Blockchain and Smart Contracts

Manar Abdelhamid
The British university in Egypt
01091239674,+20
Manar.abdelhamid@bue.edu.eg

Ghada Hassan
The British university in Egypt & Ain Shams University
01002180606,+20
Ghada.hassan@bue.edu.eg

ABSTRACT

This paper presents an introduction to the current state of art of the Blockchain and Smart Contract technologies. Blockchain is a fast-disruptive technology becoming a key instrument in share economy. The Blockchain-based Smart Contract aim to automatically and securely execute the needed responsibilities of a contract without the support of a centralized execution authority. The Smart Contract runs on top of the Blockchain to facilitate, execute and enforce an agreement between un-trusted parties without the interfere of third party to trust it as this Smart Contract is an executable code that runs with rules on the Blockchain. Smart Contracts have some features that serve the goals of social justice and fairness. The paper presents the basic important information about the structures of the Blockchain and Smart Contract technologies and conduct a comparison between the different methodologies used in the Smart Contracts. The issues faced within the Smart Contract technology are surveyed. The four key issues are identified as: codifying, security, privacy and performance issues. We survey case cases of usage of the Blockchain in various business sectors like real estate, voting system and supply chain. The paper aims to assist a developer to grasp the big picture of the Blockchain technology and to further assist in the decision process of suitability of the technology to a specific application area.

Keywords

Blockchain; Smart Contract; Cryptocurrency; bitcoin; Ethereum.

1. INTRODUCTION

Transactions that occur in any traditional system happen in a centralized manner which requires the involvement of a trusted third party. This leads to security issues as single point of failure and high transaction fees. Starting with the first technology which is Blockchain, this technology has been invented and modified to tackle these issues that could occur in traditional systems [1]. Blockchain allow un-trusted entities to interact with each other in distrusted manner without the involvement of third party. The Blockchain is a distributed database that records all the transaction that occurs in a network. Blockchain was originally

introduced for the concept of Bitcoin which is the peer to peer digital payment system [2]. Then it was used for large decentralized range of applications. Also Blockchain has many applications that can be deployed on top, one of these applications is Smart Contract.

A Blockchain is a distributed ledger maintained by network nodes. It records all the transactions and then execute them over the nodes. This execution will be sent from one node to another. All the information inserted in any Blockchain according to the type will be public. These information cannot be modified or erased. Moreover, Smart Contract is self-executing contracts. These contracts are saved on the Blockchain in the form of line of codes. The media in the last period showed a huge attention to the Blockchain and its relation with the Smart Contract which started pointing to the Smart Contract as "the next big thing" .Smart Contract has a very big impact on the Blockchain as it helps in the process. The Smart Contracts are autonomy and trusted. What makes Smart Contract important part is the availability of various backup and accuracy. This will help in protecting personal information from getting lost [3].

Smart Contract is a new concept that has been introduced to be deployed on top of the Blockchain. Smart Contract is an executable code that runs with rules to facilitate and enforce the terms of agreement between untrusted parties to work together. This concept is deployed on a system that releases digital assets to all or part of the involved parties according to the terms and conditions agreed between them. Comparing the Smart Contract with the traditional contract, we will find that Smart Contract does not rely on third party to trust the operation which will lead to low in the transaction costs. While in the traditional contracts, you need third party and a lot of paper work to reach to the results you wants which will lead to high in the transaction cost. Blockchain can be applied on different platforms which help in developing smart contact. The most common platform is the Ethereum. Ethereum language supports a complete feature and easy use of Smart Contract that allow more creation and advanced customized contract which help in applying Smart Contract [2].

The review purpose is to identify the topics that have been carried out about Blockchain based Smart Contracts. Also it will address current challenges that need to be solved in future studies. To achieve this aim, we will do a review about the Blockchain and how Smart Contract affect it. This study will help in producing good comparison between the Smart Contract platforms, the pros and cons for each and the good knowledge about the more efficient platform to be applied in the Blockchain. This study will help identifying the gaps for any future study. The main objective is to explore Smart Contract from technical view. Also this review will give us an overview to help in answering the following questions asked by different companies as "Are there clear use cases exploiting Blockchain technology and Smart Contracts in

the different sector?", "In case we want to adopt a Blockchain, what is the most suitable Blockchain architecture for our needs?" and, more in general, "Is Blockchain technology mature enough for our needs as a company?". These questions will be answered by the explanation of the developer's point of view.

The paper aims to help a developer or a company to answer their questions about the maturity of Blockchain and Smart Contract by providing an overview of both based on use cases. The advantages and disadvantages of Blockchain and Smart Contract will be explained to give the company the ability to decide according to their needs for each technology in specific sector. Section two presents an overview of the Blockchain technology and Smart Contract. Section three discusses the proposed methodologies for Smart Contracts in the literature as well the use cases that apply the Smart Contracts in different sectors. Section four concludes by presenting advantages of Smart Contract within the Blockchain and all recommended new areas for any future work in this area.

2. Background

Transactions that occur in any traditional system usually happened in centralized way which requires the involvement of trusted third party. This leads us to a security issues as single point of failure and high transaction fees. Starting with the first technology which is Blockchain, this technology has been invented and modified to tackle these issues that occur from the traditional systems [1].

Blockchain allow un-trusted entities to interact with each other in a distrusted manner without the involvement of trusted third party. Simply Blockchain is a distributed database that records all the transaction that have occurs in a network. Blockchain was originally introduced the concept of Bitcoin which is the peer to peer digital payment system [2]. Then it was used for a large decentralized range of applications. Further Blockchain has many applications that can be deployed on top of it, one of these applications is Smart Contract.

As mentioned before, Blockchain is a decentralized system that exists between all parties, which will lead to no need to pay intermediates to help in the process. Applying Blockchain helps in saving time and conflict between the systems. Moreover, it is faster, cheaper and more secure than the traditional systems that are why it is important to start converting all the traditional system to decentralized system and depend on the Smart Contracts as well to reduce the amount of papers used to be more professional and secure. A Blockchain is a distributed ledger maintained by network nodes, it record all the transactions and then execute them over the nodes. This execution will be sent from one node to another. All the information inserted in any Blockchain according to the type will be public. These information cannot be modified or erased. Moreover, Smart Contract is self-executing contracts. These contracts are saved on the Blockchain in the form of line of codes. The media in the last period showed a huge attention to the Blockchain and its relation with the Smart Contract which started pointing to the Smart Contract as "the next big thing" .Smart Contract has a very big impact on the Blockchain as it helps in the process. The Smart Contracts are autonomy and trusted. What makes Smart Contract important part is the availability of various backup and accuracy. This will help in protecting personal information from getting lost [3].

Smart Contract is a new concept that has been introduced to be deployed on top of the Blockchain. Smart Contract is a code that runs with rules to facilitate and enforce the terms of agreement between untrusted parties to work together. This concept is deployed on a system that releases digital assets to all or part of the involved parties according to the terms and conditions agreed between them. Comparing the Smart Contract with the traditional contract, we will find that Smart Contract does not rely on third party to trust the operation which will lead to low in the transaction costs. While in the traditional contracts, you need third party and a lot of paper work to reach to the results you wants which will lead to high transaction costs. Blockchain can be applied on different platforms which help in developing smart contact. The most common platform is the Ethereum. Ethereum language supports a complete feature and easy use of Smart Contract that allow more creation and advanced customized contract which help in applying Smart Contract [2].

2.1 Use Case of Blockchain

Mark Zanella in [5] gave a simple use case that can clarify the concepts of Blockchain. If a user needs to transfer a specific amount of money from one participant to another, Blockchain will be the answer. How the Blockchain works will be described in the use case. So Alice makes a statement in which she specifies the amount to be transferred to the recipient [5]. Then a validation will be returned for Alice to notify her with the complete transfer. So Alice sends a message to the network that has the Blockchain in it. The network nodes will verify the message that it is actually sent from Alice by using the credentials of her. The next step is to check whether she owns the amount to be transferred or not. To check the amount Alice has, it is needed to check the local copy of the Blockchain then analyzing its incoming and outgoing transaction. This transaction will be stored in the past block. If all these actions are valid, then she is able to send the money to the other party then this transaction is added with any other transaction that is done in the same timeframe in the block.

In case a node needs to add a block to the Blockchain, it is needed to start solving a complex mathematical problem. This complex mathematical problem will have a number which is random combined with a numeric summary of the previous block; this will lead to provide the result. After doing all these process, the other party will receive the transaction needed easily. This example showed a good description for the characteristics of Blockchain. To sum up this use case, Blockchain has important point of view for the Blockchain characteristics as mentioned by Mark Zanella which is decentralized validation that validate the transaction performed from the network nodes without the need of any intermediaries. Also data redundancy is one of the main characteristics as a local copy of the Blockchain is found in the network node that prevents any data loss. Moreover Zanella added that all the modification and deletion of data stored in the Blockchain. The last characteristic of the Blockchain is the transparency. This allows everyone in the Blockchain read the chain and any transaction stored in it.

2.2 Types of Blockchain

According to Stefen K, there are three types of Blockchain and each have specific characteristics that depend on the need of the developer and the company [6]. The Blockchain types are public Blockchain, private Blockchain and consortium Blockchain. The

public Blockchain, any unknown user can join any information of the network, access all the content of the Blockchain and can also create transaction and send them. This unknown user can verify the correctness of the Blockchain as well. So Blockchains that could be readable and possibly writable by everyone is public. Stefen K gave examples of the public Blockchain which are Bitcoin, NXT and Ethereum. While the private Blockchain, only the known users that have permissions can join the network and perform actions in it [6]. The known user can write and send transactions to the Blockchain. Therefore Blockchains that is written only by members of the organization is private chain. The private network usually depends on the company that deploys the Blockchain in it. This company is responsible for giving the permissions to the user to join the network. In consortium Blockchains, this type is a set of selected nodes are related to different institutions that control validation. The Blockchain use it to share information among different participant among these institutions. Each Blockchain is useful in different domain, for example the public Blockchain is helpful according to the needs of the company, so when no central entity is available to verify a transaction, and full decentralization is needed. While using the private and consortium Blockchains useful in different way, such as lower validation costs and shorter validation times due to the smaller number of nodes and the mathematical problem could be simplified easily. Also these two Blockchain reduce the risk of attacks and increased privacy. So how to use each Blockchain based on the amount of decentralization required, and on time and cost constraints [6].

2.3 Concept of Cryptocurrency

Cryptocurrencies have appeared as the first generation of Blockchain technology. Cryptocurrencies are basically a digital currencies based on techniques. The most common example of Cryptocurrencies is Bitcoin. The other example is the Ethereum which have emerged as the second generation of Blockchain. Bitcoin is electronic payment systems that allow any two untrusted parties to do exchange money through digital currency in a secure manner without the intervention of middle man. Ethereum is the second generation of Blockchain that allows building complex distributed applications beyond the Cryptocurrencies. This crypto-currency (Ethereum) introduced Smart Contracts which are a way to perform action by rules defined in contract. The Ethereum is a public chain that has built-in language which helps any Smart Contract and decentralized application to be written complete and easy.

2.4 Blockchain Applications

Nedaa Bakar and Karamitoso illustrated that as Blockchain has many types, it also has many applications that it is applied in it. Bakar and Karamitoso said that different number of sectors already proposed to use this technology as in government sector and intellectual property [7].The Blockchain is used in the government to record for example the voting process. This is used to verify the voting process and to enable autonomous governance system.
Further, it is used in the intellectual property to verify the authorship of any document. Nedaa added that Blockchain could help in finance as it easily transfers money from one subject to another without the interference of confirmation from bank. Also she said that Blockchain helps in commerce, internet f things and

the most important part it participates in is Education. In the education sector Blockchain is used to store information on qualifications acquired by learners, also to reduce job application frauds [7]. Human resources staff could then easily use the Blockchain to obtain information about when and where a given skill was obtained.

3. Structure of the Smart Contract

Smart Contracts are a piece of code that is stored in the Blockchain network, this piece of code is on each database shared on participant network. The contract contains the conditions to which all the parties agreed to use. If these requirement conditions met the agreed actions, then this Smart Contract will execute. In different words, Smart Contracts are self-executing contracts. This contract has specific terms between buyer and seller directly. These terms are written in line of codes.

These codes and the agreements are included within a distributed, decentralized Blockchain network. Smart Contract provide trusted transactions and agreements to be carried out among anonymous parties without middle man to authorize the process.
So simply, if the Smart Contracts are stored on every computer in the network, if all execute, they must get the same result. By this way the user will make sure that any out result will be correct. So this piece of code that is stored on the Blockchain defines specific conditions that all parties use it and agreed upon it.

Maciej Hulicki said that as time passed, researchers have realized that Blockchain could also be used to store other kinds of assets, including pieces of code. Hulicki added that "it is the birth of Smart Contract". Smart Contract is small programs that stored in the Blockchain and automatically the conditions are executed when specific action is taken. Smart Contract idea was introduced to the market in the 90s with the Blockchain technology [8]. It was connected mainly to the Ethereum Blockchain because it is the most famous Blockchain after the Bitcoin. Through the Smart Contract Stefan K said that a person can encode his rules and conditions in the Blockchain through a piece of code that is programed on top of it. He explained though a very small use case which is if a person died then Smart Contract will automatically execute the contract to transfer the money, papers and all the related information to the beneficiary. By Smart Contract no need to the third party to validate or confirm any paper work for the transference [8]. In the 90s, Nick Szabo has introduced the term "Smart Contract". Valentina Gatteshu said that Smart Contract is a code program that identified by an address in the Blockchain network.

Smart Contract has one main component that is deployed in the Blockchain which is a set of executable functions and variables. These functions and variables run when it meets certain rules. Each function in the Smart Contract executes so the transaction occurs [4]. When the execution occurs, the status of the variables in the Smart Contract will change according to the logical implementation of the function. Gatteshu added that the language used in the Smart Contract implementation is quite complex. This solidity language is for Ethereum applications. So the code is compiled into bytecode once the complier executes it as solidity. The contract will be updated in the Blockchain after all these changed happened to it and a copy will be distributed in the whole database for all users. Any user in the Blockchain network can trigger the functions of sending any kind of transactions the code

of the contract will be executed on each node for each member to as part of verification of new block [4].

According to Christidis words, she said that any Smart Contract that is deployed on Blockchain can send messages to any other Smart Contracts. These messages will be composed and sent according to the sender address and the address of recipient. She added that there is a different between message and transaction. The transaction is produced by External Owned Account while the message is produced by a Smart Contract. Christidis added that there are steps for the design methodology of Smart Contract. The setup for the Ethereum nodes is required for any users. Then a well-defined functions and variable that meets the business needs, then the process itself from one user to another [9].

As mentioned before, Smart Contracts are a piece of code which is stored in the Blockchain network, this piece of code is on each participant database. It defines the conditions to which all parties using contracts agrees, if required conditions are met certain actions are executed. Smart Contracts can be developed and deployed in different Blockchain platforms. There are three public platforms that help in developing the Smart Contract. Each public platform has its pros and cons. Through this section, all the needed information about the platforms will be discussed. So the three platforms are bitcoin, NXT and Ethereum. Moreover, Smart Contracts were applied in some application like internet of things (IOT), music rights management and E-commerce. Also this part will show us how each of these application got affected by the Smart Contract and help in the enhancement of these applications. After developing all these, Smart Contracts have different kinds of issues that face while developing. These issues will be classified into four categories; the first category is the codifying part which is the challenges that are related to the development of the Smart Contract. The second part will be security, which are bugs or vulnerabilities that might utilize to launch as attack. The third part is the privacy in which disclosing the information of the user to the public. Then finally the performance issue where it may affect the ability of the Blockchain system and Smart Contract to scale.

3.1 Smart Contract Classification

Smart Contracts have many problems that face the developer while developing the Smart Contract. These issues are classified into four categories; starting with codifying, security, then privacy and ending with performance issues. These issues are discussed in many papers. According to Chiara and Nedaa, they proposed solutions to help in developing Smart Contract more efficient.

The codifying issues have four main problems that face the developers during the developing Smart Contract, which are, the difficulty to write correct contracts and the incapacity to modify or terminate contracts. In addition to that, the lack of support to identify under-optimized contracts and the complexity of programming languages. Starting with the first issue which is the difficulty of writing correct contracts. This issue is very important, the reason behind why this issue important is that Smart Contract in general has valuable currency unite that need to be tracked correctly. If it is not executed as it should be the currency unite could disappear which leads to lose of people's money and important information. So it is proposed to make the creation of Smart Contracts semi-automate to erase the process of writing Smart Contract. The semi automate Smart Contract is to convert the human readable contract into rules that should be followed to prevent any mistakes. Also these rules will be like a guideline for the developer to write a correct Smart Contract. Adding to this

solution, a final phase which is formal verification techniques which it detects the unintended behaviors of Smart Contract. The second issue is the hard way to modify or terminate Smart Contracts. Due to the high stability of Blockchain, Smart Contracts cannot be modified, changed or even terminated after the deployment has occurred into the Blockchain. This will take us to the opposite from the law, as legal low allows the rules to be modified or terminated. To solve this issue, it is presented as a set of standards to allow Smart Contracts to be changed or terminated. The third one is the lack of support to identify under-optimized Smart Contracts. To run a Smart Contract, each computational or storage operation in the contract costs some money. There is an under-optimized Smart Contract which contains unnecessary or expensive operations. The expensive operation results in a high cost for the user. To solve this high cost issue, there are some programing patterns which lead to unnecessary extra costs. Finally the last issue is the complexity of Smart Contract programing language. Any Smart Contract now is based on procedural language. In this language, the code is executed in a sequence of steps. This means that programmers should specify what is needed to be programed and how to do it before deploying the contract. This way will lead the writing of Smart Contract to dispose to errors. Nedaa expressed that to tackle this; it was proposed to utilize logic based languages instead of procedural languages [4].

Security issues in Smart Contract have five problems that face the developer. These issues are transaction-ordering dependency, timestamp dependency, mishandled exception, criminal activities, re-reentrancy and untrustworthy data feeds. In addition to these issues surveyed several vulnerabilities in Ethereum Smart Contracts. Chiara said that if two dependent transactions execute the same Smart Contract at the same block, the execution of the contract depend on the miner. At that time it is very easy for adversary to launch an attack if the order of the execution was done in right order and in the right time. To avoid this problem, it is suggested that the use of Ethereum based functions which is SendIfReceivedto enforce the order of transactions. Also it is proposed that using guard condition to return the expected output or fails will help in tackling this issue.

Another issue is the timestamp dependency. This issue occurs when a contract uses the block timestamp as a condition to trigger and execute transactions. The timestamp is usually set as the current local time by the miner who generated the block. The problem with timestamp is that if the miner is dishonest, the dishonest miner can lead to vary the value of the time for example 15 minutes from the current time Gatteschu said [4]. It is suggested that using the block number as a random seed for the contract instead of using the timestamp because the timestamp not fixed while the block number is fixed. There is another problem called re-entrancy vulnerability. This problem when a user is trying to call a function multiple times to do a repetitive withdrawal while the balance only charged once.

In the Smart Contract there are two privacy issues: the lack of transactional privacy and the lack of data feeds privacy. In the Blockchain system, all the transactions and the user's information and balance are available and public to anyone. This means that anyone can change in the information without any approval. Smart Contract mainly used more in the financial purposes. So this means that the financial transaction and the confidential information cannot be modified and changed only if the owner does. The proposed solution is the use of restriction code into the

Smart Contract that will prevent any unknown user change modify in it. The restriction code will lead to execute the code of the contract in private way which only the involved participants in that contract change it. The second issue is the lack of data feeds privacy. When a contract requires data feeds to operate, it sends a request to the party that provides those feeds. This request is public on the Blockchain. This means that everyone on this chain will be able to see the request.

According to Karamitoso, performance is another issue in the Smart Contract. The sequential execution of Smart Contract is a problem as you have to execute one at a time in the Blockchain. This execution will affect the performance of the Blockchain systems, as the number of Smart Contract that will be executed every time will be limited [7]. The growth of Smart Contract day after day is in great increase that Blockchain can handle so performance will be very low. The proposed solution is to execute the Smart Contract parallel as they won't depend on each other. By doing so, the Blockchain systems performance would improve as more contracts will execute per second.

3.2 Smart Contract Applications

Valentina Gatteshu explained the applications that Smart Contract used in. There are many applications where Smart Contracts can be applied to. Some of these applications already used in as internet of thing and smart property, music rights management and E-commerce [4]. First, Internet of Thing and smart property is shared between many people at once through the internet. IOT use case of Blockchain-based Smart Contracts allow different node to access different properties digitally without the interference of third party. Second, the music rights management which is a possible use case to record the ownership rights of a music in the Blockchain. Smart Contract plays important rule in music managements as any music will be used in any purpose, the owner will be rewarded, and this means that Smart Contract will enforce the commercial company to pay the owner with the right distribution. Third, E-commerce is a potential use case is to facilitate the trade between untrusted parties; these parties are the seller and buyer without a trusted third party [4].

3.3 Smart Contract Platforms

There are three main platforms for the Smart Contracts that have been applied on top of the Blockchain. The first platform is the Bitcoin. Bitcoin is a public Blockchain platform that can be used to perform crypto-currency transactions with a very limited compute capability. The second platform is NXT. NXT is a public Blockchain platform that includes built-in Smart Contracts as templates. its only allows the development of Smart Contracts using those templates however it allow the user to customize Smart Contracts due to the lack of Turing-completeness in its scripting language. The third platform is the Ethereum. Ethereum is a public Blockchain platform that can support advanced and customized Smart Contracts with the help of Turing-complete programming language. Ethereum supports all kinds of functions as loops, withdrawal limits, financial aspects and more.

4. Conclusion

Blockchain technology is a distributed database that records all the transactions that occur in a network. The main feature of Blockchain that is allows the communication between untrusted parties without the existence of a middle man. The Smart Contract is deployed on top of this chain. Another distributed application that is deployed on the top of the Blockchain is Cryptocurrencies. Smart Contract is an executable code that facilitate, execute and enforce an agreement between untrusted parties. Ethereum is currently the most common Blockchain platform for developing mart contract. There are still many technical gaps faced during implementation of the Smart Contract that needs to be addressed in future studies. Some of these gaps are identified in the literature with some proposed solutions. We grouped these issues into four categories, namely, codifying, security, privacy and performance issues. There are also a lack of studies on the scalability and performance issues of the Smart Contracts. In addition, there is a lack of studies on deploying Smart Contracts on different Blockchain platforms other than Ethereum. As well studies on criminal activities in Smart Contracts.

5. REFERENCES
[1] M. Paul, "what is the Blockchain and Smart Contracts? breif introduction," medium start up for Blockchain , USA, 2017.

[2] A. rosic, "Smart Contracts: the Blockchain Technology that will replace Lawyers," Blockgeeks, Italy, 2017.

[3] A. N. a. A. Miller, "Reserch for practice: cryptocurrencies, Blockchain, and Smart Contracts," in internet measurement conference , UK, 2016.

[4] K.Christidis, "Blockchain and Smart Contracts for the internet of things," in IEEE, North Carolina, 2016.

[5] S. Tikhomirov, "Ethereum: state of knowledge and research," University of Luxembourg, Luxembourg, 2016.

[6] M. A. a. A. V. Moorsel, "Blockchain based Smart Contracts a systmatic mapping study," in international conference on Smart Contract and cryptocurrency , UK, 2017.

[7] D. M. a. P. McBurney, "Validation and verification of Smart Contracts: a Reserch Agenda," in IEEE, London , 2017.

[8] K. B. a. S. Zanella, "Formal Verification of Smart Contracts," in symposium on principles of Smart Contracts , Vienna Austria, 2016.

[9] M. B. a. L. Pompianu, "An empirical analysis of Smart Contracts:platforms, applications, and design patterns," in IEEE, Italy, 2013.

[10] I. K. N. B. Maria papadaki, "Design of the Blockchain Smart Contract," Journal of infromation security, pp. 177-190, 2018.

[11] C. P. Valentina Gattechu, "Blochchain and Smart Contract for diffrenet domains: is this technology mature enough?," p. 16, 20 February 2018.

[12] S. K. Johansen, "A comprehensive Litrature review on Blockchain as a technological enabler for innovation," scientific reserch publishing, pp. 3-20, 2017.

[13] D. Hulicki, "The Legal Framework and Challenges of Smart Contract applications," Journal of infiormation security, p. 10, 2017.