88]	decentralized	Trust management in IoT ecosystem	Theoretical analysis, case study	Both Public and private blockchain	security, privacy
[89]	decentralized	Decentralized Trust Management in Vehicle Networks	Simulation	Consortium blockchain	decentralized, tamper-proofing, consistency, timeliness, availability
[90]	decentralized	Cloud storage based on P2P architecture	Simulation	Not clear	data security, latency
[91]	decentralized	Data sharing in multi-cloud environments	Simulation	Consortium blockchain	profits, security
[92]	decentralized	Data deletion in cloud storage	Theoretical analysis, simulation	Not clear	correctness, completeness, accountability, tranceability
[93]	decentralized	Time stamping in cloud storage	Simulation	Public blockchain	accuracy, security
[94]	Semi-decentralized	Cloud data management	Simulation	Ethereum blockchain	controllability, privacy-preserving, openness and transparency
[95]	Semi-decentralized	Secure data sharing in Vehicle Edge Computing	Simulation	Consortium blockchain	security

Table 8 Comparison of performance test

Reference	Efficiency	Overhead	Effectiveness	Trust accuracy	Throughput	Security/ Privacy
[14]	√				√	√
[81]	√	√				√
[82]	√				√	
[83]	√	√			√	√
[84]	√					
[85]	√	√			√	
[86]			√			√
[87]		√				√
[88]						√
[89]			√			
[90]	√					√
[91]	√					√
[92]	√					√
[93]	√	√	√			√
[94]	√	√				√
[95]			√			

Table 9 Comparison of main contributions

Reference	Target & contribution	Improvement in Blockchain	Solution to attack
[14]	Decentralized access control for privacy protect	/	/
[81]	Trust management among IoT-related stake-holders by integrating blockchain and SDN [81]	proof-of-concept (PoC)	DDoS attacks on edge networks
[82]	An IoT-Fog/Edge-Cloud integration framework to facilitate end-to-end operations on sensitive data	/	/
[83]	Combination of blockchain, edge computing, cloud computing, SDN to construct a security framework for IoT applications	User registration, data confidentiality estimation, shortest path finding, attack detection and avoidance	probable single or cooperative security attacks
[84]	IoT-Fog-Cloud hybrid framework for secure and efficient IoT applicaitons	delay aware tree construction (DATC) algorithm and a RSA-based EPID scheme	/
[85]	A blockchain-based framework to manage data provenance of cloud including data collection, data storage and data validation [85]	/	/
[86]	Distributed solution for large-scaled data storage and protection [86]	Blockchain transactions	/
[87]	Three levels of requirements for system security [87]	/	/
[88]	Trust management in IoT ecosystems, distributed management of the IoT device life cycle and data privacy	Smart contract logic	/
[89]	A decentralized trust framework in vehicle networks to defend against malicious vehicles and RSUs [89]	/	Message spoofing attack, bad mouthing and ballot stuffing attack, compromised RSU
[90]	A blockchain-based security framework for cloud file storage and solve the file block replica placement	/	/
[91]	Incentive mechanisms for data sharing in multi-clouds systems	Combination of PoW, PoS, PBFT	/
[92]	Blockchain-based data deletion scheme	/	/
[93]	Blockchain-based time stamping scheme for cloud storage	/	malicious file owner, malicious competitor
[94]	Hybrid data management model to achieve storage efficiency	User registration algorithm, voting and counting algorithm	User Collusion Attack
[95]	Consortium blockchain to secure data management in VECONs, and a reputation-based data sharing scheme	Data Storage Smart Contract (DSSC), Information Sharing Smart Contract (ISSC) [90], combination of proof-of-storage and proof-of-work	abnormal vehicles

service applications (including cloud storage and IoT applications), the US is more concerned with trusted data provenance and data storage applications, and researchers from Singapore pay attention to blockchain-based cloud resource allocation schemes.

From the perspective of model performance argumentation, 7 of the 35 papers used theoretical argumentation and analysis methods, 20 used simulation experiments, 2 chose a prototype system, and 6 were on real testbed. This indicates that blockchain-based trust management is still in the research stage and there is still a long way to the actual application.

The performance of the approaches were tested from different perspectives, such as trust/reputation accuracy, effectiveness, efficiency, overhead, system throughput, etc. However, parts of the performance tests were done by theoretical argumentation or case study.

By introducing blockchain technology, 22 of the 35 articles adopt a completely decentralized trust management model, 12 adopt a semi-decentralized model, and only 1 uses a centralized model, indicating that blockchain is sufficient to set up a decentralized trust framework and a non-tampering authentication model.

However, these papers are very different in the following aspects.

- They applied blockchain-based trust management schemes in different environments, such as IoT, cloud computing, E-Commence, vehicular networks, etc.

- They involved different dimensions of trust, such as identity authentication, reputation management, data traceability, etc.
- and they focused on different performance aspects of related systems, such as privacy, efficiency, latency, throughput, energy consumption, etc., showing that different authors pay attention to different research and optimization points.

In addition, 12 of the 20 articles clearly analyzed the aimed attacks that could be dealt with in distributed decentralized architecture, including attacks on application scenarios and attacks against the chain structure.

Obviously, the structure of a public blockchain is more suitable for building a point-to-point fully distributed, decentralized trust framework. However, a private blockchain or alliance blockchain has its own application field, such as in a closed or semi-closed system with a clear organizational structure, for example, IoT plus cloud hybrid computing environments. Therefore, 17 of the 35 articles used public blockchain (Bitcoin or Ethereum) as the infrastructure for building trust relationships, 5 used Consortium blockchain, 2 used a private blockchain, 2 allowed both public and private blockchain, and 9 did not specify the type of blockchain they used.

Unfortunately, when utilizing blockchain technology, none of the work provided a full discussion on how to deal with smart contracts, consensus mechanisms, and incentive mechanisms, possibly because few of them had been implemented in a real system, thus no detailed description on how to implement the related mechanisms. In addition, few papers discussed how to select miners, how to encourage miners to actively generate a block containing a node's behavior trust. In terms of consensus mechanisms, most papers still used traditional mechanisms, such as proof-of-work, proof-of-stake or a combination of the two, except a few works, for example in [67, 70, 75, 81, 95] which provided their own methods. This shows that the blockchain-based trust framework still has many open issues in relation to implementation and deployment and deserve further study and clarification. Table 10 shows the summary of the comparisons.

A trust management model based on cloud-edge hybrid architecture

Trust management framework based on cloud-edge hybrid architecture

In order to utilize the massive computing and processing capabilities of a traditional cloud computing datacenter without losing the advantages of the end-to-end, decentralized, data preservation features of blockchain technology, this paper proposes a novel cloud-edge hybrid trust management framework, as shown in Fig. 21.

The framework contains the following three layers: blockchain trust layer, edge/fog trust management layer, and cloud trust management layer. The blockchain trust layer implements the peer-to-peer interconnection through the ubiquitous sensing components and communication protocols over the traditional IoT infrastructure layer and constructs distributed and decentralized trust management through blockchain architecture. Since terminals are unable to handle complex cross-group/cross-cloud trust management, an edge/fog trust layer is introduced. The edge/fog trust layer consists of a large number of edge/fog servers deployed at network edge (trust management tasks can be part of the responsibility of a common edge/fog server). MEC servers are much closer to the user/terminal than the centralized cloud server and are more capable than the terminals. Therefore, they can ensure lower latency and meet the needs of cross-group or cross-domain interactions. The cloud trust layer is located at the top of the trust management framework. It is mainly used to deal with some high-level and highly complex tasks, such as trust data mining and behavior/preference analysis, which impose high requirements on computing and storage capacity and relatively loose requirement on the response time.

Cloud service transaction model based on a double-Blockchain structure

A complete trust authentication system includes identity authentication and behavior evaluation. In general, the identity information of a node is statically stable and relatively easy to authenticate and evaluate, even in a P2P network topology. In contrast, trading behavior is dynamic, requiring a lot of computing power to record and evaluate. Therefore, to improve the integrity and

Table 10 The summary of the comparisons

Model argumentation method			Trust construction mode		
Theoretical argumentation (%)	Simulation or prototype (%)	Test bed (%)	decentralized (%)	Semi-centralized (%)	Centralized (%)
7/35 = 20%	12/35 = 62.86%	6/35 = 17.14%	22/35 = 62.86%	12/35 = 34.29%	1/35 = 2.85%
Able to deal with network attacks (Reference Id)			Improvement in the deployment and realization of blockchain (Reference id)		
[12, 65, 69, 71, 72, 80, 81, 83, 89, 93–95]			[67, 70, 75, 81, 95]		

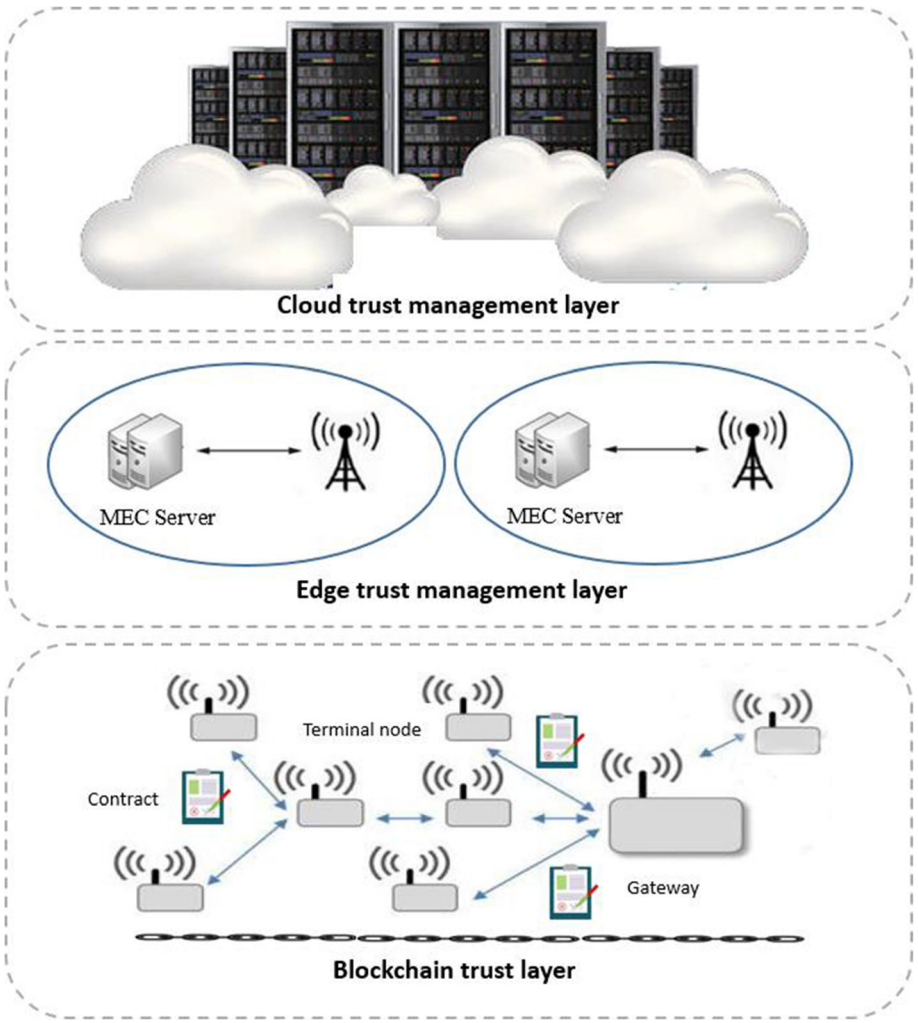

Fig. 21 Cloud-edge-end hybrid trust management framework

efficiency of trust certification in real-time transactions, a cloud service transaction model based on double-blockchain structure is proposed, as shown in Fig. 22.

Trust authentication Blockchain (TAB)

TAB is responsible for managing trust data in cloud service markets and provides trust evaluation results to other nodes. Each block in TAB contains two parts: identity trust data and behavior trust data. When a node initially joins, only identity trust is added in a block, however, as time goes by and as transactions progress, its behavior trust is continuously written in a new block. Authentication is completed by a small number of supervisors, who can be normal miners or special nodes elected by the market authority. Miners are responsible for storing and authenticating trust data and ensuring the consistency of the data through specifically designed consensus mechanisms. When nodes apply to enter the trading network, they must pay a fee to run a smart contract for the initial identity authentication. In addition, when they want to obtain the trust data of other nodes, they also pay a fee. This funding provides the incentive fee for the miners.

Trading behavior Blockchain (TBB)

TTB is responsible for generating and storing the trading data block. In TBB, the miners have two tasks, one is to receive the latest transaction results and generate the transaction block, and the other is to evaluate behavior trust, generate a trust block, and then forward it to TAB. The corresponding trust block will be confirmed and stored by the miners in TAB.

Double-Blockchain structure

With the benefits of the double-blockchain structure TAB + TBB, double-chain parallel computing can be realized, which improves computational efficiency. In addition, double-chain mutual supervision provides a

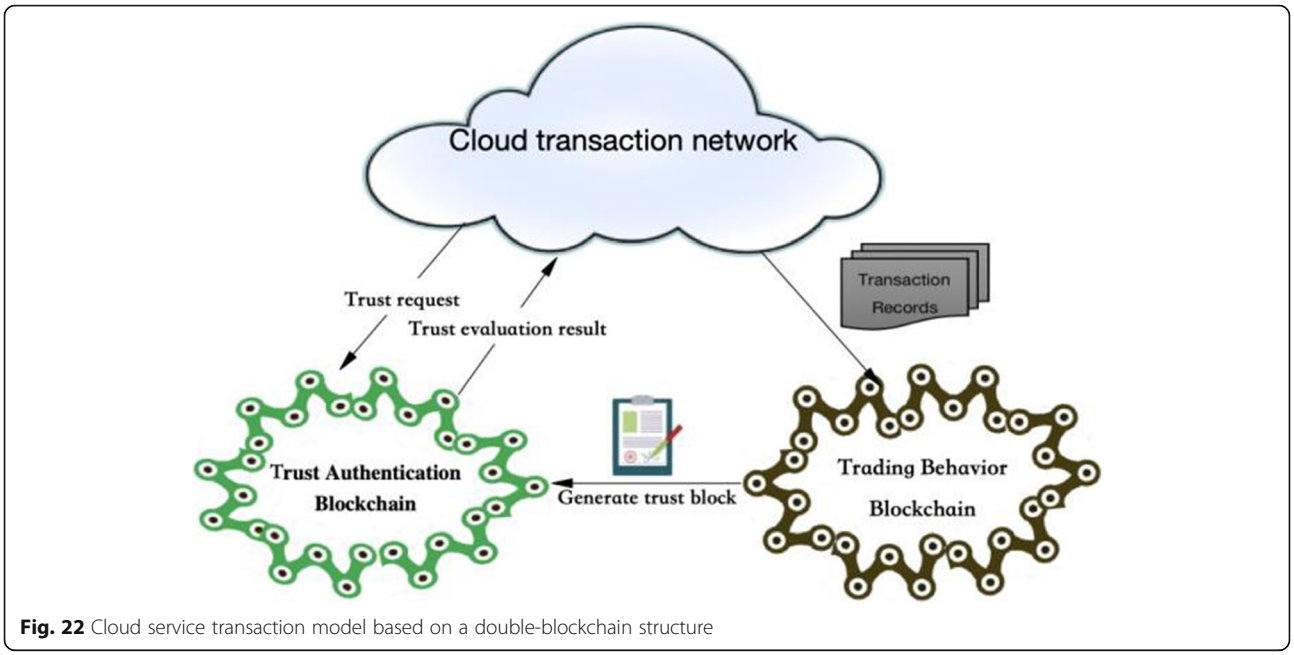

Fig. 22 Cloud service transaction model based on a double-blockchain structure

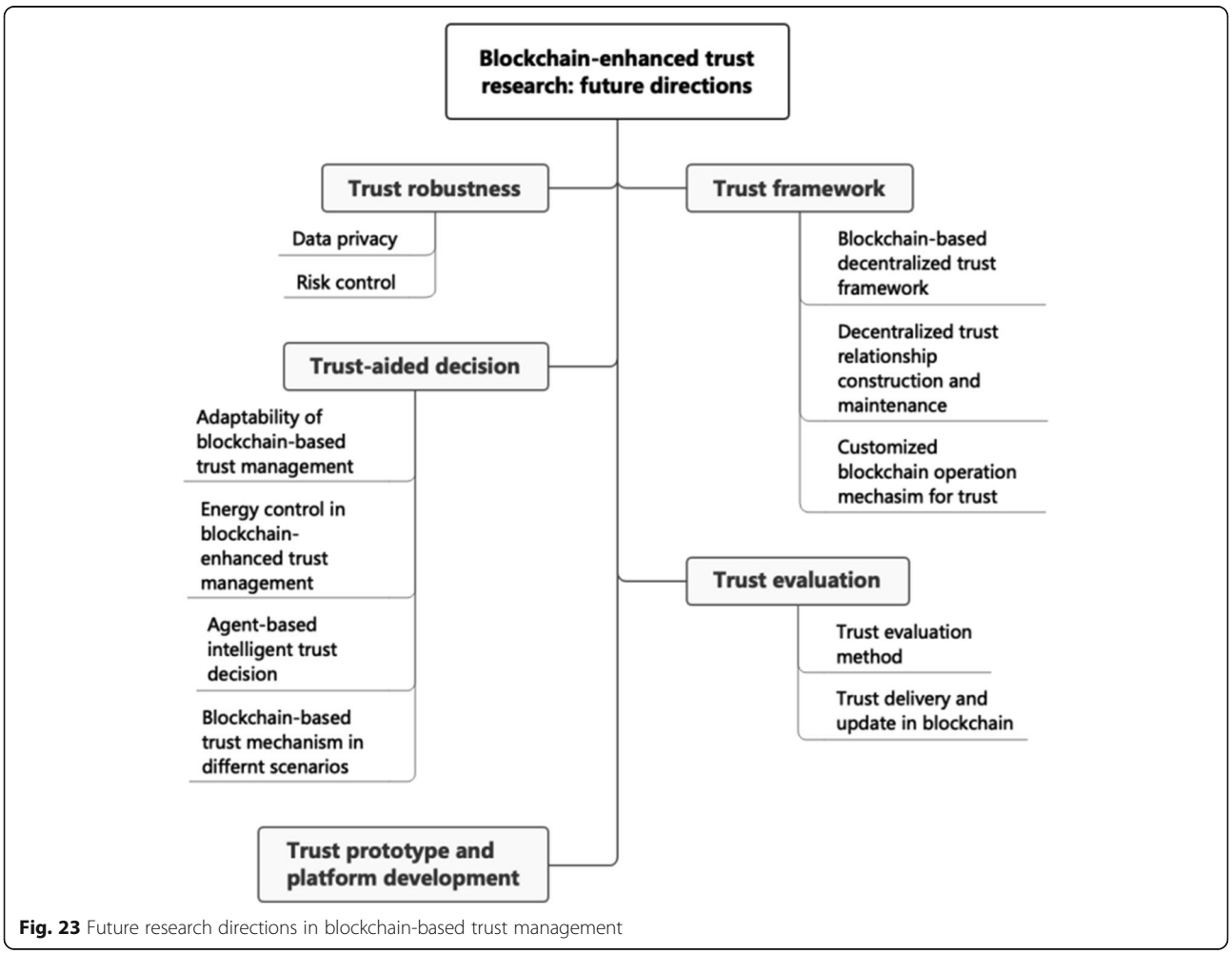

Fig. 23 Future research directions in blockchain-based trust management

higher level of security and data traceability. At the same time, because the trust value is provided by the TAB, leaving the large-scale calculation or evaluation of trust on the TBB side, this can effectively reduce latency, and finally the application of blockchain can be realized in more real-time and high-reliability scenarios.

Future research directions

Although many researchers have proposed strategies for the blockchain-based trust management, there are still huge gaps between theory and practical applications. The future research directions are listed below and classified into four modules according to different trust research branches, as shown in Fig. 23.

Trust framework

Blockchain-based decentralized trust framework

Blockchain is a natural decentralized and P2P consensus framework. However, cloud computing systems have multiple construction modes, and with the emergence of fog computing, edge computing and IoT applications, the realization method of cloud has become more and more diversified. Therefore, it's necessary for blockchain-based trust framework to consider how to adapt to different application scenarios of cloud, and propose customized and flexible trust authentication architecture.

Decentralized trust relationship construction and maintenance

In cloud computing systems, there exist many different kinds of trust relationship, including the cooperation and competition between provider and user, the cooperation and competition between broker and provider, the cooperation and competition between brokers or providers. Thus, in a blockchain-based trust framework, it's necessary to fully consider all the mentioned relationship and consider how to initialize and maintain the trust relation network.

Customized blockchain operation mechanism for trust

Smart contracts, consensus mechanisms and incentive mechanisms are the critical issues in blockchain applications. These issues still need to be addressed in the blockchain-based trust management. For example, how to encourage miners to actively participate in trust evaluation, trust decisions, and data verification, how to address the security issues of blockchain, such as attacks against smart contracts or blocks, forged transactions, etc.

Trust evaluation

Trust evaluation method

Blockchain is a kind of distributed ledger, which is very convenient to establish the complete and traceable transaction records between cloud entities. However, some specific evaluation methods are required to compute trust from the original trading records. Therefore, it is necessary to explore an appropriate trust evaluation method and study how to generate trust block from trading history.

On the other hand, blockchain is suitable for the behavioral trust management, but not good at the identity trust management. Because the identity trust authentication usually requires the assistance of a trusted third-party organization. Therefore, to build decentralized trust authentication based on blockchain, it is necessary to solve the problem of how to complete identity trust management.

Trust delivery and authorization

Trust is conditionally transitive. People can estimate trust for an unfamiliar or never-before traded entity. In a blockchain-based trust network, it is easy to accurately obtain the trust degree of a node, however, how to calculate the recommendation trust and how to grant trust permissions to a composite application or other associated nodes, are still problems which need to be addressed.

Trust-aided decision

Adaptability of blockchain-based trust management

Another issue is to improve the adaptability of blockchain-based trust management, realizing dynamic access control. A possible solution is to build a human-centric trust model, enabling services to intelligently assess their own security risks and apply a suitable security policy according to the potential attack.

Energy control in blockchain-enhanced trust management

Identity trust is usually stable and relatively easy to handle, whereas behavior trust must be updated from time to time, incurring a huge trust management overhead. The double-blockchain framework, proposed in the previous section, is one of the possible way to reduce the trust management overhead. However, the implementation details of the new framework still need to be solved. In addition, the blockchain structure will swell and explode if all the data, including cloud transactions and identity/behavior evaluation records, are all stored on the chain, imposing increasingly high processing capacity demands on participating entities. Therefore, researchers need to focus on appropriate measures to solve this problem for resource-constrained systems.

Agent-based intelligent trust decision

Blockchain-based trust framework adopts a decentralized strategy, which requires each node in blockchain network has the ability of independent decision. Software agent represents the distributed AI technology. Agents are independent, intelligent and social, and are very suitable for implementing self-maintenance and interactive behaviors on behalf of blockchain nodes. Agent-based trust decision enhances the intelligence of blockchain-based trust management.

Blockchain-based trust mechanism in different application scenarios

At present, most of the research focuses on the fields of banking, electronic authentication, intelligent transportation, etc. However, in the future, blockchain-based schemes will penetrate into some other application scenarios. For example, in a cloud-edge hybrid architecture, when the basic infrastructure of trust is constructed by blockchain, it is important to redefine the relationship between cloud data center, edge server, and terminals, along with the judicious decision on how to realize an efficient and trust collaboration.

Trust robustness

Data privacy

Privacy is another major issue which needs to be addressed. Data transparency and traceability are advantages brought by blockchain, however they also lead to privacy breaches and data abuse risks. Future research needs to find a balance between transparency and user privacy.

Risk control

Trust is a simplified security mechanism. However, due to the degree of accuracy in trust evaluation, the existence of trust thresholds, and the possible attacks on trust itself, trust-enabled interaction still faces with some risks. Therefore, the balance mechanism between trust and risk needs to be further studied.

Prototype and platform development

At present, blockchain-based researches mostly use theoretical analysis or only simulation verification, lack the testing on a prototype or a real system. Therefore, to develop a blockchain-based universal trust prototype system or platform is also a critical issue.

Conclusions

This paper introduces a taxonomy and a review of blockchain-based trust management approaches in cloud computing systems. These approaches are classified into different taxonomies according to three phases: blockchain-based basic trust framework, blockchain-enhanced trust interaction framework and mechanisms, and data management. Then, it presents a comprehensive analysis and comparison of the existing blockchain-based trust approaches. In order to improve the efficiency and adaptiveness of trust-enabled cloud computing, a novel cloud-edge hybrid trust management framework along with a double-blockchain based cloud transaction model are proposed. Finally, we suggest future directions and detail the open challenges of blockchain-based trust management schemes.

The uniqueness of this paper is that it studies the application of blockchain from the perspective of trust. Our analysis shows that using blockchain technology to construct a decentralized trust management framework has the following benefits:

- it eliminates the single point of failure and avoids data leakage,
- identity and trust behavior evidence is traceable and interpretable, trust evaluation results are convincing, the malicious use of data is prevented,
- and it is especially suitable for constructing IoT trust relationships.

However, the article also reveals that there is a huge gap between the theory of the method and the actual application. All in all, utilizing the blockchain technique to build a more credible and safe cloud transaction environment is a promising research direction.

Acknowledgments

The authors would like to thank the support of the laboratory, university and government, and the hard work of the editors and reviewers.

Authors' contributions

All authors take part in the discussion of the work described in this paper. The author(s) read and approved the final manuscript.

Authors' information

Wenjuan Li received a Ph. D degree in 2012 from Zhejiang University, Hangzhou China, in computer science. She is currently an associate professor in Hangzhou Normal University, she worked as a post-doctor in Shanghai Tiao Tong University from Oct. 2015 to Mar. 2019, and a visiting scholar in CLOUDS Lab at University of Melbourne from Dec. 2017 to Dec. 2018. Her research interests include cloud computing, social network and trust.

Jiyi Wu received a Ph. D degree in 2011 from Zhejiang University, Hangzhou China, in computer science. He is now a director of Artificial Intelligence Association, Zhejiang Province. His research interests include service computing, trust and reputation.

Jian Cao is currently a Professor with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, China, and the Deputy Head of the Department. He is also the Leader of the Lab for Collaborative Intelligent Technology. He leads the Research Group of Collaborative Information System. His research interests include networks computing, service computing, and data analytics. He has authored or co-authored over 180 journal and conference papers in the above-mentioned areas.

Nan Chen is a lecturer in Hangzhou Normal University. Her research interests include social network and trust management.

Qifei Zhang received a Ph.D degree in 2013 from Zhejiang University, Hangzhou China, in computer science. He is currently an associate researcher in Zhejiang University. His research interests include IoT, cloud computing and P2P network.

Rajkumar Buyya is a Redmond Barry Distinguished Professor and Director of the Cloud Computing and Distributed Systems (CLOUDS) Laboratory at the University of Melbourne, Australia. He is also serving as the founding CEO of Manjrasoft, a spin-off company of the University, commercializing its innovations in Cloud Computing. He has authored over 725 publications and seven text books including" Mastering Cloud Computing" published by McGraw Hill, China Machine Press, and Morgan Kaufmann for Indian, Chinese and international markets respectively. He is one of the highly cited authors in computer science and software engineering worldwide (h-index = 137, g-index = 304, 100,900 + citations). Dr. Buyya is recognized as a" Web of Science Highly Cited Researcher"for four consecutive years since 2016, IEEE Fellow, Scopus Researcher of the Year 2017 with Excellence in Innovative Research Award by Elsevier, and the" Best of the World", in Computing Systems field, by The Australian 2019 Research Review. He served as the founding Editor-in-Chief of the IEEE Transactions on Cloud Computing. He is currently serving as Co-Editor-in-Chief of Journal of Software: Practice and Experience, which was established 50 years ago. For further information on Dr. Buyya, please visit his cyberhome: www.buyya.com.

Funding
This work is supported by the National Natural Science Foundation of China under grant 61702151 and 61702320, National Key Research and Development Plan under grant 2018YFB1003800.

Availability of data and materials
Data is available upon request to the corresponding author.

Declarations

Competing interests
We formally declare that there are no know financial or non-financial competing interests in the realization of this research.

Author details
[1]Qianjiang College, Hangzhou Normal University, Hangzhou 310018, China. [2]Artificial Intelligence Association of Zhejiang Province, Hangzhou 310036, China. [3]Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China. [4]School of Software Technology, Zhejiang University, Ningbo 315048, China. [5]Cloud Computing and Distributed Systems (CLOUDS) Laboratory, the University of Melbourne, Melbourne VIC3010, Australia.

Received: 21 January 2021 Accepted: 20 May 2021
Published online: 21 June 2021

References
1. Xu M, Buyya R (2019) Brownout approach for adaptive Management of Resources and Applications in cloud computing systems. ACM Comput Surve 52(1):1–27
2. Zhu Y, Zhang W, Chen Y, Gao H (2019) A novel approach to workload prediction using attention-based LSTM encoder-decoder network in cloud environment. EURASIP J Wirel Commun Netw 247(2019). https://doi.org/10.1186/s13638-019-1605-z
3. Li X, Gui X (2010) Cognitive model of dynamic trust forecasting. J Software 21(1):163–176
4. Tahta U, Sen S, Can A (2015) GenTrust: a genetic trust management model for peer-to-peer systems. Appl Soft Comput 34(2015):693–704. https://doi.org/10.1016/j.asoc.2015.04.053
5. Sanadhya S, Singh S (2015) Trust calculation with ant Colony optimization in online social networks. Procedia Computer Sci 54(2015):186–195. https://doi.org/10.1016/j.procs.2015.06.021
6. Gao H, Huang W, Duan Y (2021) The cloud-edge-based dynamic reconfiguration to service workflow for Mobile ecommerce environments: a QoS prediction perspective. ACM Transact Int Technol 21(1):1–23. https://doi.org/10.1145/3391198
7. Zhang P, Kong Y, Zhou M (2017) A novel trust model for unreliable public clouds based on domain partition. In Proceedings of IEEE 14th International Conference on Networking, Sensing and Control (ICNSC). IEEE, pp 275–280
8. Li W, Ping L, Pan X (2009) Trust model to enhance security and interoperability of cloud environment. In: Proceedings of CloudCom'09 the 1st International Conference on Cloud Computing. Beijing. Springer, Berlin, pp 69–79
9. Li W, Wu J, Zhang Q, Hu K, Li J (2014) Trust-driven and QoS demand clustering analysis based cloud workflow scheduling strategies. Cluster Comput 17(1):1013–1030
10. Li X, He J, Du Y (2015) Trust based service optimization selection for cloud computing. Int J Multimedia Ubiquitous Engineering 105(2015):221–230
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 Veh Technol:1. https://doi.org/10.1109/TVT.2021.3068990
12. Xie L, Ding Y, Yang H, Wang X (2019) Blockchain-based secure and trustworthy internet of things in SDN-enabled 5G-VANETs. IEEE Access 7: 56656–56666. https://doi.org/10.1109/ACCESS.2019.2913682
13. Fu X, Yu FR, Wang J, Qi Q, Liao J (2019) Resource Allocation for Blockchain-Enabled Distributed Network Function Virtualization (NFV) with Mobile Edge Cloud (MEC), IEEE INFOCOM 2019. In: IEEE conference on computer Communications workshops (INFOCOM WKSHPS), Paris, France, pp 1–6
14. Yang C, Tan L, Shi N et al (2020) AuthPrivacyChain: a Blockchain-based access control framework with privacy protection in cloud. IEEE Access 2020(8):70604–70615
15. Horvath A III, Agrawal R (2015) Trust in Cloud Computing: a User's perspective. Proceedings of the IEEE SoutheastCon 2015. IEEE 2015:1–8
16. Harbajanka S, Saxena P (2016) Survey paper on trust management and security issues in cloud computing. Symposium on colossal data analysis and networking (CDAN). IEEE 2016:1–3
17. 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
18. Huang J, Nicol D (2013) Trust mechanisms for cloud computing. J Cloud Comput Adv Syst Applications 2(9):1–14
19. Noor T, Sheng Q, Zeadally S, Yu J (2013) Trust management of services in cloud environments: obstacles and solutions. ACM Comput Survey 46(1):1–30
20. Monir M, AbdelAziz M, AbdelHamid A et al (2015) Trust Management in Cloud Computing: a survey. In: In proceedings of IEEE seventh international conference on intelligent computing and information systems (ICICIS'15), IEEE 2015, pp 231–242
21. Chandni M, Sowmiya N, Mohana S et al (2017) Establishing trust despite attacks in cloud computing: a survey. In proceedings of WiSPNET 2017. IEEE 2017:712–716
22. Lansing J, Sunyaev A (2016) Trust in Cloud Computing: conceptual typology and trust-building antecedents. ACM SIGMIS Database 47 2(2016):58–96
23. 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
24. Matin C, Navimipour J, Jafari N (2017) A comprehensive study of the trust evaluation mechanisms in the cloud computing. J Service Sci Res 9(1):1–30
25. Deshpande S, Ingle R (2017) Trust assessment in cloud environment: taxonomy and analysis. In: Proceedings of international conference on computing. IEEE 2017, pp 627–631
26. Alhanahnah M, Bertok P, Tari Z (2017) Trusting cloud service providers: trust phases and a taxonomy of trust factors. IEEE Cloud Computing 4(1):44–54
27. Hawlitschek F, Notheisen B, Teubner T (2018) The limits of trust-free systems: a literature review on blockchain technology and trust in the sharing economy. Electron Commer Res Appl 29(2018):50–53. https://doi.org/10.1016/j.elerap.2018.03.005
28. Cho J, Chan K, Adali S (2015) A survey on trust modeling. ACM Computing Surveys 48(2):1–40
29. Granatyr J, Botelho V, Lessing O et al (2015) Trust and reputation models for multiagent systems. ACM Comput Surveys 48(2):1–42
30. 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
31. Belotti M, Bozic N, Pujolle G et al (2019) A Vademecum on Blockchain Technologies: When, Which and How. IEEE Commun Surveys Tutorials 21(4): 3796–3838. https://doi.org/10.1109/COMST.2019.2928178
32. Ali M, Vecchio M, Pincheira M, Dolui K, Antonelli F, Rehman M (2019) Applications of Blockchains in the Internet of Things: A Comprehensive Survey. IEEE Commun Survey Tutorials 21(2):1676–1717

33. 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. https://doi.org/10.1109/COMST.2020.2975911
34. Gai K, Guo I, Zhu L, Yu S (2019) Blockchain Meets Cloud Computing: A Survey. IEEE Communications Survey Tutorials. https://doi.org/10.1109/COMST.2020.2989392
35. Saad M, et al. (2020) Exploring the Attack Surface of Blockchain: A Comprehensive Survey, IEEE Communications Surveys & Tutorials, 22(3): 1977–2008
36. 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
37. Cole J, Milosevic Z, Raymond K (2011) Decentralized trust management. In: van Tilborg HCA, Jajodia S (eds) Encyclopedia of cryptography and security. Springer, Boston
38. Li H (2016) Study on trust model and controversy discovery under web 2.0 circumstance. Doctor thesis, XiDian University, China
39. Kuwabara K (2000) Reputation systems: facilitating Trust in Internet Interactions. Commun ACM 43(12):45–48
40. Kamvar S, Schlosser M, Garcia-Molina H (2003) The Eigentrust algorithm for reputation management in P2P networks. ACM 2003:640–651
41. Xiong L, Ling L (2004) PeerTrust: supporting reputation-based Trust for Peer-to-Peer Electronic Communities. IEEE transactions on knowledge \& data
42. Li W, Ping L, Pan X (2010) Use trust management module to achieve effective security mechanisms in cloud environment. In: Proceedings of 2010 international conference on Electronics & Information Engineering IEEE, p 2010
43. Li X, Ma H (2015) T-Broker: A Trust-Aware Service Brokering Scheme for Multiple Cloud Collaborative Services. IEEE Transact Information Forensics Security 10(7):1402–1415
44. Mrabet M, Saied B, Saidane L (2016) A new trust evaluation approach for cloud computing environments. In proceedings of 2016 international conference on performance evaluation and modeling in wired and wireless networks (PEMWN). IEEE
45. E. Abdallah, M. Zulkernine, Y. Gu , et al. 2017. TRUST-CAP: A Trust Model for Cloud-Based Applications. in Proceedings of IEEE Computer Software & Applications Conference. IEEE 2017
46. Singh S, Sidhu J (2015) A collaborative trust calculation scheme for cloud computing systems. 2015. In proceedings of international conference on recent advances in Engineering & Computational Sciences. IEEE 2015
47. Nagarajan R, Selvamuthukumaran S, Thirunavukarasu R (2017) A fuzzy logic based trust evaluation model for the selection of cloud services. In proceedings of international conference on Computer Communication & Informatics. IEEE 2017
48. Pooranian Z, Shojafar M, Garg S, Taheri R, Tafazolli R (2021) LEVER: secure Deduplicated cloud storage with EncryptedTwo-party interactions in cyber-physical systems. IEEE Transact Industrial Informatics. https://doi.org/10.1109/TII.2020.3021013
49. Zhang P, Kong Y, Zhou M (2017) A novel trust model for unreliable public clouds based on domain partition. In proceedings of IEEE international conference on networking. IEEE 2017
50. Yefeng R, Durresi A (2017) A trust management framework for cloud computing platforms. In proceedings of IEEE 31st international conference on advanced information networking and applications (AINA), IEEE 2017
51. Felipe B, Fiorese A (2017) A trust reputation architecture for cloud computing environment. In proceedings of IEEE/ACS international conference on computer systems & applications, IEEE 2017
52. Zhu C, Nicanfar H, Leung V et al (2015) An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration. IEEE Transactions Information Forensics Security 10(1): 118–131
53. U. Kashif, Z. Memon, A. Balouch, et al. 2015.Distributed trust protocol for IaaS cloud computing. In proceedings of international Bhurban conference on applied sciences\& Technology, IEEE 2015
54. Hu C, Liu J, Liu J (2011) Services selection based on trust evolution and union for cloud computing. J Commun 7(2011):71–79
55. Wang Y, Zhou J, Tan H (2015) CC-PSM: A Preference-Aware Selection Model for Cloud Service Based on Consumer Community. Mathematical Problems in Engineering, Hindawi Publishing Corporation, 2015, p 170656
56. Meng X, Ma J, Lu D, Wang Y (2014) Trust and behavioral modeling based two layer service selection. Journal of Xidian University 4(2014):198–204
57. Yan S, Zheng X (2010) A user-centric trust and reputation method for service selection. In proceedings of the 2010 international symposium on intelligence information processing and trusted computing. IEEE 2010:101–105
58. Hang C, Singh M (2011) Trustworthy service selection and composition ACM Transaction on Autonomous and Adaptive Systems 6(2011):1
59. Wang H, Yu C, Wang L, Yu Q (2015) Effective BigData-space service selection over Trust and heterogeneous QoS preferences. IEEE Transact Services Comput 4(2015):644–657
60. Cao B, Li B, Liu J (2013) An on-demand service composition method based on trustworthy quality of service. J Xi'an Jiaotong Univ 2(2013):131–138
61. R. Du, J. Tian, H. Zhang. 2013. Cloud service selection model based on trust and personality preferences. 1(2013), 53-61
62. Li W, Cao J, Qian S, Buyya R (2019) TSLAM: a trust-enabled self-learning agent model for service matching in the cloud market. ACM Transact Autonomous Adaptive Syst 4(2019):1–41
63. Li W, Cao J, Hu K, Buyya R (2019) A trust-based agent learning model for service composition in Mobile cloud computing environments. IEEE Access 7:34207–34226
64. Alexopoulos N, Daubert J, Muhlhauser M, Habib S (2017) Beyond the hype on using Blockchains in Trust Management for Authentication. In proceedings of 2017 IEEE Trustcom /BigDataSE/ICESS. IEEE 2017:1–15
65. Bendiab K, Kolokotronis N, Shiaeles S et al (2018) WiP: a novel Blockchain-based trust model for cloud identity management. In proceedings of 2018 IEEE 16th Intl Conf on dependable. Autonomic Secure Comput IEEE 2018: 724–729
66. Moinet A, Darties B, Baril JL (2017) Blockchain based trust & authentication for decentralized sensor networks. Preprint version submitted to IEEE Security & Privacy, Special Issue on Blockchain, arXiv:1706.01730. https://arxiv.org/pdf/1706.01730.pdf
67. Liu Y, Zhao Z, Guo G, Wang X et al (2017) An identity management system based on Blockchain. In proceedings of 2017 15th annual conference on privacy. Security Trust IEEE 2017:44–53
68. Nayak S, Narendra N, Shukla A et al (2018) Saranyu: using smart contracts and Blockchain for cloud tenant management. In proceedings of 2018 IEEE 11th international conference on cloud computing. IEEE 2018:857–861
69. Z. Yang, K. Zheng, K. Yangy, et al. 2017. A Blockchain-based reputation system for data credibility assessment in vehicular networks. In proceedings of the 2017 IEEE 28th annual international symposium on personal, indoor, and Mobile radio Communications (PIMRC), IEEE 2017
70. 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. https://doi.org/10.1109/INFOCOM.2019.8737580
71. Fernando P, Wei J (2020) Blockchain-Powered Software Defined Network Enabled Networking Infrastructure for Cloud Management. In: Proceedings of 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), IEEE doi:arXiv:1909.01851
72. Kaynak B, Kaynak S, Uygun Ö (2020) Cloud manufacturing architecture based on public Blockchain Technology. IEEE Access 8:2163–2177. https://doi.org/10.1109/ACCESS.2019.2962232
73. 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
74. Ye F, Zheng Z, Chen C et al (2017) DC-RSF: a dynamic and customized reputation system framework for joint cloud computing. In proceedings of the 2017 IEEE 37th international conference on distributed computing systems workshops. IEEE 2017:275–279
75. Xie W, Zhou W, Kong L et al (2018) ETTF: a trusted trading framework using Blockchain in E-commerce. In proceedings of the 2018 IEEE 22nd international conference on computer supported cooperative work in design. IEEE 2018:612–617
76. Y. Zhang, R. Deng, X. Liu, et al. 2018. Outsourcing Service Fair Payment based on Blockchain and its Applications in Cloud Computing .IEEE Transactions on Service Computing, 2018(Early Access)

77. 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
78. Jiao Y, Wang P, Niyato D, Suankaewmanee K (2019) Auction mechanisms in cloud/fog computing resource allocation for public Blockchain networks. IEEE Transact Parallel Distributed Syst 30(9):1975–1989. https://doi.org/10.1109/TPDS.2019.2900238
79. Xiong Z, Feng S, Wang W, Niyato D, Wang P, Han Z (2019) Cloud/fog computing resource management and pricing for Blockchain networks. IEEE Internet Things J 6(3):4585–4600. https://doi.org/10.1109/JIOT.2018.2871706
80. 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
81. Kataoka K, Gangwar S, Podili P (2018) Trust list internet-wide and distributed IoT traffic management using blockchain and SDN. In proceedings of 2018 IEEE 4th world Forum on internet of things (WF-IoT). IEEE 2018:296–301
82. Tuli S, Mahmud R, Tuli S, Buyya R (2019) FogBus: a Blockchain-based lightweight framework for edge and fog computing. J Syst Software 154(2019):22–36. https://doi.org/10.1016/j.jss.2019.04.050
83. Medhane DV, Sangaiah AK, Hossain MS, Muhammad G, Wang J (2020) Blockchain-enabled distributed security framework for next-generation IoT: an edge cloud and software-defined network-integrated approach. IEEE Internet Things J 7(7):6143–6149. https://doi.org/10.1109/JIOT.2020.2977196
84. Lee J, Kerns SC, Hong S (2019) A Secure IoT-Fog-Cloud Framework Using Blockchain Based on DAT for Mobile IoT. In: IEEE 10th annual ubiquitous computing, electronics \& Mobile communication conference (UEMCON), New York City, NY, USA, pp 0213–0218. https://doi.org/10.1109/UEMCON47517.2019.8993056
85. Liang X, Shetty S, Tosh D et al (2017) ProvChain: a Blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In proceedings of the 2017 17th IEEE/ACM international symposium on cluster. Cloud Grid Comput IEEE 2017:468–477
86. R. Li, T. Song, B. Mei, et al.2018. Blockchain for large-scale internet of things data storage and protection. IEEE transaction on service Computing, 2018(Early Access)
87. Shafagh H, Burkhalter L, Hithnawi A et al (2017) Towards Blockchain-based auditable storage and sharing of IoT data. In proceedings of CCSW'17. IEEE 2017:45–50
88. Yu B, Wright J, Nepal S et al (2018) IoTChain: establishing Trust in the Internet of things ecosystem using Blockchain. IEEE Cloud Comput 5(4):12–23
89. Z. Yang, K. Yang, L. Lei, et al. 2018. Blockchain-based decentralized Trust Management in Vehicular Networks, IEEE internet of things journal, 2018(early access)
90. Jiaxing L, Jigang W, Long C (2018) Block-secure: Blockchain based scheme for secure P2P cloud storage. Inf Sci 465:219–231
91. Shen M, Duan J, Zhu L, Zhang J, Du X, Guizani M (2020) Blockchain-based incentives for secure and collaborative data sharing in multiple clouds. IEEE J Selected Area Commun 38(6):1229–1241. https://doi.org/10.1109/JSAC.2020.2986619
92. Yang C, Chen et al (2018) Blockchain-based publicly verifiable data deletion scheme for cloud storage. J Network Comput Application 103:185–193. https://doi.org/10.1016/j.jnca.2017.11.011
93. Zhang Y, Xu C, Cheng N, Li H, Yang H, Shen X (2019) Chronos+: an accurate Blockchain-based time-stamping scheme for cloud storage. IEEE Trans Serv Comput 13(2):216–229
94. Zhu L, Wu Y, Gai K et al (2018) Controllable and trustworthy blockchain-based cloud data management. Future Generation Comput Syst 91(FEB): 527–535
95. J. Kang, R. Yu, X. Huang, et al. 2018. Blockchain for secure and efficient data sharing in vehicular edge computing and networks, IEEE internet of things journal, 2018(early access)

Publisher's Note