American Journal of Engineering and Applied Sciences

Review

Blockchain: Methods, Applications and Technology Progress

[1]Cheryl Ann Alexander and [2]Lidong Wang

[1]*Technology and Healthcare Solutions, Inc., Vicksburg, MS, USA*
[2]*Institute for Systems Engineering Research, Mississippi State University, Vicksburg, MS, USA*

Article history
Received: 02-12-2018
Revised: 29-12-2018
Accepted: 05-01-2019

Corresponding Author
Cheryl Ann Alexander
Technology and Healthcare Solutions, Inc., Vicksburg, MS, USA
Email: tech.health.sol@gmail.com

Abstract: Blockchain is gaining great attentions in various applications. Blockchain is a shared ledger concept which is highly secure due to the nature of its construction. It is immutable, needs a consensus to add a block to the chain, is held secure by a hash function and is visible to all participants within the blockchain. The methods, impacts and benefits of blockchain are introduced. The applications and the technology progress of the blockchain technology are presented, which include applications and progress in Internet of Things (IoT) and cloud, medical applications and healthcare, supply chain security and management in identity, resources, ownership, mobility and keys for heterogeneous vehicular network.

Keywords: Blockchain, Internet of Things, Cloud, Healthcare, Supply Chain, Management

Introduction

Providers of online services and contents, including e-commerce and big data provider sites, can frequently capture enormously huge volumes fromend users' Personally Identifiable Information (PII). In addition, some end users have major anxieties about the security of personal datastored on the cloud. Blockchain elements have been used to deal with the issues of privacy and trust in data transfer, data verifiability and data security using a designed mathematical cryptosystem. A hash-based mathematical protocol permits the system to be cryptographically invulnerable and complicated. Transactions are confirmed by the consensus of members in the system, therefore enabling a digital distributed consensus (Banerjee and Joshi, 2017).

The blockchain technology, which provides provenance and transparency, has been used to mitigate problems between electricity consumers and companies such as electricity bills and utility. A smart contract that performs arranged procedures to secure a trust-based system among participants contributing to the network has also been fulfilled. Blockchainis highly effective because it can be used to the use of electricity by users and it offers a platform without any handling from other participants (Gao *et al*., 2018). The insurance market includes certain characteristics (processes performed, services delivered, customers served, etc.) which has made blockchain adoption especially controversial because it is not yet clear whether it is ideal for investment; however, investigation has been initiated with the conception of B3i that is the first blockchain-centered insurance consortium (Gatteschi *et al*., 2018).

Keeping the Internet of Things (IoT) devices safe can be a difficult task to achieve. Many security policies are developed to make devices small, cheap and easy to use, which increases the security breach risk. Ensuring that legitimate devices are the only ones included in blockchain private networks is necessary; therefore, root servers need to authenticate any device prior to providing it to the nodes list. Each communication must be authenticated and encrypted effectively to ensure confidentiality and integrity. The blockchain technology has been a suggested resolution for developing more secure IoT systems (Singh *et al*., 2018).

A feasibility and value analysis of a blockchain group slice broker case study was presented based on a resource configuration framework. This case fostered an industrial automation process to dynamically and independently attain the slice necessary to ensure more competent operations. By demonstrating the general applicability of the blockchain network slice broker/ledger use case, a higher value than expected was proven for resource management and configuration. One benefit was that most of the investigated micro processes were applicable to the 5G network slice broker and ledger platform; the blockchain technology abilities powerfully support the execution of the process mechanisms (Valtanen *et al*., 2018).

Networks and communication resources use primarily closed sources and centralized structures, which opposes privacy and data security values. A centralized system cannot completely endure the conception of fast, consistent, transparent and nonstop communications. Communication conceivable with blockchain technology is decentralized, distributed, immutable, as well as transparent. A user can manipulate their own digital identity, communicating as well as sharing with trust. One blockchain-based communication application, Cryptouch, has been proposed (Sarıtekin *et al*., 2018). Another fast-becoming important technology for future networks growing a demand for local services is Device-to-device (D2D) communication. For users of the D2D network, fairness can be enforced by using a blockchain-based credit structure which is merged with the connectivity-aware task scheduling scheme (Hong *et al*., 2017).

The purpose of this paper is to introduce the methods, applications and technology progress of the blockchain technology. The organization of this paper is as follows: the next section introduces the methods and materials of the blockchain technology; then the impacts, benefits, applications and technology progress are presented; and the final section is the conclusion.

Methods and Materials

The elementary idea of blockchain technology is rather uncomplicated: a shared, replicated log file (otherwise known as a ledger). Data are time-stamped as well as sequential. A one-way function generates a short bit string (i.e., 512 bits); it is contingent upon individual data and its location within the log. Blockchain technology offers a reliable method to record shared data. A blockchain can be simply defined as a publicly verifiable ledger which can maintain the integrity of individual participants (Orman, 2018). A blockchain can be regarded as a digital distributed ledger utilized to register and share information through a peer-to-peer network (Fig. 1).

Table 1 (Kokina *et al*., 2017) lists several significant blockchain concepts. Special participants known as miners solve complex mathematical problems which unlocks transactions and sorts them into blocks and checks the validity; this starts a consensus protocol to append the blocks into the blockchain. Bitcoin utilizes proof-of-work (PoW) to obtain consensus: only a miner that successfully solves a difficult computational puzzle (i.e., solving for the right nonce for the block header) can append a blockchain (Dinh *et al*., 2018). Miners can be anyone and connect with each other in a peer-to-peer network over the Internet. Any server can join the block chain network. Users then connect to the peer-to-peer network and issue cryptographically secured transactions. The miner must solve the puzzle to form a block, consuming both capitals and operational resources for each block-this wasting of resources is part of the checks in the design which enable financial integrity and security in the decentralized consensus system and the solution is called proof of work (PoW) (Eyal, 2017).

Table 1: Several significant concepts of Blockchain

Concepts	Description
Miner (Forger under PoS)	Providing the computing power of creating blocks and verifying transactions; storing the blockchain.
Block	Containing transactions which need miner's verification and then are added into a blockchain.
Hash	Uniquely identifying each block of a blockchain
Hash function	Generating a hash (also called hash code) with a fixed length.
Smart contract	Agreements stored in a blockchain which will be implemented when pre-specified conditions are satisfied.
Consensus protocol	Rules about stating the kind of prize the miners can get and how miners use resources to build blocks, attain consensus (such as verifying blocks).

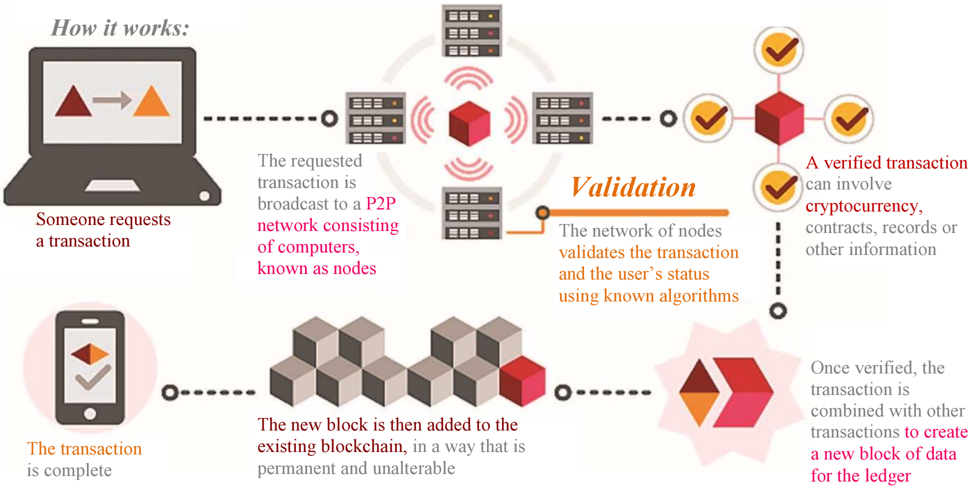
How it works:
Someone requests a transaction
The requested transaction is broadcast to a P2P network consisting of computers, known as nodes
Validation
The network of nodes validates the transaction and the user's status using known algorithms
A verified transaction can involve cryptocurrency, contracts, records or other information
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger
The new block is then added to the existing blockchain, in a way that is permanent and unalterable
The transaction is complete

Fig. 1: The blockchain technology and its work process (Ducas and Wilner, 2017)

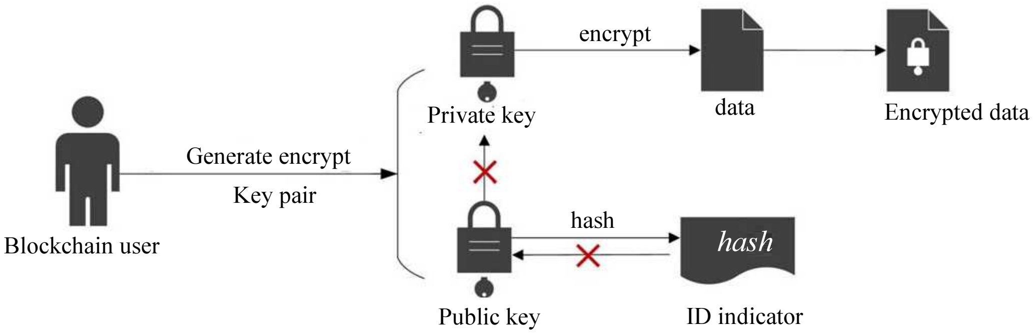

Fig. 2: Preserving-privacy of blockchain (Dai *et al*., 2017)

Blockchain uses the asymmetric encryption mechanism to allow users to encrypt data with a private key which functions as the ID indicator of the user. The hash value of a user's public key is calculated and serves as the public address. The hash value does not have any relationship with the actual user's identity, therefore making the user's personal private data safe. The process of calculating a hash value is reversed, which means an adversary cannot calculate a user's public key from the public user address and calculating the private key from the public key is not possible. Therefore, blockchain accomplishes the objective of conserving user anonymity and privacy (Dai *et al*., 2017). Figure 2 shows the privacy protection of blockchain.

To offer transparency, blockchain creates a tamper-proof digital ledger of transactions and the ledger can be shared with all participants simultaneously. Because cryptography permits a secure method for adding to the ledger it is conceivable for blockchain technology to decrease or eliminate integrity violations such as corruption and fraud while also decreasing transaction costs. This correspondingly allows the production of smart ("tagged") property and gives the blockchain participant the ability to control it with a smart contract (Kshetri and Voas, 2018). Some researchers proposed a privacy-preserving blockchain incentive mechanism in crowd sensing applications. A cryptocurrency is built on the blockchains and is applied as a secure motivation approach. High quality users or contributors can get their payments which are recorded in transaction blocks. Miners will verify the transaction according to the sensing data assessment criteria published by the server. Because the transaction information can disclose a user's privacy, node cooperation verification has been developed to achieve k-anonymity privacy protection (Wang *et al.*, 2018).

The tamper-proof and immutable features of the blockchain technology propose incredible potentials in building an infrastructure with accountability for the business of web-based services. But, many existing consensus protocols of public blockchains suffer from any of resource overheads, performance issues, fairness pitfalls, or security weaknesses. Most consensus protocols of consortium/private blockchain do not support large scale networks due to scalability limitations. A consensus protocol named Proof-of-Trust (PoT) consensus has been have proposed. The PoT protocol avoids the low throughput and resource intensive pitfalls related to Bitcoin's "Proof-of-Work" (PoW) mining, while dealing with the scalability issue related to the traditional Paxos-based and Byzantine Fault Tolerance (BFT)-based algorithms (Zou *et al*., 2018).

Impacts, Benefits, Applications and Technology Progress

Certain features of blockchain, such as the decentralized, immutable, trustless, as well as irreversible stand as favorable for multiple Information Technology (IT) applications. A novel Emission Trading Scheme (ETS) model customized for Industry 4.0 integration has been developed. Blockchain technology and smart devices were utilized in the model to improve the compliance measure of the ETS policy. Blockchain characteristics such as immutability and transparency can ensure data accuracy which is necessary to ensure the scheme (Khaqqi *et al*., 2018). Table 2 (Kim and Justl, 2018) shows various applications of Blockchains and Impacts or Effects. Table 3 (Dorri *et al*., 2017) lists some major benefits of blockchain compared traditional methods.

Applications and Progress in Internet of Things and Cloud

Fog and edge architectures deliver a link amid centralized clouds as well as the environment with sensors and IoT. However, trust needs to be ensured for an open environment which crosses organizational boundaries and is subject to security problems. The problems can be the integrity and source of data, the identity of software applications and hardware devices and the contractual character of composition. The architecture design which maintains orchestration trust for edge clouds has been proposed. The provenance framework is supported by permissioned blockchain technology (Pahl *et al*., 2018).

Table 2: Some applications of the blockchain technology

Blockchain Applications	Impacts or Effects	Examples
Records management	Creating secure and almost immutable records.	Personal government records (e.g., certificates of birth, death and marriage), medical records
Transaction clearance	Much decreased settlement time	Transactions of real estates, secure trading
Supply chain management and authentication	Permitting parties along the supply chain (e.g., retailers, end-consumers) to verify the quality and origin of the products.	Luxury goods, diamonds
Smart contracts	Excellent certainty among contract parties without intermediaries.	Distribution and shipping agreements

Table 3: Some advantages of blockchain over traditional methods

Applications	Traditional methods	Blockchain advantages
Car-sharing services	• Central authorization	• Distributed authorization
	• Central accounting and payment	• Private and distributed security, accounting and payments
	• Users can be tracked using their identity	• Users utilize changeable identities
Insurance	• Privacy-sensitive data need to be continuously sent to the insurance company for services	• Privacy-sensitive data is shared on demand instead of a continuous data exchange
	• Users lack control over exchanged data	• Users can control exchanged data
	• Often not secure	• Distributed, secure and privacy-preserving in data exchange
Electric vehicles	• The behavior and location of a user can be tracked.	• Data such as user's location keep private
	• Central accounting and payment	• Private and distributed security, accounting and payments
Wireless remote software update (WRSU)	• Lack of privacy	• Privacy-preserving
	• Partial participation: not addressing a full chain	• End-to-end
	• Centralized-not scalable	• Scalable due to distributed data exchange and security
	• Only an original equipment manufacturer can verify communications or the history of update downloads.	• Update history and authenticity of the software can be verified publicly.

An architecture for arbitrating permissions and roles in IoT was recently presented; the architecture, a completely distributed access control system for IoT founded on the blockchain technology. It was supported by a proof of concept operation as well as assessed in real-time IoT situations. Evidently, blockchain technology might be utilized as access management technology in exact scalable IoT scenarios. As a comparison to further centralized system proposals, this method has advantages such as accessibility, lightweight, transparency, mobility, scalability and concurrency to access control in IoT (Novo, 2018).

After analyzing the challenges of large-scale IoT networks due to novel communication paradigms, a distributed secure IoT network architecture called DistBlockNet and which comprises a Software Defined Networking (SDN) base network has been presented based on the blockchain technology to meet new service requirements as well as to tackle future as well as existing trials. DistBlockNet can improve a system's capacity and performance. The core character of the DistBlockNet model is to detect security threats; implement protections such as access control, data protection and threat prevention and mitigate network attacks including DDoS/DoS attacks and cache poising/ARP spoofing. The DistBlockNet model also has the function of decreasing the attack window time by permitting IoT forwarding devices to rapidly inspect and download the most current table of flow rules if essential (Sharma *et al*., 2017).

A privacy-aware Blockchain Connected Gateway (BC gateway) has been designed, where the blockchain network is used as the underlying architecture for the administration of privacy preferences of IoT devices in the blockchain network. It means that the designed BC gateway utilizes the blockchain technology to manage and protect the sustained user preferences from being altered. Thus, the BC gateway enhances user privacy protection while legacy IoT devices are used (Cha *et al*., 2018). A decentralized solution for IoT data trusted exchange was presented created on the blockchain technology to ensure IoT data exchange performed in a completely transparent and trusted environment. A prototype based on the Ethereum blockchain and smart contracts was realized; its decentralized, transparent and auditable features were presented (Huang *et al*., 2017). The framework of IoT data exchange can be divided into three layers and it is shown in Fig. 3.

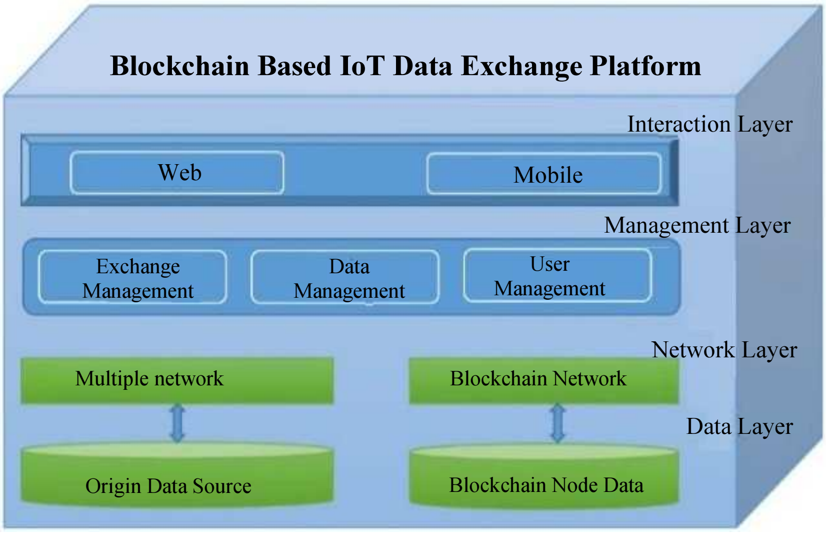

Fig. 3: The architecture of an IoT data exchange platform based on the blockchain technology (Huang *et al*., 2017)

In Industrial Internet of Things (IIoT), Peer-to-Peer (P2P) energy trading ubiquitously happens in different scenarios such as microgrids, vehicle-to-grid networks and energy harvesting networks. But there are general privacy and security challenges resulting from non-transparent and untrusted energy markets in the scenarios. The blockchain technology was used to develop a secure energy trading system called energy blockchain to deal with the security challenges. This energy blockchain avoids a trusted intermediary and can be extensively used in general scenarios of P2P energy trading (Li *et al*., 2018).

Most research at present in cloud trust concentrates on keeping a trustworthy hardware platform through attestation authenticated by a Trusted Third Party (TTP). A method has been presented for improving cloud trust which leverages blockchain to track data and reduce the problems due to depending on TTPs for storage and policy evaluation. The Ethereum blockchain was proposed to use for smart contracts and storage as the vehicle for the policies. The main contribution of this work lies in: (1) reduces the dependence on a TTP for attestation; (2) avoids the conflict of interest through putting policy storage into a decentralized blockchain; and (3) uses smart contracts forstoring and functionally evaluating the policies (Kirkman and Newman, 2018).

A blockchain-based distributed cloud architecture with Software Defined Networking (SDN) has been presented, which enables controller fog nodes at the edge of the network to meet the required design principles. The presented model provides secure, low-cost and on-demand access to the most competitive computing infrastructures in an IoT network. The presented model enables cost-effective high-performance computing through building a distributed cloud infrastructure. In addition, a secure distributed fog node architecture which uses SDN and the blockchain technology was presented (Sharma *et al*., 2018). A blockchain-based publicly verifiable data deletion scheme was developed. The scheme enables a data owner to detect the malevolent operation of a cloud server if the cloud server does not delete the data honestly. The primitive of Blockchain was introduced to solve the public verification problem in the secure data deletion scheme. The proposed protocol can obtain public verification due to the advantages of the blockchain system (Yang *et al*., 2018).

Medical Applications and Healthcare

MeDShare, a system which deals with the problem of the data sharing among big data custodians of in a trust-less situation in medical applications, has been proposed based on blockchain. The system provides data auditing, provenance and control for shared healthcare data in cloud repositories of big data entities. MeDShare can monitor entities which access data for malicious utilization from a data custodian system. In MeDShare, data sharing and transitions from an entity to the other, along with all actions conducted on the MeDShare system, are stored in atamper-proof approach. The development of the system uses smart contracts as well as an access control mechanism to track the behavior of the data and revoke access to offending entities in case of detecting the permissions violation on data (Xia *et al*., 2017).

There has been interest in applying blockchain to secure the management of healthcare data. The strong feature of blockchain in data integrity offers immutability. Any data, as soon as they are stored in blockchain, cannot be changed or deleted. But personal medical data are protected by privacy laws; many of the data do not permit personal data to be maintained perpetually. This type of data has been suggested being stored outside of the blockchain in a conventional or a distributed database; however, the hashes of the data are saved in the blockchain. Health data are stored outside of the blockchain and thereby could be secured, deleted and corrected as appropriate. Immutable hashes of the healthcare data are saved on-chain for authenticity and accuracy check for the off-chain medical data (Esposito *et al*., 2018).

A medical treatment exchange system for patients (customers) has been presented based on a blockchain network. The system is a platform which records and encrypts patients' medical information using the blockchain technology and further improves security due to its restricted counterfeit. It provides approved users with services to share medical information uploaded on the blockchain through the role-based access control. Furthermore, results from the designed system complying with domestic laws using the distributed blockchain ledger and eventually granting preliminary approval for sharing information were presented (Kim and Hong, 2017). A framework for cross-domain image sharing has been developed, which utilizes a blockchain as a distributed data store to establish a ledger of radiological studies and patient-defined access permissions. The blockchain framework eliminates a third-party access to protected health information, satisfies many criteria of an interoperable healthcare system and can be easily generalized to domains beyond medical imaging (Patel, 2018).

Modern technologies in wireless sensing and mobile computing have prompted the concept of pervasive social network (PSN)-based healthcare. A secure system for PSN-based healthcare has been proposed. The healthcare blockchain has been used for a node to share healthcare data with others. An improved version of IEEE 802.15.6 display authenticated association protocol has been developed to initialize the secure links. The protocol works better since it requires an unbalanced computational load (Zhang *et al*., 2016).

A management system for nail analysis has been proposed. It used microscope to capture nail images and a preprocessing algorithm for nail image analysis was developed to segment the lunula and nail plate efficiently. A lunula and nail plate image helps researchers do further analysis of a users' disease or healthcare. Nail images are data with personal privacy and can be used in identity management. When the image data are stored in the system, the system can use the blockchain technology to protect the privacy and integrity of the data and build users' trust in the system (Lee and Yang, 2018).

Supply Chain Security

The supply chain is a promising area for employing the blockchain technology. There have been blockchain startups in this area. For example, Everledger (www.everledger.io) has used blockchains to track diamonds' features such as cut and quality; help reduce risk and fraud for insurers, banks and open marketplaces. Data transparency and data sharing with others are main concerns for most companies which provide intermediary services in industries. Overall, blockchains are a good choice to provide traceability in supply chain management (Lu and Xu, 2017).

A crowd-validated and independent online shipment tracking framework which complements current enterprise-based supply chains management has been proposed. A blockchain ledger can be public (open or permission less) or private (permissioned).The proposed framework leverages blockchain, distributed databases and the hybrid peer-to-peer communication model to send independently validated shipment tracking information to all stakeholders in pseudo real-time. The privacy requirements of trading partners were considered through a combined private-public ledger architecture while the necessary SC visibility for critical decision-making was provided (Wu *et al*., 2017).

Blockchain can improve supply chain security, which is shown in Table 4 (Kshetri, 2017). Blockchain's public availability makes it possible to trace back every product to the origins of raw materials and transactions can be linked to identify users with vulnerable IoT devices. Blockchain can also deal with crisis situations such as product recalls after security vulnerabilities are detected (Kshetri, 2017).

Management in Identity, Resources, Ownership, Mobility and Keys for Heterogeneous Vehicular Network

Experimental test bed results for a method of user identity management were presented for cloud-based blockchain applications. Cryptographic identity tokens on the first packet was inserted using a BlackRidge Technology endpoint on a Windows host to request a new session. Identity-based end-to-end security that extends from the blockchain client to the server-side application and fabric was performed. Identity-based network segmentation and traffic separation were also demonstrated, which enables multiple users to securely share the same blockchain infrastructure, enables automated regulatory compliance audits and reduces the risk of DDoS attacks (DeCusatis *et al*., 2018).

Table 4: Supply chain security improvement through Blockchain

Directions	Blockchain's Roles
Device manufacturers/supply chain network providers → Downstream supply chain partners/device owners	• Ensuring return of products when recalls are issued • Finding users with vulnerable devices • Registering updates, patches and part replacements throughout a product's lifetime
Device manufacturers/supply chain network providers → Upstream supply chain partners	• Tracing back products to the origins of raw materials • Identifying the source of problem items/parts

An explosion of data has taken place with the development of cloud computing and many applications in IoT. Large volumes of data are generated in Datacenters (DCs), which not only evoke various potential data-driven services but also consume substantial energy each day. A decentralized resource management framework has been developed based on the blockchain technology, where requirements can be arranged by the DCs themselves without relying on the scheduler in cloud DCs. Furthermore, a request migration method with an embedded smart contract in the framework for saving costs was proposed based on reinforcement learning. Finally, simulations were performed based on Google cluster traces and the real electricity price, which demonstrated better performance in saving energy compared with other algorithms in DCs (Xu *et al*., 2017).

A Product Ownership Management System (POMS) of RFID-attached products for anti-counterfeits that can be used in the post supply chain has been proposed. With the help of the proposed POMS, a customer can reject the purchase of counterfeits even with genuine RFID tag information if sellers do not possess their ownership. A proof-of-concept experimental system employing Ethereum, a blockchain-based decentralized application platform, was implemented and its cost performance was evaluated (Toyoda *et al*., 2017).

A distributed mobility management (DMM) solution for flattened fog network architectures has been proposed based on the blockchain technology. The proposed blockchain-based DMM enables to handle hierarchical security issues without affecting the network layout. It meets the requirements of fully distributed security using three blockchains and resolves the de-registration issues that affect the existing DMM solutions. It also greatly reduces signaling burden compared with existing DMM solutions, leading to reduced energy consumption (Sharma *et al*., 2018).

A framework for providing secure key management within the heterogeneous network has been presented. The Security Managers (SMs) play a key role in the framework by capturing the vehicle departure information, encapsulating block to transport keys and then executing rekeying to vehicles within the same security domain. Akey management scheme for key transfer among SMs in heterogeneous Vehicular Communication Systems (VCS) networks has been developed (Lei *et al*., 2017).

Conclusion

Blockchain is a secure, immutable, method of storing data in blocks provided a consensus is reached among all the participants. Blockchain is a successful P2P network that uses cryptography, mathematically complex equations and the hash function to provide security and immutability. The impacts of the blockchain technology lie in: creating secure and almost immutable records, excellent certainty among contract parties without intermediaries, allowing parties to track and verify the quality and origin of products, etc. Blockchain technology can be used in healthcare, supply chain management, insurance, auctions, etc. It can be used as access management technology in specific scalable IoT scenarios. This energy blockchain avoids a trusted intermediary and can be extensively used in general scenarios of P2P energy trading with security. The blockchain technology helps protect privacy and secure the management of healthcare data through keeping the data outside of the blockchain in a traditional or a distributed database and storing the hashes of the data in the blockchain. Blockchain enables to trace back every product to the origins of raw materials and improve supply chain security. It also enables to secure management in identity, resources, ownership, mobility and keys for heterogeneous vehicular network.

Acknowledgement

Authors would like to thank Technology and Healthcare Solutions, Inc. for support.

Author's Contributions

Both the authors contributed equally to prepare, develop and complete this manuscript.

Ethics

This article is original. Authors declare that are not ethical issues that may arise after the publication of this manuscript.

References

Banerjee, A. and K.P. Joshi, 2017. December. Link before you share: Managing privacy policies through blockchain. Proceedings of the IEEE International Conference on Big Data (Big Data), Dec. 11-14, IEEE Xplore press, USA, pp: 4438- 4447. DOI: 10.1109/BigData.2017.8258482

Cha, S.C., J.F.Chen, C.Su and K.H. Yeh, 2018. A Blockchain connected gateway for BLE-based devices in the internet of things. IEEE Access, 6: 24639-24649. DOI: 10.1109/ACCESS.2018.2799942

Dai, F., Y. Shi, N. Meng, L.Wei and Z. Ye, 2017. From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues. Proceedings of the 4th International Conference on Systems and Informatics (ICSAI) Nov. 11-13, IEEE Xplore press, China, pp: 975-979, DOI: 10.1109/ICSAI.2017.8248427

DeCusatis, C., M. Zimmermann and A. Sager, 2018. Identity-based network security for commercial blockchain services. Proceedings of the IEEE 8th Annual Computing and Communication Workshop and Conference, Jan. 8-10, IEEE Xplore press, USA, pp: 474-477. DOI: 10.1109/CCWC.2018.8301713

Dinh, T.T.A., R. Liu, M. Zhang, G. Chen and B.C. Ooi *et al*., 2018. Untangling blockchain: A data processing view of blockchain systems. IEEE Trans. Knowledge Data Eng., 30: 1366-1385. DOI: 10.1109/TKDE.2017.2781227

Dorri, A., M. Steger, S.S. Kanhere and R. Jurdak, 2017. Blockchain: A distributed solution to automotive security and privacy. IEEE Communi. Magazine, 55: 119-125. DOI: 10.1109/MCOM.2017.1700879

Ducas, E. and A. Wilner, 2017. The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada. Canada's J. Global Policy Analysis, 72: 538-562. DOI: 10.1177/0020702017741909

Esposito, C., A. De Santis, G. Tortora, H. Chang and K.K.R. Choo, 2018. Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Computing, 5: 31-37. DOI: 10.1109/MCC.2018.011791712

Eyal, I., 2017. Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities. Computer, 50: 38-49. DOI: 10.1109/MC.2017.3571042

Gao, J., K.O. Asamoah, E.B. Sifah, A. Smahi and Q. Xia *et al*., 2018. GridMonitoring: Secured sovereign blockchain based monitoring on smart grid. IEEE Access, 6: 9917-9925. DOI: 10.1109/ACCESS.2018.2806303

Gatteschi, V., F. Lamberti, C. Demartini, C. Pranteda and V. Santamaría, 2018. To Blockchain or Not to Blockchain: That Is the Question. IT Professional, 20: 62-74. DOI: 10.1109/MITP.2018.021921652

Hong, Z., Z. Wang, W. Cai and V. Leung, 2017. Blockchain-empowered fair computational resource sharing system in the D2D network. Future Internet, 9: 85. DOI: 10.3390/fi9040085

Huang, Z., X. Su, Y. Zhang, C. Sahi and H. Zhang *et al*., 2017. A decentralized solution for IoT data trusted exchange based-on blockchain. Proceedings of the 3rd IEEE International Conference on Computer and Communications, Dec. 13-16, IEEE Xplore press, China, pp: 1180-1184. DOI: 10.1109/CompComm.2017.8322729

Khaqqi, K.N., J.J. Sikorski, K. Hadinoto and M. Kraft, 2018. Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application. Applied Energy, 209: 8-19. DOI: 10.1016/j.apenergy.2017.10.070

Kim, K. and J.M. Justl, 2018. Potential antitrust risks in the development and use of blockchain. J. Taxation Regulation Financial Institutions, 31: 5-16.

Kim, K.J. and S. Hong, 2017. A trusted sharing model for patient records based on permissioned blockchain. J. Internet Computing Services, 18: 75-84.

Kirkman, S. and R. Newman, 2018. A cloud data movement policy architecture based on smart contracts and the ethereum blockchain. Proceedings of the IEEE International Conference on Cloud Engineering, Apr. 17-20, IEEE Xplore press, USA, pp: 371-377. DOI: 10.1109/IC2E.2018.00071

Kokina, J., R. Manchaand and D. Pachamanova, 2017. Blockchain: Emergent industry adoption and implications for accounting. J. Emerging Technologies Accounting, 14: 91-100. DOI: 10.2308/jeta-51911

Kshetri, N. and J. Voas, 2018. Blockchain in developing countries. IT Professional, 20: 11-14. DOI: 10.1109/MITP.2018.021921645

Kshetri, N., 2017. Can blockchain strengthen the internet of things? IT Professional, 19: 68-72. DOI: 10.1109/MITP.2017.3051335

Lee, S.H. and C.S. Yang, 2018. Fingernail analysis management system using microscopy sensor and blockchain technology. Int. J. Distributed Sensor Netw. DOI: 10.1177/1550147718767044

Lei, A., H. Cruickshank, Y. Cao, P. Asuquo and C.P.A. Ogah *et al*., 2017. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet Things J., 4: 1832-1843. DOI: 10.1109/JIOT.2017.2740569

Li, Z., J. Kang, R. Yu, D. Ye and Q. Deng *et al*., 2018. Consortium blockchain for secure energy trading in industrial internet of things. IEEE Transactions Industrial Informatics, 14: 3690-3700.

Lu, Q. and X. Xu, 2017. Adaptable blockchain-based systems: a case study for product traceability. IEEE Software, 34: 21-27. DOI: 10.1109/MS.2017.4121227

Novo, O., 2018, Blockchain Meets IoT: An architecture for scalable access management in IoT. IEEE Internet Things J., 5: 1184-1195. DOI: 10.1109/JIOT.2018.2812239

Orman, H., 2018. Blockchain: The Emperors New PKI? IEEE Internet Computing, 22: 23-28. DOI: 10.1109/MIC.2018.022021659

Pahl, C., N. El Ioini, S. Helmer and B. Lee, 2018. An architecture pattern for trusted orchestration in IoT edge clouds. Proceedings of the 3rd International Conference on Fog and Mobile Edge Computing, Apr. 23-26, IEEE Xplore press, Spain, pp: 63-70. DOI: 10.1109/FMEC.2018.8364046

Patel, V., 2018. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health Informatics J. DOI: 10.1177/1460458218769699

Sarıtekin, R.A., E. Karabacak, Z. Durgay and E. Karaarslan, 2018. Blockchain based secure communication application proposal: Cryptouch. Proceedings of the 6th International Symposium on Digital Forensic and Security, Mar. 22-25, IEEE Xplore press, Turkey, pp: 1-4. DOI: 10.1109/ISDFS.2018.8355380

Sharma, P.K., M.Y. Chenand and J.H. Park, 2018. A software defined fog node based distributed blockchain cloud architecture for IoT. IEEE Access, 6: 115-124. DOI: 10.1109/ACCESS.2017.2757955

Sharma, P.K., S. Singh, Y.S. Jeongand and J.H. Park, 2017. Distblocknet: A distributed blockchains-based secure SDN architecture for IOT networks. IEEE Communications Magazine, 55: 78-85. DOI: 10.1109/MCOM.2017.1700041

Sharma, V., I. You, F. Palmieri, D.N.K. Jayakody and J. Li, 2018. Secure and energy-efficient handover in fog networks using blockchain-based DMM. IEEE Communi. Magazine, 56: 22-31. DOI: 10.1109/MCOM.2018.1700863

Singh, M., A. Singh and S. Kim, 2018. Blockchain: A game changer for securing IoT data. Proceedings of the IEEE 4th World Forum on Internet of Things, Feb. 5-8, IEEE Xplore press, Singapore, DOI: 10.1109/WF-IoT.2018.8355182

Toyoda, K., P.T. Mathiopoulos, I. Sasaseand and T. Ohtsuki, 2017. A novel blockchain-based Product Ownership Management System (POMS) for anti-counterfeits in the post supply chain. IEEE Access, 5: 17465-17477. DOI: 10.1109/ACCESS.2017.2720760

Valtanen, K., J. Backmanand and S. Yrjölä, 2018. Creating value through blockchain powered resource configurations: Analysis of 5G network slice brokering case. Proceedings of the Wireless Communications and Networking Conference Workshops, Apr. 15-18, IEEE Xplore press, Spain, pp: 185-190. DOI: 10.1109/WCNCW.2018.8368983

Wang, J., M. Li, Y. He, H. Li and K. Xiao *et al*., 2018. A blockchain based privacy-preserving incentive mechanism in crowdsensing applications. IEEE Access, 6: 17545-17556. DOI: 10.1109/ACCESS.2018.2805837

Wu, H., Z. Li, B. King, Z. Ben Miled and J. Wassickand *et al*., 2017. A distributed ledger for supply chain physical distribution visibility. Information, 8: 137. DOI: 10.3390/info8040137

Xia, Q., E.B. Sifah, K.O. Asamoah, J. Gao and X. Duand, 2017. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access, 5: 14757-14767. DOI: 10.1109/ACCESS.2017.2730843

Xu, C., K. Wangand and M. Guo, 2017. Intelligent resource management in blockchain-based cloud datacenters. IEEE Cloud Computing, 4: 50-59. DOI: 10.1109/MCC.2018.1081060

Yang, C., X. Chen and Y. Xiang, 2018. Blockchain-based publicly verifiable data deletion scheme for cloud storage. J. Network Computer Applications, 103: 185-193. DOI: 10.1016/j.jnca.2017.11.011

Zhang, J., N. Xue and X. Huang, 2016. A secure system for pervasive social network-based healthcare. IEEE Access, 4: 9239-9250. DOI: 10.1109/ACCESS.2016.2645904

Zou, J., B. Ye, L. Qu, Y. Wang, M. A. Orgunand L. Li, 2018. a proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services. IEEE Trans. Services Computing. DOI: 10.1109/TSC.2018.2823705