Understanding of Blockchain Application and Smart Contracts

Author's Details:
[(1)]**Thanh Thao Pham** [(2)]**Thi Duyen Vu** [(3)]**Thi Thu Trang Nguyen**
[(1) (2) (3)]University of Economics - Technology for Industries, Vietnam
Correspondence: Thanh Thao Pham, 456 Minh Khai, Hai Ba Trung, Ha Noi

Abstract:
The birth of "smart contracts" has based on developments in the emerging field of Blockchain application: computerized transaction protocols that autonomously execute the terms of a contract. With a lot of advantages which I will analyze below, Smart contracts are really offering the promise of increased commercial efficiency, lower transaction and legal costs, and anonymous transacting.

Keywords: *Smart contracts, Blockchain*

1. Introduction

Blockchain technology – dates back to the early 1990's, has to be one of the biggest innovations of the 21stcentury given the ripple effect it is having on various sectors, from financial to manufacturing as well as education.

The first work on a cryptographically secured chain of blocks was described in 1991 by Stuart Haber and W. Scott Stornetta. They wanted to implement a system where document timestamps could not be tampered with. In 1992, Bayer, Haber and Stornetta incorporated Merkle trees to the design, which improved its efficiency by allowing several document certificates to be collected into one block.

The first Blockchain was conceptualized by a person known as Satoshi Nakamoto in 20081. Nakamoto improved the design in an important way using a Hashcash-like method to timestamp blocks without requiring them to be signed by a trusted party and introducing a difficulty parameter to stabilize rate with which blocks are added to the chain. The design was implemented the following year by Nakamoto as a core component of the cryptocurrency bitcoin, where it serves as the public ledger for all transactions on the network.2

In August 2014, the bitcoin Blockchain file size, containing records of all transactions that have occurred on the network, reached 20 GB (gigabytes). In January 2015, the size had grown to almost 30 GB, and from January 2016 to January 2017, the bitcoin Blockchain grew from 50 GB to 100 GB in size.

Launched in 2008 by Nakamoto: Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, (2008); for useful background materials, see also http://www.projectbitcoin.com/ and https://bitcoin.org/en/. Nick Szabo, Smart Contracts: Building Blocks for Digital Markets (1996).

The words block and chain were used separately in Satoshi Nakamoto's original paper, but were eventually popularized as a single word, Blockchain, by 2016.

According to Accenture, an application of the diffusion of innovations theory suggests that Blockchains attained a 13.5% adoption rate within financial services in 2016, therefore reaching the early adopters phase. Industry trade groups joined to create the Global Blockchain Forum in 2016, an initiative of the Chamber of Digital Commerce.3

In May 2018, Gartner found that only 1% of CIOs indicated any kind of Blockchain adoption within their organizations, and only 8% of CIOs were in the short-term "planning or active experimentation with Blockchain".4

2. Blockchain

2.1. Concept and features

Don & Alex Tapscott, authors Blockchain Revolution in 2016 stated that ―The Blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.

A Blockchain is, in the simplest of terms, a time-stamped series of immutable records of data that is managed by a cluster of computers not owned by any single entity. Each of these blocks of data (i.e. block) is secured and bound to each other using cryptographic principles (i.e. chain).

First and foremost, Blockchain is a public electronic ledger built around a P2P system that can be openly shared among disparate users to create an unchangable record of transactions, each time-stamped and linked to the previous one. Every time a set of transactions is added, that data becomes another block in the chain. Blockchains are a distributed ledger comprised of blocks. Each block is comprised of a block header containing metadata about the block, and block data containing a set of transactions and other related data. Every block header contains a cryptographic link to the previous block‘s header. Each transaction involves one or more Blockchain network users and a recording of what happened, and it is digitally signed by the user who submitted the transaction.

Blockchain can only be updated by consensus between participants in the system, and once new data is entered it can never be erased. It is a write-once, append-many technology, making it a verifiable and auditable record of each and every transaction.

Blockchains are tamper evident and tamper resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company, or government). At their basic level, they enable a community of users to record transactions in a shared ledger within that community, such that under normal operation of the Blockchain network no transaction can be changed once published. Hence, anything that is built on the Blockchain is by its very nature transparent and everyone involved is accountable for their actions. Blockchain implementations are often designed with a specific purpose or function. Example functions include cryptocurrencies, smart contracts (software deployed on the Blockchain and executed by computers running that Blockchain), and distributed ledger systems between businesses.

There are two general high-level categories for Blockchain approaches that have been identified: Public permissionless, and private permitted. In a permissionless Blockchain network anyone can read and write to the Blockchain without authorization. Permissioned Blockchain networks limit participation to specific people or organizations and allow finer-grained controls. Knowing the differences between these two categories allows an organization to understand which subset of Blockchain technologies may be applicable to its needs. Despite the many variations of Blockchain networks and the rapid development of new Blockchain related technologies, most Blockchain networks use common core concepts

Blockchain has some basic features:

(a) Immutable

Immutability is undoubtedly one of the most significant Blockchain features. It means that no Blockchain developer or user can alter or delete the data in the ledger or add new content without any validation. This feature ensures immutability. When a Blockchain transaction happens all the nodes in the network will have to say it‘s valid or it won‘t get added to the ledger.

(b) Decentralized

Blockchain definition, you came across the word ―decentralized.‖ In reality, it means that here is no single person or governing authority that looks over the framework. But in a typical network structure, everything heavily depends on the client-server model. But here, a single person or group looks after the whole

infrastructure. This is one of the significant benefits every Blockchain developer should look for. It promotes user rights. Thus, it offers more benefits: (1) Gets rid of human-made errors, so it‘s more fault-tolerant; (2) More control for users over their properties; (3) Highly secure because it‘s more expensive, more hackers to stack the system; (4) Gets rid of all third-party integrations; (5) No chance of being scammed as the system runs entirely on algorithms; (6) Every change is reviewed by the nodes, which promotes transparency and introduces an authentic architecture, people would have a hard time cracking the code and attacking it.

(c) Enhanced Security

It gets rid of the central authority, but that does not mean that anyone can do anything they want. That would be a severe risk to every node. In reality, to promote privacy and security, all the data on the ledger is heavily encrypted. Here, in Blockchain definition, a term called cryptography is heavily mentioned. In reality, cryptography is one of the complex mathematical algorithms outside. There‘s no way to crack the code. Furthermore, if anyone wants to change any value in the block, it will generate a completely different outcome that won‘t be linked to the original change. Additionally, every block comes with a unique hash ID. However, changing the hash ID is impossible. Also, to make a Blockchain transaction, need help from both public and private keys. Figuring out other users private keys is also impossible.

(d) Distributed Ledger

Another cool feature of Blockchain is the distributed nature of the system. In reality, all the nodes maintain the ledger, and so the overall computational power gets distributed among them. In the case of the public Blockchain, everyone can see the ledger without any issues. However, in private, the things change a bit, but still, it‘s viewable.

(e) Consensus

The consensus is a crucial factor when it comes to Blockchain. Without consensus, the Blockchain system won‘t work. In reality, the consensus algorithms help the network make decisions. Without any consensus, no Blockchain can make a fair judgment of the blocks being added.

2.2. Type of Blockchains

There are three primary types of Blockchains, which do not include traditional databases or DLT that are often confused with Blockchains: (a) Public Blockchains like Bitcoin and Ethereum; (b) Private Blockchains like Hyperledger and R3 Corda; (c) Hybrid Blockchains like Dragonchain7.

a) Public Blockchains which are open source, allow anyone to participate as users, miners, developers, or community members. All transactions that take place on public Blockchains are fully transparent, meaning that anyone can examine the transaction details. Public Blockchains are designed to be fully decentralized, with no one individual or entity controlling which transactions are recorded in the Blockchain or the order in which they are processed. In addition, they can be highly censorship-resistant, since anyone is open to join the network, regardless of location, nationality, etc. This makes it extremely hard for authorities to shut them down. Lastly, public Blockchains all have a token associated with them that is typically designed to incentivize and reward participants in the network.

b) Another type of chains are private Blockchains, also known as permissioned Blockchains, possess a number of notable differences from public Blockchains. In this type, participants need consent to join the networks, and transactions are private and are only available to ecosystem participants that have been give permission to join the network. That‘s reason why private Blockchains are more centralized than public ones. They are valuable for enterprises who want to collaborate and share data, but don‘t want their sensitive business data visible on a public Blockchain. These chains, by their nature, are more centralized; the entities running the chain have significant control over participants and governance structures. Private Blockchains may

or may not have a token involved with the chain. Besides, there is another Blockchain type- Consortium Blockchains. But sometimes they are considered a separate designation from private Blockchains. The main difference between them is that consortium Blockchains are governed by a group rather than a single entity. This approach has all the same benefits of a private Blockchain and could be considered a sub-category of private Blockchains, as opposed to a separate type of chain. This collaborative model offers some of the best use cases for the benefits of Blockchain, bringing together a group of ―frenemies‖- businesses who work together but also compete against each other. They are able to be more efficient, both individually and collectively, by collaborating on some aspects of their business. Participants in consortium Blockchains could include anyone from central banks, to governments, to supply chains.

c) The hybrid nature of Dragonchain Blockchain platform is made possible by patented Interchain capability, which allows people easily connect with other Blockchain protocols. Allowing for a multi-chain network of Blockchains. This functionality makes it simple for businesses to operate with the transparency they are looking for, without having to sacrifice security and privacy. Also, being able to post to multiple public Blockchains at once increases the security of transactions, as they benefit from the combined hash power being applied to the public chains.

3. Development of Blockchain recently

Ever since January of 2009, Blockchain technology has been growing and evolving. What was once thought of as a fad, now stands on the brink of changing technology in a way that history will come to see as the time before Blockchain, and everything that came after.

The Blockchain evolves into something much more than what it started out as. All new concepts go through a process of developing a refined set of advancements along the way, Blockchain has been going through this transformation since its inception.

In the beginning, the Blockchain was merely the technology supporting Bitcoin. That beginning produced:

- Decentralization of currency and financial transactions
- Decentralization of data/information storage using a distributed, decentralized database
- Eliminated the need for ―trusted‖ 3rd parties to verify transactions
- Resistance to censorship, immutable, and corruption
- Introduced the Proof of Work Consensus Method, which is what makes the Blockchain unique as it combines computational processing power through the use of nodes connected to the network. These nodes verify all transactions and secure a public ledger.

Many experts could see that Blockchain had a use case that far exceeded Bitcoin‘s need. They analyzed the situation by using the same method used to develop the structure of the internet (known as the internet protocol suite or TCP/IP Stack) and saw that Blockchain was introducing a radical change to the internet itself, and so the need to act as a platform having its own applications built on top of its core just like Windows OS was built on top of DOS.

However, the Bitcoin Blockchain at the time could not fulfill their expectations since the source code did not allow for Turing complete smart contracts. This means that their automated system could not simulate human behavior and prowess.

Vitalik Buterin, a Russian-Canadian programmer, wanted Blockchain technology to allow for this level of scripting, and since the Bitcoin Blockchain couldn‘t scale up enough to make this happen, Vitalik decided to take it upon himself to get it done. In 2014 he put together a little project called Ethereum.

The Ethereum project was an evolutionary step in Blockchain technology, which has seen many vast improvements. These improvements allowed for Blockchain to become a platform through the concept of a virtual distributed machine. Ethereum and other similar platform projects are known as distributed virtual machines because they can run decentralized applications on their Blockchains.

This technology can now program conditional transactions and build Turing complete smart contracts, giving it the ability to emulate human behavior. Another thing that Ethereum brought was the ability to conduct micro-payments, so it can handle small value transactions, which is essential if you want Blockchain technology to apply to businesses (as an example) like large retail food chains or coffee houses. With the ability to run applications on top of the Blockchain, it introduces the concept of tokenized digital assets. An example of this would be Factbars.

Ethereum also birthed the idea of DAO, which is a decentralized corporation running entirely on smart contracts. These would govern finances and company policy on the Blockchain. But as the Blockchain and companies interweaved there were a few problems that cropped up.

There was also the issue of cross-chain interoperability that if/when these projects became the norm and the services need to interact to create user friendliness amongst the varied applications on different Blockchains would be required.

Another issue was big data and widespread adoption. Would manually programmable smart contracts be something practical to use? How would organizations analyze the big data that Blockchains provided?

For these things to happen Blockchain technology needs to take another leap forward. One answer is parallel transactions or directed acyclic graph technology, which allows for many parallel streams of data to run at the same time on a network. This has the effect of dividing up the work and preventing a bottleneck that can slow transactions down to a crawl. This also allows for decentralized mining and cuts down on fees.

Side chains also bring with them another solution. With these, you can transfer a tokenized asset over to another Blockchain, which keeps the main Blockchain freed up to handle more transactions while the transactions happening on the sidechain won‘t be recorded until the users return the assets to the main chain, or a required recording of assets by the main chain occurs.

Cross-chain technology will solve interoperability. Projects such as the Lightning Network, which is still being built, will allow users and assets to communicate and trade withholdings from another Blockchain.

It‘s always fun to look back at emerging technology to evaluate all the steps it had to go through to get it to where it is today. Just like the days of Pong, which lead to Atari, Nintendo, and then to PlayStation and so on. The Blockchain is quickly solving the problems that stand in its way of becoming the biggest thing to technology since the computer.

Today the Blockchain is probably a lot like where Atari was in the 80s, we are still at the relatively early stages, but it won‘t be long before we see the Blockchain reaching into all of our lives. And for those who know how to make the right speculations, the chance to make money while helping this technology grow will be there for the taking. One day we are going to look back and remember the days when Blockchain took mass adaption, it‘s not that far away, and once we turn the corner, the world is going to be a vastly better place.

4. Fundamental of Smart contracts

Blockchain technology can be used to implement other decentralised services besides currency transactions where trust is inbuilt based on Blockchain intrinsic properties. One of the main reasons is the extra features that can be incorporated on top of Blockchain, one of the most important of which is probably the use of smart contracts.

4.1. Definition

A smart contract is a self-enforcing piece of so ware that is managed by a P2P network of computers. Smart contracts are eccient rights management tools that provide a coordination and enforcement framework for agreements between network participants, without the need of traditional legal contracts8. By another way, Smart contracts are computer programs that are capable of carrying out the terms of agreement between parties without the need for human coordination or intervention. They can be used to formalize simple agreements between two parties, the bylaws of an organization, or to create tokens. These agreements can be recorded and validated into a Blockchain which can then automatically execute and enforce the contract usually under _if-then‘ instructions: _if‘ something happens (for example, if you rent and pay for a car and short-term insurance) _then‘ certain transactions or actions are carried out (the car door unlocks and the payment is transferred). A smart contract enables two or more parties to perform a trusted transaction without the need for intermediaries. The way in which transactions are verified and added on the Blockchain guarantees that conflicts or inaccuracies are reconciled, and that in the end there is only one valid transaction (no double entries).

In the Internet we use today, the business models and ―raison d‘etre‖ of many tech giants like Amazon, eBay, Airbnb, Uber, etc. result from the lack of such a trustful native settlement layer. Smart contracts provide a solution to exactly that problem. They can formalize the relationships between people and institutions and the assets they own over the Internet, entirely P2P, without the need for trusted intermediaries. Although the concept of smart contracts is not new, Blockchain technologies seem to be the catalyst for smart contract implementation. A more primitive form of a smart contract is a vending machine. The rules of a transaction are programmed into a machine. You select a product by pressing a number related to that product, insert the coins, and the machine acts as a smart contract by checking whether you inserted enough money. If yes, the machine is programmed to eject the product, and if you inserted too much money, it will also eject the change. If you didn‘t insert enough money, you wouldn‘t get the product, or if the machine ran out of money, you would not get your change back. Automatic vending machines not only slashed transaction costs by making dedicated stores obsolete, but they also expanded service, offering 24/7 availability instead of limited opening hours of a kiosk.

A smart contract can simply be defined as a computer code that runs on top of the Blockchain.9 It contains a set of rules that determine how the involved parties can interact with each other. So, whenever these predefined rules are met, automatically the agreement is enforced. It‘s the purest form of decentralized automation.

The smart contract code is responsible for facilitating, verifying, and enforcing the negotiation or performance of a transaction or an agreement.

The idea of smart contracts was initially conceived in 1993 by Nick Szabo a cryptographer and computer scientist. He described them as a kind of digital vending machines. At the time he gave an example that explained how users could input value or data and in turn receive a finite item from a machine like a soft drink or a snack.

Szabo‘s original idea of smart contracts was broad enough that some smart contracts will fulfill the requirements of a legally enforceable contract while others will not11. Szabo‘s idea lay dormant for many years because the technology did not yet exist to support the implementation of smart contracts12. Then, in 2009, the Bitcoin blockchain emerged itself a limited form of a smart contract13. Later, Ethereum offered an enhanced ability to build more complex smart contracts by using a specific smart contract language (Solidity) to enable developers to write complex processes in a short span of code14. The rise of these protocols led to the resurgence of the smart contract idea and its increasing popularity as a tool for enhancing business processes and efficiencies. Integrating Szabo‘s original idea into the new technological age of blockchains, however, has proved more difficult than perhaps initially anticipated.

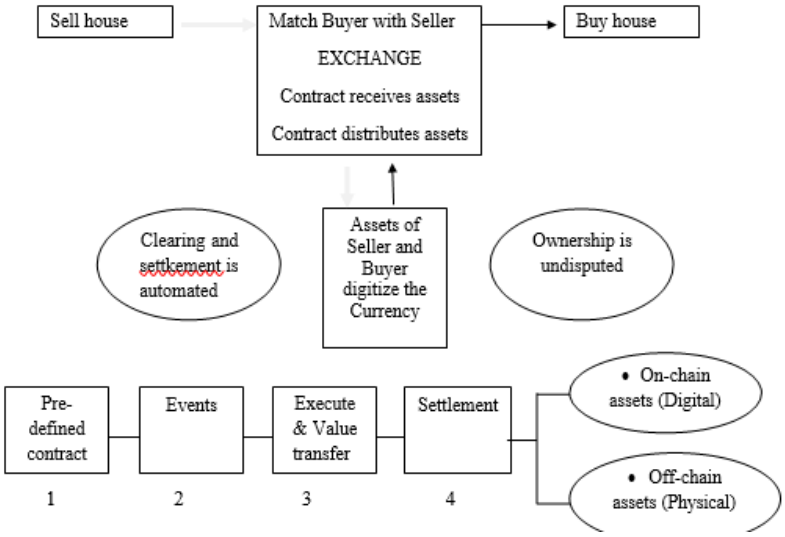

Fig. 1. How smart contracts work

Step 1: Terms are established by all counterparties, such as:

- Variable interest rate
- Currency of payments
- Currency rate
- Conditions for execution (e.g: time and date, LIBOR rate at given value)

Step 2: Event triggers contract execution

- Even can refer to:
- Transaction initiated
- Information received

Step 3: Terms of contract dictate movement of value based on conditions met Step 4:

a. For digital assets on the chain, such as a crytocurrency, accounts are atomically settled

b. For assets represented off the chain, such as stocks and fiat. Changes to accounts on the ledger will match off-chain settlement instructions.

4.2. Characteristics

A smart contract has the following characteristics:

- Self-executing: A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized Blockchain network. Contract operations can be self-executing - occurring automatically, without taking the further step of being ―self-enforcing,‖ like the difficult-to-reverse step of forfeiting a deposit through a Blockchain transfer. Only slightly less visible than the efficiency advantages to codified contracts are (he easier and better communications between contract makers and contract

implementers, and the potentially enhanced trust among contracting parties that may flow from employing reliable, transparent, automated operations inside a Smart Contract.16

• Immutable: Once a smart contract is deployed, the code cannot be changed by a party unilaterally. Thanks to the immutability feature, the performance of the contract is guaranteed to take place in exactly the same manner in which it is coded; the contract does not allow for any modifications and/or reversal. Furthermore, unless programmed to do otherwise, it will remain on the Blockchain forever and cannot be misplaced or lost. The history of the transactions forming part of the contract is also recorded on the Blockchain forever and thus this too makes for greater transparency and safekeeping.

• Self-verifying: Smart contracts can self-verify the conditions that are placed inside a contract by interpreting data. ... A triggering event such as a due date, expiration date, strike price or other conditions is set so that the contract is easily interpreted and automatically executed according to the terms written in the code.

• Auto-enforcing: A smart contract is a self-enforcing agreement embedded in computer code managed by a Blockchain. The code contains a set of rules under which the parties of that smart contract agree to interact with each other. If and when the predefined rules are met, the agreement is automatically enforced. Specifically, Smart contracts can also be applied for the benefit of consumers by automatically enforcing their rights (instead of their duties). For example, these consumer- friendly Smart contracts are becoming increasingly widespread in the insurance industry, with Blockchain-based insurance policies providing for pay-outs that are automatically triggered once predetermined parameters are met. For instance, flight-delay decentralized application provide for such automated payments whenever flight-delay decentralized applications provide for such automated payments whenever flight delays or cancellations arise.17

Mechanisms

The operation of smart contracts can hardly be decoupled from the underlying Blockchain. State of a Blockchain is updated when a valid transaction is recorded on chain, and smart contracts can be used to automatically trigger transactions under certain conditions. We categorize smart contracts to public smart contracts and permissioned smart contracts according to the Blockchain platforms they operate on.

As the expectation and requirements for smart contracts are often diff erent for the two categories, we below discuss them separately. We consider all smart contracts on permissioned, consortium or private Blockchains as permissioned smart contracts.

• Public Smart contract: Public Blockchains set no requirement for peers to participate, hence all peershave the right to deploy smart contracts. In order to prevent spamming, wheninstantiating or invoking smart contracts on a public Blockchain, one is often required to pay a certain amount of fee. Limited by its functionality, thescripting language used in Bitcoin–Scripts –is hardly used in constructing complex contractual terms. While the general-purpose Solidity language in Ethereum can be used for a much wider variety of applications. Accordingto Etherscan, among the one million Ethereum accounts that altogetherhold 105.6 million Ethers, a half of them are contract accounts with a totalbalance of 12 million Ether. Competitors such as Neo and EOS, are also independent Blockchains facilitating peer consensus and smart contracts. To show the popularity of diff erent platforms, we obtained the number ofpublicly available smart contract projects deployed on Github from thebeginning of 2015 till early 2019.To give readers an intuitive idea of how smart contracts work on pub-lic Blockchains, we below explain the mechanism of Ethereum contracts. Ethereum uses PoW mining protocol for network consensus. Ethereum smart contracts reside in Ethereum Virtual Machines (EVMs),which isolates them from the Blockchain network to prevent the code running inside from interfering with other processes. Once deployed, the smartcontract obtains a unique address that is linked to a balance, similar to anexternally controlled account (EOA) owned by a user. A smart contract cansend transactions to an EOA or another contract.

• Permissioned Smart contracts: Permissioned smart contracts, residing on permissioned Blockchains are be-coming increasingly popular in business collaborations. Compared to the in efficient and expensive validation processes of public Blockchains, permissioned Blockchains are more suitable in stimulating business collaborations. As an example, the Hyperledger project, primarily driven by the Linux Foundation, aims to improve business processes and collaborations that involve multiple parties. Among the collection of projects in Hyperledger, Fabric serves a foundation. Compared to public PoW Blockchains, Fabric reduces the cost of consensus by implementing a Practical Byzantine Fault tolerant (PBFT) protocol, and leveraging channels for parallel and secure transaction processing. Channels allow participants to form virtual groups and keep their independent ledgers that are invisible to other channels. Channels provide the flexibility for business consortium to securely share information only to relevant parties. On a Fabric network, transaction ordering is handled by a central orderer that collects transactions submitted by committers and takes votes from endorsers for permanently recording transactions in blocks. The blocksize can be customized in either number of transactions or time of waiting. Chaincode is the equivalence of smart contracts in Hyperledger. All participating peers are required to execute all transactions and smart contracts individually for synchronization. The IBM Blockchain is built on top of Fabric. In addition, to further reduce the burden of Blockchain peers, some suggest that complex business logics should be moved to a separate middle layer beyond the Blockchain. For instance, Microsoft Azure is developing Cryptlets, where a central host executes smart contracts to support the separation of data and logic on permissioned Blockchains.

5. Benefit and potential application of Smart contract in realistic

5.1. Benefit of smart contracts

(a) 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, ownership of virtual resources with support for their transmission and atomic exchange can be realized. To do this, the following form of statements can be used:

1) "Participant X is an owner of resource A"; 2) "Participant Y proposes to exchange resource A to their resource B from participant X (or any other, or from the list)"; 3) "Participant X is agreed to the exchange of resource B to A from participant Y"; 4) "Participant Y cancel the offer of exchange of resource A to B from participant X". Statement "1" can be used for the transmission and creation of a resource. For atomic exchange, statement "2" can be used and followed by "3" or "4" in case of cancel the offer20. It should be noted that users could publish statements without having the necessary resource. Such statements should be ignored, and it is necessary to track who owns what resources, considering the entire history of the transactions to determine the invalid statements.

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.

(b) 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. Hence, changes cannot be easily implemented, once the contract is established. 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, anorganization 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.

(c) 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

(d) 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. 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.

(e) 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 shareholders22. 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.

Few innovations in the Blockchain world have been as revolutionary as smart contracts. A type of self-executing agreement where the terms between buyer and seller are directly written into the code itself, these mechanisms unalterable, almost impossible to hack, and helps guarantee that both sides to an agreement aren‘t ripped off.

Smart contracts also allow for more complex transactions to be carried out between two anonymous parties without the need for a central authority, enforcement system, or legal guidance. Essentially, this means that smart contracts can be programmed to enable a wide variety of actions.

5.2. Potential application of Smart contract in realistic

With a number of smart contracts bringing listed above, no one doubts their long-term staying power and ability to truly revolutionize the world we live in. Hence, Gartner – known as a global research and advisory firm providing information, advice, and tools for leaders in IT, finance, HR, customer service and support, communications, legal and compliance, marketing, sales, and supply chain functions, has estimated that by 2022, so called ratified unbundled smart contracts will be in use by more than 25% of global organizations23. There are many industries that can benefit from this kind of technology.

Public Smart Contracts

Public Blockchains enable convenient development and testing of smart contract applications or dApps. Public smart contracts make it possible for startups to raise funds through ICOs. Big enterprises on the other hand, mainly want to take the advantage of permissioned smart contracts for incorporating their models and enforcing business procedures. Some of the popular use cases include: banking, Electronic Medical Record (EMR), IoT data management. In addition, there are also other interesting applications such as smart waste management, real estate, and ride- sharing arcade city.

- Health Care and Medical Records: One major application area of smart contracts is related to healthcare and access control of medical records. Blockchain technology and smart con-tracts are seen by many healthcare professionals as a secure way of sharing and accessing patients‘ EMR. Smart contracts can feature multi signature approvals between patients and providers to only allow authorized users or devices to access or append the record. They also enable interoperability via collaborative version control to maintain the consistency of the record. Besides benefit patients and their care providers, smart contracts can also be used to grant researchers access to certain personal health data and enable micro-payments to be automatically transferred to patients for participation. However, the realization of these applications is limited by the immature infrastructure of most public Blockchains and high development costs. There are also concerns about policies and users‘ willingness to publicize their personal information.

- Identity Management: uPort is an identity management framework that leverages public Ethereumsmart contracts to recover accounts and protect user privacy in the case ofa device loss. The main component uPort identifier is a unique 20-byte7 hexadecimal string representing the address of a proxy contract that lies in-between a controller contract and an application contract. uPort enables users to replace their private key while maintaining an on-chain persistent identifier. If a valid user brings a new device, she can seek for approval from a list of existing recovery delegates, and replace the old user address with a new one. Similarly, Sovrin is a digital identity management platform built on a public Blockchain. Identity management frameworks using Blockchain still need to go through a number of enhancements before adoption. In the case of uPort, the publicity of the recovery delegates of a user poses the security risk of compromising user identities.

Permissioned Smart Contracts

Permission smart contracts has been used for the more sensitive business use cases such as banking, supply chain, Internet of Things (IoT) because the public smart contract has many risk threat to user privacy.I will talk about some of the permissioned smart contracts use cases below:

• Banking: Smart contracts can be used to enforcing rules and policies in banking, forexample, the mortgage service. According to a report made by Capgemini Consulting, with smart contracts in mortgage, consumers could potentially save 480960 USD per loan, while banks would be able to cut 3-11billion USD of annual costs in the US and Europe24. Banks can also use smartcontracts to streamline clearing and settlement processes. It has been reported that more than 40 global banks have participated in a consortium totest smart contracts for clearing and settlement activities. In addition,the know your customer (KYC) and anti money laundering (AML) policiescan also be embedded easily with the smart contract logic. However , the compatibility of legacy system with permissioned smart contracts is a big challenge and people have difficulty when expanding them. And the most important thing is secure against attacks thatare aimed at stealing of assets or tampering of the contract code.

• Provenance & Supply Chain: Blockchain can be used to enable some of the key properties in supply chainsand logistics including transparency, optimization, security and visibility of various operations in the transportation of goods. A supply chain with continuous, real-time access to reliable, shared data is more efficient than traditional supply chains. Provenance of the product via the blockchain also raises the bar on quality in production by reducing the risk of wastage and spoil age.Despite the advantages of using blockchains , the resistance from banks, exchange networks and trusted intermediariesmay also delay the blockchain adoption.

• Insurance: In the insurance industry, smart contracts can perform error checking, routing, approve workflows, and calculate payouts based on the type of claim andthe underlying policy. For example, the processing of travel insurance claimscan be automatically verified against flight delays or cancellations. Smart contracts can help remove the human factor involved in the process, there-fore decreasing the overall administrative cost for the insurers and increasing the transparency for the consumers. Nonetheless, technological limitations and legal regulations are major challenges to be addressed before shifting to smart contracts for insurance policies. Another drawback is the inflexibility of smart contracts. Traditional contracts can be amended or terminated upon agreement between both parties, but smart contracts as computer programs have no such mechanism. Moreover, more authorities are needed to recognize the legality of financial smart contacts.

Overall, smart contracts facilitate development of decentralized applications and have great potential to reshape business procedures.

• IoTA promising but controversial application scenario is the use of blockchainand smart contracts for IoT data management. Intuitively, as both systemsare decentralized in nature, blockchain could be used to enhance trust inIoT systems that constantly share and exchange a large amount of data.However, the other properties of blockchain and IoT do not seem to fit naturally together. Firstly, IoT data is often sensitive, and should not be sharedwith everyone else. Secondly, blockchains are resource-consuming. Even withlighter consensus mechanisms, having all IoT devices to execute all programsis redundant considering their limited processing capability. Similarly, Chain of Things is also trying to merge blockchainwith IoT to achieve security, reliabiltiy an interoperability.

6. Conclusion

Although smart contracts have great potential to reduce transaction cost and minimize outcome uncertainty, that currently can replace only the types of contractual provisions that can be represented in specific and objective terms, such as ―If X occurs, then execute step Y‖. Subjective provisions, such as whether a party used commercially reasonable efforts, cannot be translated into smart contracts. In this respect, smart contracts are not particularly ―smart‖.

In addition, smart contracts will often need to rely on external (for example: off-chain) resource before they can execute transaction. The reliance on off-chain resources; rather, that data must be ―pushed‖ to the smart

contract, so the parties need to agree on a single, definitive, off-chain resource willing to and capable of pushing relevant data to the smart contract. Without such clarity, there would not be consensus as to whether to the contract should trigger, and the transaction would not execute.

In order to address these issues, parties to smart contracts use ―oracles‖-trusted third parties that retrieve mutually-agreed off-chain information and then push that information to the smart contract at predetermined times. While oracles represent an elegant, and for the time-being necessary, solution to smart contracts' functional need to access off-chain resources, they introduce a potential point of failure in what might otherwise be a fully automated and decentralized transaction system. An oracle might cease conducting business, experience a system failure, be hacked, or provide erroneous data. Indeed, a hacker looking to impact smart contracts would likely have an easier time exploiting the oracle's data feed than hacking the smart contract itself.

Moreover, the disadvantages of the smart contacts limit their application in various are relating to technology often outpaces the law and the regulatory framework. This has been a noticeable trend with respect to smart contracts.

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. 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.

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. 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.

Traditionally, the establishment of a valid contract covers various constructs, which make it legally enforceable. We know 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. 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, the smart contracts is that breaches of contracts are rare to occur, as the execution of the contract is dependent on the predefined conditions which are also triggered by an event that neither of the nodes in the network has control over.

REFERENCES

i. *Riccardo de Caria, A Digital Revolution in International Trade, The International Legal Framework for Blockchain Technologies, Virtual Currencies and Smart Contracts: Challenges and Opportunity.*

ii. *Aaron Wright & Primavera De Filippi Decentralized, Blockchain Technology and The Rise of Lex Cryptographia.*

iii. *E Allan Farnsworth, _Comparative Contract Law' in Mathias Reimann and Reinhard Zimmermann (eds), The Oxford Handbook of Comparative Law (OUP 2016) 901; Arthur von Mehren, _A General View on Contract', International Encyclopedia of Comparative Law: Contract in General, vol VII/1 (Mohr Siebeck 2008) 19ff.; Caroline Bradley, _Private International Law-Making for the Financial Markets' (2005) 29 Fordham Int'l L.J. 127, 158f. Tapscott and D. Tapscott, ―How blockchain is changing finance,‖*

iv. *Harvard Business Review, vol. 1, no. 9, 2017 Tapscott and D. Tapscott, ―How blockchain is changing finance,‖*

v. *Harvard Business Review, vol. 1, no. 9, 2017*

vi. *Nakamoto, S., Bitcoin: A Peer-to-Peer Electronic Cash System, (2008), available at: https://bitcoin.org/bitcoin.pdf.*

vii. *Ametrano, F. M., Hayek Money: The Cryptocurrency Price Stability Solution, (August 13, 2016). Available at SSRN: https://ssrn.com/abstract=2425270 or http://dx.doi.org/10.2139/ssrn.2425270.*

viii. *(8) Digital Transformation in Government and Blockchain Technology, speech delivered by Minister for Cabinet Office Matt Hancock at D Digital Catapult, Kings Cross, London on the 26th April 2016. Available at: https://www.gov.uk/government/speeches/digital-transformation- ingovernment-and-blockchain-technology.*

ix. *Perugini, M. L. & Dal Checco, P., Smart Contracts: A Preliminary Evaluation, December 2015. Available at: https://ssrn.com/abstract=2729548.*

x. *Szabo, N., Smart Contracts, 1994, unpublished. Szabo, N., The Idea of Smart Contracts, 1997. Available at: http://szabo.best.vwh.net/idea.html .*

xi. *Richard R Orsinger, The Rise of Modern American Contract Law (2015) 1 www.orsinger.com/PDFFiles/the-Rise-of-American-Contract-Law.pdf.*

xii. *Vitalik Buterin, Ethereum White Paper (2014), http://blockchainlab.com/pdf accessed 22 January 2019; for a more detailed explanation of blockchain technology, see, e.g., Primavera De Filippi and Aaron Wright, Blockchain and the Law (HUP 2018)*

xiii. *Martin Fries, Smart Contracts: Brauchen schlaue Verträge noch Anwälte (2018).*

xiv. *Cardozo Blockchain Project, Research Report #2: „Smart Contracts‖ & Legal Enforceability‘ (2018) https://cardozo.yu.edu/sites/default/ .*

xv. *Christiane Wendehorst, Consumer Contracts and the Internet of Things in Reiner Schulze and Dirk Staudenmayer (eds), Digital Revolution: Challenges for Contract Law in Practice (Nomos 2016).*

xvi. *Stéphane Blemus, Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide, (2017) .*

xvii. *Under German law, the enforcement of such an act is governed by § 888 code of civil procedure (ZPO) which is regulating actions that may not be taken by others, cf. Merih E Kütük and Christoph Sorge, Bitcoin im deutschen Vollstreckungsrecht (2014).*

xviii. *The Law on Electronic transaction No. 51/2005/QH11 dated November 29, 2005;*

xix. *The Civil Code Law No. 91/2015/QH13, The Civil Code Law No. 91/2015/QH13;*

xx. *The Law on Postal services No. 49/2010/QH12 dated June 17, 2010;*