Design of the Blockchain Smart Contract: A Use Case for Real Estate

Article *in* Journal of Information Security · January 2018

DOI: 10.4236/jis.2018.93013

CITATIONS
151

READS
14,615

3 authors:

Ioannis Karamitsos

33 PUBLICATIONS **259** CITATIONS

SEE PROFILE

Maria Papadaki

The University of Manchester

18 PUBLICATIONS **212** CITATIONS

SEE PROFILE

Nedaa Al Barghuthi

Higher Colleges of Technology, United Arab Emirates, Sharjah

21 PUBLICATIONS **247** CITATIONS

SEE PROFILE

Scientific Research Publishing

Journal of Information Security, 2018, 9, 177-190
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Design of the Blockchain Smart Contract: A Use Case for Real Estate

Ioannis Karamitsos[1], Maria Papadaki[2], Nedaa Baker Al Barghuthi[2]

[1]Rochester Institute of Technology, Dubai, UAE
[2]British University of Dubai, Dubai, UAE
Email: ixkcad1@rit.edu, maria.papadaki@buid.ac.ae, 20170910@student.buid.ac.ae

How to cite this paper: Karamitsos, I., Papadaki, M. and Al Barghuthi, N.B. (2018) Design of the Blockchain Smart Contract: A Use Case for Real Estate. *Journal of Information Security*, **9**, 177-190.
https://doi.org/10.4236/jis.2018.93013

Received: April 10, 2018
Accepted: June 26, 2018
Published: June 29, 2018

Abstract

Blockchain is a fast-disruptive technology becoming a key instrument in share economy. In recent years, Blockchain has received considerable attention from many researchers and government institutions. This paper aims to present the Blockchain and smart contract for a specific domain which is real estate. A detailed design of smart contract is presented and then a use case for renting residential and business buildings is examined.

Keywords

Blockchain, Ethereum, Smart Contract, Smart City, Real Estate

1. Introduction

In the recent years, there has been an increasing interest in the Blockchain technology. The Blockchain is a novel disruptive technology based on cryptography. It has been known of the work of Nakamoto [1] in 2008 who showed how this technology can become the core component to support transactions of the digital currency (bitcoin) [2]. With the introduction of Blockchain, many fields such as finance, accounting, and real estate will receive a positive impact using the benefits of this technology. One area in which blockchain technology could play a vital role is real estate and smart cities.

Globally, real estate is undergoing a major evolution and transformation towards smart cities. Smart cities are being developed and a plethora of network, services, and transactions are integrated into the city planning initially and daily use. It is anticipated that the evolution of technology, not only improves life, for example for tenants or office workers, but also enhances building performance and sustainable energy.

The Blockchain is known to be the distributed public ledger for all transactions, eliminating the need of trust between the users and the central administrator and the control is distributed among different computers/nodes in the peer-to-peer (P2P) network. Moreover, the Blockchain resolved the double-spend problem using P2P technology in combination with public/private key cryptography.

Zhao *et al.* [3] defined the Blockchain as "a distributed database comprising records of transactions that are shared among participating parties". According to Deloitte [2] [4], Blockchain is "just another type of database for recording transactions—one that is copied to all computers in a participating network".

Blockchain by definition is a chain of blocks of information that registers transactions with some characteristics. Each transaction conducted with Blockchain technology is registered, time-stamped, and consecutively widely published with a unique symbol. Transactions are inserted in the chain of blocks, and each block is composed by a unique hash function (alphanumeric string resulting from coding data with cryptographic private and public keys), a nonce (a unique number to the block) and by a hash function from the previous block. The first block is called genesis block. Therefore, an attempt to forge a block involves the need to forge preceding blocks. This makes the mechanism safe and secure from attempts to change a transaction.

Many people and researchers believe that blockchain applications in different vertical industries could lead to three generations of the Blockchain, namely Blockchain 1.0, Blockchain 2.0 and Blockchain 3.0. The Blockchain 1.0 is the decentralization of money and payments and is used for digital currency. Further, Blockchain 2.0 is used for smart contracts, assets, and properties. It is considered as the decentralization of finance. Moreover, Blockchain 3.0 is the decentralization of the digital society and is used for applications that relate to for example to the Internet of things (IoT), health and government entities.

This paper discussed the benefits of Blockchain technology applied in the smart contract for the real estate and smart cities domains. The paper is organized as follows. In Section 2, the key contribution of the work is presented and the general introduction of blockchain technology and related work is presented in Section 3. Blockchain layered approach is presented in Section 4. Section 5 has discussed the development phases of Blockchain applications. Smart contract and design methodology were described in Sections 6 and 7. Finally, a used case for smart cities is examined in Section 8.

2. Key Contributions of Proposed Work

We propose a design methodology for the smart contract which enables development of different use cases using Blockchain technology. A detailed state finite functions and processes are described for a specific use case providing noteworthy contributions to real estate domain. In this frame, the blockchain becomes the enabler for the development of paperless layer for all city transactions, in a secure fashion for the optimum management of the smart city's assets. With this

work, the smart contract provides a secure, distributed and shared decentralized ledger of all assets and transactions between landlord and tenants.

3. Background and Related Work

In its generic form, blockchain technology refers to a fully distributed cryptographically system that captures and stores a consistent, immutable and linear event log of transactions between networked actors. In such a network, blockchain technology enforces transparency and guaranteed eventual, system-wide consensus on the validity of an entire history of transactions. According to Tschorsch and Scheuermann [5], Blockchain technology can not only process currency transactions but can also ensure that transactions comply with programmable rules in the form of "smart contracts". All these transactions could be validated between parties who fully trust each other without relying on a trusted middleman.

Glaser [6] highlights all banks are currently engaged in developing a vision of what this technology means for their business. Walsh *et al.* [7] discussed in research and practice that the main parameters for Blockchain implementations such as security, data privacy, and usability are subject to select the best algorithm to ensure consensus and validity.

Tschorsch and Scheuermann [5], found that proof-of-work approaches that require high levels of energy but guarantee relatively high levels of consistency and protection against forgery by any actor in the network (e.g., in Bitcoin) compete against less costly ones.

Such alternative approaches require a portion of a trust in some elements of the network, such as actors based on the resources they put at risk during validation (e.g., proof-of stake) or in the manufacturers of devices that are used to validate transactions (e.g., proof-of-elapsed time in Hyperledger Sawtooth Lake).

For the design and deployment of Blockchain implementations [8] [9] there are different parameters that are required to be considered while designing and deploying the implemented blockchain. The selection criteria are as follows:

- Type of consensus mechanism
- Programming language
- Type of cryptocurrency used for mining
- Authorized participant in Blockchain network (who is allowed to participate in this network)

Tschorsch and Scheuermann [5] investigated the different methods for the validation and consensus of the transactions providing different balances regarding availability, consistency, and trustworthiness.

Glaser [6] found that using layered approach for the technical decisions will provide more different applications for Blockchain technology beyond from the single cryptocurrency exchanges such as Bitcoin.

Several studies investigate Blockchain technology as a disruptive way for entirely new business models and organization allowing financial transactions with trustless partners without any additional measures of security.

A number of authors have promoted the vision of a trust-free economy with truly virtual organizations and automatic business transactions of IoT devices [8] [9] [10] [11] [12]. Conversely, Atzori [13] argues that the current blockchain techniques are generally not suitable for IoT applications because IoT devices may have to work with the low computational capability or very low power and the validation time is very low as well. The main concern for Blockchain technology is the efficiency. Blockchain requires a specific validation process to create a new transaction record which leads to a significant latency of confirmation time and a waste of powerful computing resources. Today the validation time for each transaction such as Bitcoin is about 10min achieving 7 transactions/sec as the maximum throughput.

Some researchers have attempted to improve the efficiency of the Blockchain. Zyskind *et al.* [14] proposed a lightweight decentralized blockchain data management architecture to protect the personal data and ensures users own and control their data. The proposed method improves the efficiency by using off-chain data storage.

Precisely, the authors implemented a protocol that turns a blockchain into an automated access-control manager that does not require trust in the third party.

Paul *et al.* [15] proposed a new method that improves the energy efficiency in Bitcoin. The authors added some extra bytes in the present header field to utilize the timestamp more effectively.

Blockchain technology platforms can be programmed into two types public and private as depicted in the following Table 1.

- Public (Permissionless) fully public blockchain where anyone can read and write.
- Private (Permissioned) blockchain which allows defining different permissions on different users on the network. There can be different permissions for different operations on the blockchain.
- Blockchain with smart contracts enabled into it such as the capability of building business logic and business process mechanism into the chain. Typical examples are Ethereum or Hyperledger Fabric.
- Blockchain with cryptocurrency transactions. This is only being deployed for transaction capabilities transferring an amount of value from one account to another. Typical examples are Bitcoin or Multi-Chain.

It is apparent from Table 1 that the two Blockchain types (public or private) is very important decision parameter for the smart contract implementations.

Table 1. Network types of blockchain.

	Public Blockchain	Private Blockchain
With Smart Contract	Ethereum	Ethereum/Hyperledger
With Cryptocurrency Transaction	Bitcoin	Multichain

For the public Blockchain, the block validation/mining includes reward mechanisms to incentivize miners to verify and validate transactions. To date, the reward amount is about 0.25 BTC for each transaction. On the other hand, for the private group Blockchain implementations are more focus on permissioning mechanisms that allow for granting participation rights to accountable and identifiable participants while denying them access to others rather incentivize mining mechanisms.

4. Blockchain Layered Approach

The technological components underlying the Blockchain layers include transactions, block, consensus, applications and smart contract. All these components are separated into different layers which are equivalent to the blockchain ecosystem. The key aspects of blockchain can be divided into six layers listed as follows: network, transaction, the blockchain, trust, application and security layers. Each of these layers has different properties and characteristics as shown in the following Figure 1. The network layer refers to P2P network with Ethereum or Hyperledger nodes.

The transaction layer refers to transactions triggered by the users or smart contract. The Blockchain layer has used to refer to the block status containing all the necessary information whereas the trust layer refers to the consensus protocol for the block and transactions validation.

The application layer encompasses applications, state machine, and smart contract. This layer is always separated from the blockchain layer with the smart contract to be the most important component as will be discussed in the following section 6. The security layer is very vital for the Blockchain technology. The blockchain technology is vulnerable to many types of attacks such as eclipse, selfish mining and 51% attack. The 51% attack is the most cited attack on the blockchain.

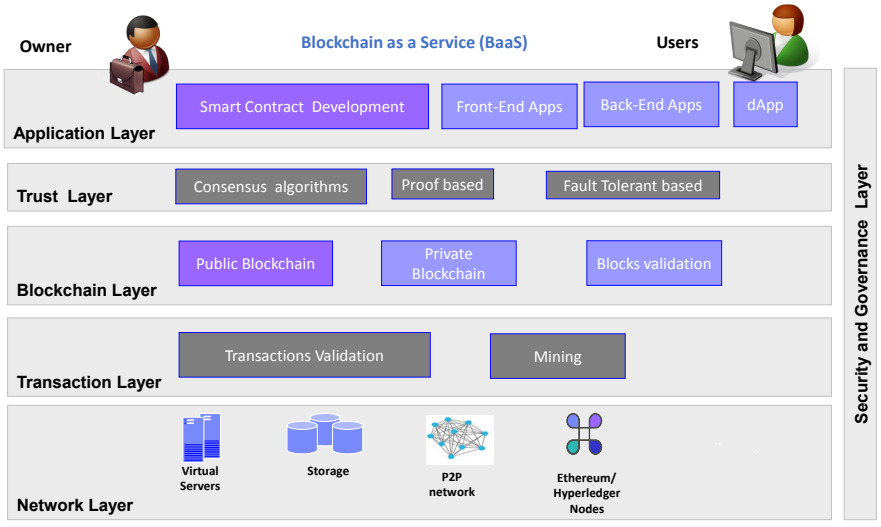

Figure 1. Proposed Illustration of Blockchain layers.

A "51%" attack is still possible for an attacker that controls less than half of the network hash rate. But in this case, the probability of success depends on what percentage of the hash rate the attacker controls and the number of blocks. Only when the attacker controls > 50% of the network hash rate is possible of success 100% [13]. This node then can dominate all other nodes modify the records in the blockchain.

Yli-Humuto *et al.* [16] and Lim *et al.* [17] performed a security analysis that found many security breaches have occurred including DDOS and private account hacking. Atzori [1] found that privacy and confidentiality are still open problems with Blockchain because all the Blockchain nodes are shared with access to all data.

5. Development Phases of Blockchain Applications

For the design and implementation of the Blockchain applications the following phases such as analysis, design, and implementation are presented in the following **Figure 2**.

Figure 2. Development phases for blockchain applications.

In the analysis phase, we collect and analyze the requirements of the blockchain application to be developed. Identify the entities/parties involved, their roles and relationships. The entities can be physical (assets or users) or virtual (such as concepts).

In the design phase, we model the entity attributes as state variables and interactions between them as functions. In addition, we captured the constraints and dependencies.

In the implementation phase, we implement the smart contract for the blockchain applications. The main components of the smart contract are state variables, functions, modifiers, and events in a high-level programming language such as Solidity. In the next sections, we described the smart contract in details. If a user interface friendly is required then the DApp implementation is mandatory as we described in the next section.

Decentralized Applications (DApps)

A Decentralized Application (DApp) is an application that uses smart contracts providing a friendly user interface to smart contracts. A typical example of DApp is a cryptocurrency application that runs on a blockchain network. A Decentralized application structure is composed by a front-end interface (Web Browser, HTML, CSS) and a back-end interface (Web3 JavaScript). As described in **Figure 3**, the DApp application interacts with the Ethereum node (EVM) using JSON RPC. JSON RPC is a stateless and lightweight remote procedure call (RPC) protocol that is used by Ethereum clients to interact with an Ethereum node.

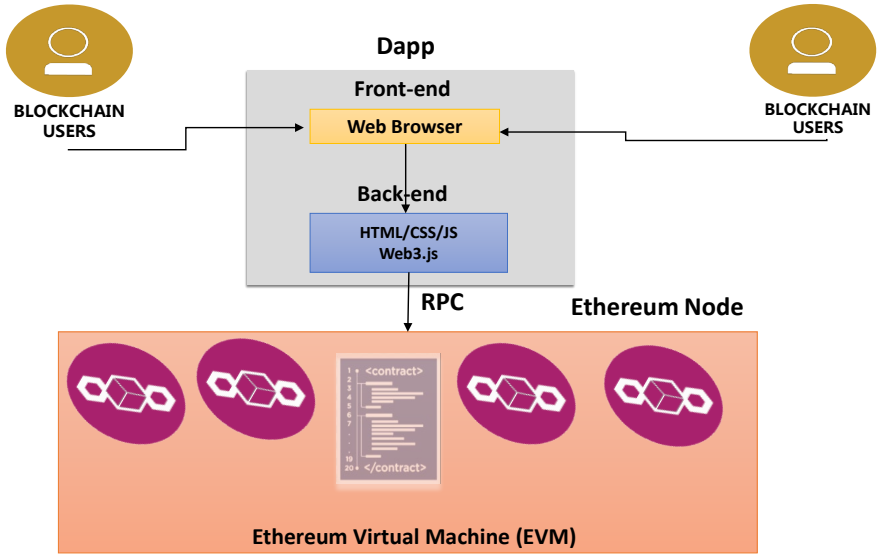

Figure 3. DApp structure.

For the development of the Decentralized application (DApp) the following steps are required:

- Design and implement smart contract in a high-level language (Solidity).
- Compile the contract to generate a binary file.
- Deploy the contract on Ethereum Blockchain network using Ethereum clients (Geth, PyEthApp).
- Build a Web application (Front-end) that interact with the smart contracts.

For this use case, the blockchain technology requires two parts:

- An Ethereum smart contract using Solidity as the programming language which resides on the Ethereum Virtual Machine (EVM) block.
- A Distributed App (DApp) composed by front-end and back-end applications in which interacts with the smart contract and the users (landlord/real estate owner and tenants).

6. Smart Contract Structure

Back to 1997, Nick Szabo [18] has introduced the term "smart contract". A smart contract is a code program identified by an address in the Blockchain network. The main components of the smart contract are a set of executable functions and state variables. Each transaction has input parameters which are required a function in the contract. During the execution of a function, the status of the state variables is changed depending on the logic implementation.

The smart contract code is written in high-level languages such as Solidity and Python for Ethereum applications. The code is compiled into bytecode using compilers as Solidity or Serpent. The contract code will be uploaded into the Blockchain network once the compiler is executed without any errors. Each contract will be assigned a unique address by the Blockchain network.

Any user in the Blockchain network can trigger the functions of sending any

kind of transactions. The contract code is executed on each node member in the Blockchain network as a part of their verification of new blocks.

Smart contracts deployed on a Blockchain network can send messages to other contracts. The message is composed by the address of the sender, the address of recipient, value of transfer, and a data field which contains the input data to the recipient contract. There is a difference between message and transaction, in which transaction is produced by External Owned Account (EOA) while the message is produced by a smart contract as shown in Figure 4.

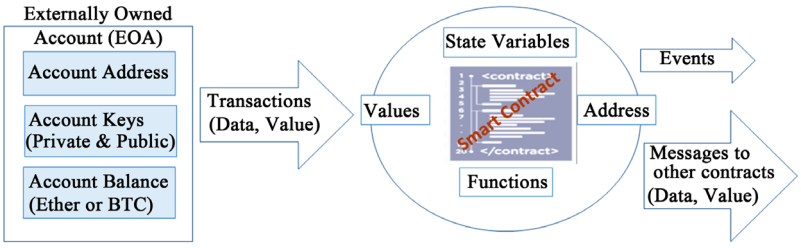

Figure 4. Smart contract structure.

Ethereum is one of the preferred technologies for the development of the smart contracts. The main components for the transactions are based on state machine and functions. It is a Turing-complete contract processing and execution platform based of a Blockchain decentralized shared ledger. The design and the implementation of the Ethereum are totally independently from the cryptocurrency Bitcoin. A high-level programming language called Solidity is used to write smart contracts and decentralized applications (Dapps). The programmer can create their transactions formats, state transitions and events functions, and rules for ownership. The software code is executed on virtual machine referred to as the Ethereum Virtual Machine (EVM) [19].

7. Design Methodology for Smart Contract

The design methodology for the smart contract is composed by the following steps. First, for any users the setup of the Ethereum nodes is required; second, the business services/functions are defined and finally, the processes between the users are described. In the following sections, the above steps are presented in details.

7.1. Ethereum Node Setup

The components of the Ethereum node are actors, roles, business services and processes as described in the following Figure 5.

7.1.1. Actors and Roles

For the definition of smart contract, we need to design the application template which is one-to-many users. The actors for the smart contract are as follows:

- The Contract Owner usually is landlord or real estate owner who is responsible for the development of the smart contract and external owned account (EOA).

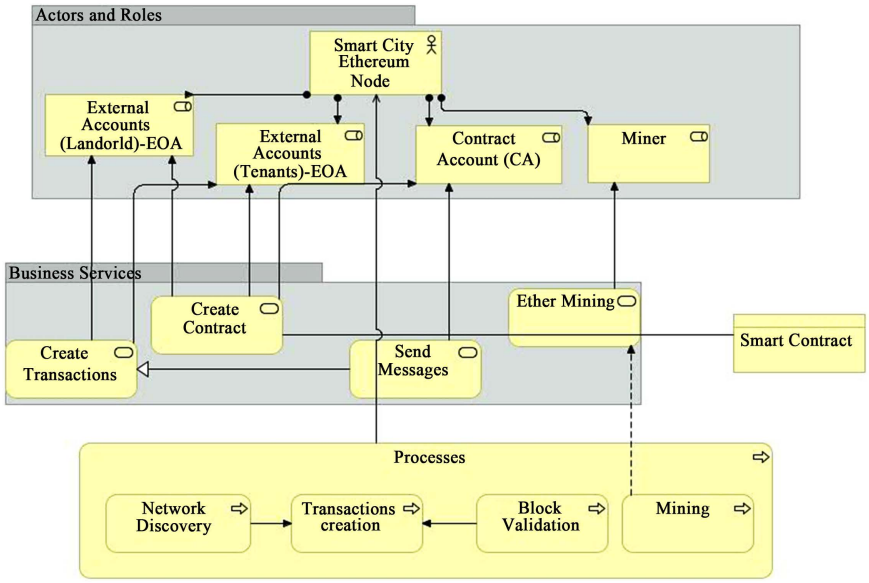

Figure 5. Proposed rental system-use case components.

- Users/Tenants who are responsible for the creation of their Ethereum Wallets in order to have access in the public/private blockchain P2P nodes.

7.1.2. Business Services-Functions

The business services and functions that required for the smart contract are the following:

- Create transaction;
- Create smart contracts;
- Send messages;
- Mine Ether or BTC.

7.1.3. Ethereum Processes

For the Ethereum platform, we have four processes which are:

- Block Validation: This process is for validating block.
- Network Discovery: This process is necessary for a new node to join the P2P Blockchain network.
- Transaction Creation: It allows users to create transactions and allows smart contracts to create events and messages.
- Mining: This process describes the mining process and broadcasting a new block to the network.

8. Use case: Smart Contract for Real Estate

For this use case, the Ethereum Blockchain platform is selected. The real estate acts as landlord for the properties which requires renting a number of residential and business properties using blockchain technology as shown in **Table 2**.

In the next sections, we described the phases for the smart contract development in which consist of analysis, design, and implementation phases.

Table 2. Real estate use case.

Type of Blockchain	Private Blockchain Network
Services offering	Renting Residential/Business Properties

8.1. Analysis Phase

During the analysis phase, a collection of requirements from different personas into the organization are required. Then a set of workshops are developed to understand how the blockchain technology and smart contracts can provide benefits in the organization and identify the actors, roles, and responsibilities.

Actors/Roles

Externally Owned Accounts (EOA): The Landlord and Tenants as considered as external owned accounts. These accounts are controlled by private keys. This actor can create transactions to transfer value, create smart-contracts or call contract functions.

Contract Accounts (CA): These accounts are controlled by their own code. Every time it receives a message, its code executes, allowing it to read and write to internal storage and send messages to other contracts or create contracts in return.

Miners: They validate the transactions and blocks. The transactions are wrapped into a block and a proof-of-work will be provided for this block. After validating the transaction into the block, an amount is provided to miners as a reward. For the specific use case, we have selected private Blockchain then the mining is not required since the parties are already known and trusted.

8.2. Design Phase

After identifying the entities and set up the accounts, the design of the smart contract will be developed. The main components of the smart contract as we had described in the previous Section 6 are functions, processes, state variables, events, and transactions.

8.2.1. Real Estate Smart Contract Functions

The smart contract is between a landlord/real estate owner and tenants. The purpose of the contract is to make sure that the rental agreement is signed, the rental amount is paid on time, and the termination of the contract is executed correctly. The following describes the smart contract functions:

Functions-Created: The Landlord initiates the contract by setting up the rental terms and the details of landlord and tenants. After that, the state of the contract is set to "CREATED".

Functions-Started: Tenant signs the contract and rent begins and the state of the tenant is set to "STARTED" when the state is "STARTED", the rental agreement cannot be confirmed again, thus eliminating the possibility of overwriting the current tenant.

Functions-Rent Collection: The smart contract collects rent from the tenants and sends it to the landlord. This is a powerful feature of this contract to makes it "SMART".

Functions-Terminated: When the Landlord terminates the contract, the state set to "TERMINATED" and all balance deposit is sent to the tenant after checking the status of the property.

8.2.2. Real Estate Smart Contract Processes

For this use case, the process is one-to-many parties and the definition of the processes is described as follows:

1) Rent Contract Signature Process

In this process, as shown in Figure 6, both parties sign the smart contract (rental agreement) which include in details the rental value, payment frequency, and landlord and tenant's details.

2) Rental Payments Process

This process is based on terms and conditions of the rental agreement. The smart contract initiates the lease payments from the tenants to landlord and FM contractors using different mode of payments as depicted in Figure 7.

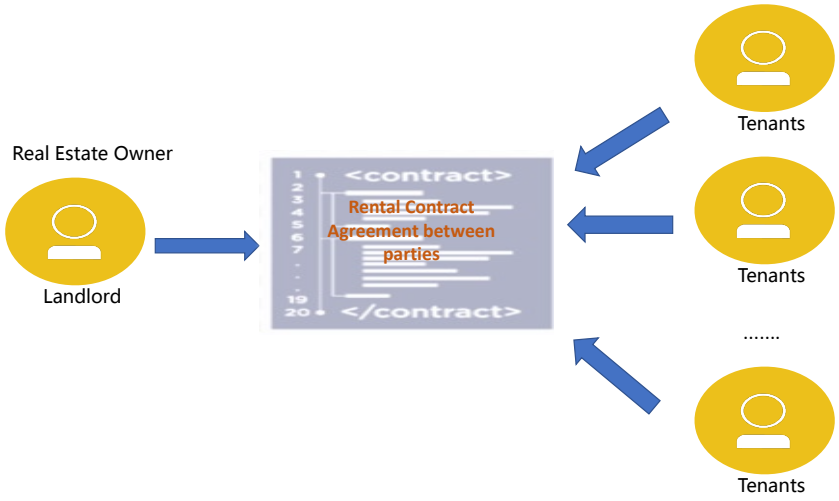

Figure 6. Process rent contract "signature".

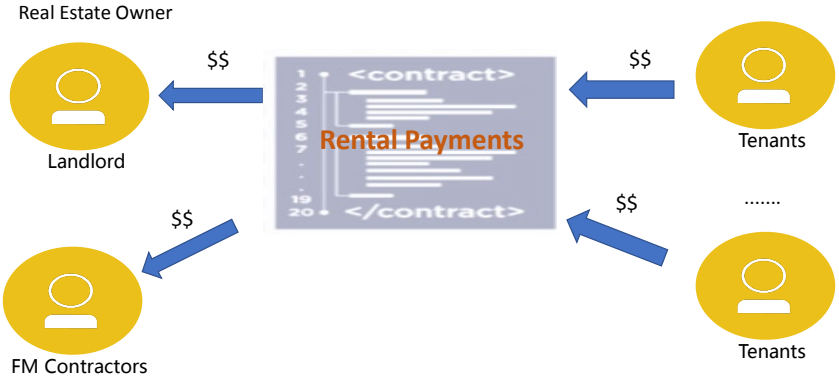

Figure 7. Process rent contract "payments".

3) Termination Rent Contract Process

This process is on the termination rental as shown in Figure 8. The smart contract triggers the payment of security deposit back to tenants after checking and adjusting any damage repair charges.

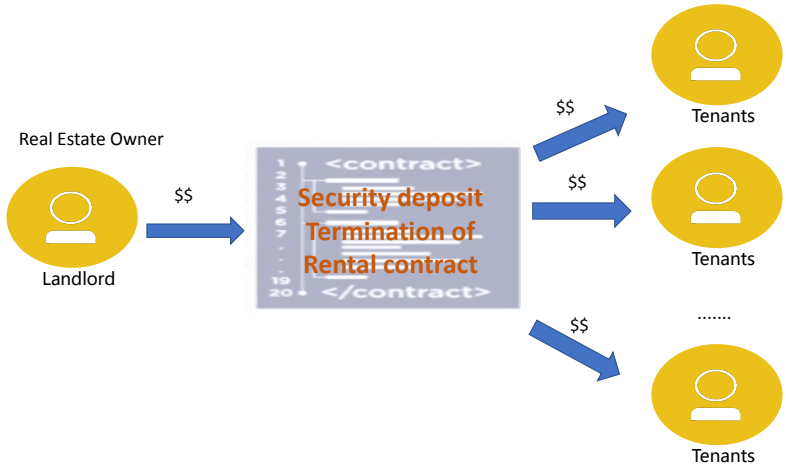

Figure 8. Process rent contract "termination".

8.3. Implementation Phase

In the implementation phase, the code programming for the smart contract is started using Solidity. Functions and processes are defined in the design phase and translated into code program. The content of the smart contract is shown in the following Figure 9.

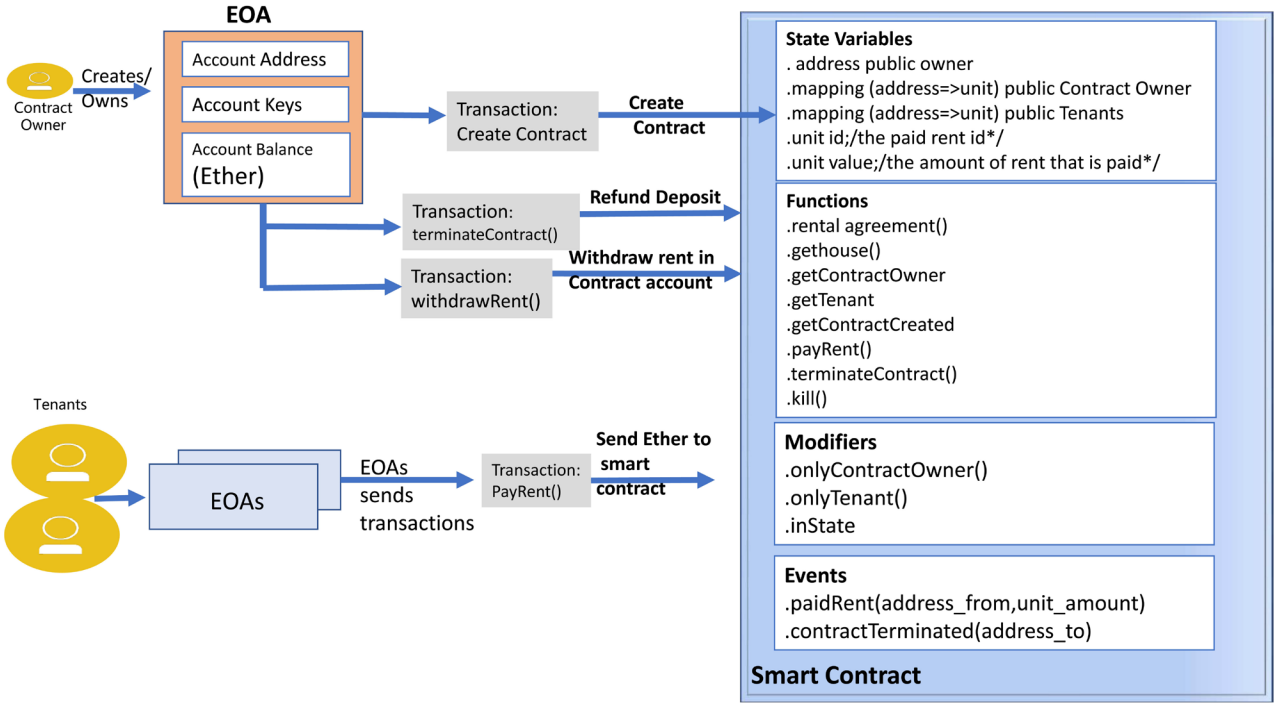

Figure 9. Implementation of the real estate smart contract.

9. Conclusion & Future Work

This paper has presented an overview of the Blockchain technology as a disruptive technology for real estate industry. This study was designed to determine the effect of smart contract with the various components for the implementation. Real Estate development should assess whether and when Blockchain can be used as a technology in their organization. For the adoption of Blockchain into the organization, it is important to meet certain requirements in order to improve the efficiency of the current processes. Perhaps Blockchain technology did not cover the whole process in their organization, however, the cost/benefits analysis should be prepared once the smart cities owner identifies a process that is ready for Blockchain technology.

The benefits of using smart contract and blockchain technology for real estate are as follows:

- **Different parties can modify database:** In the real estate ecosystem, multiple parties such as owners, tenants, and financial management (FM) operators involve the management of real estate properties. They have access to modify a variety of information with the Blockchain. This eliminates the modification between the parties.
- **Trustless among entities and parties**: During the real estate development, different entities might not have any business relationships previously. Thus, this might increase the lack of trust.
- **Advantage of Disintermediation**: With the Blockchain, trusted intermediators such as notary and brokers are not required since the transactions can be independently verified and automatically validated.
- **Transactions advantage**: In real estate companies, different transactions related to different parties (such as landlords, tenants and FM services) are part of the same database. The real estate companies face difficulties to separate the number of invoices. With the Blockchain technology, we can separate transactions between the parties seeking to improve the efficiency of the invoicing process. As an example, in the net rent lease structure, the tenant pays the facility services (such as cooling and maintenance services) directly to the FM companies and the base rent amount directly to the landlord.

A state finite function and process work is presented in details. Future work needs to assess the impact of the different platform such as Hyperledger Fabric for the specific use case presented in this paper.

References

[1] Nakamoto, S. (2018) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[2] Deloitte. (2016) What Is Blockchain? https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-what-is-blockchain-2016.pdf

[3] Zhao, J.L., Fan, S. and Yan, J. (2016) Overview of Business Innovations and Research Opportunities in Blockchain and Introduction to the Special Issue. *Financial*

Innovation, **2**, 28. https://doi.org/10.1186/s40854-016-0049-2

[4] Deloitte. (2017) A New Game Changer for the Media Industry? https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-media-telecommunications/deloitte-PoV-blockchain-media.pdf

[5] Tschorsch, F. and Scheuermann, B. (2016) Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Communication Survey Tutorial*, **18**, 2084-2123. https://doi.org/10.1109/COMST.2016.2535718

[6] Glaser, F. (2017) Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain Enabledsystem and Use Case Analysis. 50*th Hawaii International Conference on System Sciences* (*HICSS* 2017), Waikoloa, Hawaii, USA, 1-14.

[7] Walsh, C., Reilly, P.O., Gleasure, R., Feller, J., Li, S. and Cristoforo, J. (2016) New Kind on the Block: A Strategic Archetypes Approach to Understanding the Blockchain. 37*th International Conference on Information Systems*, Dublin, 1-12.

[8] Beck, R., Stenum Czepluch, J., Lollike, N. and Malone, S. (2016) Blockchain the Gateway to Trust-Free Cryptographic Transactions. 24*th European Conference on Information Systems*, Istanbul, Turkey, 1-14.

[9] Christidis, K. and Devetsikiotis, M. (2016) Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, **4**, 2292-2303. https://doi.org/10.1109/ACCESS.2016.2566339

[10] Puschmann, T. and Alt, R. (2016) Sharing Economy. *Business & Information Systems Engineering*, **58**, 93-99. https://doi.org/10.1007/s12599-015-0420-2

[11] Glaser, F. and Bezzenberger, L. (2015) Beyond Cryptocurrencies—A Taxonomy of Decentralized Consensus Systems. 23*rd European Conference on Information Systems*, Munster, 1-18.

[12] Glaser, F., Zimmermann, K., Haferkorn, M., Webe, M.C. and Siering, M. (2014) Bitcoin—Asset or Currency? Revealing Users' Hidden Intentions. 22*th European Conference on Information Systems*, Tel Aviv, 9-11 June 2014, 1-14.

[13] Atzori, M. (2015) Blockchain Technology and Decentralized Governance: Is the State Still Necessary? https://doi.org/10.2139/ssrn.2709713

[14] Zyskind, G., Nathan, O. and Pentland, A. (2015) Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE Security and Privacy Workshops, San Jose, 180-184.

[15] Paul, G., Sarkar, P. and Mukherjee, S. (2014) Towards a More Democratic Mining in Bitcoins. In: Prakash, A. and Shyamasundar, R., Eds., *Information Systems Security*, Vol. 8880 of Lecture Notes in Computer Science, Springer International Publishing, Berlin, 185-203.

[16] Yli-Huumo, J., Ko, D., Choi, S., Park, S. and Smolander, K. (2016) Where Is Current Research on Blockchain Technology? A Systematic Review. *PLoS ONE*, **11**, e0163477. https://doi.org/10.1371/journal.pone.0163477

[17] Lim, I.K., Kim, Y.H., Lee, J.G., Lee, J.P., Nam-Gung, H. and Lee, J.K. (2014) The Analysis and Countermeasures on Security Breach of Bitcoin. In: *International Conference on Computational Science and Its Applications*, Springer International Publishing, Berlin, 720-732. https://doi.org/10.1007/978-3-319-09147-1_52

[18] Szabo, N. (1997) Formalizing and Securing Relationships on Public Networks. *First Monday*, **2**, No. 9. http://firstmonday.org/ojs/index.php/fm/article/view/548/469

[19] Buterin, V. (2015) On Public and Private Blockchains. Ethereum Blog, Crypto Renaissance Salon. 7th August 2015.