Blockchain-based Reputation System in Agri-Food Supply Chain

Conference Paper · February 2020

CITATIONS
3

READS
294

6 authors, including:

Umair Sarfraz
5 PUBLICATIONS **8** CITATIONS
SEE PROFILE

Muhammad Waseem Malik
COMSATS University Islamabad
2 PUBLICATIONS **3** CITATIONS
SEE PROFILE

Muhammad Sohaib Iftikhar
COMSATS University Islamabad
8 PUBLICATIONS **4** CITATIONS
SEE PROFILE

Nadeem Javaid
COMSATS University Islamabad
1,302 PUBLICATIONS **11,236** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Load and Price Forecasting in Smart Grid View project

Balancing energy consumption in UASNs View project

Blockchain-based Reputation System in Agri-Food Supply Chain

Affaf Shahid, Umair Sarfraz, Muhammad Waseem Malik, Muhammad Sohaib Iftikhar, Abid Jamal, and Nadeem Javaid

Abstract Supply chains are evolving into automated and highly complex networks and are becoming an important source of potential benefits in the modern world. However, it is challenging to track the provenance of data and maintain traceability throughout the network. The traditional supply chains are centralized and dependent on third party for trading. Centralized systems lack transparency, accountability and auditability. In our proposed solution, we have presented a blockchain-based reputation system in Agriculture and Food (Agri-Food) supply chain. It leverages the key features of blockchain and smart contract deployed over ethereum blockchain network. Although blockchain provides an immutable network for supply chain events, it still fails to solve the problem of trust among entities. Therefore, a reputation system is required that logs reviews of sellers and maintains the trust between trading entities.

1 Introduction

The supply chain management is a group of processes and sub processes involved in supply chain activities. The supply chain activities involve the flow of goods and services to transform a raw material into a final product. It is also interpreted as a network of entities that are part of the system from production till trading. The network is divided into several stages and span upto months while completing the entire process. In such scenario , if the final product lacks in quality, it becomes difficult to track the root cause of the problem [1]. With the increasing demands of end consumers and their keen interest in the provenance of data, it has become

Affaf Shahid, Umair Sarfraz, Muhammad Waseem Malik, Muhammad Sohaib Iftikhar, Abid Jamal, and Nadeem Javaid (Corresponding Author),
COMSATS University Islamabad, Islamabad 44000, Pakistan; email: nadeem-javaidqau@gmail.com

fundamental part of Agri-Food supply chains to track the movement of products from origin to the end consumers.

For the purpose of gaining end consumers trust, the supply chain authorities have to be quick and accurate in responding. It is also important for supply chain authorities to comply towards quality, integrity and credibility of the entire process. Several solutions are proposed to track the provenance of data. While, several countries like Canada and China have already started to work on the law and regulations. Canada has enforced the use of tags and bar codes to identify the provenance of the product. China has also proposed solutions to track the entire process [2]. These application, enforce to improve the traceability schemes in order to achieve quality, transparency, credibility and security.

The supply chain networks also perform the trading of the products between different entities. These networks work in a centralized manner and involve third party to complete the trading process. The centralized systems result in the falsification of information. Therefore, the information between Agri-Food supply chain entities is inconsistent. The third parties for the trading process also lack credibility and trustfulness while performing transactions.

The emergence of blockchain as a base technology of Bitcoin is recognized by several industries around the globe, e.g., finance, Electronic Medical Records (EMRs) [3], Internet of Things (IoT) [4], [5], [6], energy [7] and many more. Blockchain is a secure by design system that can overcome aforementioned risks through its features like immutability, transparency, traceability and security. Bitcoin, the decentralized peer-to-peer digital currency is the most popular application that is based on blockchain technology [8]. However, the current Bitcoin network is not a one-size-fit all solution, especially for data-driven domains as it faces latency, storage and throughput issues [9]. Several network architectures and distributed consensus protocols that keep the integrity of a blockchain while enabling high throughput and improved storage capabilities have been explored. Similarly, an efficient monitoring of production of Agri-Food products is critical in terms of product safety. The growing concerns of consumers and government regarding food quality has also renewed the concept of traceability in supply-chain. The traditional supply-chains suffer with centralization and become vulnerable both in terms of management and data modification. However, blockchain plays a significant role in evolution of supply chain with its inherent properties. Moreover, it also provides smart contracts leveraging safe trading transactions among systems. Despite of the trust less nature of blockchain-based Agri-Food chains, it is hard for the end-consumers to trust the product owner and quality of the product before performing a transaction.

Additionally, the traditional centralized storage schemes are unable to handle large amount of data produced during supply chain processes and consequently cause bottleneck. Therefore, several decentralized storage schemes are proposed in literature to overcome the issues like high latency, low throughput and bottlenecks. In paper [10] a blockchain-based soybean traceability scheme is proposed. The solution uses ethereum smart contracts and Interplanetary File Storage System (IPFS)

to achieve complete traceability. The storage medium is IPFS [1]. IPFS uses the technologies like an incentivized block exchange and Distributed Hash Table (DHT). In IPFS, nodes do not trust each other and there is no single point of failure. However, the data stored in IPFS gets available if the hash of the data is available. IPFS nodes also act selfishly while backing up data. While, authors in [11] have proposed an efficient storage scheme for Agri-Food tracking. The transaction hash in the proposed solution is stored in a secondary database. To retrieve data from IPFS, the transaction hash is accessed from secondary database. Using that transaction hash, IPFS hash is retrieved from the blockchain. However, if the secondary database fails, whole system will fail. Similarly, Paper [12] has proposed an auditable protocol for transparent, tamper-proof and verifiable transactions between trading entities. The trading entities are Merchant, Logistics Company and Consumers. However, authors have not considered credibility of merchants and trust between trading entities. Therefore, to overcome aforementioned issues, our paper aims to contribute in the growing work on blockchain-based Agri-Food supply chains. The proposed solution uses ethereum smart contracts to assure an efficient, secure and trsuted environment for the trading entities. It maintains the integrity and immutability of the reviews registered through smart contract. It also provides a detailed performance analysis of the proposed scheme in terms of gas required.

1.1 Related Work

In this section, the work done in existing literature is summarized based on problems and respective solutions proposed. In paper [13], authors proposed a blockchain-based Agri-Food supply chain system. It uses a systematic preventive approach for food safety i.e., Hazard Analysis and Critical Control Points (HACCP). They discussed the pros and cons of using RFID tags and Agri-Food supply chain traceability. In traditional storage schemes, the data is stored in centralized storage. After the invention of blockchain many decentralized storage systems are used to store the data in a decentralized manner. Paper [11] proposed an efficient storage scheme for Agri-Food product tacking. Authors used IPFS along with secondary database to achieve the traceability.IPFS is a network used to store and share data in a decentralized file system. To retrieve data from IPFS, the transaction hash is accessed from secondary database. Using that transaction hash, IPFS hash is retrieved from the blockchain. However, if the secondary database fails, whole system will fail. Authors in [10], proposed an approach for efficient transactions of soybean traceability in Agri-Food supply chain. The proposed solution overcomes the problems of centralized solutions and eliminates the need for a trusted third party. It maintains high integrity, reliability and more security. However, authors have not considered the accountability and auditability of the data delivered and automated payments. While, it has also not tackled ”dispute” in case of failed trading transactions. Paper

[1] A popular, decentralized, peer-to-peer file storage system

[14] has proposed a proof of delivery mechanism to deliver physical assets between multiple transporters. In the proposed solution, all the entities are act honestly by incentivizing the trading entities. Automated payments through ethers are also the part of proposed solution. However, the proposed scheme has used a key and asset while transporting the asset. The key and the asset delivered have no relation between them and as a result, transporters can easily tamper the asset to be delivered. Paper [12] has proposed an auditable protocol for transparent, tamper-proof and verifiable transactions between entities. It has also proposed a pre-verification technique to overcome the limitation in paper [14] However, credibility of merchants is not considered. In [15], a decentralized storage mechanism along with ethereum blockchain is proposed. The paper aims at overcoming the risks of centralized storage, i.e., leakage of the sensitive data and a single point of failure. The decentralized storage mechanism used is IPFS. In the proposed framework, before storing the data in IPFS, the file is encrypted using a file encryption algorithm. The ciphertext obtained after encryption is uploaded to IPFS. IPFS provides the hash of the stored file which is recorded in ethereum blockchain. However, the proposed solution if

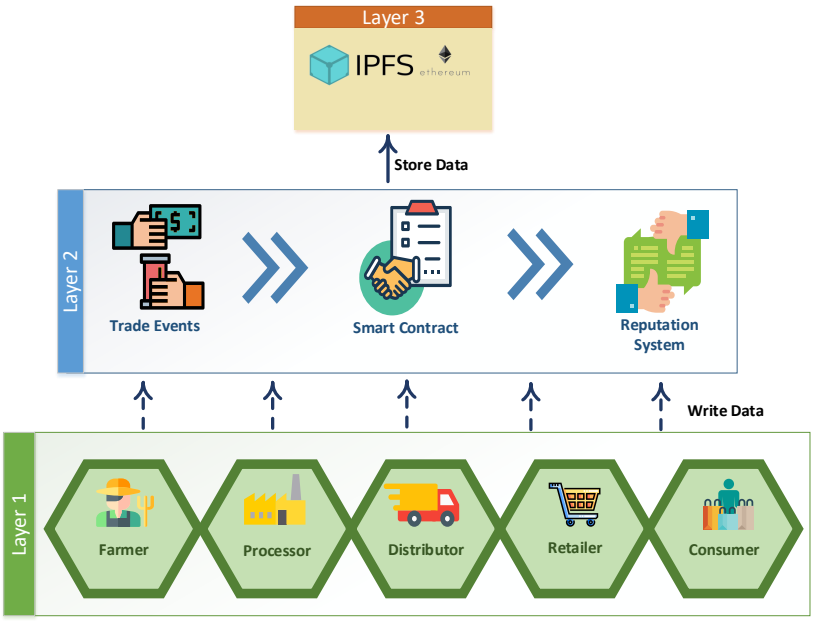

Fig. 1: System Model

applied in IoT scenario, will not work efficiently because of the increased computational overhead.

The authors in [16] have proposed an approach for trustless privacy preserving reputation system. The proposed solution maintains the anonymous ratings of products and provides the correctness and security analysis of the proposed scheme. However, no performance analysis is provided that is required to guarantee efficiency of token generation. Additionally, there is no link between the ratings and the transactions and are consequently prone to malicious users. Paper [17] has discussed the existing and proposed solutions that work on maintaining trust and reputation while performing online transactions. The authors have then proposed an agenda for reputation systems. Every online transactional platform has the problem of truthfulness between the seller and buyer. This is for the reason that the both parties do not directly meet to perform the transaction. Therefore, a review system is required that maintains the sellers reviews against his profile and helps buyers to evaluate the seller and products beforehand. A blockchain-based reputation system is proposed in paper [18]. The proposed solution provides data credibility in the vehicular networks. Each message that is transfered from one entity to another is reviewed on the basis of environment traffic. Each review is then blocked and chained in the network. Based on these reviews, the vehicles are able to trust the messages obtained. However, the credibility of the entities that transfer messages is not maintained.

2 System Model

In this section, we describe our proposed solution. To achieve complete traceability and trust in supply chain management of Agri-Food chains, our proposed model consists of three layers. The first layer is comprised of supply-chain entities involved in Agri-Food chain. The trading events produced from first layer are written on second layer and are then recorded on the blockchain. At the second layer, the transactions from the first layer are stored in a ledger. and it only keeps the hashes of data in order to increase storage space. These transactions are processed by strict access control strategies that define the rules who can access or write data to IPFS. A reputation system is also part of the second layer. This reputation system is responsible for invoking smart contracts to provide service based reviews to the providers. Once the transaction is completed, the buyers register reviews which are also stored on IPFS. For the next transaction, the buyers request reviews of sellers and perform transactions on the basis of those reviews. The reputation system provides the trust values to the sellers in order to increase the trust among trading entities. The trust values are the quality ratings of the services provided by the sellers. These trust values are stored against the digital profiles of trading entities in blockchain based supply-chain. The last layer is storage layer that stores the data from layer two and leverages the blockchain system with high throughput, low latency and scalability.

The first layer consists of multiple supply-chain entities that interact through smart contract with specific roles and permissions. Following are the entities involved:

- **Farmer;** Farmer is the first entity in Agri-Food supply chain and is the first one to invoke smart contract for trading. Farmers produce large amount of crops and take the responsibility for assuring and monitoring the crop growth details. IoT devices in the farms are responsible for gathering images and videos of the seed's health, crop growth details and saving it on IPFS. Blockchain stores the hashes of data stored in IPFS.
- **Processor;** Processor buys the crops from farmers and is responsible for selling a finalized product to distributors. The processor also maintains and monitors temperature, storage and moisture of crops while eliminating the extra material and converting it to a finalized product.
- **Distributor;** Distributor maintains a warehouse by buying finalized products from processors and is responsible for selling it to the retailers.
- **Retailer;** Retailer is responsible for buying the finished traceable products from distributors and selling it to customers in smaller quantities. Traceable product refers to specific identifiers of the goods that allow tracking the provenance data.
- **Consumer;** Consumer is an end user who buys and consumes the products from retailers.

Moreover, to ensure traceability, each entity in the supply chain will be identified by a unique key. Similarly, the product traceability is achieved by unique identifiers of the products per lot. In order to achieve complete traceability, we record the trading transaction from initiation, add the product ID and lot ID to each succeeding transaction and record the hashes to maintain hash chain.The transactional data is stored in IPFS. While, the hashes to the data are recorded as metadata in ethereum blockchain in order to overcome the limitation of IPFS. In order to write or access transactions from IPFS, access control list is maintained. Hence ensures the privacy and confidentiality in the network.

A reputation system as shown in figure 2 is introduced in layer two of the proposed model. The reputation system is responsible for assuring the credibility of product owner and the asset delivered. It maintains the immutability and integrity of the reviewed registered in the system. In contrast to the traditional reputation systems, the reviews are recorded in IPFS while its hash is stored in blockchain. In this way, immutability and integrity of reviews are maintained. Reputation system is triggered while the trade events occur between the buyers and sellers.

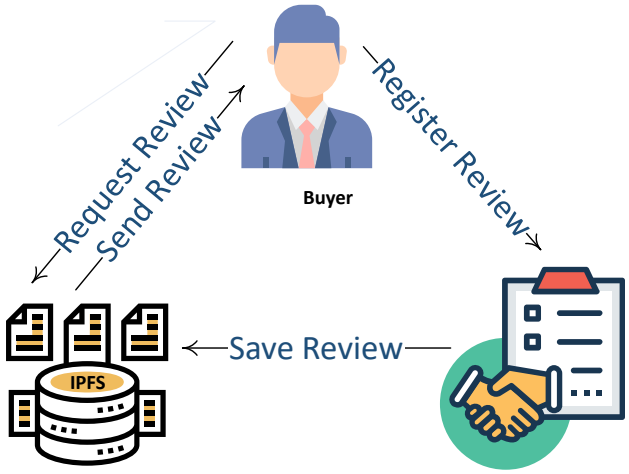

Fig. 2: Reputation System

The purpose of this system is to ensure trust among the trading entities and make sure that the buyer knows the reputation before purchasing the data from seller. Whenever the entities sign a smart contract for trading, smart contract for reputation is also triggered that provides the reviews of available data sellers. Once the trading is successfully performed, the buyer also registers review for the seller on the basis of the goods received. The review registered by the buyer is then stored against the seller profile in blockchain system. The smart contract as shown in Figure 2 consists of four functions, i.e., RegisterReview(), SearchRatings(), SearchReview and IsReviewExist(). The four functions are responsible for checking whether a review already exists,checking its content and ratings and registering a review. The registering function takes metadata, ratings of the asset and review details as input. These values are then used by the end consumers to evaluate the quality of the product and reputation of the product owner. Functions for searching a review and ratings, i.e., SearchReview(), SearchRatings()are used to get the existing ratings and review details of a seller.

3 Simulation and Results

In this section, we will discuss the simulation tools and performance results of the proposed system. For the simulations purpose, an open-source platform for blockchain, i.e. Ethereum is used. Ethereum uses blockchain technology to develop decentralized applications. It enables users to make smart contracts to make agreements, without any third party involvement. To assess the performance of blockchain-based supply-chain network, we have used Remix Integrated Development Environment (IDE), Ganache and Metamask. Remix facilitates in writing, exe-

cuting and testing a smart contract. The language used for writing a smart contract in remix is Solidity. Whereas, Ganache provides the virtual accounts with pre-defined amount of crypto-currency. After each transaction, the crypto-currency is deducted from the account that performed transaction. Each account in Ganache has its own private key and unique address. However, Metamask is an extension in browser that acts as bridge between Ganache and Remix IDE and helps them connect.

The specifications of the system are: intel core i5, 2.4 GHz processor, 8 GB RAM and 500 GB storage. The performance parameters used to evaluate proposed solution's performance are as follows:

- Transaction and execution cost of smart contracts.
- Total amount of gas consumed for different input strings length in review system.
- Mining time for different input strings length in reputation system.

The detailed gas consumption of contracts and their functions are described below. In figure 3, the gas consumption of reputation system smart contract is shown. The reputation system consists of four functions, i.e., RegisterReview(), SearchRatings(), SearchReview() and IsReviewExist(). It is clearly visible from the graph that RegisterReview() function takes the maximum execution and transaction gas as compared to the other functions. This is because the RegisterReview() function is responsible for saving the reviews against the user's profile in blockchain and perform more logically complex operations. Therefore, the transactional costs for other functions are relatively less. The execution cost depends on computational complexity of the transactions as they are carried out. While the transaction cost is the combination of execution cost and the cost of sending smart contract code to the ethereum blockchain.

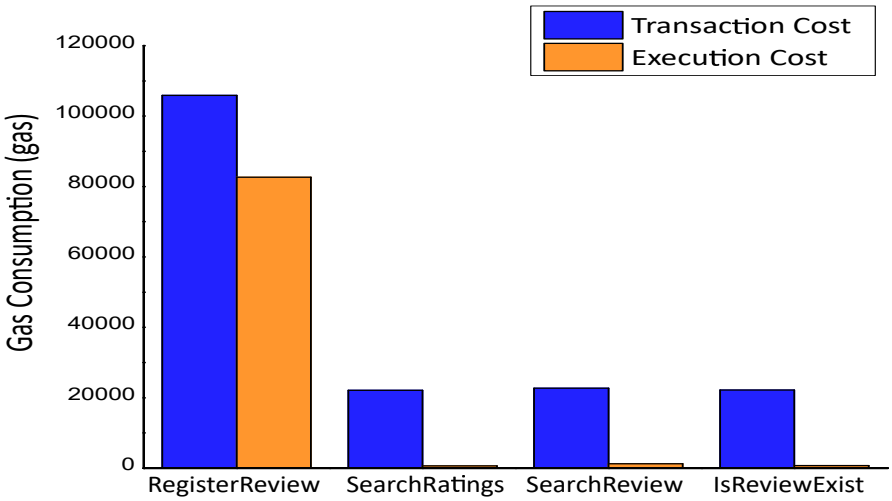

Fig. 3: Gas Consumption of Review System

Figure 3 below shows the gas consumption against the length of input string provided for each review. By plotting the graph for different lengths of input strings, we have concluded that the relation between gas consumption and length of input string is directly proportional, i.e., by increasing the length of an input string, the consumption of the respective sting also increases. Therefore, we can say that longer reviews will cost more as compared to the shorter ones.

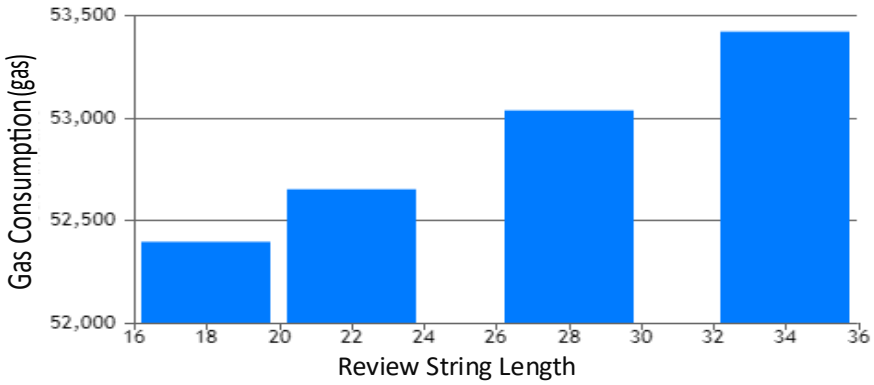

Fig. 4: Gas Consumption against Input String Length

In order to compare the mining time of reviews against the input string length, we plotted a graph as shown in figure 4. The input values provided in the reputation system are processed as strings. We provided the input values of different lengths and investigated its effect over the mining time for each string. It was observed that the mining time for input was totally different and concluded that the different lengths of input strings does not effect the mining time. However, the mining time of transaction is dependent of the transactional conditions in a network. Miners in a network are responsible for calculating a nonce that must be less than a target value. Hence, if the target value has more difficulty level, mining will also increase and vice versa.

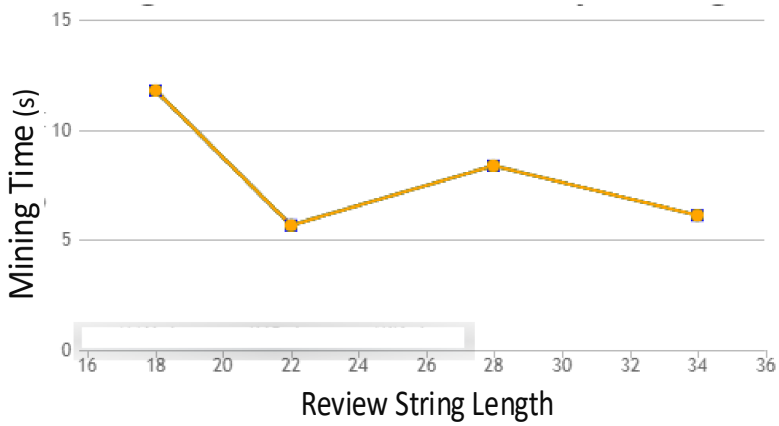

Fig. 5: Mining Time against Different Input Length

4 Conclusion

It is no harm to say that online business transactions whether in IoT, e-commerce, vehicular networks, supply chains, etc. are increasing with the growing days. Therefore, a plenty of solutions are being transferred from centralized to decentralized peer to peer networks. Blockchain, since its evolution, is helping several industries to maintain a peer-to-peer decentralized network and keep up with the technological advancements like secure transaction, immutability, integrity, transparency and traceability. In this regard, supply chain industry has gained numerous benefits to grow, move towards decentralization and achieve a trustless environment. However, despite the trustless nature of blockchain, it is hard to fully maintain trust between the merchandiser and buyer of the product. This is because the entities do not perform their business in real and buyer doubts the credibility of the merchandiser. In this paper, we have proposed a blockchain-based reputation system in Agri-Food supply chain. The system is proposed to maintain the credibility of the trading entities and quality ratings of the products. Moreover, it also maintains the immutability and integrity of the registered review as they are based on blockchain. Blockchain makes it impossible for the network entities to delete or modify a review. We have also provided detailed discussion and simulation results. The results show that our system requires certain amount of waiting time to mine the transaction. However, the waiting time is independent of the input length of reviews.

References

1. Galvez, Juan F., J. C. Mejuto, and J. Simal-Gandara. "Future challenges on the use of blockchain for food traceability analysis." TrAC Trends in Analytical Chemistry 107 (2018): 222-232.
2. Tripoli, Mischa, and Josef Schmidhuber. "Emerging Opportunities for the Application of Blockchain in the Agri-food Industry." FAO and ICTSD: Rome and Geneva. Licence: CC BY-NC-SA 3 (2018).
3. Muqaddas Naz, Fahad A. Al-zahrani, Rabiya Khalid, Nadeem Javaid, Ali Mustafa Qamar, Muhammad Khalil Afzal, and Muhammad Shafiq. "A Secure Data Sharing Platform Using Blockchain and Interplanetary File System." Sustainability 11, no. 24 (2019): 7054.
4. Mubariz Rehman, Nadeem Javaid, Muhammad Awais, Muhammad Imran, and Nidal Naseer. "Cloud based secure service providing for IoTs using blockchain." In IEEE Global Communications Conference (GLOBCOM 2019). 2019.
5. Tanzeela Sultana, Ahmad Almogren, Mariam Akbar, Mansour Zuair, Ibrar Ullah, and Nadeem Javaid. "Data Sharing System Integrating Access Control Mechanism using Blockchain-Based Smart Contracts for IoT Devices." Applied Sciences 10, no. 2 (2020): 488.
6. Turki Ali Alghamdi, Ishtiaq Ali, Nadeem Javaid, and Muhammad Shafiq. "Secure Service Provisioning Scheme for Lightweight IoT Devices with a Fair Payment System and an Incentive Mechanism based on Blockchain." IEEE Access (2019).
7. Omaji Samuel, Nadeem Javaid, Muhammad Awais, Zeeshan Ahmed, Muhammad Imran, and Mohsen Guizani. "A blockchain model for fair data sharing in deregulated smart grids." In IEEE Global Communications Conference (GLOBCOM 2019). 2019.
8. Chuen, David Lee Kuo, ed. "Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data." Academic Press, 2015.
9. Andoni, Merlinda, Valentin Robu, David Flynn, Simone Abram, Dale Geach, David Jenkins, Peter McCallum, and Andrew Peacock. "Blockchain technology in the energy sector: A systematic review of challenges and opportunities." Renewable and Sustainable Energy Reviews 100 (2019): 143-174.
10. Salah, K. H. A. L. E. D., N. I. S. H. A. R. A. Nizamuddin, R. A. J. A. Jayaraman, and M. O. H. A. M. M. A. D. Omar. "Blockchain-based Soybean Traceability in Agricultural Supply Chain." IEEE Access (2019).
11. Hao, JinTao, Yan Sun, and Hong Luo. "A Safe and Efficient Storage Scheme Based on BlockChain and IPFS for Agricultural Products Tracking." Journal of Computers 29, no. 6 (2018): 158-167.
12. Wang, Shangping, Xixi Tang, Yaling Zhang, and Juanjuan Chen. "Auditable Protocols for Fair Payment and Physical Asset Delivery Based on Smart Contracts." IEEE Access 7 (2019): 109439-109453.
13. Tian, Feng. "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things." In 2017 International Conference on Service Systems and Service Management, pp. 1-6. IEEE, 2017.
14. Hasan, Haya R., and Khaled Salah. "Blockchain-based proof of delivery of physical assets with single and multiple transporters." IEEE Access 6 (2018): 46781-46793.
15. Wang, Shangping, Yinglong Zhang, and Yaling Zhang. "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems." IEEE Access 6 (2018): 38437-38450.
16. Schaub, Alexander, Rémi Bazin, Omar Hasan, and Lionel Brunie. "A trustless privacy-preserving reputation system." In IFIP International Conference on ICT Systems Security and Privacy Protection, pp. 398-411. Springer, Cham, 2016.
17. Jøsang, Audun, Roslan Ismail, and Colin Boyd. "A survey of trust and reputation systems for online service provision." Decision support systems 43, no. 2 (2007): 618-644.
18. Yang, Zhe, Kan Zheng, Kan Yang, and Victor CM Leung. "A blockchain-based reputation system for data credibility assessment in vehicular networks." In 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC), pp. 1-5. IEEE, 2017.