International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 07 | July 2020 www.irjet.net p-ISSN: 2395-0072

AN INTRODUCTION TO BLOCKCHAIN TECHNOLOGY

Haritha R[1], Shyma Kareem[2]

[1]*Student, Master of Computer Application, Department of CSE, Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, India*
[2]Assistant. Professor, *Department of CSE, Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, India*

Abstract - *Blockchain is a technology that was born with the cryptocurrency Bitcoin and that can provide secure communications, data privacy, resilience, and transparency. A blockchain acts as a distributed ledger-based on a chain of data blocks linked by hashes that allow for sharing information among peers that do not necessarily trust each other, thus providing a solution for the double-spending problem. Such features have popularized blockchain in the last years and it has already been suggested as a key technology. Blockchains are tamper-resistant digital ledgers implemented in a distributed fashion and usually without a central authority. In contrast with the conventional processes, in Blockchain, there are multiple shared copies of an equivalent database which makes it challenging to wage a data breach attack or cyber attack. Anything that is built on the blockchain is by its very nature transparent and everyone involved is responsible for their actions. This technology has become the backbone of a new type of internet by allowing the distributed information. Originally devised for the digital currency, Bitcoin, (Buy Bit coin) the tech community has now found other potential uses for the technology for different applications related to smart health, measuring systems, and logistics, e-voting, or smart factories.*

Key Words: Blockchain, Bitcoin, Peer to Peer Architecture, Public Key Cryptography, Hashing, Digital Signature, Merkle Tree, Consensus Protocol, Proof of Work, Proof of Stake.

1. INTRODUCTION

In 2008 a pseudo name Satoshi Nakamoto introduced a cryptocurrency Bitcoin [3]. Along with open-source Bitcoin software, the underlying technology Blockchain was also released later in 2009. Blockchain technology is showing a significant potential to disrupt several information technology domains. With its biggest success, the Bitcoin system, blockchain technology has drawn attention to its distinct features, including decentralization, transparency and openness, immutability and tamper detection, provenance, peer-to-peer (P2P) transactions, smart contracts, incentive mechanisms, distributed ledger technology, correctness, support of cryptocurrencies, and threatening users from double-spending[1]. Any transactions are completely recorded in the public ledger in a permanent and verifiable way. Blockchain technology has massive potential to convert the working methodologies of several industries and government organizations [2]. Besides the financial industry, we have also seen a significant rise of interest in blockchain technology in other domains [5], [6]. This interest has become evident in complex engineering domains such as energy and the Internet of Things (IoT). The key components of a blockchain system include: 1) linked linear data structures to incrementally append data items (termed as transactions) in existing valid blockchains, 2) cryptographic algorithms to generate hash keys to anonymously access the data items on the blockchain, 3) consensus algorithms to ensure the validity of changes in already stored data, and 4) message passing protocols to enable P2P communication over the underlying network. Blockchain technologies use a variety of consensus algorithms such as proof-of-work [7], proof-of-stake [4]. Comparing to traditional payment systems such as Visa, PayPal, and so on; Bitcoin is very much time-consuming. But as blockchain works in a decentralized and distributed peer-to-peer network, it has no third-party involvement to control over the assets of customers, and the powerful computers involved in the mining process are contributing in securing the blockchain bit by bit, the blockchain-based systems are considered as safe, secure and reliable. Furthermore, it also provides a tamper-proof ledger of technologies by replicating the same copy of the blockchain in the overall network. However, this security and elimination of third-party involvement have to pay in terms of delayed transactions for maybe a long period, currently, there are thousands of transactions are pending in memory pool. To overcome the latency issues still preserving the security and discouraging third-party involvement, several platforms have come into play. Most of those platforms are using blockchain technology by relaxing its time consuming and processing hungry PoW algorithm [10].

1.1 Background

Blockchain is a public ledger to record all the transactions over the peer-to-peer network, the transactions are waiting for a specified time in the memory pool, which is a shared memory space of all the nodes in the network to get bundled as a block. Once the block is generated it gets signed by cryptographic signature also known as a hash, blockchain in Bitcoin uses SHA256 (Secure Hash Algorithm) a cryptographic hash function to secure the transactions [8]. After block generation it is forwarded to the network, all of the nodes of the blockchain network can participate in the competition of mining the block to discover the correct hash

key by iterating through different nonce each time. The miner who successfully finds out the correct nonce broadcasts the nonce and block to the network as their Proof-of-Work (PoW), where the other nodes in the network verify the block by applying the received nonce, if the block is correct it is added to the main blockchain, and if not then it is discarded, this verification process is known as Consensus [9]. The miner whose block is added to blockchain receives a reward in terms of freshly released bitcoins for his efforts [10]. The addition of a new block in blockchain works as a data structure, where every new block is referenced to its previous block.

Once the block is added to the blockchain it is probabilistically impossible to edit or delete that block. In Bitcoin, every 10 minutes a new block is added to the blockchain, thus tampering with existing block requires incredible computation power to mine all the succeeding blocks before the addition of another new block. The mining operation is an expensive operation, in Bitcoin, the complexity of the mathematical puzzle of generated hash is adjusted after every 2 weeks [11]. The addition of the latest hardware technologies to speed up the mining process has increased the difficulty level of the mathematical puzzle so that a normal computer would take more than a year to solve it, this is the reason why ASIC machines have come in to play [12]. There are 144 blocks added every day in blockchain, the average number of transactions per block depends on the number of transactions that can fit in 2 MB of memory. A single transaction roughly requires 570 bytes, which means the number of transactions is approximately 3500 per block [13].

1.2 Bitcoin Concept

Bitcoin is a digital currency and payment system introduced by the pseudonymous Satoshi Nakamoto in 2008 [14]. The system functions as a peer-to-peer decentred network in which payments are sent directly between the parties involved, instead of relying on central institutions to settle payments. Bitcoin uses cryptographic proof to make this happen. Hence, Bitcoin is also considered to be a cryptocurrency.

Each user in the Bitcoin network owns public and private key pairs. Bitcoin value is associated with a chain of transactions in which each transaction consists of the private key signature of the hash of the input transaction and the payee's public key. If the payer wants to send these Bitcoins to the payee owning a public/private key. To do so, the payer takes the hash of the input transaction – proof that he/she owns the Bitcoin value – and the public key of the payee. He/she then hashes these values and signs the hash with its private key, thus creating a new transaction to the payee. The transaction consists of the hash of the input transaction, the output address, and the payer's signature. Since only the payer has the private key corresponding to the public address, (s)he is the only one capable of generating a transaction for this address via signing, thus spending the Bitcoin value associated with this address. To avoid double-spending of Bitcoins, the system adopts blockchain as the public ledger.

2. KEY ELEMENTS OF BLOCKCHAIN

2.1 Peer to Peer Architecture

A peer-to-peer (P2P) network is a group of computer systems in which they can share information and resources. Instead of having a central server to act as a shared drive, each computer acts as the server for the files stored upon it. In peer to peer architecture, all the autonomous and distributed system is aggregate in a large number of heterogonous nodes called peers, which incorporate each other to fulfill some objectives. Blockchain technology works on the principle of P2P architecture which helps the technology to be more secure and efficient. Blockchain technology can be used in many industries but mostly used is 'Cryptocurrencies'. A P2P network is a central point when it comes to doing a transaction within a blockchain. All the nodes can transact with each other in the blockchain. Now, all the P2P networks are decentralized and that is why blockchain is also known as decentralized applications. This characteristic makes blockchain more secure and hard to hack or break into.

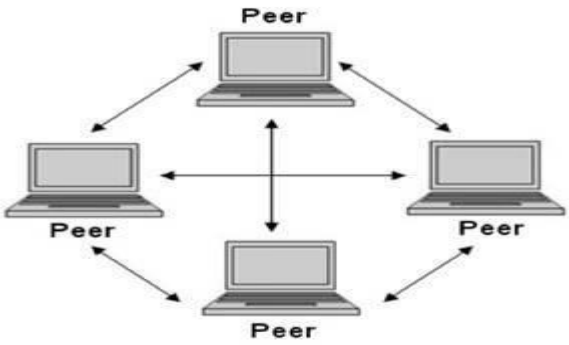

Fig -1: Peer to Peer Architecture

2.2 Public Key Cryptography

Blockchain users interact securely with the blockchain by leveraging public-key/asymmetric cryptography. Public-key cryptography is also essential for the so-called wallets, which are private key containers that store files and simple data. Thus, in a blockchain system each user has a wallet that is associated with at least a public address (usually a hash of the user public key) and a private key that the user needs for signing transactions. For instance, in blockchains like Bitcoin every transaction ends up being 'sent' to the public address of the receiver and is signed with the private key of the sender. In order to spend bitcoins, their owner has to demonstrate the ownership of a private key. To verify the authenticity of the received currency, every entity that receives bitcoins

verifies its digital signature by using the public key of the sender.

2.3 Hash Function

Information security uses cryptography on several levels. The information cannot be understood without a key to decrypt it. The information maintains its integrity during conversion and while being stored. Cryptography also aids in nonrepudiation. This means that the sender and the delivery of a message can be verified.

Hash functions like SHA-256 is commonly used by blockchains because they are easy to check, but really difficult to forge, thus allowing the generation of digital signatures that blockchain users need to authenticate themselves or their data transactions in front of others. When a user sends a secure message, a hash of the message is generated and encrypted, and is sent along with the message. When the message is received, the receiver decrypts the message and hash value. Then, the receiver creates another hash from the received message. If the two hashes are same, then a secure transmission has occurred. This process ensures that the message is not altered by an unauthorized end user.

Hash functions are also used by blockchains to link their blocks (i.e., groups of transactions that are considered to occur at the same time instant). Such blocks are linked in chronological order, containing each block the hash of the previous block. Finally, it is worth mentioning that hash functions are used in blockchains for generating user addresses (i.e., user public/private keys) or for shortening the size of public addresses [16], [15].

2.3 Digital Signature

Digital Signatures are used for authentication where private key is used for signing and public key is used for verification**.** A blockchain usually makes use of public-key cryptosystems for securing information exchanges between parties by authenticating transactions through digital signatures. During the signature process, the signer signs with a private key, while the public key, which is shared publicly, is used to verify that the signature is valid. Thus, when a signing algorithm is secure, it is guaranteed that only the person with a private key could have generated certain signature. Initially a message is signed with digital signature by sender before transmitting to recipient. It also contains hash of values to detect illegal modifications by malicious human intermediaries.

Digital Signature Algorithm (DSA) has been used for transmission of electronic funds, interchange of data, distribution of software, storage of data Digital signature's security depends upon the private key of the signer. Digital signature consists of the signature generation and verification algorithms. Comparing with the physical signature, digital signature has the capability that, it cannot be changed nor copied by someone else, and also the signers of the signature cannot repudiate signature later.

2.4 Merkle Tree

The cryptographic hash function employed by Bitcoin is the SHA-256 algorithm. This stands for "Secure Hashing Algorithm", whose output is a fixed 256 bits in length. The basic functions of Merkle trees in Bitcoin are to store, and eventually prune transactions in every block. Merkle trees are created by continuously hashing pairs of nodes until there is only one hash left (this hash is called the Root Hash, or the Merkle Root. They are constructed from rock bottom up, from hashes of individual transactions.

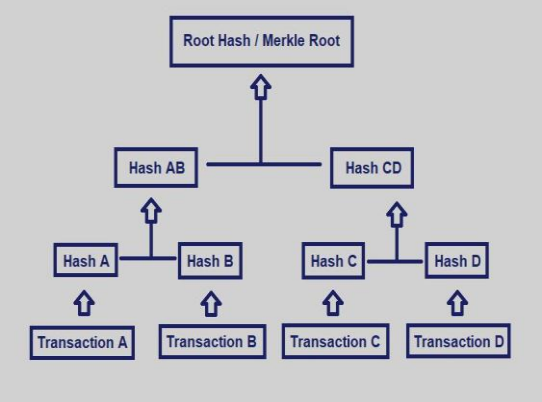

Fig -2: Peer to Peer Architecture

Four transactions in a block: A, B, C, and D. Each of those is hashed, and therefore the hash stored in each leaf node, leading to Hash A, B, C, and D. Consecutive pairs of leaf nodes are then summarized in a parent node by hashing Hash A and Hash B, resulting in Hash AB, and separately hashing Hash C and Hash D, resulting in Hash CD. The two hashes (Hash AB and Hash CD) are then hashed again to supply the basis Hash (the Merkle Root).This process are often conducted on larger data sets, too: consecutive blocks are often hashed until there's just one node at the highest . Hashing is typically conducted using the SHA-2 cryptographic hash function, though other functions also can be used. The Merkle Root summarizes all of the info within the related transactions, and is stored within the block header. It maintains the integrity of the data. Using a Merkle tree allows for a fast and straightforward test of whether a selected transaction is included within the set or not.

3. CORE COMPONENTS OF BLOCKCHAIN

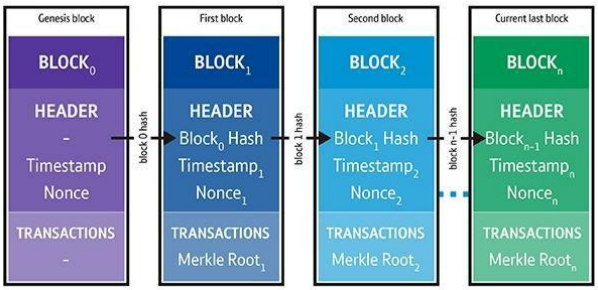

Fig -3: Component of Blockchain

1. Node

User or computer within the blockchain architecture (each has an independent copy of the entire blockchain ledger).

2. Block

A data structure used to keep a group of transactions distributed to all nodes in the network. It includes data, block header, Time stamp (when block is created), version of blockchain, hash of the block, Merkle root, Proof of work that used to verify the block.

3. Chain

A sequence of blocks in a specific order.

4. Miners

Specific nodes which perform the block verification process before adding anything to the blockchain structure.

5. Consensus

A set of rules and arrangements to carry out blockchain operations.

4. WORKING

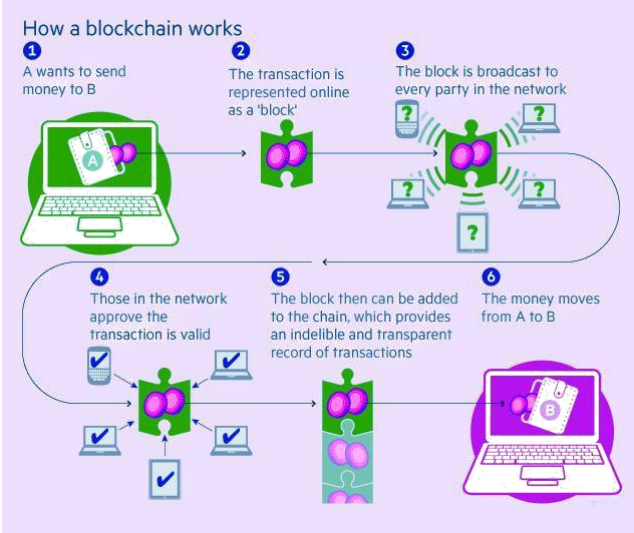

Fig -4: Working of Blockchain

When the individual transfer money the following things will happen:
1. That request for the transaction first represents online to the block itself.
2. Once that information receives by the block then it again sends to the parties of the users.
3. Once this request received by the parties it then analyzed and approved by all the parties.
4. After approval of request that new block can now officially added to the chain.
5. After adding block money is transferred to the second individual.

4.1 Consensus Algorithm

A consensus algorithm may be a procedure through which all the peers of the Blockchain network reach a standard agreement about this state of the distributed ledger. In this way, consensus algorithms achieve reliability within the Blockchain network and establish trust between unknown peers during a distributed computing environment. Essentially, the consensus protocol makes sure that each new block that's added to the Blockchain is that the one and only version of the reality that's prescribed by all the nodes in the Blockchain. The Blockchain consensus protocol consists of some specific objectives like coming to an agreement, collaboration, co-operation, equal rights to each node, and mandatory participation of every node in the consensus process. Thus, a consensus algorithm aims at finding a standard agreement that's a win for the whole network. Consensus algorithm is the most important factor of the entire blockchain system, for the reason that its efficiency determines the blockchains performance directly.

With the continuous development of blockchain technology, the consensus algorithm is constantly adapting to the emerging requirements from the earliest Proof of Work (PoW) to the later Proof of Stake (PoS), Delegated Proof of Stake (DPoS) [19], Practical Byzantine Fault Tolerance (PBFT) [18] and some other improved consensus algorithms such as Proof of Burn (PoB) [21], Proof of Activity (PoA) [22], Proof of Luck (PoL) [20], and Stellar Consensus Protocol) (SCP) [23]. The computation cost, security and consensus efficiency of the above are different [17]. Performance of blockchain networks significantly relies on the performance of the adopted consensus mechanisms, e.g., in terms of data consistency, speed of consensus finality, robustness to arbitrarily behaving nodes (i.e., Byzantine nodes [25]) and network scalability. Compared with the classical Byzantine consensus protocols allowing very limited network scalability [25], [26]

4.1.1 Proof of Work

Proof of Work (PoW) mechanism, first used for spam filtering, now is applied to achieve the consistency of node data in Bitcoin. And if a participant wants to generate and write a new block into the blockchain in the Bitcoin system, it must solve the puzzle of proof-of-work given by the blockchain network. PoW competes to generate blocks through owning more computing resources than others. In order to add blocks to a blockchain, some proof of work has to be communicated. Bitcoin uses PoW concept as consensus mechanism, which scales over 1000 of nodes. PoW requires the initiator to solve a puzzle, a mathematical or cryptographic operation by brute forcing and to produce a value (also called wining value), which is less than a defined one as set forth by the network. At times, more than one node produces winning value at the same time to add block and thereafter ask for reward. This situation creates a fork and is resolved by the network by analyzing the maximum value of prove-of-work i.e. maximum work done by a node. The update request by the node with minimum proof-of-work is discarded. This way the consistency of state among all nodes is ensured. PoW fits best for those networks that requires scalability. Mostly permission less blockchains utilize PoW as they have authenticity of the participating node, as a result the network size becomes very large. It suffers from few drawbacks, it requires every node to invest huge amount in purchasing equipment used in the mining process. It is more vulnerable to attack because of its open nature. It supports very low transaction rate of only 7 per second, which is far less as compared to Visa or Master card, which offers 10000 transactions per second. In case of fork, the transaction confirmation takes too much time. Beside it requires significant energy expenditure, and high latency; however, to ensure safety of consensus process, the operation is quite acceptable.

4.1.2 Proof of Stake

Proof of Stake (PoS) was firstly implemented by Sunny King's Peer coin and its mining difficult is adjusted based on the number of stakes held by workers. Simply put, the more stakes you have, and the easier it is to generate the block. PoS are an improved version of PoW, based on the assumption that the people with more stakes will not attack the network. Although PoS is more energy saving and efficient than PoW, the assignment mechanism to generate blocks is extremely unfair, for the reason that the assignment in PoS is based on the number of stakes the node owning [24].

5. APPLICATIONS

5.1 Internet of Things

The internet of things was by far the most popular "application" field. IoT was initially discussed, with blockchains ability to leverage its user privacy protection through public key anonymization which was identified as a valuable resource for maintaining privacy in a future with millions of interconnected devices sharing data and engaging in constant communication. Furthermore, the decentralized and immutable nature of the blockchain ledger allows IoT based devices quick, easy and distributed access to the information while permitting constant contributions and additions to the data set from various parties due to the integral security of the information. Finally, smart contracts were found very valuable in allowing IoT devices to interact directly with one another, helping further push the boundaries of automation and remove steps of human intervention from the process of communications and processing.

5.2 Energy

Blockchain research on energy predominately focused on the usefulness of blockchains decentralized nature in democratizing the energy supply and demand industry while accommodating a more scalable and flexible solution for the world with consumers alternating as providers on the energy grid. The blockchains privacy and anonymity features allow for the induction of multiple consumers and providers in the market and the creation of micro grids within the energy sector while preserving the data consumption and pricing preferences of the individuals engaging in the transactions. Finally, smart contracts allow the energy sector to automate and self-execute transactions between the various participants, enabling machine to machine interactions and allowing government authorities to reliable identify green energy sources and provide the appropriate motivation incentives to their producers.

5.3 Finance

In Finance, blockchains decentralized ledger allows for easy and convenient access to user's financial information from multiple locations while limiting the impact and loss of wealth and information due to the shutdown or bankruptcy of a central authority. The decentralization also allows global currencies tied to international market values rather than national banks and currency systems. Furthermore, the ability to anonymize transactions and maintain privacy allows for greater interaction between the various parties within the financial system and facilitates the exchange of goods and services directly between individuals rather than through businesses as the private identity is kept confidential while allowing a secure exchange. Smart contracts allow the creation of level 3 ledgers capable of not only executing certain financial contracts and commitments but also automating the execution process and criteria given preset conditions and values, thereby allowing a more sustainable and flexible financial system.

5.4 Healthcare

Blockchain is also suggested as a method to spur and grow innovation in the healthcare sector, with the decentralization of patient data allowing users immediate and quick access to their important medical information from anywhere in the world rather than having to go through the service provider, furthermore, the immutability of the ledger would allow patients and their health service providers to freely update the ledger without concerns over data integrity and any party modifying the information for nefarious purposes. This will also increase accountability in the medical field, as mistakes would not be hidden; in addition, the enhanced privacy and anonymity of interaction within the blockchain will strengthen doctor-patient confidentiality while also allowing medical professionals open access to massive amounts of medical data previously walled off for privacy concerns.

5.5 Government

Whether through aspects of eGovernment, digital identity, voting or measuring instruments; governments stand to gain significantly from the potential of blockchain applications. Through the decentralization of the dataset, governments can expand and enhance the quality of their services by removing the need for database administration and maintenance. It will also allow for proper digital voting as it solved the important problem of entrusting the voting data in the hands of a single company or database with the motivation to manipulate the information. Decentralization will also help better run measuring instruments and the data they capture and run by removing the obstacle of costly computing and storage equipment and securing the information from manipulation through the blockchain, the immutability will also allow for the creation of a proper digital identity capable of removing the obligation of physical proof documents as the ledger will be trustable enough to confirm the information. The enhance privacy through public/private keys will allow the government to more freely grant access to its data to other government agencies and research groups allowing for a better understanding of current problems and proposals of solutions as needed. The added privacy will also improve the voting process by providing regulators and the government access to all voting information but maintaining the private identity of the voters themselves. Smart contracts will help alleviate the bureaucratic process of government systems by simplifying multi-step basic procedures thereby improving the overall efficiency and quality of services provided.

5.6 Blockchain in Cloud – Outsourcing

Blockchain solutions are adopted in cloud computing, such as, in the author adopted blockchain for providing trusted solution for outsourcing of services and for their customer's secure payment. Trust is a real concern in cloud computing adoption. However, by enabling blockchain underlying the cloud services it will strengthen the outsourcing business and will get more customers. Similarly, in the author has given more detailed analysis and results regarding the trusted payment system among the users and outsourcing service providers.

5.7 Vehicular Industry

Automobile industry is also adopting blockchain technology due to its cutting edge benefits. Volkswagen has shown the use of IOTA Tangle system for autonomous cars. BMW is using blockchain technology for managing its asset and logistics. BMW, Ford, Renault and General Motors are among the 30 companies in Mobility Open Blockchain Initiative (MOBI) along with IBM, Bosch and Blockchain at Berkeley. MOBI's mission is to accelerate the adoption of blockchain and to make sure that the industry is on the same page, not only by changing the mode of transportation, but also through use cases ranging from autonomous payment to ride sharing .Toyota is investing in blockchain supply chain management since 2016 through R3CEV consortium.

Renault working on its car passport system based on blockchain suggests Blockchain technology is also effective in tracking vehicles transporting goods. It will allow all stakeholders involved in transporting process to check relevant data and status while providing traceability and transparency. However, in best of our knowledge there is no work so far which uses blockchain technology for vehicle life cycle tracking. The authors of this paper are currently working on a project related to implementing a blockchain based prototype system for vehicle life cycle tracking in Saudi Arabia. The project consists of designing and implementing a complete life cycle of vehicle tracking, starting from manufacturing, customs, registration,

violations to buying and selling. We designed a secure and transparent architecture over selected blockchain platform.

6. ADVANTAGES

- Accuracy of the Chain
- Cost Reductions
- Decentralization
- Efficient Transactions
- Private Transactions
- Secure Transaction
- Transparency

7. DISADVANTAGES

- Speed Inefficiency
- Illegal Activity
- Cost
- Central Bank Concerns
- Hack Susceptibility

8. CONCLUSION

Blockchain can be considered as the newest technology stressing the paradigms of "Internet of Things", icollaboration, artificial intelligence, technostress, and the dark side of digital innovations. Blockchain seems to have stung all industries and created a buzz-seeking opportunity for enhanced business processes and building trust. Yet, some industries such as the financial sector might see it as a disruptive technology that cannot be avoided and needs to be managed. Blockchain technology does offer a promising future; it has likely suffered from the hype of its potential applications. This hype opened the door for questionable and fraudulent enterprises claiming Blockchain technology as their core business. While this may have eroded some trust and confidence particularly in the finance and technology sectors, it has offered the benefit of increasing public attention and interest in the topic. Consequently, it has provided an incentive for academic research into its technical aspects and applications.

REFERENCES

[1] M. H. U. Rehman, K. Salah, E. Damiani and D. Svetinovic, "Trust in blockchain cryptocurrency ecosystem", IEEE Trans. Eng. Manag.

[2] K. Bheemaiah, Why Business Schools Need to Teach About the Blockchain, Grenoble, France:Global Ecole De Management, 2015, [online] Available: https://ssrn.com/abstract=2596465.

[3] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, [online] Available: http://www.bitcoin.org.

[4] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake", Aug. 2012, [online] Available: https://www.semanticscholar.org/paper/PPCoin%3A-Peer-to-Peer-Crypto-Currency-with-King-Nadal/0db38d32069f3341d34c35085dc009a85ba13c13.

[5] K. Salah, M. H. U. Rehman, N. Nizamuddin and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges", IEEE Access, vol. 7, pp. 10127-10149, 2019.

[6] M. Nassar, K. Salah, M. H. ur Rehman and D. Svetinovic, "Blockchain for explainable and trustworthy artificial intelligence", WIREs Data Mining Knowl. Discovery, vol. 10, pp. e1340, Oct. 2019.

[7] I. Bentov, C. Lee, A. Mizrahi and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]", ACM SIGMETRICS Perform. Eval. Rev., vol. 42, no. 3, pp. 34-37, Dec. 2014.

[8] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things", IEEE Access, vol. 4, pp. 2292-2303, 2016.

[9] G. Seibold and S. Samman, "Consensus immutable agreement for the Internet of value", 2016, [online] Available: https://home.kpmg/cn/en/home/insights/2016/09/blockchain-consensus.html.

[10] R. A. Memon, J. Li, J. Ahmed, A. Khan, M. I. Nazir and M. I. Mangrio, "Modeling of blockchain based systems using queuing theory simulation", Proc. 15th Int. Comput. Conf. Wavelet Active Media Technol. Inf. Process. (ICCWAMTIP), pp. 107-111, Dec. 2019.

[11] R. A. Memon, J. P. Li and J. Ahmed, "Simulation model for blockchain systems using queuing theory", Electronics, vol. 8, no. 2, pp. 234, Feb. 2019.

[12] M. Jabłczynska, K. Kosc, P. Ryś, R. Ślepaczuk, P. Sakowski and G. Zakrzewski, Why you should not invest in mining endeavour? The efficiency of BTC mining under current market conditions, Warsaw, Poland, 2018.

[13] Trending Blockchain Cryptocurrency, Apr. 2019, [online] Available: https://cryptoslate.com/.

[14] Bitcoin Core Developers Bitcoin Core, Jan. 2017, [online] Available: https://bitcoincore.org/.

[15] L. Wang, X. Shen, J. Li, J. Shao and Y. Yang, "Cryptographic primitives in blockchains", J. Netw. Comput. Appl., vol. 127, pp. 43-58, Feb. 2019.

[16] M. Raikwar, D. Gligoroski and K. Kralevska, "SoK of used cryptography in blockchain", Sep. 2019.

[17] Z. Yan, G. GuoHua, D. Di, J. Feifei and C. Aiping, "Security architecture and key technologies of blockchain", J. Inf. Secur. Res., vol. 2, no. 12, pp. 1090-1097, 2016.

[18] M. Castro and B. Liskov, "Practical Byzantine fault tolerance", Proc. Symp. Operating Syst. Design Implement, pp. 173-186, 1999.

[19] T. Y. Song and Y. L. Zhao, "Comparison of blockchain consensus algorithm", Comput. Appl. Softw., vol. 25, no. 8, pp. 1-8, 2018.

[20] M. Milutinovic, W. He, H. Wu and M. Kanwal, "Proof of luck: An efficient blockchain consensus protocol", Proc.

1st Workshop Syst. Softw. Trusted Execution, pp. 2, Dec. 2016.

[21] Slimcoin: A Peer-to-Peer Crypto-Currency with Proof-of-Burn (Mining Without Powerful Hardware), May 2014, [online] Available: http://www.doc.ic.ac.uk/~ids/realdotdot/crypto_papers_etc_wortw_reading/proof_of_burn/slimcoin_whitepaper.pdf.

[22] I. Bentov, C. Lee, A. Mizrahi and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake", ACM SIGMETRICS Perform. Eval. Rev., vol. 42, no. 3, pp. 34-37, 2014.

[23] D. Mazires, the Stellar Consensus Protocol: A Federated Model for Internet-Level Consensus, Jul. 2015, [online] Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.696.93&=&rep=rep1&=&type=pdf.

[24] Z. B. Zheng, S. A. Xie, H. N. Dai, X. Chen and H. Wang, "An overview of blockchain technology: Architecture consensus and future trends", Proc. IEEE Int. Congr. Big Data, pp. 557-564, Jun. 2017.

[25] F. B. Schneider, "Implementing fault-tolerant services using the state machine approach: A tutorial", ACM Comput. Surv., vol. 22, no. 4, pp. 299-319, Dec. 1990.

[26] M. Castro and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery", ACM Trans. Comput. Syst., vol. 20, no. 4, pp. 398-461, Nov. 2002.