Australian Journal of Basic and Applied Sciences
2019 September; 13(9): pages 34-41
DOI: 10.22587/ajbas.2019.13.9.3
Original paper
Journal home page: www.ajbasweb.com
AENSI Publications

Application of Blockchain Technology for Secure Data Transactions in Organizations

Abeer AlSereidi[a], Khalid Almarri[b]

[a,b] The British University in Dubai, Project Management Department, Faculty of Business and Law, PO Box 345015, Dubai, United Arab Emirates.

Correspondence Author: Dr Khalid Almarri, The British University in Dubai, Project Management Department, Faculty of Business and Law, PO Box 345015, Dubai, United Arab Emirates.

Received date: 18 June 2019, Accepted date: 23 September 2019, Online date: 29 September 2019

Abstract

The application of Blockchain technology in organization is continuously gaining momentum. Yet, minimal attention has been directed to the application of the Blockchain technology for secure data transaction.
The study will investigate how Blockchain can be used for secure and private data transaction across organizations
This is a qualitative phenomenological study. Data collection was conducted through purposive sampling g the targeted staff of five hospitals in Dubai that apply the Blockchain technology in service delivery and interviewing them. Data was collected through audio recording of the responses from participants, transcribing them and recording the results in a table. Discussion of results/qualitative analysis was conducted through reference to the interviewee responses and discussing their implication
The study findings shed more light on the application of Blockchain technology in ensuring securing the shared data and ensuring that authorized people do not get access. Other aspects that the project identifies include core concepts of Blockchain technology and its organizational application with emphasis on secure data transaction/information sharing, specific problems that organizations can apply block-chain technology to resolve, and challenges of using Blockchain technology in securing data transactions in organizations.

Keywords: Cyber security, Blockchain, Healthcare organizations.

INTRODUCTION

Technology has always been utilized by organizations positively. Currently, the application has increased significantly making most organizations to restructure and incorporate the changes that have been brought about by the changing technology (Gococo, 2017). The introduction of Blockchain technology has had a significant impact on organizational performance. According to Mainelli and Smith (2015), Blockchain technology is a growing list of documents, stored in blocks and whose security is guaranteed using mutually distributed cryptography shared between all nodes present in a system. The technology allows the transfer of digital information without a possibility of copying, editing or leakage unless one is given access. It, therefore, became the backbone invention of the online transaction.

Blockchain technology is an ingenious and revolutionary invention that is transforming the internet and online activities in a big way. Since its inception, it has become a significant inspiration to the development of online currency and bitcoin, owing to its ability to share information securely without chances of copying or corrupting it (Ahmed, 2017). Today, technologists are weighing its application in many organizations to serve a wide range of functions, one of them being information transaction. Despite its increased application in the various fields, its potential as a means of secure data transfer has not been tapped exhaustively. Therefore, this research paper will analyze how Blockchain technology can be incorporated in various organizations as a secure method of data transfer.

Blockchain Technology and Data Transaction

The information that is stored in a Blockchain remains as shared, meaning that it is accessible to different organizations and users over the internet provided that they have accessibility rights. According to Mainelli and Smith (2015), the stored information is subject to consistent reconciliation. Most importantly, the information has no central location point, which means that the data is public, and does not require central authority or a third party, thus increasing integrity. Millions of computers host the data

Citation: Abeer AlSereidi & Khalid Almarri., Application of Blockchain Technology for Secure Data Transactions in Organizations. Australian Journal of Basic and Applied Sciences, 13(9): 34-41. DOI: 10.22587/ajbas.2019.13.9.3

simultaneously thus eliminating a chance of having a single source of an original version of data. It, therefore, makes it difficult for hackers or saboteurs to corrupt it since its origin is not centralized.

Sharing information across organizations is a crucial strategy that has the potential to enhance their performance and effectiveness (H. C. B & Irvine, 2016). One of the major concerns affecting data transactions/information sharing across organizations relates to privacy concerns. Many organizations may also be reluctant to share information since such actions may compromise their competitiveness. Additionally, the complexity of organizational data is itself a challenge in the implementation of secure data sharing system across organizations.

The aim of this study is to investigate how Blockchain can be used for secure and private data transaction across organizations. The research will focus on how Blockchain technology can be applied by organizations and be a solution to the increasing danger to the privacy of organization data through hacking or any other form of unauthorized entry. In the end, the paper will make a recommendation and suggest ways through which organizations can utilized to improve the privacy and security of data during transfer.

LITERATURE REVIEW

Blockchain is a new technology that has invited a lot of interest among researchers and scholars alike. Researchers have in fact developed prototypes to test its applicability in various fields including hospital data, banking, law firms among others (Mendling et al., 2017; Kosba et al., 2016).

Smart Contracts

Kosba, Miller, Shi, Wen, & Papamanthou (2016) describe that businesses and individuals can use blockchains in smart contracts technology. As such, mutually, distrusting parties enter into contracts without the need for a third party. The smart contracts work in such a way that if one of the sides breaches the contracts, the decentralized blockchains ensures that the honest party gets a commensurate compensation after the breach (Kosba et al. 2016). The smart contracts are computer coded contracts with the potential of self-enforcing when a party tries to breach the agreed terms, and they can monitor external inputs from trusted sources such as financial exchange, meteorological services with the aim of settling contracts as precisely as stipulated (Peters and Panayi, 2016).

For example, taking a bitcoin transaction as an example of a simple contract for transferring a specified amount of digital currency (bitcoin) from an account to another, on a specific condition say for instance if dollar to euro rate reaches a particular point with a period. The smart contracts will monitor the situation of the forex, and if the conditions are met, the block chains will automatically transfer the amount to the instructed account. The block chains are permanent unless the parties instruct it to self-destroy (Peters and Panayi, 2016). Therefore, organisations can utilize the block chains in smart contracts. Blockchain technology is also used in controlling ownership of property or assets as in 'smart property'. The property can be shares of a company, land, car, house, etc. The data contained is considered as secure and privacy of involved parties upheld (Wang, et al, 2016; Ramachandran, et al. 2017).

Cloud Storage

Other than financial application, institutions such as hospitals and law firms are finding Blockchain technology a useful method for storing data (Crosby, Pattanayak, Verma, & Kalyanaraman, 2016). Crosby et al. (2016) explain that Blockchains are in essence a distributed database of records shared among the participants. As such, they note that block chains are used to store legal documents, health records, marriage licenses, private securities digitally by storing fingerprints of the digital asset rather than storing the digital asset itself. The data is encrypted and stored in the block chains in cloud storage servers safely and with utmost security, and with an assurance that the data cannot be tampered with or altered (Shrier, Wu, & Pentland, 2016). Therefore, researchers agree that organizations can use Blockchain technology for safekeeping of their sensitive data safe.

Digital Currency

The origin of block chains was an invention of crypto-currency such as bitcoins, bitshares, and lite coins. These are digital currencies, and they can be used to settle transactions, pay employees, buy goods among other deals. These transfers work using open source key cryptology, one being public and the other private. According to Blundell-Wignall (2014), bitcoins move from one public address to another public address, but the receiver needs a secret key to decrypt the bitcoins to a usable form. Both private and public keys are alphanumeric strings that are formed from a sophisticated encryption process, which uses a "hash" function to derive numbers and letters randomly to create the public and private keys necessary for the transfer or decrypting the coins (Back et al., 2014). The receiver stores the coins in an online mobile wallet but can as well transfer them in an offline wallet known as cold storage to minimize the risk of hackers targeting private keys stored in the hard drive (Micheler & von der Heyde, 2016). Therefore, Blockchain technology allows online transaction with crypto-currency for buying goods, paying for services among other operations.

Decentralized Consensus

Blockchain consists of standards and regulations concerning how every node in the chain exchanges information. The entire system works to ensure that only valid information gets in and that just legit transactions get in only once through decentralized security and consensus (Shrier, Wu, & Pentland, 2016). In the system, nodes stored in the system have the responsibility of maintaining decentralized security and agreement in all transactions. Then, the system splits data and stores it in different nodes,

Citation: Abeer AlSereidi & Khalid Almarri., Application of Blockchain Technology for Secure Data Transactions in Organizations. Australian Journal of Basic and Applied Sciences, 13(9): 34-41. DOI: 10.22587/ajbas.2019.13.9.3

which then collaborate to compute functions without leaking information between the nodes (Shrier, Wu, & Pentland, 2016). The researchers say that each has a piece of meaningless data if used individually. Therefore, they conclude that by decentralizing data use and control, no individual party in the system can manipulate data or even delete making the data secure safe and valid.

Block Chains as Distributed Ledgers

A Blockchain is distributed ledger held publicly and contained information about a transaction and all parties involved in the traction throughout the history of the transaction (Vukolić, 2015). The researcher describes that the Blockchain consists of hash chains of blocks, with records of the genesis block and then transactions or movements of the bitcoin or data with its predecessor. This string is vital as it provides a proof-of-work since every member of the chain gets a notification concerning certain transactions or changes in some information (Luu et al., 2016). Sending the transactions back to other users ensures that each record or transaction that a person changes can be validated traceable, and secured by using keys and signatures. The result is a record of strings of the transaction for accountability, which one can only equate to ledgers.

Safe and Secure

The Blockchain is an incorruptible and secure system that can be used for storing and transacting online with no risk of attack. The system puts all participants on an equal footing who jointly trust proof of work, form rules and enforce them together, which in return scraps off the need for a central body for ensuring the security of transactions or data in the system (Dilley et al., 2016). Further, the system has the "…ability to cryptographically verify other participant behaviors, enforcing rules based on mathematics that anyone can check and no one can subvert" (Dilley et al., 2016, p. 1). Therefore, as Luu et al. (2016) notes, the system is safe, secure, accurate, and verifiable because no one can alter or change the transactions once the system records it.

Hash – Providing Authenticity

Every block in the chain is divided into two sections referred to as the header and the transaction part. The header's content is the previous block information (hash), and it acts as a reference to the mixture that came before it. In addition, it contains information about the current block, data, which will serve as the connecting information for the next block (Back et al., 2014). This makes the blocks hard to change and easy to verify, thus giving it authenticity because the information in each block has a string from which the source can be traced.

Suitability of Block Chain Given Its Current State

Among the most critical factor in determining the appropriateness of Blockchain as it is today is to analyze its ability to cope with massive transaction loads. VISA which is a universal payment system handles about 4000 transactions every second, but with a capacity of up to 47, 000 per second (Trillo, 2013). In comparison with the Blockchain ability, it is only capable of handling seven transactions every second given the fact that Blockchains can carry a maximum size of 1MB (Beck et al., 2016). This is a clear indication that if Blockchain were to operate on a large scale, then it ought to increase its capacity and match the global standards.

Furthermore, Beck et al. (2016) describe a challenge they noted using a prototype they created for Blockchain technology, as block time. The researchers explain that the waiting period for a transaction was 12 seconds, which is far beyond many transaction platforms available today. The current technology and internet allow systems to process transactions almost immediately (Beck et al., 2016). Blockchain, as it is now, has a time lag of 12 seconds meaning that it needs a lot of improvements before it can be rolled out.

Nonetheless, Kosba et al. (2016) developed a prototype dubbed Hawk as a decentralized smart contract system that does not store the chain's transaction in the open as the bitcoin technology does. The Hawk intended to determine a way that Blockchain would have transactional privacy. Other than providing transactional privacy, the researchers describe this prototype as having the potential to allow a Hawk programmer to write smart contracts intuitionally without relying on cryptography. Besides, even without relying on cryptography, the Hawk was able to generate an effective cryptographically protocol in situations that users decided to interact with the system using, "…cryptographic primitives such as zero-knowledge proof" (Kosba et al. 2016, p. 839). So far, there are several prototypes of Blockchains that need improvement for them to be successfully applied for business.

CHALLENGES OF USING BLOCK CHAINS

Network Reliability and Throughput

On yet another prototype, Ali, Nelson, Shea, & Freedman (2016) describe the challenges they faced using their Namecoin Blockchain while transacting 200,000 transactions and updating 33, 000 on their system. First, are network reliability and throughput. The number of entries depending on the throughput of the underlying Blockchain, meaning that the number of updating new registers or updates relies on the number of transactions sent and confirmed over a given period. Besides Mendling et al. (2017) confirms this but explains that the situation may be worse particularly when there is congestion and poor network signal (Mendling et al., 2017; Nelson, Ali, Shea, & Freedman, 2016). This would consume a lot of time putting in mind that a typical Blockchain consumes 65 minutes to be sure that the transaction is safely in the ledger (Mendling et al., 2017). As such, the reliability of the system was compromised because the Blockchain system could not perform transactions consistently.

Selfish Mining

Citation: Abeer AlSereidi & Khalid Almarri., Application of Blockchain Technology for Secure Data Transactions in Organizations. Australian Journal of Basic and Applied Sciences, 13(9): 34-41. DOI: 10.22587/ajbas.2019.13.9.3

Second, block chains have the potential for selfish mining. In the mining of bitcoins, which is similar to recording or mining data in block chains, exhibited signs of greedy mining attack. This means the participants in the system rejected some blocks and then an abrupt increase in blocks after working selfishly (Ali et al., 2016; Umeh, 2016). Also, the researcher describes that in the production of block chains of say for instance data related, there were signs of selfish mining behaviors regardless of whether the attack was deliberate or not.

Consensus-Breaking Changes

Finally, consensus-breaking changes is also a significant challenge. Ali et al. (2016) note that some significant updates such as changes to name pricing need everyone in the net to update their software. It is difficult to get all the players in the system to upgrade their systems because they want to make extra profit. Other than working with a prototype, block chains have general challenges that institutions may encounter for both currency transactions and data systems.

First is the endless ledgers. This challenge poses a significant problem particularly in auditing because one node may take 1-3 days to download, verify and boot up (Ali et al., 2016). Second is the limit of data storage. Blockchains cannot typically hold much data, and they are only in the order of Kilobytes. This means that all nodes must record all the copy of the Blockchain, which in return consumes a lot of space (69GB) to synchronize (Ali et al., 2016). Other challenges include limited bandwidth and slow writes which makes the usability potential of the Blockchain a challenge (Mendling et al., 2017). Further Blockchains have a challenge of security mainly because the system is a public network (Mendling et al., 2017). Confidentiality and security are not guaranteed because block chains replicate data all over the net.

RESEARCH METHOD

In a bid to achieve the objectives of this research, qualitative approach was applied. This approach is essential for offering considerable variability in the methods applied for data collection and offers a chance to apply the mixed-methods approach (Bryman and Bell, 2011). Additionally, qualitative data cannot only assess theory but also allow the application of other theoretical ideas. Rudestam and Newton (2015) indicate that qualitative studies have the potential to implement the data analysis, sampling perspectives and instrumentation which are normally more accurate and opposite to the viewpoints of the people undertaking more conventional inquiries. In essence, qualitative study seeks to collect simplified and clear information that includes the primary perspectives of individuals that would be, otherwise, overlooked by other approaches. The qualitative research designs that are normally used include case study, grounded theory, phenomenology, narrative and ethnography (Rudestam et al., 2015). This study employed the phenomenology design.

From a philosophical point of view, phenomenology is defined as the framework for research that provides the capacity to offer a humanistic point of view (Roberts, 2013). This qualitative approach describes the lived experiences, with the focus on identifying the manner in which individuals, with experience in a phenomenon, can pass the knowledge to those without such experiences. Contrary to the conventional cause-and-effect models associated with the quantitative models, the phenomenological qualitative approach yearns to identify the humane subjectivity in addition to real-life experiences (Gee, Loewenthal, and Cayne, 2013). Therefore, interviewing a sample of health care staff from the sample hospitals that use the Blockchain technology unravels the importance of its role in securing data transactions in organizations rather than forming abstract theories through quantification methods.

When conducting a study that features human beings, the risk of causing unexpected harm is a high likelihood, meaning that all pertinent safety precautions should be considered (Yin, 2016). Once the researcher has ascertained that the methodology is accurate and cannot affect the respondents, he/she is supposed to ensure that all respondents have read, understood, and signed the consent forms.

Data collection was characterized by a qualitative phenomenological study that involved interviewing the targeted staff of five hospitals in Dubai that apply the Blockchain technology in service delivery. According to Bryman and Bell (2011), qualitative interviews allow the expression of the point of view of the researcher as well as new ideas. Semi-structured interviews were applied in the study whereby a series of questions were included to ensure comparison in terms of roles, individuals and hospitals. However, a certain level of flexibility was applied to ensure that any important extra view from the respondent was included in the interview. Although questions for the management were different from those of other employees, they were all linked to the previous research as seen in the literature review regarding the topic. Since the study will contribute to the existing literature on the topic, the semi-structured interviews ensure that the arising issues from the literature are addressed while the findings will make essential recommendations for practice.

The proposed study focused on health care facilities in Dubai i.e. hospitals that apply the Blockchain technology for any function. In this regard, data collection was conducted using purposive sampling. Bryman and Bell (2011) argue that purposive sampling is characterized by the use of a strategic sample, relevant research questions and sample population. Sampling the organizations involved in the research was a form of convenience sampling since the sample was based on the availability and whether they had installed the Blockchain technology. Interviews were collected from the management and staff of the care hospitals with a view to exploring the details of the application of this technology from the users. Before undertaking these interviews, a request to the hospital regarding the intention to undertake the study was made. Then, the target hospital staff were then contacted and furnished with the specifics of the study. Finally, the interviews were scheduled at a mutually convenient time. Data was collected through audio recording of the responses from participants and then transcribed by the researcher and the results recorded in a table. Discussion of results/qualitative analysis was conducted through reference to the interviewee responses and discussing their implication. A semi-structured interview guide was created to ensure that the interviews were within the intended scope, providing the researcher with the ability to inquire more and discover more topics. More of the interviews lasted for approximately 45

Citation: Abeer AlSereidi & Khalid Almarri., Application of Blockchain Technology for Secure Data Transactions in Organizations. Australian Journal of Basic and Applied Sciences, 13(9): 34-41. DOI: 10.22587/ajbas.2019.13.9.3

minutes, with face-to-face, Skype, video call and calls being the mode of communication. Interviews held face to face were conducted in the offices within the respective hospitals. The consent for recording the conversations was first sought from the participants.

Data analysis was approached through the focus on qualitative data procedures as outlined by Vaismoradi et al. (2016) and Miles, Huberman, and Saldana (2013). Miles and his colleagues see the need for disclosing all the steps and techniques involved while Vaismoradi and his colleagues some researchers fail to analyze their data properly leading to inaccuracies and inconsistencies. The collected data was transcribed through the used of TranscribeMe. The transcribed data was verified through listening to the recordings against the transcript. The data collected in audiotapes will be affixed with pseudo to protect the identity of the respondents.

RESULTS AND DISCUSSION

Uses of block chain technology

Respondents associated Blockchain with many uses in a hospital setting. According to respondent #1, #4, #5, & #18. Blockchain technology is the most secure means of entering into transactions, whether inter-organizational or when dealing with payments from individual patients.

Interviewee #1 "…use of Blockchain has significantly improved the way we offer services and relationships with our business partners. One of the essential aspects of Blockchain technology that aids in smooth financial transactions is smart contracts. Once we get into a financial contract through the smart contract, the other party cannot default since the decentralized block chains cover us…"

This response is in tandem with what has been observed in the review whereby smart contracts are revolutionizing organizations in the various economic sectors (Kosba et al. 2016; Peters and Panayi, 2016). With such an application, it would be much easier for hospitals as well as health care organizations to perform their operations efficiently and conduct business without the risk of losing resources. Secure data transactions are ensured through the use of smart contracts since Blockchain technology enables a consensus to be distributed among member parties. Thus, every transaction involving these digital assets can be verified without compromising the confidentiality of the data and that of the involved parties.

Interviewee #18, "…when pre-agreed conditions among participants in these 'smart contracts' are met, then the members can automatically make payments as per the contract. This allows transparency and confidentiality of the 'smart contract' and terms…"

In fact, according to the IT specialists (#20, #17, #16, #13, and #9), the main reason for the installation of the Blockchain technology is majorly technological:

Interviewee #13; "Nowadays, my main role is to ensure that this technology works, especially its security function. I would say that this is the main reason why I am still working here."

The security of stored data, especially the patient information, is ensured through the utilization of the cloud storage. The interviewees affirmed that the application of Blockchain technology has greatly assisted in solving the monumental challenge of unauthorized access to patient information.

Interviewee #6: "…I have always had security problems in the past before this hospital started to use the Blockchain technology to store patient information. Before its installation, I would assure patients of information safety but deep down, I knew that unauthorized access is possible through hacking. However, things are better now with Blockchain…"

The IT specialists indicated that although the system is based on open standards that normally pose many security threats, Blockchain technology has a tamperproof system. The feature allows data accessibility while ensuring integrity and safety without the need for third parties. The open standard allows access to patient information anywhere and saves the costs related to travelling and carrying of physical documents especially in situations where the patient is seeking medical assistance from a different hospital/doctor. Privacy/security for the stored information in Blockchain technology is ensured through encryption and storing information in safe cloud storage servers with utmost security. This is one of the most important roles of Blockchain technology that has also been mentioned in the literature by various researchers such as Crosby, Pattanayak, Verma, & Kalyanaraman, (2016); Crosby et al. (2016) and Shrier, Wu, & Pentland (2016) among many others.

Another use of the Blockchain technology identified by the interviewees is safe settlement of financial obligations. In essence, the technology is used to settle transactions, buy goods, services, and pay employees among other roles. According to the executives (#1, #5, #12 and #18) that were interviewed in this study, use of bitcoins is a milestone since Blockchain system is equipped with safety measures that prevent hacking.

Interviewee #5: "…well, any system is prone to compromise especially when the users do not take the required safety precautions. However, Blockchain has so far proven to be relatively impenetrable to other transactional systems…"

Thus, in addition to curbing theft, the Blockchain technology helps to keep the details of any financial transactions private and only accessible to the authorized parties. The technology's capacities to ensure privacy was explained by one of the IT specialists briefly:

Interviewee #13: "…the mobile wallet minimizes the risk of hacking the private keys located in the hard drive…".

Core concepts of Blockchain technology for secure data transaction

Although most of the respondents did not understand much regarding the technical bit of the Blockchain technology that is essential for secure data transactions, the IT specialists pointed out some of the core concepts.

Citation: Abeer AlSereidi & Khalid Almarri., Application of Blockchain Technology for Secure Data Transactions in Organizations. Australian Journal of Basic and Applied Sciences, 13(9): 34-41. DOI: 10.22587/ajbas.2019.13.9.3

Interviewee #9: "…the system ensures that only the valid information is permitted to pass through. This means that the contents of the transactions and information that is being fed must agree with the security systems configured in the Blockchain technology; otherwise, the information will not be allowed in…"
In this regard, once the valid information and legit transactions have been permitted in the Blockchain systems through a consensus, the information is redistributed for storage in the various nodes without compromising its integrity. The secured information cannot be manipulated or deleted once it is securely decentralized in the system.

Block Chains as Distributed Ledgers
According to interviewee #3, another core aspect of Blockchain technology that makes it essential for secure data transaction is its ability to capture personal details of the users.
Interviewee #3: "….once the personal details are captured, tracking is made possible. Every person in the chain is also provided with a notification of the transaction or any form of changes made…"
Notifying other users regarding a new transaction ensures that they are updated about any changes as well as the identities of the persons accessing the stored data. In fact, interviewee #4 and #14 (hospital clerks) equates the Blockchain with a ledger. This is because it contains distributed information and the details of all the parties involved are recorded. This allows authorized persons to access all the information that they require from just logging in.
Interviewee #14: "…since the installation of the Blockchain, it has been easy for me since I easily access all information required; technically, I perform all my roles in a digital platform thanks to Blockchain…even the security lapses and unauthorized entries that always compromise the integrity of the stored information has greatly improved under the new technology… "
These responses confirm the findings of Vukolic (2015), Luu et al. (2016) and Dilley et al. (2016) that Blockchain not only acts as a ledger, but as a safe haven for records. All users are given a chance to participate in securing data by engaging everyone in the formulation and enforcement of rules. In essence, the system eliminates the need for a regulatory body that secures information. This aspect of Blockchain technology bestows a sense of personal responsibility of all users to information integrity, especially in a hospital set-up where the security of patient data is highly pertinent. Notably, the ability of the Blockchain technology to utilize cryptography is one of the major aspects that upholds data security.
Interviewee #9: "….the fact that the system can cryptographically verify the behavior of the users, and generate information based on the statistics that no person can be allowed to change makes it safe…"
Technically, every block in the chain has a head-section that connects it to the previous block, and transfers information along the chain. In essence, the chain is interconnected and all the information can be traced to a specific string. This interconnectivity makes the information stored in the Blockchain technology easy to verify and difficult to change.
Interviewee #17: "…although I am not completely privy to the specific details technical aspects of this technology, it is amazing how all the information accessed can be traced to the source whereas at the same time it cannot be change unless you are authorized to do so. Frankly speaking, the technology has really attracted my curiosity to the extent that one of my future endeavors is to attain expert skills regarding its use…"

Challenges associated with use of Blockchain technology
This study has found out that the Blockchain technology is characterized by various challenges. One of the major challenges to effective application of this technology is its limited ability to handle large loads of transactions. According to the IT specialists (#16 and #17), its capacity is relatively low and with its increased application, this might create many problems if not rectified.
Interviewee #16: "….less than 10 transactions in a second are not adequate. This is a technology that is expected to be applied in large scale in the future; its capacity should be therefore exceptional…"
The waiting period for transactions was also noted to be relatively long compared to other transactional platforms. This, however, does not mean that Blockchain is among the slowest transactional technologies only that it is not the best among the best. Another challenge associated with the application of Blockchain technology is the lack of skills among users. The hospital workers that were interviewed termed lack of skills as one of the reasons that makes it difficult for them to apply this technology.
Interviewee #14: "…although the technology has proven to be highly effective in ensuring privacy and security of data, I am yet to completely understand how it operates. Some of my roles involves checking and filling in patient information on the technology, meaning that being conversation with this technology is highly paramount…"
Implementing the consensus-breaking changes is also a challenge since some significant updates such as changes to name and pricing require all system users to update their software. Updating is a process that sometimes takes a lot of time. Therefore, convincing all the players to upgrade is a problem since they are all intent in utilizing the available time to make more profit. Finally, the installation of this technology is not a guarantee of an automatic safety to the stored data. Safety precautions must be applied, meaning that hospitals have to ensure that the required measures are upheld at all times.

RECOMMENDATIONS, FUTURE PROSPECTS AND CONCLUSION

There is a need to ensure that health care workers are well equipped with skills on how to apply the technology since one of the major challenges is the lack of skills. Additionally, hospitals have an obligation of ensuring that the Blockchain remains secure through checking it regularly for any bleaches: otherwise, the technology will not serve its intended purpose. For instance, there should also be a series of digital access signatures only available for authorized persons, meaning that access can only be possible through the signature. Ensuring that the patient information in the Blockchain is secure requires the contribution of every user. In this regard, all users are supposed to be informed that they have a responsibility to maintain safety and integrity.

Citation: Abeer AlSereidi & Khalid Almarri., Application of Blockchain Technology for Secure Data Transactions in Organizations. Australian Journal of Basic and Applied Sciences, 13(9): 34-41. DOI: 10.22587/ajbas.2019.13.9.3

With the current expectation that many institutions are looking forward to utilize it in their daily operations, there is a need to upgrade the Blockchain's capacity that meets the global standards. In fact, its capacity should exceed any other transaction platforms since its application in the various sectors is expected to increase significantly.

Blockchain technology is experiencing constant changes at all spheres of its application. In this regard, there is a need to encourage further research through the introduction of Blockchain technology related topics in conferences and promoting more research ideas on the technology. From this research, it is clear that more technology is required in both the academia and innovation strategies. The advantages and disadvantages of this technology should be communicated more while its application outside the cryptocurrencies is supposed to be communicated more.

The objective of this thesis was to investigate how Blockchain can be used for secure and private data transaction across organizations. A lot of progress has been made in block chain technology during the period when the thesis was being written. From the study, it is clear that Blockchain technology is essential for secure data transactions across organizations. It can be described as a database of records spread among parties or public ledger of all transactions carried out and which is shared among member parties. Every transaction must be verified by majority consensus of the members and once carried out; transaction cannot be deleted or altered. This technology has made digital information and records unchangeable and permanent. It facilitates data collection, authentication, and management that are trustworthy.

Reliance on a third entity for security and confidentiality of digital records and information is prone to alteration, hacking and being compromised. Blockchain technology enables a consensus distributed among member parties whereby every transaction involving these digital assets can be verified without compromising the confidentiality of the data and that of the involved parties. It is thus considered as a secure way of transacting data in an organization.

Blockchain technology is applied in 'smart contracts'. These are computer programs which execute the terms of a contract automatically. When pre-agreed conditions among participants in these 'smart contracts' are met, then the members can automatically make payments as per the contract. This allows transparency and confidentiality of the 'smart contract' and terms. Blockchain technology meets the challenges of traditional storage network. With this system, users are able to transfer and share data securely without depending on a third party. This has improved security and privacy when transacting data in organizations. In addition to secure data transfer, other benefits the Blockchain technology include data provenance, an immutable audit trail, and decentralized management. The solutions that they offer include encrypting of sensitive data, careful design and implementation, use of a virtual private network, and using the technology as an index of health data.

REFERENCES

Abou Hana, M. (2017). Innovation in the UAE: From First Foundations to 'Beyond Oil'. *Global Policy*, *8*(3), 414-417.

Ahmed, O. (2017). *Block chain Technology: Concept of Digital Economics*. Retrieved from https://mpra.ub.unimuenchen.de/80967/1/MPRA_paper_80967.pdf

Ali, M., Nelson, J. C., Shea, R., & Freedman, M. J. (2016, June). Blockstack: A Global Naming and Storage System Secured by Blockchains. In *USENIX Annual Technical Conference* (pp. 181-194)

Anand, A., McKibbin, M., & Pichel, F. (2016). Colored coins: Bitcoin, Blockchain, and land administration. In *Annual World Bank Conference on Land and Poverty*.

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., ... & Wuille, P. (2014). *Enabling Blockchain innovations with pegged sidechains*. Retrieved from http://www.opensciencereview.com/papers/123/enablingBlockchain-innovations-with-pegged-sidechains .

Beck, R., Czepluch, J. S., Lollike, N., & Malone, S. (2016). Blockchain-the Gateway to Trust-Free Cryptographic Transactions. In *ECIS* (p. ResearchPaper153).

Blundell-Wignall, A. (2014). The Bitcoin question: Currency versus trust-less transfer

technology. *OECD Working Papers on Finance, Insurance and Private Pensions*, (37), 1.

Bryman, A. & Bell, E. (2011). *Business research methods*. 3rd ed. New-York: Oxford University Press Inc.

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., ... & Song, D. (2016). On scaling decentralized Blockchains. In *International Conference on Financial Cryptography and Data Security* (pp. 106-125). Springer Berlin Heidelberg.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*, 6-10.

Dilley, J., Poelstra, A., Wilkins, J., Piekarska, M., Gorlick, B., & Friedenbach, M. (2016). Strong Federations: An Interoperable Blockchain Solution to Centralized Third Party Risks. *arXiv preprint arXiv:1612.05491*.

Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data. In *Proceedings of IEEE Open & Big Data Conference*.

Gee, J., Loewenthal, D. & Cayne, J. (2013). Phenomenological research: The case of Empirical Phenomenological Analysis and the possibility of reverie. *Counselling Psychology Review, 28 (3), 52-6.*

Gococo, E., (2017). How Tech Savvy Are You? The Impact Of Technology On The Real Estate Sector. *Business In Calgary*, 27, 9, pp. 56-64, Business Source Complete, EBSCO*host*, viewed 24 October 2017.

H. C. B., & Irvine, J. (2016). The Blockchained Health Record. *The Health Care Blog*, 2016-10.

Ichikawa, D., Kashiyama, M., & Ueno, T. (2017). Tamper-Resistant Mobile Health Using Blockchain Technology. *JMIR mHealth and uHealth*, *5*(7).

Johansen, S.K. (2017). *A Comprehensive Literature Review on the Blockchain Technology as an Technological Enabler for Innovation*. Working Paper. DOI: 10.13140/RG.2.2.12942.77121

Citation: Abeer AlSereidi & Khalid Almarri., Application of Blockchain Technology for Secure Data Transactions in Organizations. Australian Journal of Basic and Applied Sciences, 13(9): 34-41. DOI: 10.22587/ajbas.2019.13.9.3

Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016, May). Hawk: The Blockchain model of cryptography and privacy-preserving smart contracts. In *Security and Privacy (SP), 2016 IEEE Symposium on* (pp. 839-858). IEEE.

Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, *24*(6), 1211-1220.

Linn, L. A., & Koo, M. B. (2016). Blockchain for health data and its potential use in health it and health care related research. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*.

Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016, October). A secure sharding protocol for open Blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 17-30). ACM.

Mainelli, M., & Smith, M. (2015). Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka Blockchain technology). *The Journal of Financial Perspectives*, *3*(3), 38-69.

Mendling, J., Weber, I., van der Aalst, W., Brocke, J. V., Cabanillas, C., Daniel, F., ... & Gal, A. (2017). Blockchains for Business Process Management-Challenges and Opportunities. *arXiv preprint arXiv:1704.03610*.

Micheler, E., & von der Heyde, L. (2016). Holding, clearing and settling securities through Blockchain technology Creating an efficient system by empowering asset owners.

Miles, M. B., Huberman, M. A., & Saldaña, j. (2013) *Qualitative Data Analysis*. Thousand Oaks: Sage.

Nelson, J., Ali, M., Shea, R., & Freedman, M. J. (2016, June). Extending existing Blockchains with virtualchain. In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL'16),(Chicago, IL)*.

Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through Blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In *Banking Beyond Banks and Money* (pp. 239-278). Springer International Publishing.

Ramachandran, A., & Kantarcioglu, D. (2017). Using Blockchain and smart contracts for secure data provenance management. *arXiv preprint arXiv:1709.10000*.

Roberts, T. (2013). Understanding the research methodology of interpretive phenomenological analysis. *British Journal of Midwifery*, *21*(3), 215-218.

Rudestam, K. E., & Newton, R. R. (2015). *Surviving Your Dissertation: A Comprehensive Guide to Content and Process* (4th ed.). Thousand Oaks, CA: SAGE Publications.

Shrier, D., Wu, W., & Pentland, A. (2016). *Blockchain & infrastructure (identity, data security* http://cdn.resources.getsmarter.ac/wpcontent/uploads/2016/06/MIT_Blockain_Whitepaper_PartThree.pdf .

Trillo, M. (2013). *Stress Test Prepares VisaNet for the Most Wonderful Time of the Year*.*Visa.com*. Retrieved 24 November 2017, from https://www.visa.com/blogarchives/us/2013/10/10/stress-test-prepares-visanet-for-the-most-wonderful-time-of-the-year/index.html

Umeh, J. (2016). Blockchain Double Bubble or Double Trouble? *ITNOW*, *58*(1), 58-61.

Vaismoradi, M., Jones, J., Turunen, H. & Snelgrove, S. (2016). Theme development in qualitative content analysis and thematic analysis. *Journal of Nursing Education and Practice, 6(5), 100-110*.

Vukolić, M. (2015). The quest for scalable Blockchain fabric: Proof-of-work vs. BFT replication. In *International Workshop on Open Problems in Network Security* (pp. 112-125). Springer, Cham.

Wang, H., Chen, K., & Xu, D. (2016). A maturity model for Blockchain adoption. *Financial Innovation*, *2*(1),- 12.

Yin, R. K. (2016). *Qualitative Research from Start to Finish* (2nd ed.). New York, NY: The Guilford Press.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?-A Systematic Review. *Plos One*, *11*, 10.

Zyskind, G., Nathan, O., & Pentland, A. S. (2015). Decentralizing privacy: Using Blockchain to protect personal data. In *Security and privacy workshops* (SPW), 2015 IEEE (pp. 180–184).