WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

BLOCKCHAIN AND PEER TO PEER NETWORK PROTOCOL

MAHESH SOLANKI[1], Dr. VISHAL SHRIVASTAVA[2], Dr. AKHIL PANDEY[3], Dr. AKHIL PANDEY[4]

[1]B.TECH. Hosteler, [2]Student,[3]Professor, [4]Assistant Professor
Information Technology
Arya College of Engineering & I.T. India, Jaipur
[1]solankimaheshmali@gmail.com
, [2]vishalshrivastava.cs@aryacollege.in,[3]akhil@aryacollege.in

ABSTRACT:

Blockchain is made up of networks of consecutive blocks that are linked to one another by pointers to their previous block. These create a chain. Blockchain technology provides a database like support through creation of digital ledgers, in an effort to facilitate distributed transactions. The use of blockchain in real-world applications is faced with numerous challenges. This research proposes to comprehend the approach, its features and the concepts of implementation of transactional systems in terms of distributed transactions across web resources. The research also analyzes the recent trends and issues in the application of blockchain in most large-scale public utility use cases in e-commerce.

1 Introduction

A blockchain is an ever-growing chain of blocks of records that are protected through linking to one another and with the use of cryptography. Every block is connected to the previous one, it is timestamped and its transaction information (Leopard, 2020). Blockchain technology has been mainly recognized in recent years to create digital currencies or cryptocurrencies for e-commerce and banking. Bitcoin was the first cryptocurrency (Chen et al., 2020). It is maintained by a distributed system which is fully decentralised. It is founded on peer-to-peer (P2P) networks (Feld et al., 2016). Blockchain can be thought of as a different data format for storing state changes as in a database. Decentralised P2P system is used by blockchain for processing database transactions. Formation of digital ledgers is one of the key responsibilities of blockchain system. In finance, a ledger is a book used to maintain an account of its financial transactions. In blockchain, there are ledgers which are maintained and shared among several parties and as a proof of authenticity, every transaction is signed digitally. Once entries are added in these blockchain-based distributed

1.1 Digital currency transactions

Example 1: Cryptocurrency transaction
Consider two users, users A and B. This transaction will proceed as follows:

•User A wants to transfer Bitcoins to user B by
encrypting transaction details and broadcasting it worldwide.

• Users everywhere confirm sender and receiver authenticity, and if a transaction can occur.

• If confirmed, the transaction would be included within a block (containing a group of other transactions).

• Transaction would indicate Bitcoins are decreased from user A wallet and transferred to user B wallet (Jimi, 2018).
Examples of cryptocurrency are Ethereum, Dash, Ripple, Monero, NEM and Litecoin (Cointelegraph, 2013).

This research takes into account the pertinent points related to transaction commitment. The rest of the manuscript is structured as follows. In Section 2, we discuss motivation and background, Section 3 we discuss basic building blocks of distributed ledger yechnology, Section 4 blockchain architecture for P2P transactions is discussed, in Section 5 distributed system with P2P network is discussed, Section 6 transactions in commit protocols are discussed, Sections 7
and 8 address transaction management in distributed ledger technologies and implementation issues in blockchain. Lastly we conclude with industrial relevance of blockchain in Section 9, related work in Section 10 and summary and conclusions in Section 11.

2 Motivation and background

Conventional banking has financial institutions which are committed to the management of money. The bank accepts money deposits from the clients and employs these funds to lend it to individuals or businesses for charging some interest on it. Traditional banking requires some time duration to complete any transaction since it is based on the number of mediators. It also holds one main ledger containing all the credits and debits. Each member of the business network maintains a copy of ledger and the ledger is refreshed each time any asset enters or leaves the organisation (Singh, 2019). There are very few desirable features which can be attributed to traditional banking. These are:

1 Efficiency: Conventional banking involves overheads since various parties need to conduct and operate their businesses. They need to also maintain and update their ledger efficiently. Hence, human resources are needed to process transactions (Singh, 2019).

2 Maintenance costs: There is a maintenance fee on every transaction. Likewise, with time as an element, an internal audit will consume time on the business network (Singh, 2019).

3 Vulnerable: Conventional banking is susceptible to either fraud or malicious alteration to the ledger due to cyber-attack (Singh, 2019).

Basic building blocks: digital ledger technology
There are few building blocks in blockchain which construct a digital ledger. These are described as follows:

1 Transaction: Transaction transfer the assets Bitcoin and monetary unit values from one user to another.

2 Blocks: Transactions are kept in blocks (thus the name blockchain). They create the distributed ledger.

3 Nodes: These are the system executing the blockchain software. There exists also a unique form of nodes known as full nodes. These nodes replicate the whole blockchain from the beginning of time. These nodes will include a new transaction into the highest block (Singh, 2019).

4 Mining: Mining is the process through which
transactions are verified or settled, that is, are included in the block.

5 Nonce: A nonce is a once-only number, that is, it is utilized for a certain reason and never repeated. It is utilized in order to prevent duplicate transactions where that might have adverse effects. There is a chance that information which is inserted into a database may also have an equivalent identifier. When a nonce is prefixed to the identifier, the identifier will be made unique, preventing duplication by chance (Lynda, 2017).

6 Hash function: Hash function is a computational algorithm that receives data of any size, acts on it and delivers a number as hash, which is fixed-size data. Regardless of whether the input data is a single character or a large word, the size of the resulting hash is the same. Hashing a string to a signature is known as hashing. Hashing is a one-way process (Tewari and Gupta, 2020). The hash function will take any length string and produce a fixed-length output, but it is not possible to take the fixed-length output data and reverse it the string (Lynda, 2017). In blockchain, the digital fingerprint is created using the hashing algorithm Secure Hashing Algorithm (SHA-256). SHA-256 produces a 256-bit-length hash (Barnden and Srinivas, 1991).

7 Smart Contracts: Transactions are typically intended by clients and thereafter evaluated on the blockchain using a group of rules referred to as smart contracts.
Benefits of smart contracts:

•The parties in the contract can be anonymous.
• The precise contract execution rules and sanctions may be programmed and enforced automatically.
• The contract-related activity may be monitored without compromising the privacy of the parties (Singh, 2019).

4 Architecture for P2P transactions using blockchain
A blockchain is essentially a distributed database with a P2P network. It consists of a sequence of ever-expanding blocks that store the data (similar to traditional public ledger in which every transaction is noted) and do not allow tampering and modification of the data (Huang et al., 2017). Figure 3 illustrates an example of a blockchain. The block header contains the previous block's hash. A single block in blockchain contains a single block of parent. The initial block without a parent block in blockchain is referred to as the genesis block.
One block consists of a block header and a block body, as indicated in Figure 4. A header block consists of the following:

• Block version: To ensure conformity to block validation, it shows a set of rules that has been established. • Merkle's root hash tree: It is the hash value of the entire block transactions. • Timestamp: The real time in seconds (universal time from 1 January 1970).

• Bits: An acceptable block hash's target value.

• Nonce: A four-byte regulation, typically initialized at zero and increasing with each hash computation.

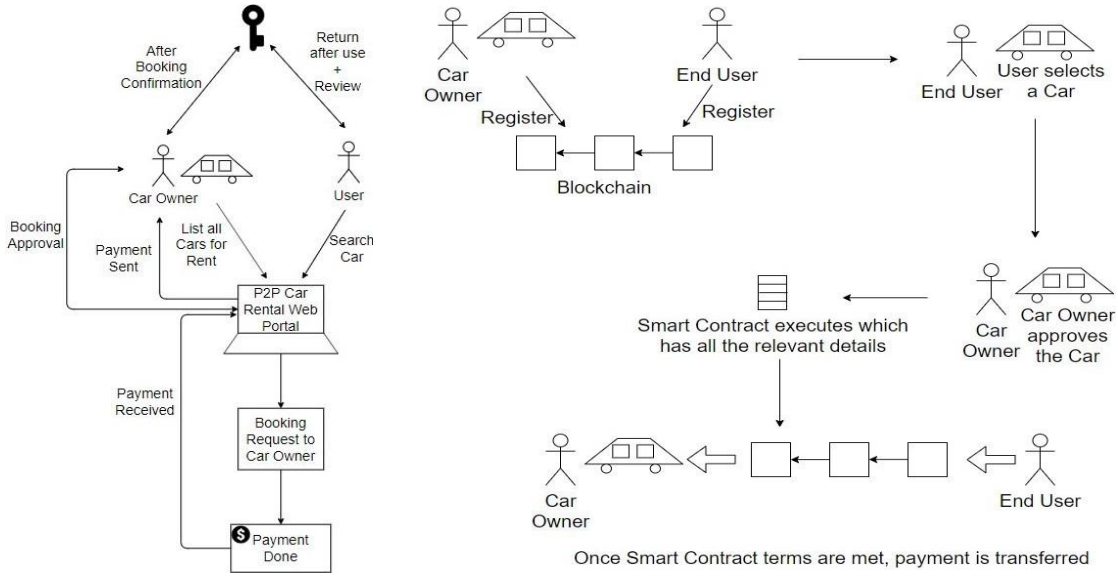
• Parent hash block: A 256-bit hash value indicating the previous block.

The frame of a block consists of a transaction counter and transactions. The size of a block and size of every transaction varies based on the broadest range of transactions brought by a block. As indicated in Figure 3, whenever a block is appended to this chain, a set of values is appended to the new block (previous block hash, previous block pointer). Therefore, if one block has been tampered with, it can be identified by comparing it with the hash of the previous block. If the hash value of one block is altered, the hash values of the subsequent blocks will also need to be altered. It is not feasible to modify the blockchain using this hash-validated pointer format (Silberschatz et al., 2011).

Figure 2

(a) Car rental in blockchain

(b) P2P car rental process



(a)

(b)

Source: (a)Intelligence (2019) and (b)Fatbit (2019)

Also, in order to prevent a single node or set of nodes from being tampered, the chain must be copied throughout the blockchain network on multiple independent nodes. Since the blockchain is duplicated in different nodes, there should be a distributed consensus algorithm to keep the right state of blockchain. Decisions are made by majority nodes (Silberschatz et al., 2011). The above method will be effective if a group of nodes are under some control on the blockchain. This will render it extremely difficult for other nodes to control the majority nodes.

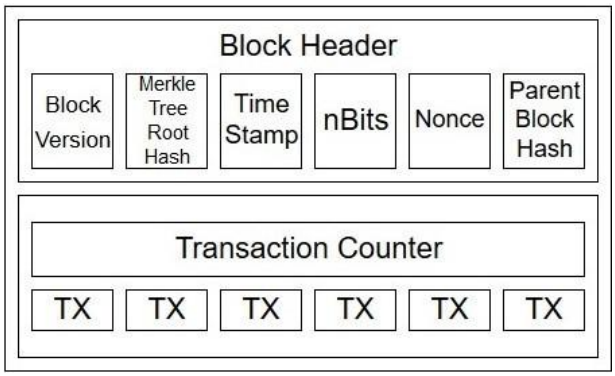
Asymmetric cryptography is implemented to authenticate the authentication of blockchain transactions. For an unreliable environment, digital signature based on asymmetric cryptography is implemented

5 Distributed system with P2P network

A P2P network has a group of devices sharing and storing files autonomously. Each single device or node is a peer (Amoretti and Zanichelli, 2016). For financial technology, any exchange of digital commodities or cryptocurrency among any two members is referred to as P2P across a distributed network. This platform allows consumers and dealers to conduct trades without any intermediary. In some instances, websites offer a P2P platform that connects borrowers and lenders. In the majority of usage scenarios, P2P architecture is implemented in distributed computing applications like online shopping sites, live streaming sites and web search engines (Agrawal et al., 2007).

Figure 4

Block structure



Source: Zheng et al. (2017)

5.1 Working of a P2P network

The collection has a distributed network of users. There is no server or central authority, as every node contains a copy of all the files. Each node can upload or download files and share it with other nodes. Each node is both a client and downloads files from various nodes and when it behaves as a server, it is source for other nodes to download files (Susilo et al., 2015). Such P2P structures are more efficient and faster as the number of users continue to increase. The distributed nature of P2P networks renders them more resistant to cyberattacks (Dai et al., 2019).

5.2 P2P transactions

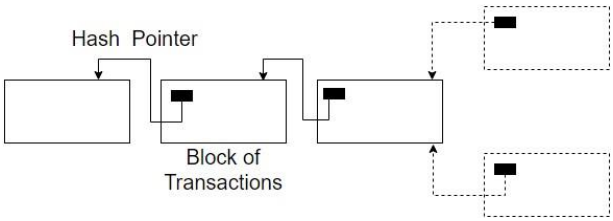
Blockchain technology is a method of transaction validation and transaction recording that lacks centralized platform. In a blockchain network, similarly, P2P facilitates peer-to-peer information interaction among nodes, so each individual will have transaction records by way of P2P transaction validation (Sharma et al., 2017).
The key difference between two-phase commit and P2P commit is that in two-phase commit, the coordinator must wait for all the participants to move into the required actions to commit the process while in P2P commit, every pairing set of interacting nodes must act. The remaining nodes (or pairs) may proceed with their pairwise interactions independently as transactions. A P2P transaction is shown in the Figure 1(b) and two-phase commit is shown in Figure 1(a). P2P trading and car rental examples are discussed in the subsequent sections.

6 Transactions in commit protocols

6.1 Two phase commit

In two-phase commit, a central site acts as the coordinator (Ragunathan and Reddy, 2010). It controls the execution of transaction at other sites. Every slave can abort the transaction with a 'no' answer in the first round. A commit protocol is therefore characterized by a state diagram. For coordinator and slave, there are four different local transaction states: initial state q, wait state w, abort state a and the commit state c. A site remains in the initial state until it makes a decision to abort the transaction unilaterally. If the site does not abort, it will move to wait state. This is an indefinite state in which the outcome is yet to be determined. Following the wait state, the site either moves to commit state or abort state. This is illustrated graphically in Figure 8 (Liu et al., 1998).
The two-phase commitment goes on in two steps. The coordinator sends a round of messages to participants in the first phase, to vote to commit or abort the transaction. In the second stage, the coordinator sends another round of messages to the participants to commit or drop the transaction as voted. Once the second phase is complete, no modification is done to the data state until a coordinator's commit message is received by the participant.
Let N = number of read-write transaction operations, and C = number of participants involved in the execution of the transaction.

• For committing a transaction: Two phase commit requires 4C messages and 2C + 1 number of log forces.
• For aborting a transaction: There will be two cases:
Case 1
If a site failure happens or if at least one participant returns a 'no' vote, a transaction can abort during execution of its operations. 4C messages (reduced by one for each failed voting participant) and 2C + 1 log forces (reduced by one for each failed voting participant) are utilized to abort the transaction.
Case 2
There is no need for a vote and a single round of 2C messages needs to be sent with C + 1 log forces (Skeen, 1982).
Figure 6
A fork in blockchain



7 Transaction management in distributed ledger technologies

There are numerous new uses of blockchain transactions. Blockchain technology will be used by all the devices which are part of the internet of things (IoT). Blockchain technology may be required by governments and smart cities. A smart contract is a computer program that can enable the exchange of money, land, stock, or something of value more easily transferred. Smart contracts are embedded digitally and, upon fulfillment of the conditions, the application of blockchain technology enables them self-execution (Buterin et al., 2017). Smart contracts based on blockchain technology operates with no downtime, fraud, or third-party intervention. An example of blockchain-based smart contracts is Ethereum (Wood et al., 2014). Ethereum offers smart contracts with the ability to execute automatically, which allows the customers to pay in digital currencies and control their assets. Ethereum also allows

developers to develop and deploy decentralised applications.

7.1 Identity management with blockchain

Blockchain has various potential applications across numerous industries. One of the most likely possibilities is identity management. It is a way of establishing one's identity. Systems ask users to register their own details, credit cards, debit cards and other embedded chips cards which various organisations use for authenticating identity. Identities may be stored on blockchain. Take an example of the system developed on Ethereum with a decentralised app called uPort (Lynda, 2017). uPort, its first creators believe, is an open-source software initiative that seeks to create a global unified sovereign identity for individuals, companies, organisations, devices, and bots.
P2P state diagram

7.2 Blockchain in web services

Blockchain systems are infrastructure support for the web services. Take an example by Gupta and Roy (2017). The blockchain facilitates interoperability for health records. Health and medical incidents metadata are kept on a blockchain but the actual documents are kept on a universal health cloud. Hence, only a patient's metadata like patientID, hospitalID, visitID and hash are kept on the blockchain.
Therefore, if a patient's visit goes to two different hospitals. At the first hospital, a record will be made on the blockchain in the universal health cloud. The visit metadata and URL will be in this transaction. The patient must sign this transaction using his/her key. At the second hospital, the patient must share his/her key for the hospital authority to access the transactions in blockchain. Only the concerned authority possessing the patient's key can really read the transactions by decrypting them. Smart contracts can also be encoded to perform some instructions like emergency contacts and insurance.
Blockchain technology is typically implemented on top of web services. Amazon Web Services (AWS) offers an easy method to construct scalable blockchain network and ledger business applications. AWS offers a managed and scalable blockchain service, easier to set up and deploy blockchain networks (Amazon, 2020).

8 Implementation considerations in using blockchains

Blockchain has few implementation challenges which are enumerated as below:

1 Blockchain implementation cost: Hedera anticipates that 10,000 cryptocurrency transactions could be executed within a second. However, if such transactions were executed, each transaction would require a state proof. Consequently, all-time would be taken by answering queries instead of transaction processing, which can result in lower throughput (Haig, 2019).

2 Blockchain endpoint location: Endpoints generate new blocks through the mining step in the PoW protocol. The location to place endpoints of blockchain has a great effect on bandwidth, computation, and space usage. This is thus a significant architectural issue in the blockchain (Liao et al., 2017).

3 Loss of blockchain key: To open a blockchain account, one requires a key. The blockchain key is an extremely long string of letters and numbers, so it cannot be guessed. As per Madnick (2019), the blockchain key is kept anonymous so that nobody knows who the key belongs to. In blockchain if a person loses the blockchain key, the blockchain account can never be opened again.

4 Irremovable history: Blockchain possesses an immutability feature such that once a record is entered on the blockchain, it will be stored permanently. If blockchain is utilized to hold criminal records and an individual desires his record to be removed. It is impossible with blockchain. The individual's past will be stored permanently on the blockchain. Therefore, blockchain cannot be utilized in every type of application (Somers, 2019).

5 Distributed control issue: Since blockchain is a decentralised system, it has numerous servers (nodes) operating at the same time and cannot be shut down. There is no 'on' and 'off' switch. Therefore, if there is a software bug in any application, anybody with an ill intention can exploit it (Somers, 2019).

6 Scalership – increasing the number of users: The number of the users of blockchain has been on the increase that implies the online transactions have been on the rise. This kind of increase can result in slowing down the validation of the transactions. Prior to the authentication of the transaction the basis of the same must be validated (Meva et al., 2018). Therefore, the blockchain must be more scalable than previously.

7 Security and privacy concerns: Transactions that are executed through blockchain become transparent to all the accessible users on a network. It will lead to the revelation of useful information about sensitive departments to everyone. This way, offering security and privacy to such departments is a problem of the blockchain (Liao et al., 2017). This issue can be resolved by personalising data settings available to only specified individuals or sources (Meva et al., 2018). This issue can also be resolved by implementing a permissioned blockchain so that only specific users of the organisation can access the precious data.

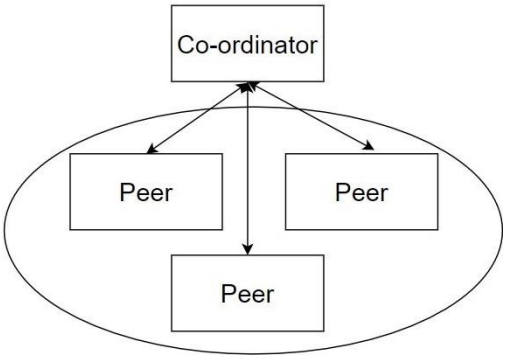
8 Unsustainable energy use: The other challenge experienced by the blockchain is additional energy consumption by it when it runs on such operations, which involve very complex scientific computations for business verification. An industry standard solution for this issue is needed (Review, 2020).

9 Spending attacks issues: Majority attack (Frankenfield, 2019) can be conducted by hackers or commonly known as 51% attack is conducted by miners who have over 50% of network's processing power. The attackers block new transactions, disrupt the payments and also succeed in reversing the Frankenfield (2019) transaction. In a double spending attack (Koteska et al., 2017), a person keeps the same Bitcoin to spend again for services.

9 Industrial significance of blockchain

Blockchain can be used to trace foods from manufacturers to stores and consumers, digitally and securely. IBM blockchain platform provides end-to-end capability that customers must enable and build, execute, govern, and protect their own small business networks successfully. IBM has been looking to streamline blockchain power from the distribution chain. IBM, together with Samsung, developed the 'autonomous decentralised P2P telemetry' (ADEPT) framework, using elements of their
Bitcoin's built-in design to establish a network of distributed devices decentralised internet of things.
ADEPT employs three device protocols: Bit Torrent (for document sharing), Ethereum (for smart contracts) and even TeleHash (like P2P messaging), whereas blockchain is the answer for general logistics enhancement so that errors or fraud can be prevented in addition to cost savings, waste, and delays. Blockchain can also assist in enhancing inventory management and identifying issues more efficiently. (Tijan et al., 2019).

Figure 10



Abort stage in P2P network

10 Related work

A blockchain in its current state is by no means its final state. There are alternative distributed ledger technologies (DLT) that have the ability to alleviate the primary issues.

1 Holochain is an organization that offers a new type of DLT (Holochain, 2019). It provides an efficient and scalable cryptocurrency pattern with no need for specialized hardware or consensus. It allows tracking and billions and trillions of interactions per second.

2 Hedera Hashgraph Platform (Haig, 2019) is a permission ledger with the use of the hashgraph consensus algorithm. It can handle an approximate 10,000 transactions per second of cryptocurrency. Using a 'gossip' protocol, Hedera verifies and broadcasts the transactions. Hashgraph 'gossips' the data on the network to some nodes (which are pre-determined) and the data is then sent over the network to other nodes. The gossip protocol broadcasts transactions performance better than PoW chains. Hedera Hashgraph offers four main services such as a cryptocurrency service, a smart contract service, a file service and a consensus service. The cryptographic service includes an in-built cryptographic time-stamping service. Hedera Hashgraph provides asynchronous Byzantine fault tolerance mechanism to all its third party applications. Hedera Hashgraph can support stablecoins (cryptocurrency), financial markets and exchanges or even real-time games. Hedera Hashgraph can also be used in short-term private keys to encrypt a message.

11 Transaction failure before it is committed

Summary and conclusions

Blockchain enables a P2P system that can utilize smart contracts and smart bonds for numerous users without third-party interference. Through the application of cryptography, node-to-node network transactions can be secure. This research provides the management of P2P transaction concepts related to blockchain. It takes into account blockchain technology and its impact on future implementations. This research also addresses different transactions in the blockchain and P2P transactions. The key implementation problems in blockchain also have been addressed in detail. For blockchain applications, blockchain technology implementation can be viewed as stable storage and log-structured storage. Stable storage support makes the system secure. Information in stable storage is never lost. By better ethical standards, blockchain has the potential to become a mighty instrument to enhance business, finance, healthcare, governance, and much more.

REFERENCES

1. Agrawal, D., El Abbadi, A. and Suri, S. (2007) 'Attribute-based access to distributed data over P2P networks', International Journal of Computational Science and Engineering, Vol. 3, No. 2, pp.112–123.
2. Amazon (2020) Blockchain on AWS [online] https://aws.amazon.com/ blockchain/.
3. Amiri, M.J., Agrawal, D. and Abbadi, A.E. (2019) 'CAPER: a cross-application permissioned blockchain', Proceedings of the VLDB Endowment, Vol. 12, No. 11, pp.1385–1398.
4. Amoretti, M. and Zanichelli, F. (2016) 'Distributed reputation management for service-oriented peer-to-peer enterprise communities', International Journal of Computational Science and Engineering, Vol. 13, No. 2, pp.147–157.
5. Aznar, F., Pujol, M. and Rizo, R. (2012) 'Macroscopic definition of distributed swarm morphogenesis', Connection Science, Vol. 24, No. 4, pp.162–192.
6. Balusamy, B. and Krishna, P.V. (2017) 'Simplified and efficient framework for managing roles in cloud-based transaction processing systems using attribute-based encryption', International Journal of Computational Science and Engineering, Vol. 14, No. 2, pp.135–149.
7. Barnden, J. and Srinivas, K. (1991) 'Encoding techniques for complex information structures in connectionist systems', Connection Science, Vol. 3, No. 3, pp.269–315.
8. Bitcoin (2009) Bitcoin is an Innovative Payment Network and A New Kind of Money [online] https://bitcoin.org/en.
9. Bloembergen, D., Hennes, D., McBurney, P. and Tuyls, K. (2015) 'Trading in markets with noisy information: an evolutionary analysis', Connection Science, Vol. 27, No. 3, pp.253–268.
10. Buterin, V. et al. (2014) A Next-Generation Smart Contract and Decentralized Application Platform, White Paper, Vol. 3, No. 37.
11. Chen, W., Zheng, Z., Ma, M., Wu, J., Zhou, Y. and Yao, J. (2020) 'Dependence structure between Bitcoin price and its influence factors', International Journal of Computational Science and Engineering, Vol. 21, No. 3, pp.334–345.
12. Cointelegraph (2013) What is Cryptocurrency. Guide for Beginners [online] https://cointelegraph.com/news/hedera-hashgraph-deeplook-into-10-000-transactions-per-second-claim (accessed 2020).
13. Dai, Y., Li, G. and Xu, B. (2019) 'Study on learning resource authentication in MOOCs based on blockchain', International Journal of Computational Science and Engineering, Vol. 18, No. 3, pp.314–320.
14. Ethereum (2020) Ethereum is a Global, Open-Source Platform for Decentralized Applications [online] https://www.ethereum.org.