Computer Systems Science & Engineering
DOI:10.32604/csse.2021.015547
Article

Tech Science Press

Smart Contract: Security and Privacy

Leena S. Alotaibi and Sultan S. Alshamrani[*]

Department of Information Technology, College of Computer and Information Technology, Taif University, P.O. Box 11099, Taif, Saudi Arabia
[*]Corresponding Author: Sultan S. Alshamrani. Email: susamash@tu.edu.sa

Received: 27 November 2020; Accepted: 14 February 2021

Abstract: Smart contracts are simply self-activated contracts between two parties. The idea behind their implementation relies on the concept of blockchain, wherein the details and execution of the contract are turned into code and distributed among users of a network. This process controls counterfeiting and money laundering by its ability to trace who owes whom. It also boosts the general economy. This research paper shows how smart contracts in modern-day systems have changed the approach to money tracing. We present case studies about the uses of smart contracts with high levels of security and privacy. As a building block of smart contracts, a brief description of blockchain is provided in an introduction. Among other cryptography methods and techniques, the usage of hashing and hash functions in blockchain security are also explained. We also explore the real-time applications of blockchain and smart contract techniques in real estate. The main advantage of this research paper is that it discusses a state-of-the-art subject, as most of the articles referenced in this paper are from 2018 and onward.

Keywords: Blockchain; cryptography; smart contract; security

1 Introduction

Smart contracts are self-activated contracts among different parties. The method behind the implementation of smart contracts is the use of blockchain, whereby the details and execution of the contract are turned into code and distributed among the users of a network. This mode of implementation ensures that the clauses of a contract cannot be tampered with, ensuring security and increasing efficiency. Smart contracts are known for increasing work efficiency because they are executed at a specified time without any delay. Money is transferred immediately to the receiving party. Therefore, smart contracts spare the involved parties the hassle of waiting for the money to be transferred and wait time for confirmation of the transfer. Additionally, as smart contracts are recorded and saved as lines of code, no critical data of any type is lost as the code behaves autonomously. If a contract were written on paper and transported from one place to another physically instead, it could not maintain such a level of security or privacy, and could be tampered with [1].

In a logistics department, the implementation of smart contracts ensures that all orders are delivered on time and shipments are completed without any missing or wrong items. However, to fully understand what a smart contract is and to understand its mechanics, one must understand what blockchain is—it is the main technology behind the workings of a smart contract.

The term blockchain is made up of "block," which is the information about a given transaction; and "chain," which is how the data is linked together after it is recalled from devices across the internet. Blockchain data is almost continuously verified over and over across multiple devices with each occurring transaction. The reason behind the high security of the blockchain is the absence of a centralized network of computers. This ensures that the blocks are spread far and wide, making it impossible for hackers to alter the data in the blockchain without becoming exposed and having the faulty data rectified. Fig. 1 gives a brief overview of how blocks are connected. It shows that links in the chain maintain a relation to the previous block to maintain security [2,3].

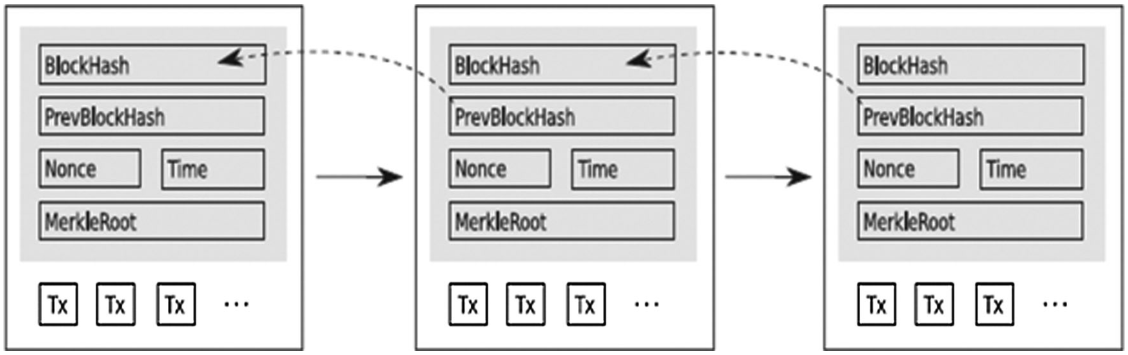

Figure 1: Blockchain block datagram [2]

Moving on to the next step, to understand what a smart contract is, it is worth mentioning that a smart contract also behaves as a smart ledger. A smart ledger is a ledger that is distributed among devices, just as a blockchain is distributed across devices. Besides performing the duties of a regular ledger, where records of all monetary transactions are recorded, they also give third-party financial firms the ability to provide secure services regarding the handling, maintenance, and distribution of the company's ledgers. A smart ledger is also considered proof of all transactions related to a certain company or institution because it belongs to the family of programs that implement the concept of blockchain. This means that the ledger data is also divided into blocks that are distributed across decentralized networks. These blocks are linked together using cryptography [4,5].

Smart contracts require data encryption. They require a highly trustworthy source that will be claimed by all shared parties using public random numbers picked from a larger set, streaming through the checking process, which must be untraceable [1].

In this research paper, we explore what a smart contract is, smart contract mechanics, observations, and notes on how the smart contract in modern-day systems has changed the approach to contracts. Three case studies about the uses of smart contracts with high levels of security and privacy will be presented.

2 Background

Although the concept of smart contracts existed before blockchain technology's testing phase, it was fully implemented after understanding and testing blockchain. Smart contracts were proposed in 1994 and elaborated later, in 1996. American programmer and cryptographer Nick Szabo worked on smart contracting as an idea. Nick introduced the idea that smart contracts could be written and transferred as lines of code. Simply, the details of the contract were to be written as codes and protocols that are self-executed at a time agreed on by the involved parties. However, even though Szabo's concept was appealing, firms and companies could not apply this concept due to insufficient technological advancements: blockchain and smart distributed ledgers still did not exist at that time [6,7].

The concept of blockchain was first introduced later in 2008, by a person or group known as Satoshi Nakamoto [6]. It was introduced to assist with the workings of the online cryptocurrency Bitcoin. Of course, this also paved the way for smart ledgers to be formed and introduced into society; this in turn allowed Szabo's smart contract concept to be put to practical use [6].

In the future, blockchain will not only be used in the financial sector, but also in healthcare, agriculture, voting systems, the Internet of Things (IoT), banks, money transfers, smart contracts, supply chain logistics, and many other important sectors of society.

To explain cryptocurrency and its relationship with the smart contract, we must first understand the workings of cryptocurrency in detail. Cryptocurrency, also known as a consensus mechanism, is defined as a mechanism that tolerates faults and errors. It is used in blockchain and computer systems alike for reaching an agreed-upon data value. Since public, open blockchain works as a decentralized system on a worldwide scale, the information is then shared among all users, who work on creating the next approved proof of work. That enables users to dictate how the next transaction is added to the blockchain. Regarding the blockchain itself, as mentioned above, the blocks are transactions, and the chain describes how the data is linked together [7,8].

How does a blockchain truly operate? What mechanisms are used to form the structure now known as blockchain? First, a single blockchain is made up of nearly 1 MB per block. During its writing, there are a total of 525,000 blocks per blockchain. Now, the question is, what exactly links all the blocks with one another? The answer is a hash. Each block is assigned a digital signature. Each signature is unique and corresponds to its respective block. When creating a hash, each action and transaction is special. A cryptographic hash is a complex formula that takes any input string and turns it into a unique 64-digit output string. Thus, for any change whatsoever to happen to the information stored in a block, a new hash unique to that block must be created (which means a new 64-digit output string). A peculiar fact about the hash function is that for any user's input, the expected output is always the same. If the input is different—even if the change is insignificant—the output becomes entirely new and unique to reflect the new input [9].

As a matter of course, because any small change leads to completely changing a block's unique hash, the next step is to know that these changes are often conveyed as transactions between parties. Now, we should describe how these transactions are done and what sort of significance they hold in the larger scheme of things in the operation of the smart contract. By definition, a transaction is the exchange of money or items of similar monetary value. Thus, a transaction between two parties dealing in cryptocurrency must have a record of such an exchange to avoid the double-spending problem that cryptocurrency was made to solve in the first place. Records of any transactions occurring worldwide are kept in the blockchain. However, a single block can only hold a limited amount of data. This is where the chaining of blocks comes to light: each transaction, with its order of occurrence preserved, is kept in blocks that are not initially linked together. They are linked through the unique hash reserved for each unique block, creating what is called a blockchain.

Since the origin of a blockchain has been clarified, what remains in the enigma of a blockchain is knowing when the unique hash of a block is accepted by a person or group. For starters, proof of work is required from a person who decides how the next transaction is added to the blockchain. But what makes a hash signature eligible in the first place? First, it must begin with a number of zeroes. One might think the zeroes at the beginning could be reduced or that their location could be changed from the very beginning so as to make a signature unique. Unfortunately, they must remain as they are without any changes whatsoever. This is because the metadata for the unique hash must remain constant at all costs. As for the remaining numbers, they are randomly inputted and changed repeatedly until a unique hash signature is found for the corresponding block input data. The continuously changed part is known as the “nonce” belonging to the block [10–12].

At this point, the characteristics required for a signature hash to be unique have been described. Next, we describe what exactly makes the blockchain known for its security and how the data in it remains unchanged. The blockchain has been characterized as unchangeable for very simple reasons: Blockchain data is spread among a large number of people, who are continuously trying to be the next person to find the unique hash signature for each block in the blockchain. If a person tries to tamper with the data inside a block, they will have to find a unique hash signature for it. While searching for an innumerable number of possibilities, more unique hash signatures are simultaneously created. To do that, the person in question would need to have more computational processing power than the rest of the internet combined, which is considered the value of a 51% attack. However, ignoring the difficulty of the action itself, pulling off such a stunt would require far more capital than the amount gained by altering the data in a specific blockchain. Thus, tampering remains an extremely difficult action to execute [1,13].

3 Literature Review

As mentioned previously, transferring smart contract data using blockchain will reduce the processing time of transfer ownership and any banking papers. It will save time because no third parties are involved. Every owner has to register an immutable blockchain ledger that stores connected pieces of information. These ledgers are authenticated to all users. The security method blockchain uses to transfer data and maintain security is the SHA-256 cryptographic algorithm. Any illegal attempt to change data on this ledger requires huge computational power greater than 50% of the internet. Hackers would need to hack more than 51% of users to declare their hacking successful. They would also need to change the information on at least 51% of all computers one by one to attain the new result. This hacking includes changing the list of historical data saved in sequence among those computers. Any traceback will reveal the inconsistencies [14].

Many examples can provide illustrations of smart contract work. For example, the license to evaluate any product is a smart contract. A licensor grants a license to evaluate a product, and the licensee cannot publish the results of their evaluation unless the licensor approves. The licensor can remove any publication within 24 h. The licensor grants permission to the licensee to publish their evaluation, and the license can end if the licensee violates the agreement [15,16].

Fig. 2 shows a state machine that can be used in the procedural code. The process goes through six states from beginning to end. It starts when the licensor obtains a license, then enters the second state in which they request publication approval. They can repeatedly ask until gaining approval, then move to a third state: getting a commission to use or publish commentary. Then, the licensor enters the fourth state, which is to gain a commission to use or publish with no commentary. In the fifth state, no material is removed or commented on. The final stage if acceptance or rejection of the licensor’s publication. In the next section, we describe examples of the state machine at work.

For another example of how a smart contract is executed, say an owner has property to be rented or sold in Riyadh, Saudi Arabia. A potential buyer or renter is looking forward to living in Riyadh. The traditional way to rent or sell real estate is to hire a realtor, who will add fees of their own and cannot guarantee the owner fulfillment of the contract terms. With a smart contract, the process changes to include only the owner and renter as individuals, who will deal through blockchain. The potential renter sends a rent request, which is stored. The owner places the address of the apartment and door access code in storage as well. The owner receives payment confirmation, and the renter receives the property address and license to access it. In the above example, any of the next three situations can happen:

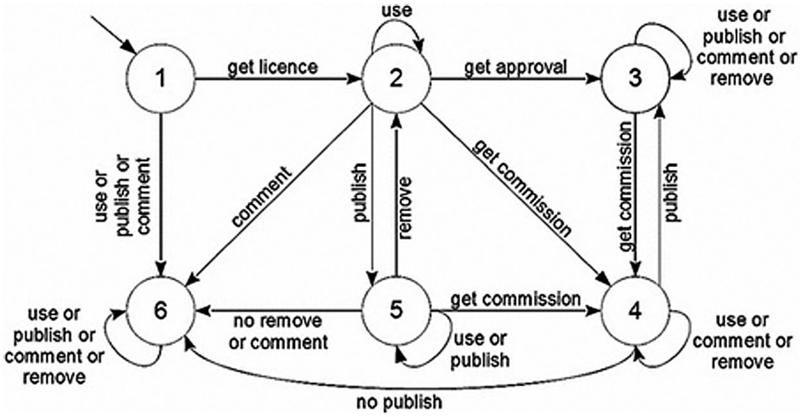

Figure 2: State machine of license [15]

Situation 1: The renter finds everything acceptable. In this case, the owner receives the money agreed upon earlier.

Situation 2: The renter finds everything unacceptable. In this case, the potential renter gets back their deposit.

Situation 3: The renter does not show. In this case, the owner gets compensation from the prospective renter per contract terms. The rest of the advanced payment is refunded to the renter. The contract ends [16].

In this section, we have gone through three cases studies about smart contract.

Case study 1: Managing investment funds in France.

ConsenSys created the Codefi program, which builds business models for real estate agencies; land registry companies; and buying or selling land, houses, or any buildings.

Codefi is used in managing investment funds. In 2019, Mata Capital Company in France decided to invest in distributed funds using blockchain to buy a hotel in Paris that has eleven floors and initially cost about €26m. Mata Capital Company cooperated with ConsenSys Company, the owner of Codefi. Codefi also helps many investors buy and share mutual funds, as they all share their property assets regardless of the investment type (investors may be retail companies or agents). The program implements the blockchain concept. It also allows people with as little as €1 to 10 to become investors. Nowadays, the market shows that investors' funds start at €1000 to 100,000 and above. Investment also creates opportunities for fraud but using the blockchain will eliminate this problem. Using Codefi, Mata Capital Company dealt with ConsenSys in the form of lunch tokens that were secured by blockchain and which consisted of three investment funds worth €350m [17].

Mata Capital Company needed to control who could buy using the "know your customer" principle and the shares of each investor. Gripping and verifying the right customers was the first obstacle that Mata Capital Company faced. Mata Capital Company uses an Ethereum chain-defined whitelist to validate eligibility for purchasing tokens through the platform [17].

The technology used in Ethereum (see Fig. 3) was first invented in 2013, mainly for use with Bitcoin and blockchain for its integrity and authenticity verification. However, Ethereum has gained a bad reputation because it causes delays compared to other technologies. The competition against many new technologies and the dependency shows on Buterin's fame raises rumors [18].

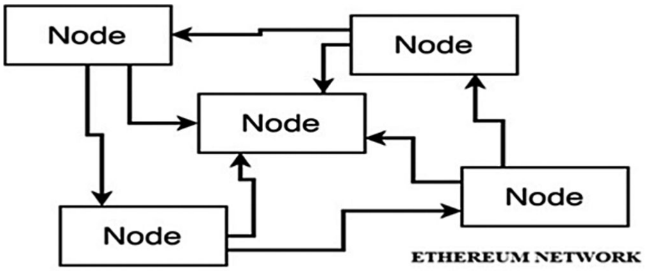

Figure 3: Ethereum network [2]

Tokenizing assets is predicted to be worth more than $2 trillion over the next two years in the real estate sector as companies use smart contracts to transform properties. Tokenizing has proven to be good at managing transaction data and organizing listings of owners and properties. Cushman & Wakefield's estimate increased participation in real estate investment with great liquidity, less risk, less complexity, more efficiency, and greater transparency.

Case study 2: Real estate asset, smart contract tokenization in the UK

Her Majesty's Land Registry cooperates with ConsenSys and Codefi on a project to record the ownership of the 25 million owners in the British system as a step to digitize information and implement smart blockchain contracts. Transferring ownership will be available after registering data. The project handles data worth $8.7 trillion. The project is supposed to increase the speed and transparency of ownership operations. It will also help in addressing the below-mentioned points:

1. Investors register maintenance is a burden and needs a lot of money.
2. High price of the investment ticket, which discourages the investor to invest.
3. Price swings.
4. Existence of various parties and intermediates.
5. Low level of transparency.
6. Many secondary markets increase the cost.

A title token prototype has been invented for shared property. Each token works as a block that represents the ownership of property. The program has eased the working process. The project used the ERC1400 standard and Ethereum technology for the creation and deployment of smart contracts. One privilege the project used was the ability to classify assets by type. ConsenSys' diligence alone audited the smart contract. Using blockchain in the US saves $1.7 billion in expenses annually [19].

Case study 3: Monitoring logistics smart contract

This case is about pharmaceutical utilities logistic activity. The challenge is the intermediate parties. The solution is a smart contract that reduces intermediate vendors. The model deals with multiple agents and smart contracts. Goods transported in logistics systems go through many nodes. The solution shows that blockchain's use of a multi-agent model solves a lot of problems. The agents in this model are:

1. The seller, Pharmacy.
2. The producer, Pharmacy.
3. And the shipping company.

Each block in the blockchain entails transactions between agents and the smart contract see Fig. 4. The multi-agent model can be used with things that someone buys or sells, but not for land registries or money transference (it mainly helps logistics companies) [12].

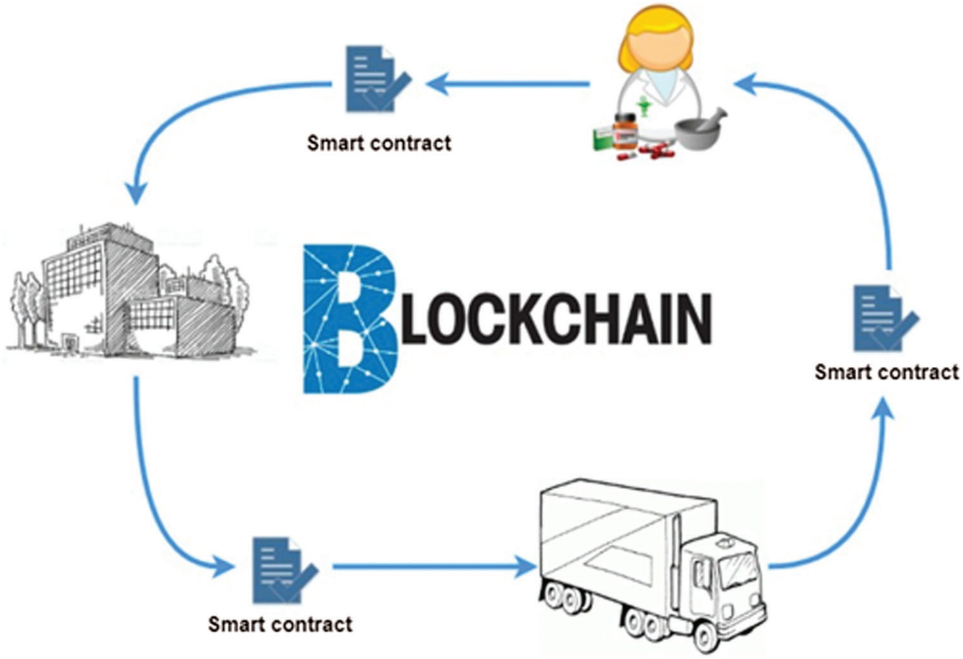

Figure 4: Logistic smart contract in blockchain [12]

4 Discussion

This paper discussed smart contracts via three case studies to show the pros and cons and the models used, broadening the understanding of smart contracts, land registries, and logistics businesses. The models proposed helped ameliorate drawbacks in the abovementioned cases. A comparison table among the above three case studies is shown in Tab. 1 below:

Table 1: Three case studies compared

	Case study 1 Managing investment in France	Case study 2 Real estate asset, smart contract tokenization in the UK	Case study 3 Monitoring logistics smart contract
Implemented in	Hotel market share	Land of Queen Elizabeth	Pharmacy logistics
Used technology	Ethereum technology	Tokenizers and Ethereum technology	Multi-agent model
Problems	Ethereum has a bad reputation	A big change at once	More than two parties at the same time in one operation
Results	Using smart contract helps to increase investment and enhance the economy		

5 Conclusion

Smart contracts must be considered as a new way to transfer ownership that ensures security, privacy, and time savings.

Using blockchain will be a great step toward enhancing security and a great way of doing business. The technology can be used in many fields, and predictions show enhancements in all aspects of the fields involved.

The main advantage of this research paper is that it represents the state of the art. Most of the sources used in this research are from 2018 onward. The case studies show increased profitability and security compared to traditional land registry, share owning, and logistics methods. All are characterized by cryptographic hashing to secure and connect data.

Funding Statements: Taif University Researchers supporting Project number (TURSP-2020/215), Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] P. Mell, J. Kelsey and J. Shock, “Cryptocurrency smart contracts for distributed consensus of public randomness,” in *Int. Sym. on Stabilization, Safety and Security of Distributed Systems*, Cham: Springer, pp. 410–425, 2017.

[2] A. Khanna, A. E. Hassanien, S. Bhattacharyya, I. Pan and D. Gupta, “Int. conf. on innovative computing and communication, *Proc. of ICICC*, cham: Springer, 2, 2019.

[3] P. Eze, T. Eziokwu and C. Okpara, “A triplicate smart contract model using blockchain technology,” *Circulation in Computer Science-Disruptive Computing Cyper-Physical Systems (CPS), and Internet of Everything (IoE)*, vol. 2017, no. 01, pp. 1–10, 2017.

[4] C. Alexopoulos, Y. Charalabidis, A. Androutsopoulou, M. A. Loutsaris and Z. Lachana, “Benefits and obstacles of blockchain applications in E-government,” in *Proc. of the 52nd Hawaii Int. Conf. on System Sciences*, Hawaii, US, 2019.

[5] P. Treleaven, R. G. Brown and D. Yang, “Blockchain technology in finance,” *Computer*, vol. 50, no. 9, pp. 14–17, 2017.

[6] H. Hou, “The application of blockchain technology in E-government in China,” in *Int. Conf. on Computer Communication and Networks (ICCCN)*, Vancouver, BC: IEEE, pp. 1–4, 2017.

[7] 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 Age*, Delft The Netherlands, pp. 1–9, 2018.

[8] B. K. Mohanta, S. S. Panda and D. Jena, “An overview of smart contract and use cases in blockchain technology,” in *Int. Conf. on Computing Communication and Networking Technologies (ICCCNT)*, Bangalore: IEEE, pp. 1–4, 2018.

[9] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, “An overview of blockchain technology architecture, consensus, and future trends,” in *International Congress on Big Data (BigData Congress)*, Honolulu, HI: IEEE, pp. 557–564, 2017.

[10] I. Eyal, “Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities,” *Computer*, vol. 50, no. 9, pp. 38–49, 2017.

[11] S. Underwood, “Blockchain beyond bitcoin,” *Communication of the ACM*, vol. 59, no. 11, pp. 15–17, 2016.

[12] R. Casada-Vara, A. González-Briones, J. Prieto and J. M. Corchado, “Smart contract for monitoring and control of logistics activities: pharmaceutical utilities case study,” in *Int. Conf. on Soft Computing Models in Industrial and Environmental Application*, Cham: Springer, pp. 509–517, 2018.

[13] J. Yli-Huumo, D. Ko, S. Choi, S. Park and K. Smolander, “Where is current research on blockchain technology?—a systematic review,” *PloS One*, vol. 11, no. 10, pp. e0163477, 2016.

[14] F. Idelberger, G. Governatori, R. Riveret and G. Sartor, “Evaluation of logic-based smart contracts for blockchain systems,” in *Int. Symp. on Rules and Rule Markup Languages for the Semantic Web*, cham: Springer, pp. 167–183, 2016.

[15] H. Subramanian, “Security tokens: Architecture, smart contract applications and illustrations using SAFE,” *Managerial Finance*, vol. 46, no. 6, pp. 735–748, 2019.

[16] ConsenSys, Mata Capital, “Blockchain Case Study on Real Estate Investment Management,” Retrieved November 10, 2020, from https://codefi.consensys.net/mata-capital.

[17] ConsenSys, "French Asset Manager Promotes Trust, Transparency and Efficiency for Real Estate Investors by Tokenizing Ownership of a Paris Hotel," Retrieved November 10, 2020, from https://codefi.consensys.net/mata-capital.

[18] Real estate asset tokenization in the UK, HMLR CASE STUDY, Retrieved November 11, 2020, from https://www.upgrad.com/blog/guide-to-ethereum-pros-cons-uses-application.

[19] M. H. Miraz and M. Ali, "Applications of blockchain technology beyond cryptocurrency, 1801(03528), *arXiv preprint arXiv*, 2018.