Analysis of Multi-layer Information Flow in a Four-Layer Blockchain Model

Fernando Rebollar, Marco A. Ramos, J. R. Marcial-Romero, and J. A. Hernández-Servín(✉)

Facultad de ingeniería, Universidad Autónoma del Estado de México, Cerro de Coatepec S/N, Ciudad Universitaria, 50110 Toluca, Mexico
joseph_servin@uaemex.mx
https://www.uaemex.mx/

Abstract. The blockchain technology allows nowadays to decentralise information and the use of cryptographic techniques make this technology secure and reliable thus adding functionality for sharing information through smart contracts among other functionalities. One of the main disadvantages of this process is scalability in the speed of transactions making the systems slow for practical applications. In this paper, a multilayered approach is proposed in order to address the problem of improving speed in transactions; the method is presented by means of a case study analysis, by dividing the information in four-layers based on blockchain which allow users to participate and contribute to decentralise information thus making the service more reliable. The main contribution in this paper is the analysis that shows interaction for sharing information between different layers thus monitoring the behaviour when transactions are being made.

Keywords: Blockchain · decentralization · smart contracts · government services · digital services

1 Introduction

The offer and need of digital services, in the public and private sector has steadily grown [1]; being an example the governments of developed countries that have increased the number of digital services offered to their citizens. These services provide some advantages such as reduced costs, time and bureaucracy reduction [2]. These types of services operate in a centralised manner and the administrators depend on the same entity, in which trust plays a crucial role. To keep an optimal functionality of the system, is that honesty of a centralised entity must be present at all costs. Since, in real life this is normally not the case, it is necessary to decentralise the information and mechanisms that prevents a dishonest entity to be able to corrupt the system and make malicious changes.

Blockchain can provide decentralisation of technological services [3], while keeping information verified at each step of the process by providing full transparency, integrity and immutability of that information [4]. As an example, smart

R. Silhavy and P. Silhavy (Eds.): CSOC 2023, LNNS 723, pp. 338–348, 2023.
https://doi.org/10.1007/978-3-031-35317-8_31

contracts using block-chain [5], which one can loosely define as being a digital assets containing secure digital agreements that are important to the actors involved in the transactions. These one of the key features where cryptography techniques play an important role in the development of secure and reliable digital transactions. On the other hand, decentralisation becomes important since multiple computers (or nodes) store information at different locations thus using a consensus algorithm to keep information uncorrupted; making almost impossible to modify.

The advantages of blockchain had already been recognised by the government of different countries around the world. To some extent, some services are already in use such as money remittance in the United Arab Emirates to Nepal [6]. Another successful example is property registration in Rwanda which has been reported to avoid legal disputes among their citizens by keeping a clean track of the titles. This saves money, which is normally spend in legal disputes for rigged transactions in purchasing land [7]. Nonetheless, difficulties arise in block-chain technologies when the number of transactions increases per second in various digital services [8], thus the need for alternative improvements of the systems. The proposal to address these problems in this paper, is a multi-layer block-chain system that divides the information into four-layers [9]. This way, each layer specialises in a certain type of information. The model has the capacity to support several digital services, in order to decentralise and monitor the information handled by the system, to allow voluntary nodes to participate in order to validate blocks and help to keep secure the information. This article presents an analysis of a case study using the four-layers of the proposal. In Sect. 2, we describe a multi-layer blockchain for government services, using four-layers and how in this model is possible to decentralise information by levels, defining some properties and its operation by identifying the general architecture. In Sect. 3, a case study of a four-layer blockchain model is analysed, reviewing the information flow between the layers that make up the model and finally in Sect. 4 the conclusions are presented.

2 Four-layer Blockchain Model

The blocks that make up a blockchain contain different types of information. Examples of this information are hash values table, index tables, stored data (usually encrypted), transaction information, smart contracts as well as files, although files are not usually stored in blockchain, because the size of the blocks will increase the speed of transactions [10] by saturating the network with large files. The model separates the information typically contained in a block [9]. As a result, an analysis is performed on each piece of information contained within the block. The properties that have the highest priority are obtained. Based on these properties, the information placed in a layer is intended to guarantee the chosen properties. In similar models, it has been shown that separating the information into layers allows the optimisation of the blockchain-based service. The model, after analysing the key requirements of blockchain-based applications, typically

uses four types of data: (1) index-keys to identify hashes, (2) transactions that are performed, (3) smart contracts to enforce autonomous execution and (4) log files that are evidence of application-related processes (when required). The four-layer model is described in detail as follows:

1-Index-Keys. This layer is dedicated to storing index tables containing the hash of all pieces of information within the layers. Therefore, it will be implemented using a public blockchain using the PoW (Proof of Work) consensus protocol [11] which corresponds to a public blockchain type. By only storing indexes, this layer will be the one with the smallest block size and the highest level of decentralisation. It is also possible for citizens to participate in the validation of these blocks, generating greater trust in the information stored. The blocks in this layer are interconnected in a staggered order with the other three layers.

2-Transactions. Dedicated to store transactions, i.e., it stores the information necessary for all transactions that take place. To improve the speed of transactions, this layer is less decentralised than layer 1 by implementing a private blockchain using the PBFT (Practical Byzantine Fault Tolerance) consensus protocol [12], which corresponds to a type of private blockchain. Layer 2 queries information from layer 1 to validate that transactions are only from previously registered and valid users.

3-Smart Contracts. Stores all information related to smart contracts. This layer also uses the PBFT consensus protocol, which corresponds to a type of private blockchain. Layer 3 interacts with layer 1 to validate users who can create smart contracts. It also interacts with layer 2, as smart contracts execute one or more transactions.

4-Files. Stores files in the formats required by the application. This layer uses the Interplanetary File System (IPFS), a P2P protocol and network that is used to store and share data in a distributed manner [13].

Depending on the application, a node can give access to a file by adding the content identifier in a transaction or in a smart contract. Layer 4 does not use a consensus protocol as it is not necessary.

2.1 Properties of the Four-Layer Model

The following properties describe the generation of the blocks and the connection between layers. In order to specify and explain the behaviour of the model, its attribute on each layer is structured in a unique way so that the desired results can be obtained later on. The transaction rate is the capacity to process different amounts of information in a given period of time (t); the greater the amount of information, the more difficult it is to maintain and reduce the time required for processing. That is why the transaction rate is affected by the size of the blocks, the level of decentralisation and speed of generation of the blocks. The following properties refer to each one of these.

To describe the transactions some notation is first introduced. Let L_j be the jth layer, where j is the number of the layers, and L_j consist of a set blocks

indexed by x_{ij} where $i = 1, ..., n_j$ and n_j is the number of blocks within the layer j, since every layer has a different number of blocks that is changing from layer to layer in a descending way. That is, if n_j is the total number of blocks within the layer j which at the same time takes t_{ij} time to generate each block in any given layer j. Here, $t_j = \sum_i t_{ij}$ is the total time that it takes to generate all blocks within the j layer.

Remark 1 (Block generation speed). Depending on the digital service an appropriate block generation must be configured, however, the following must taken into account: In the layer $L_j = \{x_{1j}, x_{2_j}, ..., x_{n_j j}\}$ such that j is the layer number, so in the case of a four-layer system we have that $j = 1, 2, 3, 4$. The x_{1j} block is the first one of each layer and t_{ij} is the unit of time in which each x_{ij} is generated and it is satisfied that $t_{ij} \leq t_{i(j+1)}$. The above means that every block on each layer, with the same index takes less time to be generated that the block in the next layer with the same index. Therefore, a layer generates a larger amount of blocks in a given period of time compared to the next layer. If we denote by f a process applied to an specific block which outputs always a new block, thus we can represent this formally as $\forall x_{ij} : f(x_{ij}) = x_{(i+1)j}$ for $j = 1, 2, 3, 4$; That is, we must always generate a new block in each layer, so all four blockchain layers will keep generating new blocks whenever they are required. However, it is also true that there is a block at different layer that comes from previous layers with already generated blocks. If we denote this process by g we can formally expressed this as $\exists x_{ij} : g(x_{ij}) = x_{(i+1)j+1}$ for $j = 1, 2, 3$. Except for layer 4 which cannot unchained any new block since it is the end of process. The level of decentralisation refers to two aspects: the first one is the number of nodes that hold a complete copy of the information (architectural decentralisation), and the second one corresponds to the organisation that control the nodes (political decentralisation). Political decentralisation increases the integrity and security of information. This is reason why layer 1 is public and allows any anonymous node to contribute to the process; whereas layers 2, 3 and 4 are private with defined nodes.

Remark 2 (Level of decentralisation). Let K_{ij} be the number of nodes that hold a copy of the blockchain for each block i and layer $j = 1, 2, 3, 4$. The higher the number of nodes that hold a copy of a layer, the higher the level of decentralisation that the system complies with. This requirement is satisfied with $K_{ij} > K_{i(j+1)}$. The above guarantees that level of decentralisation keeps going down, where the first layer is the one with highest decentralisation compared to any other layer.

The block size has a significant influence on the fast distribution of the block to each node, therefore, depending on the digital service an appropriate block size must be configured. The following must be fulfilled in order to achieve that.

Remark 3 (Block Size). The block size of each layer must satisfy $|x_{ij}| < |x_{i(j+1)}|$ for $j = 1, 2, 3, 4$. Here $|\cdot|$ measures the size of the block in whatever units the size of a single character is measured which can be bytes. Thus, blocks in layer 1 are

smaller compared to blocks in lower layers, in order to be inversely proportional to remark (2).

With above remarks in mind, the behaviour of block generation can accurately be monitored for step of the process or layer. The maximum block size can also be controlled to ensure an optimal decentralisation level. These properties all together have an impact on the transaction rate for each layer in the whole system.

By making all properties hold in the system, one can be sure that the 4-layer model is able to distribute blocks to the nodes efficiently. This also will keep a good transfer speed, as each layer has an adequate block size in accordance with their level of decentralisation. Also, a consensus algorithm, can be used to obtain the best possible performance when implemented in the system.

3 Analysis of a Case of Study

The four-layer model presented can be seen as a reference framework that can be used on different scenarios. It is possible to use as many layers as necessary, as an example four possible scenarios are described in [9]. It could be the case that service does not need to store files so a four-layer system is unnecessary (scenario 2). Another case is when a service lacks or does not provide smart contracts so a three layer system (scenario 3) may not be necessary. The other scenario is when a service does not need neither smart contracts nor to store files, so it does not require layer 3 and 4 (scenario 1).

Scenario number 4 takes into consideration all of its functionalities, that means all four-layers are required. Layer labelled 1 generates their respective cryptographic keys to subsequently generate transactions in layer 2. These, in turn, create smart contracts in layer 3, where files are generated and stored in layer 4. This creates one or more transactions at layer 2, and these transactions are store their respective indexes at layer labelled 1 in our case. We have chosen this scenario as it is the most complete scenario to perform the analysis, see the system sequence diagram, Fig. 1.

The following paragraph is a detailed description of diagram of Fig. 1 on each step of the process.

1. The administrator registers and configures the set of rules, policies, users and processes of the service at layer 1.
2. At layer 1 the necessary cryptographic keys are generated, such as hashes, public and private keys needed to ensure the integrity and security of the information.
3. The users authorised to perform signed transactions at layer 2, therefore one or more transactions are generated with the parameters of digital signatures, transaction identifiers and transaction data.
4. Transactions can generate smart contracts at layer 3 to automate future transactions in the services, which as parameters carry the smart contract identifier, the transaction information that generates the smart contract and the smart contract data.

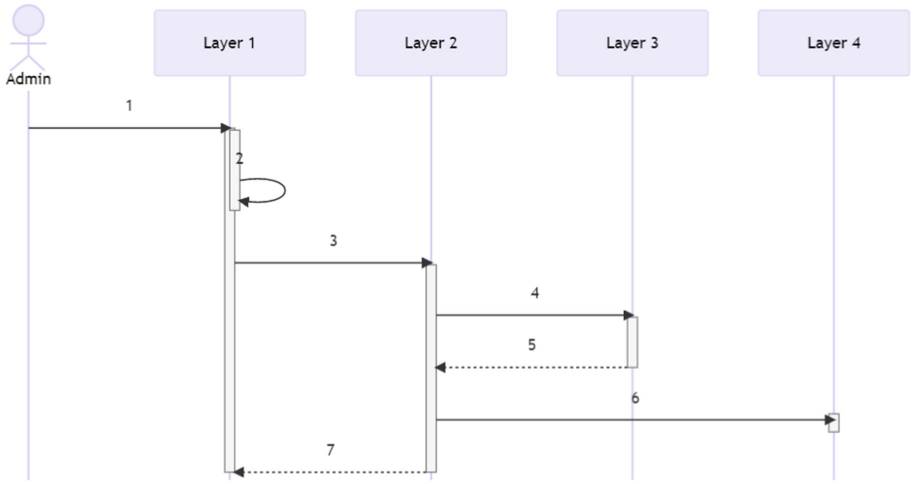

Fig. 1. When all 4 layers are used: keys and indexes, transactions, smartcontracts and files

5. Smart contracts can generate transactions in layer 2 when executed, for each transaction that is generated, the transaction identifier, the smart contract information that generates the transaction and the transaction data are stored.
6. Transactions can generate files in layer 4, which as parameters carry the file identifier, the information of the transaction that generates it and the file data.
7. Once the transactions are completed, the transaction identifiers, smart contract identifiers and file identifiers are returned to layer 1 to be saved.

3.1 Fines System

This section describes a possible case in actual production and what information flow might look like. The case of study for the four-layer model might be well applied to a system for charging fines when an administrative rule is violated such as traffic light rule violation. In governments, the fine system is administered by a specific police department. This department has control of the system which in theory a fine cannot be overruled unless is authorised by a law enforcement entity. It is also possible to keep track of revenues from collection of fines, and the information may also be readily available to other government entities.

The multi-layer blockchain control system for tracking fines is decentralised to one department. The patterns stored in the blockchain blocks cannot longer be modified or deleted. Theoretically, this is true but the system may have flaws and that depends on the level of security implemented using cryptography. Particularly, smart contracts have the property of automate the transaction of paying the fine, its status and can also be automatically linked to the collection depart-

ment. One possible configuration is as shown in Fig. 2 for a four-layer model. The regional division of a country into states and municipalities is highlighted. Different countries could have more regional divisions where the model can be adapted.

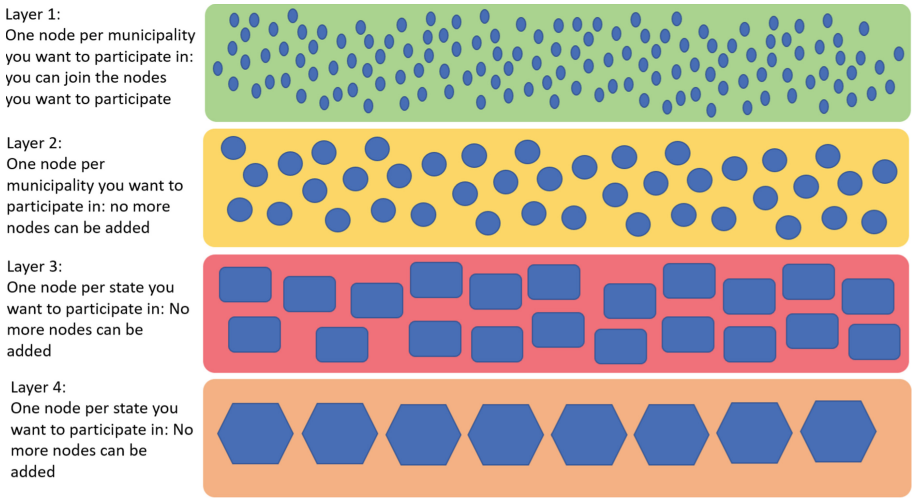

Fig. 2. Possible nodes that should participate in each layer, the size of the figures represents the storage capacity required by the nodes and the number of figures in each layer is the recommended number of nodes to have.

In Fig. 2, layers 4, 3 and 2 as described in the model, they work as a private blockchain so the nodes are pre-established and identified; whereas layer 1, the nodes work as a public blockchain so they can be anonymous and not necessarily identified. This allows anonymous nodes to participate to further decentralise the information. The four-layer model describes, that it can work with few nodes in each layer, although the more nodes the more decentralised and secure the information is. Layer 4 is responsible for storing the documents evidence of the fine payment in the form vouchers and invoices. Layer 3 contains smart contracts for the payment of fines or cancellation of fines in case the fine is invalid due to legal issues. It could also contain smart contracts to link automatic collections as desired. Resources to storage requires less capacity and can be more decentralised than layer 4. Layer 2 is responsible for issuing the system's fines, which in this case can only be issued by a registered, authenticated and authorised agents. It is also responsible for fine payments confirmation. Layer 2 blocks require authorised nodes when is necessary to have a high transfer rate per second to handle the fines and payments. Layer 1 contains transaction, smart contract and document identifiers. It also contains information of the authorised agents to create the fines (names, electronic signatures, etc.). Layer 1 consists of blocks that any authorised or anonymous node can consult and verify the information, which in

our case of study could be any citizen. They are the blocks that operate with the highest transparency to the public and are therefore easy to audit. Also voluntary nodes are allowed to contribute computing power to validate the blocks of this layer and contribute to make the information more reliable.

This case of study should be adapted taking into account differences between locations and policies where is to be implemented. But it could also unify fine systems at different locations, e.g. municipal, state and federal systems. The flow of information as shown in Fig. 3, where rules, policies, users, etc. of digital services are configured in layer one. The authorised officers involved to issue fines can be registered. Once they are registered, their cryptographic keys are generated and they are authorised to issue fines. The fines are registered in layer 2. In this case, smart contracts can also be generated in layer 3 every time a fine is issued. This allows automatisation to enforce a fine. In this case a fine can be paid or not in case the corresponding authority decides not to do so. The advantage of the smart contract is that automatically detects payments or revoked obligation to do, issued by the corresponding authority. After the occurrence of either event, a proof file is saved in layer 4 and the compliance transaction is also generated, which in turn saves the indexes in layer 1 where the corresponding evidence is stored.

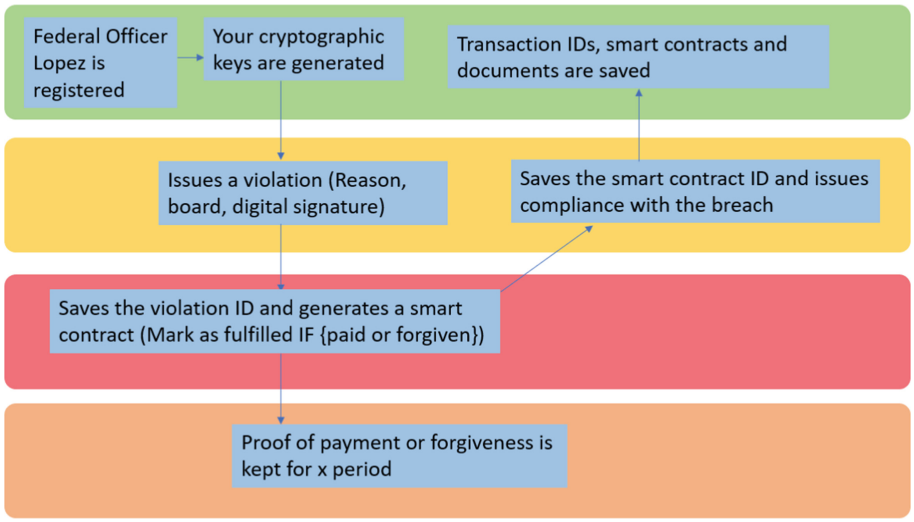

Fig. 3. Information flow using the 4 layers of the case study in a fine system.

In case someone wants to look up a particular violation in the past, it is very simple to track it down since the properties of a blockchain keeps the violation history. This is stored and protected against any future changes.

3.2 Some Considerations When Implementing the Case Study

The blockchain-based multi-layer proposal model could be used in some of the digital services of governments, to make the process of sharing information transparent. There are some considerations to take into account in order to increase effectiveness because there are risks that can affect the objective. Some of the considerations are as follows:

1. The hardware and software requirements are unrestricted for team participation. Teams with heterogeneous characteristics are eligible to participate. Any team that wants to participate can join the network. Computers with a higher capacity to calculate hashes per second will contribute more to the network.
2. External participants will not be able to make changes to the data contained in the blocks.
3. Volunteers participating in the network may or may not be rewarded. By contributing computational power, governments may set positions to reward participants or not, but it is desirable that there is no reward at all so as not to generate interests unrelated to the original purpose. However, it is not excluded that rewards for participation could be distributed.
4. Multiple individuals and non-governmental organisations may be interested in contributing even if there is no reward. Public universities are candidates for decentralised testing. They may even benefit from teaching blockchain courses, where a viable practice is to ask students to voluntarily participate in such a network to supplement their learning.
5. Participating teams could be restricted to being located within the same country. The use of VPNs would allow teams from other countries to participate in the system, but if they wanted to restrict this, a mechanism would have to be found and implemented to prevent this.
6. A possible restriction so that only citizens belonging to a country can participate is to administer an access control to the blockchain by means of an official ID of the country that implements it.

Depending on regional laws and different types of digital services to be added to the system, there may be extra considerations to analyse.

4 Conclusions

The case of study shown is a practical example of the four-layer blockchain-based model that could be implemented, the design of the model is specifically created to be used by governments for greater control, transparency and functionality in sharing information.

The case study shows how it divides and organises the different types of information needed in the four-layers with a focus on delivering an efficient digital service with a high transaction rate. This separation supports file storage without

affecting transaction speed or smart contract execution times, as opposed to using a single layer.

For the case of study to work as described, it is assumed that the authorities in charge of avoiding and paying an infringement use digital signatures. This automate and make it possible to use layer 3 as smart contracts, but it is also possible to adapt it to scenarios 3, 2 or 1 described in [9], because of the flexibility of the four-layer model. This can be adapted to different requirements, unlike similar works that are associated to a single use case. Multiple services could coexist in a four-layer model implementation, so the infringement system could work and coexist with other services. The case study does not contemplate yet, non-human autonomous agents (IoT and smart city environment) to issue fines but it is compatible with that environment. It is possible to upgrade the systems and add these entities to issue fines. There are several challenges to improve inherited from blockchain [14–16], some important challenges are regarding the efficiency of transactions as they increase in number. The multi-layer model aims to decrease some of the disadvantages. Currently, the proposal uses elliptic curve cryptography and we are exploring to switch to hyperelliptic curve cryptography (or genus 2 elliptic curves) which could have a shorter key size compared to elliptic curve cryptography and could have better performance [17,18].

Finally, to increase trust and transparency, it is proposed to let people know the precise implementation of the system via a sharing model such as open source, available to the community to avoid any suspicious of hidden backdoor to corrupt the system. In this way, everyone can review and validate their implementation and operation, and be able to download and compare versions using hashing to validate that the code that was deployed is the same code that is running.

References

1. Lipschultz, J.: Free Expression in the Age of the Internet: Social and Legal Boundaries. Routledge (2020)
2. Gabison, G.: Policy considerations for the blockchain technology public and private applications. SMU Sci. Tech. L. Rev. **19**, 327–336 (2016)
3. Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V., et al.: Blockchain technology: beyond bitcoin. Appl. Innov. **2**(6–10), 71 (2016)
4. Wüst, K., Gervais, A.: Do you need a blockchain?. In: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), pp. 45–54. IEEE (2018)
5. Buterin, V.: A next-generation smart contract and decentralized application platform (2014). https://github.com/ethereum/wiki/wiki/White-Paper
6. OECD: The development potential of remittances using blockchain technology in Nepal (2021). https://oecd.org/finance/blockchain/The-development-potential-of-remittances-using-blockchain-technology-in-Nepal.pdf
7. T. new times: How RWANDA uses blockchain technology to ease land transactions (2021). https://newtimes.co.rw/news/how-rwanda-uses-blockchain-technology-ease-land-transactions
8. Jun, M.: Blockchain government-a next form of infrastructure for the twenty-first century. J. Open Innov. Technol. Mark. Compl. **4**(1), 7 (2018)

9. Rebollar, F., Aldeco-Perez, R., Ramos, M.A.: Modeling a multi-layered blockchain framework for digital services that governments can implement. J. Intell. Fuzzy Syst. **42**(5), 4551–4562 (2022)
10. García-Morales, E.: Luces y sombras sobre el impacto del blockchain en la gestión de documentos. Anuario ThinkEPI **12**, 345–351 (2018)
11. Kaur, S., Chaturvedi, S., Sharma, A., Kar, J.: A research survey on applications of consensus protocols in blockchain. In: Security and Communication Networks, vol. 2021 (2021)
12. Cachin, C.: Architecture of the hyperledger blockchain fabric. Workshop Distrib. Cryptocurr. Consens. Led. **310**, 2–15 (2016)
13. Steichen, M., Fiz, B., Norvill, R., Shbair, W., State, R.: Blockchain-based, decentralized access control for IPFS. In: 2018 IEEE iThings and IEEE GreenCom and IEEE CPSCom and IEEE SmartData, pp. 1499–1506. IEEE (2018)
14. Peck, M.E.: Blockchain world-do you need a blockchain? This chart will tell you if the technology can solve your problem. IEEE Spectr. **54**(10), 38–60 (2017)
15. Yang, R., Yu, F.R., Si, P., Yang, Z., Zhang, Y.: Integrated blockchain and edge computing systems: a survey, some research issues and challenges. IEEE Commun. Surv. Tutor. **21**(2), 1508–1532 (2019)
16. Moin, S., Karim, A., Safdar, Z., Safdar, K., Ahmed, E., Imran, M.: Securing IoTs in distributed blockchain: analysis, requirements and open issues. Futur. Gener. Comput. Syst. **100**, 325–343 (2019)
17. Martínez, V.G., Hernández-Álvarez, L., Encinas, L.H.: Analysis of the cryptographic tools for blockchain and bitcoin. Mathematics. **8**(1) (2020)
18. Frey, G., Shaska, T.: Curves, Jacobians, and cryptography. In: Algebraic Curves and Their Applications, pp. 279–344. American Mathematical Society Providence (2019)