Adoption of blockchain technology improving supply chain management system in small and medium cyber security enterprises

Lee Chen, Lixuan Zhang, Chang Li, Zheng Xiang
Faculty of Computer Science and Information System, Universiti Teknologi MARA (UiTM), Malaysia

ABSTRACT

Blockchain technology has been known as a digital currency platform since the emergence of Bitcoin, the first and the largest of the cryptocurrencies. Hitherto, it is used for the decentralization of markets more generally, not exclusively for the decentralization of money and payments. The decentralized transaction ledger of blockchain could be employed to register, confirm, and send all kinds of contracts to other parties in the network. In this paper, we thoroughly review state-of-the- art blockchain-related applications emerged in the literature. A number of published works were carefully included based on their contributions to the blockchain's body of knowledge. Several remarks are explored and discussed in the last section of the paper.

KEYWORDS: blockchain; adoption; cryptocurrency; review; applications

1.0 INTRODUCTION

A software system can be characterized into two main architectural approaches, i.e. centralized and distributed. In centralized software system, the nodes are located around and connected with one central node of coordination. Distributed system, on the contrary, have several connected nodes without any central node of control. Fig. 1 illustrates the contrast of these two architectures [1-9]. There are several benefits of a distributed system, i.e. having more computing power by combining the computing power of all connected nodes, an increased reliability due to the fact that it does not have a single of failure, and so forth. However, several drawbacks of a distributed system include communication overhead and security issues which is related to misuse network access by untrustworthy nodes [10-19]. Meanwhile, blockchain can be seen as a part of the imple- mentation layer of a distributed software system. The data integrity in distributed systems can be achieved and main- tained using blockchain. Furthermore, blockchain could be also considered as a purely peer-to-peer system which is made up of the individual nodes in a network. Dishonest and malicious peers become the crucial integrity threat in peer-to-peer systems. The individual nodes try to exploit the system for their own purposes since unknown peers with unknown reliability and trustworthiness may exist. Thus, these critical problems are needed to be solved by blockchain [20-28]. Along with blockchain, Bitcoin was originally invented by Nakamoto as the first and most prevalent cryptocurrency. It enables trustless and reliable transaction where a centralized management is not required though the users do not trust each other or there are unreliable users in the network. Since then, blockchain has drawn a lot of attention to the decentralized transaction ledger functionality which could be used to register, confirm, and send the payment or contracts [29-34]. Furthermore, blockchain technology has been applied beyond financial transactions, to any kind of transaction and applica- tions, i.e. healthcare, utilities, real estate, and the government sector. These are found to be feasible as the blockchain structure develop for Bitcoin is portable and extensible. Originally, the main area for blockchain is connecting cryp- tocurrencies with conventional banking and financial institu- tions. Blockchain technology offers a novel banking ecosystem thus enabling financial institutions to conduct their financial transactions directly between themselves without any cen- tral authorities or intermediaries. Every transaction must be authenticated through the agreement of more than half of those participating in the network [34-42]. This means that no participants would be able to modify any data within the blockchain without the approval of other participants. The objective of this paper is to provide and explore insight into blockchain technology and its current practical applications. The paper thoroughly classifies the published works found in the literature, i.e. academic journals, conferences, technical reports, and so on. Regarding the review studies about blockchain technology, several works have been conducted [43-49]. However, most studies have not considered a comprehensive discussion

about blockchain-related applications. The rest of the paper is structured as follows. Section II presents an overview of blockchain technology, whilst Section III describes in detail about the practical facets of blockchain. Several remarks and an in-depth discussion are given in Section IV, and finally some concluding remarks are drawn in Section V.

2.0 LITERATURE REVIEW

Blockchain is a type of distributed ledger (data structure) which contains information about transactions or events. It is replicated and shared among the participants in the network [1-14]. The size of chain unceasingly increases since blocks are added and chained to the previous block using a hash function (see Figure 2 for further illustration of the Bitcoin's blockchain as an example). A cryptographic hash function is used to produce a hash. For instance, Bitcoin uses SHA-256, whilst Litecoin and Primecoin use Scrypt and Cunningham chain, respectively. In addition, it enables us to simply verify the input mapping to a given hash value [15-27]. It would not be feasible for two different inputs having the same hash. The ledger in the blockchain is validated and preserved by a network node (user) in pursuance of consensus mechanism (a collection of rules that allow users to reach a mutual agreement) thereby a central authority or intermediary is not required. Each node keeps a complete replica of the entire ledger. As the first aim of blockchain is to solve the problems exist in Bitcoin cryptocurrency, Section III discusses in detail the practical implementation of the blockchain for financial transaction [28-33].

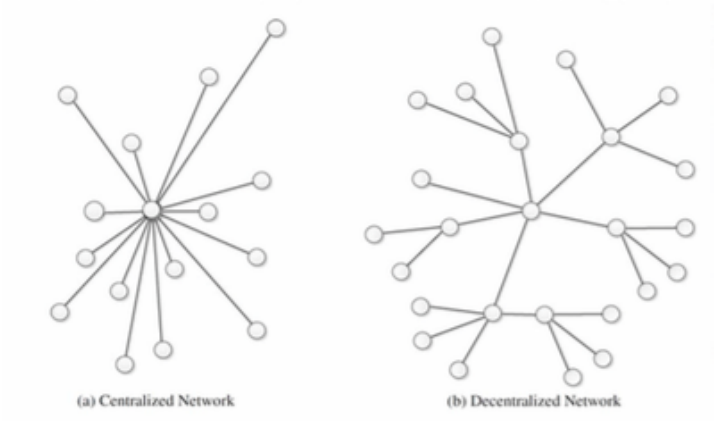

Fig. 1. Centralized and distributed network architecture

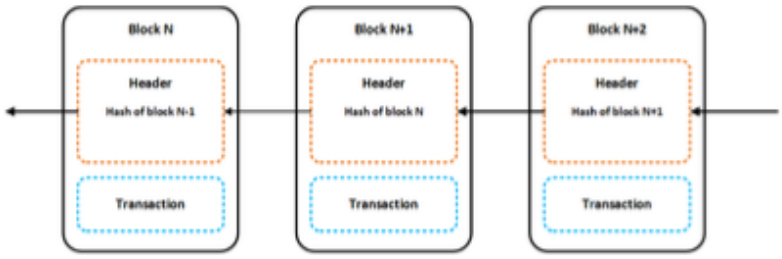

Fig. 2. A chain of blocks - blockchain in the Bitcoin

3.0 METHODOLOGY & RESULT

In this section, the implementation of blockchain technology in different areas are thoroughly discussed. Furthermore, such applications have been categorized into several groups, i.e. financial services, healthcare, business and industry, and other novel applications [1-17].

A. Financial Service

Blockchain has been widely applied for financial transaction which is so-called cryptocurrency. Nowadays, cryptocurrencies have appeared as prominent software systems. Recalling the above-mentioned of Fig. 2, the first block or genesis block (is not appeared in the figure) contains the first transaction. The hash of the first block is forwarded to the miner, who employs it and generates a hash for the second block. In similar fashion, the third block creates a hash that comprises of the first two blocks, and etc. All blocks in the blockchain can be traced back to the genesis block. Cryptocurrency has its own currency (coin). Mining is the process of introducing a new block into blockchain. Each node uses blockchain to verify whether the coin is legitimate or if it has not spent already. Before the transaction records are appended into blockchain, a greater number of participants reach an agreement. Mining process is a resource-intensive task, thus makes it tough for an attacker to validate an invalid transaction. Each mined-block is verified to see if it has whether a valid proof of work or a proof of stake. The followings are the prevalent steps in cryptocurrency: (i) a generated address (public key) is available for a user who has a wallet, (ii) a private key is assigned to the wallet. It is used to sign transaction and proving ownership, (iii) the payer sends coin to the payee using given address and sign it using payer's private key, and finally (iv) the transaction is validated via min- ing process. Eleven cryptocurrency sytems are included in our study, i.e. Bitcoin, Litecoin, Peercoin, Primecoin, Ripple, Ethereum, Permacoin, Blackcoin, Auroracoin, Darkcoin, and Namecoin. Ta- ble I summarizes the afore-mentioned cryptocurrency systems which is presented in chronological order of occurrence.

TABLE I
THE CURRENT EXISTING CRYPTOCURRENCY SYSTEMS

Cryptocurreny	Year	Hash Function	Mining Method
Bitcoin [4]	2008	SHA-256	Find all possible nonce values by computing proof of work and other users agree and verify the proof.
Litecoin [11]	2011	Scrypt	Similar to Bitcoin (proof of work)
Peercoin [17]	2012	SHA-256d	proof of work and proof of stake
Primecoin [12]	2013	Cunningham chain	proof of work
Ripple [18]	2014	EC digital signature	consensus system
Ethereum [19]	2014	Ethash	proof of work
Permacoin [20]	2014	Floating digital signature	proof of retreivability
Blackcoin [21]	2014	Scrypt	proof of stake
Auroracoin [22]	2014	Scrypt	proof of work
Darkcoin [23]	2014	X11	proof of work
Namecoin [24]	2015	SHA-256d	proof of work

B. Healthcare

Blockchain has a tremendous potential in addressing the in- teroperability issues exist in the current healtcare systems. It can be used as a standard which allows the stakeholders, i.e. healthcare entities, medical researcher, etc to share electronic health record (EHR) in a secure manner. Sharing of EHR enables us to improve the quality of medical care and enhance the recommendation for doctors, for instance. However, managing healthcare data, i.e. acquiring, storing, and analyzing is not a simple task, particularly in case of privacy issues. Healthcare data should not be revealed to other parties which it might be vulnerable to be used fraudulently by malicious users or attackers. In order to get the better of those issues, a healthcare data gateway (HDG) based on the blockchain storage platform is proposed. It

is a smartphone application which can be used to manage and control the data sharing easily. The proposed system enables users to process the patient data without exposing patient privacy. Furthermore, a private blockchain cloud is used to stored the data thus ensuring the medical data can not be altered by anybody, including physicians and patients. The work emphasizes on the designing of a new system to prioritize patient agency, called MedRec. It is a distributed ledger protocol that uses public key cryptography to create blockchain. The blockchain replicas are distributed on each node in the network. Similar to prior work, blockchain technology is used as a access control in order to automate and track certain tasks, i.e. append a new record, change in viewership rights, etc. Furthermore, smart contracts on an Ethereum blockchain is utilized to create intelligent representation of EHR that are stored in each individual node. Subsequently, the application of pervasive social network (PSN) based healthcare using blockchain is proposed. PSN allows us to share medical data acquired by medical sensors. PSN-based healthcare system comprises two main security protocols, i.e. an authentication protocol between medical sensors and mobile devices in wireless body area network (WBAN) and an EHR data sharing using blockchain in PSN area. Each node in the PSN is responsible for gener- ating and broadcasting of medical data transactions, i.e. node address and medical sensors. The miners, on the other hand, are responsible for transaction verification and new block creation. Lastly, a blockchain-based access control mechanism is pro- posed. Access control includes identification, authen- tication, and authorization process. It ascertains a condition of being accountable where user access can be traced for what particular action in a system. The proposed system permits users to access EHR from a shared data pools using blockchain after verifying their identity and cryptographic keys. To achieve user's authentication, an identity based authentication is adopted. In addition, an efficient lightweight block format is proposed to enhance the current implementation of blockchain. Table II compares the related study of blockchain technology for healthcare application.

C. Business and Industry

The emergence of Internet of Things (IoT) has brought many advantages such as delivering an inter- connection be- tween objects and humans. This motivates authors in to propose an e-business architecture which is particularly developed for IoT environment. For this purpose, distributed autonomous corporation (DAC) is adopted as an entity that gives transaction services in the absence of human interven- tion. The core of the proposed system is a transaction mode in which peer to peer transaction is performed autonomously, whilst Bitcoin and IoTcoin are adopted as the currency and exchange certificate, respectively. The authors consider the importance of food safety and quality when proposing a agri-food supply chain traceability system using RFID and blockchain technology. Blockchain is adopted for ensuring the shared and published information is reliable and valid. Furthermore, a term 'smart manufacturing' in the era of Industry 4.0 is also extensively discussed. Industry 4.0 denotes the flexibility of products and services to be shared over the Internet or other networks, i.e. blockchain. With regard to the supply chain management, Industry 4.0 is expected to attain the circumstance of decen- tralization and self-regulation. To date, an extension of cloud computing which is so-called fog computing or edge computing, has been attracted authors to develop a fair payment system based on Bitcoin. Fog computing can be regarded as a large-scale, ubiquitous, and decentralized system which processes any computing tasks. The proposed system is established to improve the traditional e-cash system which needs a trusted authority, i.e. bank to generate payment token. By employing the Bitcoin-based payment, the fog users (outsourcers) can directly make a transaction to the fog nodes (workers) without involving third party. The authors argue that the proposed system can assure a payment for any completed tasks performed by honest workers regardless of the outsourcers is malicious or not.

TABLE II
THE CURRENT EXISTING BLOCKCHAIN FOR HEALTHCARE

Study	Year	Hash Function	Mining Method
HDG [29]	2016	NA	NA
MedRec [30]	2016	Ethash	proof of work
PSN [31]	2016	NA	NA
BBDS [32]	2017	SHA-256	proof of work

D. Other Implementations

In this section, the current implementation of blockchain in many areas such as right management system, reputation sys- tem, digital content distribution system, WiFi authentication and IoT security are discussed. The two papers present and discuss a new concept of decentralized right management system by using blockchain technology (BRIGHT). It is entirely different with the tradi- tional approach in which a central third-party is commonly taken into account. The proposed system is expected to have a strong mechanism against attack and it enables us to lower user's service fees. In addition, a reputation system is great potential to measure the trust valuation of us in the commu- nity. It is measured based on our previous transactions and interactions in such network, i.e. e-commerce website. By involving blockchain in the reputation system, it can solve the major issues exist in the current reputation system, i.e. freeloaders.

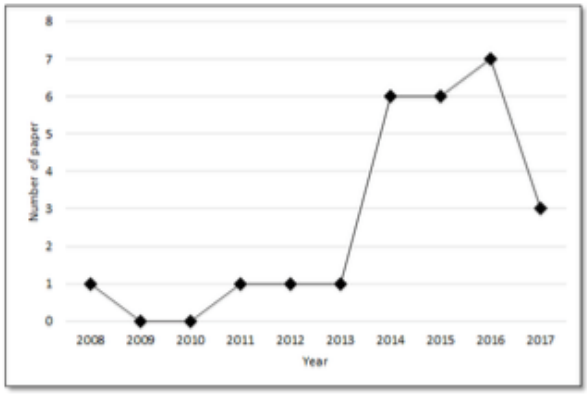

Fig. 3. Paper distribution by year

A new authentication protocol for WiFi is proposed. This is based on Bitcoin 2.0 which is an alternative cash system derived from Bitcoin. At first, users have to install an application called Auth-Wallet then the tokens called Auth-Coins are issued. Users and access points exchange the tokens for authentication. At last, the implementation of blockchain for smart home security is described. In order to provide secure access control to the IoT devices, a private and local blockchain is utilized. In addition to allowing a lightweight security mechanism for smart home devices, the blockchain also generates an immutable time-ordered of transactions. Also, smart home miner is considered to be a device that centrally processes transactions in the smart home.

4.0 CONCLUSION

Twenty-six research papers which are related with blockchain applications were thoroughly discussed. The papers were carefully chosen from the online database, i.e. Google Scholar in terms of their practical implementation. The lit- erature were searched using a keyword 'blockchain' which yielded about 9,840 results, and finally 26 papers were consid- ered for classification. Fig. 3 depicts distribution of papers by year of publication. It is obvious that the number of blockchain technology-related papers have increased significantly since it firstly appeared in 2008. It is also worth mentioned that blockchain has fascinated researchers as this technological innovation brings the possibility of cooperatively produce and maintain transactions (distributed ledger) in the network. There are tremendous advantages of blockchain such as speed, robustness, openness, and so forth. Before the trans- action is appended into blockchain, all participants in the network have to reach an agreement. However, blockchain is not an universal cure for all problems and there are several issues that have been identified such as financial transaction for criminal activities, legal aspects, and other economic risks. Blockchain become one of the promising technology in the future if well exploited. The state-of-the-art research papers which are related with blockchain technology have been reviewed and discussed. A number of papers were comprehensively chosen from the online database then they were classified into several different areas. This paper offers an understanding of the current blockchain research and its real-world implementations.

REFERENCES

[1] Wong, Lai-Wan, et al. "Unearthing the determinants of Blockchain adoption in supply chain management." International Journal of Production Research 58.7 (2020): 2100-2123.

[2] Hazen, Benjamin T., et al. "Supply chain management for circular economy: conceptual framework and research agenda." The International Journal of Logistics Management 32.2 (2021): 510-537.

[3] Bozorgasl, Zavareh, and Mohammad J. Dehghani. "2-D DOA estimation in wireless location system via sparse representation." In 2014 4th International Conference on Computer and Knowledge Engineering (ICCKE), pp. 86-89. IEEE, 2014.

[4] Craighead, Christopher W., David J. Ketchen Jr, and Jessica L. Darby. "Pandemics and supply chain management research: toward a theoretical toolbox." Decision Sciences 51.4 (2020): 838-866.

[5] Wieland, Andreas. "Dancing the supply chain: Toward transformative supply chain management." Journal of Supply Chain Management 57.1 (2021): 58-73.

[6] Nunes, L. J. R., T. P. Causer, and D. Ciolkosz. "Biomass for energy: A review on supply chain management models." Renewable and Sustainable Energy Reviews 120 (2020): 109658.

[7] Saragih, Jopinus, et al. "Supply chain operational capability and supply chain operational performance: Does the supply chain management and supply chain integration matters." Int. J Sup. Chain. Mgt Vol 9.4 (2020): 1222-1229.

[8] Golmohammadi, Amir-Mohammad, Negar Jahanbakhsh Javid, Lily Poursoltan, and Hamid Esmaeeli. "Modeling and analyzing one vendor-multiple retailers VMI SC using Stackelberg game theory." Industrial Engineering and Management Systems 15, no. 4 (2016): 385-395.

[9] Ahmadinejad, Farzad, Javad Bahrami, Mohammd Bagher Menhaj, and Saeed Shiry Ghidary. "Autonomous Flight of Quadcopters in the Presence of Ground Effect." In 2018 4th Iranian Conference on Signal Processing and Intelligent Systems (ICSPIS), pp. 217-223. IEEE, 2018.

[10] Harini, Sri, et al. "Analysis supply chain management factors of lecturer's turnover phenomenon." International Journal of Supply Chain Management (2020).

[11] Zavareh, Bozorgasl, Hossein Foroozan, Meysam Gheisarnejad, and Mohammad-Hassan Khooban. "New trends on digital twin-based blockchain technology in zero-emission ship applications." Naval Engineers Journal 133, no. 3 (2021): 115-135.

[12] Sodhi, ManMohan S., and Christopher S. Tang. "Supply chain management for extreme conditions: research opportunities." Journal of Supply Chain Management 57.1 (2021): 7-16.

[13] Cheung, Kam-Fung, Michael GH Bell, and Jyotirmoyee Bhattacharjya. "Cybersecurity in logistics and supply chain management: An overview and future research directions." Transportation Research Part E: Logistics and Transportation Review 146 (2021): 102217.

[14] Zeinali, Behrad, and Jafar Ghazanfarian. "Turbulent flow over partially superhydrophobic underwater structures: The case of flow over sphere and step." Ocean Engineering 195 (2020): 106688.

[15] Hadiana, Hengameh, Amir Mohammad Golmohammadib, Hasan Hosseini Nasabc, and Negar Jahanbakhsh Javidd. "Time Parameter Estimation Using Statistical Distribution of Weibull to Improve Reliability." (2017).

[16] Asamoah, David, et al. "Inter-organizational systems use and supply chain performance: Mediating role of supply chain management capabilities." International journal of information management 58 (2021): 102195.

[17] Bahrami, Javad, Viet B. Dang, Abubakr Abdulgadir, Khaled N. Khasawneh, Jens-Peter Kaps, and Kris Gaj. "Lightweight implementation of the lowmc block cipher protected against side-channel attacks." In Proceedings of the 4th ACM Workshop on Attacks and Solutions in Hardware Security, pp. 45-56. 2020.

[18] Zeinali, Behrad, Jafar Ghazanfarian, and Bamdad Lessani. "Janus surface concept for three-dimensional turbulent flows." Computers & Fluids 170 (2018): 213-221

[19] Gölgeci, Ismail, and Olli Kuivalainen. "Does social capital matter for supply chain resilience? The role of absorptive capacity and marketing-supply chain management alignment." Industrial Marketing Management 84 (2020): 63-74.

[20] Tönnissen, Stefan, and Frank Teuteberg. "Analysing the impact of blockchain-technology for operations and supply chain management: An explanatory model drawn from multiple case studies." International Journal of Information Management 52 (2020): 101953.

[21] Amini, Mahyar, and Aryati Bakri. "Cloud computing adoption by SMEs in the Malaysia: A multi-perspective framework based on DOI theory and TOE framework." Journal of Information Technology & Information Systems Research (JITISR) 9.2 (2015): 121-135.

[22] Saragih, Jopinus, et al. "The impact of total quality management, supply chain management practices and operations capability on firm performance." Polish Journal of Management Studies 21.2 (2020): 384-397.

[23] Amini, Mahyar. "The factors that influence on adoption of cloud computing for small and medium enterprises." (2014).

[24] Lahane, Swapnil, Ravi Kant, and Ravi Shankar. "Circular supply chain management: A state-of-art review and future opportunities." Journal of Cleaner Production 258 (2020): 120859.

[25] Amini, Mahyar, et al. "Development of an instrument for assessing the impact of environmental context on adoption of cloud computing for small and medium enterprises." Australian Journal of Basic and Applied Sciences (AJBAS) 8.10 (2014): 129-135.

[26] Xu, Song, et al. "Disruption risks in supply chain management: a literature review based on bibliometric analysis." International Journal of Production Research 58.11 (2020): 3508-3526.
[27] Marbun, Dahlena Sari, et al. "Role of education management to expediate supply chain management: a case of Indonesian Higher Educational Institutions." International Journal of Supply Chain Management (IJSCM) 9.1 (2020): 89-96.
[28] Amini, Mahyar, et al. "The role of top manager behaviours on adoption of cloud computing for small and medium enterprises." Australian Journal of Basic and Applied Sciences (AJBAS) 8.1 (2014): 490-498.
[29] Tsai, Feng Ming, et al. "Sustainable supply chain management trends in world regions: A data-driven analysis." Resources, Conservation and Recycling 167 (2021): 105421.
[30] Amini, Mahyar, and Nazli Sadat Safavi. "Critical success factors for ERP implementation." International Journal of Information Technology & Information Systems 5.15 (2013): 1-23.
[31] Maheshwari, Sumit, Prerna Gautam, and Chandra K. Jaggi. "Role of Big Data Analytics in supply chain management: current trends and future perspectives." International Journal of Production Research 59.6 (2021): 1875-1900.
[32] Amini, Mahyar, et al. "Agricultural development in IRAN base on cloud computing theory." International Journal of Engineering Research & Technology (IJERT) 2.6 (2013): 796-801.
[33] Amini, Mahyar, et al. "Types of cloud computing (public and private) that transform the organization more effectively." International Journal of Engineering Research & Technology (IJERT) 2.5 (2013): 1263-1269.
[34] Alexander, Anthony, et al. "Managing the "new normal": the future of operations and supply chain management in unprecedented times." International Journal of Operations & Production Management ahead-of-print (2022).
[35] Amini, Mahyar, and Nazli Sadat Safavi. "Cloud Computing Transform the Way of IT Delivers Services to the Organizations." International Journal of Innovation & Management Science Research 1.61 (2013): 1-5.
[36] Amini, Mahyar, and Nazli Sadat Safavi. "A Dynamic SLA Aware Heuristic Solution For IaaS Cloud Placement Problem Without Migration." International Journal of Computer Science and Information Technologies 6.11 (2014): 25-30.
[37] Amini, Mahyar, and Nazli Sadat Safavi. "A Dynamic SLA Aware Solution For IaaS Cloud Placement Problem Using Simulated Annealing." International Journal of Computer Science and Information Technologies 6.11 (2014): 52-57.
[38] Sadat Safavi, Nazli, et al. "An effective model for evaluating organizational risk and cost in ERP implementation by SME." IOSR Journal of Business and Management (IOSR-JBM) 10.6 (2013): 70-75.
[39] Sadat Safavi, Nazli, Nor Hidayati Zakaria, and Mahyar Amini. "The risk analysis of system selection and business process re-engineering towards the success of enterprise resource planning project for small and medium enterprise." World Applied Sciences Journal (WASJ) 31.9 (2014): 1669-1676.
[40] Sadat Safavi, Nazli, Mahyar Amini, and Seyyed AmirAli Javadinia. "The determinant of adoption of enterprise resource planning for small and medium enterprises in Iran." International Journal of Advanced Research in IT and Engineering (IJARIE) 3.1 (2014): 1-8.
[41] Safavi, Nazli Sadat, et al. "An effective model for evaluating organizational risk and cost in ERP implementation by SME." IOSR Journal of Business and Management (IOSR-JBM) 10.6 (2013): 61-66.
[42] Perevozova, Iryna, et al. "Integration of the supply chain management and development of the marketing system." International Journal of Supply Chain Management 9.3 (2020): 496-507.
[43] Khoshraftar, Alireza, et al. "Improving The CRM System In Healthcare Organization." International Journal of Computer Engineering & Sciences (IJCES) 1.2 (2011): 28-35.
[44] Abdollahzadegan, A., Che Hussin, A. R., Moshfegh Gohary, M., & Amini, M. (2013). The organizational critical success factors for adopting cloud computing in SMEs. Journal of Information Systems Research and Innovation (JISRI), 4(1), 67-74.
[45] Newiduom, Ladson, Keypi Jackson, and Ibrina Browndi. "Information Technology and Cloud Computing Altering the Searching and Training of Involved Urban Planning." International Journal of Science and Information System 4.2 (2019): 90-95.
[46] Opuiyo, Atora, et al. "Three-Dimensional Modelling of Urban Temperature Landmasses and Its Planning Consequences." International Journal of Smart City Planning Research 20.21 (2019): 426-430.
[47] Embouma, Mike, et al. "Smart Green Evenhanded Metropolis Actions against Urban Planning in European Union." International Journal of Basis Applied Science and Study 56.14 (2019): 1218-1222.
[48] Zhang, Lixuan, et al. "Blockchain and cryptocurrency for announcing securely timestamped script submission and peer review reaction using the supply chain management ." International Journal of Science and Information System 9.3 (2021): 86-92.
[49] Li, Chang, et al. "Investigative success factors concerning adoption of blockchain technology on behalf of e-government improvement ." International Journal of Basis Applied Science and Study 11.6 (2021): 642-647.