Computers and Electrical Engineering 81 (2020) 106526

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Blockchain for cloud exchange: A survey[☆]

Shaoan Xie[a], Zibin Zheng[a], Weili Chen[a], Jiajing Wu[a], Hong-Ning Dai[b,*], Muhammad Imran[c]

[a] School of Data and Computer Science, Sun Yat-sen University, China
[b] Faculty of Information Technology, Macau University of Science and Technology, Macau SAR
[c] College of Applied Computer Science, King Saud University, Saudi Arabia

ARTICLE INFO

Article history:
Received 13 December 2018
Revised 17 October 2019
Accepted 25 November 2019

Keywords:
Industrial internet of things
Cloud exchange
Blockchain
Decentralization
Reputation systems

ABSTRACT

Compared with single cloud service providers, cloud exchange provides users with lower price and flexible options. However, conventional cloud exchange markets are suffering from a number of challenges such as central architecture being vulnerable to malicious attacks and cheating behaviours of third-party auctioneers. The recent advances in blockchain technologies bring the opportunities to overcome the limitations of cloud exchange. However, the integration of blockchain with cloud exchange is still in infancy and extensive research efforts are needed to tackle a number of research challenges. To bridge this gap, this paper presents an overview on using blockchain for cloud exchange. In particular, we first give an overview on cloud exchange. We then briefly survey blockchain technology and discuss the issues on using blockchain for cloud exchange in aspects of security, privacy, reputation systems and transaction management. Finally, we present the open research issues in this promising area.

1. Introduction

There is a paradigm shift from conventional computer-aided industry to *smart industry* driven by recent advances in Industrial Internet of Things (IIoT) and Big Data Analytics (BDA) [1]. During this evolution, Industrial IoT (IIoT) plays a critical role of connecting the physical industrial environment to the cyberspace of computing systems [2]. However, IIoT nodes (such as sensors, Radio Frequency IDentification (RFID) tags and smart meters) typically have the limited computational capability and finite battery. Therefore, most of them cannot be used to conduct extensive computing tasks, such as data analytics.

Cloud computing, one of most promising information and communication technologies (ICT), is an efficient method to potentially overcome the limitations of IIoT nodes. As a model for enabling on-demand network access to configurable computer resources, it also frees people and enterprises from large hardware costs and low productivities. Thereafter, the proliferation of business and research applications of cloud services has driven a rapid development of the global cloud market. Additionally, cloud service revenue is expected to reach over 300 billion dollars in 2021.

[☆] This paper is for CAEE special section SI-bciot. Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. Shaohua Wan.

[*] Corresponding author.
E-mail address: hndai@ieee.org (H.-N. Dai).

https://doi.org/10.1016/j.compeleceng.2019.106526

Table 1
Glossary.

Acronyms	Terms	Acronyms	Terms
CloudEX	Cloud EXchange	RFID	Radio Frequency IDentification
BDA	Big Data Analytics	IIoT	Industrial Internet of Things
IOT	Internet of Things	AWS	Amazon Web Services
IP	Internet Protocol	ICT	Information Communications Technology
IaaS	Infrastructure as a Service	PaaS	Platform as a Service
SaaS	Software as a Service	SLA	Service Level Agreements
IT	Information Technology	UTXO	Unspent Transaction Output

Generally, people purchase cloud services from cloud-service providers such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform and Alibaba Cloud. These cloud giants have their own cloud marketplaces, thereby letting consumers struggle in choosing appropriate and cost-effective services [3]. The absence of competitions results in these providers usually offering their cloud services at a higher price than in a competitive market structure. Meanwhile, the single cloud-service provision cannot fulfill the demands of deploying different types of cloud services for a company across the world.

Recently, the concept of **Cloud Exchange** (CloudEX) has been put forward as a potential solution to the single cloud service provision. Consumers and providers are allowed to publish their requirements and offers within CloudEX platforms. Meanwhile, CloudEX simplifies the process of provisioning and managing connections among multiple cloud services while it was a burden on consumers. CloudEX platforms like Equinix Cloud Exchange (https://www.equinix.com/) are springing up and cloud giants like AWS, Azure are also cooperating with these CloudEX platforms. However, as CloudEX adopts conventional models, in which CloudEX is fully controlled by an organization. The centralization of CloudEX platform may result in a number of problems such as vulnerability to single point of failure and tampering of transaction information. Moreover, when users are looking for suitable resources, dishonest cloud providers may display harassment advertisements. In addition, a CloudEX platform needs to deal with the transaction dispute between consumers and service providers while the final judgment can be unfair since the CloudEX might have a bias toward a certain user or provider.

Therefore, a decentralized CloudEX that is not owned by any single entity is becoming a trend. However, it is challenging to implement a decentralized CloudEX platform in untrusted environment. Fortunately, blockchain has the potential to address this problem. Blockchain, first proposed in 2008, is essentially a distributed database that maintains a continuously-growing list of data records which are tampering-resistant. Transactions are stored in the blockchain while each participant of the network stores a full copy of blockchain, thus preventing single point of failure. To preserve user privacy, blockchain users make transactions via public and private keys instead of real identity. Now blockchain has been applied to various industrial sectors such as bank systems, digital assets, identity certification.

The integration of blockchain and exchange system has attracted a lot of attention from the public. Nasdaq has launched its blockchain-based private market for trading pre-IPO shares, in which the blockchain has been used to store the transaction records as it is secure and reliable. Additionally, many capitalization exchange markets including the Korea Exchange, London Stock Exchange, Tokyo Stock Exchange are investigating the adoption of blockchain to reduce the exchange cost.

Blockchain technology has the great potential to address the challenges of conventional exchange platforms. However, there are few research papers addressing the integration of blockchain with CloudEX. To bridge this gap, we present an overview on using blockchain in cloud exchange. The main contributions of this paper are to give a comprehensive survey of CloudEX and investigate how blockchain technology can benefit CloudEX from different aspects. In addition, we also discuss several research issues which are of great importance to devising future blockchain-based CloudEX systems. We believe that this article sheds a light on blockchain-based CloudEX development.

The rest of this paper is organized as follows. Section 2 introduces the overall trading process in CloudEXs and analyze the problems and challenges for existing CloudEXs. Section 3 presents the benefits of blockchain technology to existing commercial markets. Section 4 shows the connections between blockchain and CloudEX could lie in many areas including the reputation system, user privacy protection and transaction dispute resolution. Section 5 lays out four future directions for blockchain-based CloudEXs. Finally, this paper is concluded in Section 6. Table 1 lists the main terms and acronyms throughout this paper.

2. Cloud exchange

2.1. Introduction of cloud exchange

Although most of users purchase cloud resources from those cloud service providers, e.g., Amazon, Microsoft, Google and Alibaba, the absence of competitive rivals may allow those ICT giants to monopolize the cloud service market. On one hand, they can increase service prices arbitrarily since users have no other choices. On the other hand, they may provide singular services lacking of flexibility and adaptability. The emergence of CloudEX brings convenience to customers with low service price and adaptable cloud service. Nowadays more and more CloudEX platforms are appearing with the increasing types of

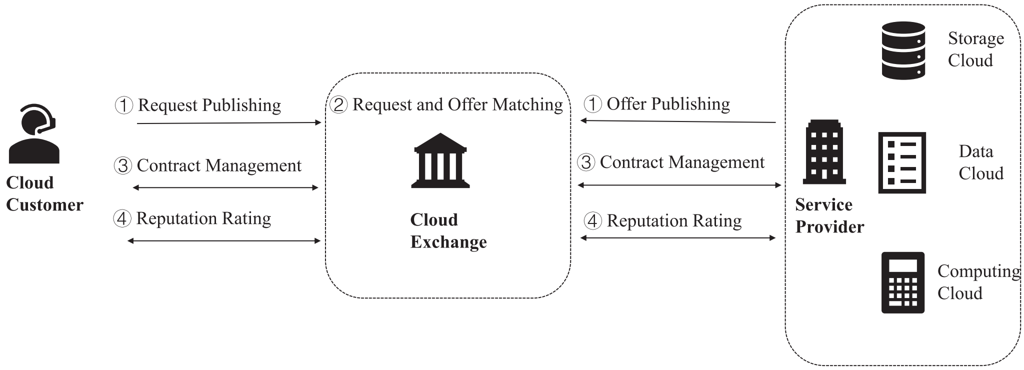

Fig. 1. Trading process in cloud exchange. Users publish their demands and Enterprises publish their different types of resources (such as computing and data storage) to the CloudEX platform. Then, the CloudEX platform that matches these requirements will offer the cloud services to end users. After that, users and enterprises sign on the contract so that users can use the resources provided by enterprises. Finally, users and enterprises rate the reputation of each other based on their behaviours during the transaction.

cloud services that can be traded on CloudEX platforms. We then introduce the trading process in CloudEX in this section and analyze the potential problems behind such model in next section. The whole process resembles purchasing resources on Amazon or other companies but is also different in several aspects.

Fig. 1 gives an illustration of trading process in cloud exchange.

2.1.1. Request and offer publishing

At the beginning, customers send their requests and service providers will publish their resources to the CloudEX. Three types of services are offered: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Before the registration of a resource or service in the market directory, its information has to be evaluated by the market. In some CloudEX systems, resources are registered according to the fact that the service is hardware service or software service [4].

2.1.2. Request and offer matching

Matching principles of customers' requests and providers' offers varies in different cloud markets since the adopted market models may be distinct. CloudEX can employ different market models to achieve maximum resource utilization. In [5], CloudEX also supports those economic models: Commodity market, Auction model, Monopoly, Bargaining model, Contract-net model. The process of trading varies in different market models. It is worth noting that the matching schemes used in the same market model can also be totally unlike each other. Furthermore, the matching does not need to be one-to-one. Ref. [6] proposes a novel architecture which allows the cooperation among different cloud providers in a Geo-distributed manner.

2.1.3. Contracting management and settlement

If a customer and a provider are matched, they need to negotiate explicit conditions. For instance, they reach an agreement on the penalty of violating the contract. After negotiations, a legally-binding contract will be created automatically. In the signed contract, a set of appropriate service level agreements (SLAs) with constraints, compensations and provisioning policies for both sides are stated clearly [7]. SLA is an important part of cloud resource trading but it is not prevalent in grid computing. Settlement can be divided into two parts: *service delivery* and *payment* [7]. In service delivery phase, users get access to the cloud resources. Different kinds of services (i.e, IaaS, PaaS and SaaS) will be delivered in different ways. These service models also place a different level of security requirement in the cloud environment. As for payment, it varies for different exchanges. Some exchanges will act like the trusted intermediaries and they would keep the funds until the users have confirmed the transactions. On the contrary, some exchanges do not get involved with the payments as consumers will pay service providers directly.

2.1.4. Reputation rating

Actually reputation system is optional for CloudEXs in real life and some exchanges disregard it to save efforts. But we want to highlight the importance of reputation system as it enables a more reliable trading between customers and service providers.

After the settlement, users will be required to rate their partners' behaviours and these feedbacks will then be stored in the reputation system. The reputation system is widely adopted in modern lives. The introduction of the reputation system counters the tendency of an increasing probability of fraudulent activities [8] as it punishes dishonest behaviours and encourages upright actions. Reputation systems can be generally classified into three types. Honest behaviours would be praised in the *positive reputation system* while dishonest actions can be punished in the *negative reputation system*. The

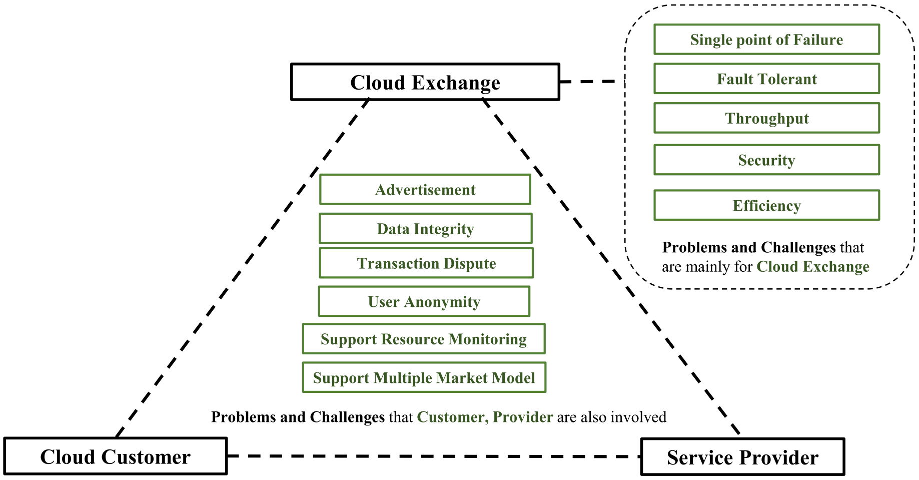
Cloud Exchange
Single point of Failure
Fault Tolerant
Throughput
Security
Efficiency
Problems and Challenges that are mainly for Cloud Exchange
Advertisement
Data Integrity
Transaction Dispute
User Anonymity
Support Resource Monitoring
Support Multiple Market Model
Problems and Challenges that Customer, Provider are also involved
Cloud Customer
Service Provider

Fig. 2. Problems and challenges for centralized cloud exchange (CloudEX). We firstly list the problems that are more related to cloud exchanges, such as single point of failure and security problems. Then we list the major problems and challenges for the three roles (cloud exchange, cloud customer and service provider) in the whole transaction.

hybrid reputation system combines the key characteristics of both positive and negative reputation systems. It increases the reputation score if one behaves honestly while decreases the score if one makes frauds.

2.2. Challenges

CloudEX has already provided considerable convenience for its clients. Nevertheless, since CloudEX technology is still immature, there are numerous problems and challenges that CloudEXs have to face. In this section, key problems and challenges are summarized in Fig. 2.

Firstly, we introduce the problems that are more related to CloudEXs though they might have potential effects on cloud customers and service providers.

- *Single point of failure with reputation system*. When a transaction ends, users will be required to give each other a reputation score for their performances during the transaction. Since CloudEX has its own reputation score calculation algorithm, the reputation scores will be stored on its central server. The centralized design may result in the single point of failure. Meanwhile, malicious users who have hacked into the system can change transaction records as they want. It highlights the need for a decentralized reputation system and blockchain can help build it.
- *High throughput demand*: A successful and large CloudEX always faces the challenge of throughput: it might receive tens of thousands of requests from users and need to handle them in a very short period.
- *Fault tolerant*: Failures are inevitable in any system (e.g., the central server of the market shutdown suddenly), but a reliable exchange should be able to resume its services from the closest point before the failures [9].
- *Efficiency*: Efficiency plays an important role in deciding users' preferences for the market. For example, no one will use the system again if the user has to wait for 10 minutes for a single search request. There should be a simple but functional interface to facilitate the whole process of transactions. Apart from that, algorithms in the market such as ranking and matching mechanisms need to be efficient to reduce the users' waiting time.
- *Security*: An influential CloudEX can attract the attention of hackers or malicious attackers. They might try to hack into the market system to get some improper revenues. For example, some low-ranked sellers can hack into the system to tamper the reputation scores or some hackers can sell the privacy information of users in the market). Hence a CloudEX ought to be secure enough to defend the attacks. To address such problem, one may employ blockchain technology to maintain a malicious attacker Internet Protocol (IP) address list so that they are blocked. Further, encryption algorithms are inherently embedded into the blockchain to protect user privacy.

Next, we present problems and challenges that exist in the interactions between CloudEX, cloud customer, service providers.

- *Data integrity*. In data-trading businesses, sellers need to upload their resources like complete data to CloudEX before they publish the resources publicly. Since resources are stored on CloudEX, there can exist various problems. For example, administrators might steal or tamper the data. Users are aware of this kind of risks but they have no choice but to trust the central exchange. The SETI@Home project, perhaps the most well-known example of large-scale distributed computing, has already experienced data integrity problems as the unknown and untrusted entities tamper with the computation process. Blockchain can be used to approach this problem easily. For example, one could build a blockchain-based data access control mechanism like [10]. Since blockchain is immutable, the data access records are kept permanently.

- *Advertisement*. When users are browsing the items in the marketplace, items are usually listed according to some ranking algorithms. Since CloudEX platforms are typically close-source, no one has the knowledge of their sorting principles. Consequently, some cheating behaviours can be hidden in these platforms. Those providers with low-quality products can bribe CloudEX to obtain a relatively high ranking while letting others with high-quality services rank much lower.
- *Transaction dispute*. Disputes on products happen frequently and CloudEX plays the role of arbitrator who is responsible for negotiating between buyers and sellers. However, sometimes it is difficult to tell which party in the transaction is dishonest. For example, Alice bought a cloud resource for a week from Bob. But after a week Alice found it strange and realized that the resource from Bob was not up to the standards as he promised. Therefore, Alice came to CloudEX for a refund because she thought the products are unqualified but at the same time Bob argued that he had provided the qualified services. This kind of disputes occurs frequently in our daily lives. Blockchain can help tackle this problem from many different aspects. For example, blockchain can be used to maintain the log which records all the operations to the cloud resources. In this way, any changes to the cloud resources could be traced. Therefore, this problem can be solved. More details are in Section 4.
- *Support resources monitoring*: Disputes between a buyer and a seller is sometimes a ticklish problem for markets. Therefore, in order to assure the quality of the services provided by sellers, exchanges are supposed to require service providers to run monitoring programs on offered but unleased resources. When it comes to disputes in a happening transaction, the market should monitor the usage of resources and check the compliance with SLA instantly.
- *Anonymity*: Users' privacy is significant to any market exchange, and thus users' real identities should be hidden from the public. Otherwise, users will not take such a risk and choose to make transactions with known service providers. Blockchain is well known for its anonymity and could be utilized to achieve user anonymity in CloudEX.
- *Support multiple market models*: Different models have different pricing methods and matching strategies, which are beneficial for market developments as it offers multiple choices for users (e.g., service providers can put their resources into the commodity market to get more revenue). Meanwhile, incumbent extra resources can be utilized in such a generic model.

3. Blockchain

Blockchain is famous for its decentralized manner. It allows transactions to be made without any third party. We believe that blockchain can be used to improve the performance of CloudEX. Before investigating the combination of blockchain and CloudEX, we first give a brief introduction of blockchain and illustrate what benefits blockchain can bring to incumbent exchange platforms in real life.

3.1. Concept of blockchain

Blockchain consists of a sequence of blocks, each of which holds a complete list of transaction records like the conventional public ledger. Unlike the conventional databases, blockchain distinguishes itself from others with its unique characteristics:

- *Decentralized*: The blockchain network can be open to the public and everyone (aka a node) can participate in the consensus process. Each node maintains the whole blockchain.
- *Immutable*: It is nearly impossible to tamper a transaction if the transaction is packed into the blockchain. Each block contains a block header which contains a merkle tree root. The merkle tree root is generated by hashing all the transactions in the block. So if a transaction in the block is tampered, the block header will change, too. As a result, any change made to the block can be detected quickly.
- *Fraud free*: Broadcasted transactions will be checked by the nodes thereby fraud transactions being deserted. A block is generated through mining in each round. If a miner has succeeded in mining the block, he/she will broadcast the block to the network. Other nodes in the network will validate the block. Blocks with fraud transactions will be rejected by honest miners.
- *Secure*: Compared to those exchanges that use central servers, blockchain is more secure. If a blockchain is public, everyone can join it and each node need not to trust other nodes. Meanwhile, most of the blockchains are using *proof of work* which is convinced to be safe only when 51% of the computing resources have been controlled by one node.
- *User anonymity*: Each user will be given a pair of public key and private key. Since users only use addresses to make transactions, it is hard to track the real identity of users.
- *Auditability.* Unspent Transaction Output (UTXO) model is used to store user balance information in Bitcoin blockchain. Each transaction needs to specify some previous unspent transactions. Miners validate the transaction and check if the referred transactions are unspent.

For a more comprehensive survey of blockchain technology, we refer readers to [2,11]

3.2. Existing blockchain-based exchanges

Although there is no realistic platform of the integration of CloudEX and blockchain, many existing exchange platforms, in which other resources (e.g., stock, digital currency, energy) can be traded, have demonstrated the performance improvement.

Table 2
Examples of blockchain-based markets.

Name	Market Type	Benefits brought by blockchain
Nasdaq Linq	private security market	less settlement time and risk exposure, lower administrative burden
CounterParty	digital currency market	safer, lower transaction fee
Bitshares	digital assets market	lower transaction fee, more reliable transaction process
Enerchain	energy product market	safer, peer to peer trade, more reliable transaction process

We present an overview of existing blockchain-based exchange platforms. The developing experience on these blockchain-based exchange platforms can help to construct practical CloudExs in the coming future. Table 2 summarizes our findings.

Nasdaq Linq is a global blockchain-based electronic marketplace for buying and selling securities. In 2015, Nasdaq announced that a private securities transaction was recorded in its blockchain, which represents a major advance in the application of blockchain technology for private companies. With blockchain technology, Linq reduces settlement time significantly, reduces settlement risk exposure, lowers capital cost and systemic risk, and lowers the administrative burden. Additionally, with the great auditablility of blockchain, users of Linq can easily track their securities.

CounterParty is a financial platform for creating peer-to-peer financial applications on top of Bitcoin. CounterParty is also a decentralized digital currency exchange. Within the decentralized exchange, users can create their own virtual assets and trade without a middleman. Being built on top of Bitcoin blockchain, it gains the security of the robust Bitcoin network; this implies that the CounterParty blockchain will not be attacked unless Bitcoin blockchain is attacked.

Bitshares claims that almost anything can be traded in its decentralized exchange. Bitshares supports companies to issue their own stock on the Bitshares network and allows handy cost-effective tradings with complete protection against naked shorting. Since there is no untrusted middleman in CloudEX, trading in decentralized exchanges will be much more reliable. Additionally, transaction fees will be much cheaper compared with centralized exchanges.

Enerchain supports peer to peer energy products trading. Users send orders anonymously to the network and other users will click the order to make the transaction. Users trade energy products including power and gas with Enerchain tool and there is no third party in the transaction.

4. Blockchain for cloud exchange

In this section we investigate the integration of blockchain with CloudEX. Fig. 3 gives an illustration to summarize the challenging issues of conventional CloudEX systems and discuss the potentials brought by blockchain to overcome the challenges. In particular, Section 4.1 discusses that Blockchain can enhance CloudEX security and user privacy. We then present the blockchain-based reputation systems in CloudEX in Section 4.3. Transaction negotiation and dispute management have always been concerns to CloudEX and we explore the possible integration of blockchain with conventional transaction dispute solutions in Section 4.3.

4.1. Security and privacy assurance

Issues: CloudEXs should provide a safe and reliable environment for customers and service providers. So CloudEXs are obligated to protect user security and privacy in transaction. SaaS, PaaS and IaaS provide users softwares as services, application platforms and infrastructure resources, respectively. The different service models determine the diversity of security requirements. For example, with regard to SaaS, data privacy concerns are more important than other concerns since sensitive data of enterprises are processed and stored at the SaaS vendors, which are vulnerable to privacy leakage. While it comes to PaaS, users gain more control over the cloud services. Service providers ought to be aware of security below the application levels such as network intrusion prevention. Additionally, to ensure data security, the data should be inaccessible between applications. IaaS tends to face security issues based on the cloud deployment model. Apart from the hardware, infrastructure pertains to the path where it is getting transmitted. In a typical cloud environment, data will be transmitted from source to destination through umpteen number of third-party infrastructure devices. Data can be routed through an intruder's infrastructure. Moreover, Jenson et al. [12] presented some technical issues of security coming from cloud services usages, such as attacks on XML signatures and browser-based cloud authentications.

Privacy issues have existed for a long time within the context of cloud services, and many companies still have security and privacy concerns when moving their data to the cloud. As service providers are actually third-parties, it may have weaker privacy protections than enterprises themselves. In CloudEXs, users have to store their data in the cloud and thus their data is not owned or controlled by themselves. Malicious service providers can sell data to other users without authorization. At the same time, service providers will always replicate enterprises' data in multiple data centers for users' availability. This benefits users in a short term but it might cause problems if providers do not clear up the data on purpose after the transactions.

Blockchain solutions: Security and privacy are crucial for CloudEXs. Fortunately, blockchain can help CloudEXs solve the above-mentioned challenges. In the following, we introduce several applications in which the security and reliability are greatly enhanced by blockchain. Nowadays, an increasing amount of malicious softwares (malware) are put into Internet and

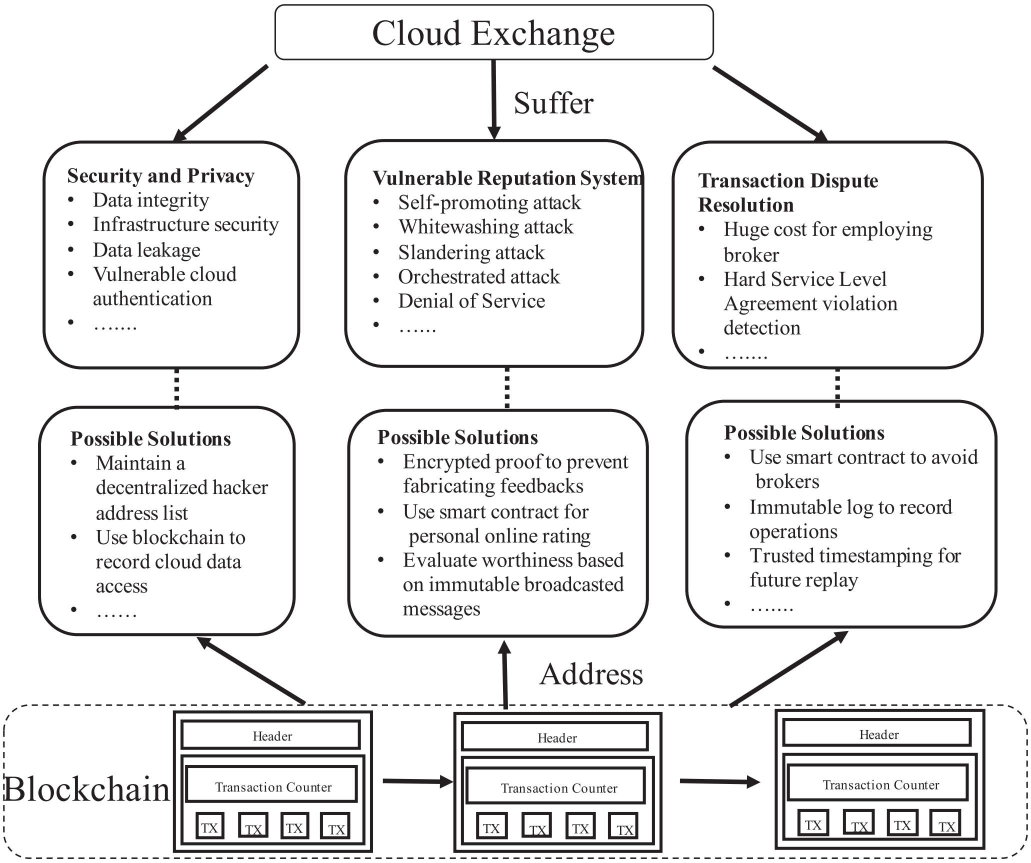
Cloud Exchange
Suffer
Security and Privacy
• Data integrity
• Infrastructure security
• Data leakage
• Vulnerable cloud authentication
• ....
Vulnerable Reputation System
• Self-promoting attack
• Whitewashing attack
• Slandering attack
• Orchestrated attack
• Denial of Service
• ......
Transaction Dispute Resolution
• Huge cost for employing broker
• Hard Service Level Agreement violation detection
• ....
Possible Solutions
• Maintain a decentralized hacker address list
• Use blockchain to record cloud data access
• ......
Possible Solutions
• Encrypted proof to prevent fabricating feedbacks
• Use smart contract for personal online rating
• Evaluate worthiness based on immutable broadcasted messages
Possible Solutions
• Use smart contract to avoid brokers
• Immutable log to record operations
• Trusted timestamping for future replay
• ....
Address
Blockchain
Header
Transaction Counter
TX
TX
TX
TX

Fig. 3. Conventional CloudEXs suffer from limitations due to the centralization while blockchain can decentrallize CloudEXs to improve the reliability and security.

it becomes more difficulty to identify those softwares. Generally speaking, there should be a server storing all the identified malware samples for future malware verifications. Obviously, an open-source malware library will reduce the burden of each company. However, it can be an openly-facing target for attackers. To this end, BitAV [13] based on blockchain was proposed as a decentralized server. It is proven to be a viable solution for network-based scanning. It is much harder to attack BitAV than any centralized servers. Users' privacy-concerned data are gathered legally or illegally day by day but they have no choice but to tolerate. Ref. [14] provides the first implementation of a decentralised and self-tallying Internet voting protocol. The protocol was implemented by a smart contract on ethereum and it allows the tally to be computed without requiring a tallying authority. Zyskind et al. proposed a protocol that turns blockchain into an automated access-control manager [10]. Their protocol gathers data from our mobile device and stores key index information on blockchain. Data can be accessed only when the software tools are granted with our authorizations. With blockchain, our privacy is guarded reliably. Furthermore, blockchain can also be utilized to guarantee the security and the reliability of decentralized systems, such as cloud systems and distributed databases. In the metadisk project (https://bravenewcoin.com/), a peer-to-peer cloud storage system is enhanced on security and efficiency through blockchain technology. Ref. [15] proposed a blockchain-based data sharing framework that sufficiently addresses the access control challenges associated with sensitive data stored in the cloud using immutability and built-in autonomy properties of the blockchain. The system permits users to request data from the shared pool after their identities and cryptographic keys are verified. Ref. [16] proposed a Blockchain-based approach to sharing patient data. They also applied extra measures of security on the blockchain such as network-wide keys and smart contracts, keeping security a top priority. Ref. [17] presented a conceptual framework for blockchain-based healthcare ecosystems. In this system, when new healthcare data for a particular patient is created (e.g., from a consultation, and medical operation such as a surgery), a new block is instantiated and distributed to all peers in the patient network. After a majority of the peers have approved the new block, the system will insert it in the chain. Instead of using blockchain to achieve decentralization, Bag et al. [18], Azad et al. [19] apply homomorphic cryptographic systems and non-interactive zero-knowledge proof to achieve privacy-preservation and well-formedness.

As for CloudEXs, many solutions mentioned above might be utilized to improve CloudEXs. For example, CloudEXs can develop auxiliary platforms like BitAV [13]. They can use this blockchain-based platform to store the list which records those customer accounts who are banned from CloudEXs owing to malicious behaviours. Meanwhile, CloudEXs can provide

Table 3
Comparison of diverse attacks on reputation system.

Type	Actions	Vulnerable target	Examples
Self-promoting	Fabricate positive feedbacks	A system without the source authentication system	Anonymous users, sybil attack
Whitewashing	Profit through malicious behaviours and reenter with new identity	A system where identities can be changed easily	Anonymous users
Slandering	Harm other people's reputation	A system without the source authentication system	Anonymous users
Orchestrated	Use different strategies and attackers are divided into several groups	Nearly all kinds of systems	Oscillation attack
Denial of Service	Send requests to server continuously in order to make it inoperable	A system which requires instant returns	Sybil attack, anonymous users, out of range attack, false rating

data-access recording services like [10]. These services are based on blockchain and access records are immutable. As a consequence, any private data leaking is detectable. In this way, blockchain can well protect users' data from leaking or accessing without authorization.

4.2. Blockchain-based reputation systems

Issues: The ability to assess one's reputation in a market is quite essential as it can be used to measure to what extent one can be trusted. The reputation system helps parties quantify the trust of each other so that users prefer to make transactions with the ones with higher reputation scores. Different kinds of attacks [20] which can help malicious people gain more business partners in CloudEXs and Table 3 gives a comparison of them. It is worth noting that these attacks are classified according to the attack goals instead of the attack methods [20].

- *Self-promoting attack*: It can be performed by a single person or an organization. A single person may falsify positive feedbacks to increase his or her reputation scores when the reputation authentication mechanism does not work normally. Participants can collude together to make real positive feedbacks for each other to increase their own reputation score finally. It is quite difficult to find out the collusions. Since transactions can be made in a very short period in CloudEX, self-promoting attacks by colluded users can be launched easily. For example, an attacker may perform a sybil attack to promote a user's reputation.
- *Whitewashing attack*: It is also called self-serving attacks. Malicious attackers behave dishonestly to earn profits in several transactions as long as their reputation scores have not reached the underline of CloudEX. After profiting through their vicious actions, they reenter the market with a totally new identity and a fresh reputation. This attack always happens in those markets in which identities can be changed easily. Anonymous user attack is one of the whitewashing attacks. The solution to the whitewashing attack is to identify real identities of users. If a CloudEX requires users to register with their real identity, this attack can be almost prevented.
- *Slandering attack*: Contrast to self-promoting attacks, malicious attackers can benefit by harming other competitors' reputation. They gather as a group and make plenty of negative feedbacks about their rivals. In a system without data authentications, slandering attacks may degrade some legitimate users reputation and let others choose malicious users instead. The anonymous-users attack can also be regarded as one of the slandering attacks since anonymous users can gather together as a group and harm their rivals. At the same time, their bad reputation records can be less suspicious. It is also difficult to discover collusion slandering attacks. In CloudEX, users can choose whether to make transactions with the selected potential partners. So slandering attack is hard to implement in CloudEX.
- *Orchestrated attack*: Orchestrated attacks can be more effective than the aforementioned attacks since they utilize different strategies. Unlike the simple fabrications in self-promoting, attackers in orchestrated attacks change behaviours frequently and sometimes they will be deliberately divided into several hostile groups to perform attacks. Oscillation attack [21] is one kind of orchestrated attacks, in which people form teams which play different roles. Collusion here becomes increasingly difficult to be identified because attackers might play different roles at different time. Reputation system in CloudEX is vulnerable to this kind of attack.
- *Denial of Service*: Non-rational attackers will perform such attacks trying to subvert the whole reputation system. They can send requests to the server continuously to cause the server overloaded, inoperable or even worse. The market that works with a paralyzed reputation system can let malicious users with unqualified reputation scores seize the opportunities to earn illegal money. At the same time, the out-of-range rating and the false rating may result in the system runtime error. For example, if the reputation rating choices are A, B, C and the attacker inputs F. The system may have troubles in dealing with this input and consequently the whole system crashes.

Blockchain solutions: Centralized reputation systems are vulnerable to malicious attacks. Thus, a decentralized reputation system is going to gain momentum in the future. Blockchain can be the foundation of a decentralized reputation system. A simple feedback based reputation on top of Bitcoin blockchain was proposed to solve the centralization problem [22]. This method adopts a scheme to connect a Bitcoin payment with its service: three outputs in the transaction, in which one is for change, another one is for service provider, the last one with zero amount is for service. By tracking all the transactions before, a service's reputation can be easily calculated. On the contrary, Dennis et al. [23] proposed a more complex blockchain-based reputation system for peer-to-peer network. The reputation is restricted to one bit of data in order to reduce network loads and increase efficiency. To prevent fabricating positive feedbacks through collusions, it requires a receipt to prove that the users have really received the file. The receipt which is encrypted with the receiver's private key contains timestamps and hash of the file.

Smart contracts can also be used to construct a reputation system. The white page of Ethereum mentioned that one can easily create a name registration system with a few lines of codes. Moreover, Yasin et al. [24] proposed a smart contract management framework referring to personal online ratings based on digital identity. Ref. [25] proposed a new reputation system for data credibility assessment in a vehicular network based on the blockchain techniques. Based on ratings stored in the blockchain, vehicles are able to calculate the reputation value of the message sender and then evaluate the credibility of the message. The work of [26] proposed a blockchain-based anonymous reputation system (BARS) to break the linkability between real identities and public keys to preserve privacy. They used two blockchains to achieve the certificate and revocation transparency. Ref. [27] proposed a dynamic and customized reputation system framework to evaluate the credibility of cloud service vendors. They incorporated a Blockchain-based module into cloud service reputation system to prevent the credit value from being artificially tampered. The work of [28] implemented a protocol that is built into the blockchain technology, by allowing for access control, transactions and data storage that are indelible as the blockchain itself.

4.3. Transaction negotiation and dispute management

Issues: to brokers and the brokers submit those service requests to CloudEX. Brokers act as agents when users find it troublesome to navigate the marketplace to find suitable services. Brokers are known to have existed for a long time and users employ these brokers to trade on their behalf as trading can take a lot of time and efforts. Though convenient, brokers account for a large percent of the whole transaction costs. On the other hand, quality and reliability of the services are becoming increasingly important when the service-oriented architecture is being used widely. After the negotiations between customers and service providers, both of them will commit to an agreement called Service Level Agreements (SLA). Expected level of services between the customer and the provider is stated in the agreement including the response time and the throughput. It is obvious that these parameters in the agreement need to be monitored carefully in case of violation of the agreement. We anticipate that the management service will be handling financial penalties similar to the real world utility industry practices. However, it is hard to achieve this in practice because there is actually no financial binds to users. An alternative of finding a middleman to receive funds is also not reliable. When users put in their data or deploy the applications, it means that users have lost the full control over their data. Data can be stolen or deleted accidentally. Now with SLA, the management responsibilities have been declared at both customers and service providers and neither of them is in good position to solve the problems. Disputes can arise easily if there is something wrong with the data or applications. Users may suspect service providers' honesty while service providers may blame the users. It is hard to tell whether a node is trustworthy or not especially in an environment where nobody knows each other. Apparently, such problems may discourage the cloud business. Thus some strategies must be put forward to determine either the buyer or seller has caused the problem. Third party mediator has been used as a solution as they can find out who is to be blame after service inspection. However, taking the issue of security into consideration, both parties in transactions will not reveal all the SLAs to an untrusted middleman.

Accountability is regarded as an efficient means to address those troubles. An accountable system maintains a tamper-resistant record that provides non-repudiable evidence of all nodes' actions. Within an accountable system, faults can be quickly detected and each fault can be linked to exactly one party, which is of great importance to transaction disputes. An accountable cloud [29] offer the following facilities:

- *Tamper-resistant logs*: Each node maintains a log which records all of its operations including sending messages and receiving messages. Once the log is tampered, users can easily detect it, thereby providing a solid basis for accountable clouds.
- *Virtualization-based replay*: Users can replay the inputs in the log into the software instances to validate the process if the software is deterministic. If the software is not deterministic, users can still check it by comparing the results of running the same software in similar virtual machines.
- *Trusted timestamp*: It aims to solve SLA violation problems. By adding trusted time-stamp information in the log, we can replay the operation in another machine with similar conditions promised by service providers. If the time segments differs greatly, it is obvious that the service provider violated SLA.
- *Sampling*: By having the cloud perform frequent checkpoints and allow the customers to audit segments randomly, SLA violations can be detected with a high probability.

Table 4
Methods to solve transaction dispute.

Methods	Aim	Requirements	Blockchain fitting characteristics
lightgray *Tamper-evident log*	Detecting incorrect execution	Logs are tamper-evident	Immutable
Virtualization-based replay	Detecting incorrect execution	Logs are tamper-evident	Immutable
Trusted timestamping	Detecting SLA violation	A trusted middleman to record time	Reliable and trusted
Sampling	Detecting SLA violation	Logs are tamper-evident	Immutable

Accountability for correctness works well but there still exist some flaws. For example, there is currently no way to achieve accountability for confidentiality.

Blockchain solutions: Scoca et al. [30] propose to use smart contracts to avoid the role of broker. Smart contracts were proposed in 1997 and implemented by blockchain. Within the context of blockchain, smart contracts are codes stored in the blockchain and are executed in a prescribed manner. They firstly use the dSLAC language to specify parties' needs and establish smart contracts. There has been a problem in the combination of smart contract and cloud matchmaking as the matchmaking does not always make exact match. So they propose a utility function which evaluates the agreements according to both parties' preferences. Then negotiation can be achieved automatically. A smart contract can be deployed on blockchain and the funds can be sent to the contract address. Funds in the contract can only be transmitted once the transaction is over.

Table 4 summarizes our major findings.

- *Tamper-evident log*: Logs used for recording inputs and outputs should be tamper-resistant, which means that user can easily detect the tamper in the file while blockchain is designed to be immutable. All the information stored in blockchain cannot be tampered and any changes will be detected by any honest miner.
- *Trusted timestamping*: Lacking mutual trust, the instant timestamping service can only be provided by a trusted middleman. Apparently, blockchain can play the role of a trusted middleman charging low fees. Each node of the blockchain network has a full copy of the blockchain. Thus, fake timestamps can be easily discovered, leaving the node no choice but to insert the correct timestamps into the log.

As for visualization replay and sampling, they are all based on the hypothesis that the logs are correct, which is ensured by blockchain technology.

5. Open research issues

As we have discussed in previous sections, blockchains can be leveraged to enhance existing CloudEXs. However, there are a number of issues to be resolved since the blockchain technology and CloudEX development are still in infancy. We present four possible future directions which are of great significance to future CloudEXs.

5.1. Heavy blockchain network

Although blockchain is famous for its decentralized network, it requires each node to store full records of the transactions. The size of the well-known Bitcoin blockchain has exceeded 180 Gigabytes. A CloudEX customer may be reluctant to spend such huge storage to save all the transactions. The heavy size of blockchain highly limits the wide application of blockchain-based CloudEXs. To address such problem, some lightweight blockchain systems have been proposed. They need not to store the whole transaction but the headers of each block for verification of transactions. However, given only a very small amount of CloudEX users maintaining the blockchain, CloudEX which has larger computing power might easily overwrite the blockchain and reverse the transaction (For details about rolling back blockchain transactions, readers can refer to [11]). In this way, blockchain that is no longer decentralized is not safe anymore.

5.2. Incorporating smart contract

In the past time, smart contract was just a fantasy owing to the limited technology development. In recent years, armed with blockchain technology, smart contracts are gaining wide attention from the world for its great capability in executing contract laws automatically. Users can send the contract to the blockchain and the contract clauses will be executed automatically once the prescribed conditions are satisfied. Built on top of blockchain technology, smart contract can make transactions in CloudEX more convenient and more efficient. Currently, there are few studies about the integration of smart contracts with cloud computing while this incorporation is expected to bring considerable benefits to existing CloudEXs.

5.3. Blockchain-based market model support

To satisfy requirements of all kind of customers, a CloudEX is obligated to implement many popular market models such as commodity market, auction model, and bargaining model. Building such models requires intensive efforts since it entails the expert knowledge of these market models. Establishing different market models based on blockchain make the problem more complicated. In addition, supporting more market models means the complexity of the system is increasing and it can also introduce many software engineering problems in development, such as the development process heterogeneity and management policy heterogeneity.

5.4. Comprehensive transaction dispute resolution

As we have explored in previous sections, blockchain can help address the commonly transaction disputes between service providers and cloud customers. But there are many problems that may not be well handled by blockchain technology. For example, the advertisement situation where CloudEX displays advertisement without warning is hard to solve. Meanwhile, to remove potential SLA violations, CloudEX can monitor the cloud resources used by the cloud customers. However, it is hard to determine how the resources should be monitored. Too strict resource monitoring might requires the running information of the cloud resources which might leak users' privacy-concerned data or cause other vulnerabilities.

6. Conclusion

We have witnessed the proliferation of various cloud applications. However, current cloud service markets are mainly dominated by several cloud service providers who can monopolize the service price especially in this less-competitive environment. Meanwhile, the single-product market structure cannot provide end users with flexible cloud services that fulfil diverse demands. Therefore, cloud exchange (CloudEX) is a necessity to reshape the incumbent cloud market. On the other hand, most of existing CloudEX platforms are based on centralized architecture, thereby resulting in vulnerabilities of single point of failure, malicious attacks and tampered data. Blockchain offers a potential decentralization solution to the challenges of current CloudEX platforms. Blockchain can guarantee the trustworthy transactions even in trust-less environment by executing decentralized consensus protocol. Thus, the third intermediary is no longer necessary so as to save the cost. Moreover, transaction records are tamper-resistant since each node keeps a full copy of the ledger.

In this paper, we present a survey on the integration of blockchain with CloudEX. We discuss the challenges for existing CloudEX platforms, in which blockchain can be leveraged to decentralize CloudEX platforms, which have a number of advantages compared with the centralized CloudEXs. In particular, armed with blockchain technology, decentralized CloudEX platforms can reduce privacy leakage risk, mitigate the single point of failure, guarantee fairness in the transaction dispute.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The work described in this paper was supported by the National Key Research and Development Program (2016YFB1000101), the National Natural Science Foundation of China (61472338, U1811462). Imran's work is supported by the Deanship of Scientific Research at King Saud University through research group number RG-1435-051.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.compeleceng.2019.106526.

References

[1] Dai H-N, Wong RC-W, Wang H, Zheng Z, Vasilakos AV. Big data analytics for large scale wireless networks: challenges and opportunities. ACM Comput Surv 2019;52(5) Article 99. doi:10.1145/3337065.

[2] Dai H-N, Zheng Z, Zhang Y. Blockchain for internet of things: a survey. IEEE Internet Things J 2019;6(5):8076–94. doi:10.1109/JIOT.2019.2920987.

[3] Zhang M, Ranjan R, Haller A, Georgakopoulos D, Menzel M, Nepal S. An ontology-based system for cloud infrastructure services' discovery. In: 8th international conference on collaborative computing: networking, applications and worksharing (CollaborateCom); 2012. p. 524–30.

[4] Han S-M, Hassan MM, Yoon C-W, Huh E-N. Efficient service recommendation system for cloud computing market. In: Proceedings of the 2nd international conference on interaction sciences: information technology, culture and human, Seoul, South Korea; 2009. p. 839–45.

[5] Buyya R, Ranjan R, Calheiros RN. Intercloud: utility-oriented federation of cloud computing environments for scaling of application services. In: Proceedings of international conference on algorithms and architectures for parallel processing, Busan, Korea; 2010. p. 13–31.

[6] Wang H, Shi P, Zhang Y. Jointcloud: a cross-cloud cooperation architecture for integrated internet service customization. In: 2017&nbsp;IEEE 37th international conference on distributed computing systems (ICDCS); 2017. p. 1846–55.

[7] Menychtas A, Gomez SG, Giessmann A, Gatzioura A, Stanoevska K, Vogel J, Moulos V. A marketplace framework for trading cloud-based services. In: Proceedings of international workshop on grid economics and business models, Paphos, Cyprus; 2011. p. 76–89.

[8] Keser C. Experimental games for the design of reputation management systems. IBM Syst J 2003;42(3):498.

[9] Garg SK, Vecchiola C, Buyya R. Mandi: a market exchange for trading utility and cloud computing services. J Supercomput 2013;64(3):1153–74.

[10] Zyskind G, Nathan O, et al. Decentralizing privacy: Using blockchain to protect personal data. In: Proceedings of security and privacy workshops (SPW), San Jose, California; 2015. p. 180–4.

[11] Zheng Z, Xie S, Dai H-N, Wang H, Chen X. Blockchain challenges and opportunities: a survey. Int J Web Grid Serv 2018;14(4):352–75.

[12] Jensen M, Schwenk J, Gruschka N, Iacono LL. On technical security issues in cloud computing. In: Proceedings of IEEE international conference on cloud computing, Maimi, Florida, USA; 2009. p. 109–16.

[13] Noyes C.. BitAV: fast anti-malware by distributed blockchain consensus and feedforward scanning. 2016. arXiv:160101405.

[14] McCorry P, Shahandashti SF, Hao F. A smart contract for boardroom voting with maximum voter privacy. In: International conference on financial cryptography and data security; 2017. p. 357–75.

[15] Xia Q, Sifah EB, Smahi A, Amofa S, Zhang X. Bbds: blockchain-based data sharing for electronic medical records in cloud environments. Information 2017;8(2):44.

[16] Peterson K, Deeduvanu R, Kanjamala P, Boles K. A blockchain-based approach to health information exchange networks. In: Proceedings of NIST workshop blockchain healthcare, vol. 1; 2016. p. 1–10.

[17] Esposito C, De Santis A, Tortora G, Chang H, Choo K-KR. Blockchain: a panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput 2018;5(1):31–7.

[18] Bag S, Azad MA, Hao F. A privacy-aware decentralized and personalized reputation system. Comput Secur 2018;77:514–30.

[19] Azad MA, Bag S, Hao F. Privbox: verifiable decentralized reputation system for online marketplaces. Future Gener Comput Syst 2018;89:44–57.

[20] Hoffman K, Zage D, Nita-Rotaru C. A survey of attack and defense techniques for reputation systems. ACM Comput Surv (CSUR) 2009;42(1):1.

[21] Srivatsa M, Xiong L, Liu L. Trustguard: countering vulnerabilities in reputation management for decentralized overlay networks. In: Proceedings of the 14th international conference on World Wide Web. ACM; 2005. p. 422–31.

[22] Carboni D.. Feedback based reputation on top of the Bitcoin blockchain. 2015, arXiv:150201504

[23] Dennis R, Owen G. Rep on the block: a next generation reputation system based on the blockchain. In: Proceedings of 10th international conference for internet technology and secured transactions (ICITST), London, UK; 2015. p. 131–8.

[24] Yasin A, Liu L. An online identity and smart contract management system. In: Proceedings of computer software and applications conference (COMPSAC), Atlanta, Georgia, USA, vol. 2; 2016. p. 192–8.

[25] Yang Z, Zheng K, Yang K, Leung VCM. A blockchain-based reputation system for data credibility assessment in vehicular networks. In: Proceedings of 28th IEEE annual international symposium on personal, indoor, and mobile radio communications (PIMRC); 2017. p. 1–5.

[26] Lu Z, Wang Q, Qu G, Liu Z. Bars: a blockchain-based anonymous reputation system for trust management in vanets. In: Proceedings of 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE); 2018. p. 98–103.

[27] Ye F, Zheng Z, Chen C, Zhou Y. DC-RSF: a dynamic and customized reputation system framework for joint cloud computing. In: Proceedings of IEEE 37th international conference on distributed computing systems workshops (ICDCSW); 2017. p. 275–9.

[28] Owiyo E, Wang Y, Asamoah E, Kamenyi D, Obiri I. Decentralized privacy preserving reputation system. In: Proceedings of IEEE third international conference on data science in cyberspace (DSC); 2018. p. 665–72.

[29] Haeberlen A. A case for the accountable cloud. ACM SIGOPS Oper Syst Rev 2010;44:52–7.

[30] Scoca V, Uriarte RB, De Nicola R. Smart contract negotiation in cloud computing. In: Proceedings of 10th international conference on cloud computing (CLOUD); 2017. p. 592–9.

Shaoan Xie is a graduate student at Sun Yat-Sen University, China. He received his bachelor degree in Computer Science at Sun Yat-sen University in 2016. His current research interests include blockchain and data mining.

Zibin Zheng is a professor at Sun Yat-sen University, Guangzhou, China. He received Ph.D. degree from The Chinese University of Hong Kong in 2011. He received ACM SIGSOFT Distinguished Paper Award at ICSE'10, Best Student Paper Award at ICWS'10, and IBM Ph.D. Fellowship Award. His research interests include services computing, software engineering, and blockchain.

Weili Chen is currently working toward the Ph.D. degree in the Department of Data and Computer Science, Sun Yat-Sen University, China. His research interests include blockchain and data mining.

Jiajing Wu received the B. Eng. degree in communication engineering from Beijing Jiaotong University, Beijing in 2010 and the Ph.D. degree from Hong Kong Polytechnic University, Hong Kong, in 2014. In 2015, she joined the School of Data and Computer Science, Sun Yat-sen University, Guangzhou, where she is currently an Associate Professor. Her research interest includes network science and its applications.

Hong-Ning Dai is an Associate Professor in Faculty of Information Technology at Macau University of Science and Technology. He obtained the Ph.D. degree in Computer Science and Engineering from the Chinese University of Hong Kong. He has published more than 100 peer-reviewed papers in refereed journals and conferences. His research interests include big data analytics and Internet of Things.

Muhammad Imran is working as an Associate Professor in the College of Applied Computer Science at King Saud University, Saudi Arabia. His research interests include mobile & wireless networks, IoT, cloud/edge computing, and information security. He has published more than 150 research articles in refereed international conferences and journals. He serves as an associate editor for many international journals.