Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 06, No. 04, December 2020.

HYBRID BLOCKCHAIN

Hazem W. Marar[1] and Rosana W. Marar[2]

(Received: 10-May-2020, Revised: 28-Jun.-2020 and 20-Jul.-2020, Accepted: 8-Aug.-2020)

ABSTRACT

Blockchain is a revolutionary technology that gained widespread popularity since the emergence of crypto-currencies. The potential uses of Blockchain surpassed digital currency into a wider space that includes the Internet of Things (IoT), security applications and smart embedded systems, among others. As the number of Blockchain users increases, several drawbacks start to emerge, since Blockchains consume excessive amounts of energy to store and manipulate data. Furthermore, the limited scalability nature of Blockchains due to their massive storage requirements might become an issue. To improve the overall performance, several challenges in the current Blockchain structure should be tackled. This paper presents a hybrid system architecture that combines the distributed nature of Blockchains with the centralized feature of servers. Users will connect to servers via personal Blockchains, while servers will share a chain of Blockchains to ensure integrity and security. This will significantly decrease the storage requirements of end-users and enhance the scalability of networks. Businesses will highly benefit from this proposed structure, since it creates a reliable scalable business model.

KEYWORDS

Blockchain, Bitcoin, Crypto-currency, Distributed, E-commerce, Hybrid.

1. INTRODUCTION

Since the emergence of Bitcoin in 2008 [1], crypto-currencies and hence Blockchain technology have gained widespread popularity. The technology features enable it to become the infrastructure for a new generation of internet interactions that include secure online payments [2]-[3], data exchange and transaction of digital assets [2]-[4]. Blockchain provides a decentralized, open, Byzantine fault-tolerant transaction mechanism [5]-[7]. Users can consider Blockchain as a sort of data structure that consists of an ever increasing number of blocks linked together through cryptography. Each block includes a cryptographic hash of the previous block, a timestamp and data that users wish to exchange throughout the network [8]-[9]. Data blocks are shared among users and not saved on a centralized server. The chain of blocks continuously grows when new blocks are appended into it and this change will be reflected to all users within the chain. Hence, by design, Blockchain is relatively resistant to data modification. However, in order to append a new block to the chain, computers, called miners, compete and run a complex hashing algorithm trying to produce a valid block hash. This will dissipate huge amounts of disproportionate power and time. Furthermore, the ever increasing chain of blocks will require massive storage capabilities from all users, limiting the scalability of such technology. Blockchains are governed by a consensus algorithm used as a mechanism to achieve the necessary agreement on the validity of data among distributed processes. With the recent advances in Blockchain technology, numerous consensus algorithms were proposed to make endpoints reach an agreement on the order and state of blocks of transactions and update the distributed ledger accordingly [10]-[11]. In this paper, a hybrid Blockchain architecture that is suitable for online banking and e-commerce platforms is proposed. The proposed solution addresses the storage and power consumption requirements while improving the Blockchain's integrity and security. The paper is organized as follows: Section 2 introduces the Blockchain technology and its methodology, whereas Section 3 illustrates the architecture of the proposed hybrid solution and Section 4 concludes the paper.

1. Hazem W. Marar is with Department of Electrical Engineering, Princess Sumaya University for Technology, Amman, Jordan. Email: h.marar@psut.edu.jo
2. Rosana W. Marar is with Department of Computer Graphics and Animation, Princess Sumaya University for Technology, Amman, Jordan. Email: r.marar@psut.edu.jo

2. BLOCKCHAIN TECHNOLOGY

Blockchain is a distributed transactional database that is governed by network consensus and secured by advanced cryptography. As illustrated in Figure 1, a Blockchain consists of a series of datasets that are composed of chains of data blocks. Each block holds several transactions (TX_n). Once a set of transactions is complete, an additional block is appended to the chain, hence representing a complete ledger of transactions history. The chain of blocks continuously grows when new blocks are appended into it and this change will be reflected to all users within the chain.

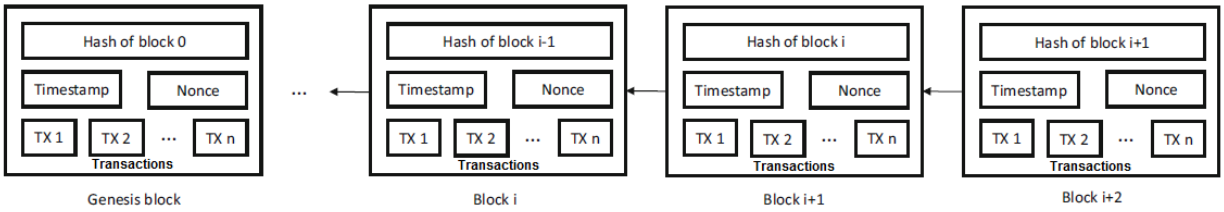

Figure 1. Basic blockchain structure.

In addition to the transactions, each block holds a Unix time timestamp which indicates the time of each transaction. Moreover, each block has a 256-bit hash value of the previous parent block and a nonce, which is a random number that verifies the hash. Several hashing algorithms can be used, but the SHA-256 cryptographic hash is the most common [7]. Hash values are unique and therefore, any alteration in the data would immediately change the respective hash value. As a result, this structure ensures the security and integrity of the entire Blockchain down to the first block known as the Genesis Block. In order to alter the contents of any block, network consensus must be achieved. This implies that a minimum of half the endpoints connected throughout the network reach a common agreement about the present state of the current distributed ledger or transaction. Hence, in large networks, Blockchain is relatively resistant to data modification due to the huge number of endpoints. On the other hand, the computational power and storage power required are immense. Various research studies around Blockchains have been published in recent years to analyze and tackle the issues and limitations in Blockchains and evaluate consensus algorithms. The practical byzantine fault tolerance algorithm (PBFT), the proof-of-work algorithm (PoW), the proof-of-stake algorithm (PoS) and the delegated proof-of-stake algorithm (DPoS) are the four main methods of reaching consensus in the current Blockchain technology. In PBFT, each node in the network maintains an ongoing internal state. When a message is received, nodes use the message in conjunction with their internal state to run a computation algorithm to validate the message. After reaching a decision about the new message, the node shares that decision with other nodes in the system. A consensus decision is determined based on the total decisions submitted by all participating nodes. This method of establishing consensus requires less effort than other methods. However, anonymity can be a great risk on the system.

An alternative method of reaching consensus within a Blockchain is the proof-of-work (PoW) algorithm, which is used by Bitcoin. In contrast to PBFT, PoW does not require all nodes on the network to participate and submit their individual conclusions in order for a consensus to be achieved. Rather, PoW is an algorithm that uses a hash function. Transactions can then be independently verified by all other system participants. The scheme allows for easy, broad participation while maintaining anonymity.

Proof-of-stake (PoS) algorithm is similar to PoW algorithm, but the participation in the consensus building process is restricted to a predefined set of nodes known for having a legitimate stake in the Blockchain. The hash function calculation is replaced with a simple digital signature which proves ownership of the stake. A more centralized way of achieving consensus is using the delegated proof-of-stake (DPoS) system. The algorithm works in a similar manner as in the PoS system, except that individuals choose an entity to represent their portions of stake in the system.

In [12], a specially designed attack scenario is presented, in which collaborating miners' revenue can be larger than their fair share. Such attacks can have significant consequences on the Blockchain structure.

Miners might prefer to join the attackers and the colluding group will expand in size until it becomes a majority. At this point, the Blockchain system ceases to be a decentralized system. In [13], a decentralized smart contract system that does not store or show financial transactions is presented. Normally, all transactions, including flow of money, are exposed on the Blockchain. Such information might be useful by hackers and network attackers to track money and assets. Using such decentralized smart contract system retains transactional privacy from the public's view. In [14], a highlight of the weaknesses and limitations of Bitcoin technology is presented. This includes the theft or loss of Bitcoins due to malware attacks, structural problems and scalability issues, like delayed transaction confirmation, data retention and communication failures. A fair exchange protocol that improves the users' anonymity is used to improve the quality of the existing Bitcoin technology. In [15], a new mechanism for securing Blockchains' contracts is presented. By introducing a credibility score measure, a hybrid Blockchain that prevents an attacker from monopolizing resources is introduced. Credibility is a vital factor in any contract or transaction. Contractors must develop a good knowledge about each other to build up credibility and trust. The more contracts a contractor has with different people, the more credibility he/she gains. The mechanism proposed creates a hybrid Blockchain based on the proof-of-stake and credibility score methods. The proposed system uses the proof-of-work algorithm to introduce a hybrid solution in which power and storage requirements are minimized while improving the network's scalability and security.

Since Blockchain is a decentralized distributed ledger, it has to be managed by a peer-to-peer network adhering to a common protocol for communication and appending new blocks. Therefore, each peer in the network will have a copy of the Blockchain. Any alteration in the Blockchain will involve the alteration of all subsequent blocks, which requires consensus of the majority of the network. In its current form, the hash value of each block is generated by miners. Mining is a process at which specialized computers compete to solve a complex computational problem and produce a valid hash. Hence, miners secure the network and process every transaction. The SHA-256 cryptographic hash chooses any 256-bit number ranging from 0 to 2^{256}. The target is a 256-bit number that all Blockcahin clients share. The SHA-256 hash of a block's header must be lower than or equal to the current target for the block to be accepted by the network. The lower the target, the more difficult it is to generate a block. The maximum target defined by SHA256 mining devices is illustrated in equation 1.

$$T_{Max} = 0x00000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF \quad (1)$$

We define (D) to be the difficulty of finding a valid hash for a given block. D can be defined as in Equation 2 [16]-[17]:

$$D = \frac{T_{Max}}{T_{Cur}} \quad (2)$$

where, T_{Max} is the maximum target of the hash value and T_{Cur} is the current target hash that the miner found.

Difficulty can be simply defined as the ratio between the maximum target and the current target. T_{Max} and T_{Cur} can be expressed as in Equations 3 and 4 [16]-[17]. The maximum target is defined as $(2^{16} - 1) \times 2^{208}$ or approximately 2^{224}. Since there are 2^{256} different values that a hash can take, a random hash has a chance of about 2^{-32} to be lower than the maximum target.

$$T_{Max} = (2^{16} - 1)2^{208} \cong 2^{224} \quad (3)$$

$$T_{Cur} = \frac{(2^{16}-1)2^{208}}{D} \quad (4)$$

The expected number of hashes (N) that a miner needs to calculate to find a block with a given difficulty (D) is illustrated in Equation 5 [2]:

$$N = \frac{2^{256}}{\frac{(2^{16}-1)2^{208}}{D}} = \frac{2^{256}D}{(2^{16}-1)2^{208}} = \frac{2^{48}D}{(2^{16}-1)} = \frac{2^{48}D}{(2^{16}-1)} \cong 2^{32}D \quad (5)$$

Thus, every hash produced by a given miner has a probability (P) to validate a given block, as seen in Equation 6:

$$P = \frac{1}{2^{32}D} \quad (6)$$

Miners from all around the world compete using powerful dedicated mining computers to generate a valid hash. From the equations above, it is evident that such process imposes high levels of power consumption. Currently, adding a single transaction to the Bitcoin Blockchain platform consumes about 600 kWh [18]-[19] and the annual power consumption for the Bitcoin network is about 77.78 TWh, which is comparable to the power consumption of Chile. Furthermore, every node in the public Blockchain network has a local copy of the entire Blockchain. This drains huge amount of storage. Currently, the Bitcoin database exceeds 250GB and is growing up in a sharp exponential rate, as seen in Figure 2. The overall Bitcoin network is consuming more than 1000 TiB of storage per year [20] and is increasing in a sharp rate. This is due to the increase in the number of users of the Bitcoin network. Such properties will restraint the use of this technology in banking and commercial businesses.

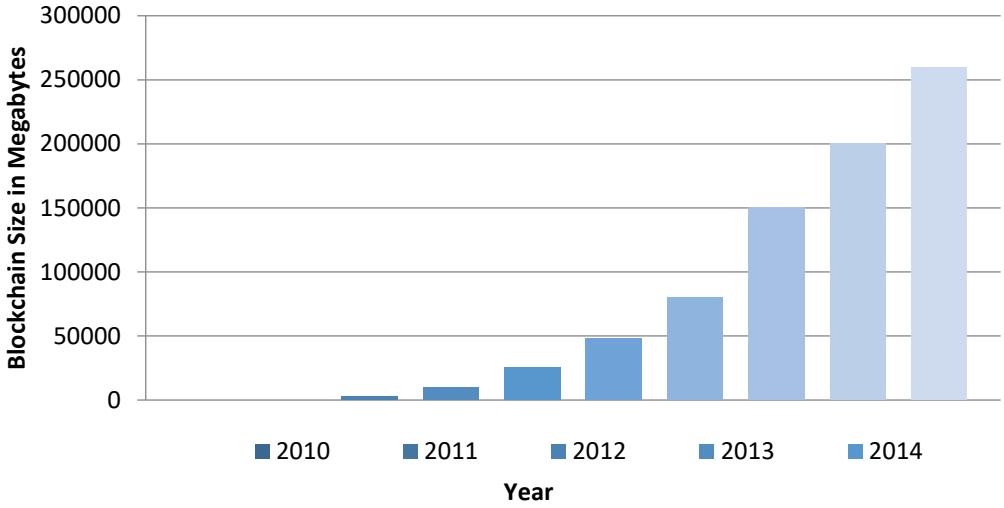

Figure 2. Size of blockchain database.

3. Proposed Hybrid Blockchain

To minimize the computational power and storage requirements, a hybrid Blockchain model that combines the centralized feature of servers with the distributed nature of Blockchains is proposed. Figure 3 illustrates the network infrastructure of the proposed system.

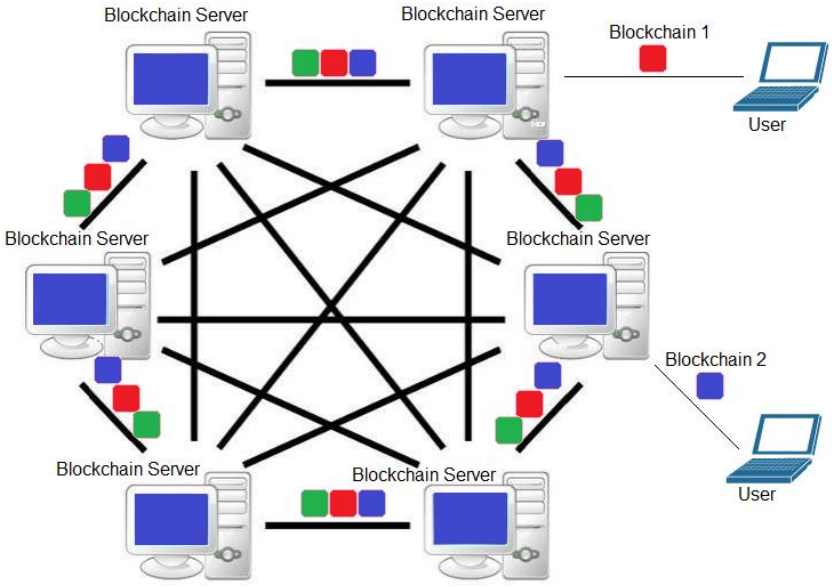

Figure 3. Proposed hybrid blockchain network infrastructure.

The proposed model can be highly beneficial to modern online businesses. Banks and e-commerce platforms have several servers distributed over a large geographical area. Using the proposed model, two sets of networks are defined: a personal Blockchain through which users can interface with the network servers and a global Blockchain consisting of interconnecting servers. The global Blockchain can be viewed as a chain of Blockchains that is distributed among servers and being updated periodically. In such scheme, users can access their respective personal Blockchain, hence accessing their private information only. No user can get hold of other users' personal data, which improves data privacy. Moreover, single or multiple private miners owned or governed by the local business policies are distributed among the network. Miners control the appending of new blocks and mapping hashes throughout the network without competing to solve a complex mathematical formula. This scenario can improve the network's security, since securing a Blockchain might require knowing participating miners' computational capabilities. This, in turn, aids in detecting potential selfish mining attacks [21-[22]. Normally, miners use the Proof-of-Work (PoW) as the security algorithm and compete trying to solve a complex computational challenge imposed by the PoW protocol. As a result, miners consume a huge amount of power [23]-[24], [15]. The proposed design includes single or multiple private trusted miners distributed throughout the network. Furthermore, the mining process can be fairly distributed among miners, hence immensely reducing the power consumption requirements of maintaining a Blockchain. Figure 4 illustrates the detailed architecture of the proposed Hybrid Blockchain.

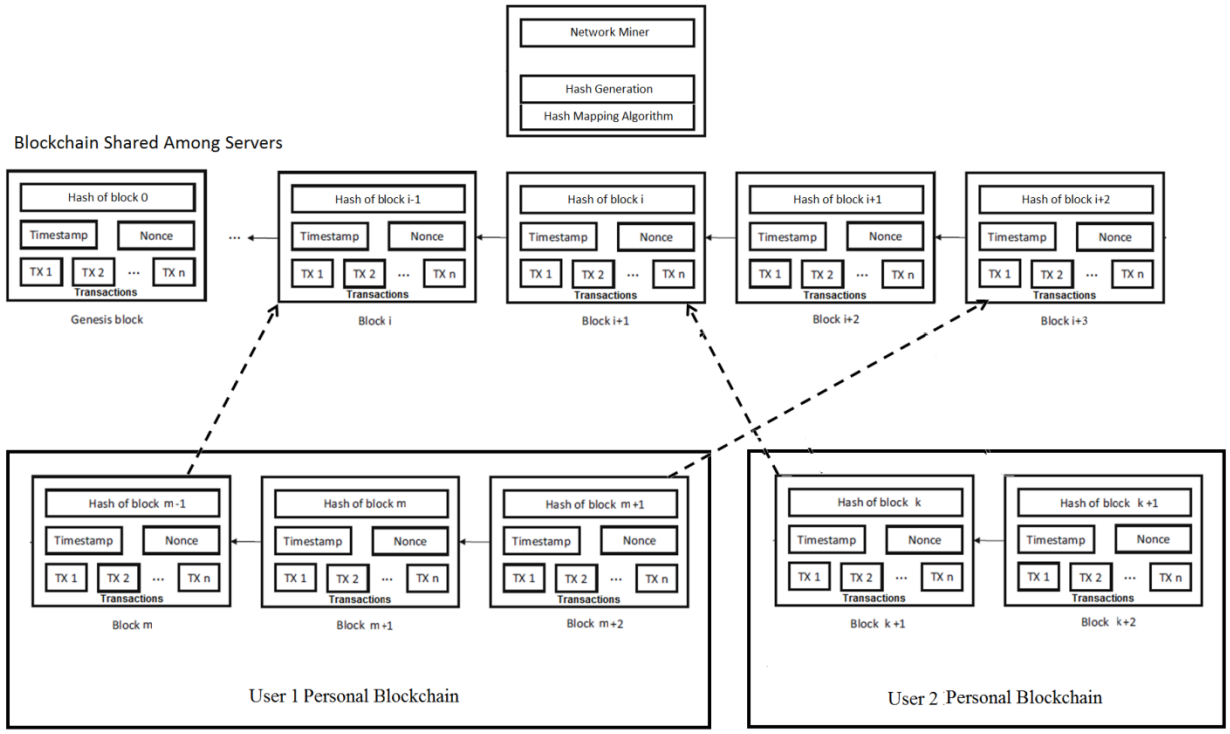

Figure 4. Proposed hybrid blockchain architecture.

In this scheme, every user has a copy of his/her personal Blockchain consisting of his/her personal transactions and information. Whenever a user executes a transaction, a broadcast request message is sent from the user's device to the miners throughout the network. Upon receiving the message, a specific miner, based on an election algorithm, will compute and produce a global hash and a private hash which is sent back to the user. Transactions and data blocks of the user's personal Blockchain are linked together through the received private hash. The user's data is saved locally on his device and also broadcasted to the data servers throughout the network. Hence, the locally saved user's Blockchain represents 50% of his/her overall personal network. The other 50% is represented by the business's servers. Each server holds a copy of a global Blockchain consisting of blocks from all connected users. The blocks are linked through a global

hash generated by the network's miner. Users can only access their respective information. Therefore, no user can access or view other users' personal data, hence improving data privacy.

Since miners are responsible for the generation of private and global hashes, a mapping algorithm should be used to track any network change. Mapping algorithms, in their simplest form, can be look-up-tables that are controlled by miners to translate and govern any change in the network. Furthermore, to reduce power consumption for maintaining the Blockchain, the mining process can be fairly distributed among miners. The distribution process can be based on an election algorithm to assign a miner. The election algorithm can be chosen upon the miner's geographical area, the miner's workload, user's ping signal latency or even randomly. Figure 5 illustrates an example of an election algorithm based on a specific user's ping signal latency.

```
1:   R_i = Request signal from user ⟨i⟩
2:   L_i = Latency of ping signal from miner to user ⟨i⟩
3:   M_j = Miner (j) in the network

4:   receive( R_i):
5:    do
6:       ping (i)
7:      calculate (L_i)
8:      broadcast (M_j, L_i)

9:   get(⟨M_j, (L_i)⟩ )_i:
10:   find (min(M_j, (L_i)) ∀j
11:   assign( M_j)
```

Figure 5. A sample election algorithm based on ping signal latency.

As seen in Figure 4, the network of each user is composed of the user's personal device, representing 50% of the network, along with the servers' network representing the remaining 50%. This scheme offers high levels of data security. This is due to the fact that hackers need to control the majority of the network's servers in addition to the client's device to achieve network consensus to alter or access only a single block. Assuming that there are several servers in a network, Equation 7 describes the minimal amount of devices "*K*" needed to alter a given user block, whereas Equation 8 illustrates the minimum amount of devices "*K*" needed to control several blocks within the network.

$$K \geq \frac{\sum S}{2} + 1 \tag{7}$$

$$K \geq \frac{\sum S}{2} + n \tag{8}$$

where,

S is a server holding the chain of Blockchains.
n: Number of different users within a selected portion of the Blockchain.

To reach consensus in conventional Blockchains, attackers only need to control a half of the nodes holding the data. Figure 6 illustrates the improved security of the proposed design against the current Blockchain system by comparing the minimal number of devices "*K*" needed to control the network as the number of users "*n*" increases.

Figure 7 presents the consensus algorithm used in the proposed design. Miners initiate the consensus protocol in the network through a '*proposed*' function illustrated at lines 7–14 of the algorithm, allowing them to propose new blocks. Afterwards, processes within the network decide whether a new block at a given index is valid at lines 16-23. Appending a new block is shown at line 24 depending on the function *get-main-branch( )*. Line 11 maps a global hash used in the servers' network with a local hash used within the personal network.

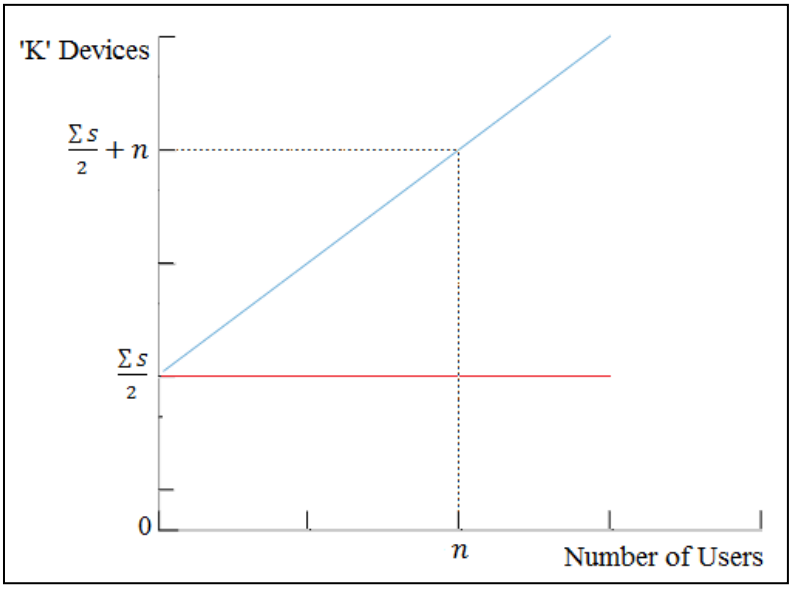

Figure 6. Number of devices to achieve network majority.

1: $j_i = \langle BL_i, PO_i \rangle$, *the local Blockchain at node* po_i *on the servers network is a directed acyclic graph of blocks* BL_i *and pointers* PO_i
2: $\ell_i = \langle B_i, P_i \rangle$, *the local Blockchain of a given user at node* p_i *on the user network is a directed acyclic graph of blocks* B_i *and pointers* P_i
3: bl, b *are blocks with the following fields*
4: $parent$, *the block preceding* bl, b *in the chain*
5: $pow, proof - of - work\ nonce\ of\ bl, b\ to\ verify\ the\ hash$
6: $children$, *the blocks succeeding* bl, b *in the chain*

7: $proposed(\,)_i$:
8: *do*
9: $nonce = random\_number(\,)$
10: *create block* $bl : bl.parent = last\_block(j_i)\ and\ bl.pow = nonce$
11: $Ln = map\_nonce(nonce)$
12: *create block* $b : b.parent = last\_block(\ell_i)\ and\ b.pow = ln$
13: $broadcast\ (\{\{bl\}, \{\langle bl, bl.parent\rangle\}\})$
14: $save\ (\{\{b\}, \{\langle b, b.parent\rangle\}\})$

15: $received(\langle B_j, P_j \rangle\,)_i$:
16: $BL_i \leftarrow BL_i \cup B_j$
17: $PO_i \leftarrow PO_i \cup P_j$
18: $B_i \leftarrow B_i \cup B_j$
19: $P_i \leftarrow P_i \cup P_j$
20: $\langle \overline{BL_\iota}, \overline{PO_\iota} \rangle \leftarrow get\_main\_branch(\,)$
21: $\langle \overline{\overline{B}_\iota}, \overline{\overline{P}_\iota} \rangle \leftarrow get\_user\_branch(\,)$
22: $if\ bl_0 \in \overline{BL_\iota} \wedge \exists\ bl_1, \dots, bl_m \in BL_i : \langle bl_1, bl_0 \rangle, \langle bl_2, bl_1 \rangle, \dots, \langle bl_m, bl_{m-1} \rangle \in PO_i\ and$
23: $b_0 \in \overline{\overline{B}_\iota} \wedge \exists\ b_1, \dots, b_m \in B_i : \langle b_1, b_0 \rangle, \langle b_2, b_1 \rangle, \dots, \langle b_m, b_{m-1} \rangle \in P_i\ then$
24: $append(b_0)$

Figure 7. Consensus algorithm.

4. CONCLUSION

As centralized systems need a central owner to connect and govern all other users and devices, the system structure is highly dependent on the network connectivity. Hence, abrupt failure of the entire system due to connectivity or security issues is likely to occur. Therefore, decentralized systems emerged as an alternative solution to resolve the security issues. One of the most recent promising decentralized architectures is Blockchain technology. Ever since, Blockchain has been adopted by businesses, e-commerce platforms and digital currencies like Bitcoin. However, as Bitcoin and related crypto-currencies have become increasingly popular, they have hit scalability and reliability issues. The process of improving scalability has been obstructed by an inherent trade-off between performance metrics and security requirements of the system

architecture. This paper proposes a hybrid Blockchain system that is suitable for banks and e-commerce businesses. Users can connect to servers using personal Blockchains, while servers share a chain of Blockchains throughout the business's private network. Miners governed by the business's policies control the appending of new blocks and mapping hash values. Having private miners will dramatically reduce power consumption demands and improve the overall quality of the Blockchain technology. This solution diminishes the space requirements of end users and enhances the security of the system by introducing personal networks. The proposed hybrid solution inherits the simple deployment and affordable maintenance in centralized systems while promoting resource sharing and improved scalability and fault-tolerance in decentralized systems.

REFERENCES

[1] S. Nakamoto, Bitcoin: Peer-to-Peer Electronic Cash System, 2008.

[2] I. Eyal, A. Efe Gencer, E. Gün Sirer and R. van Renesse, "Bitcoin-ng: A Scalable Blockchain Protocol," Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI '16), pp. 45-59, Santa Clara, CA, USA, March 16–18, 2016.

[3] L. W. Cong and Z. He, "Blockchain Disruption and Smart Contracts," The Review of Financial Studies, vol. 32, no. 5, pp. 1754-1797, 2019.

[4] R. Beck, M. Avital, M. Rossi and J. B. Thatcher, "Blockchain Technology in Business and Information Systems Research," Business & Information Systems Engineering, vol. 59, pp. 381-384, 2017.

[5] A. Wright and P. De Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia," SSRN, ID. 2580664, Elsevier, 2015.

[6] G. Zyskind, O. Nathan and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," Proc. of IEEE Security and Privacy Workshops, pp. 180-184, San Jose, CA, USA, 2015.

[7] Z. Zheng, S. Xie, H.-N. Dai, X. Chen and H. Wang, "Blockchain Challenges and Opportunities: A Survey," International Journal of Web and Grid Services, vol. 14, no. 4, pp. 352-375, 2018.

[8] M. Nofer, P. Gomber, O. Hinz and D. Schiereck, "Blockchain," Business & Information Systems Engineering, vol. 59, no. 3, pp. 183-187, 2017.

[9] J. Lindman, V. K. Tuunainen and M. Rossi, "Opportunities and Risks of Blockchain Technologies–A Research Agenda," Proceedings of the 50th Hawaii International Conference on System Sciences, pp. 1533-1542, [Online], Available: http://hdl.handle.net/10125/41338, 2017.

[10] V. Gramoli, "From Blockchain Consensus Back to Byzantine Consensus," Future Generation Computer Systems, vol. 107, pp. 760-769, 2020.

[11] J.-H. Huh and S.-K. Kim, "The Blockchain Consensus Algorithm for Viable Management of New and Renewable Energies," Sustainability, vol. 11, no. 11, ID. 3184, [Online], Available: https://doi.org/10.3390/su11113184, 2019.

[12] I. Eyal and E. Gün Sirer, "Majority Is Not Enough: Bitcoin Mining Is Vulnerable," Proc. of International Conference on Financial Cryptography and Data Security, pp. 436-454, Springer, Berlin, Heidelberg, 2014.

[13] A. Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-preserving Smart Contracts," Proc. of IEEE Symposium on Security and Privacy (SP), pp. 839-858, San Jose, CA, USA, 2016.

[14] S. Barber, X. Boyen, E. Shi and E. Uzun, "Bitter to Better—How to Make Bitcoin a Better Currency," Proc. of the International Conference on Financial Cryptography and Data Security, pp. 399-414, Springer, Berlin, Heidelberg, 2012.

[15] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu and J. Kishigami, "Blockchain Contract: Securing a Blockchain Applied to Smart Contracts," Proc. of the IEEE International Conference on Consumer Electronics (ICCE), pp. 467-468, 2016.

[16] D. Meshkov, A. Chepurnoy and M. Jansen, "Short Paper: Revisiting Difficulty Control for Blockchain Systems," Proc. of International Workshop on Data Privacy Management, Cryptocurrencies and Blockchain

Technology, pp. 429-436, Springer, Cham, 2017.

[17] D. Kraft, "Difficulty Control for Blockchain-based Consensus Systems," Peer-to-Peer Networking and Applications, vol. 9, no. 2, pp. 397-413, 2016.

[18] H. Vranken, "Sustainability of Bitcoin and Blockchains," Current Opinion in Environmental Sustainability, vol. 28, pp. 1-9, 2017.

[19] K. J. O'Dwyer and D. Malone, "Bitcoin Mining and Its Energy Footprint," Proc. of the 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014), pp. 280-285, 2014.

[20] E. Francioni and F. Venturelli, "The Dusk Network and Blockchain Architecture," WEB3 Symposium, Amsterdam, The Netherlands, [Online], Avaialble: https://dusk.network/uploads/dusk-whitepaperv1.pdf, 2018.

[21] P. H. Gleichauf, "Blockchain Mining Using Trusted Nodes," U.S. Patent Application Publication, Pub. no. US 2018 / 0109541 A1, [Online], Available: https://patentimages.storage.googleapis.com/23/4f/69/4bbc963131ccbc67/US20180109541A1.pdf, May 14, 2019.

[22] A. Shariar, Md. A. Imran, P. Paul and A. Rahman, "A Decentralized Computational System Built on Blockchain for Educational Institutions," Proceedings of the International Conference on Computing Advancements, pp. 1-6, [Online], Available: https://doi.org/10.1145/3377049.3377058, 2020.

[23] M. Crosby, Nachiappan, P. Pattanayak, S. Verma and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," Applied Innovation Review (AIR), no.8, pp. 6-19, June 2016.

[24] BitFury Group, "Proof of Stake *versus* Proof of Work," White Paper, Version 1, pp. 2-26, [Online], available: https://pdfs.semanticscholar.org/6990/0bac4097a576414f69f1998c11089fb5bb94.pdf, September 2015.

[25] J. Spasovski and P. Eklund, "Proof of Stake Blockchain: Performance and Scalability for Groupware Communications," Proceedings of the 9th International Conference on Management of Digital EcoSystems, pp. 251-258, [Online], available: https://pure.itu.dk/portal/files/83126213/Proof_of_Stake_Blockchain_Performance_and_Scalability_for_Groupware_Communications.pdf, 2017.

ملخص البحث:

تعدّ "سلسلة الوحدات" تقنية ثورية اكتسبت شعبية واسعة منذ ظهور ما يُعرف بالنقود الخفيّة. وقد تخطى استخدام هذه التقنية العُملة الرقمية الى ميدانٍ أرْحب شمل إنترنت الأشياء، وتطبيقات الأمان، والأنظمة الذكية، على سبيل المثال لا الحصر. ومع تنامي أعداد مستخدمي تلك السلاسل، بدأت بعض السلبيات بالظهور؛ إذ إنّ تلك السلاسل تستهلك كميات زائدة من الطاقة لتخزين البيانات ومعالجتها. من ناحية أخرى، فإن الطبيعة المحدودة لتلك السلاسل من حيث قابليتها للتوسيع، بسبب المتطلبات الهائلة اللازمة لتخزين البيانات، ربما تشكل معضلة. ولتحسين الأداء الإجمالي، لا بدّ من التغلُّب على العديد من التحديات في البنية الراهنة للسلاسل موضوع هذه الدراسة.

تقدم هذه الدراسة بنيةً هجينةً لسلاسل الوحدات تجمع بين الطبيعة التوزيعية للسلاسل والسمة المركزية للخوادم. في النظام المقترح، يتصل المستخدمون عبر السلاسل الشخصية، بينما تتشارك الخوادم سلسلةً من سلاسل الوحدات لضمان سلامة النظام وأمانه. وهذا من شأنه أن يقلص من متطلبات التخزين للمستخدمين النهائيين ويحسن من قابلية الشبكات للتوسيع. ومن المؤمل أن تستفيد مؤسسات الأعمال من البنية المقترحة؛ لأنها تخلق نموذج أعمالٍ موثوقاً وقابلاً للتوسيع.