ISSN 2347 - 3983
Volume 7, No. 12 December 2019
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter267122019.pdf
https://doi.org/10.30534/ijeter/2019/267122019

A New Era with Blockchain Technology in Saudi Arabia

Abeer A. AL-Otaibi, Mohammed A. AlZain, Ben Soh*, Mehedi Masud, Jehad Al-Amri
College of Computers and Information Technology, Taif University, Saudi Arabia
*La Trobe University, Bundoora 3086, Australia

ABSTRACT

Recently, digital developments have led to revolutionary new technologies such as the Internet, smartphones, smart machines and digital currency, and have changed culture and concepts around the world. Culture represents the identity of the human environment and the development and openness of society in the transmission of information and knowledge to generations. In both public and private sectors, sensitive information with the integrity of data should remain safe and confidential and cannot be infringed upon, which constitutes the underlying principle of the new technology, blockchain. To that end, in this paper we survey research related to blockchain in the last four years from 2015 to 2018. We then explore the implications of this new blockchain technology in the Kingdom of Saudi Arabia. On the basis of this study, recommendations on future blockchain technology research directions in Saudi Arabia are also provided.

Key words: Blockchain, smart contract, bitcoin, digital technology،cryptography.

1. INTRODUCTION

The use of technology has increased so that it has become a large proportion in our lives and led to deal with them in the areas of work [1] [2], study and communication with the outside world with ease and with the advancement of science, technology and knowledge will take over our lives [3]. where continuously produce new technologies that make life easier and better in dealings [4]. One of these techniques is blockchain technology, where it is a decentralized technology no one controls the processes through it which no intermediary or third party is involved. After the widespread spread that occurred after the revolution of Bitcoin technology, which is the first application of the blockchain system, where blockchain far exceeds that limited to cryptocurrencies can be applied in smart contracts, financial and bank transfers without any third party with full reliability and Safely, can keep personal information and display behind the nickname. We will learn about the stages of blockchain technology[5] [6]. The first stage used to support the first application was made on the Bitcoin currency and transactions through which such as financial transactions such as money transfer and payment without intermediary[7, 8]. The second stage combines Bitcoin currency and smart contracts to expand the use of blockchain in financial transactions and improve them in the replacement and automatic network movement[9, 10]. The third stage Blockchain technology has a wide range of fields ranging from financial and social administrators, art and culture, art and media, health [11] and other public realms, where it represents the challenge and competition of the traditional and the existence of a reliable third party central and will revolutionize the future and will change many and many rules of li [6]. This paper focuses on the survey of what has been reached in the past four from year 2015 to 2018 years. Moreover, also points out the future directions and on the suggestions and how to apply it in the Kingdom of Saudi Arabia.

This paper is organized as follows. In Section 2, we present the background of blockchain. Blockchain applications are deal with in Section 3, while Section 4 discusses the challenges and difficulties faced by blockchain. We provide a theoretical analysis of blockchain in Section 5 and future blockchain research directions in KSA in Section 6. Section 7 concludes this paper.

2. BACKGROUND

Blockchain is : A set of technologies and systems that are configured with encryption[12] [13, 14], computer algorithms, functions and mathematical problems to ensure the health and safety of access, this technology combines peer-to-peer networks and distributed consensus algorithms to solve synchronization problems from the distributed database. Manuel way moreover that almost impossible to penetrate because the data is formed in a series of blocks Saved p system and if he wants to modify the block with a specific cannot modify in other chains [15] [5].

2.1 Blockchain concept

We also pointed out that the concept of blockchain a set of techniques that include encryption [16], mathematics and algorithms and adopts a peer-to-peer system. Building integrated infrastructure in several areas and contains a complete list of transaction logs, i.e., they are linked sequentially from several blocks and each block is linked to the previous and referred to in an encrypted way, sign

transactions digitally using a public key Encryption, which uses two keys, consists of a public key and a private key, which are humid Mathematically each other. Because of his difficulty the math that has been used becomes very difficult for anyone trying to violate this information and guess this key, which makes it more complex and difficult to access them and more secure information. The first block in the chain is called Block configuration. Clusters are recognized by cryptographic hash values that are generated by an algorithm (SHA256). These hash values are part of the block header. The point is given to the mother and can move to the blocks of the children that the identity of the son deliberately on the mother and so until it reaches the grandchildren and grandchildren to be a generation of blocks. Hash. The hash function is one that takes input of any length and Publishes output with unique length. Any mass has fragmented data and any event or praise. For example, user X tries to change certain information recorded in the mass and this update will know about all the blocks and this increases the reliability of the blockchain system. [5, 17]. The following diagram fig.1[18] describes the structure inside a block and some of the coefficients that occur inside the block show us briefly what the structure is inside the block and how it is transmitted: [18]

- Prev Hash: Possible to be known as the mother block, which is the links of each block we enter data as shown within the previous block to the so-called hashtags function, as we have established that the hashtags function returns us the value and the value we will assign to the Prev Hash function in the new block.
- Timestamp: Its function is the time in which the block was found and also other tasks with respect to time eg for the time the data is being updated.
- Tx Root: The function of this field hash values to confirm and verify and repeat this method to be left only one entity and this field is known as another named Merkle [19].
- Version: There is a protocol version.
- Nonce: this is used in PoW which proves its role and the correct result that was reached, and we will talk about in details in section 1.3.
- Bits: This field shows us the difficulty in PoW will discuss in detail in section 1.3.

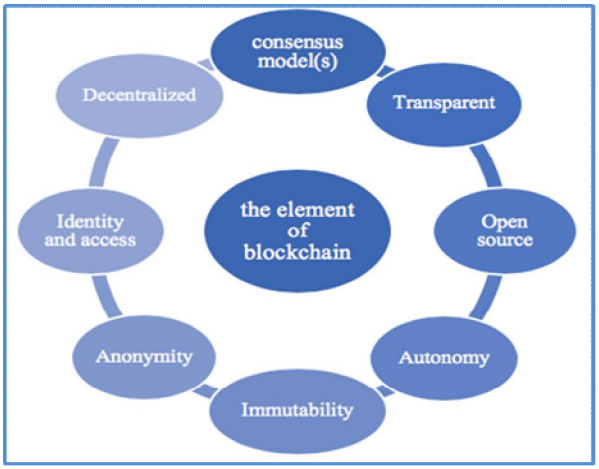

Figure 1: What it's Contains Inside a Block[5].

There are many elements of blockchain techniques and in this paper, we will discuss eight elements of blockchain are as follows: These elements are illustrated in Figure 2.

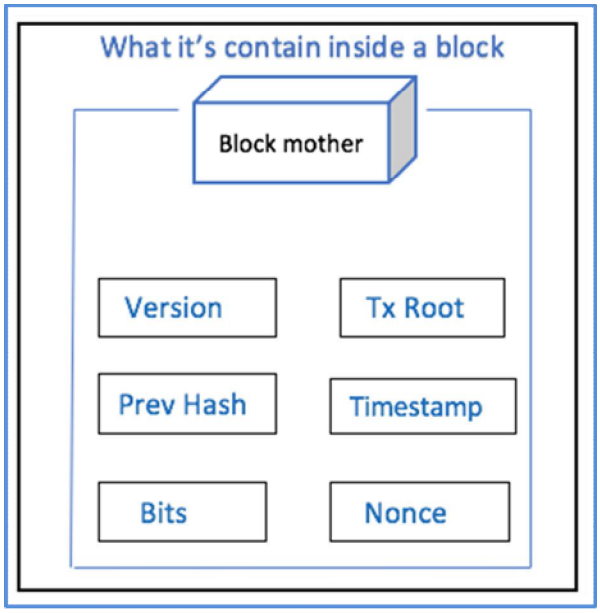

Figure 2: The Element of Blockchain, Adapted From[5].

Decentralized: In the sense that it does not depend on a third party or intermediary in transactions such as traditional systems and that all the transaction must be achieved from (the central bank in financial matters or the court in matters of contracts and transfer of ownership, etc.) Without a third party within the blockchain system where the information will be updated and stored data and deal with it easily [5, 17].

The consensus model(s): help maintain the sanctity of the data recorded on the blockchain. Nodes and other transactions will be examined [20]. So, it can be any counterfeiting easily detected. It states that consensus mechanisms and issues can be produced when the consensus mechanism including a blockchain fork, and consensus fail [21]. The consensus protocol has three characteristics that depend on applicability:

1-Safety: Consensus protocol must be safe and sound and free from defects and differences, in the sense that all nodes must produce the same output and is valid in accordance with the rules of the protocol.

2-Liveness: The consensus protocol effectively promises you all non-defective nodes
To give a valid value

3-Fault Tolerance: The consensus protocol provides authentication while providing recovery to a failed node of consensus sharing [5].
Transparent: record the data is transparent to each node and updates these are verified periodically at a specific time without a request or Permission and authorization, and this

verification and review corresponds to the self-review of the ecosystem with numerical values, which increases the reliability and security of blockchain technology system[5][17].

Open source: it means no users think anybody can access to their information's or them data because the blockchain system A decentralized available and public but It is true that the data is publicly registered but can hide the identity under the code or nickname and this increases the confidence [5, 17].

Autonomy: This is what distinguishes blockchain technology and makes it a leader and is considered a miracle is the independence and the transition from the idea of centralization to decentralization in many things that need confidence, security, confidentiality and privacy without interference or intermediary[5, 17].

Immutability: immutable means that it is not possible to remove and change the data, no matter how much time is spent, and can return to it in any time and found it, as in the case it is sound it did not happen been erased, deleted, altered, damaged, falsified, erased or altered its location. He will only be able to acquire it if he gets more than 51% of the node at the same time [5, 22].

2.2 Mechanisms of Blockchain

The core mechanisms of blockchain technology full into as follows:

1) New and recent data are recorded in the node that has been transferred and casting very widely in the network.

2) The role of receiving node it's examines the content of the message that it has received if the message is valid and allows it to be stored into a block and if it is incorrect, refuse it.

3) All receiving nodes in the network implement the work algorithm proof of work (PoW) or proof of stake (PoS) in PoW will discuss in detail in sections 1.3 and 1.4.

4) In the fourth and final step, after Implementation of the consensus algorithm it's mean the function consensus is that all blockchain nodes agree on the same message correctly and adding the new block in the chain will discussed in detail in Section 2.1, the block is stored in the chain, this means that each node in the network will accept and grant this block to enter and then be deployed and expanded on the chain base based on this block.

2.3 Proof of Work (PoW)

PoW proof of work is the first consensus algorithm that was used for this is the most famous in the mechanisms of consensus, and it is part of the data. It is the system responsible for the generation and creation of new blocks in addition to maintaining the security of the blockchain network through the mining process. PoW asks each node to find a difficult puzzle solution, the first node who is solve the puzzle will have this right to append the new block of the current series. In particular, before the solution imposes on all nodes where the verification occurred and put the transact formation such as mentioned in the previous section 1.1 Prev Hash and Timestamp, in a block. This puzzle is then solved, and then a secret value is guessed. This field is called nonce and is then placed in the block. All the information in the cluster header will then be combined together and interfered with the SHA-256 hash function [23]. If the result emerges below the defined T threshold, and is determined based on difficulty, then the secret value is accepted. Other than that, the node must make another guess for the secret value, until he finds the answer. After adjusting the difficulty of the puzzle After appending all the 2016 blocks, the average speed for adding a new block in the chain is 1. Figure 6 describes the handle handling value that you guessed. Thanks to the use of SHA-256, guessing makes the value very difficult. PoW as a mine, the work of searching for a suitable nonce is called mining [18].

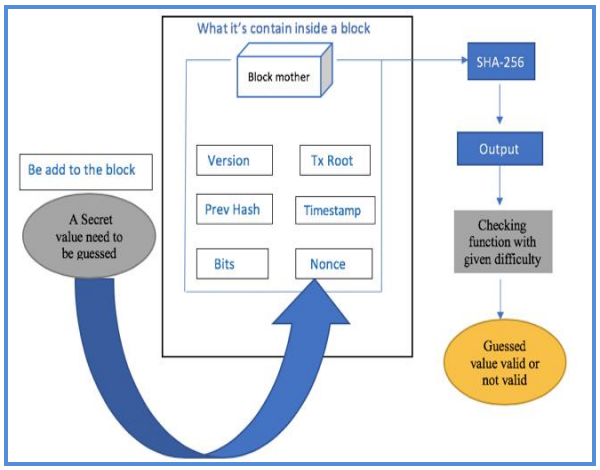

Figure 3: The Nonce Handling Process: Presumed Hidden Value. Adapted from [18].

2.4 Proof of Stake (PoS)

Proof of Stake (PoS) it's a protocol which it is a proof that a user can mine or examining transactions in a block depending about what user have amount the user holds. It does not require expensive computing power that is the result of wasting a lot of electricity like PoW. Provides more protection such as malicious attack that may affect the network. that it's mean Proof of Stake trusts when the person has a lot of currency involved, that it's mean his protocol trusts that if person have more currency involved, becomes less vulnerable to attack. the Miners in PoS must evidence the Royal strengths to show the amount of money that if people have more currency involved, becomes less vulnerable to attack. But, this choice it's consider is unjust based on the looking from the wealthiest one in the network, in which it explains the protocol it is in details and with examples to understanding [24]. here is the role of PoS to deal with this disparity. It is then presented and discussed first in the Bitcoin Forum of 2011 [18]. PoS had some variables and research

contributions to this. The basic idea of consensus algorithms was to use the quota to determine who would get it and PoS had some variables and research contribution to it, and the idea was used. This quota is essential for consensus algorithms to determine who will get a chance to close the next set of series. If you own a large stake you will become more confident. No one wants to do any fraudulent business to attack the chain that contains a lot of his profits. In addition, the use of PoS requires attackers to have at least 51% of all the risks in the network to execute a double spending attack, which is very difficult, which combines PoS and PoW.

2.5 Proof of Stake (PoS)

Blockchain types are divided into three types:

1) Public blockchain: Without permission and publicly open to everyone enables anyone to join and participate. Without a third party, you can write, read, verify and obtain consensus with confidence figure 3 describe public blockchain.

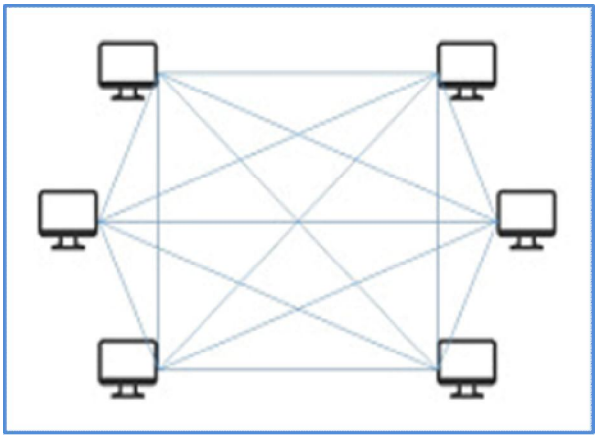

Figure 4: Describe the Public of Blockchain.

2) Consortium blockchains: A node that has authorization and has power can be selected in advance. In addition to having some business partnerships, we categorize the data in blockchain into two open and special types, and this group is partially decentralized. Examples of the consortium are R3CEV and Hyperledger. Fig4. Describe the consortium of blockchains.

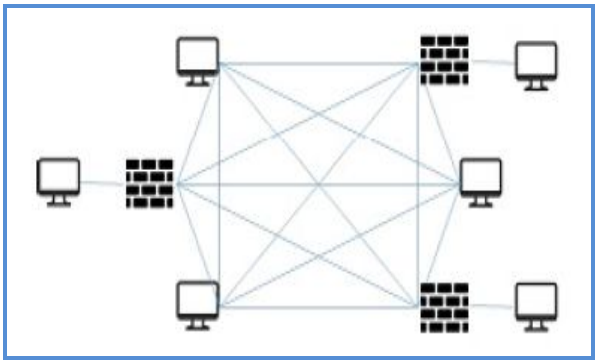

Figure 5: Describe the Consortium of Blockchain.

3) Private blockchain: Here the node will be bound and limited, no one can participate in any node in blockchain, that is the data has a strict management access to it where it cannot be allowed to unauthorized and this indicates the rigor and authority exercised. Fig5 describe private of blockchain. Away from the concept of the types of blockchain and the characteristics of each type only to want and need public blockchain for its comfort and in some blocks such as privet blockchain or consortium require privet control. Fig6.describe the Privet of blockchain.

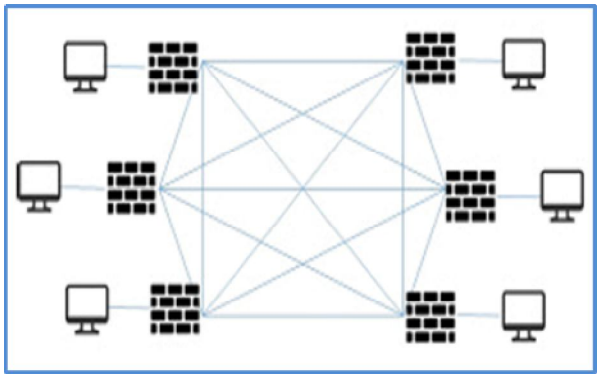

Figure 6: Describe the Privet of Blockchain.

3. APPLICATIONS OF BLOCKCHAIN

The reason for the revolution that has made blockchain the modern world is that Blockchain technologies can be used in many areas and felids, and not only in financial application, but also in other industries that we will learn in this section.

A.Digital Currency: Bitcoin

The first appearance of the blockchain world is the spread of the cryptocurrency revolution in Bitcoin, it does not need a central bank and online payment system and is more anonymous through regular electronic transfers. In the Bitcoin design all transactions and data are kept in the general ledger, so the sender and receiver of each transaction are identified only by the keys, which are two encrypted public key. This leads to a common misconception it inherently provides anonymous use [25] .

B.Smart Contract: Ethereum

Smart Contract is a digital contract that will instantly conduct the digital assets of the user formulating the right and duty of a user. The implementation is automatic and not only that the normal procedure on the computer, but deeper than that where he is one of the participants in the contract due to several things, the most important of which is the response to the message received and also store data in addition to it could also send messages or send outside. A smart contract defined as series of code on a blockchain which is defined by a specific address. Includes a list that can be applied of functions and state variables. When transactions are made to these functions, the functions will be executed. The transactions include criteria of input which are required by the contract functions. For variables in the nodes change status depends on several things, the most important of which is the application

of logic and the implementation of the system on the function. Contracts can be written in different languages of the highest level (such as Solidity and Python)[26, 27]. Smart contract language compiler optimizations (such as Serpent and Solidity) it's used for converting contracts to byte code. Once the contracts have been compiled, they are submitted to the Blockchain network, which creates the contracts exclusive addresses. Ethereum: Ethereum is a Blockchain platform that is open and programmable[28]. It is possible to create a wide range of applications or services or can also create different contracts on the platform and is using its digital currency known as called ETH[28, 29]. Smart contract must be important things and elements such as time that increase the reliability and success of the contract. the Ethereum Virtual Machine it's situation time an implemented for smart contract in Ethereum Virtual Machine (EVM) it's time setting for smart contracts in Ethereum.in addition all nodes in Ethereum network turn on in(EVM). The operation of how it runs as a box containing sand and provides an implementation environment that is isolated. Every node in the Blockchain network implement the same installations as smart contracts provide redundancy in execution. Although this huge count of repeated is not an effective method to implementation but if there is no centralized authority or trusted third party, consensus must be maintained in the network.

C.Hyperledger

Founded in late 2015 by the Linux Foundation, it has approximately 130 members in a wide range of industries[30]. It uses robust architecture and identity characteristics, that depend on the specific CLIs and REST APIs. Moreover, it uses modular architecture with interoperability protocols.

4. Blockchain challenges and difficulties

It is well known that anything in the beginning will face difficulties and challenges and will not be accepted until after prove the extent of confidence, guarantee and future it examples one of them it’s blockchain technology faces future opportunities as it can acquire and reduce the meaning of the mediator and central in addition to the challenges. Some challenges and difficulties can be overcome only as the technology matures and develops and enhances it in the future. This will lead to many future opportunities for blockchain application to be accepted. Challenges and difficulties will be discussed in the section as well as future opportunities in the next section. Challenges are to prove and ensure in the most important aspects such as security, confidence and confidentiality and we will look for the most important in the blockchain.

Security concerns: The worries the world and makes any new technology unacceptable at the outset is the guarantees and the integrity of their data and confidentiality of information. The most important feature of blockchain technology is the security of data and the way to access data in a blockchain network is essential. Blockchain network access and data can enforce the need for authentication execution for authentication and authorization. Data encryption can provide the organization with protection against breach of data security and control of data access in a blockchain network. Public and private keys are used together with data encryption to obtain a very high level of security. One of the most important and vital aspects of information systems is to maintain data consistency and integrity. Blockchain ensures user data integrity based on the basic characteristics of proof and tracking. The integration of sequential segmentation and encryption makes it very difficult for any user or nodes in the network to tamper with the data in the blockchain**.**

Scalability: : This means the ability to increase the use of blockchain, of course, will increase the number of daily transactions, so the size of the blockchain will be huge and all transactions will be stored and saved in each node and then be able to validate and validate the source and validity of the current transaction before the transaction. The blocks in the blockchain can create a problem in delaying the transaction and this is in the case if there are small transactions, understand that miners prefer to validate transactions that cross the larger limits. As stated in [31], the solutions proposed in the issue of scalability are that we can categorize block blocks into two categories: storage is improved as well as redesigning blockchain. The database will be saved with the rest of the non-empty addresses. Furthermore, a lightweight client can be used as an alternative to the scalability issue [17] .

Privacy leakage: Of course, blockchain can be exposed mainly to cross-border privacy leaks because the fact that details and monitoring of all public keys are visible to the world in the network. Proposed solutions so that we can achieve anonymity in major groups are broadly categorized in mixing solution and anonymous solution. Anonymous means a service that unlinks the payment assets of a transaction to prevent analysis of the transaction graph as mentioned in [31].

.

Selfish mining: Selfish Mining is a challenge facing Block. A block may be prone to fraud if a small fraction of the fragmentation strength is used. The miners retain the mined blocks in Selfish mining without transmitting to the network and establish a private branch that will only be transmitted after certain criteria have been met. In this situation, honest miners are wasting a lot of time and money when Selfish miners are mining the private chain.

Personal identifiable information: Personal identi Possible Information (PII)it's any information that could be used to set free the identity of an individual. [32] Discuss in details Privacy Policy on Communication and Location.

Security: Security when talk about Security means a lot of definitions it could be terms of confidentiality, integrity and availability as discussed in [33]. It is ever a brave in the open networks like as public blockchains. Congeniality is low in deal systems that fake information through its network. integrity is the sequences métier, although many problems remain. Because of broad replication, accessibility in blockchains is high in terms of readability relative to writing availability. Because of these properties, the 51% majority attack is more theoretical in a large blockchain network.

5. THEORETICAL ANALYSIS

Blockchain is the most important characteristic and enjoyment of the characteristics, which led to the revolution and questions of the world is decentralization and this introduces us to a new concept and a new world as this concept poses a problem and lack of acceptance of it and also their lack of confidence and can be rejected and not receptive, decentralization denies the existence of something natural and usual and reliable and is central Decentralization provides us with the means of rest and wait of several steps that may reach days and months in the central and may lead to delays in things that cannot tolerate this delay, but as a reliable source is currently accepting this solution despite its bad aspects. And that decentralization corrects all aspects of the bad in addition to several features to keep pace with the development and advancement in technology, but it will be unacceptable at first because of their trust and ignorance of it and their expectation and perception that it is insecure and vulnerable to violation and theft and disclosure of data and information. . So, in [28, 29] [5] [21] it was clarified the decentralization of the blockchain and its definition and features that are not known to all and it may be the beginning of the journey in the coming years. Then he mentioned some of the applications that have been implemented in blockchain, the most important of which is Bitcoin, which launched the blockchain revolution, where the technology was known blockchain after the revolution Bitcoin, a digital currency payment decentralized network managed by its users without any central authority or intermediary or third party, where the availability of a fully integrated electronic payment system and money that is traded via the Internet only, which made the world know what Bitcoin and where it came from and the method of transfer is done using addresses only where you can own a private address or get several other address[15]. Discuss the beginning and origin of Bitcoin. That's there was someone called Satoshi Nakamoto in 2008 and issued an open source code in 2009 and then Satoshi Nakamoto disappeared from the world of forums but continued popularity and encryption in 2013, where the reason behind the popularity and continuity of Bitcoin is his popularity is the startups and also sites, which were due to investment [17]. After Bitcoin was recognized and traded with many companies and sites, Bitcoin reached a lot of attention and attracted tremendous successes with profits of up to $ 10 billion in 2016. Smart contracts are also an important application and a strange name and a bit confused because it is actually and not a real contract as some believe that it is not something that needs to be complied with or endorsed. Contract in part of the agreement, law and order can be used to hold it accountable, and this is quite the opposite in a smart contract. A smart contract is not supported by anyone, it's a set of self-executing instructions and commands. In the sense of a smart contract, only software is able to send transactions to other accounts on a blockchain without any interference from any central party, broker or third party. [26, 27] Smart contracting tools rely on reliable security servers. The Smart Contract concept seeks to achieve the original vision of the parties that interact with a reliable and secure virtual computer and implement programs that contain data and information[17]Smart contract is considered to be part of the code as it can be automatically implemented by miners, as it is currently possible to achieve many functions in many areas such as banking. Smart contract research has been classified into two types: The development is the development of intelligent contract ie the development of intelligent contract platform and the second type is evaluation in the sense of code analysis and performance evaluation. Cryptocurrencies are divided into two types which are those that can and should be mined [PoW] in the sense of extraction and pre-established. The basis of both types are the mechanisms of working in blockchain technology. It relies on solving complex mathematical equations to preview the units of coefficients. These resolved mathematical issues are part of the encryption process and in turn protect transactions from unauthorized access. [17]The working guide (PoW) is known as a consensus strategy used in a grid where each node in the grid calculates the hash value of a cluster header that is constantly variable since consensus requires a condition that the result be equal or smaller than a given value. The decentralized network requires that all participants must calculate the hash value continuously and also using different variations to reach the desired target. Then, these transactions will then be validated in the new cluster. [9] All verified nodes are required to place verified transactions, then add other information such as PrevHash and also Timestamp into a block. Proof-of-Stake in order to make such cryptocurrencies, super-powerful computers are not needed [17]. Proof of ownership uses a formula that in turn searches for the lowest hash value with the quota size, and if there is a 50% owner representing all coins, he will no longer be able to control the creation of new blocks on his own. Sometimes the quota is other things. Compared to PoW, PoS offers more power and more efficiency [18].Using PoS requires an attacker to possess at least 51% of all the risks in the network in order to be able to attack a double spend, which makes it clear to us that it is very difficult.

In the table 1 shows in detail the beginning of the blockchain where it started in Bitcoin, which launched us the blockchain revolution, which led to the expansion and the multiplicity of applications where it was applied in smart contracts and also

the mechanism of action blockchain as well as types of blockchain and how to maintain the identity of the individual and cannot appear in his name and forget the most important Blockchain, which makes it different and distinct from jealousy, is decentralization and non-intervention of a third party.

A survey showed that the use of blockchain has reached a turning point, and that exploration is towards building practical business applications. Hence the questions and the search for answers by the most rigorous, realistic and logical executives. The questions show us that conscious and logical and explain that technology is ready. Executives need to know what and how to use this technology for them. Survey demonstrates wide and varied use cases and applications unlike last year through a wide range of sectors. The answers show a balanced view of expectations and fears to the contrary from last year. Blockchain is still a subject of controversy that is likely to be accepted and rejected and may change and show the opposite. Those who answered no soon change their answer after watching the blockchain keep pace with the evolution and offer better strategies in the future. Naturally, the future cannot be accurately predicted and how it will be, but we may put some questions. This question was asked (Deloitte's 2019 Global Blockchain Survey) and the answers were collected in general about which group is making the key decisions in blockchain as nearly half of those respondents indicated that it was professional as the group was making the key decision on blockchain, but it could be enhanced in blockchain realization that it was a technology-based and evolutionary solution. There are also about a third of respondents pointing out and citing senior management that the emergence of technology as a focus-solving strategy. The diagram describes these questions and their answers in general and approximate percentage. As reported by Deloitte's 2019 Global Blockchain Survey Show the result of their answers to the survey question in the fig.7. **The of question survey was:** which area of your organization or project is making the key business about its blockchain activities?[34]

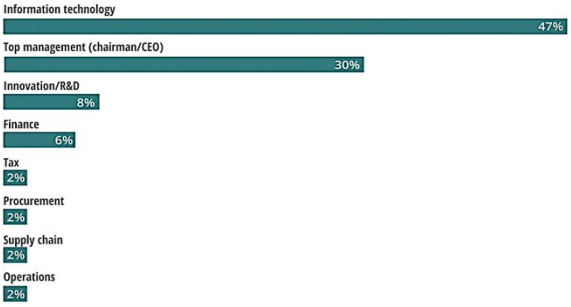

Figure 7: Result of Their Answers to the Question of Survey. adoptive from [34].

We know that the most important applications of blockchain and its revolution are smart contracts and a question was asked about the importance of smart contracts and their utility to your organization according to (Deloitte's 2019 Global Blockchain Survey) and the answer most respondents which It's been about 58% believe that one of the capabilities of blockchain and it will form a future and a great benefit to them. The question of survey according to Deloitte's 2019 Global Blockchain Survey: How important are smart contracts to your organization or project as a potential benefit of blockchain? See the result of their answers to the survey question in the fig.8[34].

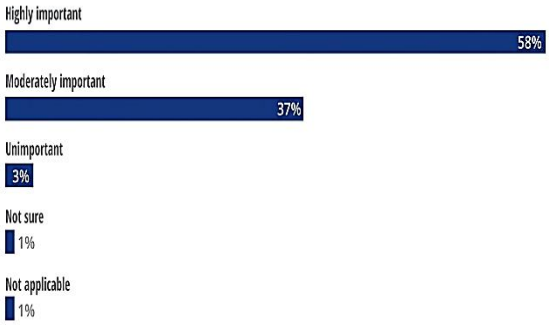

Figure 8: Result of Their Answers to the Question of Survey adoptive from [34].

6. FUTURE WORK: SUGGESTIONS APPLICABLE IN KSA

We seek to provide a mechanism for future work in order to provide a stable and safe in general in the world and specially in KSA after we have learned about a new technology called Blockchain about its importance and its applications, we will review in this section and highlight its importance and how to apply them in Saudi Arabia. Can be applied in many of our applications such as applied in financial matters such as banks and real estate where there will be a development and a huge evolutionary leap in the Kingdom and we will get rid of manual papers and waiting hours that may take time and delays in our transactions. If applied in real estate will save a lot of trouble and fatigue in going to a real estate office and then hold it manually and pay the amount to the third party and then ratified and this takes time and money and effort, but with blockchain will save us all the trouble.

7. CONCLUSION

Overall this survey highlighted the blockchain technology. It includes all aspects of the structure of the blockchain and the mechanisms of how blockchain works. Types of blockchain are also reviewed with respect to some of the consensus algorithms used in Blockchain, which are divided into two basic types: evidence-based consensus and algorithms based on voting. Based on the two most important applications of blockchain, viz. Bitcoin and smart contracts, we discussed how to apply and develop blockchain in the Kingdom of Saudi Arabia based on the characteristics of the blockchain and peer-to-peer decentralization. This decentralized characteristic has a large and tremendous ability to conduct many operations for many users and this is what we want to provide for processing in KSA institutions.

		Application of blockchain			Types of blockchain			Mechanisms of blockchain work	
Year	Decentration	Smart contract	Bitcoin	Hyperledger	Public	Consortium	Private	PoW	PoS
2015	√		√		√		√		
2016	√					√			
2016	√	√		√	√	√	√	√	√
2017	√				√		√		
2018	√	√	√	√	√	√	√	√	√
2018	√	√	√		√	√	√		
2018	√	√	√	√	√		√		
2018	√							√	√
2019	√	√	√	√	√	√	√	√	√

Table 1:. Related Work on Blockchain.

REFERENCES

1. Alzain, M.A. and E. Pardede. *Using multi shares for ensuring privacy in database-as-a-service*. in *2011 44th Hawaii International Conference on System Sciences*. 2011: IEEE. https://doi.org/10.1109/HICSS.2011.478
2. AlZain, M.A., et al. *Cloud computing security: from single to multi-clouds*. in *2012 45th Hawaii International Conference on System Sciences*. 2012: IEEE. https://doi.org/10.1109/HICSS.2012.153
3. Alsaif, S.A., et al., *From Learning Management Systems to a Social Learning Environment: A Comparative Review and the Implications.* International Journal of Smart Education and Urban Society (IJSEUS), 2019. **10**(1): p. 1-18.
4. Samra, H.E., et al., *A Conceptual Model for Cloud-Based E-Training in Nursing Education*, in *Knowledge-Intensive Economies and Opportunities for Social, Organizational, and Technological Growth*. 2019, IGI Global. p. 295-310.
5. Huynh, T.T., T.D. Nguyen, and H. Tan. *A Survey on Security and Privacy Issues of Blockchain Technology*. in *2019 International Conference on System Science and Engineering (ICSSE)*. 2019: IEEE.
6. Glaser, F., *Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis.* 2017.

7. Mettler, M. *Blockchain technology in healthcare: The revolution starts here*. in *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*. 2016: IEEE.
8. Huckle, S., et al., *Internet of things, blockchain and shared economy applications.* Procedia computer science, 2016. **98**: p. 461-466.
9. Swan, M., *Blockchain thinking: The brain as a decentralized autonomous corporation [commentary]*. IEEE Technology and Society Magazine, 2015. **34**(4): p. 41-52.
10. Wei, P., et al., *Blockchain data-based cloud data integrity protection mechanism.* Future Generation Computer Systems, 2019.
11. Samra, H.E., B. Soh, and M.A. Alzain. *A Conceptual Model for an Intelligent Simulation-Based Learning Management System Using a Data Mining Agent in Clinical Skills Education*. in *2016 4th International Conference on Enterprise Systems (ES)*. 2016: IEEE.
https://doi.org/10.1109/ES.2016.17
12. Faragallah, O.S., et al., *Block-based optical color image encryption based on double random phase encoding.* IEEE Access, 2018. **7**: p. 4184-4194.
13. AlZain, M.A. and J.F. Al-Amri, *Application of Data Steganographic Method in Video Sequences Using Histogram Shifting in the Discrete Wavelet Transform.* International Journal of Applied Engineering Research, 2018. **13**(8): p. 6380-6387.
14. AlZain, M.A., *Efficient Image Cipher using 2D Logistic Mapping and Singular Value Decomposition.* INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, 2018. **9**(11): p. 196-200.
15. Garay, J., A. Kiayias, and N. Leonardos. *The bitcoin backbone protocol: Analysis and applications*. in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. 2015: Springer.
16. Alzain, M., *Chaos Baker-based Image Encryption in Operation Modes.* INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY, 2018. **17**(1): p. 7153-7163.
17. Zheng, Z., et al., *Blockchain challenges and opportunities: A survey.* International Journal of Web and Grid Services, 2018. **14**(4): p. 352-375.
18. Nguyen, G.-T. and K. Kim, *A Survey about Consensus Algorithms Used in Blockchain.* Journal of Information processing systems, 2018. **14**(1).
19. Merkle, R.C. *A digital signature based on a conventional encryption function*. in *Conference on the theory and application of cryptographic techniques*. 1987: Springer.
20. Swanson, T., *Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems.* Report, available online, Apr, 2015.
21. Yan, M., et al. *Data aggregation scheduling in probabilistic wireless networks with cognitive radio capability*. in *2016 IEEE global communications conference (GLOBECOM)*. 2016: IEEE.
22. Halaburda, H., *Blockchain revolution without the blockchain.* Bank of Canada Staff Analytical Note, 2018. **5**. https://doi.org/10.2139/ssrn.3133313
23. Akarca, D., et al. *Blockchain Secured Electronic Health Records: Patient Rights, Privacy and Cybersecurity*. in *2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT)*. 2019: IEEE.
24. Larimer, D., *Transactions as proof-of-stake*. Nov-2013, 2013.
25. Fleder, M., M.S. Kester, and S. Pillai, *Bitcoin transaction graph analysis.* arXiv preprint arXiv:1502.01657, 2015.
26. Kosba, A., et al. *Hawk: The blockchain model of cryptography and privacy-preserving smart contracts*. in *2016 IEEE symposium on security and privacy (SP)*. 2016: IEEE.
27. Bahga, A. and V.K. Madisetti, *Blockchain platform for industrial internet of things.* Journal of Software Engineering and Applications, 2016. **9**(10): p. 533.
28. Watanabe, H., et al. *Blockchain contract: Securing a blockchain applied to smart contracts*. in *2016 IEEE international conference on consumer electronics (ICCE)*. 2016: IEEE.
29. Gencer, A.E., et al., *Decentralization in bitcoin and ethereum networks.* arXiv preprint arXiv:1801.03998, 2018.
30. Pustišek, M. and A. Kos, *Approaches to front-end iot application development for the ethereum blockchain.* Procedia Computer Science, 2018. **129**: p. 410-419.
31. Zheng, Z., et al. *An overview of blockchain technology: Architecture, consensus, and future trends*. in *2017 IEEE International Congress on Big Data (BigData Congress)*. 2017: IEEE.
32. Elmaghraby, A.S. and M.M. Losavio, *Cyber security challenges in Smart Cities: Safety, security and privacy*. Journal of advanced research, 2014. **5**(4): p. 491-497.
33. Mendling, J., et al., *Blockchains for business process management-challenges and opportunities.* ACM Transactions on Management Information Systems (TMIS), 2018. **9**(1): p. 4.
https://doi.org/10.1145/3230712
34. Deloitte, *Deloitte's 2019 global blockchain survey*. 2019.