Turkish Online Journal of Qualitative Inquiry (TOJQI)

Volume 12, Issue 5, June 2021: 1236 – 1246

Research Article

Challenges and its Solutions with Blockchain Technology Adoption in Enterprises

Ranju S. Kartha [1]

Abstract

Blockchain is going to be a very critical technology for future development of the world. This technology is useful in storing immutable data ensuring that no one will alter data. Since it is decentralized and traceable, no central authority can control it, making it less corruptible. The enterprises are starting to use Blockchain to achieve operational efficiency by automating business process or digitizing records, tracking and tracing physical and digital assets and securing sharing of information. The number of threat vectors grows exponentially as blockchain networks become more complex. While it significantly reduces traditional risk it also creates new risks. This paper highlights the risks and challenges with blockchain adoption, also proposes some of the solutions. Blockchain is an inter-organizational technology, so how do this technology bring people from different organization together is the biggest challenge. There are many other issues like interoperability, latency issues, smart contract vulnerabilities, security concerns and throughput issues etc. But people are still exploring and finding new ways of implementing blockchain technology in daily life due to its versatility resulting in new and innovative applications. So blockchain technology is revolutionary with the potential to improve or develop new systems in different industries and areas.

Keywords: Blockchain Technology, Consensus Algorithm, Decentralized Application, Distributed Ledgers, Immutability, Smart Contracts.

Introduction

Digital transformation is the prerequisite of the organization to remain competitive in the fast-changing world. Blockchain changed the thinking of people and business, it is a revolutionary technology that is going to remake the future. Big companies as well as business have felt the importance of this new technology. So many of the biggest organizations and business owners are focusing on blockchain. With blockchain, people from all around the world can exchange information quickly, effectively, securely and efficiently. That is why businesses and banks are trying to adopt this new technology to work effectively and improve their transactions. This technology which fundamentally influences the way that our economy, governance systems and business functions and changes our conceptual understanding of trade, ownership and trust.

[1] Dr., Mangalam College of Engineering, Ettumanoor, Kerala, Computer Science and Engineering Department, ranju.kartha@mangalam.in

Received: , Accepted:

Blockchain is definitely needed as this is the age of smartphones and world wide web. The rest of this paper is organized as follows: Section 2 describes the need of blockchain technology in today's world. Section 3 comprises the working of blockchain technology and section 4 addresses risk and challenges with adoption of blockchain technology in various enterprises. Section 5 proposes some of the solution to prevent risks in blockchain adoption and Section 6 presents the conclusion and future scope.

Need of Blockchain Technology

In today's world, advanced digital transactions take place every moment of each day- orders, payments, account tracking and much more. With Often It is observed that the world is standing up to modern challenges in the midst of COVID-19. The challenges include:

- Trust Deficit
- Fake Menace
- Anonymity
- Access to quality capital
- Supply chain agility and resiliency
- Need constant reconciliation
- No single version of truth

Trust

Trust is a desire, where a person will have an expectation that the person on other side will work with integrity. Nowadays we are facing a huge amount of trust deficit- when we are buying a product, we are not sure about how it is come. We are not sure about the source of the news article we read, there are many fake menaces which is going on in and around us and government is finding hard to detect. In the case of a company, it is coordinated with supplier, bank, customer, auditor and insurer. Each entity maintains its own set of accounts and it has separate transactions. But everything has to be subject to reconciliation, so there is no single version of truth. Blockchain is an evolution of ledger technology. It is maintaining a record of transactions in our lives. So, we can track the ownership of assets before/ during/ after any transaction in a secure and transparent way.

Fake Menace

Nowadays, because of the use of smart phones the world captures over 1 trillion computerized images and recordings annually. There are countless applications are available for any of us to download and use to edit manipulate and alter images and even videos. Today's world people depend on social media pictures and recordings more than ever before and on the other side we don't believe them. Due to the transparency, traceability and decentralization nature of the Blockchain, it can be conceivable to check the realness of the data or the source of information and build trust in news shown on the Web. The Blockchain in news industry enables the content to be produced and distributed over the internet in an immutable and secure way (Akash 2020).

Anonymity

It refers to data obtained from respondents who are totally unknown to those concerned with the survey. Anonymity is essential as it offers protection to those who are most at risk of experiencing retaliation for their action or beliefs such as those who support potentially controversial organizations. Blockchain provides anonymity which means nobody knows how many blockchain assets we have and who we traded with. In blockchain technology only the person with private key can access all of the transfer information.

Access to Quality Capital

Most of the small businesses needs additional capital to start to grow to reach their potential but there are some barriers. Blockchain provides significant benefits to businesses by enabling easier, cheaper, and faster access to capital through programmable digital assets and securities (ConsenSys 2020).

Supply chain Agility and resilience

Supply chain resilience is an approach that assists a country to make sure that it has diversified its supply risk across many supplying nations rather than being dependent just one or few. While globalization has provided unlimited opportunities, it has also increased competition complexity and vulnerability. Blockchain technology could make supply chain management simpler and more transparent. Using this technology companies can manage and monitor risks within the supply chain ensure quality of delivered parts and track delivery status. Companies can also use smart contracts to manage and pay for supply chains autonomously. Smart contact could assist with shipping and logistics tracking valuable products as they travel around the world. Using blockchain technology, companies have a complete picture of their products at all stages of the global supply chain bringing transparency to the production process while reducing the cost of manufactured goods.

Need Constant Reconciliation

Disruption in the finance industry has become the new normal, and migrating to a growth mindset is the most effective way for accounting and finance professionals to prepare for what’s ahead (Blackline 2017). Account reconciliation are an effective way to keep a digital eye on everything from household budgets to the finances of publicly traded companies. Most of the companies uses double entry accounting to perform an account reconciliation. But double entry accounting system has many problems such as complexity, cost, accuracy and time spent doing and verifying entries. A blockchain is a distributed, digital ledger which represents a significant innovation by offering a disinter-mediated solution to record keeping and growth of the digital economy. Since the blockchain is a shared ledger that processes transactions in real time, it has the potential to improve accounting efforts by lowering overall costs which are associated with reconciliation of ledgers, it makes reconciliation untenable.

No Single Version of Truth

In computerized business management, single version of the truth, is a technical concept describing the data warehousing ideal of having either a single centralized database, or at least a distributed synchronized database, which stores all of an organization's data in a consistent and non-redundant form (Wikipedia 2019). In today’s world with the growing complexity of our technology, it getting harder to find and maintain the single version of truth. It is one of the important requirements in digital transformation. Blockchain technology provides a single version of the truth of an agreement, by validating all digital transactions using consensus algorithm within the network (Sally 2019).

Blockchain Technology

Blockchain is a decentralized digital public ledger used to record transactions across many computer systems implemented in such a way that any record cannot be altered or changed without changing all the subsequent blocks. It is a new way of securing trust, transferring the values and storing the data. Blockchain is a digital record of transactions and its name comes from its structure, in which individual records called blocks, are connected together in a single list called chain. It's a new type of database, where information held on a blockchain exists as a distributed shared ledger, so the records are truly public and easily verifiable.

In this technology, there is no one has control of ledger, no one can falsify anything on the chain, there is no double spending is possible and finally anyone's identity can be kept completely secret. There no centralized version of information exists for the hacker to corrupt. It is additionally less vulnerable since it uses consensus algorithms to validate each transaction. Following are the four key features of this technology:

Distributed Ledgers

Blockchain is a decentralized distributed ledger, every transaction goes through the blocks and which is distributed across a number of systems in a real time basis over a peer-to-peer network. So, the ledgers are stored and maintained by all the participating nodes in the network.

Immutability

Each block header has a field that references the previous block hash key, thus forming a continuous chain of blocks. If anyone tries to tamper any block, then the whole blockchain will get dissolved, so the blockchain is immutable.

Privacy

Blockchain uses cryptographic hash functions, public and private key cryptographic techniques to ensure secure, authenticated and verifiable transactions.

Trust/Consensus

No one can alter the data without everyone finding out, it uses consensus algorithm to validate data. The consensus mechanism is used to decide which block will be added to the network. A transaction is valid only when, more than 50% of the nodes in the network should agree the consensus about its validity (Bellini 2020).

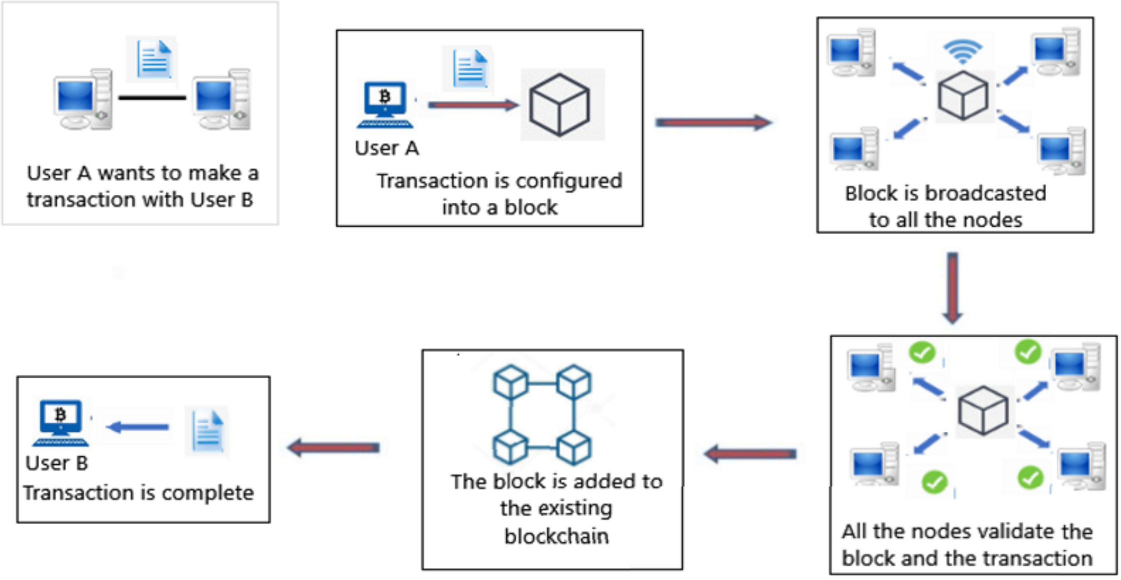
User A wants to make a transaction with User B
User A
Transaction is configured into a block
Block is broadcasted to all the nodes
All the nodes validate the block and the transaction
The block is added to the existing blockchain
User B
Transaction is complete

Figure 1. **How Blockchain works**

In Figure. 1, user A wants to make a transaction with user B, whenever a new transaction occurs, it creates a new block with new data which is broadcast to peer-peer network consisting of computers, known as nodes. Using known algorithms, the nodes in the network validates the transaction and the user's status. A verified transaction might involve records, cryptocurrency, contracts 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 added to the existing blockchain which is permanent and unaltered. The block thus created is identified using a unique code called hash. Each block has a block header and block data. Block header contains hash of the current block, timestamped batches of recent valid transactions and hash of the previous block. The block data having list of validated and authenticated transactions, thus forming a contiguous chain of blocks called blockchain. Blockchain network uses consensus mechanism which is agreed upon a signal value of truth that gets added to the blockchain.

The pillars of the blockchain structure are the contents of the block loop connection, validating the new block with the P2P consensus and verifying the communication with the encrypted signature (Cheng 20217). Blockchains are consumers of advanced cryptographic primitives including cryptographic hashing and digital signature. In blockchain technology all transactions are chained together by their hash value, once committed to the chain all records are immutable. It is impossible to alter a previous record without altering every party's chain. If one node compromised, it can no longer participate in the chain until it regenerates, the true chain from the other participants.

With blockchain, every time an asset is used or consumed, the owner of the asset signs the transfer with a private cryptographic key. In order to initiate the transaction, the owner requires both the asset and the private key. After broadcasting, anyone in the network can use owner's public key to guarantee the digital signature coming from private cryptographic key is authentic. Thus, blockchain will check the validity of the key and ownership of the asset. Therefore, even if the asset is cloned, it cannot be used without the private key. Once the transaction has been committed to the chain, the owner of the asset will have changed. This means, each node that receives a second transaction requesting the transfer of ownership, it will check that there was a previous transaction that already transferred the asset and will reject that transaction. This will prevent double spending. So cryptographic system plays an important role in the inner working of blockchain technology and public key encryption scheme serves as the premise for blockchain transactions.

In blockchain system consensus mechanisms are used to ensure records are true and honest. There are various consensus mechanisms, the difference is the way the consensus is reached. Cryptocurrencies like bitcoin and Ethereum use a Proof- of-Work mechanism. Each transaction in the network is validated by having people solving a complicated math puzzle attached to it. This is done by powerful computers and are known as miners. A reward in the form of a cryptocurrency is issued to the first minor who cracks the puzzle. The minor who has first solved the hash puzzle is allowed to broadcast the block in the network. The block also includes the solution to the puzzle, also called nonce in the block header. Other miners on the network will receive the block and they validate this block before they append it to their chain of blocks.

Blockchain technology is providing cybersecurity and protecting precious data against attacks. Communication reliability and safety will also significantly improve with this technology. Peer-to-peer ride sharing apps allow the owners to pay automatically and the reduction in complicated bureaucracy is also one of the achievements of blockchain. With blockchain, corruption can be easily be traced instead of traditional systems which are very slow. With blockchain sensitive medical information about patient is stored in a decentralized database that is accessible to the authorized doctors. So, treating health problems with Blockchain will become easy and convenient. Hence, this technology ensures that each and every deal is a real one.

Risks And Challenges in Blockchain Technology

Every technology has advantages but simultaneously also possess some limitations that need to be considered while using that technology. In today's world Healthcare systems, Banking, Cyber Security, Real estate, Automotive industry, Bitcoin, Voting, Payment and Transactions and Smart Cities etc. uses blockchain technology. This paper points out some of the real barriers to greater adoption of blockchain technology.

Distributed Ledgers

Many industries especially big enterprises they need to follow particular regulatory compliance and whenever we deal with blockchain, we will keep that in mind. Countries like US take a lead on how regulation on cryptocurrencies should take place within the united states framework. So, the enterprises need to adopt new smart regulatory hands-off approach for implementing blockchain technologies in their financial services and other sectors (Yeoh 2018).

Scalability

Blockchain is a decentralized secured network, whenever a new transaction is created it needs to propagate to the network, it reduces the transaction speed. Scalability is an important issue in blockchain because of the limitation in the size of the block that can hold data and block creation time. Even if the block creation time is reduced, it is quite difficult to solve due to the security issues. There is a limit to block size due to the transmission overload of the network, even if the size can be increased by a certain amount.

Integration with the legacy system

Blockchain is running on the latest technology due to which its too difficult to get it synced with older systems as those systems or software need to be modified to incorporate the changes due to which overhead cost is increased to meet the blockchain requirements. Thus, it might take a lot of funds or human expertise and also it is a time-consuming process. To solve this issue, the enterprises must find way to sync their existing system with blockchain solutions.

Less Privacy

In blockchain the identities of users are anonymous, but still with the transaction patterns it is feasible to connect the user's identity with that address and can get information about the user.

Potential security threats

Real time transaction is a biggest challenge in blockchain technology. Private blockchains are generally smaller and easily disrupted by traditional DDoS. Assets can be compromised when it is moved between blockchains, this causes interoperability risk. If the private keys used to sign the transactions placed on blockchain are not managed properly, it will result in severe security attacks. Traditional measures like load balance, redundancy and anti-DDoS measures can solve the above issues.

51% Attack

Government and enterprises need to control their data access for their security purpose, it is a great concern while they adopting blockchain technology. Since the blockchain is transparent, it is difficult to implement with sensitive data. Blockchain is the network of people. Blockchain work under the assumption that honest nodes control the network. A miner's performance is based on the amount of computational power they have and this is usually referred to as hash rate or hashing power. Miners usually grouped together in mining pool so they can combine their mining power and become more efficient. If attacker nodes collectively control more computational power than the good ones in the network is so-called 51% attack. The attacker would be able to prevent new transactions from gaining confirmations to slow down or even completely prevent transactions between users. He would be also able to perform double spending. For preventing the above attack, organizations must ensure that there is no single miner or a group of miners or mining pools that are capable of controlling more than 50% of the network's mining hash rate. Random mining group selection technique can reduce the mining power of each miners and defend against 51% attack (Yang 2019).

Selfish Mining or block withholding

Miner attacker can produce their own blockchain privately by leveraging miner's power. A selfish miner achieves this by not announcing block to the network and receiving reward when they have discovered a block. So, the blockchain grow much faster and much longer as soon as attackers can present their blockchain to the public consensus mechanism. Using this block withholding strategy, the attacker can gain profit with 25% of total computational power.

Complexity

Since blockchain includes lots of mathematical complex calculations it is difficult to understand by beginners. If the blockchain makes the consensus mechanisms more complex, it may introduce new level of risks. Data integrity is directly linked to the security of the consensus mechanisms. So, enterprises need custom consensus mechanisms that requires thorough thinking to avoid the complexity in blockchain.

Initial costs for setup

For setting up blockchain in an organization in first time is very expensive as it is installed for specific enterprise and therefore the initial cost is very high. After setting up, only few resources are available, so the organization should need some experts to fulfill demand. So, they are paying high to hire the resources which are qualified.

Consumption of Energy

Miners spend a very large amount of mining power to solve the computations using proof-of-work algorithm to validate each and every transaction in the blockchain. This process is highly energy consuming.

Lack of in-house capabilities

Lots of enterprise deciding not to do anything with blockchain because of lack of in-house capabilities including skills and understanding. They believe that local expertise is not enough to implement blockchain system in their enterprise. User awareness program, traditional endpoint security measures, security update and anti-virus solutions are essential to solve this issue.

The adoption of blockchain with other technologies in an organization, there is a need of redesigning business and application workflow as well as adoption by all users.

Solutions and Discussions

Despite the challenges it has wide ranging possibilities and potential to enhance the quality-of-service delivery, while improving confidentiality and integrity of data. While adopting blockchain technology organizations mainly focusing on:

Private blockchain

It is actually deployed internally in the organization; it cannot be accessible by everybody whoever having internet access. Private blockchains are smaller and centralized networks and their membership is limited and closely operated and controlled by one entity. It can be able to mine the blocks in one minute or we can set fixed time duration. By comparing with the public blockchain, it is secure and scalable.

Permissioned blockchain

In this case it can control who has access or who can do changes in the blockchain. Each node in blockchain need permission to read the information on the blockchain, that limit the participants that can made transaction on the blockchain. Permissioned blockchain are large distributed network however they may or may not be based on open-source code. They operate under the leadership of a known entity that determines the role that individuals can play within the network.

Integration with multiple chain

Lots of enterprises currently leveraging multiple clouds and build integration and working together in one ecosystem.

Consortium blockchain

In this, the power does not reside with a single authority, it operated under the leadership of a group. There are two types of nodes in the network, validator nodes and member nodes. Here the control over the network is given only to a few predetermined nodes called validator nodes and only these nodes can take part in consensus mechanisms. The read access is public or restricted to a set of participants, this entirely depends upon the blockchain. So, it is s partially decentralized network, which is faster and provides higher scalability and transaction privacy.

Decentralized Application (Dapp)

It is an open-source application that operates autonomously on a decentralized public blockchain. It cannot be controlled any single entity, and it generates and uses tokens by following a standard cryptographic algorithm.

Consensus Algorithms

Enterprises uses blockchain with various consensus algorithms to protect themselves against 51% attack, such as Proof of Work, Proof of Stake and Delegated Poof of Stake. These algorithms make it very impractical for an attacker to successfully conduct a 51% attack. Blockchain uses a specific set of rules for generating new blocks, one of the rules to create a new block must be proportional to the total computing power of the proof of work mechanism.

This means that we actually own to have the computing power required to create a new block, which makes it very difficult and costly for an attacker to do. Since mining is so intense, the miners have a very strong incentive to keep mining honest rather than attempting a 51% attack or sybil attack.

***Figure 2.* Layers of blockchain architecture**

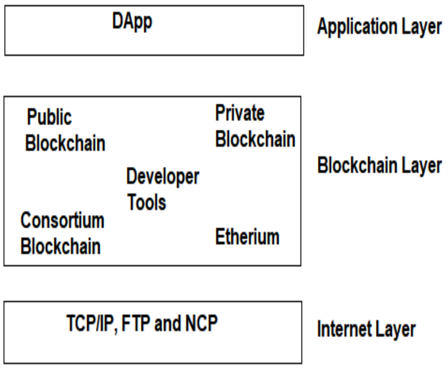

Figure 2 shows the layered architecture of blockchain- Application Layer, Blockchain layer and Internet Layer. The TCP/IP protocol is a set of rules that the end points in the telecommunication connection be used, when they communicate.

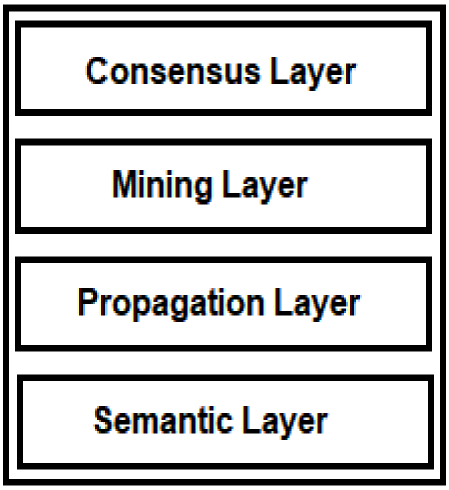

***Figure 3.* Blockchain Layer**

This paper proposes four layers inside the blockchain layer, that is shown in Figure 3. Consensus layer - decides on the methods of consensus and network participation where the network rules are applied to regulate the participants. Mining layer - will perform the mining operation, Propagation layer - manages the distribution of blocks and Semantic layer - decides how the newly created block related to the previous block in the network. Consensus layer decides on the methods of consensus and network participation where the network rule are applied to regulate the participants. There is a client application DApp that will invoke the smart contract and it will execute all nodes in the network. Client application can get all the transactions in the blockchain. It can also integrate other applications to trigger blockchain activity directly, for instance we can connect to IoT device to blockchain. Blockchain based solutions often bring together in many enterprises, which requires the development of common standards for data storage, processing and protection. This paper proposes some of the security measures to solve the risks and challenges in the blockchain technology.

- Every enterprise must have some expertise, they should have deep knowledge in blockchain technology.
- Define the organization goals, that should be synced with security goals of blockchain technology.
- Choose the type of the blockchain according to their need in their enterprise.
- Next is to find the risk and challenges in blockchain technology in their organization by performing risk assessment mechanisms.
- Define the security governance and control to prevent the risks in blockchain adoption in various application.
- The enterprises have to choose the security vendors to implement proper security measures. If an organization chooses the right architecture at the beginning, then the blockchain can foster privacy.
- After the implementation of security measures, the proper audit should be done regularly and monitor all the transactions properly.
- The software behind a blockchain has to be written perfectly, a coding error could make the blockchain vulnerable to attacks.

Conclusions

Blockchain is definitely a breakthrough in the digital financial world and it is going to be the stronger technology for future generations. So blockchain technology is revolutionary with the potential to improve or develop new systems in different industries and areas. This technology has already made great changes in the financial as well as the other fields in the world. In the future it is expected to grow more and surely its future is bright. Due to its immutability, traceability and transparency, blockchain can helps in reducing cost, inefficiencies and security threats. It creates new risks, while it significantly reduces some of the traditional risk. This new technology may involve unforeseen risks, so professionals must anticipate risk like never before and gear up for the same. The blockchain technology integrating with other existing systems is the key part of enterprise applications. It’s a comparatively young technology and that undergoes rapid improvement and a few of the most important problems are still remain today.

References

1. Akash Takyar, Blockchain in fake news - transforming news industry, https://www.leewayhertz.com/blockchain-fake-news/
2. Blackline Magazine, August 24, (2017), https://www.blackline.com/blog/rpa/why-care-about-blockchain-now/
3. Bellini E, Y. Iraqi and E. Damiani,(2020) "Blockchain-Based Distributed Trust and Reputation Management Systems: A Survey”, IEEE Access, vol. 8, pp. 21127-21151.
4. Cheng S, B Zeng and Y Z Huang, (2019) “Corrigendum: Research on application model of blockchain technology in distributed electricity market”, IOP Conf. Ser.: Earth Environ. Sci. 93, 012065.
5. ConsenSys, Blockchain in Institutional Capital Markets, https://consensys.net/blockchain-use-cases/capital-markets/

6. Sally Jasmin Sarma, May 24, (2018), Blockchain: A single version of the truth of an agreement, https://medium.com/@sally.sarma01/blockchain-a-single-version-of-the-truth-of-an-agreement-217637665ddf
7. Smetanin S., A. Ometov, M. Komarov, P. Masek, Y. Koucheryavy, “Blockchain Evaluation Approaches: State-of-the-Art and Future Perspective”, *Sensors (Basel),* 2020, *20,* 3358.
8. Wang L, X Shen, J Li, J Shao, Y Yang, (2019), “Cryptographic primitives in blockchains”, Journal of Network and Computer Applications, Volume 127, Pages 43-58.
9. Wikipedia, July 1, (2019), Single version of the truth, https://en.wikipedia.org/wiki/Single_version_of_the_truth.
10. Yang X., Y. Chen and X. Chen, (2019), "Effective Scheme against 51% Attack on Proof-of-Work Blockchain with History Weighted Information," *IEEE International Conference on Blockchain,* Atlanta, GA, USA, pp. 261-265.
11. Yeoh, P., (2017), "Regulatory issues in blockchain technology", Journal of Financial Regulation and Compliance, Vol. 25 No. 2, pp. 196-208.
12. Zhang R. , R. Xue, L. Liu, (2019), “Security and Privacy on Blockchain”, *ACM Computing. Surveys*. Article 1.
13. Zheng, H. Xie,X. Dai, Chen, H. Wang, (2017), "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”, IEEE International Congress on Big Data, Honolulu, HI, USA, pp 557-564.
14. Zheng Z., S Xie, Hong-Ning Dai, X Chen, H Wang, (2018), “Blockchain challenges and opportunities: a survey”, International Journal of Web and Grid Services (IJWGS), Vol. 14, No. 4.