Blockchain Technology To Support Italian Tax Process

Piergiorgio Ricci[1], Valentina Mammanco[2]

[1] Department of Enterprise Engineering, University of Roma "Tor Vergata", Italy, Department of tax information system, Ministry of Economy and Finance, Italy
[2] Department of Economic and Social Affairs, UNICEF, Italy.

ARTICLE INFO	ABSTRACT
Keywords: *Blockchain, Information and Communication Technology, E-Government, Digital Fiscal Process, Big Data*	The rapid spread of blockchain technology and all its applications has aroused great interest from the scientific world and is likely to change many business contexts in the coming years. The fiscal area represents a strategic sector for the public administration and the recent introduction of the electronic tax process by the Italian Ministry of Economy and Finance has made it possible to significantly improve the resolution of tax disputes. With the aim of overcoming some of its data security limits, in this work we propose a blockchain based solution designed to improve the conduct of the digital tax process by making it safer, faster and with lower transaction costs. In particular, the main improvements relate to two different dimensions of analysis, on the one hand a better level of privacy guaranteed by the introduction of trial files within a blockchain network, on the other hand the use of smart contracts ensures the enforceability of the court's decision and reduces transaction costs related to the conduct of the tax process. The specific model designed is based on a permissioned blockchain and an algorithm for reaching distributed consent, for which we describe in detail the principles of operation that allow the different entities involved to take part in the tax process.

1. Introduction

Blockchain technology was proposed by Satoshi Nakamoto, the unknown person who in 2008 published a scientific article in which Bitcoin cryptocurrency was introduced (Satoshi & Nakamoto, 2008). This is a novel concept based on a number of existing tools, such as encryption, timestamping and digital signature, which, when combined allow to make business processes more efficient in terms of security and execution time (Kshetri, 2017). Blockchain technology belongs to the class of *Distributed Ledger Tecnologies* (*DLTs*) and it has many potential fields of application (Underwood, 2016) such as financial services, healthcare and supply chain management, for this reason the World Economic Forum predicts that by 2027, blockchain

⬜ Corresponding Author E-Mail Address: piergiorgio.ricci@uniroma2.it

technology will contribute to 10 percent of the global GDP[1]. One of the main domains in which this technology could fully exploit its potential is public administration (Davidson, De Filippi, & Potts, 2016) and in particular the fiscality area. Recently, the Italian Ministry of Economy and Finance has introduced the telematic tax process which from 15 July 2017 is active throughout the Italian territory, at the end of a gradual extension to the regional level that began on 1 December 2015 and it will become mandatory by July 2019. This new method has significantly improved the tax process, but there are still limits related to the security and integrity of the data processed, which require expensive systems for tracking users working on procedural files and their activities in compliance with the requirements of the Italian Data Security Authority. Blockchain technology represents a solution to the problem of judicial data security allowing a lean, economical and secure management of the procedural file. In particular, it is able to ensure full compliance with the requirements of Italian Data Protection Authority by providing confidentiality and non-tampering of the documentation deposited by the parties for the conduct of the trial also preventing any changes or replacements of attached documents going beyond the security levels guaranteed by the digital signature alone. In addition to the security requirements, expressed in terms of privacy and immutability of the procedural bundle, the introduction of a series of smart contracts allow the certainty of the enforceability of the decision of the court as well as the reduction of transaction costs associated with the conduct of tax process.

2. Blockchain technology

Technically, a blockchain consists of a distributed ledger on which all the transactions or, more generally, all the digital events are recorded permanently and shared among the entities that are interested in it. (Michael, Nachiappan, Pradan, Verma, & Kalyanaraman, 2016) Compared to traditional architectures for data management based on client server interaction, the blockchain is characterized by a distributed operating model, in fact, all parties involved in the system, that are organized in a peer-to-peer network, keep track of its informative content organized into blocks that are linked together by pointers from the genesis to the final block (Beck, Avital, Rossi, & Thatcher, 2017). Each of them contains a cryptographic hash of the previous block, a timestamp and a collection of data tamper-proof stored. This type of architecture can increase data security and prevent the formation of connectivity bottlenecks unlike in a centralized architecture that relies on a single point of security and authority over the underlying database. Block's confidentiality and inalterability is guaranteed through the use of cryptographic techniques based on secure algorithms such as *SHA256* which consists of a hash function that starting from an input of variable size produces an output of prefixed length (Gilbert & Handschuh, 2011). The added value of this type of function is represented by the "one way" property that allows to make it almost impossible from the computational point of view to reconstruct the value provided in input on the basis of the output produced. For this reason this cryptographic technique finds great application in the activities of mining and creation of addresses in the Bitcoin cryptocurrency system. Each new block introduced in a blockchain is approved by using an algorithm of distributed consent that is predetermined by the participants in the system (Mingxiao, Xiaofeng, Zhe, Xiangwei, & Qijun, 2017). Recently, several algorithms have been developed to reach distributed consensus each of which fits into a specific context. In the following subsections we describe the most common among them.

---

[1] Global Agenda Council on the Future of Software & Society - Deep Shift Technology Tipping Points and Societal Impact

Consensus algorithms

There are several algorithms used to reach consensus in a distributed system, whose choice depends on the computational capacity of the network, the number of its participants and the level of security to be achieved. The consensus algorithm that is currently most widespread is known as Proof of Work (Gervais et al., 2016) and is the basis of the block generation in the Bitcoin cryptocurrency that uses a scheme based on SHA256 encryption known as HashCash system. The idea behind this mechanism was launched in a scientific article in which it was attempted to solve the problem of spam emails. (Dwork & Naor, 2007) Essentially, a proof of work consists of a portion of data that is difficult to generate and, at the same time, it is easy to verify that it corresponds to specific predetermined requirements. In the proof of work mechanism used by Bitcoin, a subset of users with a large computing capacity known as miners, starting from a nonce, which represents a number that can only be used once, and a hash function, they try to guess a random a number that combined with the data gives the target hash identifier (block id) for that block of transactions (Malone & O'Dwyer, 2014). In particular, the algorithm consists of searching for that random number that if provided as input offers as output a hash id for the block of interest that presents a predetermined number of zeros at the beginning. This is a very complex procedure from a computational point of view and requires a lot of execution time and requires a huge energy consumption. It is important to underline that hash functions, such as SHA256, guarantee the non-alterability of the data, in fact they offer different output results in case of changes in the input values. In order to overcome the electricity consumption problem, other distributed consensus algorithms have been proposed, such as the Proof of Stake mechanism used by Ethereum, in which the creator of the next block is chosen on the basis of a series of requirements established by the network participants (Spasovski & Eklund, 2018) (Saleh, 2018). Other mechanisms for distributed system consensus that have found less dissemination are Proof of Authority (Blockchain et al., 2018) and Proof of Space.

Types of blockchain

There are different types of blockchain, each of which is more suitable for a specific application context on the basis of the number of entities involved and the level of confidentiality to be achieved. (Buterin, 2015) The different types of blockchain and their characteristics are summarised in Table 1.

2.1.1 Public blockchains

The most common are the public blockchains that are widely used in the field of cryptocurrencies. They are unpermissioned, in fact anyone can partecipate in the consensus process without a permission, by simply running software on their own machine. The most popular algorithm for reaching distributed consensus in public blockchains is the Proof of Work. The classic application of this type of blockchain is in the field of cryptocurrencies where anyone can send and visualize transaction which are anonymously stored.

2.1.2 Private blockchains

Private blockchains are permissioned network where read and write permissions may be restricted to an arbitrary extent on the basis of a central authority decision. This type of architecture can be used for internal purposes within a single organisation without the need to reach an external consensus. The main advantages over traditional solutions based on centralized databases are integrity, immutability and confidentiality in a fault-tolerant work environment since

there are no single points of failure. It also helps reducing transaction costs and guarantees compliance with national privacy laws. In order for private blockchains to work, it is necessary to define the identities of the entities involved in the system and to establish precise rules regarding the modification of the distributed ledger.

2.1.3 Federated or Consortium blockchains

Participation in a federated blockchain is restricted to a group of entities that are authorized to read and write its informative contents. These are therefore permissioned networks in which consensus is reached through a predetermined set of nodes that respect precise rules. For example, the right to write on the ledger could be restricted to specific entities, while the right to consume its content could be public. They are widely used in the banking sector and allow to reduce transaction costs and data redundancy.

Table 1: Comparison of the different types of blockchain

TYPE OF BLOCKCHAIN	PUBLIC	FEDERATED CONSORTIUM	PRIVATE
PARTICIPANTS	Permissionless	Permissioned	Permissioned
CONSENSUS MECHANISM	Proof of Work, Proof of Stake	Voting or multiparty consensus algorithm	Voting or multiparty consensus algorithm
TRANSACTION FREQUENCY	Long (10 minutes or more)	Short (msec)	Short (msec)

(1)

3. Italian electronic tax process

Italian tax justice

The concept of Tax Justice finds its basis in the principles enunciated by the Italian Constitution, according to which "everyone is required to contribute to public expenses" because of "their ability to pay" to fulfill "the mandatory duties of political, economic and social solidarity"[2].The financial administration is entrusted with the task of quantifying the basic necessities, of progressively distributing it according to income and collecting it through the imposition of a tax. When the taxpayer considers this tax unjust, he can appeal to a judge (tax commission) by activating a set of tools that allow him to assert his reasons against the financial administration. The Tax Commissions area Provincial and Regional, they are in charge of managing the appeals of all the taxpayers who consider the requests of the financial administration to be unfounded. The action field of the Tax Commissions are determined according to the subject of the appeal (object) and the place in which they operate (territorial area). Furthermore, the topic falls within the jurisdiction of the Tax Commissions, such as taxes, the real estate registry and the evaluation, surcharges, additional charges, administrative penalties imposed by financial offices, interest and any other accessory. The Provincial and Regional Commissions have different responsibilities and duties. Provincial Commissions are competent, at first instance, for disputes with tax companies (incomes, import tax, public property) territorial bodies, collection agents and all other imposers who have their headquarters in their district. The Regional Commissions are competent for appeals against

---

[2] Italian Constitution, article 2 and article 53

the decisions of the provincial tax commission that are based in their district. Each Tax Commission is divided into several sections that are in turn composed of a president, a vice president and no less than 4 judges. Each section consists of 3 judges who decide within the college except for the case of the single judge in the judgment of compliance for disputes of value not exceeding 20.000 Euros. The tax process has a complex structure that expects bodies and subject of tax jurisdiction, introduction of the process, the handling of appeal, the decision of the appeal, other procedural institutions, such as judicial conciliation, precautionary protection, precautionary measures and finally all the justice expenses that include the modalities of payment of the tax contribution, the copying rights and the legal support.

Telematic Tax Process

The subject matter of the Italian tax jurisdiction is composed of all disputes relating to taxes in general and the tax process is carried out with the objective of resolving a tax dispute between the two parties involved in it. With the aim of overcoming the limits of the traditional paper process from July 2017 the telematic tax process was introduced, which will become mandatory throughout the country from July 2019. The user has the opportunity, after registering through the dedicated portal, to access the information system of the Tax Justice (ISTJ - TTP) and to file the documents and procedural documents already notified to the other party. Furthermore, tax judges, taxpayers, professionals and tax authorities are able to consult the trial file containing all the documents and deeds of the quarrel they are interested in from home or from their offices. The digitalization of the stages of notification, the filing of the appeal and the documents entails have considerable advantages for all the actors of the tax process in terms of simplification, transparency of procedural requirements and duration of the dispute. The electronic tax process is regulated by Article 16-bis of Legislative Decree no. 546/92, by the decree of the Minister of the Economy and Finances 23 December 2013, n. 163, and by the implementing Decrees. Starting from 15 December 2015 the faculty to avail of the electronic notification and filing procedures was gradually extended in the 2016-2017 two-year period in the tax Commissions of the regions identified in the implementing Decrees. From 15 July 2017 appeals can be notified and filed electronically to all tax commissions and also counter-arguments can be filed by electronic means. Regarding the mandatory use of TTP, the current provisions give to the party the right to file appeals on paper, regardless of the electronic mode chosen by the other party. Therefore, the TTP can become mandatory only following the issue of a specific law. It has been realized through the provision of a series of software applications able to interact with the different stakeholders, in particular they allow to store procedural files in compliance with all the security requirements provided by Italian privacy guarantor for the processing of judicial data. The main security measures relate to the tracking of all activities relating to procedural bundles from filing to the decision of the court of tax judges. Currently these activities are carried out with the use of very expensive systems that produce logs on all the operations related to the procedural bundles and on the subjects that perform them. It is clear that the use of centralized architectures for this type of activity is expensive and cannot guarantee the confidentiality and immutability of the data processed. There are also cases of proceedings initiated without payment of the tax contribution by the claimant or others in which the party losing the case does not comply with the provisions of the judgment issued by the tax court.

Italian Data Security Authority Recommendations

The Italian Data Security Authority provides for a series of measures relating to the processing of judicial data by electronic systems. The following subsections describe the main measures that affect the conduct of the tax process in digital form.

Evaluation of subjective characteristics

The attribution of the functions of system administrator must take place after evaluating the experience, the capacity and the reliability of the designated subject, who must provide a suitable guarantee of full compliance with the current provisions on the subject of treatment, including the safety profile.

Individual designations

The designation of a system administrator must be in each case individual and needs to consider the analytical listing of the operating areas allowed based on the assigned authorization profile.

List of system administrators

The identifying details of the system administrators natural persons, with the list of the functions assigned must be reported in an internal document to be kept updated and available in the event of checks also by the Guarantor. In case the activity of the system administrators concerns indirectly services or systems that treat or allow the processing of personal information of workers, the public and private owners as employers are required to disclose or know the identity of system administrators in the context of their organizations, according to the characteristics of the company or service, in relation to the various IT services to which they are assigned. In the case of system administration services outsourced, the data controller must directly and specifically store, for any eventuality, the identifying details of the natural persons in charge as system administrators.

Activity verification

Annually, the owners or the data processors must subject the work of the system administrators to a verification activity, in order to check its compliance with organizational, technical and safety measures with respect to the treatments of personal data required by current regulations.

Access Logging

System administrators must adopt suitable systems for the registration of logical accesses (computer authentication) to computer systems and electronic archives. The registrations (access log) must have characteristics of completeness, inalterability and possibility of verifying their integrity adequate to achieve the purpose of verification for which they are required. The records must include the time references and the description of the event that generated them and must be kept for a reasonable period, not less than six months.

4. A blockchain based solution to improve Italian electronic tax process

System architecture

The proposed solution is based on an open source open framework powered by IBM known as Hyperledger Fabric that allows the creation of a blockchain network and the implementation of smart contracts. The network nodes are in execution at the territorial commissions and their data storage processes guarantee high reliability and fault tolerance. The system architecture has been designed following a modular extensible approach based on four pillars layers: data store, smart contract, coummunication and consensus. Data store layer allows data collecting in a secure and permanent manner offering access to other modules. Smart contract layer is responsible for processing smart contracts and determining wheter they are valid by executing their business logic. Communication layer is concerned with ensuring communication among peer-to-peer nodes that participate in a shared ledger instance. Communication layer is responsible for generating an agreement on the order and confirming the correctness of the ledger's informative content. In addition to the tiers described above there are a number of services that allow to manage identities by providing authentication and authorization during network operations as well as a set of policy services that dictate the rules of system operation. Users and applications can interface to blockchain through REST Application Program Interfaces (APIs) in order to ensure full integration with the systems currently in operation in the context of the telematic fiscal process. The blockchain architectural model chosen for the implementation of the telematic fiscal process is the federated one. The federation is made up of judges and officials working for territorial commissions that represent the nodes of the network and contribute to reaching the distributed consensus on the ledger. In particular, each territorial commission has the right to insert and view the procedural files under its competence while all the commissions will participate in the elaboration of the algorithm for the achievement of distributed consent on all transactions to be introduced into the blockchain including the approval of smart contracts containing the rules for the conduct of the tax process. The architectural scheme allows the use of the most common mechanisms for achieving consensus such as through the use of lottery based algorithms including Proof of Elapsed Time (PoET) and Proof of Work (PoW) or through the use of voting-based methods including Redundant Byzantine Fault Tolerance (RBFT). Each of these approaches targets different network requirements and fault tolerance models. Among the consensus algorithms that are most suitable for the context of interest we have selected the voted based that allows a fair trade off between scalability and speed as well as providing low latency processing times. Specifically, as also explained in the next section, the consent on a digital procedural dossier to be inserted in the ledger is reached when the majority of nodes, represented by the competent officials working for the tax commissions, validates it, whereas the consent to the final dispositive of the judgment becomes valid when it is validated by all the judges of the competent tax court.

System operation

The objective of the work is to improve the security of data management in the context of the telematic tax process and to ensure the enforceability of the tax court decision on the appeal. In order to achieve these purposes we introduce blockchain technology adopting a solution that is fully integrated with the tax information systems and applications currently in operation (SIGIT - PTT). Specifically, blockchain technology is completely transparent to the user who, in order to initiate a tax appeal, registers on the application managed by the Italian Ministry of Economy and Finance and deposits the required documentation. At the base of the functioning of the system

there is a blockchain network that represents a technical infrastructure capable of offering ledger and smart contract services to applications in which all the territorial tax commissions partecipate organised in a consortium. The system can be seen as a collection of participating entities, events and objects with their own status, as shown in Figure 1. Specifically, the occurrence of an event is transcribed in an immutable form in the blockchain and if it is validated by the participating entities in accordance with the endorsement policy, it will contribute to updating the status of the objects involved. The entities participating in the system are officials of territorial tax commissions and tax judges as highlighted in Figure 2. In order to be eligible to use a service, each of them must have a digital identity encapsulated in an X.509 digital certificate that determine the exact permissions over resources and access to information that actors have in a blockchain network. The system logic is based on smart contracts that define the rules of operation of the process, representing the computer transcription of the regulations on the tax process, for this reason they must necessarily be approved by all territorial tax commissions. Specifically, they contain all the rules relating to the conduct of the process that are invoked by the judges and staff of the commissions generating transactions that are recorded in the blockchain. Each activity related to the tax process generates an event that causes the execution of a specific smart contract that will transcribe it in the blockchain in order to be validated by the competent entities. The tax process itself represents a system business object and all smart contracts invoked by system participants through applications go to update their status and register it in the blockchain. In other words, each smart contract defines specific activities to be carried out at a specific procedural stage and and requires the validation of the entities provided by the endorsment policy in order to be considered valid. The invocation of a smart contract generates a transaction to be recorded in the blockchain. Although all transactions are recorded in the blockchain, whether valid or invalid, only valid transactions contribute to the world state update. The appeal procedure begins when the claimant files his appeal via the online procedure. The document is inserted in the blockchain through a transaction that requires validation by the operators of the competent tax commission territorially following which the status of the appeal will be updated. Once the case file has been uploaded into the blockchain and approved by the competent staff, the judge is authorised to proceed with the procedural decision. In particular, when the appointed judge takes a decision, he proceeds with its implementation by invoking the methods provided in the smart contracts that govern the process. The other members of the college will endorse the decision in order to update the status of the trial in concluded. The court's decision is finalised by invoking the methods used to transfer the amount provided for by the losing party to the winning party, thereby ensuring the enforceability of the operative part of the judgment. The digital tax flow is shown in Figure 3.

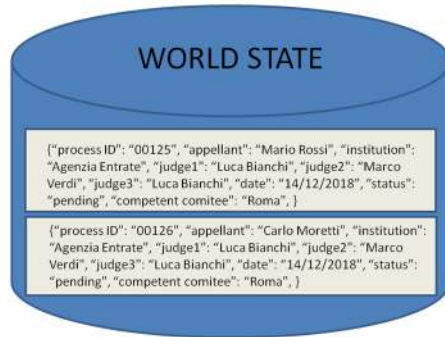*Figure 1: An example of state of the business object trial file*

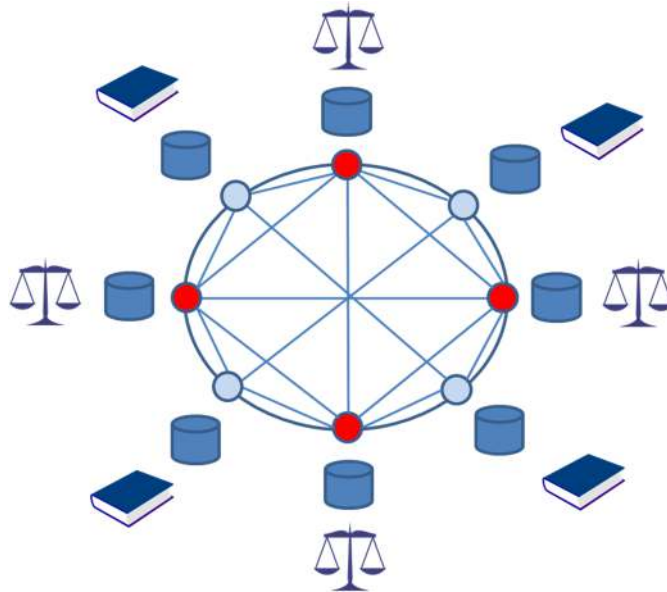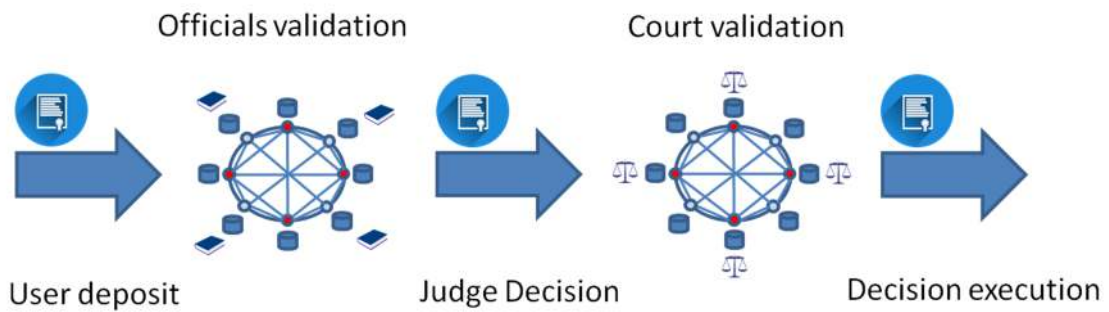*Figure 2: Permissioned validation network with officials and judges nodes*

Figure 3: The flow of a digital tax process

5. Conclusion

In this study, we propose an innovative solution to improve the conduct of the telematic fiscal process through the use of blockchain technology. The information technologies currently used, such as web applications for filing files and digital signatures, although they have considerably improved the process, do not guarantee the enforceability of the court's decision and do not allow the maximum levels of security to be reached, in fact the control of the integrity of the file, including its replacement or the removal of any attachments, is entrusted to expensive and not always secure log systems. Given the confidentiality of the data involved and the procedures used, our attention was focused on consortium blockchain that allow defining specific rules of operation based on the entities that participate in the system. Specifically, a consortium has been created made up of all the Italian territorial tax commissions that are territorially competent for the management of procedural files and the conduct of processes. The improvements resulting from the proposed solution can be evaluated under two different dimensions of analysis, on the one hand, the introduction of blockchain technology makes the procedural bundles confidential and unalterable over time as provided for by the provisions of the Italian privacy guarantor and the European GDPR, on the other hand, the use of smart contracts allows to reduce trial times and to be certain of the enforceability of the court's decision. The use of smart contracts also allows to ensure the correct payment of the tax contribution, in fact it is precisely this last event that initiates the execution flow of the tax process. In order for the system to be fully implementable, regulatory adaptations are needed in addition to the technical rules of Italian Agency for Digitalization (Agid) on distributed ledger technologies. Surely the strategy developed guarantees greater uniformity in the work of the various territorial tax commissions and is also applicable to other domains such as the electronic civil process that will be analyzed in future work.

References

[1] Beck, R., Avital, M., Rossi, M., & Thatcher, J. B. (2017). Blockchain Technology in Business and Information Systems Research. *Business and Information Systems Engineering*. https://doi.org/10.1007/s12599-017-0505-1

[2] Blockchain, P., De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2018). PBFT vs Proof-of-Authority: Applying the CAP Theorem to. In *CEUR Workshop Proceedings*.

[3] Buterin, V. (2015). On public and private Blockchains. *Blog.Ethereum.Org*. https://doi.org/10.5949/liverpool/9780853239963.003.0009

[4] Davidson, S., De Filippi, P., & Potts, J. (2016). *Economics of Blockchain. SSRN*. https://doi.org/10.2139/ssrn.2744751

[5] Dwork, C., & Naor, M. (2007). Pricing via Processing or Combatting Junk Mail. In *Advances in Cryptology — CRYPTO' 92*. https://doi.org/10.1007/3-540-48071-4_10

[6] Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the Security and Performance of Proof of Work Blockchains. https://doi.org/10.1145/2976749.2978341

[7] Gilbert, H., & Handschuh, H. (2011). Security Analysis of SHA-256 and Sisters.

https://doi.org/10.1007/978-3-540-24654-1_13

[8]Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*. https://doi.org/10.1016/j.telpol.2017.09.003

[9]Malone, D., & O'Dwyer, K. J. (2014). Bitcoin Mining and its Energy Footprint. https://doi.org/10.1049/cp.2014.0699

[10]Michael, C., Nachiappan, Pradan, P., Verma, S., & Kalyanaraman, V. (2016). BlockChain Technology: Beyond Bitcoin. *International Journal of Hyperconnectivity and the Internet of Things*. https://doi.org/10.4018/ijhiot.2017070101

[11]Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2017). A review on consensus algorithm of blockchain. In *2017 IEEE International Conference on Systems, Man, and Cybernetics, SMC 2017*. https://doi.org/10.1109/SMC.2017.8123011

[12]Saleh, F. (2018). Blockchain Without Waste: Proof-of-Stake. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3183935

[13]Satoshi, N., & Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic cash system. *Bitcoin*. https://doi.org/10.1007/s10838-008-9062-0

[14]Spasovski, J., & Eklund, P. (2018). Proof of Stake Blockchain. https://doi.org/10.1145/3167020.3167058

[15]Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM*. https://doi.org/10.1145/2994581