Tech Science Press

Real Estate Management via a Decentralized Blockchain Platform

Iftikhar Ahmad[1,*], Mohammed A. Alqarni[2], Abdulwahab Ali Almazroi[3] and Laiba Alam[1]

[1]Department of Computer Science and Information Technology, University of Engineering and Technology, Peshawar, Pakistan
[2]Department of Software Engineering, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia
[3]Department of Information Technology, College of Computing and Information Technology at Khulais, University of Jeddah, Jeddah, Saudi Arabia
[*]Corresponding Author: Iftikhar Ahmad. Email: ia@uetpeshawar.edu.pk
Received: 23 July 2020; Accepted: 25 September 2020

Abstract: Blockchain technology is one of the key technological breakthroughs of the last decade. It has the ability to revolutionize numerous aspects of society, including financial systems, healthcare, e-government and many others. One such area that is able to reap the benefits of blockchain technology is the real estate industry. Like many other industries, real estate faces major administrative problems such as high transaction fees, a lack of transparency, fraud and the effects of a middleman including undue influence and commissions. Blockchain enables supporting technologies to overcome the obstacles inherent within the real estate investment market. These technologies include smart contracts, immutable record management and time-stamped storage. We utilize these key properties of blockchain technology in our work by proposing a system that has the ability to record real estate transactions in a private blockchain, using smart contracts. The immutability of the blockchain ledger and transactions can provide a safe space for the real estate business. Blockchain technology can also assist the authentication process by hastening background checks. Personal digital keys are provided to parties that are involved in a contract, thus minimizing the risk of fraud. We also discuss the rationale behind the advantages of using a blockchain in this manner, and how we selected the consensus mechanism for our proposed system.

Keywords: Blockchain; real estate; smart contracts

1 Introduction

Blockchain is an emerging technology that has changed many aspects of modern finance; however, its use cases are not limited to financial systems [1]. In the past, blockchains have been used in healthcare [2], the Internet of Things [3], smart cities [4] and many other domains [5–8]. In addition, blockchains are likely to transform the foundations of society by overhauling outdated mechanisms with updated infrastructures befitting a virtualized world. In its early stages, blockchain technology was largely associated with the electronic currency Bitcoin, but the wider technological advantages were not appreciated until much later [9]. Blockchain technology offers many benefits such as speed, reliability, immutability, traceability,

transparency, decentralization and trust [10]. These advantages present blockchains as a replacement for outdated technologies in various domains where such factors are key requirements [10].

The real estate industry is estimated to be worth $162 trillion and $29 trillion in residential and commercial real estate respectively [11]. It is considered to be one of the safest options of investment, with comparatively higher returns than other investment options, but like other businesses, real estate is also facing a number of challenges. These challenges include the involvement of a third party for verification, associated monetary and time costs related to administration, access and verification of records, the use of commission-based agents, transparency issues concerning the ownership of property and a dependence on centralized systems that are susceptible to security breaches. Blockchains can offer smart contracts that assist in the removal of any third-party involvement in real estate dealings. We utilize this key property of blockchain technology in our research by proposing a system that will record real estate transactions on a private blockchain, with the support of smart contracts. Furthermore, the immutability of the blockchain ledger can provide a safe space for the real estate business. Blockchains can also help in the authentication process by speeding up background checks and providing personal digital keys to concerned parties, thereby reducing the risk of fraud.

The main objective of this work is to identify how blockchain technology and the real estate industry can interact to find a mechanism which records all important transactions on a private blockchain. In addition, the study also identifies the nature of the consensus mechanism.

The remainder of the work is organized as follows; Section 2 presents a brief overview of blockchain technology; Section 3 provides a succinct literature review of blockchain's application in various domains; Section 4 presents an architectural overview of the proposed system; Section 5 discusses the construction of the system and Section 6 concludes the work, along with discussing opportunities for further research in the field.

2 Blockchain

A blockchain is a distributed ledger which stores all transactions in a transparent and immutable manner [10]. A transaction can be any piece of information—monetary, a digital event or a basic database entry. The building unit of a blockchain is a *block*. A block can store multiple transactions, which are included in the blockchain by the agreement of the majority of the participating entities. Moreover, immutability in the context of blockchain means that once something has been recorded on the blockchain, it can never be altered—the data is secure and indisputable [10].

Fig. 1 is a simplified pictorial representation of a standard blockchain, in which each block consists of two parts—a data part that contains transactions and a header part that stores the hash pointer of the previous block. A hash pointer serves two purposes—firstly it stores the address of the previous block (ensuring that all blocks are interconnected and traceable) and secondly it confirms the pointers are hash pointers, i.e., it not only saves the address of the previous block, but ensures the hash values are dependent on the contents of the block as well [10]. Thus, immutability is achieved, as changes made in the contents by a malicious user will require changes in all subsequent blocks, rendering it impossible to edit the contents of a blockchain once it is recorded [10].

3 Literature Review

Although blockchain technology came to prominence via the widely known cryptocurrency Bitcoin, the technology itself has expanded into various other domains [1–8]. Some notable use cases of blockchain technology are found in education, healthcare, finance, city planning and e-government [1–8]. In the following text, we present a summarized review of the literature related to blockchain's application in wider society.
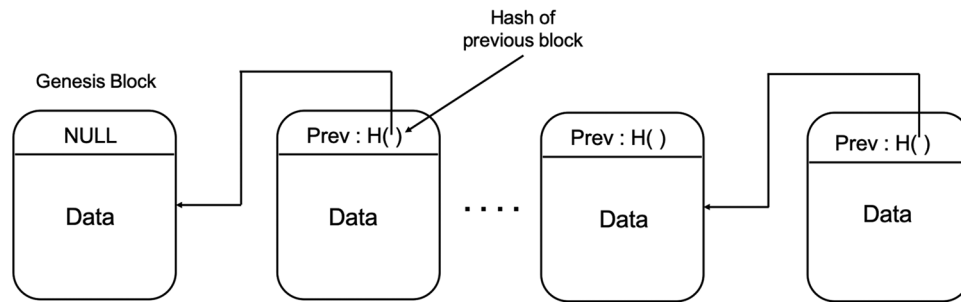
Figure 1: A simplified view of a blockchain

Xia et al. [2] presented by MeDShare—a blockchain-based healthcare management system that provides data auditing, access control, and origin tracking of medical data in a cloud repository. The system implements smart contracts as well as an access control mechanism to ensure the provisioning of data to authorized persons. Halamka et al. [12] advocate for the use of blockchain in healthcare data processing, whereas Cichosz et al. [13] argue that diabetes patients generate a lot of medical data that requires cross-institutional access. This results in the need for complex data management and sharing policies. The authors propose a blockchain-based platform to ensure the safe and timely sharing of personal medical data.

Ølnes et al. [5] propose blockchain as a supporting technology for the realization of e-government. The authors present digital ID management and secure document handling as key areas for e-government. Batubara et al. [14] conducted a detailed review of the literature encompassing the applications of blockchain technology within the context of e-government. The authors found that notwithstanding its useful applications, the absence of global legal and regulatory frameworks is a major implementation barrier.

Novo [3] proposes the use of blockchains for access control in the Internet of Things (IoT). The author observes that IoT devices are more ubiquitous than ever and are spread over a large geographical area. The reliance on a centralized access model can lead to serious performance and security issues. The author presents a new blockchain-based architecture which is evaluated using realistic IoT use cases. Dori et al. [15] criticize the computational complexity and limited scalability of blockchain, rendering the practical application of blockchains in IoT ineffective. The authors propose a concept called Lightweight Scalable Blockchain (LSB), which achieves decentralization by creating an overlay network, accessible to high resource devices. Furthermore, a distributed consensus mechanism is proposed to reduce the computational complexity of the mining process. The proposed mechanism is validated in a smart home setting through a quantitative study, in order to demonstrate the resilience of the proposed approach to a number of security attacks. Other studies in the domain of IoT include [16–18].

Blockchain technology is used extensively throughout smart cities around the world to address various data related challenges. These include blockchains in the smart economy [4], transparency in the global supply chain [19], equity crowdfunding and smart elections [20,21]. Blockchain technology is also used in education [6], privacy management and the shared economy [7,22,23].

4 Design Formulation

4.1 Architecture of the Proposed System

We utilize a layered architecture approach in our system, which consists of four layers, as shown in Fig. 2. The functionality of each layer is as follows:
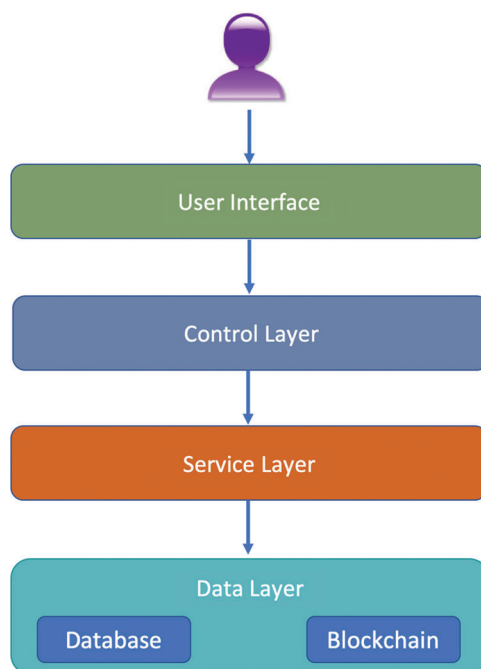
Figure 2: Architecture of the proposed system

4.1.1 User Interface Layer

The user interface layer is the front-end system, accessible to all users where the users can interact with the other sub-systems. Various functionalities are visible to the user, based on the user's privilege level. The main purpose of the user interface layer is to provide a gateway for communication between the end user and the various sub-systems.

4.1.2 Control Layer

The control layer is responsible for access control, ensuring that users can perform tasks based on their privilege level e.g., a user who is not the owner cannot be allowed to set the price of an asset. Likewise, only asset owners are authorized to modify an asset's properties—such as the area of the asset, price, etc. Finally, the control layer protects the system from intrusion.

4.1.3 Service Layer

The service layer acts as an intermediary between the control layer and the data layer. It acts as the business logic container, covering business logic rules. The control layer and service layer also safeguard against the direct exposure of data to users.

4.1.4 Data Layer

The data layer consists of a blockchain, and acts as a database for the entire system. The database is used to store user's credentials, such as usernames and passwords. The data is encrypted using AES-256-GCM, protecting credentials from malicious users. In addition, the blockchain is used to store the records of all assets, including the ownership details.

4.2 Proposed System Overview

Fig. 3 is a pictorial representation of the key components of our proposed system. The figure describes important entities and defines their interaction with one another.
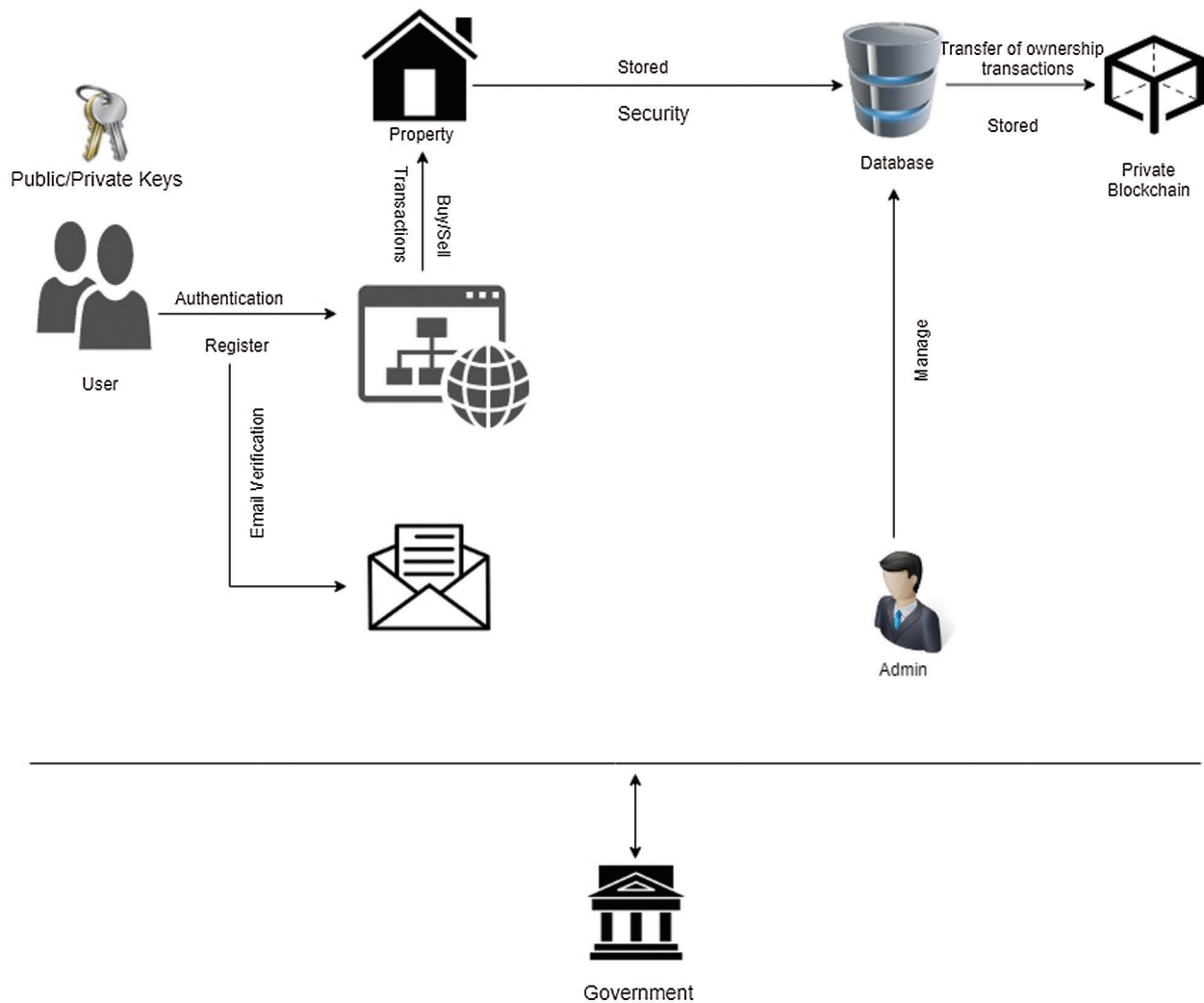
Figure 3: Overview of the proposed system

The government represents the entity that is responsible for the provision of assets to the real estate market. Note that it can also be a private organization who initially owns all the assets. Admin is responsible for the overall management of the system, including system maintenance, delisting of properties that do not meet policy guidelines and user management (however admin does not have access to the blockchain and therefore cannot change the records stored in the blockchain).

A user who wants to buy a property registers themselves in the system and is assigned a username and password. During this process, the user's email address is also verified, after which the user is assigned the role of a "registered user". A registered user can browse all of the listed assets and can show interest in purchasing an asset. A registered user cannot modify an existing listing or change the properties of the assets. A user is assigned the role of "owner" after they successfully buy an asset. An owner can list an asset for sale, modify its description, amend its price and accept a purchase offer. Once a registered user offers a price that is accepted by the owner, a smart contract is executed between the buyer and seller. The smart contract is considered successful (i.e., the ownership is transferred from seller to buyer) if both buyer and seller complete all the requirements. The requirements may include payment of a necessary fee

to the government and/or the receipt of a monetary amount by the owner. An escrow system is used to ensure that the required amount is transferred by the buyer along with a transfer of ownership. Furthermore, the benefits of the escrow system include peace of mind for both buyer and seller, as well as more efficient dispute management. Upon successful transfer of ownership, the privilege level of a registered user is changed to owner and the privilege level of an owner is relegated to that of a registered user. The relegation occurs only if the user does not own any other property. It is pertinent to note that at the time of registration, every user is assigned a set of private and public keys. The same keys are used for the transfer of ownership, which is itself recorded on the blockchain. Both registered users and owners can generate a new set of keys, however if an owner wants to use the newly generated keys, they have to transfer the owned assets to the newly generated public and private key combination.

5 Construction of the System

This section describes the design approach, the nature of blockchain technology alongside its use in our proposed system and the consensus mechanism used to allow the insertion of transactions in the blockchain.

5.1 Use Cases

We identify two main classes of users in our system—admin and a common user, which is simply referred to as "user". The use case of each category of user will also be explained.

5.1.1 User Use Case

Users can perform the functions indicated below in the user use case diagram (Fig. 4). A user should be able to register themselves in the system by verifying their email address. After successful registration, the user can log in. A registered user can search for various properties that are listed on the web-based application and offer a price for a listed asset. A user is also able to list their pre-owned properties for sale and accept or decline an offered price.
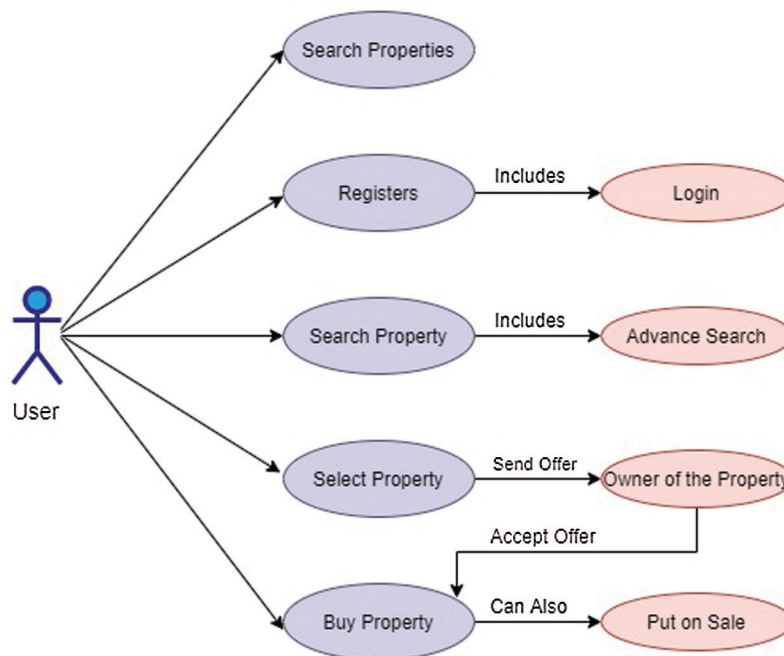

Figure 4: User use case diagram

5.1.2 Admin Use Case

The use case diagram for admin is presented in Fig. 5, demonstrating the various tasks upon log in which require admin supervision. Admins can also list a new property that is not yet owned by any individual or organization. In addition, an admin can edit the attributes of their listed assets. It is pertinent to note that like common users, admins can only read the data from the blockchain and can only write data for a change of ownership of asset that is transferred for the first time.
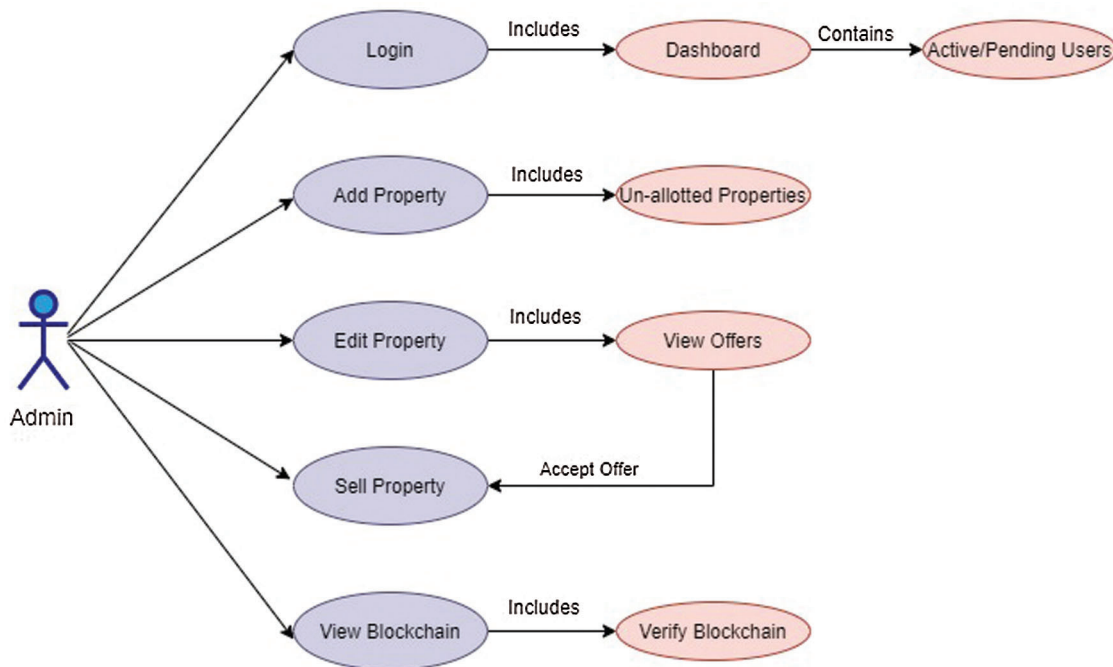

Figure 5: Admin use case diagram

5.2 Smart Contracts

Smart contracts are essentially an alternative use of crypto contracts—computer programs that automate the transfer of resources (such as assets) among parties when a pre-defined set of conditions are met [10]. Furthermore, smart contracts define guidelines and corresponding penalties, automatically imposing those obligations on participants during the process. Smart contracts benefit a variety of areas and omit the need for a third party.

In our proposed system, smart contracts are used to automate the transfer of ownership between buyer and a seller. As stated earlier, a set of conditions must be met—such as the transfer of an amount of money from a buyer to a seller and/or the payment of a fee to the government—before the transfer of ownership can be completed. In requiring this interaction, smart contracts provide a safety net to buyers and sellers alike.

5.3 Nature of Blockchain

The blockchain is the single most important element of our proposed system. It is used to ensure that all records are stored in a transparent and immutable fashion. The blockchain also ensures that the transfer of ownership of an asset can only be initiated by the owner of said asset. This restriction is enforced via the use of a set of public and private keys. Public keys are used to represent the owner of an asset whereas private keys are used to encrypt the transaction generated by the respective owner. The authenticity of the

message can be verified by using the public key of the owner without requiring the owner to disclose the private key.

A blockchain can either be classified as public or private. In a public blockchain, no individual or organization owns or controls the blockchain and the blockchain is publicly available to anybody. Any individual can obtain a pair of public and private keys to become a part of the ecosystem. Furthermore, the combination of public and private keys can be used to add records and blocks. The Bitcoin blockchain is the most well-known example of a public blockchain. Unlike its public alternative, a private blockchain is not open to the general public. It is a permissions-based blockchain with conditions in place to restrict the public from accessing its contents via the permission of a statutory body, such as an admin.

After carefully considering the requirements of our system, we opted to use a private blockchain in order to restrict access to the general public. This is primarily a design decision and a private blockchain may not be feasible for all blockchain-based systems. Implementing a private blockchain ensures that all users are required to register themselves with the relevant organization (a government agency or a public company) and access to the blockchain is permitted only after said verification is completed.

5.4 Consensus Mechanism

A blockchain has no central authority. As such, an important aspect of any blockchain is its consensus mechanism, which plays a vital role in deciding which blocks must be added to the blockchain. For a blockchain to work, the various nodes need to come to form a consensus. The consensus mechanism in the Bitcoin network works in the following manner [10]. Initially, all new transactions are broadcasted by the respective nodes to its immediate neighbors, which in turn sends them to their neighbors. Following on from this, every node collects new transactions and adds them to the block. Each node called a "mining node" or a "miner" solves a mathematical puzzle to obtain a random number in a pre-defined range, which is called *nonce*. If a node successfully computes the nonce, it broadcasts it to other nodes as proof of work. Proof of work is computationally expensive to compute, but very easy to validate, which makes it an ideal mechanism for consensus development in the Bitcoin blockchain. The node which solves the computational puzzle obtains the right to suggest a new block to the blockchain. Nodes show approval of the block by extending the blockchain via the newly approved block.

A private blockchain is a permissions centered system, in that it allows a limited number of users to access the blockchain. Network validation is conducted either directly via the network creator, or by a set of rules written as a code by the network creator. In a private blockchain, the consensus is centralized and therefore faster, which in our case does not require mining. Moreover, the private blockchain of our own system doesn't need an incentive mechanism. This would require too much computational power and isn't necessary for the purposes of what we are proposing. In addition, our private blockchain has an access control layer built into the layered architecture which controls the addition of new blocks into the blockchain.

5.5 Fraud Prevention

An important consideration in real estate management is the prevention of fraud, which can take many forms. The two most common are false listings and fake documents. False listings are properties for sale which are not owned by the lister. A private blockchain prevents this by ensuring that only the owner of the property has the ability to list a property. A fake documents fraud occurs when an imposter presents themselves as the owner of a property by exhibiting counterfeit ownership documents. As blockchain technology does not require paper-based verification and uses private keys to control ownership of a property, this negates the risk of fake document fraud. In short, the combination of smart contracts and the use of private and public keys as a built-in mechanism in our proposed system prevents several real estate frauds.

6 Conclusion and Future Directions

Currently, there are many problems associated with the management of real estate systems and the most important among them is fraud, a lengthy administrative processes and access/verification problems. In this study, we propose a system that securely stores transactions related to the ownership and transfer of properties on a private blockchain. The blockchain is immutable and no changes can be made once a record is inserted. A combination of private and public keys, as well as smart contracts, are used to allow the ubiquitous yet secure transfer of ownership.

There are various opportunities for further research in this field, such as migrating the proposed system from a private to public blockchain and identifying new blockchain consensus mechanisms. Another avenue of investigation would be to explore the possibility of integrating various cryptocurrencies in the current system, as well as other payment mechanisms.

References

[1]   A. Tapscott and T. Don, "How blockchain is changing finance," *Harvard Business Review*, vol. 1, no. 9, pp. 2–5, 2017.

[2]   Q. I. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du *et al.,* "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[3]   O. Novo, "Blockchain meets IoT: An Architecture for scalable access management in IoT," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, 2018.

[4]   J. Sun, Y. Yan and K. Z. Zhang, "Blockchain-based sharing services: What blockchain technology can contribute to smart cities," *Financial Innovation*, vol. 2, no. 1, pp. 1–9, 2016.

[5]   S. Ølnes and A. Jansen, "Blockchain technology as support infrastructure in e-government," in *Lecture Notes in Computer Science*, vol. 10428. Cham: Springer, 2017.

[6]   W. Gräther, S. Kolvenbach, R. Ruland, J. Schütte, C. Torres *et al.,* "Blockchain for education: lifelong learning passport," in *Proc. 1st ERCIM Blockchain Workshop 2018*, Amsterdam, Netherlands: European Society for Socially Embedded Technologies, pp. 1–8, 2018.

[7]   H. Wang, S. Ma, H. Dai, M. Imran and T. Wang, "Blockchain-based data privacy management with Nudge theory in open banking," *Future Generation Computer Systems*, vol. 110, pp. 812–823, 2020.

[8]   Y. Yan, Y. Dai, Z. Zhou, W. Jiang and S. Guo, "Edge computing-based tasks offloading and block caching for mobile blockchain," *Computers, Materials & Continua*, vol. 62, no. 2, pp. 905–915, 2020.

[9]   R. Beck, "Beyond bitcoin: The rise of blockchain world," *Computer*, vol. 51, no. 2, pp. 54–58, 2018.

[10] A. Narayanan, J. Bonneau and E. Felten, *Bitcoin and Cryptocurrency Technologies: A comprehensive Introduction*. 1st ed. Princeton, New Jersey: Princeton University Press, 2016.

[11] B. Wallace, "How real estate will be revolutionized on the blockchain, hackernoon, 2–18." 2018. [online] Available: https://hackernoon.com/how-real-estate-will-be-revolutionized-on-the-blockchain-63e0f0c8327.

[12] J. D. Halamka, A. Lippman and A. Ekblaw, "The potential for blockchain to transform electronic health records," *Harvard Business Review*, vol. 3, no. 3, pp. 2–5, 2017.

[13] S. L. Cichosz, M. N. Stausholm, T. Kronborg, P. Vestergaard, O. Hejlesen *et al.,* "How to use blockchain for diabetes health care data and access management: An operational concept," *Journal of Diabetes Science and Technology*, vol. 13, no. 2, pp. 248–253, 2019.

[14] F. R. Batubara, J. Ubacht and M. Janssen, "Challenges of blockchain technology adoption for e-government: A systematic literature review," in *Proc. of the 19th Annual Int. Conf. on Digital Government Research: Governance in the Data*, Delft, the Netherlands, pp. 1–9, 2018.

[15] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "LSB: A lightweight scalable blockchain for IoT security and anonymity," *Journal of Parallel and Distributed Computing*, vol. 134, pp. 180–197, 2019.

[16] P. P. Ray, D. Dash, K. Salah and N. Kumar, "Blockchain for IoT-based healthcare: Background, consensus, platforms, and use cases," *IEEE Systems Journal*, pp. 1–10, 2020.

[17] J. Wu, M. Dong, K. Ota, J. Li and W. Yang, "Application-aware consensus management for software-defined intelligent blockchain in IoT," *IEEE Network*, vol. 34, no. 1, pp. 69–75, 2020.

[18] M. Du, K. Wang, Y. Liu, K. Qian, Y. Sun *et al.,* "A three-dimensional blockchain architecture for IoT security," *IEEE Wireless Communications*, vol. 27, no. 3, pp. 38–45, 2020.

[19] M. Pilkington, "Blockchain technology: Principles and applications," in *Research Handbook on Digital Transformations*. Cheltenham, UK and Massachusetts, USA: Edward Elgar Publishing, 2016.

[20] H. Zhu and Z. Z. Zhou, "Analysis and outlook of applications of blockchain technology to equity crowdfunding in China," *Financial Innovation*, vol. 2, no. 1, pp. 1–11, 2016.

[21] K. Hegadekatti, "Analysis of present day election processes vis-à-vis elections through blockchain technology," 2017. [online] Available: https://ssrn.com/abstract=2904868.

[22] S. Huckle, R. Bhattacharya, M. White and N. Beloff, "Internet of things, blockchain and shared economy applications," *Procedia Computer Science*, vol. 98, pp. 461–466, 2016.

[23] A. Pazaitis, P. De Filippi and V. Kostakis, "Blockchain and value systems in the sharing economy: The illustrative case of backfeed," *Technological Forecasting and Social Change*, vol. 125, pp. 105–115, 2017.