JACET

J. ADV COMP ENG TECHNOL, 6(4) Autumn 2020

Development of Blockchain Technology

Behnam Kiani Kalejahi[1], Jala Quluzada[2], Sabnam Maharrəmli[3]
1- Department of Biomedical Engineering, Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, IRAN. (bkiani@khazar.org)
2,3- Department of Computer Science, School of Science and Engineering, Khazar University, Baku, Azerbaijan.

Received (2020-11-22) Accepted (2021-01-16)

Abstract: *Blockchain technology is the first successful Bitcoin Network. It enables the ledger to become more decentralized and secure. Since it is not limited to bitcoin and controlled by third parties by government, corporations, or banks, the technology is capturing several industries, including cryptocurrency, infrastructure& hardware, financial technology, Internet & mobile and so on. Blockchain is used as a public ledger to verify all peer-to-peer system transactions and maintain traded bitcoin spending from central authorities while bitcoin has distributed transactions. Achieving high Blockchain-based performance and privacy & security are global issues that are desire to be overcome as claims show they are still significant challenges in many Blockchain applications. This paper presents an introduction to Blockchain and the process of this technology in the way of outlining Blockchain types. Also, recent advances, challenges, real economy integration, and current situations of this technology have been listed.*

Keywords: *Blockchain, transaction, nodes, privacy, scalability, consensus, future directions.*

How to cite this article:
Behnam Kiani Kalejahi, Jala Quluzada, Sabnam Maharrəmli. Development of Blockchain Technology. J. ADV COMP ENG TECHNOL, 6(4) Autumn 2020 : 265-272

I. INTRODUCTION

Nowadays, healthcare systems are substantially getting high experienced through intensive improvements, reforms, and other global interventions. No matter what is discussed, it is evident that the healthcare industry is one of the slowest growing among all particular industries. Hence, it is impossible to underestimate the importance of healthcare, and it had better not to say that no innovative changes have been done over the past years. The opportunities presented by governmental and non-governmental organizations to a foreseen future technology-based community with economic uncertainties and epidemiological instabilities play an important and sustainable role in the healthcare system. More specifically, today's society applies one of the relevant principles: qualitative and quantitative approaches to socio-economic determinants, mainly defined as a part of health and disease. It focuses on collective responsibility and the whole of the state population, partnership with people's clinical services. However, new technological improvements help to access healthcare with more complete and innovative alternatives.

Healthcare data make healthcare much more efficient in advance in big data analysis as the privacy of health information, and basically, it reduces the costs in financial services. With concrete acquired information based on healthcare data, the high quality of patient care will effectively increase. Big data targets to analyze patients' and consumers' physical and clinical data to remove traditional data processing. It is also preferable to use data analysis to determine the rise of value-based

care and reduce the time complexity in full health services. Big data also helps medical professionals and doctors predict precise treatments and diagnoses to improve patients' healthcare. It allows doctors to make decisions to identify possible serious problems quickly.

One of the most available technologies is Blockchain, which deals with writing entries in the record of data information and preventing manipulation in the subsequent blocks. By using this decentralized digital ledger, each user can check extensively recorded information linked via health data. More precisely, Blockchain is a systematically structured method of record keeping and transactions. It is almost used in the Business sector, Education, Healthcare, Digital Marketing, Retail, and Information Technology. Blockchain helps the healthcare industry follow the transformation of systems and transactions that are stored across all network resources. Particularly regarding its essential advancements in technology, it may propose developing integration, increased efficiency, privacy, security, and other opportunities. Now, we are going to look upon the following effective determinants of Blockchain. In this paper, we will focus on Blockchain, challenges and recent advances in terms of scalability and privacy leakage, consensus algorithm, the current situation of this technology, real economy integration, and finally, conclusion.

Blockchain is jointly distributed, a particular subset of DLTs cryptographic techniques and decentralized digital ledger, enabling data tamper-proof and mainly data shortage consistency. It assures to keep records instead of one knowing each ledger is decentralized. There is no central control, making transactions efficiently managed without third parties such as regulatory agencies and local banks. Blockchain is the most widely recognized element of DLTs in which this subset synchronizes and records in terms of chains of blocks. All DLTs are not Blockchains. Blockchain is simply a chronological database with a chain of blocks containing hashes that show entire and previous blocks.

The role of hashes in data is to link each block's components to get a chain of blocks and create security for the Blockchain data. However, if the block's hash value is changed, all other subsequent blocks will completely be altered with other sequences meaning that all will be invalid. The hashes also contain a minimum required number of zero that determines how difficult the data is for blocks. The nature of every block replicates the hash value of the previous block by starting the same number of zeros. Synchronized and constantly updated records build Blockchain's foundation, and their transactions are shared through a network. The content of each block with its records should be changed and calculated in Blockchain data with all other subsequent hashes. Thus, through the consensus mechanism, all distributed network users have a copy version of the public ledger followed under some rules even if they do not trust each other. The reason behind this offered set of rules is to validate the transaction in a new block. The record nodes in verification aim to check what other nodes and the latest block participate. Once exponential data changes inside happen through unauthorized alterations, it possibly becomes more complicated to resolve by simply using basic computers. In case the data is allowed to be confirmed, then it cannot be deleted and changed. Therefore, the Blockchain is more practically secure, efficient, tamper-proof, and intuitively permanent.

It is applicable to distinguish Blockchain's functionality and base structure in terms of validating transactions, read access, and execute transactions. Blockchain is whether permissionless or permissioned depends on transactions how an individual validates and sends them or how entities are authorized to validate and execute them, or separately. Blockchain can also be defined as private only if authorized individuals can read and access Blockchain contents. If it is used publicly for anyone, a Blockchain can be readable and accessible.

This table gives the overall details about an example of Blockchain types, which are categorized as both public permissionless and permissioned Blockchains, also categorized as private permissionless and permissioned Blockchains. The blue-colored dots describe those who cannot participate in the validation system; instead, they are counted in the network. Conversely, yellow-colored dots demonstrate nodes that can participate in a consensus mechanism and can validate system transactions.

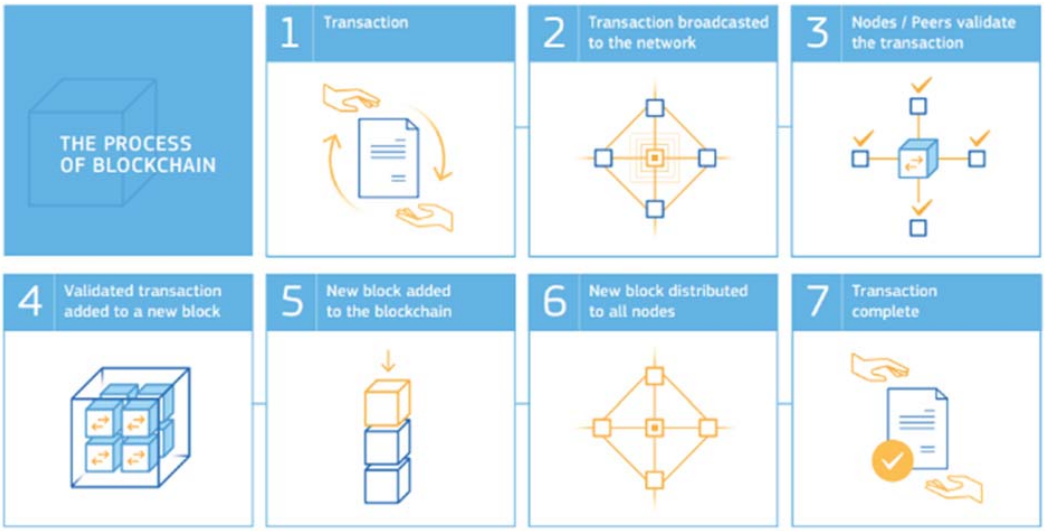

Fig.1. Process of blockchain

Blockchain type	Explanation	Example	Visualisation
Public permissionless blockchains	In these blockchain systems, everyone can participate in the blockchain's consensus mechanism. Also, everyone worldwide with an internet connection can transact and see the full transaction log.	Bitcoin, Litecoin, Ethereum	
Public permissioned blockchains	These blockchain systems allow everyone with an internet connection to transact and see the blockchain's transaction log, although only a restricted number of nodes can participate in the consensus mechanism.	Ripple, private versions of Ethereum	
Private permissioned blockchains	These blockchain systems restrict both the ability to transact and view the transaction log to only the participating nodes in the system, and the architect or owner of the blockchain system is able to determine who can participate in the blockchain system and which nodes can participate in the consensus mechanism.	Rubix, Hyperledger	
Private permissionless blockchains	These blockchain systems are restricted in who can transact and see the transaction log, although the consensus mechanism is open to anyone.	(Partially) Exonum	

Fig. 2. Examples of Blockchain types

In addition to a blue circle, it indicates that transactions can be observed only by nodes on the circle. Having no blue circle means anyone can access and read Blockchain's transaction history through an internet connection.

II. CHALLENGES AND RECENT ADVANCES

Blockchain fundamentally has a great potential to manage every possible sector; instead, this technology's usage has some limits based on associated advances and challenges.

Privacy Leakage: Even though Blockchain controls the privacy considering public and private keys, users still conduct public and private keys without any identities. A recent study shows that their Bitcoin transactions can reveal users' private information. The values of balances for a public key are easily seen, and transactional privacy has no guarantee [1],[2]. In addition to the research, a method to connect a user's IP address with a pseudonym developed by professor cryptographer Alex Biryukov [3] was offered if the user is in a firewall network in which this system prevents unauthorized internet users from accessing private networks. However, the major target is not to propose multiple methods or to identify a set of nodes where it connects [3] because even those sets might be used to detect the source of transactions. Thus, to improve Blockchain's anonymity, two generic methods, "anonymous" and "mixing", could be proposed.

Anonymous: Transaction graph analyses and transaction amounts are hidden, which means wherever payments' amounts and destination go through the system, the origin of payments are not connected with the entire transaction. From the perspective of Zerocoin's [4] privacy protocol, miners have access to validate coins from a list of available coins, and the digital signature is not validated over a transaction.

Mixing [5]: Many users pseudonymously have the same addresses to make their transactions through Blockchain. When a user transfers funds from multiple input addresses (with input address A) to multiple output addresses (output address B), the mixing method allows him/her to provide anonymity, but a dishonest intermediary can reveal the relationship between the first user with address A and the second user with address B. User A can send funds to user B by transferring funds to the intermediary first. The intermediary then sends these transactions to user B with multiple outputs and multiple inputs (e.x d1, d2, B, d3, etc, c1, c2, c3, etc., respectively). The relationship between user A and user B is locked, but the intermediary could transfer user As funds to his address. Also, he could share the private information of those individuals. Instead, detecting cheating and dishonesty is to check the user transfer data and other requirements, whether they are converted into codes or not by an intermediary. The optimal solution is to shuffle output address through decryption mixnets used by CoinShuffle or central mixing server provided by Coinjoin.

Scalability: The importance of Blockchain is substantially increasing and becoming more confidential for all specific sensitive data. Generating new blocks needs to have been designed with proper time interval and block size so that the Blockchain as Bitcoin does perform given 7 transactions per second. In most cases, there is a time conflict with the supply of transactions due to the high transaction fee preferred by miners. Redesigning Blockchain and storage optimization of Blockchain are two categorized addressing tips of scalability problem of Blockchain as following;

Redesigning Blockchain: Blockchain is redesigned when the generated key block in every epoch is done to make the nodes responsible for microblocks. As a result, network security and block size together can support network addressing. Bitcoin-NG [6] (Next Generation) contributes microblock to transactions and key blocks for leaders to obtain sustainable microblocks with the longest chain strategy.

Storage optimization of Blockchain: J.Bruce in his "The mini-Blockchain scheme" shared cryptocurrency scheme instead of old transactions that were already forgotten. Operating an entire copy of the ledger is more complicated for nodes. Moreover, the easiest way to balance empty and non-empty addresses is to apply the account tree

(a simple database). Another alternative is named VerSum [7] that allows expensive outcomes to be calculated over large inputs. It compares the results of multiple servers and accelerates the correct calculation process by comparing both outcomes.

Today the problem of Blockchain scalability cannot be solved by decreasing or increasing block size. It also covers the problem of Blockchain value propositions. Reducing the complexity of hashes and changing parameters are not even enough to focus on scalability. The table below demonstrates 5 different scenarios. In this section, an increase in TPS (transaction per second) can be obtained by increasing block size variable B and a decrease in block generation time variable (TB).

TABLE1
Blockchain scalability

	Scenario #	S0 The current Bitcoin Scenario	S1 Increasing Block Size to 377.5MB	S2 Increase Only Block Generation Time to 1.5s	S3 TB = TR	S4 TB scaled by same factor as Block Size Increase
	Adjustment	Default	B = 377.5	TB = 1.6s	TR = 14s	B = 2MB
A	Bitcoin Block Size (B) in Bytes	1,048,576	395,808,000	1,048,576	1,048,576	2,097,152
B	Block Generation Time (TB) in Seconds	600	600	1.589522193	14	28
C	Average Transaction (Tx) Size in Bytes	380	380	380	380	381
D	Average Transactions per Block = A/C	2,759.41	1,041,600.00	2,759.41	2,759.41	5,504.34
E	Blockchain Transactions per Second (TPS) = D/B	4.6	1736.0	1736.0	197.1	196.6

III. CONSENSUS ALGORITHMS

Maintaining the security stability and integrity of a system is a crucial part of each Blockchain. Proof of Work was the first cryptocurrency consensus algorithm proposed by Satoshi Nakamoto, also known for the first decentralized digital currency implemented on Bitcoin. The consensus protocol allows every transaction in Blockchain to be verified and secured. In contrast, the consensus algorithm is a common agreement that presents reliability and trust among unknown peers to collaborate with every node. Every distributed node supports the validity of transactions. It is also a challenge to distribute any nodes to be consistent. In this way, whether there is a central node that could determine all the same distributed nodes through ledgers or not is a real provided question as well. Hence, today some common approaches have been proposed to reach a consensus.

1. Strategies to consensus:

Proof of work or simply PoW is the original algorithm to arrange proper blocks to the chain and confirm all transactions [8]. It is usually implemented in most cryptocurrencies as an application. One of the most widely used and recognized form is Bitcoin, which presents changing the complexity based on the network system at a given period. Additionally, although the random selection is an appropriate solution to record the transactions in a decentralized network, no guarantee is offered to ensure the block of transactions on nodes in case they can be more likely an attack to the network. Therefore, the valid blocks should be directly generated to choose the right nonce to function. Miners and a nonce are major components of block header that should simultaneously alter each other to obtain different hash values. The following certain values must be greater than calculated values or the same. [9] After all, the node subject to its target value makes the block move to other nodes so that they could easily set the right confirmation

of hash value. Validated block could be added to Blockchains as new block is appended by miners.

The consensus algorithm has various types of chains that can be utilized within the larger network and subnetwork. One of byzantine consensus algorithms co-called Tendermint [10] is determined as selecting a proposer in a round to arrange a block that is not confirmed. Three major steps could be shown as following: A) Commit step- it accounts for validity and transmission of a node and a commit respectively for blocks. Those blocks are accepted where nodes get 2/3 of commits. B) Prevote step- it explains proposed blocks in which validators decide whether to distribute a prevote. C) Precommit step- tells how the nodes responds in terms of 2/3 of prevotes (over this rate it spreads a precommit) and 2/3 of precommits (over this rate it enters the commit stage) for proposed blocks.

2. Comparison between consensus algorithms [11]

Tolerated power of adversary: Gaining control on the network is required nearly 51% of hash power. In case there exits excess revenue in PoW systems, 25% of hash power is gained through a selfish mining strategy. [10]

Energy-saving: if the target value could be reached significantly, the required electricity could also have immense scale. Energy is saved efficiently in the consensus process for Ripple, Tendermint, and PBFT without mining.

Examples: PBF is highly used to acquire consensus by Hyperledger Fabric. Additionally, the Ripple protocol is fulfilled by Ripple, and the Tendermint protocol are devised by Terder mint to the same extent.

Node identity management: Ripple, DPOS, PoS, PoW have free access to the network with nodes. While a given primary in each round is selected with respect to the identity of every miner b PBFT, a proposer in each round is selected in the way of clearly knowing the validators.

IV. THE CURRENT SITUATION OF BLOCKCHAIN

Blockchain is one of the most widely known technology fields in technology application and popularization for most countries such as the UK, US, Australia, South Korea, and UAE. Blockchain was a highly invested field by the UK, approximately 19 million. In addition to the fact that the US came up with a new idea of consensus mentioned as "These Innovations Should Be Fostered Not Smothered". Australia identified recognition of the systems through actively used Blockchain technology. This technology was considered an optimal alternative for developing a trading platform in terms of the stock exchange in South Korea's Bank. Whereas Dubai also was an active user of this technology, the country has created the Global Blockchain Committee, including the Dubai government, Blockchain Start-ups, and other 30 members.

Council of China issued to explore Blockchain from the perspective of learning edge computing

TABLE2
Consensus algorithms comparison

Property	PoW	PoS	PBFT	DPOS	Ripple	Tendermint
Node identity management	open	open	permissiond	open	open	permissiond
Energy saving	no	partial	yes	partial	yes	yes
Tolerated power of the adversary	<25% computing power	<51% stake	<33.3% faulty replicas	<51% validators	<20% faulty nodes in UNL	<33.3% byzantine voting power
Example	Bitcoin [2]	Peercoin [21]	Hyperledger Fabric [18]	Bitshares [22]	Ripple [23]	Tendermint [24]

and deep research of application in industrialized social Internet. President Xi Jinping mentioned how the role of artificial intelligence and internet communication could accelerate a new blossom era of information technology in 2018, May 28 at the CAS (the Congress of the Chinese Academy of Sciences) and CAE (the Congress of the Chinese Academy of Engineering). Undoubtedly, "the 13th Five-Year" National Informatization Plan was proposed to encourage guidance and incentive policies on Blockchain technology in the vicinity of various cities, especially Guangdong, Jiangsu, Gansu, Beijing, Xiong'an, and also Shanghai.

Source: China Academy of Information and Communication Technology Trusted Blockchain Initiatives in December 2018.

Service and technology expansion, industry services, and development of further platforms and infrastructure are the main elements supporting Blockchain development's overall application by having the entire downstream and upstream structure. The table below demonstrates the Blockchain applications development time frame in the following months and years.

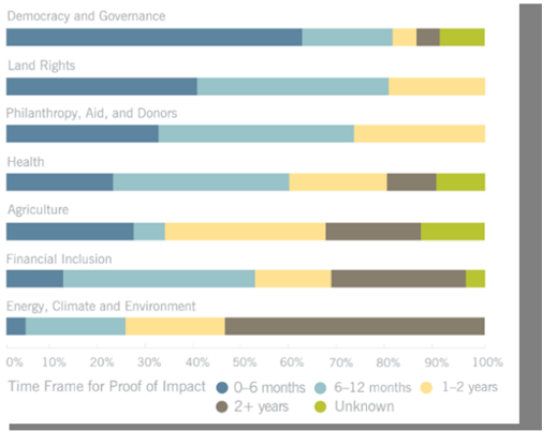

Fig. 3. China Academy of Information and Communication Technology Trusted Blockchain Initiatives in December 2018.

Blockchain is a worldwide industry that involves over 1242 companies around the world. However, industry classification shows various industries where the number of Blockchain companies engages in have large percentage change across world countries in July 2018 meaning that E-commerce & Commodity Trading (50) is nearly 5% of whole as same as Infrastructure & Hardware (56, 5%), Media (56, 5%). On the other hand, Vertical industry solutions, Financial technology, and Internet & Mobile are 7%, 12% and 12%. The largest is cryptocurrency-based technologies (467, 38%), and the least ones are Investment agency (15, 1%) and Training (5,0%). (Fig 3 and 4)

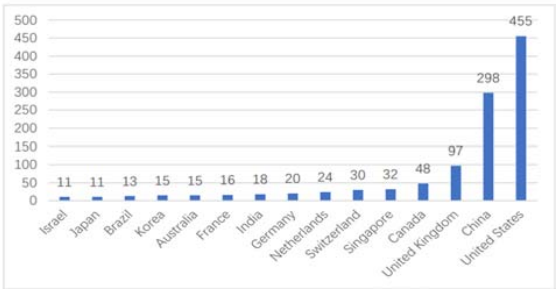

Fig. 4. China Academy of Information and Communication Technology Trusted Blockchain Initiatives in December 2018.

In February 2018, the statistics show that talent supply experienced high growth throughout the last 2 or 3 years, more specifically, 2017 and 2016, even if the growth rate of talents cannot match with demand for those in Blockchain. Surprisingly, demand for talents is small and total supply has not increased as much as demand (still 2 percent of global artificial intelligence talents). The chart below gives more valid information about how various percentages in the distribution of talents are accounted for in the world's countries. Unfortunately, the cities like Shanghai, Hangzhou, and Beijing have less demand for Blockchain talent, and New York (25%), Britain (6%), India (7%) have relatively high demand. (TABLE 4)

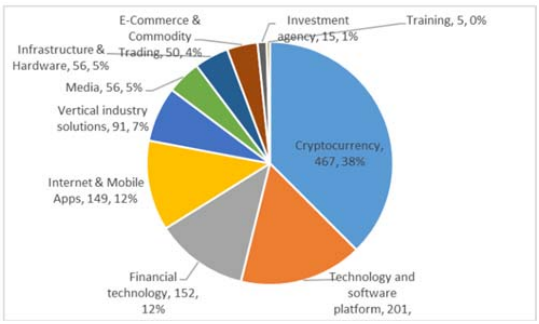

Fig. 5. Distribution of talents in different fields

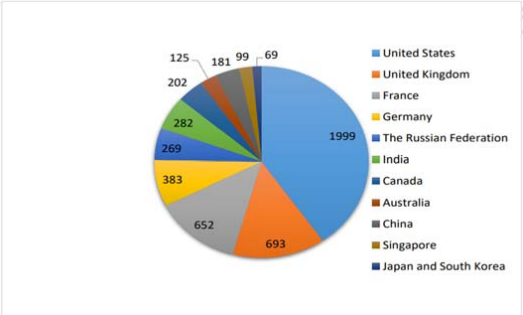

Fig. 6. Distribution of talents in the world's countries

V. CONCLUSION

In this paper, Blockchain offers the sharp growth and sustainable performing functions, operating the environment of most industries in many countries, its unique trust and innovative-based characteristics and future developing perspective of the digital economy. We all discussed Blockchain's general introduction, where it comes from, and how it systematically works in different conditions, Blockchain types and more precisely, visualization, examples, and explanations. Moreover, we listed challenges and recent advances of this technology in which scalability and privacy leakage were base subcategories. Consensus algorithms were focused, and approaches mainly node identity management, examples, tolerated power of the adversary, and details proposed energy saving. The last conversation was covered by real economy integration and Blockchain's current situation, knowing how the countries and target cities responded to their development of artificial intelligence and supply of talents. Our target is to set potential future directions and in-depth Blockchain-related strategies to develop sustainable contributions in future technology.

REFERENCES

1. S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of bitcoins: Characterizing payments among men with no names," in Proceedings of the 2013 Conference on Internet Measurement Conference (IMC'13), New York, NY, USA, 2013

2. A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The Blockchain model of cryptography and privacy-preserving smart contracts," in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858

3. A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin p2p network," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 2014, pp. 15–29

4. I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," in Proceedings of IEEE Symposium Security and Privacy (SP), Berkeley, CA, USA, 2013, pp. 397–411

5. M. Moser, "Anonymity of bitcoin transactions: An analysis of mixing ¨ services," in Proceedings of Munster Bitcoin Conference ¨ , Munster, ¨ Germany, 2013, pp. 17–18

6. I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoinng: A scalable Blockchain protocol," in Proceedings of 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), Santa Clara, CA, USA, 2016, pp. 45–59.

7. J. van den Hooff, M. F. Kaashoek, and N. Zeldovich, "Versum: Verifiable computations over large public logs," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 2014, pp. 1304–1316

8. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

9. S. King, "Primecoin: Cryptocurrency with prime number proof-ofwork," July 7th, 2013

10. J. Kwon, "Tendermint: Consensus without mining," URL http://tendermint. com/docs/tendermint {} v04. pdf, 2014.

11. M. Vukolic, "The quest for scalable Blockchain fabric: Proof-of-work' vs. bft replication," in International Workshop on Open Problems in Network Security, Zurich, Switzerland, 2015, pp. 112–125.