International Journal of Safety and Security Engineering
Vol. 11, No. 2, April, 2021, pp. 201-205
Journal homepage: http://iieta.org/journals/ijsse

Secured Resource Allocation for Authorized Users Using Time Specific Blockchain Methodology

Vejendla Lakshman Narayana*, Divya Midhunchakkaravarthy

Lincoln University College, Wisma Lincoln, No. 12-18, Jalan SS 6/12, 47301 Petaling Jaya,Selangor Darul Ehsan, Malaysia

Corresponding Author Email: lakshmanv58@gmail.com

https://doi.org/10.18280/ijsse.110209

Received: 29 August 2020
Accepted: 13 March 2021

Keywords:
resource allocation, blockchain, authorized users, malicious activities, unauthorized user prediction

ABSTRACT

The utilization of energy in blockchain division is high as resource allocation models are using this technology and the rundown of resource utilization cases is continually developing. The communicated and permanent nature of blockchain innovation might be utilized to quicken the progressing change to increasingly decentralized and digitalized vitality frameworks and to address a portion of the difficulties the business is confronting in providing security in identification of authorized users and resource allocation transactions among the authorized users. The allocated resources to the users need to be recorded, otherwise the attackers may use them for malicious operations. In any case, blockchain is a developing innovation and it is viewed as a basic vulnerability by numerous users as the difficulties and chances of execution are still to a great extent. There is in this way an absence of information and shortage of dynamic gadgets for getting why, when and how the innovation can include significant worth. The proposed Resource Allocation for Authorized Users using Time specific Blockchain Methodology (RAAUTBM) performs resource allocation to authorized users to avoid malicious actions among blockchain-based use cases and increase practical information about how blockchain could be actualized. The RAAUTBM model verifies all the users for allotting access to the system. The proposed model allots the resources only to the authorized users and to identify the malicious users and remove them from the framework. The resources once allotted to a user remains for a time interval and then the resource is re-allotted to other authorized users for avoiding delay. Resource exchanges in this segment are known to be dull and wasteful, to a limited extent because of the absence of promoted straightforwardness. This research work centers around the advancement of a blockchain application that can improve the resource exchange procedure among authorized users. The proposed model is compared with the traditional methods and the results demonstrate that the proposed model is effective in allocating resources only to the authorized users.

1. INTRODUCTION

Blockchain innovation is the recent trend that creates blocks for advanced records of physical and authoritative data, it does likewise accompany difficulties. These are because of the absence of normalization and restricted instances [1]. Thus the execution of the proposed model is very unpredictable. At present, the rightness of archives should be approved by authorized nodes in the system, because of the absence of normalization [2]. For the framework to include esteem information, for example, reports and investigation systems must be normalized [3]. On the off chance that this is conceivable, the record-keeping application could be connected to different collection levels by method of an API [4]. Along these lines, information could be naturally approved without the requirement for prophets, and dissected by the client. Resource allocation among the authorized users reduces the malicious actions like denail of service, packet droppings, fake message transmission in the group of transactions which improves security [5].

Additionally, approval controls in the system could be significantly more point by point. This could make the proposed application appropriate for overseeing physical and authoritative information, which, significantly, could upgrade the exchange procedure [6]. The procedure is division wide known to be awkward, anyway there is certifiably not an extraordinary enough motivator for one single gathering to build up a blockchain foundation – all gatherings would need to join to utilize it for it to be significant [7]. Moreover, all corporate gatherings could profit by greater unwavering quality, straightforwardness and efficiency [8]. Thus, a coordinated effort between keeps funds with an enormous market inclusion that would be best positioned to start to lead the pack in normalizing reports for financing and, thusly, the advancement of a blockchain foundation as proposed. The resource allocation in blockchain is depicted in Figure 1.

The proposed model utilize a blockchain based foundation to improve the recede and flow exchange procedure of an resource [9]. During approval of the application, all gatherings showed that the application is an intriguing initial move towards an advanced and progressively straightforward environment [10]. The structure and nature of information these are the primary components in a resource exchange as are fundamental if the procedure is to be smoothed out and accessibility will be improved by actualizing the proposed blockchain framework [11]. The application improves the

manner in which explicit resource are comprehended by organizing physical and legally binding data in a single spot, and ensures the nature of the information by utilizing the blockchain resources [12]. Consequently, the resource is of vast incentive for the eventual fate of resource information with the authorized users and the exchange procedure. The resource exchange process that creates blocks is depicted in Figure 2.

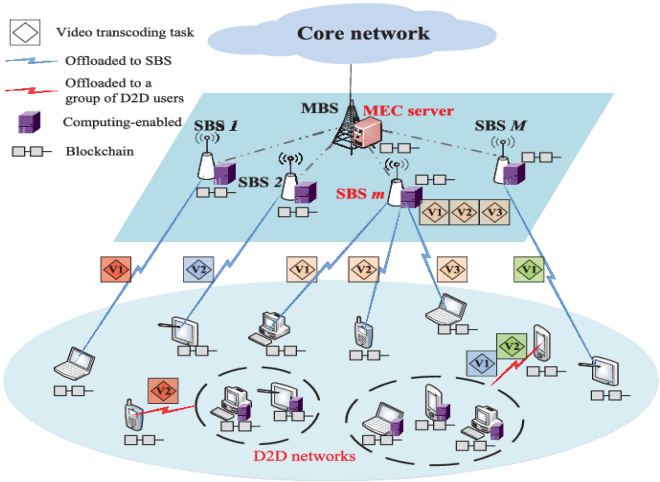

Figure 1. Resource allocation process

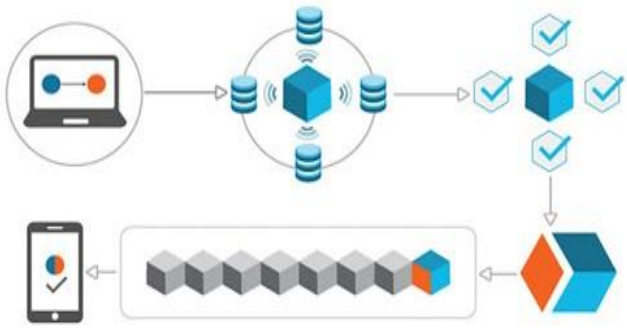

Figure 2. Resource sharing block generation process

Advanced change will get basic as ongoing communication between the two gadgets and various on-screen characters over the energy esteem chain will be a need for constant coordination of the network for sharing resources. As the business is now moving ceaselessly from the customary, brought together structure of the past, new rising innovations, for example, blockchain that can encourage the continuous change will conceivably have a significant effect [13] Given the decentralized and computerized nature of the innovation, blockchain could be utilized to all the more likely to help the data streams between various members and gadgets in the vitality framework while smoothing out exchanges. To put it plainly, blockchain is a disseminated and on the whole looked after database, a changeless record of exchanges. Recognized from the more typical focal design where information is stored on just a couple of servers, a duplicate of the blockchain is stored locally by each group for avoiding unauthorized users [14]. The chain of information records is consistently developing as new blocks that are approved over the circulated users before being connected to the chain [15]. The process of creating block of linked transactions in resource allocation is indicated in Figure 3.

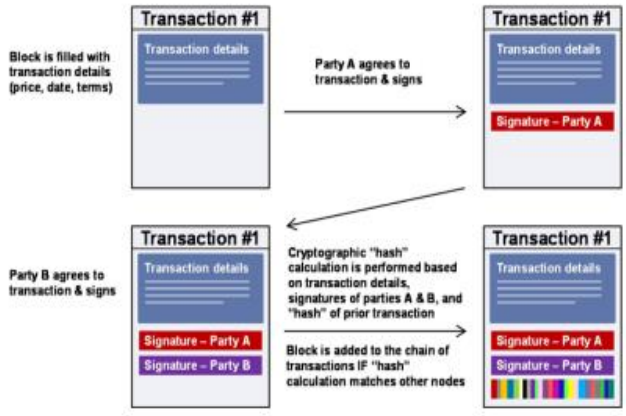

Figure 3. Resource allocation updating process

All the users of the system can check that each new block in a chain is substantial by methods for cryptographic hashing, while the legitimacy of every resource exchange depends on the generally utilized open key encryption model [16]. The decentralized idea of blockchain empowers applications to work without the need of outsiders [17]. The innovation has besides developed from supporting just straightforward resource exchanges to having the option to run code that actualizes progressively complex standards for completing the users tasks.

By setting up a decentralized and secure data arrangement, the utilization of blockchain can possibly offer a significant change in the manner for secured resource sharing so that only authorized users are allowed to make use of the resources. Various blockchain based ventures are rising inside this field and new users have to get authorization from the organization for accessing the available resources. While blockchain innovation could transformative affect a few procedures, the innovation is neither developed enough nor reasonable to comprehend the entirety of the difficulties inside the resource allocation progress [18]. Thus, it is inconsequential to follow the present promotion and commit to without cautiously considering and assessing the innovation.

2. LITERATURE SURVEY

Nakamoto et al. [1] proposed a model that is one of the quickest developing markets in the virtual world. Resource allocation stages are expected to give stages to various clients to learn on the web. It is additionally called Resource management system (RMS). It gives set-ups of resources that help allocation based on task completion time, upkeep, execution time. It very well may be separated into two classifications: Open-source stages and Proprietary arrangement based stages. For Open-source stages, they are ordinarily based on extensible structures that let users alter and change the frameworks to suit their particular needs. The blockchain-based data exchange frameworks in which the blockchain-based access control layer is applied to the providers' existing databases are used. These systems stored on the blockchain only the metadata to identify the actual data and its permissions.The model accuracy in resource handling is less as the model does not verify the user authentication before alloting resources.

Zhang et al. [2] proposed open exchange resources that are

commonly exchanged more regularly than private resources. Thus open markets are more fluid than private markets. Exchanges inside the private market for the most part including entire resources instead of portions of benefits (open market). Obligation and value are two different sorts of capital resources, both can be exchanged either open or private kinds of advantages. Alsaffar et al. [3] characterized obligation resources as resources that give their proprietors the privilege to future incomes paid out by borrowers on advances. By method of difference, value resources give their proprietors the rights to the leftover incomes created by a fundamental resource. Blockchain and other systems are limited to the authorization and undeniability of those individuals in sensitive transactions. Blockchain is used in this work to propose an individual health records system which safeguards privacy in support of non-repudiation, transparency and tamper resistance properties.The model fails to schedule the resources based on user requests. The waiting time of users is more in this model that need to be overcomed.

Numerous individuals know blockchain as the innovation behind the 'Bitcoin', a computerized money presented by Kochar and Sarkar [4]. To comprehend the innovation behind the 'Bitcoin', it is essential to recognize Bitcoin from the fundamental innovation. Bitcoin is a computerized money: a P2P electronic money framework. This money framework uses a blockchain as an (exchange) record to record moves of money, as Bitcoins, starting with one gathering then onto the next, working freely of an outsider. Nonetheless, blockchain innovation potential uses reach out a long ways past this computerized money. Blockchain innovation is 'intended to accomplish predictable and dependable understanding over a record of occasions, called resource exchanges, between free members who may have different inspirations and targets. The biggest challenge is the cost of storage. The costs of storage are very high, since the data is processed after the authentication process; the information has to be replicated; each complete node within the blockchain network has to be synchronised.

3. PROPOSED METHOD

Blockchains regularly follow a multi-layered plan design with four layers. At the base layer, the principles and structure are characterized with its agreement conventions, cryptographic natives and different calculations. The subsequent layer is the place where the decentralized storage, handling and communication happen. This layer establishes the synchronization, security, availability, and secrecy of information just as the administration and authorization of complex consent settings for members and outsiders. The third layer is the decentralized registering stages layer. The top layer, which is the Application layer, is utilized for handling the initial three layers into a valuable application.

To have the option to send and get resource exchanges safely and evidently over a blockchain arrangement, a cryptographic strategy called asymmetrical cryptography is utilized with key size of 1024 bytes. This technique is based on a couple of keys where one is an open key and the other one a private key. These keys are numerically related so that if a bit of secret data were encoded with any of the two keys, just the other reciprocal key could decode it. In blockchain, Public Key Encryption is utilized when an exchange is sent between two friends in the blockchain arrangement, where private keys are just known to the maker, and the open key is circulated to anybody in the system.

A cryptographic hash work is mapping information from an area of self-assertive length to a piece string of a fixed length. The capacity takes an info, which is normally any arrangement of bits in the portrayal of "0s" and "1s" and returns a fixed size worth string as result. A cryptographic hash work is by plan a single direction work. This implies by just transforming the slightest bit in the info grouping, the result of the capacity will be totally extraordinary. In Bitcoin, to have the option to confirm a block, one must run hash calculations on numerous occasions before finding the necessary hash esteem. The multifaceted nature of discovering this hash will rely upon the security prerequisites of a particular blockchain arrangement. In Bitcoin, finding the one of a kind hash is by plan fundamentally troublesome. The hash calculation is depicted in Figure 4.

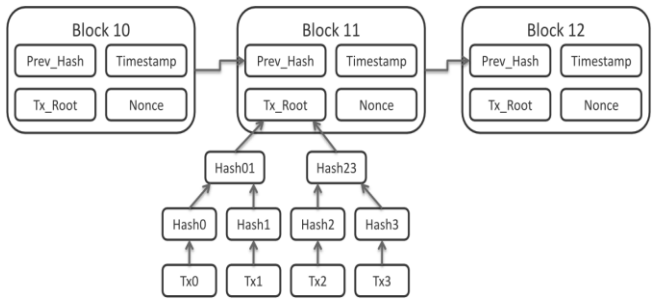

Figure 4. Hash calculation

Approval resource code model claims the most coordinated capacities just as the most thorough approval process. The most noticeable element of this sort of method lies acquainting User authentication by the service provider. The process of user authorization is done as follows

- Step-1: Initially all the nodes or users have to register with the Service Provider (SP).
- Step-2: The SP after registration provides a Secret ID and shares to the user and creates a block.
- Step-3: All resources provided by the service provider is allotted with a Resource ID.
- Step-4: When a user requests a resource, user has to provide the secret key for validation.
- Step-5: SP will check the generated block for user validation and checks whether use is authorized or not.
- Step-6: If unauthorized user, SP allots a Terminated ID (TID) for such kind of users to block them in future transactions also to avoid malicious actions.
- Step-7: If authorized users, SP will display the available resources with Resource ID.
- Step-8: Users can send resource request to SP with relevant Resource ID and SP will allot the resource to the user for specific time frame.
- Step-9: The resources can be shared among the users after specific time is completed.
- Step-10: SP does not allot more than 3 resources at a time to a user and after time elapsed, resources will be retraced and allotted for other users.
- Step-11: Blocks are generated for every transaction done for analyzing the use of resources and also to check for any malicious actions in the group.

A block is a fundamental creation of Blockchain. From a scale point of view, Blockchain is a chain of blocks where each block is connected to its previous block by reference to the past block header's hash. There are three sections in a single block: block header, exchange counter and exchanges. Exchange counter alludes to the absolute number of exchanges in this block while exchanges mean all resource exchanges. Block header is an intricate structure including form, previous block hash, root, timestamp, target and nonce. Timestamp contains the rough creation time of the block for further analysis.

4. RESULTS

The proposed resource allocation model is implemented in ANACONDA SPYDER that creates blockchain for every user transaction and for every allocated resources. The proposed model aims in avoiding malicious actions like denail of service, packet droppings, fake resource requests, data modifications etc., in the group and to provide a platform for exchanging resources for completing users tasks effectively. The proposed model is compared with the traditional Blockchain Based Resource Allocation (BBRA) model. The results depict that the proposed model performs better allocation strategy in allocating resources and avoiding malicious actions among the group of users. The calculation time of user id in the proposed model is compared with the traditional model and the results are depicted in Figure 5.

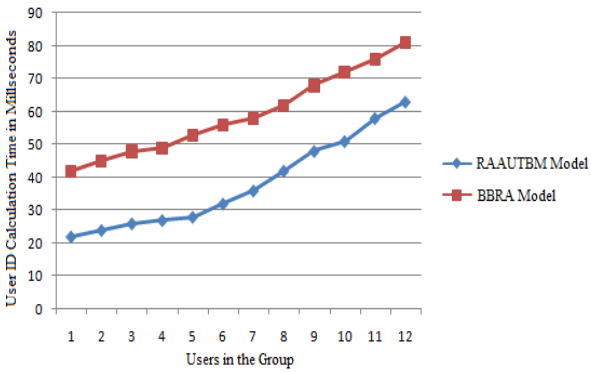

Figure 5. User ID calculation time

The resource allocation time in the proposed method is less when compared to the traditional method. The resource allocation time need to be less so that the system performance is considered as effective. The resource allocation time levels are depicted in Figure 6.

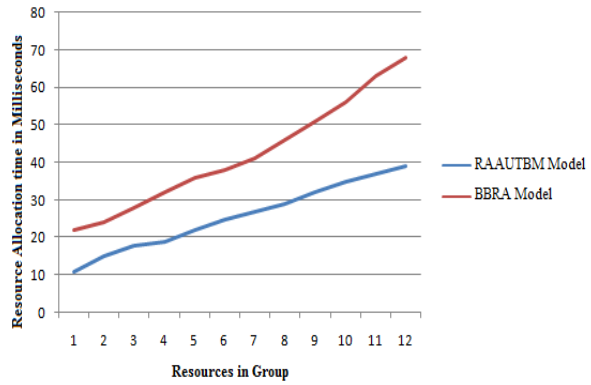

Figure 6. Resource allocation time

The user validation time in the proposed method is low when compared to the traditional method. The user validation time need to be less so that the system performance is considered as effective and also malicious actions is also reduced. The resource allocation time levels are depicted in Figure 7.

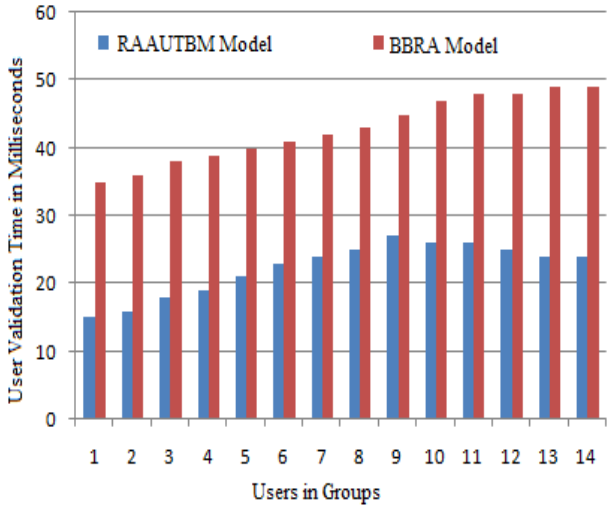

Figure 7. User validation time

The unauthorized users are detected and not allowed to access the service provider resources. The unauthorized users detection time is less in the proposed method that represents the proposed method is better and secure. Figure 8 depicts the unauthorized detection levels of the proposed and existing methods.

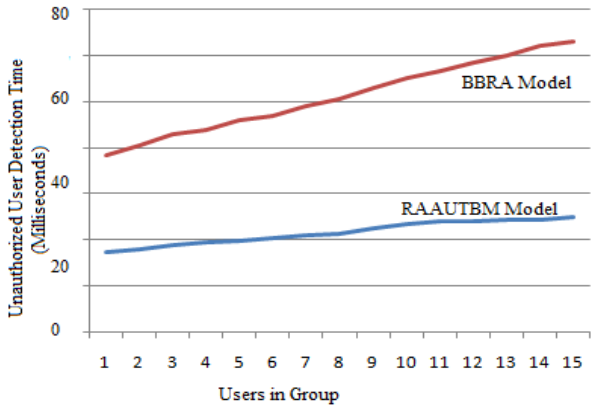

Figure 8. Unauthorized user detection time

5. CONCLUSION

As applications and transactions which require centralized or trusting third parties architectures to be checked can now be carried out with the equal certainty in a decentralized manner, Blockchains introduced serious disturbances to the conventional business processes. The inherent features of the blockchain design and architecture include accountability, robustness, auditing and protection. The proposed work performs resource allocation to authorized users to avoid malicious actions among blockchain based use cases and increase practical information about how blockchain could be actualized. Blockchain innovation is the recent trend that

creates blocks for advanced records of physical and authoritative data. The generated blocks are fixed and cannot be modified so that security level is also high as it is easy to identify the nodes that are malicious. Blockchain is a node system that communicates by means of a protocol with one another. At present, the rightness of archives should be approved by authorized nodes in the system, because of the absence of normalization. The proposed work creates blockchain based on the resource allocation to the users that are authorized by the service provider.

REFERENCES

[1] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf, accessed on 24 September 2019.

[2] Zhang, H., Zhang, Y., Gu, Y., Niyato, D., Han, Z. (2017). A hierarchical game framework for resource management in fog computing. IEEE Communications Magazine, 55(8): 52-57. https://doi.org/10.1109/MCOM.2017.1600896

[3] Alsaffar, A.A., Pham, H.P., Hong, C.S., Huh, E.N., Aazam, M. (2016). An architecture of IoT service delegation and resource allocation based on collaboration between fog and cloud computing. Moblie Information Systems, 2016: 1-15. https://doi.org/10.1155/2016/6123234

[4] Kochar, V., Sarkar, A. (2016). Real time resource allocation on a dynamic two level symbiotic fog architecture. 2016 Sixth International Symposium on Embedded Computing and System Design (ISED), Patna, India, pp. 49-55. https://doi.org/10.1109/ISED.2016.7977053

[5] Chen, M.H., Dong, M., Liang, B. (2018). Resource sharing of a computing access point for multi-user mobile cloud offloading with delay constraints. IEEE Transactions on Mobile Computing, 17(12): 2868-2881. https://doi.org/10.1109/TMC.2018.2815533

[6] Agarwal, S., Yadav, S., Yadav, A.K. (2015). An architecture for elastic resource allocation in Fog computing. Int. J. Comput. Sci. Commun., 6(2): 201-207. http://www.csjournals.com/IJCSC/PDF6-2/31.%20Swati.pdf.

[7] Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton Univers. Press.

[8] Rudlang, M. (2017). Comparative analysis of bitcoin and ethereum. Master's thesis, Norwegian University of Science and Technology.

[9] Al Omar, A., Rahman, M.S., Basu, A., Kiyomoto, S. (2017). MediBchain: A blockchain based privacy preserving platform for healthcare data. In: Wang G., Atiquzzaman M., Yan Z., Choo KK. (eds) Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS 2017. Lecture Notes in Computer Science, vol 10658. Springer, Cham. https://doi.org/10.1007/978-3-319-72395-2_49

[10] Dai, W., Dai, C., Choo, K.R., Cui, C., Zou, D., Jin, H. (2020). SDTE: A secure blockchain-based data trading ecosystem. IEEE Transactions on Information Forensics and Security, 15: 725-737. https://doi.org/10.1109/TIFS.2019.2928256

[11] Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., Wang, F. (2017). Secure and trustable electronic medical records sharing using blockchain. AMIA Annual Symposium Proceedings, pp. 650-659.

[12] Gai, K., Wu, Y., Zhu, L., Xu, L., Zhang, Y. (2019). Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks. IEEE Internet of Things Journal, 6(5): 7992-8004. https://doi.org/10.1109/JIOT.2019.2904303

[13] Natoli, C., Gramoli, V. (2016). The blockchain anomaly. 2016 IEEE 15th International Symposium on Network Computing and Applications (NCA), pp. 310-317. https://doi.org/10.1109/NCA.2016.7778635

[14] Guo, R., Shi, H., Zhao, Q., Zheng, D. (2018). Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. IEEE Access, 6: 11676-11686. https://doi.org/10.1109/ACCESS.2018.2801266

[15] He, D., Zhang, Y., Wang, D., Choo, K.K.R. (2018). Secure and efficient two-party signing protocol for the identity-based signature scheme in the IEEE P1363 standard for public key cryptography. IEEE Transactions on Dependable and Secure Computing, 17(5): 1124-1132. https://doi.org/10.1109/TDSC.2018.2857775

[16] Neisse, R., Steri, G., Fovino, I.N. (2017). A blockchain-based approach for data accountability and provenance tracking. CoRR abs/1706.04507.

[17] Nijeholt, H.L.A., Oudejans, J., Erkin, Z. (2017). DecReg: A framework for preventing double-financing using blockchain technology. BCC 2017 – Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, Co-Located with ASIA CCS 2017 (2017), pp. 29-34. https://doi.org/10.1145/3055518.3055529

[18] Niu, Y., Wei, L., Zhang, C., Liu, J., Fang, Y. (2017). An anonymous and accountable authentication scheme for Wi-Fi hotspot access with the Bitcoin blockchain. 2017 IEEE/CIC International Conference on Communications in China (ICCC), pp. 1-6. https://doi.org/10.1109/ICCChina.2017.8330337