Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online) DOI: 10.7176/JIEA
Vol.9, No.5, 2019

Smart Contracts Implementation, Applications, Benefits, and Limitations

Silas Nzuva
School of Computing and Information Technology, Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya

Abstract
The world today has realized the vast technological evolution that has greatly shaped the production and management functions of business enterprises. Traditional contracts can take weeks or even months to initiate, and there have been numerous instances of breaches and lack of trust for contracts in both the private and public sector. A smart contract can be defined as a self-executing contract that utilizes blockchain technology to digitally enforce, verify, or facilitate the performance or negotiation of a contract. Owing to the security and decentralized system exhibited by blockchain technology, smart contracts can foster transaction credibility between contracting parties without the necessity of third parties as exhibited in traditional contracts. Any business organization that aims at achieving greater heights in management and production dimensions must consider utilizing robust technologies that are aimed at bolstering its competitive edge. Owing to the newness of smart contracts, characterized by very few studies on the same, this research reviews how smart contracts through blockchain technology can be implemented in an organization to enhance performance and outlines the applications, benefits, and limitations associated with such contracts.
Keywords: Blockchain technology; smart contracts; smart contract applications; smart contract benefits; smart contract implementation; cryptography; cryptocurrency
DOI: 10.7176/JIEA/9-5-07
Publication date:September 30th 2019

1. Introduction

The emergence of advanced technologies has led to increased competition between business as each tries to utilize the latter to bolster the employees' productivity and the general performance of the firm [7]. As a result, technology has become a critical backbone of organizational operations and a core driver of organizations' innovations and competitiveness. According to Iansiti et al., business enterprises have shifted from the traditional ways of business and have consequently adopted modern, more reliable and cost-efficient mechanism; smart contracts are some of these mechanisms [20].

Any financial transaction that is carried out by an organization with third parties can be viewed as a form of a contract, however simple, or complex the transaction is. Essentially, financial openness and transparency are some of the core aspects of successful organization management as they create an environment that is conducive not only for investment but also for the establishment of trust with different organization stakeholders [7]. The blockchain technology is a common buzzword today, perhaps due to the unique technology that it is based on. A blockchain is a chain of transaction records, usually referred to as blocks, that grows autonomously, and all the records are linked together to form a chain, and secured through cryptographic techniques. [36] A block may contain one or more records, and each block holds the hash function of the preceding block, the transaction data, and timestamp [36]. Once the block is completed and committed, it is chronologically added to the blockchain and cannot be modified.

These characteristics of the blockchain technology make it highly useful as it is secure, reliable, and the ability to monitor the digital transaction is warranted [24]. The blockchain technology has vastly been used in cryptocurrencies such as Bitcoin and Etherium. Cryptocurrency can be viewed as a virtual or digital currency that entails the use of cryptography to promote the security of the financial transaction. As such, a cryptocurrency can be used as a secure medium of exchange as it utilizes high cryptography to ensure verifiability of asset transfer, control of unit creation and evades regulations that may otherwise be imposed by bodies such as government institutions [20].

A smart contract can be defined as a self-executing contract that utilizes blockchain technology to digitally enforce, verify, or facilitate the performance or negotiation of a contract [8]. Owing to the security and decentralized system exhibited by blockchain technology, smart contracts can foster transaction credibility between contracting parties without the necessity of third parties as exhibited in normal contracts.

Organization performance is greatly determined by the strategies employed by the management in streamlining organizational processes, operations, and bolstering the employees' productivity. Being a new technology, smart contracts through blockchain technologies bear the ability to positively or negatively impact the performance of a firm; hence, such a study is critical. Any business organization that aims at achieving greater heights in management and production dimensions must consider utilizing robust technologies that are

aimed at bolstering its competitive edge. Owing to the newness of smart contracts, characterized by very few studies on the same, this research at out setting the benefits of smart contracts and how they can successfully be implemented organizational setting.

2. Blockchain Technology Use in Smart Contracts

2.1. Past Studies

The technological revolution has seen the emergence of new systems and technologies that are more efficient and reliable [36]. Likewise, smart contract technology is made to replace the traditional forms of contracts to promote transactional safety, efficiency, and reduce possible contract beaches. Kosba et al. argues that the smart contracts systems, which are based on blockchain technology have emerged as a result of the efficiency, reliability, and security that has been noted in the decentralized cryptocurrencies such as, Litecoin, Etherium, and Bitcoins among others, which the authors pinpoint that they may be the future of online financial transactions. Essentially, smart contracts are built on a new blockchain that is characterized by distributed consensus, assuming the existence of no conflicting computation resources [24].

Luu et al. examined the security of transactions in smart contracts by investigating the smart agreements that run on the Etherium blockchain technology [26]. According to the authors, the Etherium smart contract system has presently seen increased adoption and holds virtual coins tuning to millions of dollars [26]. It is worth noting that the majority of the smart contract systems today are often run in synchrony with the respective cryptocurrencies; as at present, Bitcoin and Etherium have established smart contracts systems that run under their underlying blockchain technology. To examine the security of the smart contracts, the researchers introduced various bugs that were made to manipulate the Etherium smart contacts blockchain for financial benefits [26]. Apparently, it was unveiled that though the system is significantly secure, there exist various gaps with respect to the distributed semantics of the blockchain technology under which the system runs. The authors denoted the need for the enhancement of the Etherium operational semantics to tighten the security of the system [26]. The researchers further unveiled the existence of the DAO bug, which makes blockchains vulnerable to DAO exploits; Etherium cryptocurrency lost more than $60 million in 2016 as a result of this vulnerability [26]. The security of smart contacts has as well been discussed by Peters and Panayi, who insist that precautions must be taken in rolling out the smart contract system to ensure that the system is not prone to vulnerabilities that otherwise mess up the digital assets [31].

On a different point of view, Peters and Panayi suggest that the emergence of blockchain technology may disrupt the banking industry in the new future by facilitating digital assets, automated banking ledgers, smart contracts and global money remittance [31]. This implies that it is high time for business organizations and financial institutions to start considering cryptocurrencies as a mode of payment, and smart contacts and a possible replacement of the traditional business contracts [38]. Business organizations that do not adjust to the prevailing technologies are more often than not caught unaware, and the technology becomes disruptive to their business processes and operations. Nevertheless, in the banking context, Peters, and Panayi explain that the blockchain-based technologies must be extremely smart to evade vulnerabilities that otherwise can be used by malicious attackers to propagate fraud or swindle the blockchain participants their virtual money [31]. Attacks on blockchain systems may be hard to detect and control, and hence sufficient security measures must be put in place before rolling them in the banking context

Omohundro takes a machine learning perspective with respect to smart contracts. The authors argue that the blockchain technology, smart contacts, and cryptocurrencies have resulted in new opportunities for the application of machine learning and artificial intelligence [AI] in general [30]. Zhang et al. argue that the smart contacts can be made smarter, by enhancing their ability to interpreted real-world knowledge and make more reasonable, logical, and sound decisions in online commerce [38]. By integrating AI into smart contracts and cryptocurrencies, it is possible to ensure that the blockchain follows specific safety and measures to promote the safety and reliability of the transactions [2].

A study by Christidis and Devetsikiotis on the internet of things and the emergence of smart contracts showed that a combination of internet of things and blockchain technology, which is the core framework of smart contracts, is an efficient and powerful technique that can trigger wide-scale transformation on how financial transactions are carried out or how a firm interacts with its business partners across different industries [8]. As such, the authors argue that smart contracts, internet of things, and the blockchain technology use can pave the way for new distributed applications and novel business models and processes [8]. This is because the blockchain technology allows the establishment of a distributed peer to peer network that allows for verifiable interaction between the participants without the necessity of a trusted partner. Christidis and Devetsikiotis further denote that the blockchain technologies upon which the smart contracts are built, allow for cryptographic automation of workflows and processes that are time-consuming [8].

There exists a wide array of smart contracts, depending on the type and purpose of the contract. However, though smart contracts are programmed to self-execute, some usually depends on the information that they gain

from the external sources, such as financial instruments transactions [13]. As such, having authentic data feeds into the system is very critical in enhancing the security, performance, and authenticity of the transactions. Zhang et al. developed and rolled out a Town Tier [TC] system that is made to categorically act as a bridge between the blockchain and the information sources [mostly websites] to authenticate the information that is fed to the system. The main purpose of TC is to promote confidentiality, reliability, and integrity of smart contracts [18]. Essentially, though smart contracts seem to have a bright future across all the industries, their security threshold seems questionable because a mentioned, some contacts rely on data that is external from the blockchain and the reliability, and trustworthiness of such data cannot always be guaranteed, owing to the fact that the chain holds millions of transactions [39].

2.2. How Blockchains Work

Essentially, a blockchain can be perceived as a data structure that is shared and replicated across machines on the network. According to Böhme et al., this technology was first introduced by Bitcoin, one of the leading cryptocurrencies across the globe [4]. Hillbom and Tillström explain that the introduction of the blockchain technology has aided business organization in transitioning from the traditional forms of contracts and the adopting smarter and more robust contracts that do not require the intervention by any party [18]. The use of the blockchain technology in cryptocurrencies and smart contracts aids in keeping a powerful decentralized ledger transaction that defines who owns what in the network. [8].

It is, however, critical to understanding that blockchain is a technology by itself and hence does not require cryptocurrencies for it to function. The blockchain technology can be adopted in a wide array of operations and transactions that can be carried out in a decentralized manner. A blockchain can be perceived as batched and timestamped blocks of records whereby each of the blocks contains the hash reference of the previous block. Such an aspect results in a chain of blocks. The machines in the network and which have access to the formed chains of blocks can decipher the message and interpret the state and message being sent across the network [17].

Ona different point of view, it is also critical to examine how the blockchain network operates to gain a comprehensive understanding of smart contracts implementation through blockchain technology. A blockchain network can be perceived a group of nodes/computers/ machines that have access to a given chain of blocks, and which can perform operations on the blocks, based on the information that each of the machines or node holds. For instance, a given node in the blockchain network can act as the main entrance of various users of the blockchain into the network; it is also worth noting that the users are as well able to transact on the network through their specific nodes. The end result of the blockchain is a sophisticated peer to peer network that is quite secure.

Kocarev et al. explain that in interacting with the blockchains, the users usually use a set of public and private keys [22]. Analytically, the public and private keys are cryptographic approaches that are used to warrant safe transactions through encapsulation of the data being transmitted. As such, unless a user has the key, they are unable to decipher the message being transmitted. The use of the private keys by the users in the blockchain network is made for the purpose of signing their own transactions; the public key, on the other hand, is used to address the users. As denoted by Kocarev et al., the use of the asymmetric cryptography through the public and private keys promotes non-repudiation, integrity, and authentication [22]. The users broadcast the signed transactions to the one-hop peers in the network.

- The one-hop peers in the network are typically neighboring peers. These nodes are credited with the responsibility of first validating the transactions before broadcasting them further to other peers in the network. If the transaction is deemed invalid, then it is discarded. This process continues until the transaction is spread throughout the entire blockchain network. It is essential to note that the validation process by every one-hop node in the network makes it literary impossible for invalid transactions to be broadcasted. This then reaffirms the issues of security and authenticity of the transactions.
- The validated transactions by the nodes in the network within a given time are then collected, batched, and timestamped as a candidate block. The process of collection, validation, and timestamping is usually referred to as mining. The node that performs this function then re-broadcasts the block again, back to the chain network for further action. It is, however, important to note that a consensus is often reached in selecting the mining node as well as the constituents of the block.
- The network nodes are again tasked with the responsibility of re-verifying the authenticity of the re-broadcasted block, by checking whether all the transactions held by the block are valid and whether the reference values for the previous block are accurate. The block is discarded if either of the set conditions is violated. Else, it is added to the chain of blocks, and the information it contains is updated on each of the nodes, to ensure commonality of the information broadcasted as well as an up-to-date view of the block status. It is, however, vital to note that this process occurs for every transaction to ensure security is maintained.

The success of an organization is greatly depended on a wide array of factors. Fairfield explains that the ability of the organizational leaders to adopt reliable, yet secure and efficient technologies is very critical [14]. In line with this, Delmolino et al. explain that today, the competitiveness of an organization is a multifaceted construct that must be addressed through the implementation of various strategies [11]. Technology has become a critical measure of organizational effectiveness, efficiency, and performance; any organization that does not match with the emerging trends, therefore risks being phased out by the competitor firms. On the same note, Fairfield explains that an organization should focus on technologies whose implementation will aid in smoothening organizational processes, will enhance the organizational relations with partner organizations and will eliminate inefficiencies that result from a lapse in operations management and process automation [14].
As earlier defined, a smart contract is simply a self-executing script, based on the set conditions. As such, the dimensions and applications of the smart contract in organizational settings are many. Typically, smart contracts can be implemented in various areas, ranging from contracts with the suppliers to contracts with the retailers, resellers, and the end customers. The fact that the latter is self-executing brings in the issues of integrity and openness. In an organizational setting, the technology bears the ability to positively improve the financial openness of a firm, by promoting safety, security, accuracy, and integrity of the organizational financial transactions

2.3. Validity in Smart Contracts Execution

On a different point of view, it is important to look at what entails validity of transaction in smart contracts. To better understand the issue of validity, it is vital to think of the blockchain network as a group of non-trusting computers or machines, that perform read or write on a common database. Therefore, since the machines are non-trusting, they must ensure close monitoring of one another for any transaction that is being made to the general ledger [the database] for safety purpose. To prevent possible conflicts between these machines, a set of conditions or rules must be set. To begin with, the bock chain network must ensure that the distributed environment is protected. This is achieved by helping the different users in the network to reach a common consensus on the status of the transactions. This is attained by ensuring that every transaction must conform to specific rules before being committed to the shared database.

The rules and conditions for the execution of the transactions are embedded in each of the blockchain network clients. Therefore, each client machine in the network understands what is expected of the transaction that they are executing and the peer nodes also do understand what to expect from transactions of other machines in the network. Therefore, whenever a client performs a transaction since the transactions are replicated across all the machines in the blockchain network, every client checks whether the transaction conforms to the pre-programmed rules, before being relayed further across the network [18].

To better understand this concept of the validity of reactions and which forms the core of smart contracts and associated security measures, it is prudent first to understand how also the shared database works in blockchain technology. A database usually made of tables. Each table contains a set of rows. Essentially, a row can be perceived as a single record, and the transaction is any action that seeks to create or manipulate one or more of the records. However, in the blockchain environment that is characterized by a shared database model, each of the records/rows can be mapped to a specific private and public keys. The private key is usually held by the owner of the record/transaction, while the public keys are held by other machines in the network. The public keys aids in controlling the editing of each of the record, as before the transaction is committed, all the machines in the network must be in consensus.

The following of the defined rules by each of the nodes in the network results in authenticated and timestamped blockchain that defines the network activity of the nodes [4]. Owing to the defined rules in each of the nodes, the users do not have to trust each other as their activity is already predefined by the set conditions. This gives rise to the concept of trustless environment, whereby trust emerges as an inherent property of the pre-set conditions embedded on the nodes with respect to the specific blocks within the network as well as the resultant interaction of the nodes [14].

3. Implementation of Smart Contracts

3.1. Digital Asset Transfer

Smart contracts can be as well adapted in digital assets transfer. This is highly applicable to the organization's dealings with customers and suppliers, especially where there is an exchange of money. Smart contracts can be used to transform the traditional asset transfer to digital transfer. For instance, in an organization that deals with customer credit cards, such as banks, the amount spends and account balances in the credit cards, the organization would have an aggregate database dedicated for the task. Such a database would have a typical table that would have attributes such as "amount," "owner," and “asset type” among others [14]. In the database, the table may have entries such as “Sam," “20”. On a different note, another record maybe “Tim," "0". Interpretation of the first record would indicate that Sam has a credit balance of $20, while Tim has a credit

balance of "$0. A transaction may be initiated by Sam to transfer the specified amount to Tim. Suppose Sam transfers $10 to Tim, Sam's account is debited $10, while Tim's account is credited with $10. After the transaction is committed, Sam would have $10, while Tim becomes $10. This is an example of digital asset transfer since cash is considered to be an asset that can be expressed in digital form. Logically, though the end-users receive the updated account balance instantly, what happens is the manipulation of the stored records in the database.

Multinational organizations usually interact with thousands of customers on a daily basis. While some customers are physically served, others are served by automated systems, such as online carts that are synced with check out systems. Essentially, the sale or purchase of a commodity by an organization results in a specific form of contract, which may or may not be enforceable under certain circumstances. Cong explains that a business organization owes the customers and general stakeholders a duty of care, and therefore must ensure that activities are carried out with reasonable care to ensure that both the interests of the customers and those of other stakeholders are protected [18].

Each sale or purchase by the organization can, therefore, be treated as a contract. In the case of a business organization, the purchase of any service package by the customer or the purchase of the products by the organization can , as a contract. Such contracts can be digitalized and executed as digital tokenized assets. Pettersson and Edström explain that a digital tokenized asset is the expression of any given form of asset in an electronic manner, making it possible to transfer one or more units of the assets to a different party [32]. Digital transfer of assets between the organization and its partners can be simplified just as in the example of Sam and Tim bank transfers and be expressed easily through blockchain technology, that warrants cryptographic verifiability, validity, and security through the use of the decentralized transactional model.

In implementing smart contracts through blockchain technology, a business organization can approach the latter through a trustless environment approach. This would require the implementation of a shared database, whereby each row of the respective table in the database would represent the details of a specific entity, who may be a supplier or a customer. However, rather than having the "owner' in the case of the banking example given, the attribute would contain the public key of the node /user allowed to change the record.

3.2. A Scenario for Purchasing a Service Package

A shared database would exist between the company and all other parties in the blockchain network, typically all the customers. Suppose Customer Y has five units of X [X may represent credit card balance], the respective record in the database would contain Customer Y's Public key in the "owner" column of the respective table, as well as values 5 and X in the quantity and asset type respectively. Assuming Customer Y knows the public key of Company B, then he/she should be able to transfer a certain unit of the digital asset to Company B. In this case, Customer Y would need to initiate a signed transaction using her private key that would reduce the specific asset type by the specified units in the amount. Using the public key of B, Customer Y is then able to credit Company B's amount column with the specific units of the assets reduced.

However, unlike in the relational and object-oriented database systems whereby the manipulation is done directly to the records, the blockchain technology entails the use of transaction blocks, whereby the transactions are linked to another. Therefore, after customer Y purchases new package and transfers the digital asset [money] to Company B, a new record/ row is created with the updated information and a timestamp, while the old row/ record is deleted. According to Greenspan, in smart contracts through the use of blockchain technology, rows are not modified; rather, old records are deleted, and new records with updated information created [17]. The asset balance of both the Company B and the Customer Y can then be calculated through the aggregation of the database record that corresponds to their respective public keys and whose asset type matches the digital asset that as transferred.

Table 1. Setting up smart contracts with partners by organizations.

Phase	Description
Agreement Identification	This step entails the identification of cooperative opportunities and specific outcomes by multiple parties. The parties may entail Company B and its business partners The scope of the agreement is defined; it may include but not limited to transfers, the right of use, asset swaps, and business processes, among others.
Setting conditions	The conditions act as the guiding principles for the contract execution. The smart contract is triggered by the party to the contracts or anything else defined in the contractual terms that act as a trigger event. Triggers may be a specific date, GPS location, a natural disaster occurrence, and specific financial market indices. Again, temporary conditions such as religious events, birthdays, and holidays can as well be used to trigger smart contracts. For instance, in the case of Company B, a promotion of smart contract to Customer X can be initiated if the customers' birthday is near, with the contract purporting to offer a more exclusive deal
Business Logic	As already explained, smart contracts through blockchain technology are scripted pieces of code that have been developed to and organized in a manner that triggers execution upon the happening of the trigger event or activity. In this step, a code is written with the pre-set conditions; more often than not, the conditional statement such as if, then, else is used to ensure logical and automated execution of activities
Blockchain technology and Encryption	Encryption is a critical part of the blockchain technology. Encryption using cryptographic techniques is done to warrant the security of the transactions and also ensure that verification and authentication of the communication and messages being sent across the network. The program development and encryption, however, must conform to the underlying blockchain model that the smart parties' intent to use. For instance, if the parties plan to use the Etherium blockchain architecture, then the code must be written in Etherium based blockchain programming language
Execution and processing	This entails the commitment of the initial contract transaction and subsequent transaction. Upon verification of the set conditions by each of the participating nodes in the blockchain network, the nodes reach a consensus on the validity, verification, and authenticity; the new smart contract is then written to the current block. Afterward, the code is executed, and outcomes are updated on each of the nodes in the network. These new written instructions act as the base for verification and controlling transaction processing to ensure validity.
Updating the Network	After the execution of the contract. Each of the nodes is updated on the new state. Essentially, once a transaction or a new record and subsequently executed, no alteration can be done; the only thing that can be done is appending and creating a new record. This is one of the disadvantages mentioned earlier on.

3.3. A Base Model for Adoption of Smart Contracts by Business Organizations

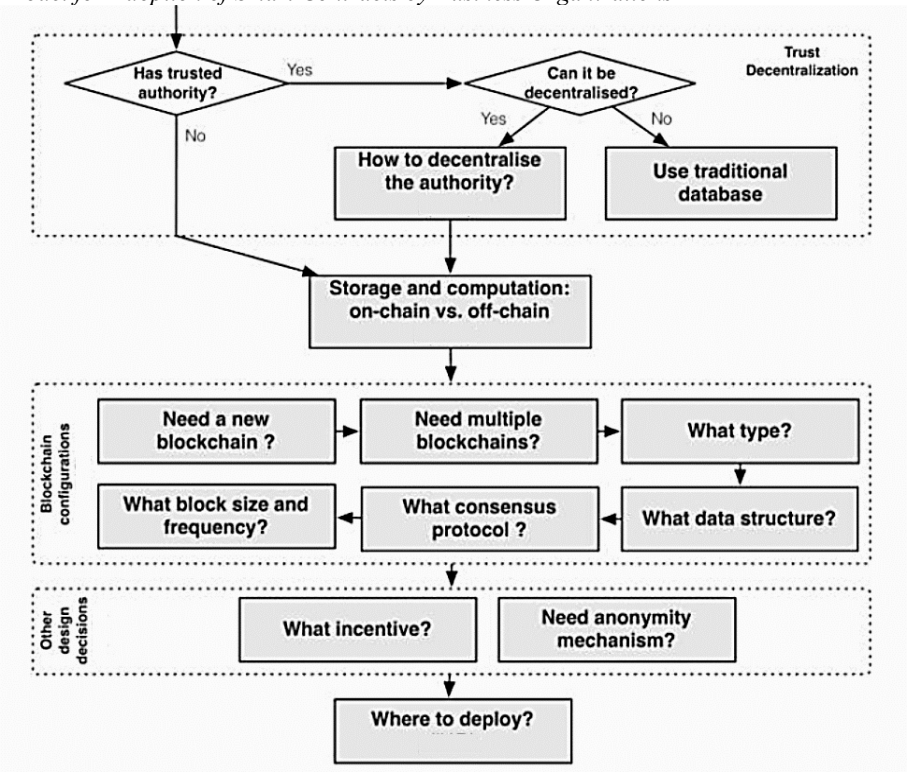

Figure 1: A model for the implementation of smart contracts

3.3.1. Phase Trust Decentralization

This phase entails establishing whether is possible to decentralize the trust of the contract in question. As earlier explained, the blockchain technology operates in a decentralized manner, an also in an environment of non-trusting partners. As such, trust decentralization is one of the critical aspects that must be ensured before implementing smart contracts. This phase would entail asking questions such as whether the contract has a trusted authority, if yes then a determination is done on whether the trust can be decentralized. Decentralization in this context implies having multiple non-trusting partners checking on the execution of the contract. If the trusted authority cannot be decentralized, then the traditional approach to the contract would be more preferred than the smart contracts. If the contract can be decentralized, the organization and the parties have to decide on how to decentralize the authority. Owing to the virtual nature of the smart contracts, this step would lead to a process of storage and computation, entailing off-chain, and on-chain computing.

3.3.2. Blockchain Configurations

This step would entail consideration and decision making regarding the configurations of the blockchain. To begin with, the parties to the contract first decide whether a bock chain is needed to solve the contract. The criticality of this process is that while some contracts would benefit from the implementation of a smart contract through blockchain technology, others would not. Hence, it is critical to determine whether the contract in question requires blockchain. Afterward, a decision ought also to be made on whether the contract requires only one blockchain or multiple blocks chains. This is because while some contracts are simple and require only one blockchain, others are quite complex and may require multiple blockchains. This is especially true in contracts that involve multiple parties and which are also interlinked with other contracts, resulting in a system of dependencies.

On a different point of view, there exist various forms of the blockchain. For instance, each of the cryptocurrencies such as the Bitcoin, Etherium, Lite coin, etc. have their underlying blockchain technology. It is, therefore, critical to first establish the type of blockchain technology that is more suitable and how it can be implemented in the contract. Afterward, it is critical to consider the data structures to be used. Essentially, smart contracts are basically coded segments. The code segments are based on specific data structures, which govern their execution. The suitability of specific data structures may depend on the contract in question. For instance, a linked list may be preferable in certain occasions that tagged union or an array. Again, a record may also be preferable in certain occasions s compared to a class or a linked list. Therefore, with the help of the developers, the parties to the contract must also establish the kind of data structure to be adopted.

Again, the blockchain configurations also encompass the consensus protocol to be employed. Consensus means how the nodes in the blockchain network come to an agreement regarding the global view of the blockchain status. These are the defined rules and conditions that govern when and how to execute transactions is to make changes in the shared database to avoid conflicts. As such, there is the need to establish rules to govern concurrent control and ensure execution of valid transactions

On a different point of view, it was earlier mentioned that a blockchain is simply a chain of blocks that has a set of records/transactions that have been verified, validated and timestamped together, with each block containing the reference of the preceding block, to ensure continuity of the chain. In this step, there is the need to determine how large the block size would be; this is realistically establishing how many transactions amount to a single block. This configuration is critical in controlling the block creation and ensuring uniformity in transaction processing.

3.3.1. Phase Trust Decentralization

After the blockchain configurations for the smart contract have been done, there is also the need to consider other business decisions. Koulu argues that the operations of an enterprise are influenced by a wide array of factors, some of which may be direct, while others may be indirect [25]. As such, it is the responsibility of the managers and top organization leaders to establish the indirect factors that affect the organizational operations and ensure that they are properly addressed. Seijas et al. bring in the concept of business logic; in otherwise, each of the smart contracts has to be within the legal and operational framework of the organizations and must positively contribute towards the achievement of the corporate goals and objectives [33].

Some of the core considerations that organizations have to make are the incentives that the customers and business partners may need to collaborate in the smart contracts. Essentially, the adoption of various technologies such as smart contracts by the firm does not imply that the business partners and customers will willingly and voluntarily support. Sergey and Hobor explain that in many circumstances, an organization has to push its business partners and customers in order to adapt and collaborate in using the new technology [34]. Pushing in the context does not literally mean dictating the customers and business partners to adopt the technology but rather, using various ways to convince the relevant parties to adopt the technology. This may entail showing the benefits of adopting the technology to the customers as well as using various incentives to lure the customers into agreeing to use the new technology. In the case of organization implementation of the smart contacts, before rolling out the technology, it would need to make a consideration of the incentives that may be useful in drawing the partners. For instance, the company can consider lowering the rates for the service packages of the customers who agree to smart contracts.

It was earlier on mentioned that the blockchain network is characterized by the anonymity aspect. Anonymity in this sense implies that the respective identities of the users in the network are anonymous, and the transaction on the ledger are treated as eliminating from an anonymous entity. The aspect of anonymity is often propagated by the existence of no-trusting parties' interaction in a decentralized environment. Depending on the nature of the contract anonymity may be necessary while in others, the anonymity aspect may not. The essence of a smart contract is to digitize traditional contracts. Hence, though necessary, anonymity is extra.

The final phase of the model is deciding when, where, and how to deploy. However, this step is dependent on the overarching blockchain architecture selected and used in developing the code. For instance, if the code was developed using the Etherium architecture, it cannot be implemented on the Bitcoin blockchain architecture. This is because the blockchain architecture for different companies differs. As such, how and where to deploy the smart contract would be depending on the underlying blockchain infrastructure chosen. On a different point of view, a specific node can as well be chosen as the entry point of the contract, where all participants access the general ledger containing the set of transactions for the smart contracts.

3.4. A Scenario for Purchasing a Service Package

The current state of organizations is characterized by traditional contract, which is characterized by low-level automation and physical exchange of assets. For instance, the businesses have a trade/sales agreement, while suppliers have the suppliers' contract with respective firms. All these contracts are documented both physically and electronically. Further, there is an intermediary, which is often a government entity credited with the responsibility of ensuring effective execution of the contracts. The main aim of the intermediary is to ensure the creation of legally enforceable contracts and also ensure that breach of the contract by either of the parties is mitigated.

On the other and, the expected states entail the use of smart contracts to automate everything and ensure that intermediaries are eliminated. For instance, there will be the existence of a smart contract between consumers and the organization, suppliers, and order organization, contractors, and the organization, etc. Essentially, after the implementation of the smart contracts, business organizations will be operating in the smart world whereby all the contracts will be programmed to self-execute, suing multiple blockchain networks. This will enhance the efficiency of the company as well as financial transparency and customers support. The result is

a well-functioning organization, which is highly efficient. Further, the implementation will also result in reduced costs, which otherwise increase the profit margins

3.5. Benefits and Applications of Smart Contracts

3.5.1 Accuracy

One of the advantages that business organizations would benefit from the implementation of smart contracts is accuracy. As explained in the processes of setting up a smart contract, all the information regarding the contract is expressed in a conditional format, using the if-then statements. For instance, when ordering a specific service package if customer x pays x units of y, then immediately credit the recipient of the amount and also open the service package for customer x. Since the majority of the contracts entail the exchange of cash. Then the smart contracts can be synced with cryptocurrencies such as Etherium, Lite Coin or bitcoin, among others, an aspect that would further enhance the robustness, accuracy, and performance of the entire system. The expression of all terms and conditions in a smart contract must be explicitly and accurate. Essentially, this is a critical requirement because transaction errors may emanate from any omission. Therefore, the automation exhibit in the smart contracts avoid the majority of the issues that are found in the traditional contracts

3.5.2. Clear Communication and Transparency

Virtually, the terms and conditions of the contract terms and conditions become explicitly visible to the different network players of the specific blockchain. Therefore, once the contract is established, changes cannot be easily implemented. Each of the transaction by either party to the contract is monitored and controlled by other network nodes in the blockchain. As a result, transparency is promoted, and issues of fraud are eliminated. In the modern era, various cases have been reported whereby the organizational is accused of defrauding the customers and not offering them the value of their money.

As aforementioned earlier, each sale of good or service by an organization results in a contract that may or may not be legally enforceable. However, in various cases, one or more parties to the contract may breach the contract terms and conditions. In the case of sales, an organization may overcharge the customer or may shorten the service package timespan agreed, without notifying the customer. The implementation of the smart contracts puts every detail of the contract into the light. Unlike in the traditional contract where the organization would have to use the legal framework as the intermediary, in the virtual world all that is needed is other nodes in the network, who are tasked with the responsibility of ensuring that each of the transaction pertaining to the contract is accurate and valid

3.5.3. Speed and Efficiency

Essentially, smart contracts do not rely on human intervention, and their implementation is guided and overseen by other nodes in the blockchain network. Therefore, once the contract is triggered, the scripted contract self-executes. This is often achieved through the use of trigger events when scripting the contact. For instance, a trigger event may be a date, time, or even an activity initiated by a party to the contract, such as the transfer of certain units of cryptocurrency from the customer's wallet to that of the company. Once a trigger event happens, the contract now starts executing itself. For instance, for online subscription-based organizations, once a specific unit of the cryptocurrency is received, then the subscription for the customer is auto-renewed.

Unlike in the traditional contracts that are less efficient and which require some form of human verification, here, the verification of whether the correct amount has been paid, and whether the correct subsection, service, and associated aspects have been given to the number is determined by the nodes in the blockchain network. As such, there is no longer reliance on the organization's developed system to determine the contracts with the customers. The organization also has no sovereign authority over the transactions as well as over the contractual agreement with the partners. Each contract is targeted as a separate entity, and each transaction, irrespective of its origin is first validated. Overly, this results in a fast, resilient and robust way of contract execution

3.5.4. Security

A study by Marino and Juels finds the smart contracts to have one of the highest security measures. Smart contracts implemented through block chin technology entail the use decentralized network made of non-trusting parties [40]. The fact that the parties in the network are non- trusting makes them keep check of one another to ensure each transaction is carried out effectively, and that there is a uniform worldview of the status of all the transactions. Again, blockchain technology is implemented through cryptography techniques. This technology entails high encryption of data and the use of both private and public keys for reading the transactions in each blockchain, as well as executing any transaction. The fact that before any node commits a transaction, the transaction must first be validated by all the odes across the blockchain network enhances the security of the smart technology.

A study carried out by Seijas explains that data encryption and specifically, the use of cryptography techniques can greatly enhance the security of communication and data exchange [33]. As such, any contract that is implemented in an encrypted manner enhances the security of the transaction and thwarts any malicious activities that may be propagated to alter the execution sequence or execute invalid transactions.

3.5.5. Cost Reduction

Essentially, top business managers are credited with the responsibility of coming up with strategies and ways of reducing costs in an organization. The main aim of setting up a business enterprise is to make profits; therefore, all the activities in an organization must be construed in a manner that promotes the achievement of corporate objectives, as well as maximizing the wealth of the shareholders [41]. In the recent wold that has seen a vast technological revolution, the success of the business enterprises is vested in their ability to keep tabs with the prevailing technologies and adopt ensures and techniques that otherwise increase the employees' productivity and performance.

The implementation of smart contracts through blockchain technology cuts the need for a middleman, such as the legal personnel. This, in turn, aids in reducing the overall organizational costs and maximizing the profit margins by an organization. In the case of multinational corporations that deal with a huge number of contracts on a daily or weekly basis, the implementation of smart contacts with its business partners and customers can greatly aid in reducing the various costs incurred in the traditional forms of contracts. The contracts can further bolster the efficiency of the organization, which is a critical ingredient for organizational success and increased performance. It is, however, critical to note that despite the security, cost reduction and efficiency aspects associated with the smart contracts, the latter is not by any chance magical, and hence may be subject to flaws. For instance, the quality and execution of the contract highly depend on the input, which is basically the coded version of the contract. Therefore, if there are flaws in setting up the smart contracts, such flaws may trigger adverse effects as well as poor quality of the output generated.

3.6. Limitations of Smart Contracts

Despite the various advantages noted and which emanate from the implementation of smart contracts, it is also crucial to note that smart contracts are associated with various limitations, the disadvantages of the smart contacts limit their application in various real-life scenarios. As attested by Kolvart et al., more often than not, technology often outpaces the law and the regulatory framework. This has been a noticeable trend with respect to smart contracts [23].

3.6.1. Immutability

Essentially, since smart contracts are scripted as a piece of codes, once set up, the contacts cannot be modified easily. In the traditional contracts, amendment of terms and conditions is often used, especially in long-term contracts whose execution is depending on real-life dynamics, and the conditions keep changing. Owing to the rigidity exhibited in the smart contracts after being established, the latter results in a wide array of practical problems more so with respect to the ease of modifying the contract terms in depending on various situations.

This is underpinned by Huckle et al., who explains that the conventional contracts have provisions that allow for the annulment, embedment, and modification of contracts [19]. The implementation of smart contracts. To a greater extent, makes it literally impossible to achieve analogous goals. Nevertheless, various actions can be taken in order to include aspects of modification and contract annulment. For instance, an escape hatch can be included in the coded contract. The escape hatch can be used to allow for the modification of the contract terms, in order to cater for the real-life contracts which are characterized by vast dynamics. Nevertheless, implementing such in the smart agreements may compromise the security apparatus, and hence may require further tightening of the transaction controls in order to ensure that the escape hatch is not used to initiate invalid transaction or transactions that are aimed at unauthorised manipulation of records This is as well noted by Kolvart et al., who explains that owing to the complexity of the smart contract and blockchain technology in general , ensuring that the right permission is granted to the right node, and that all the nodes can monitor the amendment of the contract may be quite tricky but necessary[23].

3.6.2. Contractual Secrecy

Mostly, the blockchain technology entails the sharing of smart contract across all the nodes in the blockchain network, since all the transaction is recorded on general ledger using encoded permissions in each of the nodes. Essentially, the blockchain technology entails the use of anonymity, whereby all the participants in a blockchain network are anonymous and secured. However, there is no security of the contract execution. This is because though the nodes are anonymous in their operations, the ledger is maintained public, and hence, the transactions are visible, and there is no security of such. Buterin explains that this is an area that needs to be focused because despite the nodes being anonymous, the maintenance of a public ledger in the distributed environment results in a privacy lapse [6].

While the essence of the smart contracts is to maintain a public ledger that is visible to all parties in the network and to monitor the validity and accuracy of the taxations, there is the need also to develop a protocol, which can aid in the verification of the transactions without necessarily reading the contents of the transaction. This is because though the participants and the origin of the transaction may be anonymous, the contents are not; and actually, each node can read and access the transaction contents. It is as well critical to developing measures to curb this privacy issues since security is not all about anonymity and encryption, it also entails ensuring the

content of the transaction is protected against access by other parties. As such, this aspect of smart contracts is yet to be fully addressed.

3.6.3. Legal Adjudications and Enforceability

Traditionally, the establishment of a valid contract covers various constructs, which make it legally enforceable. Kim and Laskowski explain that the key characteristics of a legally enforceable contract are; offer by one party or parties, acceptance by the other party or parties, a promise, consideration, and legal capacity mutuality and in some contracts, a written instrument [21]. While these elements of a contract are very critical, some of them are not applicable to smart contracts.

For instance, the financial sector exhibits immense regulations by the government, and specific permissions and licensures are required for a form to engage in transactions execute don general ledgers. However, despite the licensure and associated approvals, the legal enforceability of the smart contracts is yet to be established and synced with the contract law as well as other laws that give financial transactions. All elements of aspect contracts are expressed as segments of code, and the aforementioned elements of a valid contract may not necessarily be identifiable. This, therefore, necessitates the need for the translation of the legal framework governing the contracts into the software logic to ensure that besides the smart contract being self-executing, they also adhere to the legal regulations of formal contracts. Further, such tantalization should take in to account the blockchain developer's point of view, the lower's point of view and the transacting parties' points of view. Such an aspect would aid in enforcing the legality and validity of the contracts. However, as at present, the organizations that have implemented the smart contracts through blockchain technology have to continuously struggle with the aspect of the contract validity and enforceability. Nevertheless, Vukolić denotes that the upside of the smart contracts is that breaches of contracts are rare to occur, as the execution of the contract is dependent on the pre-defined conditions which are also triggered by an event that neither of the nodes in the network has control over [35].

5. Conclusions

Business organizations can use smart contracts for various transactions, such as suppliers and consumers. Under this approach, the contract would be written as a conditional (if then) program segment that would then be implemented on the blockchain [30]. Owing to the newness of smart contracts, there exists little to no existing studies on the impact of this technology on organizational performance.

The world today has realized the vast technological evolution that has greatly shaped the production and management functions of business enterprises. Traditional contracts can take weeks or even months to initiate, and there have been numerous instances of breaches and lack of trust for contracts at both private and public sector. Through the age of digitalization, there lies an opportunity to connect the businesses in a more trusted manner as well as increasing efficiency by automating contracts for a reduction in risk management in business operations. The traditional approach to contracts entails the use of a third party as well as regulators for the contract to be legally enforceable. In smart contracts, there need not be third parties since once the contract is committed, it self-executes, based on the pre-set “if-then” contract conditions [8]. The blockchain technology upon which smart contracts are built using a distributed model of the transaction processing and a public ledger, it becomes merely impossible for the committed transaction to be changed, as every node in the blockchain network receives an automatic copy of the blockchain after every new block is added. Owing to this, there is a need to examine how smart contracts affect the organization' performance

The blockchain technology has literally attracted the attention of various individuals and organizations across all the sectors, such as in real estate, utilities, healthcare, and even the public sector. This has partially been caused by the technological revolution that has seen the emergence of better and more sophisticated technologies, characterized by cognitive computing, the internet of things, and cyber-physical system. A study conducted by Fulbright on the emergence and trends in industry 4.0 indicates that technological advancement is likely to see a sharp increase over the next couple of years, characterized by the manufacturing of more smart devices [16].

The increasing interest in the blockchain technology and smart contracts is driven by the ability to execute various business operations and tasks; tasks that were previously undertaken via a trusted intermediary [14]. The researcher continues to argue that through smart contracts executed via blockchain technology, it becomes possible to warrant the security of transactions.

Blockchain makes it possible for a business organization to execute tasks with partner organizations through trusted networks irrespective of whether they have an established trust relationship with such partners or not. The absence of intermediary, which was a core characteristic of the traditional contract enhances efficient and rapid reconciliation between the parties engaged in a given contract. Morrison explains that the reliance of the blockchain technologies integral and smart contracts in specific on cryptography promotes the aspect of authoritativeness in all the transactions in the network [28].

In explaining how the smart contracts work, Seijas explains that a smart contract is simply a self-executing

script that is contained in a given block within the blockchain [33]. The scripts allow for efficient distribution and the automation of workflows. Such an aspect has made blockchain technology and smart contracts in specific an interesting subject to researchers on the internet of things and cryptography. On a different point of view. Buterin asserts that the move to adopt a decentralized approach in computing and specifically with respect to the smart contracts may or may not make sense to the layman [6]. However, Cohn explains that smart contracts built on the blockchain technology bring about a wide array of advantages and disadvantages [9].

Blockchain technology allows the expression of the traditional contracts to a self-performing/ self-executing virtual contract, based on some pre-set conditions and rules. As at present, the smart contracts cannot be said to be legally binding, as the legal framework component is yet to be added to the smart contracts architecture. A critical aspect to note, however, is that though the smart contracts may not be legally enforceable, or else, the parties may not be legally liable for the breach of contract, they may as well be used to enforce performance of parties in legal contracts. The execution of a smart contract; therefore, followers the pre-programmed instructions and once the transactions have been verified and committed, they cannot be modified or undone.

As observed in the analysis and discussion section, business organizations would benefit from two main advantages that are associated with the smart contracts implemented through blockchain technology. First, issues of debate by parties to the contract with regard to the meaning and interpretation of the contract would be limited since the interoperation of the set condition in the program segment is done by machines and hence not subject to fallible human interpretation. Further, the transaction costs are also reduced, and since the performance is executed by the computer programs and the need for the intermediary is eliminated. It is, however, critical to note that the flaws and deficiencies in smart contracts may have vast ramification not only the organization but also to the customers and the business partners.

The implementation of the outset smart contract model would ensure that business organizations are able to execute millions of contractual clauses without the necessity of human intervention. Nevertheless, it should be the responsibility of the organization to ensure the development of smart legal contracts. A smart legal contract is a concept that describes ensuring that all elements of the legal contract are adhered to implement the contract, though they may not be enforceable in such interacts. The main aim of enlisting the traditional legal framework governing contacts is to ensure that the contract produces desired results. To achieve this, a business organization would ensure that the possible elements of legal contracts, such as an offer, a consideration, and a promise are included in the scripted contract. Further observation of various regulations should so be made, such as the laws governing the consumption and sales of goods.

References

[1]. Åkerlind, G.S., 2012. Variation and commonality in phenomenographic research methods. *Higher Education Research & Development*, [e-journal] 31(1), pp.115-127.
[2]. Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J. and Wuille, P., 2014. *Enabling blockchain innovations with pegged sidechains.* [online] Available at < http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains>
[3]. Norta, A. (2015, August). Creation of smart-contracting collaborations for decentralized autonomous organizations. In *International Conference on Business Informatics Research*(pp. 3-17). Springer, Cham.
[4]. Böhme, R., Christin, N., Edelman, B., and Moore, T., 2015. Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, *29*(2), pp.213-38.
[5]. Bryman, A., and Bell, E., 2015. *Business research methods*. Oxford University Press, USA.
[6]. Buterin, V., 2014. A next-generation smart contract and decentralized application platform. *White paper*.
[7]. Chen, H., Chiang, R.H., and Storey, V.C., 2012. Business intelligence and analytics: from big data to the big impact. *MIS Quarterly*, [e-journal] pp.1165-1188.
[8]. Christidis, K., and Devetsikiotis, M., 2016. Blockchains and smart contracts for the internet of things. *IEEE Access*, [e-journal] 4, pp.2292-2303.
[9]. Cohn, A., West, T., and Parker, C., 2017. Smart After All: Blockchain, Smart Contracts, Parametric Insurance, and Smart Energy Grids. *Georgetown Law Technology Review*, *1*(2), pp.273-304.
[10]. Cong, L. W., & He, Z., 2018. *Blockchain disruption and smart contracts* (No. w24399). National Bureau of Economic Research.
[11]. Delmolino, K., Arnett, M., Kosba, A., Miller, A., & Shi, E. (2016, February). Step by step towards creating a safe, smart contract: Lessons and insights from a cryptocurrency lab. In *International Conference on Financial Cryptography and Data Security* (pp. 79-94). Springer, Berlin, Heidelberg.
[12]. Drnevich, P. L., and Croson, D. C., 2013. Information technology and business-level strategy: Toward an integrated theoretical perspective. *Mis Quarterly*, [e-journal] 37(2).
[13]. Eyal, I., Gencer, A.E., Sirer, E.G., and Van Renesse, R., 2016, March. Bitcoin-NG: A Scalable Blockchain Protocol. In *NSDI* [e-journal] (pp. 45-59).
[14]. Fairfield, J. A. (2014). Smart contracts, Bitcoin bots, and consumer protection. *Washington and Lee*

Law Review Online, *71*(2), 36.
[15]. Fowler Jr, F.J., 2013. *Survey research methods*. Sage publications.
[16]. Fulbright, N.R., 2016. Smart contracts: coding the fine print. *A legal and regulatory guide*.
[17]. Greenspan, G., 2015. Ending the bitcoin versus Blockchain debate.
[18]. Hillbom, E., and Tillström, T., 2016. *Applications of Smart contracts and smart property utilizing blockchains*(Doctoral dissertation, Masters of Science Thesis in Computer Science, Chalmers University of Technology and University of Gothenburg, Sweden. February).
[19]. Huckle, S., Bhattacharya, R., White, M., and Beloff, N., 2016. Internet of things, blockchain, and shared economy applications. *Procedia computer science*, *98*, pp.461-466.
[20]. Iansiti, M., and Lakhani, K. R., 2017. The truth about blockchain. *Harvard Business Review*, [e-journal] 95(1), pp. 118-127.
[21]. Kim, H.M., and Laskowski, M., 2018. Toward an ontology-driven blockchain design for supply-chain provenance. *Intelligent Systems in Accounting, Finance, and Management*, *25*(1), pp.18-27.
[22]. Kocarev, L., Makraduli, J., & Amato, P., 2005. Public-key encryption based on Chebyshev polynomials. *Circuits, Systems and Signal Processing*, *24*(5), 497-517.
[23]. Kolvart, M., Poola, M., and Rull, A., 2016. Smart contracts. In *The Future of Law and technologies* (pp. 133-147). Springer, Cham.
[24]. Kosba, A., Miller, A., Shi, E., Wen, Z., and Papamanthou, C., 2016, May. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *Security and Privacy (SP), 2016 IEEE Symposium* [e-journal] (pp. 839-858). IEEE.
[25]. Koulu, R., 2016. Blockchains and online dispute resolution: smart contracts as an alternative to enforcement. *SCRIPTed*, *13*, 40.
[26]. Luu, L., Chu, D.H., Olickel, H., Saxena, P., and Hobor, A., 2016, October. Making smart contracts smarter. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* [e-journal] (pp. 254-269). ACM.
[27]. Marino, B., and Juels, A., 2016, July. Setting standards for altering and undoing smart contracts. In *International Symposium on Rules and Rule Markup Languages for the Semantic Web* (pp. 151-166). Springer, Cham.
[28]. Morrison, A., 2016. How smart contracts automate digital business. *Alan Morrison, PwC Technology Forecast Series. http://usblogs. PWC. com/emerging-technology/how-smart-contracts-automate-digital-business*.
[29]. Neuman, W.L., 2013. *Social research methods: Qualitative and quantitative approaches*. Pearson education.
[30]. Omohundro, S., 2014. Cryptocurrencies, smart contracts, and artificial intelligence. *AI matters*, [e-journal] 1(2), 19-21
[31]. Peters, G.W., and Panayi, E., 2016. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the
[32]. Pettersson, J., & Edström, R., 2016. *Safer smart contracts through type-driven development* (Doctoral dissertation, Master's thesis, Chalmers University of Technology, Department of Computer Science and Engineering, Sweden).
[33]. Seijas, P. L., Thompson, S. J., & McAdams, D., 2016. Scripting smart contracts for distributed ledger technology. *IACR Cryptology ePrint Archive*, *2016*, 1156.
[34]. Sergey, I. and Hobor, A., 2017, April. A concurrent perspective on smart contracts. In *International Conference on Financial Cryptography and Data Security* (pp. 478-493). Springer, Cham.
[35]. Vukolić, M., 2017, April. Rethinking permissioned blockchains. In *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts* (pp. 3-7). ACM.
[36]. Swan, M. (2015). *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.."
[37]. Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*(3), 183-187.
[38]. Zhang, F., Cecchetti, E., Croman, K., Juels, A., & Shi, E. (2016, October). Town crier: An authenticated data feed for smart contracts. In *Proceedings of the 2016 ACM sIGSAC conference on computer and communications security* (pp. 270-282). ACM.
[39]. Pilkington, M. (2016). 11 Blockchain technology: principles and applications. *Research handbook on digital transformations*, 225.
[40]. Marino, B., & Juels, A. (2016, July). Setting standards for altering and undoing smart contracts. In *International Symposium on Rules and Rule Markup Languages for the Semantic Web* (pp. 151-166). Springer, Cham.
[41]. Saleem, M. A. (2017). The impact of socio-economic factors on small business success. *Geografia-Malaysian Journal of Society and Space*, *8*(1)