Security Issues in Decentralized Internet Blockchain and Secure Energy Trading

Abdullah Bajahzar

Department of Computer Science and Information,
College of Science at Zulfi,
Majmaah University,
Zulfi 11932, Saudi Arabia

Summary

Blockchain innovation has always pointed out hopeful prospects and interesting applications. The innovation has effectively supplanted economic transaction frameworks in different associations and can possibly patch up heterogeneous plans of action in various ventures. Despite the fact that there are a few investigations related to the protection and security issues of the blockchain, no accurate examination on the blockchain security frameworks are available. In this paper, we direct a precise report on the dangers of security to blockchain and study the comparing genuine assaults by looking at well-known blockchain frameworks. We additionally survey the security upgrade answers for blockchain, which could be utilized in the advancement of different blockchain frameworks, and recommend more ideas to motivate doing research inquire about attempts into this zone. An ideal valuing methodology employing Stackelberg game for credit-based advances is likewise suggested. Security investigation and numerical outcomes dependent on a genuine dataset delineate that the suggested energy blockchain and credit-based installment plot are secure and proficient in IIoT

Key words:
Decentralized Internet, Blockchain, Security, Cryptocurrency.

1. Introduction

Being a decentralized framework, blockchain frameworks do not need confusing other party trusted authority. Rather, to ensure the consistency and dependability of the information and exchanges, blockchain gets the decentralized agreement system. In the current blockchain systems, there are four noteworthy accord components [1], namely PBFT (Practical Byzantine Fault Tolerance), PoS (Proof of Stake), PoW (Proof of Work), and DPoS (Delegated Proof of Stake). Different agreement instruments, for example, [1] PoA (Proof of Authority), [2] PoB (Proof of Bandwidth), [3] PoET (Proof of Elapsed Time), [4] et cetera, are additionally utilized in various blockchain frameworks. The most prevalent blockchain frameworks (i.e., Ethereum and Bitcoin) utilize the PoW system.

After the Internet, the blockchain is viewed as the following huge reforming innovation, as it is reexamining the manner in which we live and work. During 2008, the blockchain was initially offered by a scientist who presented the computerized digital currency called bitcoin, in which the blockchain is a vital piece of its performing [5]. Many cryptographic forms of money with much motivated highlights have represented from that point forward, for example, the Ethereum which shows shrewd contracts [6]. The central qualities of the blockchain are represented in figure 1.

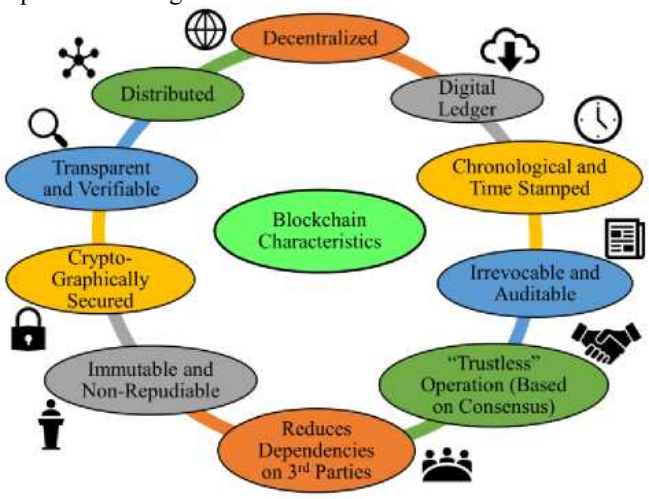

Fig. 1 Blockchain characteristics.

For various decades, we have been exchanging information, and transferal of cash and different resources through online exchanges by means of the Internet, where every one of these transactions implicated a reliable intermediate partner.

As blockchain is a fundamental advance in industry of FinTech (Financial Technology), clients are exceptionally worried for the inherent security. Moreover, some security assaults and vulnerabilities were lately

Manuscript received September 5, 2020
Manuscript revised September 20, 2020

DOI: 10.22937/IJCSNS.2020.20.09.1

announced. Loi et al. noted that 8,83 among 19,37 actual Ethereum contracts are defenseless [7]. Notice that savvy contracts including security vulnerabilities are likely to prompt budgetary misfortunes. In June 2016, for example, the offenders assaulted the smart contract DAO [8] by misusing a repeated calling vulnerability, and about 60 million dollars have been stolen.

One other example, in March 2014, the culprits abused exchange variability in Bitcoin to assault MtGox, the biggest Bitcoin exchanging stage. Also, it creates the crumple of MtGox, with an amount of stolen 450 million dollars Bitcoin [9].

Despite the fact that there are some ongoing investigations on the security of blockchain, none of them plays out an efficient investigation on the dangers to blockchain frameworks, the relating genuine assaults, and also the improvements of security. The nearest look into business to our own is [10] that just spotlight on Ethereum smart contracts, as objected to mainstream blockchain frameworks. Their business dissects the security vulnerabilities of Ethereum smart contracts, and grants scientific classification of main programming traps that can do rapid vulnerabilities [10]. Despite the fact that a progression of related assaults on smart contracts is registered in [10], there does not have a talk on security improvement. This paper handles the blockchain security from various viewpoints.

Moreover, the blockchain dispenses with the need of whatever centric authority between many gatherings performing monetary and information transactions by employing an ethical, decentralized and permanent open record. The open record is a shared circulated database over all the system members.

It is a carefully designed, cryptographically guaranteed, and changeless record of the great number of transactions that at any point happened among the members. They can see the transactions identified with them whenever they need, yet once became suitable and combined to the blockchain, the transactions cannot be adjusted nor erased, which activates the blockchain irreversible and permanent. Every exchange is examined by the members through agreement instruments without verification or confirmation by any central authority and methods for pre-characterized approval.

This decreases the expense and disposes of the odds of data adversity because of a solitary purpose of disappointment, since record duplicates are synchronized over every one of the members. Along these lines, notwithstanding its notable merits which incorporate changelessness, approval, decentralization and straightforwardness, the blockchain guarantees to give security and protection on all occasions. Figure 2 indicates the distinction between the decentralized blockchain framework and centralized execution of transactions.
These are the sections of this paper: section 2 presents the blockchain systems. Section 3 and 4 show applications and types of blockchain. Section 5 examines the challenges and issues of blockchain, and surveys of real attacks on blockchain systems. Finally, Section 7 presents conclusion of the paper.

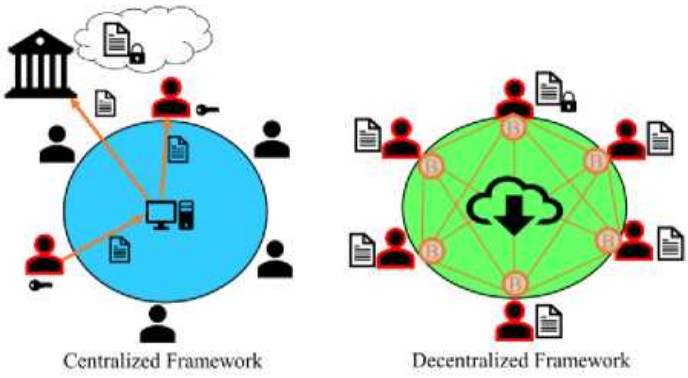

Fig. 2 Centralized versus decentralized blockchain systems.

2. The blockchain

It is an arrangement of 'N clients over a system sharing data and performing trade of assets. Rather than depending between among them, they concede to a convention called an accord calculation, which empowers them to build up common trust and considers approving the exchanges on a distributed premise. Accordingly, the building squares of a blockchain-based framework incorporate the system members and consensus protocol, for example, cryptographic hashes, confirmation of work, and digital signatures.

The system members can be people, associations or foundations participating a duplicate of the record involving their legitimate exchanges in a consecutive order. The record is made out of an arrangement of squares as indicated in Figure 3, jointly related by their mixed esteems in successive request to preserve information trustworthiness and convenience. Also, each square comprises of transactions arranged carefully marked by the owner and confirmed by whatever remains of the members previously being added to the square. A few highlights of the blockchain are currently examined.

With the above merits as a basic part of the blockchain working, it guarantees information changelessness, information honesty, information verification and approval, decentralization and information straightforwardness, hence guarantying information security crosswise over appropriated frameworks. The blockchain can be changeless. The records is changed just if more 51% of the hubs are controlled by programmers, or, in other words. The innovation is self-sufficient, and it keeps up the namelessness of the beneficiary and sender in the transaction by employing private and open nodes keys.

3. Type of blockchain

Blockchain innovations is generally partitioned into three kinds.

1) Public blockchain: The transaction can be confirmed and checked by everyone who can take an interest in the way toward having accord. Like Ethereum and Bitcoin are together public Blockchain (See figure 3).

2) Consortium blockchains or semi-private system (Fig. 4): This type suggests the hub that had specialists can be hung time, as a rule, has relations across different organizations. Also, data in blockchain may be private or open. It may be observed as partially decentralized. Two examples consortium blockchains may be mentioned, namely R3CEV and hyper record.

3) Private Blockchain (Fig. 5): Few out of every odd hub can take an interest in this blockchain, has strict expert information administration. The node will be confined.

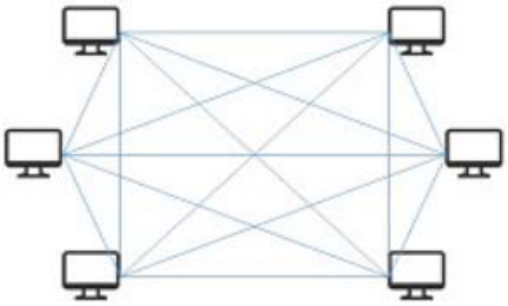

Fig. 3 Overview diagram of a public blockchain.

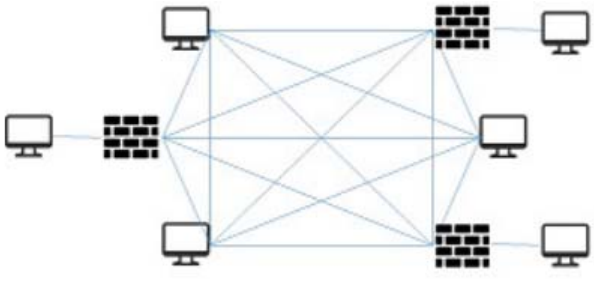

Fig. 4 Overview diagram of a consortium blockchain.

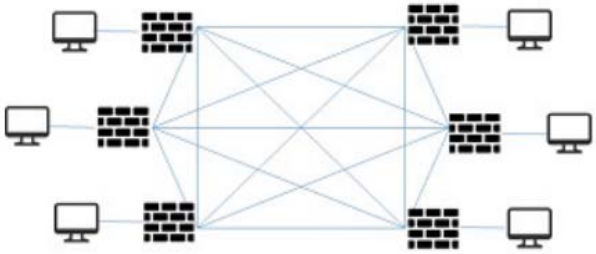

Fig. 5 Overview diagram of a private Blockchain.

4. The blockchain applications

The hopeful highlights of blockchain are disturbing various ventures pulled in towards this innovation, yet it is vital to analyses their reasonableness to every industry requirements. It is an upset however not a remedy for all the business needs. In the case that just the accompanying circumstances emerge, would organizations be able to consider conveying a blockchain oriented safety solution:

- A gathering of individuals or various gatherings much of the time creates exchanges relying on a third party.
- It is not possible to authenticate this third party. The authenticity of the exchanges is sketchy.
- The approval of exchanges is a need and consequently an improved framework recalling information trustworthiness and credibility is vital.

Information trustworthiness over privacy and preparing execution is imperative. For time-delicate applications, the blockchain is not proper because it requires investment for a square to be acknowledged in the chain. On account of bitcoin, this time is around 10 minutes.

Information in the conveyed public ledger is safe to any altering as it is very encoded utilizing propelled cryptography, consequently the innovation discovers applications in cyber security. Moreover, it kills the utilization of incorporated gadgets in the IoT and different types of systems administration. Accordingly, gadgets associated could refresh programming, oversee bugs and conveyed specifically. The innovation gives another method for overseeing trust and can be adequately connected in protection and spaces like fund, as introduced in figure 6 [11]. It wipes out the contribution of an outsider; consequently it is finding viable usage in private ride-sharing and transport. It is imagined that the blockchain can be critical applications in brilliant human services with the Internet of Health Things (IoHT) or the

Internet of Medical Things (IoMT) to give protection, security, and successful protection preparing [12].

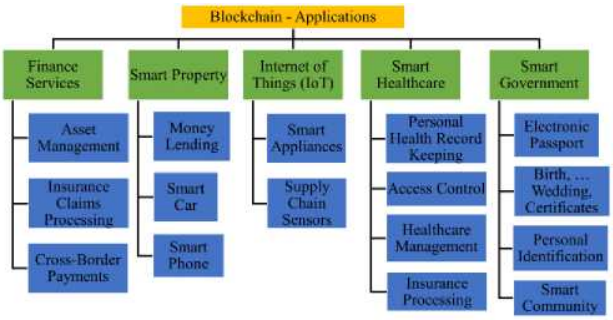

Fig. 6 Examples of blockchain applications.

4.1 Proof of Work

This function is considered a fragment of information that its production is arduous, expensive and consumes time. However, it is simple for others to check. It satisfies particular requirements. Distributing a proof of work (PoW) can be an irregular procedure involving finite alternatives. Therefore, a considerable number of testing is needed by and large prior a substantial verification of work is reproduced. Bitcoin uses the Hashcash confirmation of work framework. During ascertaining PoW, it is designated "mining". Moreover, each square has an irregular value named as "Nonce" in square header. When modifying this nonce value, Prof of Work requires to generate an esteem that makes this square header hash esteem not accurately a "Trouble Target" that had been implemented.

Trouble indicates period of time it will spend when the hub computing hash value is different from the target value. For acknowledging a block by system members, miners have to finish a PoW that handles the majority of information in the square. The deficiency of this task is balanced in order to reduce the speed of new squares production through the system to one at regular intervals. Due to the extremely unpleasant small opportunities of fruitful age, this induces a capricious way to a typical PC in the system to have the ability to create the subsequent block [13, 14].

4.2 Proof of State

PoW technique leads to consume a large amount of power and will cause a lot of power loss during the process. Thus, this issue related to power waste should be addressed. However, the amount of computing power required by Proof of Stake (PoS) is not large. For this technique, the capital that is considered is the measure of Bitcoin a digger holds. A person that holds 1% of the Bitcoin can mine 1% of the PoS block [15]. This technique enhances assurance against vindictive assault on the system. Additional insurance results from two origins:

- Performing an assault is significantly more expensive.
- Decreased attack instigations. The attacker attempts to want to possess the almost majority of the available bitcoins. Thus, the attacker will seriously suffer from his personal action.

5. Issues and Challenges of Security

Up until this time, blockchain has gained numerous regard in several areas, in any case, it likewise occurs a few difficulties and issues needs to challenge it [16, 17].

5.1 Majority attack

With PoW technique, the probability of mining a block depends on the actions performed by the miner and the related time to achieve this work. Regarding this system, the attackers will require to consolidate with the final aim in order to mine additional blocks, and advance on behalf of turning out to be mining pools and getting more processing force. To dominate this blockchain, individuals should reach to hold at least 51% of computing power. Obviously, this induces some issues related to security [18, 19]. When someone exceeds 51% of computing power, this person is able to reach Nonce value more prompt than the competitors. This person will have the opportunity to select which block is allowable. It is possible to:

1) Modify the transaction information; it might bring about multiplied spending assault [20, 21].
2) End the block checking transaction.
3) Finish mineworker mining any accessible block. In the past, a large amount of attacks were possible since the majority of transactions had significant values and their rates were slow [22].

5.2 Fork issues

An additional problem is related to fork issue. This problem is identified with decentralized purview, contract while upgrading the software. It is considered a vital concern since it includes a great range in blockchain.

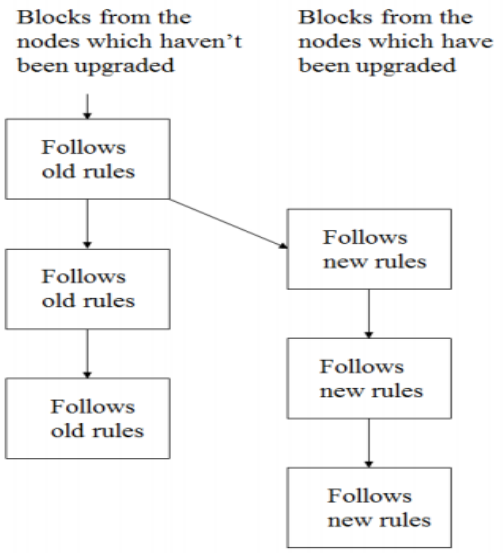

Fig. 7 Hard Fork.

Types of Forks

At the point when the new form of blockchain programming issued, new approval in majority run likewise altered to the hubs. Consequently, the hubs in blockchain system can be separated into these two kinds, the Old Nodes and the New Nodes. Thus, these are the four configurations:

1) There is an agreement between the new nodes and the block transaction transmitted by the old ones.
2) The opposite of the above situation.
3) There is an agreement between the old nodes and the block transaction transmitted by the new ones.
4) The opposite of the above situation.

As a result of the occurrence of the above mentioned situations, fork issues is split in two categories, namely Soft Fork and Hard Fork. Furthermore, the differentiation between the new and old nodes is made on the basis of the processing power.

Hard Fork

This category takes place when framework flows to new adaptation or another approval. There is no perfect connection with last variant. It involves a radical modification of the network protocol. Thus, previous invalid transactions or blocks become valid and inversely. Although new hubs registering power are further established than old ones, the later will in any case continue to retain the chain although it was accurate. Figure 7 demonstrates the hard fork issue. When Hard Fork takes place, all hubs are asked to update the agreement; the hubs that have not been redesigned will of course not continue to fill. In the event that more old hubs are progressively not revised, they will persist progressing at the other wholly unique chain. This indicates that the customary chain will split in two chains.

Soft Fork

In this category, only former transactions or blocks become invalid. The new hubs could not be in agreement with the mining of the old ones.
When Soft Fork takes place, nodes do not require to renovate the new acceptance in the meantime, it permits redesigning bit by bit not such as Hard Fork, Soft Fork just involves only one chain. It will not influence the adequacy and security of framework when nodes overhaul. Nonetheless, Soft Fork induces to the old nodes to be unconscious and the agreement rules will be altered, as opposed to the standard of each node can confirm effectively to some degree.

5.3 Blockchain scale

As blockchain enhancing, information winds up better and better, the stacking of store and registering will also getting increasingly hard, it sets aside a lot of chance to coincide information, in an identical time, information still consistently increasing, conveys a significant matter to the client when operating the framework [23].

Simplified Payment Verification (SPV) is considered an installment confirmation innovation, without keeping up full blockchain data, just requires to make use of block header message. Also, this renewal can incredibly mitigate customer supply in blockchain payment confirmation. It brings down the client's importance when exchange definitely developed later on.

5.4 Blockchain data time confirmation

Contrasted with conventional online credit card transaction, typically needs 2 or 3 days to confirm the transaction, about 1 hour is sufficient to confirm a bitcoin transaction. It is greatly advanced than the conventional operation. However, this result does not reach the requisite value.

Lightning Network is a solution to this issue [24]. This protocol takes profits of Hashed Time Lock Contracts (HTLCs). It has two-ways payment channels. This enables payments to be safely over different distributed payment channels. This authorizes the development of a system in which any peer on the system can pay some other associate independently of whether they do not straightforwardly have a channel open between them.

5.5 Current Regulations

Utilizing Bitcoin for example, the decentralized framework qualities, will feeble the national bank's capacity for controlling the monetary strategy and the cash measure, that effects on government to be concerned of blockchain innovations, experts need to explore this new matter, accelerate considering new approach, it will also have risk on the market.

5.6 Integrated Cost Issue

Clearly it will have much of expense involving time and cash to modify presenting framework, especially when it's a foundation. We need to confirm this inventive innovation not just make monetary advantages, achieve the supervision necessities, yet in addition relate with conventional association, and it mostly encounter troubles from inner association which is occurring at this point.

5.7 Blockchain Energy Performance Analysis

The overlay Cluster Head (CH) keeps up an open BC connected to two key records. These key records are: requester key records that is considered the rundown of overlay clients' PKs that are permitted to get to information for the brilliant homes connected with this cluster; asked for key records that is the rundown of PKs of smart homes linked with this group are permitted to be gotten to. Cloud storage can be utilized by the savvy home gadgets to offer and store information. Figure 8 indicates the proposed BC-based architecture. The cloud storage and a subtle element of the overlay has been discussed in [25].

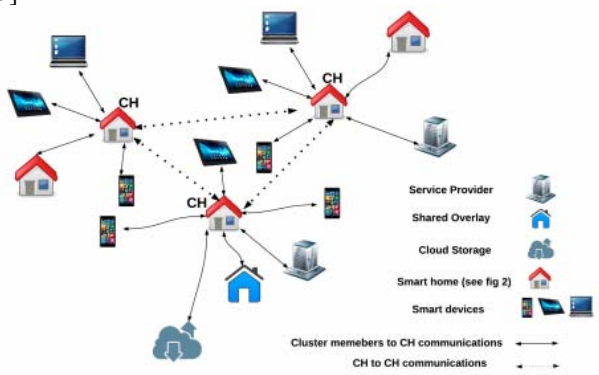

Fig. 8 The proposed BC-based architecture overview

We look at the transaction affirmation time versus the energy transaction frequency for several blockchains. The performance of the normal exchange rate related to the suggested credit-based payment process is assessed. Moreover, the rate of transaction points out the quantity of completed vitality transaction 60 minutes. The aggregate transaction affirmation time on the normal implies the normal time of performing the accord procedure of a vitality transaction for an energy hub. With the end goal of delineation, we reproduce the execution among 50 sets of IIoT hubs for 4 hours. As in Bitcoin, the transaction affirmation time related to conventional blockchains is an hour, whereas the current energy blockchain is adjusted to be 10 minutes for instance [26]. The overall number of pre-chosen EAGs is 51 in our vitality blockchain. Also, the values of the energy transaction frequency during one hour belong to the set {1, 2, 3, 4, 5} equiprobably for IIoT hubs. Every IIoT hub has 20 energy coins in the wallet for P2P energy transaction.

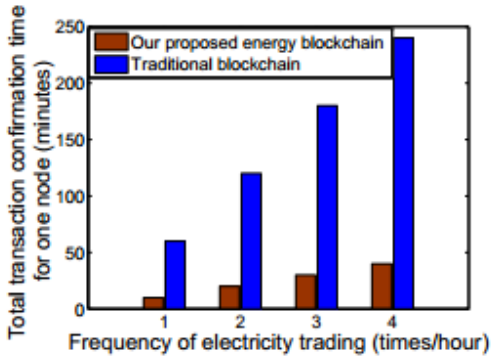

Fig. 9 Transaction confirmation time performance.

Figure 9 indicates that, regarding a conventional blockchain (e.g., Bitcoin), the mean value of the overall transaction affirmation time for a vitality hub is larger than that related to the current vitality blockchain when the vitality transaction frequency grows. This is because of the manner that our vitality blockchain just does the accord procedure on the pre-chosen EAGs rather than every single connected hub in the tconventional blockchain.
Figure 10 exhibits the mean value of the transaction rate of vitality transaction diverse plans. Amid vitality transaction, IIoT hubs without enough vitality coins can't do next vitality transaction until the last transaction accomplishing the agreement procedure. Thus, as appeared in Fig. 10, the conventional blockchain and our vitality blockchain have a furthest breaking point of the mean transaction speed in 60 minutes.

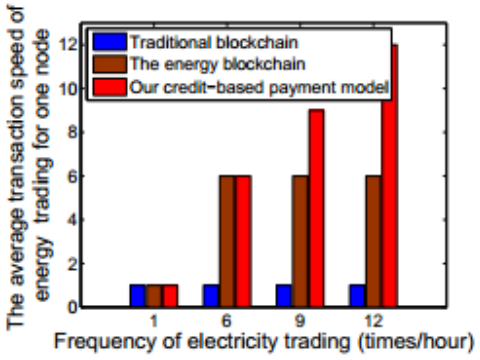

Fig. 10 Transaction speed performance.

The transaction speed of the credit-based payment scheme is larger as a result of the assistance of credit banks in EAGs. Also, these credit banks give sufficient energy coins to IIoT hubs to constantly perform energy transaction on vitality blockchain. Furthermore, there are no restriction of transaction affirmation delays. The outcomes point out that the suggested plan bolsters quick P2P energy transaction, in this way empowering continuous energy transaction among IIoT hubs.

6. Conclusion

The blockchain is a successful technology of the hundreds of years old agreement issue. This paper focuses on the blockchain's security issues. Concentrating the famous blockchain frameworks, we lead a deliberate investigation on the security dangers to blockchain. For each hazard or defenselessness, we investigate its reasons and conceivable result. It appears clearly that blockchain is a recent matter of major importance, despite the fact that there are still some issues that deserve to be investigated more deeply, some other problems have just been promoted alongside new strategies are developing on the application side.

Security investigation indicates that energy blockchain performs guaranteed energy blockchain. Numerical simulations demonstrate that the vitality blockchain and the credit-based installment plot are powerful and productive. Furthermore, some other fascinating issues can be additionally considered, for example, ideal energy aggregator determination, special plans intended for dishonorable situations incorporating IIoT hubs with fantastic or poor credit esteems.

References

[1] Z. Zheng, S. Xie, H.-N. Dai, H. Wang, Blockchain challenges and opportunities: A survey, in: International Journal of Web and Grid Services, 2016.

[2] M. Ghosh, M. Richardson, B. Ford, R. Jansen, A torpath to torcoin, proof-of-bandwidth altcoins for compensating relays (2014). URL https://www.smithandcrown.com/open-research/a-torpath-to-torcoin-proof-of-bandwidth-altcoins-for-compensating-relays

[3] Intel, Proof of elapsed time (poet) (2017). URL http://intelledger.github.io/

[4] P. technologies, Proof of authority chains (2017). URL https://github.com/paritytech/parity/wiki/Proof-of-Authority-Chains

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

[6] P. Bailis, A. Narayanan, A. Miller, and S. Han, "Research for practice: cryptocurrencies, blockchains, and smart contracts; hardware for deep learning", Communications of the ACM, Vol. 60, No. 5, 2017, pp. 48-51.

[7] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, A. Hobor, Making smart contracts smarter, in: The ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 254-269.

[8] V. Buterin, Critical update re: Dao vulnerability (2016). https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/

[9] J. Adelstein, Behind the biggest bitcoin heist in history: Inside the implosion of mt.gox (2016). URL http://www.thedailybeast.com/articles/2016/05/19/behind-the-biggest-bitcoin-heist-in-history-inside-the-implosion-of-mt-gox.html

[10] N. Atzei, M. Bartoletti, T. Cimoli, A survey of attacks on ethereum smart contracts (sok), in: International Conference on Principles of Security and Trust, 2017, pp. 164-186.

[11] Elio-David Di Iorio, 17 Blockchain Applications That Are Transforming Society, https://blockgeeks.com/guides/blockchain-applications

[12] P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. Ganapathiraju, "Everything You Wanted to Know about Smart Healthcare", IEEE Consumer Electronics Magazine (CEM), Volume 8, Issue 1, January 2018

[13] I. Bentov, A. Gabizon, and A. Mizrahi, "Cryptocurrencies without proof of work," CoRR, vol. abs/1406.5694, 2014.

[14] A. Gervais, G. O. Karame, K. W¨ust, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS'16), pp. 3–16, New York, NY, USA, 2016.

[15] S. King and S. Nadal, Ppcoin: Peer-to-peer Crypto-Currency with Proof-of-Stake, 2012. (https://archive.org/stream/PPCoinPaper/ ppcoin-paper_djvu.txt)

[16] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in IEEE Symposium on Security and Privacy, pp. 104– 121, May 2015.

[17] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on bitcoin's peer-to-peer network," in 24th

USENIX Security Symposium, pp. 129–144, Washington, D.C., 2015.
[18] N. T. Courtois and L. Bahack, "On subversive miner strategies and block withholding attack in bitcoin digital currency," CoRR, vol. abs/1402.1718, 2014.
[19] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," CoRR, vol. abs/1311.0243, 2013.
[20] G. O. Karame, "Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin," in Proceedings of Conference on Computer and Communication Security, pp. 1–17, 2012.
[21] M. Rosenfeld, "Analysis of hashrate-based double spending," CoRR, vol. abs/1402.2009, 2014.
[22] A. Gervais, H. Ritzdorf, G. O. Karame, and S. Capkun, "Tampering with the delivery of blocks and transactions in bitcoin," in Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security (CCS'15), pp. 692–705, New York, NY, USA, 2015.
[23] G. Karame, "On the security and scalability of bitcoin's blockchain," in Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS'16), pp. 1861 1862, New York, NY, USA, 2016.
[24] Y. Sompolinsky and A. Zohar, Secure High-Rate Transaction Processing in Bitcoin, pp. 507–527, Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.
[25] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: Challenges and solutions," arXiv preprint arXiv:1608.05187, 2016
[26] Z. Zheng, et al, "Blockchain challenges and opportunities: A survey". Workshop Paper, Inderscience Publishers: Geneva, Switzerland, 2016.

Author Biography

Abdullah Bajahzar received a PhD in Computer Science and Software Engineering degree from De Montfort University, United Kingdom, in 2014 and MSc Software Engineering degree from De Montfort University, United Kingdom, in 2008. He is currently working as an Assistant Professor at Majmaah University, Saudi Arabia. His research interest includes data mining, big data, IoT and data science