Proposed New Blockchain Consensus Algorithm

https://doi.org/10.3991/ijim.v16i20.35549

Mohanad A. Mohammed[✉], Hala B. Abdul Wahab
Computer Science Department, University of Technology, Baghdad, Iraq
Mohanad_ali1986@yahoo.com

Abstract—Blockchain technology considers the central technology that is used within many applications used frequently with human life. And the primary core of the blockchain is the consensus algorithm which may affect the security of the chain as well as the required resource consumption which affect mainly the blockchain performance directly. In recent years many consensus algorithms have been used and proposed such as proof of work (PoW) and proof of stake (PoS) and many others. However, these algorithms still need some improvement to the security and system resource consumption which will reduce the need for a huge amount of energy and save the environment as well as let the blockchain be useable within low computation ability devices such as the internet of things devices (IoT). This paper proposes a new consensus algorithm that ensures the integrity and authorization of nodes participating in the validation of the transaction and only a predefined number of nodes chosen randomly to participate in block addition which reduces the need for high computations power for mining and voting. The proposed algorithm needs lower time and computation costs comparable to the standard POW algorithm.

Keywords—blockchain, proof of work, PoW, proof of stake, PoS, secret sharing, consensus algorithm

1 Introduction

Open the document you would like to format and import the styles. How this Writing a new document with this template Blockchain is the current trend technology that is used in many systems to provide many features such as security, and integrity in trustless environments, it is a distributed ledger (database) that is sharable between all computers (nodes) within the network where it cannot be forged or tampered and each node participate the integrity of the distributed ledger that usually stores data related to the blockchain and users digitally. Blockchain is known by dint of the cryptocurrency specifically the Bitcoin in 2009 where it is used to save the transactions records decentralized and ensure its security without the need of the 3rd party power to guarantee the operation, this may provide the concept of transparency since blockchain consider decartelized system and all system transaction can be viewed by any user since every user (node) holds its copy of the distributed ledger which is identical in all nodes [1]. The data saved within the blockchain are collected into a defined structure named block where all information needed such as data, the hash of data, and the hash of the previous block are organized within the block. This means every block will be linked to all previous blocks and to modify a block you need to modify all previous blocks and next blocks and these blocks will form a chain of blocks that is known globally as a blockchain. Every new block added to the chain will hold the same block structure and hold the previous hash of the previous block which connects it to the chain. Using blockchain will ensure the security of these systems by the nature of the chain where all newly added blocks shall add to the end of the chain and after addition, no modification (any type of modification is prevented) is allowed, since the block is linked to the previous block using its hash and the previous one linked to the chain and so on, and lastly using the hash codes will add more level of security since any tamper will be detected [2, 3].

2 Blockchain concepts

The concept of blockchain was invented in 2009 by an unknown author called Nakamoto who proposed the blockchain and introduced blockchain as a file that is distributed and transferred to many systems that are connected as peer to peer concept without central management and the authorization is done via consensus algorithm proof of work (PoW). The data within the blockchain is stored as a file with many blocks in it that saves the hash of the current block and the hash of previous data as shown in Figure 1.

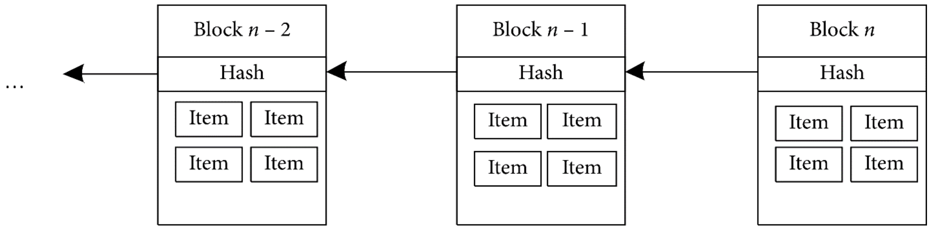

Fig. 1. Blockchain blocks

People who would like to add to the chain usually called minors where no need to identify their identity and can win and add a block to the chain by solving complex puzzles mathematically which is usually consumed computations of computer and energy and then the block added to the chain and copy of added block shares with other nodes via the distributed ledger and no need for the third party to control the operation [4]. Blockchain is divided into three main types:

1. Public Blockchain (permissionless): every user is allowed to mine this type of blockchain if he owns the required computational power and energy and if he gets authorization from other nodes he/she can (verify blocks, add new transactions, and reach the data content) the process of securing this type of chains is done via the consensus algorithm.

2. Private Blockchain (permission): this type of chain differs from the public in that authorization is given to an organization for mining the existing chain and the ability to add blocks to it whereas in public everybody can mine the chain. Any new users who would like to participate in the chain need to ask for permission from the organization's authority.
3. Federated blockchain (hybrid or partially private blockchain): the control of the chain is given to a group of organizations and any requests for mining exclusively to people within these organizations to mine and adding and reading the chain following the same consensus concept [5].

3 Consensus algorithms

The consensus algorithm is an old concept that is related to the distributed systems (traditional model) and there are many known consensus algorithms such as (proof of work (POW), proof of stake (PoS), and practical Byzantine fault tolerance (PBFT) which are employed in the design of blockchain systems), many others consensus algorithms were proposed and it can be down to three main parts:

1. Original algorithms variants: Algorithms that are derived from the original algorithms such as Bitcoin-NG which is considered an improvement to the proof of work (POW) and Algorand which is considered an improvement to the Byzantine fault tolerance (PBFT).
2. Combination of the original algorithms: The combination of both (proof of share (POS) with Byzantine fault tolerance (PBFT)) results in delegated BFT (DBFT)
3. directed acyclic graph (DAG) algorithms [petri net]: that is used the graph to follow the direction of the transaction and met the consensus like Hashgraph and Byteball [6], every consensus algorithm focus on a specific part of the consensus concept and for that reasons, many researchers in academic and industry fields analyze the consensus algorithm from the view of blockchain design and the consensus algorithm can be classified into four main modes [7].

1. Leader-biased mode: the designers focus mainly on the internal selection of the accountant
2. Voting-based mode: where the block added to the chain is very important.
3. Voting plus Committee mode: both selections of the accountant and the addition of a block are very important.
4. Fair accounting mode: where the block addition and the confirmation of the transaction are very important. (the proposed proof of secret sharing algorithm consider Fair accounting mode).

Figure 2 shows the Classification of Blockchain consensus algorithms [8].

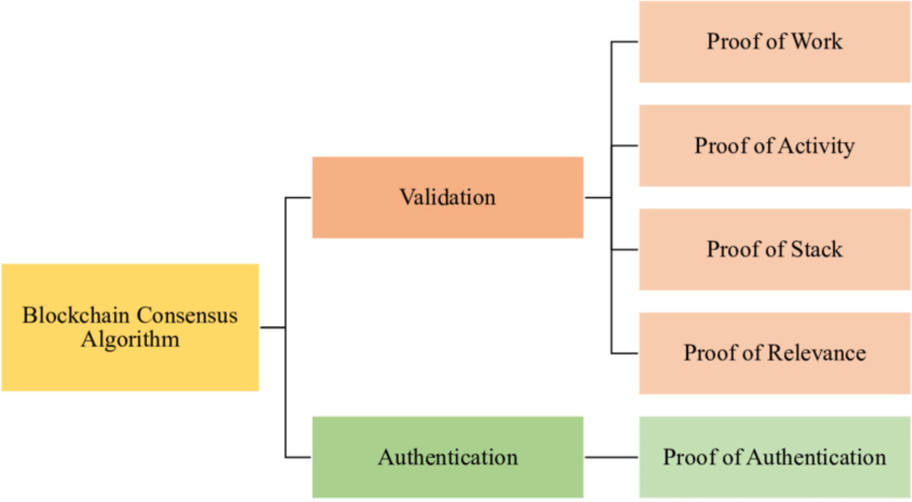

Fig. 2. Blockchain consensus algorithms classification

However, another technique used to protect the blockchain since other nodes within the network will not accept the attacker block within the blockchain only if the attacker can mine or generate blocks faster than verified nodes and with 50% of computational power required then it can be merged to the blockchain ledger and threaten the blockchain system. Many Blockchains use an important mechanism for data stores in blocks that need to be verified by other nodes without revealing the data so they use mainly blind signature technology within this research the technique used is the secret-sharing which serves the same needs [9].

4 Blockchain challenges and solutions

It is very important to the designers of the blockchain to work with many factors to reach a high level of accuracy, each factor provides a level of strength to the blockchain. Factors like consensus algorithm (which provides security and immutability to the blockchain), scalability & capacity (which aimed to determine the ability of the blockchain to accept new blocks), and chain structure (general structure of the block within the chain and how it's organized) [10]. Employing blockchain within applications that do not have a standard structure such as integrating blockchain within the internet of things (IoT) [11, 12], integrating blockchain within the metaverse and NFT deployments and its security [13], and artificial intelligence applications to analyze the blockchain data [14]. Developing blockchain from a technical perspective should be part of:

4.1 Consensus algorithm

The standard use of the consensus algorithm within the blockchain is the main consumption of computational power and energy, leading to long-term latency and low system throughput [15]. However, the new blockchain-based platform needs more capabilities and higher operational behavior. Design of a new consensus algorithm that interacts with other nodes and utilizes the group of intelligence nodes is one of the biggest challenges for system developers. The designed algorithm must increase the system throughput within the protocol and increase the number of blocks added to the chain. Increase the blockchain throughput via using the new right algorithm which could be:

- Consensus algorithm that is based on specific hardware.
- Consensus algorithm reduces the network broadcast unless specific security permission.
- Combination of existing consensus algorithms such as POW and POS.
- The general standard and features of the proposed consensus algorithm are focused on the analysis of energy consumption, execution, identity scalability, and security

4.2 Scalability and capacity

Within the blockchain, each node within the system shall maintain a backup of data (mathematically this is unrealistic when the data grows rapidly) even if lightweight verification nodes can work with this concept, more research should be made within this field to provide industrial solutions [16]. In a blockchain, each node stores all the previous transactions (historical) data which will guarantee data access, availability, and transparency but it will affect the data privacy and system performance. The node cannot store all the data indefinitely. The unlimited growth of the data volume results in data scalable and two main solutions are proposed to such a problem [17].

- Expand the general storage of the blockchain
- Restructure of the blockchain block

4.3 Chain structure

The structure of the chain is not standard and designers of the blockchain can use one of many structures available, there are many designs of the structure of the chain such as:

- Single-chain: single main structure of the chain, which means all nodes will follow the same structure.
- Multi-chain: multiple structures of the chain, more than one structure can the chain follow.

- Cross-chain: multiple cross structures of the chain, more than one structure, and crossing are acceptable. Cross-blockchain can achieve interoperability and lead to mutual trust.
- Side-chain: divided side by side chains (mainly used in anchoring Bitcoin), using many side chains that can be connected to the main chain will result in using the same chain for different applications, Using side chains and multi chains can solve the deficiencies of existing Blockchains. Using the suitable structure of the chain will improve the scalability of the entire blockchain within the network, not just a single node [18]. Never the less of consensus algorithm is used within the blockchain Many other technologies can be combined with data entered into the blockchain to increase the security of data by applying multilevel security such as fusion of multidimensional data sources [19].
- Encryption of plaintext data input using DNA standards methods [20].
- Mixing of multiple cryptography methods such as steganography and encryption techniques [21].

5 Proposed proof of secret shares (PoSS) algorithm

Designing a new consensus algorithm requires focusing on the main properties to reach high quality of the blockchain these points can be summarized as follow:

1. How to reduce the high computation cost and resource consumption.
2. How to let all nodes fairly participate in the validation of the adding operation as well as adding a block to the chain and avoid known attacks such as the Sybil attack and other attacks.
3. How to verify the congruence of the distributed ledger of both consensus and adding block nodes.

The proposed proof of secret shares (PoSS) algorithm ensures that each node within the network has the right to participate in the consensus decision and can add a block to the chain as well as verify the integrity of the distributed ledger before starting the process. However, within this algorithm, the nodes split into two main types:

- Firstly, Adding block node, the node within the network that is aiming to add a block to the chain.
- Secondly, Consensus node, the nodes within the network that are participating in the consensus process of validating the nodes, and checking ledger integrity.

5.1 The main description of the proposed proof of secret shares (PoSS)

All nodes within the network will be provided with a share of secret generated using Shamir's Secret Sharing (SSS) nevertheless it is aiming to add blocks (called adding block node)or participate within the consensus process (called consensus node) and both types of nodes will share their shares to regenerate the secret and validate each node to other within the network, a Shamir's Secret Sharing (SSS) received a secret and it will generate N shares and these shares saved to the nodes and before adding the block, the system calculates the secret according to a pre-defined threshold and check the correctness of the secret and only if a match occurs the adding block node can add data to the chain. Checking the integrity of all nodes (adding block nodes or consensus nodes) by comparing the hashes and if a node is subject to any type of tampering or modification then the process is aborted and the addition cannot proceed. Mainly the consensus process of the proof of secret shares (PoSS) consists of the following phases:

Phase 1) secret and share generating. Using one of the secret-sharing algorithms (Shamir's Secret Sharing is used within this work) to generate shares that are saved within the permission nodes within the network these shares are used to check the authorization of the node to be used within the algorithm, the secret and share generating phase consists of the following steps:

Step1: secret generating: Choose a random value that is used to generate a share using Shamir's Secret Sharing equal to the number of nodes within the network and N as the number of shares as well as the threshold value.

Step2: shares generating: According to the number of N (which is the number of permissioned nodes within the network), N number of shares is generated using Shamir's Secret Sharing and saved within the node as shown in Figure 3.

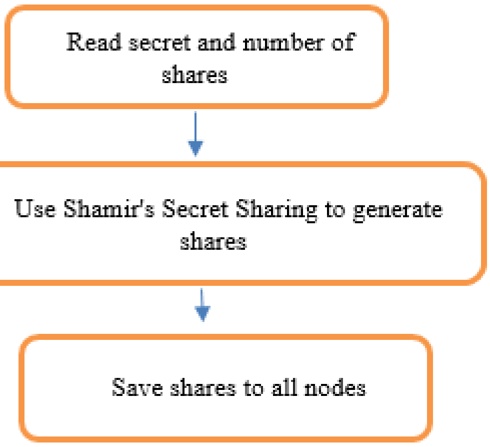
Read secret and number of shares
Use Shamir's Secret Sharing to generate shares
Save shares to all nodes

Fig. 3. Secret and share generating

Phase 2) consensus. For every node within the blockchain that either wishes to add data to the chain (adding block node) or participates in validation of the added block (consensus node) a consensus phase is run to ensure that only the authorized node participating in the process, consensus phase consists of the following steps:

Step1: nodes validation: All nodes within the network will check the integrity of the distributed ledger of each other using the hash codes generated in the previous block addition, and if the hashes of the distributed ledger are different the adding operation is aborted and further investigation is required to verify the tampered node.

Step2: secret calculating: If all the participating nodes pass the node validation then they require to provide their shares to the nodes aiming to add a block to the chain and secret calculated, if the result secret is different than the original one then the operation is aborted, otherwise, the block can be added, as shown in Figure 4.

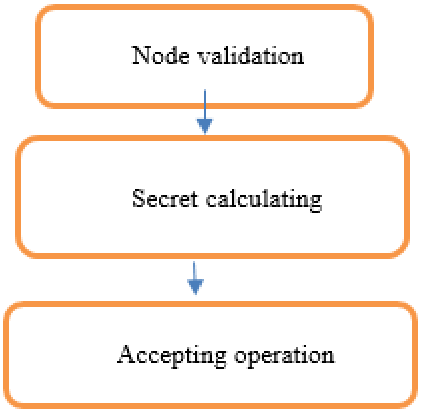

Fig. 4. Consensus phase

Phase 3) adding block. The previous two phases represent the proposed proof of secret shares (PoSS) consensus algorithm used within this work and if the nodes all pass all the phases' steps then the node is allowed to add its block to the chain adding block phase consists of the following step:

Step1: data entry: Within the permission blockchain, there is no need for the nodes to compete with each other to add data to the chain where each node is allowed to add data only if it passes the consensus step which is checking the validity of the node and secret calculating, which allow to the node to add the block and no need to mine a specific nonce to win the competition with other nodes within the network and data can be added directly.

```
  Proof of secret share (PoSS) algorithm
  Input: blockchain, data, random secret value, threshold
value N
  Output: updated blockchain
  Step1: secret generating:
  Use the random value to generate a share using Shamir's
Secret Sharing equal to the number of nodes within the
network and N as the number of shares as well as the
threshold value.
  Step2: shares generating: generate N number of shares
using Shamir's Secret Sharing and saved within the node
  Step3: nodes validation:
```

```
  Using ledger hashes to verify the integrity of the data within the network
  Step4: secret calculating:
  Each participating node provide shares to the nodes aiming to add a block to the chain and secret calculated, if the result secret is different than the original one then the operation is aborted, otherwise, the block can be added
  Step5: adding block:
  Passing the step4 then the node is allowed to add its block to the chain
```

6 Implementation and evaluation

To evaluate the proposed algorithm, it was compared to the proof of work standard algorithm (Table 1 and Table 2) where the general behavior and requirements of all consensus algorithms are provided in Table 3. As shown in Table (1) using proof of work as a consensus algorithm the input data to the chain was text data, where the first data is UOT computer science and no nonce or time required to add since it is the previous data to find the previous hash of the first block where the second data added is a blockchain with 745325 nonce and the 08.07-millisecond average time, the data added to the block (transactions) is (previous hash – current hash – nonce value – any other data can added according to the architecture required of the block). And same procedure followed with other data.

Table 1. Proof of work data

Data	Data hash	Nonce	Average time
UOT computer science	0000022af35078be6575a4b1096243cb93df4772f48973518aab0936e9086b95	-	-
Blockchain	000008e001d110c46dabe4db894c6b0ddf13f60e9f99343346222aeb2aeb2a54	745325	08.07 ms
Consensus algorithm	00000eb70ca4e3901923afdf282f98c0cf711f928fa74c0afb590c8ab09e5256	213821	03.43 ms
IoT	000008996eadcadbd7dde470b5b03c8778a4753952d055766c20369c2beb3c10	252791	03.44 ms
Security	00000cdf8e677cb5a452077d97ed799b3af55e4a4d894e71d9a4c67d577ea743	61638	01.67 ms
1986	00000b6f3987852d6c6854d9a4c2e2ec6d6856cf6b725c7d4c48a24472a4833f	845380	02.64 ms
2022	000009221aec1a3f6d87d49bc63cc07ca1678cb91aa5618712b260a4ff3da496	138283	01.33 ms

As shown in Table (2) using proof of secret sharing as a consensus algorithm the input data to the chain was text data, where the first data is UOT computer science and no time is required to add since it is the previous data to find the previous hash of the first block where the second data added is a blockchain with the 00.35 -

millisecond average time, the data added to the block (transactions) is (previous hash – current hash – nonce value (zero) – any other data can added according to the architecture required of the block). And same procedure followed with other data. Table 3 shows comparisons of the proposed algorithm behavior to other algorithms and Table 4 compare the original PoW to proposed PoSS.

Table 2. Proof of secret share data

Data	Data hash	Average time
UOT computer science	252914a46651ca1cec61960a843e0d3d7a36708c86c02c0745657015ca35571d	-
Blockchain	f56e8369059283aaba923887b33139daf0efab3eae015417394ca13676f93885	00.35 ms
Consensus algorithm	a043003a0eeab4868aa54d3d197173eb68313115187b3df4a88d59d8b37bc25b	00.28 ms
IoT	63595d834a4dfd21fde506e5a4d95ab55581454e0dc5adad36eaada1d11f813c	00.29.ms
Security	36aa19f6ec6cdebf3f3fa5be7c217b4ea193cb85e889bd5c0063f3a2b4c3cbc1	00.47 ms
1986	d9a1c2354423cb5452c979a131d996182a3f80300b84603b816cd479838c8d64	00.22 ms
2022	52995ee87edcd1156b8b49fa61ace885b533325c9d757bdff1c5d4cefd4d86aa	00.23 ms

Table 3. Comparison of the proposed algorithm and most known algorithms

Consensus s algorithm s	Designing Goal	Decentralization n level	Permission model/ Node Identity Management	Electing Miners/ verifiers Based on	Energy efficiency	Scalability	%51 Attack	Double Spending attack	Hardware dependency	speed
PoW	Sybil-proof	Decentralized	Permissionless s	Work (Hash)	No	Strong	Vulnerable e	Vulnerable e	Yes	Slow
PoS	Energy efficiency	Semi-centralized	Permissionless s	Stake	Yes	Strong	Vulnerable	Difficult	No	Fast
DPoS	Organize PoS effectively	Semi-centralized	Both	Vote	Yes	Strong	Vulnerable	Vulnerable	No	Fast
PBFT	Remove software errors	Decentralized	Both	Vote	Yes	Low	Safe	Safe	No	Slow
PoC	Less energy than PoW	Decentralized	Permissionless s	Work (Hash)	Fair	Strong	Vulnerable	Vulnerable	Yes	Slow
DAG	Speed and Scalability y	Decentralized	Permi sionless s	N/A	Yes	Strong	Safe	Safe	No	Fast
PoSS	Energy efficiency	Semicentralized	Permissioned	Secret shares	Yes	Medium	safe	safe	No	Fast

Table 4. PoSS comparable to PoW

Evaluation factor	PoSS	Pow
Transaction per second	0.15	0.0667
Block latency time	0.0333	0.1
Permission model	permission	permissionless
Trust model	Using secret sharing	Using public key
Double spending attack	Not applicable	applicable
51% attack	applicable	Applicable
Sybil attack	Eliminated by secret sharing	Applicable

7 Discussions

The proposed algorithm's main goal is to accommodate Energy efficiency and to work with a Semi-centralized environment since it originally work with private or federated blockchain and is considered Permissioned where no need for minors and the integrity and verification is done using secret sharing, PoSS meets the Energy efficiency since there is no mining or complex mathematical puzzle to solve and provides medium scalability since it is based on generating secrets and shares and sharing them with nodes and if a new node would like to participate within the permission system (private or federated blockchain) the whole process needs to re-execute or extra shares saved when generating the system. PoSS counter knew attacks on blockchain such as 51%Attack and Double Spending attacks with no need for a specific type of hardware and fast speed compared to other methods

The proposed algorithm measuring factors are

a) Consensus s algorithms: PoSS refers to proof of secret sharing
b) Designing Goal: PoSS is designed originally to accommodate Energy efficiency
c) Decentralization level: PoSS is considered Semi- centralized since it is originally targeting the private and federated Blockchains.
d) Permission model (Node Identity Management): PoSS is considered Permissioned since it is originally targeting private and federated Blockchains.
e) Electing Miners/ veriiers Based on: PoSS is mainly based on Secret shares that generate a secret and give shares to nodes and randomly select the participating node (according to the secret-sharing threshold) and use nodes shares to regenerate the nodes and only if an honest node shares the correct share can participate the process of validation of block.
f) Energy efficiency: PoSS meets the Energy efficiency since there is no mining or complex mathematical puzzle to solve to add a block and only share the secret and simple matching process
g) Scalability: PoSS provides medium scalability since it is based on generating secrets and shares and sharing them with nodes and if a new node would like to participate within the permission system (private or federated blockchain) the whole process needs to re-execute or extra shares saved when generating the system.

h) 51%Attack: The concept of a 51% attack is done when an attacker can reach 51% of the connected nodes within the system then he can do the majority voting and accept malicious blocks, in PoSS even if an attacker reaches 51% of nodes the selecting of random node and the calculating of the secret will eliminate the attack, one possible situation where this attack may success within the system where the attacker control number of node more than the specified threshold and the user randomly select all nodes from the attacker group.
i) Double Spending attack: There is no cryptocurrency reward when using the PoSS algorithm which can be used with other systems related to blockchain technology.
j) Hardware dependency: PoSS does not need a specific type of hardware to work where it can be used with any type of hardware
k) Speed: PoSS consider a fast algorithm since even if it has to do some math calculations for generating and regenerating the secret and shares but does not need a special amount of hardware to do mining for the wining node to add block.

8 Conclusions

Blockchain technology can be used within many applications to provide security and integrity of data and the core of this technology is the consensus algorithm which provides verification to the added transaction and validates the nodes trying to add blocks to the chain, many consensus algorithms proposed to meet specific requirements of system designers and users to reduce the power and resources consumption as well as keep the general characteristics of the algorithm, the proposed consensus algorithm called proof of secret share which is laying on using generated secret to derive some shares references to the predefined number of shares and number of required shares to regenerate the secret (shortly referred to as threshold) and several nodes selected randomly and generating the shares these nodes check the hashes to ensure the integrity and then using secret regenerating verify the adding node honesty to the entire nodes.

9 References

[1] Nofer, M., Gomber, P., Hinz, O. et al. Blockchain. Bus Inf Syst Eng 59, 183–187 (2017). https://doi.org/10.1007/s12599-017-0467-3

[2] Beck, R., Avital, M., Rossi, M. et al. Blockchain Technology in Business and Information Systems Research. Bus Inf Syst Eng 59, 381–384 (2017). https://doi.org/10.1007/s12599-017-0505-1

[3] Seebacher, S., Schüritz, R. (2017). Blockchain Technology as an Enabler of Service Systems: A Structured Literature Review. In: Za, S., Drăgoicea, M., Cavallari, M. (eds) Exploring Services Science. IESS 2017. Lecture Notes in Business Information Processing, vol 279. Springer, Cham. https://doi.org/10.1007/978-3-319-56925-3_2

[4] Attaran, M., Gunasekaran, A. (2019). Blockchain Principles, Qualities, and Business Applications. In: Applications of Blockchain Technology in Business. SpringerBriefs in Operations Management. Springer, Cham. https://doi.org/10.1007/978-3-030-27798-7_3

[5] Kovalchuk, L., Oliynykov, R., Bespalov, Y., Rodinko, M. (2022). Comparative Analysis of Consensus Algorithms Using a Directed Acyclic Graph Instead of a Blockchain, and the Construction of Security Estimates of Spectre Protocol Against Double Spend Attack. In: Oliynykov, R., Kuznetsov, O., Lemeshko, O., Radivilova, T. (eds) Information Security Technologies in the Decentralized Distributed Networks. Lecture Notes on Data Engineering and Communications Technologies, vol 115. Springer, Cham. https://doi.org/10.1007/978-3-030-95161-0_9

[6] Fu, X., Wang, H. & Shi, P. A survey of Blockchain consensus algorithms: mechanism, design and applications. Sci. China Inf. Sci. 64, 121101 (2021). https://doi.org/10.1007/s11432-019-2790-1

[7] Yadav, A.S., Kushwaha, D.S. Blockchain-based digitization of land record through trust value-based consensus algorithm. Peer-to-Peer Netw. Appl. 14, 3540–3558 (2021). https://doi.org/10.1007/s12083-021-01207-1

[8] Jabbar, S., Lloyd, H., Hammoudeh, M. et al. Blockchain-enabled supply chain: analysis, challenges, and future directions. Multimedia Systems 27, 787–806 (2021). https://doi.org/10.1007/s00530-020-00687-0

[9] Hussien, H.M., Yasin, S.M., Udzir, S.N.I. et al. A Systematic Review for Enabling of Develop a Blockchain Technology in Healthcare Application: Taxonomy, Substantially Analysis, Motivations, Challenges, Recommendations and Future Direction. J Med Syst 43, 320 (2019). https://doi.org/10.1007/s10916-019-1445-8

[10] Abdulsattar Jaber, T. and AbdulRidha Hussein, M., “Study on known models of NB-IoT Applications in Iraqi environments”, in <i>Materials Science and Engineering Conference Series</i>, 2019, vol. 518, no. 5, p. 052013. https://doi.org/10.1088/1757-899X/518/5/052013

[11] Abdulsattar Jaber, T. (2022). Security Risks of the Metaverse World. International Journal of Interactive Mobile Technologies (iJIM), 16(13), pp. 4–14. https://doi.org/10.3991/ijim.v16i13.33187

[12] Jaber, Tanya Abdulsattar. “Artificial intelligence in computer networks. ”Periodicals of Engineering and Natural Sciences10.1 (2022): 309–322. https://doi.org/10.21533/pen.v10i1.2616

[13] Bhardwaj, R., Datta, D. (2020). Consensus Algorithm. In: Khan, M., Quasim, M., Algarni, F., Alharthi, A. (eds) Decentralised Internet of Things. Studies in Big Data, vol 71. Springer, Cham. https://doi.org/10.1007/978-3-030-38677-1_5

[14] Vukolić, M. (2016). The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. In: Camenisch, J., Kesdoğan, D. (eds) Open Problems in Network Security. iNetSec 2015. Lecture Notes in Computer Science(), vol 9591. Springer, Cham. https://doi.org/10.1007/978-3-319-39028-4_9

[15] Queralta, J.P., Westerlund, T. (2021). Blockchain for Mobile Edge Computing: Consensus Mechanisms and Scalability. In: Mukherjee, A., De, D., Ghosh, S.K., Buyya, R. (eds) Mobile Edge Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-69893-5_14

[16] Singh, A., Parizi, R.M., Han, M., Dehghantanha, A., Karimipour, H., Choo, KK.R. (2020). Public Blockchains Scalability: An Examination of Sharding and Segregated Witness. In: Choo, KK., Dehghantanha, A., Parizi, R. (eds) Blockchain Cybersecurity, Trust and Privacy. Advances in Information Security, vol 79. Springer, Cham. https://doi.org/10.1007/978-3-030-38181-3_11

[17] N. Alseelawi, and H. T. Hazim, "A Novel Method of Multimodal Medical Image Fusion Based on Hybrid Approach of NSCT and DTCWT," International Journal of Online Biomedical Engineering, vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28011

[18] I. A. Aljazaery, and A. H. M. Alaidi, "Encryption of Color Image Based on DNA Strand and Exponential Factor," International Journal of Online Biomedical Engineering, vol. 18, no. 3, pp. 101-113, 2022. https://doi.org/10.3991/ijoe.v18i03.28021

[19] H. T. ALRikabi and H. T. Hazim, "Enhanced Data Security of Communication System Using Combined Encryption and Steganography," International Journal of Interactive Mobile Technologies, vol. 15, no. 16, 2021. https://doi.org/10.3991/ijim.v15i16.24557

[20] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Business & Information Systems Engineering,* vol. 59, no. 3, pp. 183-187, 2017. https://doi.org/10.1007/s12599-017-0467-3

[21] R. Beck, M. Avital, M. Rossi, and J. B. Thatcher, "Blockchain technology in business and information systems research," vol. 59, ed: Springer, 2017, pp. 381-384. https://doi.org/10.1007/s12599-017-0505-1

[22] H. Salim, and H. Tuama, "Secure Chaos of 5G Wireless Communication System Based on IOT Applications," *International Journal of Online and Biomedical Engineering(iJOE),* vol. 18, no. 12, pp. 89-102, 2022. https://doi.org/10.3991/ijoe.v18i12.33817

[23] S. Seebacher and R. Schüritz, "Blockchain technology as an enabler of service systems: A structured literature review," in *International conference on exploring services science*, 2017: Springer, pp. 12-23. https://doi.org/10.1007/978-3-319-56925-3_2

[24] M. Attaran and A. Gunasekaran, "Blockchain principles, qualities, and business applications," in *Applications of blockchain technology in business*: Springer, 2019, pp. 13-20. https://doi.org/10.1007/978-3-030-27798-7_3

[25] L. Kovalchuk, R. Oliynykov, Y. Bespalov, and M. Rodinko, "Comparative Analysis of Consensus Algorithms Using a Directed Acyclic Graph Instead of a Blockchain, and the Construction of Security Estimates of Spectre Protocol Against Double Spend Attack," in *Information Security Technologies in the Decentralized Distributed Networks*: Springer, 2022, pp. 203-224. https://doi.org/10.1007/978-3-030-95161-0_9

[26] X. Fu, H. Wang, and P. Shi, "A survey of Blockchain consensus algorithms: mechanism, design and applications," *Science China Information Sciences,* vol. 64, no. 2, pp. 1-15, 2021. https://doi.org/10.1007/s11432-019-2790-1

[27] A. S. Yadav and D. S. Kushwaha, "Blockchain-based digitization of land record through trust value-based consensus algorithm," *Peer-to-Peer networking and applications,* vol. 14, no. 6, pp. 3540-3558, 2021. https://doi.org/10.1007/s12083-021-01207-1

[28] S. Jabbar, H. Lloyd, M. Hammoudeh, B. Adebisi, and U. Raza, "Blockchain-enabled supply chain: analysis, challenges, and future directions," *Multimedia systems,* vol. 27, no. 4, pp. 787-806, 2021. https://doi.org/10.1007/s00530-020-00687-0

[29] H. M. Hussien, S. M. Yasin, S. Udzir, A. A. Zaidan, and B. B. Zaidan, "A systematic review for enabling of develop a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction," *Journal of medical systems,* vol. 43, no. 10, pp. 1-35, 2019. https://doi.org/10.1007/s10916-019-1445-8

[30] T. A. Jaber and M. A. Hussein, "Study on known models of NB-IoT Applications in Iraqi environments," in *IOP Conference Series: Materials Science and Engineering*, 2019, vol. 518, no. 5: IOP Publishing, p. 052013. https://doi.org/10.1088/1757-899X/518/5/052013

[31] A. H. M. Alaidi, R. a. M. Al_airaji, H. T. ALRikabi, I. A. Aljazaery, and S. H. Abbood, "Dark Web Illegal Activities Crawling and Classifying Using Data Mining Techniques," *International Journal of Interactive Mobile Technologies,* vol. 16, no. 10, 2022. https://doi.org/10.3991/ijim.v16i10.30209

[32] T. A. Jaber, "Security Risks of the Metaverse World," *International Journal of Interactive Mobile Technologies,* vol. 16, no. 13, 2022. https://doi.org/10.3991/ijim.v16i13.33187

[33] T. A. Jaber, "Artificial intelligence in computer networks," *Periodicals of Engineering and Natural Sciences (PEN),* vol. 10, no. 1, pp. 309-322, 2022. https://doi.org/10.21533/pen.v10i1.2616

[34] R. Bhardwaj and D. Datta, "Consensus algorithm," in *Decentralised Internet of Things*: Springer, 2020, pp. 91-107. https://doi.org/10.1007/978-3-030-38677-1_5

[35] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *International workshop on open problems in network security*, 2015: Springer, pp. 112-125. https://doi.org/10.1007/978-3-319-39028-4_9

[36] J. P. Queralta and T. Westerlund, "Blockchain for mobile edge computing: Consensus mechanisms and scalability," in *Mobile Edge Computing*: Springer, 2021, pp. 333-357. https://doi.org/10.1007/978-3-030-69893-5_14

[37] A. Singh, R. M. Parizi, M. Han, A. Dehghantanha, H. Karimipour, and K.-K. R. Choo, "Public blockchains scalability: An examination of sharding and segregated witness," in *Blockchain Cybersecurity, Trust and Privacy*: Springer, 2020, pp. 203-232. https://doi.org/10.1007/978-3-030-38181-3_11

[38] N. Alseelawi, and H. T. Hazim,"A Novel Method of Multimodal Medical Image Fusion Based on Hybrid Approach of NSCT and DTCWT," *iJOE,* vol. 18, no. 03, p. 115, 2022. https://doi.org/10.3991/ijoe.v18i03.28011

[39] I. A. Aljazaery, and A. H. M. Alaidi, "Encryption of Color Image Based on DNA Strand and Exponential Factor," *iJOE,* vol. 18, no. 03, p. 101, 2022. https://doi.org/10.3991/ijoe.v18i03.28021

[40] H. Alrikabi, and H. Tuama "Enhanced Data Security of Communication System using Combined Encryption and Steganography," *International Journal of Interactive Mobile Technologies,* vol. 15, no. 16, pp. 144-157, 2021. https://doi.org/10.3991/ijim.v15i16.24557

10 Authors

Mohanad Ali Mohammed Jawad received the BSc and MSc degrees in Computer Sciences in 2007 and 2015, respectively from the University of Technology. He worked within the private sector in a field related to cyber security as well as artificial intelligence. He published many articles on security and communications. His search interests are Mobile networks, cyber security, and cloud computing. current Ph.D. student in Department Computer Sciences, University of Technology, Baghdad, Iraq (Department Computer Sciences, University of Technology, Baghdad, Iraq) (email: Mohanad_ali1986@yhaoo.com).

Hala Bahjat Abdul Wahab, a Reviewer (R) of IEEE since 2010. Was born in Basra, Iraq in 1969. She received a B.S. Degree in 1990 in computer science, from Basra University, and M.Sc. degree in 2001 in computer science, from Technology University, and a Ph.D. degree in 2006 in computer science security from the department of computer science, University of Technology, Baghdad, Iraq. She received a professor's degree in 2018 from the University of Technology. From 1991 to 1995, Dr. Hala was a lecturer assistant in the computer science department at Basra University, Iraq. From 1995 to 2020, she was a lecturer in the computer science department at the Technology University, Iraq. Author of more than 65 articles. And her research interests include Information and Network Security. Prof. Hala is a coauthor of the "PGP Protocols and its Applications" book in IN TECH 2012. (Department Computer Sciences, University of Technology, Baghdad, Iraq) (email: 110005@uotechnology.edu.iq).

Article submitted 2022-09-03. Resubmitted 2022-10-02. Final acceptance 2022-10-03. Final version published as submitted by the authors.