Blockchain Technology Consensus Algorithms and Applications: A Survey

https://doi.org/10.3991/ijim.v14i15.15893

Samar Al-Saqqa (✉)
The University of Jordan, Amman, Jordan
s.alsaqqa@ju.edu.jo

Sufyan Almajali
Princess Sumaya University for Technology, Amman, Jordan

Abstract—One of the new promising technologies for the future is blockchain. It has become one of the popular techniques for various transactions and applications in many different areas such as economy, business, and government. Blockchain technology started with cryptocurrency and bitcoin applications for a safe and transparent environment. Blockchain is a hybrid technology that incorporates various technologies and tools such as mathematics, peer-peer networking, cryptography algorithms, and consensus algorithms. This survey highlights the latest studies in blockchain and consensus algorithms. The study covers the most recent blockchain applications in various domains and sectors. Furthermore, the study gives an insight into the latest adoption of the blockchain in the real world.

Keywords—Distributed ledger technology, blockchain, consensus algorithms, proof of work.

1 Introduction

Blockchain technology received significant attention recently due to the potential of applications it can support in a new and more cost-effective approach. Blockchain has started in 2008 with the idea proposed by Nakamoto [1] who introduced Bitcoin as a new payment method that helps reduce the role of the third party in verification and validation of payment transaction. Nakamoto's idea changed the traditional way of financial transactions that required a third party to verify the movements of people's money. It transmits a transaction method from being centralized to decentralized. Since 2009, many variations of bitcoin have been proposed, such as ethereum [2], and nxtcoin [3]. A common feature among these variants is that anyone who wants to keep a ledger can also join, also pull at any time. Therefore, these types are being considered public Blockchains. Blockchain is now utilized in a wide range of applications such as financial, government, supply chain and internet of things (IoT). Blockchain provides a safe and transparent environment that allows a transaction over a distributed environment with no entral node to control and own the entire transaction. Thus, any node can join the network and make transactions. The distributed nature of Blockchain avoids it the single point of failure issues and offers high integrity for transactions and data against intentional and unintentional corruption. All users can use their devices to keep a large number of transaction records in blocks that construct the chain. Blockchain has different characteristics and features, the following are its main characteristics:

- **Decentralization**: Blockchain changes the idea that requires a central node or a third party to store or verify any transaction by requiring a set of nodes to do so. Storing and updating data occur in a distributed manner.
- **Immutability**: A Blockchain transaction is recorded in a decentralized permanent record, it cannot be changed or altered once it is added. After a transaction is added, it is stored in a distributed database. This brings more trust in the transaction record.
- **Transparency**: Blockchain users can view their data and transactions in a transparent manner to all nodes. Transparency is a key element in the Blockchain for several applications such as supply chain, and financial services.
- **Anonymity:** It allows users to perform anonymous transactions, the user is linked with public address and no one will know the actual name or address. Cryptography methods are used to conceal the user identity.
- **Consensus Driven**: The verification and adding of each block to the Blockchain achieved by reaching agreement among all Blockchain nodes. This agreement happens using a consensus algorithm that encompasses rules for validating a block.

There is a tremendous amount of research in blockchain technology. Blockchain research can be classified into three categories, the first category of research focuses on blockchain security and developing and implementing new approaches to increase the security of the blockchain [4], [5]. The second category focuses on the consensus algorithms, suggesting a new algorithm, or making some variations on the existing algorithm, or building hybrid approaches of existing algorithms [6]. The third category focuses on Blockchain applications, and the adaptation and utilization of Blockchain in different areas [7], [8], [9]. In this survey, we provide an overview of the Blockchain according to the three aforementioned categories. This paper is organized as follows. We discuss Blockchain types in section two. Blockchain architecture is introduced in section three. Blockchain consensus algorithms are presented in section four. Blockchain adaptation and applications are introduced in section five, and section six provides the conclusion.

2 Types of Blockchain

There are three types of blockchain: Public, consortium, and fully private blockchains. These types can be classified into two categories permissionless and permission-based blockchain. In a permissionless blockchain, the access permissions in this type are not controlled such as in public blockchain. In a permission-based blockchain, the access permissions are more tightly controlled, it involves the consortium and a fully private blockchain [10], The following is the description of blockchain types:

1. **Public Blockchains**: The blockchain is open to the entire world. Anyone can be a part of the Blockchain network and can read, write, send a transaction, and can participate in the consensus process where all nodes have the same power. Although public blockchain is open, it is secured using cryptography algorithms similar to other types of blockchain. Two main examples of public blockchain are Bitcoin and Ethereum [1], [2].
2. **Consortium Blockchains:** Not all blockchain nodes have the write permission nor have the same transaction validation power. It is controlled by a pre-selected number of nodes, so the number of nodes added to blockchain or capable of validating the transaction is controlled and will be knowing about every node. Read permission may be public or restricted. Examples of Consortium Blockchains are Quorum and Corda [11].
3. **Fully private Blockchains**: Not anyone can be a part of this network, it has a centralized database and structure; a single entity (organization) has the write permission and has the power to make decisions and validate the transactions. Read permission may be public or restricted. Table 1, lists a comparison between the public, consortium and fully private in terms of different aspects.

3 Blockchain Architecture

Blockchain is considered as a public ledger and all the verified transactions are stored in a chain that includes blocks. The blocks are added continuously to this chain, and the chain grows with each block addition. To secure this ledger, there are different cryptography algorithms and consensus protocols used to protect the blocks from modifications and secure the blockchain from several attacks. One of the important cryptographic algorithms used in bitcoin is SHA-256, it is a hashing algorithm used for hash calculation. It takes an input of variable size to produce fixed size output, the size of output hash value using this algorithm is 256 bits. Besides the security aspect, hashing prevents users from changing the block data, since any tiny change in the blockchain block, will change the hash value completely. Blockchain uses public-key algorithms for digital signature which securely verifies the identity of a user. The public-key algorithm used in bitcoin is the elliptic curve algorithm. It is an asymmetric algorithm that uses two keys that are mathematically related, the public and private keys. The private key must be kept secret for the user and is used just by the user who owns it to encrypt the transaction when the purpose is user digital signature. The public key of the sender is used by the recipient to decrypt that transaction to validate the message integrity.

Table 1. Comparisons of Blockchain types

Aspect	Public	Private	
		Consortium	***Fully Private***
Controlled by	All Nodes	Group of organizations	One organization
Trust	Trust free	Requires some trust	Requires trust
Decentralization	Yes (Fully)	Partially	No
Access	Permission less	Permissioned	
Speed	Slower	Faster	
Validator Identity	Validators are anonymous	Validators are known	
Implementation	Harder	Easier	
Transaction cost	Expensive	Cheaper	
Consensus algorithm	Permission less (Proof of Work, Proof of Stake, or other consensus Mechanisms)	Permissioned proof of authority or another multi-party consensus algorithm	
Privacy	Less	More	
Scalability	Harder to scale	Easier to scale	
Examples	Bitcoin, Etheurem	Quorum and Corda	

3.1 Block

The blockchain is the sequence of blocks as shown in figure 1. The block is a data container that contains a set of transactions distributed to all nodes in the network. The first block in the blockchain is called genesis block, this block does not have parent block so the previous hash for it equals zero. Blockchain’s block contains two parts: header and data. Each block contains 256 bits hash value of the previous block in the chain called parent hash code which od placed in the header part. There are two more components in block header: basic information and Merkel root hash parts [8]. The header block main components are:

- **Version number**: Indicates the blockchain protocols version.
- **Timestamp**: This field specify the time of block generation in seconds.
- **Difficulty value**: This value that determines the puzzle difficulty which reflects on the time that is needed.
- **Parent hash**: 256- bits of the previous block hash value in the chain.
- **Nonce**: A random number that can be used once in communication, it is used in a hash calculation, this number which the minors have to know and solve in the puzzle calculations.
- **Merkel root hash**: The value that is calculated by hashing all block transactions.

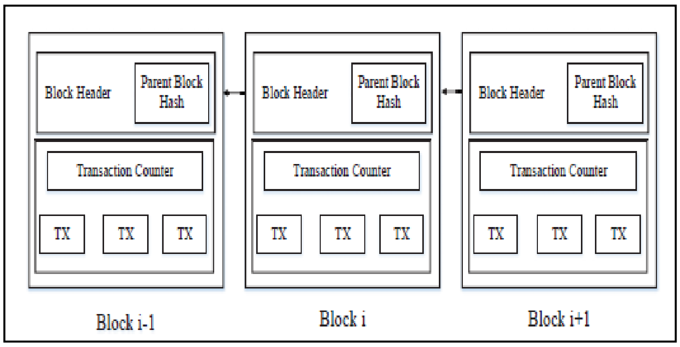


Fig. 1. Blockchain blocks [6]

3.2 Merkle tree

The fundamental component of blockchain is Merkle Tree [1]. Merkle tree allows secure verification of the contents of stored data. It generates one hash value of all transactions contained in a single block. The maximum number of transactions in each block depends on the block and transaction size. The first step in forming a Merkle tree is to perform a hash on each of the transactions. Each transaction goes through a hash function to get the transaction hash value that has a fixed size. Another hashing is performed in a Merkle tree. The previously created transactions hash values are put in pairs and the hashing is performed on that pair of hashes and once they have paired and hashed, they have paired again and hashed, this process of hashing is continuing until all transaction just meet at a single hash. This single hash is called the Merkle root. The Merkle tree is illustrated in figure 2.

3.3 Smart contracts

Smart contracts are digital, distributed contracts, assure the agreement between two parties to be done efficiently and secure regarding the transactions in the network. Smart contracts are tiny computer programs stored inside the blockchain [8]. They can be accessed by every node in the blockchain and every node can interact with. They share the blockchain with immutability characteristics, no one can change the smart contract and there is a consensus for the contract. Smart contracts are used in blockchain transactions and secure the network against attacks that aim to steal or tamper with the assets. Ethereum implements and runs smart contracts. Ethereum serves many different functions to the users, after sending their transactions to Ethereum network they can order new contacts and use functions of the contract. These transactions are recorded on the blockchain. [12], [13].

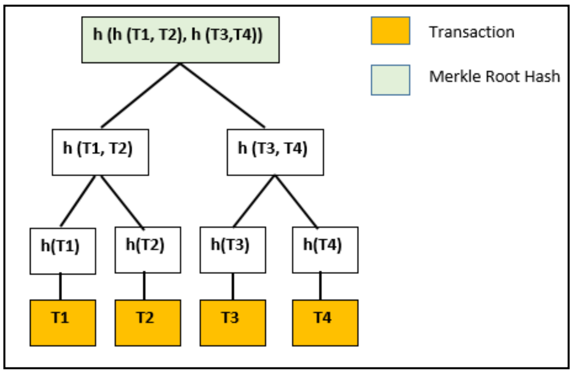


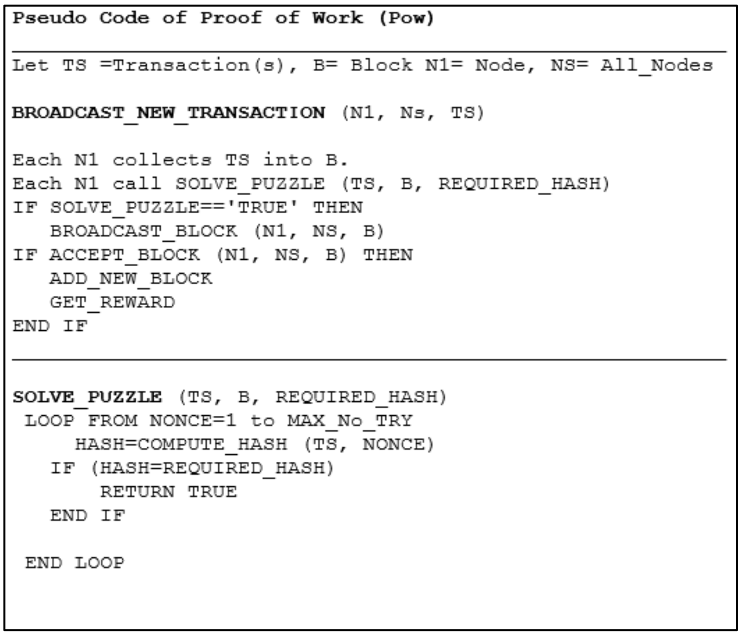
Fig. 2. Merkle Tree

4 Consensus Algorithms

All entities in the decentralized network must agree about the transaction in the network, check blockchain validity and determine if it will be added to blockchain or not, and which block to add next. For bitcoin, all entities must agree on the transaction history as decentralized networks have no centralization and no trust between network entities, the challenge here is how all these entities can agree on the correct state of the data record and how they all achieve consensus. There is a different implementation for consensus mechanisms for consensus algorithms that are used in different blockchain applications [14], they vary in different terms such as decentralization. In this section, we will summarize up to date consensus algorithms that are used in the technology of blockchain.

4.1 Proof of work

The first consensus algorithm is proof of work (PoW) which is used in the bitcoin network [1]. Proof of work idea focuses on the concept of all entities in a distributed network racing to get the solution of a difficult puzzle of calculating a hash value to get the right one to add the new block to the chain and get the reward as shown in figure 3. There are different variations of proof of work in literature. King [15] suggests a new type of PoW based on using searching for prime numbers in peer2peer designs instead of not hashcash proof of work. Cunningham and bitwin chain are used as a prime chain in the puzzle of proof of work. Another puzzle that is applied for proof of work is proposed in [16], it focused on applying the puzzle in two phases while in [17], Non-outsourceable puzzles are proposed. Proof of work is a good approach to the agreement, but it has the main disadvantage regarding efficiency. Proof of work is expensive in computation. This motivates us to propose new consensus algorithms to solve this inefficiency in proof of work algorithm. Proof of stake (PoS) is coming to solve this issue.



```
Pseudo Code of Proof of Work (Pow)
________________________________________________________
Let TS =Transaction(s), B= Block N1= Node, NS= All_Nodes

BROADCAST_NEW_TRANSACTION (N1, Ns, TS)

Each N1 collects TS into B.
Each N1 call SOLVE_PUZZLE (TS, B, REQUIRED_HASH)
IF SOLVE_PUZZLE=='TRUE' THEN
   BROADCAST_BLOCK (N1, NS, B)
IF ACCEPT_BLOCK (N1, NS, B) THEN
   ADD_NEW_BLOCK
   GET_REWARD
END IF
________________________________________________________

SOLVE_PUZZLE (TS, B, REQUIRED_HASH)
 LOOP FROM NONCE=1 to MAX_No_TRY
     HASH=COMPUTE_HASH (TS, NONCE)
   IF (HASH=REQUIRED_HASH)
       RETURN TRUE
   END IF

 END LOOP
```

Fig. 3. Proof of Work consensus pseudo code

4.2 Proof of stake

It has an advantage over proof of works that it is more energy-efficient algorithm. In proof of work, a massive amount of energy is consumed and huge computing power is used which will spend a big amount of resources on the blockchain while using proof of stake consensus algorithm there is less computation performed [18], [19]. The node has stake coins in order to get the chance to be one who has the right to add the next block to the chain. Proof of stake concept has been discussed extensively in different types of research with the main goal of how to provide secured blockchain against any future attacks [20].

4.3 Delegated proof of stake

Delegated proof of stake is another consensus algorithm. Its idea main about the stakeholders able to select a leader who votes for them and potentially passes some rewards as well. These leaders can be voted in or out at different times and they produce blocks in around robin fashions so they do not get to put them all in a row. This algorithm is more centralized, and it can operate much faster than other algorithms. One problem of this algorithm is the wealthy nodes have a lot of power in this approach and they can vote themselves in or put their friends in. [21].

4.4 Proof of activity

Proof of activity consensus algorithm is proposed, it is a hybrid approach that includes proof of work and proof of stake [22]. It starts with a proof of work allowing minors to mine empty template without any transactions then it switched to proof of stake where validators select a block to sign and rewards get split between both proof of work minor and the staker [22].

4.5 Proof of authority

This protoacol also solved the PoW energy consumtion. De Angelis et al. [23] proposed a proof of authority consensus, its idea focus on validators or notes are approved or public identities and they must publicly have verified and they must operate what it is called authority node. This protocol is not consecutive block approval and the incentive is not playing with error probability because the identity is known, this protocol can be used in public or private networks.

4.6 Proof of space or proof of capacity

The difference between the proof of work and this protocol is that here the blockchain node, instead of using computation power or the processing, it allocates an amount of disk space or memory in order to solve challenge terms to get the ability to add next block. It is a good approach that more resource that deeply apply proof of work [24].

4.7 Proof of importance

It is an expanded version of proof of stake, its idea focuses on not only the stake or amount of coins should be considered but instead, there are other metrics should be taken into consideration. It has the disadvantage that it is wasteful of resources [25].

4.8 Proof of burn

The node has to send a coin to burn address which is irretrievable in order to get a chance to mine, the chance that the node selected to mine increases with the number of coins you burn [26].

4.9 Practical byzantine fault tolerance

In case if there are malicious nodes in the system, a practical byzantine fault tolerance algorithm solves this issue. It is a replication algorithm to tolerate byzantine faults used by hyper ledger, the distributed computer network might be able to reach consensus despite the existence of some nodes that are failing or sending incorrect information. This protocol helps in reducing the effect of these nodes on the overall system [27].

4.10 Ripple

Ripple consensus algorithm is efficient within a larger network. It can utilize the presence of trusted sub-networks. It works in a cooperative manner rather than competitive; the nodes cooperate to agree on the ordering and validity of transactions in the network. This means that the nodes are working with each other instead of against each other which is a lot more efficient [28].

Nguyen et al [29], classified consensus protocols in two categories: proof-based and voting-based. Proof-based needs joining between nodes in verification to determine which nodes qualified than others to add blockchain block. Voting based needs that the blockchain node to exchange the results after a new block or transaction verification. Table 2 summarizes the consensus algorithms reference studies based on consensus classification in [29].

Table 2. Consensus algorithms References based on classification in [29]

Consensus algorithm	References
Proof Based consensus algorithm	
Proof of Work and its variations	[1],[15],[16],[17],[30],[31],[32]
PoS and its variations	[19],[20],[21]
Hybrid form of PoW and PoS	[18],[22],[26],[33],[34],[35],[36]
Voting Based Consensus	
Byzantine fault tolerance-based consensus	[27],[28],[37]
Crash fault tolerance-based consensus	[38],[39]

5 Blockchain Adaptation and Applications

Several organizations can take an advantage of blockchain major advantages: transparent, decentralized, efficient and secure. It is likely to disrupt many industries that have a middleman or third party. Many industries in this age direct to change their strategies and operations from a centralized approach to decentralized, such as banking and payments since blockchain may give financial services to people around the world [40]. There has also been widespread optimism regarding the application of blockchain such as supply chain management, human resources, forecasting, Internet of things, and healthcare[41]. Blockchain technology used in supply chain management to put the transaction in decentralized form, all distribution chain transactions are easily recorded and monitored, this minimizes the chance to errors and mistakes. Many charity organizations also used blockchain to distribute the aids in a way that assures the delivery of aids to whom deserves it, monitoring this can be done using blockchain. Blockchain technology is also applied to the Internet of Things (IoT)[42]. The traditional approach of IoT that there are many daily used devices or certain-application devices controlled by a central point, blockchain changes this approach to be distributed approach and the devices can communicate with others directly. Using smart contracts enables the buyer to buy from a seller without a central party such using the smart contract in certain industries such as retail, music, land registration and property transferring, insurance and energy management. Table 3 summarizes the blockchain applications and shows blockchain adaptation examples.

Table 3. Blockchain Applications and examples of industry adaptations

	Application	Description	Examples
1	Government	Helps to provide government operation in secure, transparent and efficient way.	Dubai Blockchain Strategy [43] Switzerland CryptoValley [44]
2	Energy management	Helps to organize the energy operations such as generation, distributions and selling between parties.	lo3energy [45], Sun Contract[46]
3	Supply chain management	Blockchain achieves management of supply chain transactions in a decentralized, and secure way.	Fluent [47] Everledger [48] Skuchain [49] Provenance [50]
4	Human Resources	Managing hiring employees in a company	Colony.io [51] Chrono.tech [52]
5	Health care	Stores and shares sensitive data and medical records	Gem [53] Tierion [54]
6	Financial and banking	Blockchain technology allows the parties to make financial and money transferring in different locations	ABRA [55] Barclays [56]
7	Online music	Provides ways to music artists to collect their selling money directly from their fans with no need to give a large percentage of sales to music distribution companies	Mycelia [57] Ujo Music [58]
8	Retail	Decentralized blockchain retail utilities connect buyers and sellers without a third party which making purchasing operation easy, reliable, and fast.	OpenBazaar [59] OB1 [60]
9	Forecasting	Provides away for prediction that is different from the traditional way in forecasting	Augur [61]
10	Online storage	Helps to reduce attack that are associated with online and cloud storage and cancel the central provider services.	Online Data Storage Storj [62]
11	Internet of Things	Provides services in a decentralized way for IoT devices and they can have connected together and communicate.	openledger [63] ARCTOUCH [64] helium [65] GRID+ [66] XAGE SECURITY [67]

			HYPR [68] NETOBJEX [69]
12	Insurance	Helps in performing many insurance services in decentralized systems such as contract and identity verifications and give new way in managing trust between the contractors	aeternity [70]
13	Private transport and ride sharing	Cancels the role of third party in ride sharing between cars owner and customers and this is done through p2p apps.	Arcade City [71] UBS [72] INNOGY [73]
14	Charity	Provides a way for the people who donates to charity organization to follow their donations and increase trust that the money will go to the people who deserve it.	BitGive [74]
15	Voting	Helps in many voting procedures processes such as the registration of voters and the verification of voters' identity. And to track the counter of voting	Democracy Earth [75] Follow My Vote [76]
16	Land registrations	Provides transfer properties services	Land Records Management in India [77]
17	Education	Helps in online education, blockchain Technology can store learning records in a trusted, distributed manner, and provide credible digital certificates. It also helps in sharing information resources and enhance digital competence by the assessment of cooperative education E-Portfolio	Full record of learning trajectory and trusted certification [78] Cloud-based Blockchain E-portfolio for cooperative education management system [79]

6 Conclusion and Future Work

Blockchain technology seems is a key technology for the future which has attracted business, and government sectors to use that technology to improve many offered services. It is originally introduced for the digital currency bitcoin then it has evolved into something bigger. Blockchain is a revolutionary technology that might change the current exchanging transactions especially the money and property transfer. In this survey, we presented a survey of blockchain technology and highlighted the latest studies in blockchain and consensus algorithms. Moreover, we discussed the latest adaptation of the blockchain. It is observed that developing blockchain is fast and spreads to cover a wide area of applications, and the system applications move away from centralization to decentralization and this concept is achieved by applying blockchain. As future work, we will consider the security of blockchain systems and address the attacks and privacy issues associated with blockchain to give a comparative analysis of different security mechanisms that are used to increase blockchain security and privacy. Moreover, we will focus on new research directions for two important blockchain applications: cloud computing and IoT.

7 References

[1] Nakamoto, Satoshi, and A. Bitcoin. "A peer-to-peer electronic cash system." Bitcoin. Available: https://bitcoin.org/bitcoin.pdf ,2008. https://doi.org/10.2139/ssrn.3440802

[2] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151: 1-32. 2014.

[3] Popov, Serguei. "A probabilistic analysis of the nxt forging algorithm." Ledger 1 69-83. 2016. https://doi.org/10.5195/ledger.2016.46

[4] Lin, Iuon-Chang, and Tzu-Chun Liao. "A Survey of Blockchain Security Issues and Challenges." IJ Network Security 19, no. 5, 2017: 653-659.

[5] Feng, Qi, Debiao He, Sherali Zeadally, Muhammad Khurram Khan, and Neeraj Kumar. "A survey on privacy protection in blockchain system." Journal of Network and Computer Applications, 2018.

[6] Zheng, Zibin, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. "An overview of blockchain technology: Architecture, consensus, and future trends." In 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557-564. IEEE, 2017. https://doi.org/10.1109/bigdatacongress.2017.85

[7] Pilkington, Marc. "Blockchain technology: principles and applications." In Research handbook on digital transformations. Edward Elgar Publishing, 2016.

[8] Lu, Yang. "Blockchain: A survey on functions, applications and open issues." Journal of Industrial Integration and Management 3, no. 04 (2018): 1850015.

[9] Morabito, Vincenzo. "Business innovation through blockchain." Cham: Springer International Publishing .2017.

[10] V. Buterin, “On public and private blockchains,” [Online]. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ .2015. [Accessed May. 23, 2019].

[11] Quorum, https://www.goquorum.com/ [Accessed May. 23, 2019].

[12] Atzei, Nicola, Massimo Bartoletti, and Tiziana Cimoli. "A survey of attacks on ethereum smart contracts (sok)." In International conference on principles of security and trust, pp. 164-186. Springer, Berlin, Heidelberg, 2017. https://doi.org/10.1007/978-3-662-54455-6_8

[13] Buterin, Vitalik. "Ethereum: A next-generation smart contract and decentralized application platform." Available: https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-White-Paper .2014. [Accessed May. 27, 2019).

[14] Wang, Wenbo, Dinh Thai Hoang, Zehui Xiong, Dusit Niyato, Ping Wang, Peizhao Hu, and Yonggang Wen. "A survey on consensus mechanisms and mining management in blockchain networks." arXiv preprint arXiv: 1805.02707, 2018: 1-33. https://doi.org/10.1109/access.2019.2896108

[15] King, Sunny. "Primecoin: Cryptocurrency with prime number proof-of-work." July 7th 1, no. 6 .2013.

[16] Eyal, Ittay, and Emin Gün Sirer. "How to disincentivize large bitcoin mining pools." Blog post: http://hackingdistributed.com/2014/06/18/how-to-disincentivize-large-bitcoin-mining-pools (2014).

[17] Miller, Andrew, Ahmed Kosba, Jonathan Katz, and Elaine Shi. "Nonoutsourceable scratch-off puzzles to discourage bitcoin mining coalitions." In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 680-691. 2015. https://doi.org/10.1145/2810103.2813621

[18] King, Sunny, and Scott Nadal. "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake." self-published paper, August 19 2012.

[19] Wiki, N. 2018. Whitepaper: Nxt. Nxtwiki.org [online] Available: https://nxtwiki.org.2018 [Accessed May. 27, 2019].

[20] Kiayias, Aggelos, Alexander Russell, Bernardo David, and Roman Oliynykov. "Ouroboros: A provably secure proof-of-stake blockchain protocol." In Annual International Cryptology Conference, pp. 357-388. Springer, Cham, 2017. https://doi.org/10.1007/978-3-319-63688-7_12

[21] Delegated proof of stake. Available: https://www.coinbureau.com/education/delegated-proof-stake-dpos/ [Accessed June. 13, 2019].

[22] Bentov, Iddo, Charles Lee, Alex Mizrahi, and Meni Rosenfeld. "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake." IACR Cryptology ePrint Archive 2014 (2014): 452. https://doi.org/10.1145/2695533.2695545

[23] De Angelis, Stefano, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, and Vladimiro Sassone. "Pbft vs proof-of-authority: applying the cap theorem to permissioned blockchain." 2018.

[24] Dziembowski, Stefan, Sebastian Faust, Vladimir Kolmogorov, and Krzysztof Pietrzak. "Proofs of space." In Annual Cryptology Conference, pp. 585-605. Springer, Berlin, Heidelberg, 2015.

[25] Proof of importance. Available: https://nem.io/xem/harvesting-and-poi/ [Accessed May. 27, 2019].

[26] P4Titan, "Slimcoin: a peer-to-peer crypto-currency with proof-of-burn," 2014 [Online].https://www.chainwhy.com/upload/default/20180703/4ae7cee40462e7951f508b28dd1d9936.pdf. [Accessed May. 27, 2019].

[27] Castro, Miguel, and Barbara Liskov. "Practical Byzantine fault tolerance." In OSDI, vol. 99, pp. 173-186. 1999.

[28] Schwartz, David, Noah Youngs, and Arthur Britto. "The ripple protocol consensus algorithm." Ripple Labs Inc White Paper 5 (2014).

[29] Nguyen, Giang-Truong, and Kyungbaek Kim. "A Survey about Consensus Algorithms Used in Blockchain." Journal of Information processing systems 14, no. 1 .2018.

[30] S. Tang, Z. Liu, S. S. Chow, Z. Liu, Y. Long, S. Liu, "Forking-free hybrid consensus with generalized proof-of-activity.", IACR Cryptology ePrint Archive 2017 (2017) 367.

[31] Sompolinsky, Yonatan, and Aviv Zohar. "Secure high-rate transaction processing in bitcoin." In International Conference on Financial Cryptography and Data Security, pp. 507-527. Springer, Berlin, Heidelberg, 2015. https://doi.org/10.1007/978-3-662-47854-7_32

[32] Liu, Zhiqiang, Shuyang Tang, Sherman SM Chow, Zhen Liu, and Yu Long. "Fork-free hybrid consensus with flexible proof-of-activity." Future Generation Computer Systems 96 515-524. 2019 https://doi.org/10.1016/j.future.2019.02.059

[33] Vasin, Pavel. "Blackcoin's proof-of-stake protocol v2." Available: https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf 71 .2014.

[34] Duong, Tuyet, Lei Fan, and Hong-Sheng Zhou. "2-hop blockchain: Combining proof-of-work and proof-of-stake securely." Cryptol. ePrint Arch., Tech. Rep 716 (2016): 2016.

[35] Chepurnoy, Alexander, Tuyet Duong, Lei Fan, and Hong-Sheng Zhou. "TwinsCoin: A Cryptocurrency via Proof-of-Work and Proof-of-Stake." IACR Cryptology ePrint Archive 2017 (2017): 232. https://doi.org/10.1016/j.future.2019.02.059

[36] Milutinovic, Mitar, Warren He, Howard Wu, and Maxinder Kanwal. "Proof of luck: an efficient blockchain consensus protocol." In proceedings of the 1st Workshop on System Software for Trusted Execution, p. 2. ACM, 2016. https://doi.org/10.1145/3007788.3007790

[37] Mazieres, David. "The stellar consensus protocol: A federated model for internet-level consensus." Stellar Development Foundation, 2015.

[38] L. Lamport, "Paxos made simple" ACM SIGACT News, vol. 32, no. 4, pp. 18-25, 2014.

[39] Raft-based consensus for Ethereum/Quorum [Online]. Available: https://github.com/ jpmorganchase/quorum/blob/master/raft/doc.md.

[40] Guo, Ye, and Chen Liang. "Blockchain application and outlook in the banking industry." Financial Innovation 2, no. 1 (2016): 24.

[41] Agbo, Cornelius C., Qusay H. Mahmoud, and J. Mikael Eklund. "Blockchain technology in healthcare: a systematic review." In Healthcare, vol. 7, no. 2, p. 56. Multidisciplinary Digital Publishing Institute, 2019. https://doi.org/10.3390/healthcare7020056

[42] Lao, Laphou, Zecheng Li, Songlin Hou, Bin Xiao, Songtao Guo, and Yuanyuan Yang. "A Survey of IoT Applications in Blockchain Systems: Architecture, Consensus, and Traffic Modeling." ACM Computing Surveys (CSUR) 53, no. 1 (2020): 1-32. https://doi.org/10.1145/3372136

[43] Blockchain, https://www.smartdubai.ae/initiatives/blockchain, [Accessed April. 10, 2020].

[44] Crypto valley zug to trial blockchain voting, https://www.swissinfo.ch/eng/, [Accessed April. 10, 2020].

[45] Lo3 energy, https://lo3energy.com/ [Accessed May. 10, 2020].

[46] Suncontract, https://suncontract.org/ [Accessed May. 12, 2020].

[47] Fluent, Fluent Network, The financial operating network for global commerce, https://www.f6s.com/fluentnetwork [Accessed May. 12, 2020].

[48] Everledger, https://www.everledger.io/ [Accessed May. 10, 2020].

[49] Skuchain, https://www.skuchain.com/ [Accessed May. 10, 2020].

[50] Provenance, https://www.provenance.org/ [Accessed May. 20, 2020].

[51] COLONY, https://colony.io/ [Accessed May. 22, 2020].

[52] Chrono.tech, https://chrono.tech/ [Accessed May. 22, 2020].

[53] Gem, https://gem.co/ [Accessed May. 22, 2020].

[54] Tierion, https://tierion.com/ [Accessed May. 10, 2020].

[55] Abra, https://www.abra.com/ [Accessed May. 20, 2020].

[56] Barclays, https://www.barclayscorporate.com/, [Accessed June. 2, 2020].

[57] Mycelia, http://myceliaformusic.org/ [Accessed May. 20, 2020].

[58] Ujo, https://ujomusic.com/ [Accessed May. 20, 2020].

[59] Openbazaar, https://www.openbazaar.org/ [Accessed April. 10, 2020].

[60] Ob1, https://ob1.io/, [Accessed April. 10, 2020].

[61] Augur, https://www.augur.net/ [Accessed April. 10, 2020].

[62] Storj, https://storj.io/ [Accessed April. 10, 2020].

[63] Openledger, https://openledger.info/ [Accessed April. 15, 2020].

[64] Arctouch, https://arctouch.com/ [Accessed April. 10, 2020].

[65] Helium, https://www.helium.com/ [Accessed May. 23, 2020].

[66] Grid, https://gridplus.io/ [Accessed May. 23, 2020].

[67] Xage, https://xage.com/ [Accessed May. 23, 2020].

[68] Hypr, https://www.hypr.com/ [Accessed May. 23, 2020].

[69] Netobjex, https://www.netobjex.com/ [Accessed May. 23, 2020].
[70] Aeternity, https://aeternity.com/ [Accessed May. 23, 2020].
[71] Arcade city, https://arcade.city/ [Accessed May. 23, 2020].
[72] Ubs, https://www.ubs.com/global/en.html [Accessed May. 23, 2020].
[73] Innogy, https://www.innogy.com [Accessed May. 23, 2020].
[74] Bitgive, https://www.bitgivefoundation.org/ [Accessed May. 23, 2020].
[75] Democracy earth, http://democracy.earth/ [Accessed May. 23, 2020].
[76] Follow my vote, https://followmyvote.com/ [Accessed May. 23, 2020].
[77] Thakur, Vinay, M. N. Doja, Yogesh K. Dwivedi, Tanvir Ahmad, and Ganesh Khadanga. "Land records on blockchain for implementation of land titling in India." International Journal of Information Management 52 (2020): 101940. https://doi.org/10.1016/j.ijinfomgt.2019.04.013
[78] Sun, Han, Xiaoyue Wang, and Xinge Wang. "Application of blockchain technology in online education." International Journal of Emerging Technologies in Learning (iJET) 13, no. 10 2018: 252-259.Available: https://www.online-journals.org/index.php/i-jet/article/view/9455. [Accessed June. 2,2020] https://doi.org/10.3991/ijet.v13i10.9455
[79] Wanotayapitak, Sukosol, Kobkiat Saraubon, and Prachyanun Nilsook. "Process Design of Cooperative Education Management System by Cloud-based Blockchain E-portfolio." International Journal of Online and Biomedical Engineering (iJOE) 15, no. 08 (2019): 4-17. Available: https://www.online-journals.org/index.php/i-joe/article/view/10374. [Accessed June 5,2020] https://doi.org/10.3991/ijoe.v15i08.10374

8 Authors

Samar Al-Saqqa is currently a teacher with the University of Jordan, King Abdullah II School for Information Technology, Information Technology Department, holds a M.Sc. and B.Sc. in Computer Science from The University of Jordan, King Abdullah II School for Information Technology, Information Technology Department. The research interests in the areas of Natural language processing, Sentiment Analysis, Machine Learning, Data Mining and e-technologies. Email: s.alsaqqa@ju.edu.jo.

Sufyan Almajali received the Ph.D. degree in computer science from the Illinois Institute of Technology, Chicago, IL, USA. He worked for several IT companies in USA, including the Director of Technology Solutions for Vertex, Chicago, the Chief Technology Officer with Secure Data Replicator, Chicago, where he supervised the development of an online real-time data replication system. He has 20 years of academic and industrial experience. He is currently an Associate Professor of Computer Science with Princess Sumaya University for Technology, Amman, Jordan. In addition to Princess Sumaya University, he taught at several universities in the states, including Chicago State University, Robert Morris University, DeVry University, and Benedictine University. His current research interests include the Internet of Things security, mobile edge computing, and network security.

Article submitted 2020-05-13. Resubmitted 2020-06-18. Final acceptance 2020-06-21. Final version published as submitted by the authors.