Blockchain based solution for securing real property transaction: a case study for North Macedonia

Admirim Aliti[1], Elva Leka[2]; Marika Apostolova[3]; Artan Luma[4]
South East European University, Tetovo, North Macedonia[1,3,4]
Polytechnic University of Tirana, Tirane, Albania[2]
aa03511@seeu.edu.mk, elva.leka@fgjm.edu.al, m.apostolova@seeu.edu.mk, a.luma@seeu.edu.mk

Abstract**:** *This paper will focus on the implementation of decentralized technologies, such as blockchain, on the issuance and management of real estate properties, starting with ownership of the certificates. The focus will be the improvement of the actual process, as well as increasing integrity and trustworthiness of ownership certificates. A series of technology and methodology selections will be made, along with the main plan of setting up the decentralized networks and enabling communication with the user. We propose a framework to manage real estate property's certificates and explain in detail the architecture of the system and each component of the system. This system will be based on Ethereum EVM, where the main execution will take place, the smart contracts will be deployed and the main dataset will be stored. IPFS will be used to store files such as photos or scanned documents and will be attached to the certificate in blockchain.*
KEYWORDS: *BLOCKCHAIN TECHNOLOGY, REAL ESTATE, CADASTRAL MANAGEMENT, TRANSPARENCY, PUBLIC ADMINISTRATION*

1. Introduction

Blockchain is being used even more in fields such as DeFi (Decentralized Finance), Education, Cryptocurrencies, NFT markets, Copyright, IoT, Health care, insurance, etc. [1,2]. However, there doesn't seem to be a solid implementation of real estate. Most solutions focus on creating a relationship between owner-client, agency-client, or investor-client, making the payment process automatic. A blockchain system that enables ownership still remains to be developed. The current process of obtaining an ownership certificate is tedious and time-consuming.

As of now, most of the institutions which issue certificates are based on a centralized system, where data is stored in a single location owned by an entity or company, or in some cases not stored digitally at all. Furthermore, actual systems are not made to handle large amounts of parallel requests and lack the integrity of the data stored. One example would be the downtime during a DDoS attack, or temporary (maybe even permanent) loss of data due to attacks, viruses and errors, or even human errors [3]. Another issue, as mentioned above, is the integrity of data stored and transparency, where digital access to the certificate is often missing.

From our literature review, we identified that there exists a gap to the implementation of blockchain in the Land Administration System (LAS), especially in real property management. LAS represents a system that is used to manage a real property with the main functions such as: (1) locating and identifying that property; (2) keeping a record of ownership of past and current data; (3) value; (4) and use of the property. It also contains data about the physical, spatial and topographic characteristics of real property [4].

Taking into consideration that LAS generates very important data seeing from a social, economic and political perspective, it is of great importance that the LAS be immutable, transparent and tamper-proof. Even though a lot of public services rely on data stored in systems that are used for LA, we still face a lot of problems in those LAS, relating to: (1) the correctness of stored data, (2) efficiency, (3) time consuming on the process of registering real estate transactions (month/years) [5]. In our previous paper [6], we have done a Systematic Literature Review and have analyzed that blockchain technology has the potential to play a critical role in the digitalization sector, not only in terms of administrative efficiency, but also in terms of increasing transparency and accessibility of services. Blockchain-based solutions facilitate citizen-government collaboration by safely streamlining and automating procedures while maintaining privacy and secrecy.

We propose to use blockchain technology to implement a system to manage real estate properties and to avoid all above mentioned actual drawbacks. Therefore, in this work, a blockchain-based framework is proposed to develop a land administration system to manage those properties. The proposed framework was simulated in Ethereum blockchain platform; and showed that the framework contributed to develop a secure, reliable, scalable, effective and efficient land administration system.

In Section II is presented a background and related work of blockchain adoption in Land Administration System. Section III presents the architecture and details about each component of the proposed system. The necessary interfaces to be implemented are described at section IV and conclusions and future work in section V.

2. Background and related work

2.1 Background

A Blockchain network is a distributed system that relies on a consensus algorithm, which responsibility is to ensure agreement on the states of certain data among distributed nodes [7]. Considering that the consensus algorithm is the core component that indicates in the performance and the way how the system behaves, it is important to choose the right consensus algorithm depending on the system needed to be implemented. There are several consensus algorithms that can be used in blockchain, which are categorized into two categories: (1) *proof-based*, which requires the nodes joining and verifying the network to show that they are more qualified than the others to do the appending work and (2) *vote-based consensus algorithm*, which requires nodes in the network to exchange their results of verifying a new block or transaction, before making the final decision [8]; such as: Proof of Work (PoW) and Proof of Stake (PoS).

For the implementation of the system, we need to develop smart contracts in the Ethereum platform. A smart contract is a piece of software that stores rules for negotiating the terms of an agreement, automatically verify fulfilment, and then executes the agreed terms [9]. The correct execution of smart contracts is enforced without relying on a trusted authority. We have chosen Solidity [10] programming language to develop the smart contracts of our system. Solidity is an object-oriented programming language developed in 2014, somewhat similar to Java. With the use of Solidity, we would encounter a new definition which is a "smart contract". This is a set of instructions that does certain actions depending on user input. These contracts operate within the internal blockchain environment called Ethereum Virtual Machine (EVM) [11], and it is where the contract will rest after its deployment and using these smart contracts we will issue and verify certificates.

2.2 Related Work

Many solutions have been proposed and developed from the perspective of using blockchain in public administration. We limit our discussion to the systems and architectures that propose blockchain-based solutions in LAS or especially in real estate certificate management.

Blockchain technology is already being used by European states, but Sweden [12] is the first country that has adopted blockchain on the country's land registry since 2016, with the intention to address security issues, reduce fraudulent activities, eliminate paperwork, and speed up transactions. Furthermore, Georgia and Netherlands have advanced in using blockchain in government. Georgia [13] created a blockchain registry system that allows citizens to verify the ownership of a property. Meanwhile, the Netherlands initiated a project in May 2018, which utilizes blockchain and Artificial Intelligence (AI) to register ownership details of a property and geographical coordinates.

In their paper [14] authors have proposed a system architecture for a blockchain-based Land Information System (LIS) in Serbia, which responsibility would be keeping track of transactions in LIS by offering immutability, increasing security, efficiency, integrity and improving the necessary time for a transaction to be processed. Furthermore, they have provided and detailed the design of the system, framework, and implementation of the system in the Ethereum platform. They argued the benefits this system could bring compared to the actual system of how transactions are handled in Serbian land administration.

Torun *et al.* [15] have proposed a hierarchical blockchain architecture for a relaxed hegemony cadastre data management in Turkey. In his study, he has identified the problem of inconsistent boundary determination and has proposed a methodology, where a transaction of a boundary change could not be booked in the land registry without the common and joint approval of all stakeholders. The study gives the design and implementation aspects of "the GIS part" of the component and aims to solve the particular problem of multiple physical boundaries for identical cadastral boundary data and for providing an approach to introduce the land owners into the core of cadastral decision making in the environment of open-data-policy, decentralization and democratization of geospatial data.

Furthermore, in their paper [16] the authors have analysed the possible applications and limitations of adapting blockchain in Land Administration. In this article are discussed all characteristics of blockchain technology and how they may have an impact in different blockchain-based implementations of land administration. The authors argue that the number of peer-reviewed papers on the possible application of blockchain in LAS is limited and blockchain implementation/development is still in the early stages.

Muller *et al.* [17] have presented the possibilities for the implementation and the potential design of a blockchain-based land register in Germany. The idea of upgrading the current electronic land registry with a blockchain solution takes into account the emerging importance of blockchain technology that has been developed in recent years. They have addressed also potential obstacles, and legal, organizational and technical issues.

Authors in their paper [18] have conducted a detailed study by analysing the adaption of blockchain technology and its implementations by various governments around the globe and additionally they have analysed the evolution of e-government based on empirical evidence from a Dubai government entity which has used blockchain technology to offer end-user services. They have analysed and addressed the challenges of using blockchain in government for public services as well.

3. Proposed solution

We propose to use blockchain technology to implement a system to manage real estate properties and to avoid all actual system drawbacks in Cadaster of North Macedonia. Therefore, in this work, a blockchain-based framework is proposed to develop a land administration system, which will be implemented and simulated in Ethereum blockchain platform and will contribute to developing a secure, reliable, scalable, effective and efficient system.

In a LAS can be stored two important kinds of information. The first is referred to as legal data, which presents ownership data and other rights of that real property. And the second is referred to spatial data, which presents real property's data about position and shape. Thus, in North Macedonia, we have two main records of a real property, which is Land register and Cadaster. Land register provides answers to questions about who an owner of certain property is and on what legal document is that right based on. Cadaster provides answer to questions regarding location of certain property, property addresses, and land use, nature and duration of tenure, details about construction buildings, population, and land taxation value.

The activities which should be considered in adapting blockchain technology in real property management are as follows: (1) What kind of implementation should be used? Public, private or hybrid approach [19] is better to fulfill all the necessary requirements of management of user identity and record the transactions?; (2) Design the system architecture; (3) Implementation and development of smart contract; (4) Testing and evaluations; (5) Analyze business potential of such a prototype.

In this paper we will be focused mostly in the first two tasks. The main function, the system should perform are: (1) to offer the possibility to save and update the real property data information; (2) to offer the possibility to the buyer to check for the interested real property related information; (3) to initiate the real property's ownership transfer process; (4) to add the transaction of 'ownership transfer process' to the blockchain network.

3.1 What we propose

The solution we propose is a collection of services deployed in different production environments. Ethereum EVM will be used to deploy and execute a smart contract, which is simply a program or set of instructions written in "Solidity" and executed on the blockchain. Smart contracts are used as a type of automation on blockchain based on predefined conditions. On top of that, an Interplanetary File System (IPFS) network [20] will be used to store large files, such as photos of a property scanned documents or aerial images.

In order to connect and interact with those networks, a set of interfaces have been developed. The interfaces are developed in HTML/CSS/JavaScript using modern frameworks such as ReactJS and libraries such as Web3JS, crypt-js and IPFS-client. These interfaces have been split in two parts by having separate interfaces for issuing certificates to the blockchain and another interface for verifying and getting certificates from the blockchain and IPFS network. The first interface will be used by the cadaster, whereas the other one by the buyers/owners of a property in order to verify ownership of a property.

3.2 The architecture of the system we propose

The architecture of the system we propose is presented in Fig. 1. As the figure shows, firstly the cadastre deploys an encrypted certificate that can only be decrypted by using the encryption key. The key is used to encrypt both blockchain and IPFS data, thus rendering them useless without the encryption key and making the system more secure. The encryption key then is communicated to the owner of the property, who then can use this key in order to view his certificate.

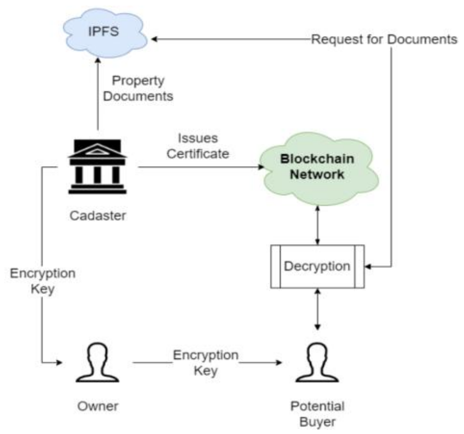

Figure 1. *The Overall Architecture of the System*

Alternatively, the cadaster stores this key in their private serves, in case the owner loses the key. Afterward, the owner can send this encryption key to a potential buyer (this is done by using a QR code, where the buyer will not be able to copy and get hold of the encryption key) and then the buyer can verify the ownership of the property. Otherwise, the owner can use the interface on his own and show the result to the buyer.

3.3 Role Configuration

The proposed solution consists of roles. We will be creating a role-based system, where the main identifier will be the blockchain address. Roles are as follows: The ministry or the highest institution to this project (government entity) will allow other entities (such as cadaster) to issue certificates. This entity also has permission to issue certificates itself. After being given permission, Cadasters will be able to issue certificates on their own. If a certificate is issued twice, its data will be retained as an older version, and the new data will be displayed to the user, thus pushing the old data further into the history changes.

When issuing a smart contract, we need to fill in a parameter called "master address". This address will be used to issue other addresses that in turn will issue certificates. This address will be owned by the main entity that owns the network. Another address would be the ROOT address, which will be used to issue the smart contract. After the deployment of the smart contract, the private key of this address will be encrypted, fragmented and stored as safely as possible. This is done because this address will be later used as a failsafe in case the master address is compromised or stolen. Being the highest address on the "hierarchical" system, it is suggested to be stored offline, encrypted and in a place hard to be accessed. Ain storage techniques include storage in a local server, offline on a USB< disc CD/DVD, paper or using services used to store classified data. The next address will belong to the issuer, and this address will be used a lot of time. This because it will be used to issue and modify certificates. For ease of use, this address will be identified by name and institution ID.

3.4 Certificate Verification

Firstly, the issuing entity issues a certificate using its address, signing it using its private key, after which this certificate is added to the network pending verification and included in a block. In case it is accepted by the network, it is checked against the smart contract, where it is checked if it fulfils all the requirements and if the issuer is valid and authorized. If everything goes as expected, it is added to the network according to the smart contract instructions, and the certificate is added to the network. Otherwise, the transaction remains verified, but the storage of this certificate to verified certificates is blocked. This means that the operation has been canceled and this certificate cannot be used. In both cases, a fee is paid to the network, so we should make sure to use an authorized address.

Due to the costs and size limits that we have in a transaction, we will need to minimize the length of data sent to the blockchain network. This will be done by offloading some data such as photos, videos, and documents on other networks, be it IPFS of a private server, where in both cases we would store the hash of this file in blockchain (unique value for each file/document), making it possible to verify the integrity of the file requested in the certificate. We should mention that every piece of information will be encrypted, and it will be impossible to view it without the encryption key. Only transaction data and block numbers will be visible. This is done in order to protect the privacy of users.

4. Interfaces

In this solution we propose two interfaces will be deployed. The interfaces will be used in order to communicate with the blockchain network. They should be easy to use because their target audience will be the common users and the public.

4.1 Verifier Interface

Verifier will make it possible to verify a certificate on the system. As input, we will need the ID of the certificate. Fig. 2 presents the flow of information from the verifier to the network.

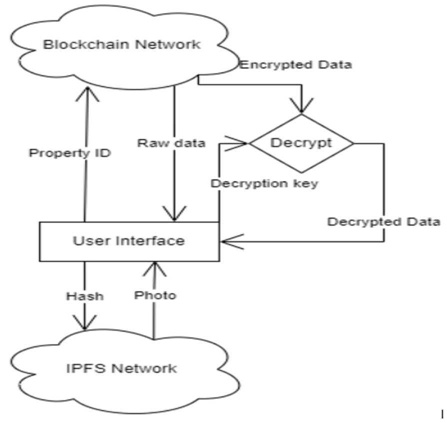

Figure 2. *Flow of information from verifier to the network*

At first basic public information will be shown, such as the type of real estate, area or description, address or location. In case these properties are enough the third party won't need a decryption key. Otherwise, the owner authorizes decryption using its decryption key. In this case private details are shown such as: Owner, Co-owners, Cadastral Zone / Coordinates, price etc. Should be noted that this information will be in accordance with the current state of North Macedonia laws. After retrieving data from blockchain, we can connect immediately to the IPFS network and retrieve its images.

4.2 Issuer Interface

This part of the software will be used by the issuing institution. In this interface, the certificate will be issued and sent to the network. After the certificate has been issued, the institution is responsible for sending the encryption key to the owner.

Initially, the user fills all the fields with the information of the ownership certificate that is required. After that, some of these fields are encrypted using the specified encryption key specified by the user or randomly generated, as it is shown in Fig. 3.

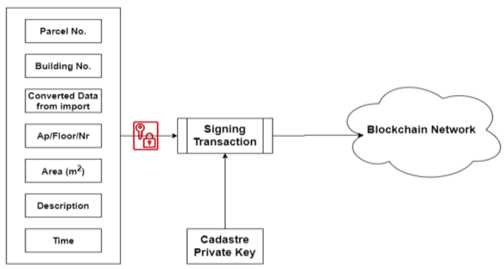

Figure 3. *The flow of information from the verifier to the network*

Once filled in, the transaction is initiated using the private key, and once confirmed it is added to the blockchain. Should be noted that this information is encrypted.

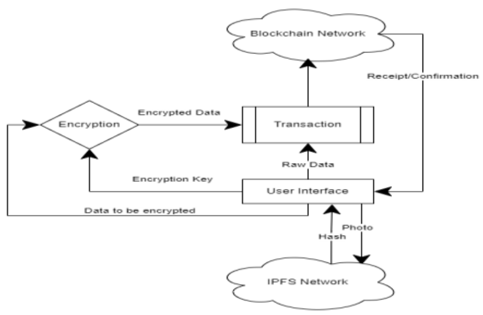

Figure 4. *The flow of information from issuer to respective network*

Along with the rest of the data, a transaction is created. The transaction takes one parameter, which is the address encryption key that will be used to issue the certificate. Once the certificate has been issued the user needs to wait for the transaction receipt. This transaction contains data such as transaction address, gas used, included block, etc. Unlike the previous case, we first connect to the IPFS, upload images, and then take their hashes. These hashes are included as part of the transaction.

5. Conclusion

In Blockchain technology as a new decentralized peer-to-peer infrastructure supports openness, transparency, accountability, identity management and trust. It has received extensive attention recently and it is applied in many fields. We believe that using blockchain technology in public administration will make a more efficient administration. The trust, transparency, and accessibility of services to the citizens will be increased by using this technology. By safely improving and automating processes in compliance with privacy and confidentiality regulations, blockchain-based solutions will strengthen the bond between citizens and the government.

In this paper we proposed to use blockchain as a mechanism to be used in public administration in the Land Administration System (LAS) ***to manage real estate properties***, in order to improve efficiency and security and to address problems like: tracking usage of Real Property, corruptions of certificates, ownership rights. This system is based on Ethereum EVM, where the main execution will take place, where the smart contract will be deployed and where the main dataset will be stored. IPFS will be used to store files such as photos or scanned documents and will be attached to the certificate in the blockchain. The system we propose aims to enable much more sophisticated systems for issuing and verifying certificates of real estate property entirely on blockchain. This includes the issuance of several certificates as per state guidelines, and verification from other third parties using decryption keys. The user is required to specify only two fields, property ID and decryption key. These services can be accessed from every device that has been connected to the internet. In each case, we can deploy the project to a private or public blockchain. We have considered that the actual implementation should not be too complex compared to the actual implementations, as well as match the costs of maintenance as closely as possible.

As future work, first we will be focused on Blockchain development and smart contract deployment. Additionally, we will work on (1) technical changes, such as IPFS orchestration, increasing the number of key distribution methods, tweaking the environment based on PoC results, lower resource usage, dockerization, 1-click node deployment as well as on (2) quality-of-life improvements, such as QR code integration, customization panel, offering printable (hard copy) certificate, better UI/UX.

References

[1] Petrov D. *et al*. The Impact of Blockchain and Distributed Ledger Technology on Financial Services. International Scientific Journal “Industry 4.0”, Vol IV, Issue 2, pp. 88-91, 201, Web ISSN 2534-997X, Print ISSN: 2534-8582.

[2] Mechkaroska D., Popovska-Mitrovikj A., Dimitrova V. Secure Big Data and IoT With Implementation of Blockchain. In International Scientific Journal “Security $ Future”, Vol. II, Issue 4, pp. 183-185, 2018, Web ISSN: 2535-082X, Print ISSN: 2535-0668.

[3] Wani, Sh., Imthiyas, M., Almohamedh, H., Alhamed, K.M., Almotairi, S., Gulzar, S. Distributed Denial of Service (DDoS) Mitigation Using Blockchain – A Comprehensive Insight. *Symmetry*, pp. 227, Vol. 13, No. 2, 1st January 2021, DOI: 10.3390/sym13020227, Published by MDPI.

[4] Pereira, S. N., Tasnim, N., Rizon, R. S., Islam, M.N. Blockchain-Based Digital Record-Keeping in Land Administration System. In *Proceedings of International Joint Conference on Advances in Computational Intelligence*, May 2021, Online ISBN: 978-981-16-0586-4, Print ISBN: 978-981-16-0585-7, pp. 431-443, DOI: 10.1007/978-981-16-0586-4_35, Published by Springer, Singapore.

[5] Ameyaw, P.D., Vries, W.T. Transparency of Land Administration and the Role of Blockchain Technology, a Four-Dimensional Framework Analysis from the Ghanaian Land Perspective. *Land 2020*, 491, DOI: 10.3390/land9120491, Published by MDPI, Available: https://www.mdpi.com/2073-445X/9/12/491.

[6] Aliti, A., Leka, E., Luma, A., Apostolova, M. A Systematic Literature Review on Using Blockchain Technology in Public Administration. In *Proceedings of 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*, May 2022, Opatija, Croatia, Published by IEEE, DOI: 10.23919/MIPRO55190.2022.9803797.

[7] Ferdous, M.S, Chowdhury, M.J.M., Hoque M.A, Colman, A. Blockchain Consensus Algorithms: A Survey. *arXiv:2001.07091v2* [cs.DC], February 2020, DOI: 10.48550/arXiv.2001.07091, Available: https://arxiv.org/pdf/2001.07091.

[8] Nguyen, G.T, Kim, K. A Survey about Consensus Algorithms Used in Blockchain. *Journal of Information Processing Systems (JIPS)*, Vol. 14, No. 1, pp. 101-128, February 2018, Print ISSN 1976-913X, Online ISSN: 2092-805X, DOI:10.3745/JIPS.01.0024.

[9] Matzut, R., Pennekamp, J., Buchholz, E., Wehrle, K. Utilizing Public Blockchain for the Sybil-Resistant Bootstrapping of Distributed Anonymity Services. In *Proceedings of the 15th ACM ASIA Conference on Computer and Communications Security (ASIACCS ’20)*, May 2022, Taipei, Taiwan. Published by ACM, New York, USA, DOI: 10.1145/3320269.3384729.

[10] Zhou, H. Fard, A. M., Makanju, A. The State of Ethereum Smart Contracts Security: vulnerabilities, Countermeasures, and Tool Support. *Journal of Cybersecurity and Privacy 2022*, ISSN: 264-800X, 2, pp. 358-378, Published by MDPI, DOI: 10.3390/jcp2020019.

[11] Norvill, R., Pontiveros, B.B.F., State, R., Cullen, A.J. Visual emulation for Ethereum’s Virtual Machine. In *Proceedings of Conference: NOMS 2018 – 2018 IEEE/IFIP Network Operation and Management Symposium*, pp. 1-4, DOI: 10.1109/NOMS.2018.8406332.

[12] McMurren, J., Young, A., Verhulst, S. *Addressing Transaction Costs Through Bockcchain and Identity in Swedish Land Transfers*. October 2018, Available at: https://blockchan.ge/blockchange-land-registry.pdf.

[13] Shang, Q., Price, A. A Blockchain-Based Land Titling Project in The Republic of Georgia, Rebuilding Public Trust and Lessons for Future Pilot Projects. *Innovations*: Technology, Governance, Globalization 2019, , Vol. 12, Issue 3-5, pp. 72-78, Online ISSN: 1558-2485, Print ISSN: 1558-2477 DOI: 10.1162/inov_a_00276.

[14] Sladic, G., Milosavljevic, B., Nikolic, S, Sladic, D., Radulovic, A. Blockcahain Solution for Securing Real Property Transaction: A Case Study for Serbia. *ISPR International Journral of Geo-Information* 2021, 10, 35, DOI: 10.3390/ijgi10010035, Published by MDPI.

[15] Torun, A. Hierarchical Blockchain Architecture for a Relaxed Hegemony on Cadastre Data Management and Update: A Case Study for Turkey. In *Proceedings of UCTEA International Geographical Information Systems Congress 2017*, 15-18 November 2017, Adana, Turkey.

[16] Stefanovic, M., Przulj, D., Ristic S., Stefanovic, D. Blockchain and Land Administration: Possible Applications and Limitation. In *Proceedings of the 5th International Scientific Conference on Contemporary Issues in Economics, Business and Management (EBM 2018)*, Kragujevac, Republic of Serbia, 9-10th November 2018, Published by IEEE.

[17] Muller, H., Seifert, M. Blockchain, a Feasible for Land Administration?”. In *FIG Working week 2019 Geospatial information for a smarter life and environmental resilience*, Hanoi, Vietnam, April 22-26, 2019, Available at: https://www.fig.net/resources/proceedings/fig_proceedings/fig2019/papers/ts01i/TS01I_seifert_mueller_10110.pdf.

[18] Khan, S., Shael, M., Majdalawieh, M., Nizamuddin, N., Nicho, M. Blockchain for Governments: The Case of Dubai Government. *Sustainability 2022*, 14, 6576, DOI: 10.3390/su14116576.

[19] Desai, H., Kantarcioglu M., Kagal, L. A Hybrid Blockchain Architecture for Privacy-Enabled and Acccountable Auctions. In *2019 IEEE International Conference on Blockchain (Blockcchain)*, 2019, pp. 34-43, Atlanta, USA, DOI: 10.1109/Blockchain.2019.00014.

[20] Nyaletey, E., Parizi, R.M., Zhang, Q., Choo, K.K.R. BlockIPFS – Blockchain-Enabled Interplanetary File System for Forensic and Trusted Data Traceability. *2019 IEEE International Conference on Blockchain (Blockchain), 2019*, pp. 18-25, DOI: 10.1109/Blockchain.2019.00012, Published by: IEEE, Online ISBN: 978-1-7281-4693-5, Print ISBN: 978-1-7281-4694-2.