Dependence on Blockchain Technology for Future Cybersecurity Advancement: A Systematic Analysis

Ayman Abdulsalam Mohamed Al-Dherasi
Zhejiang University of Science and Technology
School of Information and Electrical Engineering
Liuhe road No. 318
Hangzhou, China

Albert Annor-Antwi
Zhejiang University of Science and Technology
School of Information and Electrical Engineering
Liuhe road No. 318
Hangzhou, China

Yang Chunting
Zhejiang University of Science and Technology
School of Information and Electrical Engineering
Liuhe road No. 318
Hangzhou, China

ABSTRACT

Purpose-The aim of this research is to thoroughly analyze blockchain with respect to the role it plays in cybersecurity, and how this role may affect the future of blockchain and cybersecurity in future. Also, gaps are identified along with the shortcomings that cause these gaps. This research also identifies possible solutions to the gaps or issues. *Method:*- the research approach used here is review of the literature. Other works that address various aspects of blockchain are analyzed in breadth to show its effectiveness. *Results:*- there is a great possibility that blockchain is one of the future's greatest cybersecurity solutions. Among the major issues include quantum computing, user habits, and conflicting interests. All these issues have various ways through which they can be addressed effectively in order to brighten the future of blockchain's applicability in cybersecurity. *Conclusion:* - blockchain, as it is, promotes fraud in cryptocurrency and therefore needs modification. Blockchain only needs reinforcement from technologies such as Artificial Intelligence and Machine learning to make it the future's most dependable cybersecurity provider.

General Terms

Algorithms, Security, Cryptography, Artificial Intelligence, Machine Learning.

Keywords

Blockchain,Cybersecurity,Cryptography,Algorithm, Cryptocurrency, Encryption, Decentralization, Transparency, Ingenuity

1. INTRODUCTION

Blockchain technology is an incorruptible digital ledger of economic transactions which can be programmed to anything of value such as financial transactions online [1]. One perfect example that can explain the functionality of technology is Bitcoin's record-keeping system. It is also in some cases identified as a distributed and decentralized public ledger. Blockchain, as its name suggests, is a chain of blocks that are used in storage of information regarding transactions. These details may include dates, times, amount of money transacted transaction codes, companies transacting the money, account details, among other details. Apart from the recording, which is doing the transaction, blockchain ensures that the block of a certain transaction does not collide with other transactions [2]. So, a block remains distinguished from others.

In the recent past, Blockchain has gained much admiration for its distinguished cybersecurity capabilities, resulting in many firms becoming interested in using its strong security infrastructure to safeguard their information systems. More reasons why Blockchain has gained so much popularity include its cryptography capabilities, its aspect of being decentralized—not owned by a single entity, it is immutable—implying that no one can tamper with data stored inside it, and it is transparent which allows users to keep track of their data if they need [3]. Blockchain is heavily dependent on three major pillars which makes it strong as discussed herein. They are decentralization, transparency, and immutability.

1.1 RESEARCH QUESTIONS

RQ1: Why is blockchain so dependable, and why should it be viewed as a futuristic cybersecurity requirement?

RQ2 What gaps are in blockchain now and how can they be resolved for the sake of the future dependence on this technology?

2. LITERATURE REVIEW

This research looks into the applicability of blockchain insecurity in the future, which is guided by the current security systems that implement blockchain. This literate review how blockchain works, its various components and qualities that make it dominant and invincible when it comes to providing cybersecurity. Also, the literature focuses on the use case, which examines the working application areas of blockchain. To know how it works in details, this literature focuses on various algorithms that are used in blockchain, with the attempt to understand how they are implemented. The literature also reviews some challenges that are faced in the process of implementing blockchain. Some of the outstanding qualities of blockchain that are looked into in detail include decentralization, transparency, and immutability.

2.1 Blockchain and Decentralization

This is found mostly in cryptocurrency security, particularly Bitcoin and BitTorrent [1][4]. It is worth mentioning that security systems before were centralized, which is today considered a weak system due to the advancement that has been registered lately. Banks also have centralized systems which they consider most outstanding for safeguarding customers' money. However, there are some security issues that disfavor centralized data. Typically, when the data is stored in one spot, it becomes an easy target for adversaries, they know the right spot to attacks. Also, a centralized system would mean that the entire unit has to be disrupted by activities such as upgrading, even if it is upgrading a small part of the whole system. A worst-case scenario of centralized system, as explained by [5], is that when the data is compromised, then the whole system is. Blockchain comes to reverse all these odds by decentralizing information systems [5]. Decentralized systems do not require information to be stored in a single entity. Below is a figure ideologically showing the difference between centralized and decentralized systems.

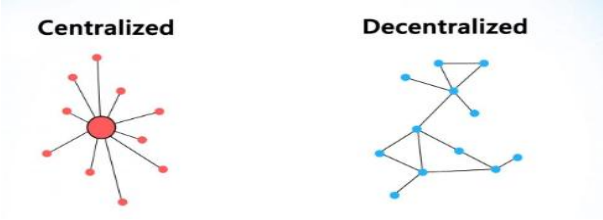


Figure 1: Centralized vs. Decentralized System [6].

Form the figure above, it is clear that interaction can only take place through the server in a centralized system, but it is possible to interact directly—in peer to peer mode—via decentralized system [6]. This is one basic characteristic of decentralized system that makes it efficient and effective when it comes to providing or reaching efficient and effective cybersecurity.

2.2 Blockchain Transparency

Complex cryptography is used in hiding details such as person's identity, which is represented by their public address which is represented by encrypted text. So, while considering transparency, one thing to consider is that a person's identity is hidden, but it is possible to track all their transactions [7]. Everyone wants to use systems that they can trust, now and in the future. Blockchain ensures that this happens by bringing about transparency in systems, which in turn builds trust. The cryptographic algorithms that are used in concealing real user details are powerful that they effectively keep away fraudsters [8]. The transparency in blockchain is further strengthened by the fact that the transactions and holdings from all public addresses are open to viewing. The transaction explorer is equipped with the public address of user, making it possible to view their transactions. This is a level of transparency that has not been there before, especially in financial systems.

Nonetheless, blockchain adds a degree of accountability in large businesses, which have not been there before. In looking at past incidences, large financial institutions have been able to use funds from their customers in their activities without the customers' consent [7][8][9]. This issue has resulted in numerous cases of financial crisis, having been recorded in relation to various financial institutions. Blockchain eliminates this by ensuring that customers can publicly see all transactions by their customers and therefore they can be able to see how the financial organization they entrust their funds with them [7][8][9]. Blockchain does not pose any limitations since a user can acquire more than one public addresses and can use them in storing holdings as well as transferring funds among different recipients.

The supply chain provides a very outstanding example of a blockchain use case. It allows for immutable tracking that applies to anything being transacted or transferred via the supply chain. This implies that consumers—who are at the receiving end of the supply chain—can know the exact composition of the products they consume. In the case of food, they get to know what is contained in it and therefore come to know if it is fair trade, marketing of genuine products, and, and observing workers' rights [9][10]. With blockchain in the supply chain, the customers can get to know the absolute source of various entities and commodities and what they contain, which imply that their ins increased transparency which in turn promotes and maintains integrity when scandals are eliminated in production and distribution. With blockchain, a firm can be able to effectively track all its transactions irrespective of which department they are carried out in.

The blockchain supply chain also greatly impacts consumer goods through assisting in tracking crucial substances such as medicine, which gives assurance that patients are able to receive the medication that they need [10]. Also, in supply chain, blockchain helps in reducing supply of counterfeit goods in the market. Blockchain could also effectively improve healthcare security by providing state-of-the-art database protection, which in turn allows patients to have convenient and safe access to their medical records when in need, mostly. Blockchain the problem of centralized information access via the successful running of a decentralized database from increased security and distribution [10][11]. The blockchain ledger is also usable in drug intake and distribution mediation, regulation compliance, as well as management of healthcare supplies. For example, it is possible for a patient to interact with a healthcare support system that is supported by blockchain which allows them to view all their claims, transactions, due payments, medical history, and all other relevant and critical details.

Before, there has not been database system in the healthcare industry that has a revolutionary power to revolutionize all operations involving cybersecurity including supply chain. Security, transparency, and immutability that comes with blockchain provide outstanding security strategies, which are enhanced by the aspect of blockchain being decentralized [12]. One outstanding aspect of blockchain that makes it effective in information management is the creation of channels that guarantee traceability of information as a means of ensuring that nothing is tampered with eliminated dishonestly, therefore providing top-notch transparency [12]. To win consumers' trust, many application developers and tech companies are trying to adopt blockchain so that they can win the trust of their customers fast. This is made possible by trust, immutability, and incorruptibility that are enabled by blockchain.

One essential question to consider asking is why transparency is very important in blockchain. Currently, more transactions are being conducted online; and blockchain will be counted on to reduce cases of unfair gameplay in the world of gaming. Blockchain provides a revolutionized aspect of online and offline gaming by providing transparency. Game developers also provide public addressed that are associated participants' activities in games, especially performance and scores. Transparency allows blockchain to effectively and considerably boost the online gaming economy which is expected to gross above $138 billion by 2019 [11].

2.3 Blockchain and Immutability

Still, trust issues dominate blockchain's immutability aspect. Immutability in blockchain can be identified as the ability of a ledger to remain unedited, unchanged, or unaltered, which implies that the ledger entries are indelible [13]. Every block of data in a blockchain cannot be changed and contains facts as well as transaction details as well as processes that use cryptographic principles using a hashing system [14]. The hashing system consists of alphanumeric strings that are generated by all blockchains separately. Each block has a digital signature or a hash that represent the user's public address. Blocks are usually retroactively coupled together and are unrelenting. This mechanism is used in ensuring that the system cannot be interrupted and more importantly, ensuring that the data stored or saved in each block cannot be altered in any way.

Immutability in blockchain is achieved via hashing or adding hash value to each block to secure it and run the codes separately. For one to understand how hashing takes place, they need to understand the cryptographic hash basics [14]. Some compilers and program debuggers, as well as database systems that use various commonly known programming languages, provide hash functions that only require programmers to pass a set of byte and the function returns a checksum signature. One popular hash function is the SHA-256 which is popular in the blockchain space. In looking at an example, a programmer in Python may run a hashing function by first importing the required library known as the "hashlib" as a package from Python's standard library, then access the "sha256" function. Below is a code snippet illustrating this process.

```
import hashlib

h = hashlib.sha256('Dummy Data')

h.hexdigest()

'49240b3cc693fd281422bbcabb5f207ae2a390003534989fb55
080799ee08d8c'
```

From the above code, the "Dummy Data" is presumed to be the username of an online user but the hashed output "*49240b3cc69….*" is the address that would reflect in public as the digital signature for the individual using the method. So, cryptography plus the blockchain hashing process equals immutability.

However, immutability of blockchain is faced with a variety of challenges which include "51 percent attack". The term "51 percent attack signifies that an attacker can be in acquisition of comping power over all users in a given network. This challenge could also be referred to as the controlling interest in generating power. This is a common challenge experienced in decentralized systems since they must implement a network, and they are composed of numerous entities that somewhat function independently. Data miners or rather adversaries, break the immutability of blockchain systems by implementing complex algorithms that can be able to reverse-engineer the hashing process used to hide various users' real identities. After this, the attackers could successfully alter the transaction data that is considered immutable. [13] explain that after achieving this, the adversaries can proceed to reverse transactions and divert others to their preferred destinations.

The age of quantum computing is here, and computing power is growing larger and larger. This is good for cybersecurity and bad at the same time. IBM is already at the verge of making quantum computing available for basic uses. Due to the high computation power possessed by these systems, having them fall on the hands of adversaries could mean that they can reverse-engineer all hashing methods and the public key of the blockchain network, which can help them locate the private key. This is a threat to dependency on blockchain for future cybersecurity, especially to transactions.

Although, the 51 percent attack threat could be resolved through the use of a countering or consensus algorithm that is delegated as proof of stake algorithm. In addressing the threat posed by the power of quantum computing, developers are recommending and implementing the integration of quantum cryptography into the core of blockchain [19]. This will make it possible to come up with a future that implements quantum practices that will use allow blockchain to use the high power into its advantage and make are records more secure. This futuristic venture helps in bringing out ways through which the future can be embraced via blockchain.

2.4 Blockchain Cryptography

Cryptography is the aspect of using algorithms or mathematical principles in storage and transmission of data in a given form, only to the intended users. It involves use of a secret key that is only shared between the individual intended to access the information and the sender. The key is used in encryption and decryption processes. A cipher—a mathematical algorithm used in data encryption and decryption—is used in creating cyphertext that is non-comprehensible to anybody until it is deciphered. This concept is used in blockchain to protect data. Blockchain makes use of cryptography for two major purposes. These are—securing the identity of a transaction initiator and to ensure that all past records remain indelible. Thus, cryptography is arguably one of the most outstanding aspects of security provision and reinforcement in blockchain. Indeed. It could be considered as the basic source.

Blockchain uses a variety of cryptography approaches which include symmetric-key cryptography and the asymmetric-key cryptography also known as the public-key cryptography. The public-key cryptography method is considered more advanced compared to the symmetrical cryptography. This makes it important to understand the symmetrical cryptography first, which gives a better understanding of the asymmetrical or public-key cryptography [14][15]. In symmetrical cryptography, a single key is used in the process of encrypting and decrypting the ciphertext. The key could be any random character—a letter or a number. Below is a visual process of how symmetrical cryptography works.

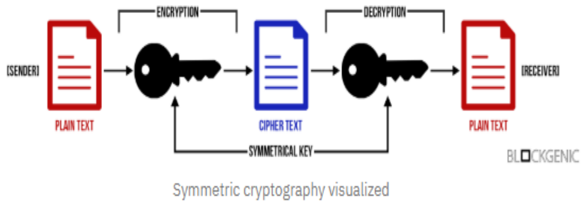
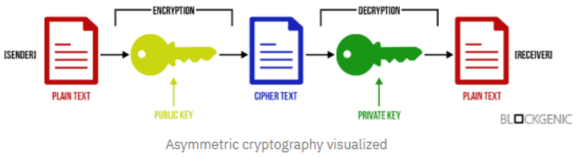


Figure 2: How Symmetrical Cryptography Works [14].

The message is composed and encrypted using a symmetrical key. The same key is used in decrypting the text to arriving at the next cyphertext. The key has to remain a secret between the sender and the recipient. If a third party gets to know the key, they can easily access the information before it reaches the intended user. This makes this method weak and hardly usable in the blockchain. Asymmetrical cryptography is similar to the symmetrical one, only that it has a solution to the herein explained weakness of the symmetrical cryptography method. Asymmetrical cryptography makes use of keypairs and not shared key. The key pairs are public and private keys, which must be involved in the encryption and decryption processes.

The public key is sometimes treated as the username, which is available for everyone to see. But, they key is usually hashed in the case of blockchain, which implies that the people viewing the transaction cannot see the real identity of an individual. The private key, on the other hand, is considered as the password. There are no chances that the public key could be used in deriving a private key and it is also impossible for the private key to authorize a transaction. Below is a graphical illustration of public and private keys concerning how they work.



Asymmetric cryptography visualized

Figure 3: Asymmetrical (Public-key) Cryptography [14].

As illustrated in the graphic above, all sender's data must be encrypted; the same treatment is given to transactions. The receiver's public key (the username) is used in encrypting the message, which guarantees safe transition of the message from the sender to the receiver. The only means through which the text can be decrypted is by using the correct private key. The usage of key-pairs allows asymmetric cryptography to be much safer [16]. They keypairs are also used for authentication purposes. But, this is not enough for blockchain to be considered secure and more futuristic. Digital signatures add another layer of security to the already-competently secure system. Indeed, digital signatures use asymmetric cryptography to provide the authentication details required to make them secure. Some essential elements in digital signatures that make them secure is the inability to corrupt them, and they are also easily verifiable [17]. The asymmetrical cryptography guarantees that the private key only belongs to a single user and therefore, each user have a distinct digital signature.

Digital signatures are created and implemented via the use of algorithms such as the RSA-based signature schemes which include RSA-PSS, undeniable signatures, Rabin signature algorithm, DSA, undeniable signature, pairing-based schemes such as the BLS, ElGamal signature scheme, and others. On top of using digital signatures and using asymmetrical cryptography processes as well as implementing other authentication and authorization processes, blockchain allows the private key to be used on smart cards, applications, hardware, and even in offline mode [14][15][16][29]. This enhances blockchain security, which is further discussed in the use cases.

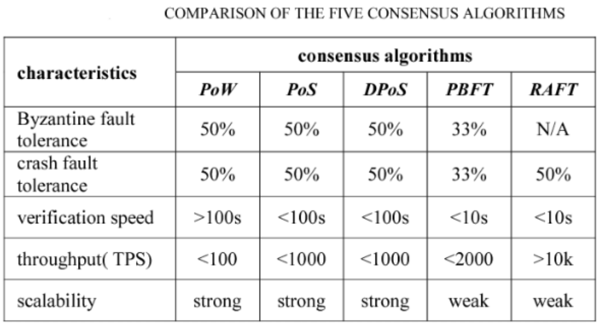
2.5 Blockchain Algorithms

Already, there is brief discussion of various algorithms along with their usage in cryptography. But, in blockchain, algorithms have far more extended use. Indeed, the future of blockchain is based on implementation of more outstanding and sophisticated algorithms to provide more sophisticated security for users. Currently, blockchain is working on ensuring that every user is in control of their algorithms and personal data related to their identity by ensuring that they can customize the details effectively. Due to the increased effectiveness of artificial intelligence and machine learning-based algorithms that study human habits and imitate them, blockchain is being pressurized to ensure that it provides customized security depending on the preferences of the users [18]. But, this has one drawback that may compromise their security by customizing the security features to weak ones.

In blockchain, algorithms are given the following responsibilities; verification of signatures, confirmation of balances, confirming the validity of a block, identifying the ways through which data miners validate blocks, and others. Other activities include establishment of commands to ensure that blocks move, establishment of procedures for the creation of new coins, informing the system on how to determine consensus. Therefore, there are consensus algorithms, mining algorithms, and traceability chain algorithms [19]. These algorithms work as follows:

Consensus algorithms: These algorithms are used in exchange for coins in the cryptocurrency systems. Consensus algorithms achieve reliability on networks that involve multiple nodes. The algorithms make sure that all the nodes conform to the rules and actions directed to them, ensuring that they are all in consensus, hence the name of the algorithm. When a transaction is initiated, the notes work on accepting it, validating it, replicating it, validating and replicating the blocks, and serving as well as storing blockchain. Nodes also define proof-of-work algorithms that miners employ [20]. Proof-of-Work (PoW) was the initial algorithm used in consensus, but because it has been faulty, newer algorithms have been implemented to undertake the same task as illustrated in the table below.

Table 1: Comparison of Consensus Algorithms [19].



COMPARISON OF THE FIVE CONSENSUS ALGORITHMS

characteristics	**consensus algorithms**				
	PoW	***PoS***	***DPoS***	***PBFT***	***RAFT***
Byzantine fault tolerance	50%	50%	50%	33%	N/A
crash fault tolerance	50%	50%	50%	33%	50%
verification speed	>100s	<100s	<100s	<10s	<10s
throughput(TPS)	<100	<1000	<1000	<2000	>10k
scalability	strong	strong	strong	weak	weak

Mining algorithms: There are three major concepts identified in data mining which are clustering and classification, association rules, a sequence analysis. Clustering or classification is identified as the analysis of data sets to generate grouping rules that can be used in further classification of data. Association rule, on the other hand, is used in implication of associating specific relationships among a set of objects in a database [21]. Lastly, sequence analysis focuses on the patterns that occur in sequence. In blockchain, mining algorithms make use of computers to represent quick guess and answer puzzles. The mining algorithms are also responsible for ruling the unique header metadata for blocks which include timestamps and software versions. This is implemented via hashing functions that return a fixed-length random string of numbers. The once values are also modified to evaluate the impact of hash values. Miners find blocks in every 12-15 seconds and try to solve the puzzles in them quickly and slowly. The algorithms are automatically adjusted to allow miners to run 12-15 seconds of solution time.

Traceability chain algorithms: Traceability is very important in blockchain since it helps track the initiator of a transaction. This improves security and the internal process performance as well as the planning activities of each node in the supply chain. Blockchain makes use of big data analytics which is created from the transaction data and then streamed in high-dimensional distribution in the computing network. Traceability chain algorithm's major goal is to ensure that the traceability decisions are arrived at quickly. Accordingly, this allows the artificial intelligence of blockchain mining algorithms to run faster than consensus algorithms because of the inference mechanism. Also, these algorithms allows a transaction to be traced from the start to the point they are completed. This approach is called Takagi-Sugeno Fuzzy cognitive maps [22]. The traceability algorithm is essential for supply chain since it gives functionality that allows all transactions to be tracked. A complete traceability system requires moving transactions like in the ones that blockchain provides. Objects need to be linked with sensors and tags that communicate with the algorithms to facilitate the traceability. This puts the virtual identity to work. Items such as QR codes, RFIDs, wireless sensors, and networks are used.

Three key subprocesses are implemented in traceability algorithms. One of them is the identification and labeling of products with the aim of facilitating product identification. The second one is capturing the data and recording which is done via scanning capabilities with electronic information which flow to optimize and retrieve data. The third entity is a linkage that provides communication to optimize data sharing between supply chain partners and protocols.

2.6 Barriers to Blockchain Adoption

According to a study presented by Cordero (2018), some of the most common barriers to blockchain adoption, as illustrate in the figure below include regulatory uncertainty, lack of trust among users, inability bring together a network, inability to configure blockchains, inability to scale, concerns of intellectual property, and compliance or audit concerns, all put in the descending order of their impact or effect to adoption of blockchain. Apparently, Japanese cryptocurrency companies lose above US$500 million to hackers and other cyber criminals every year [23]. This fault has been blamed to technological failure of providing optimal security for cryptocurrency. Typically, blockchain has gained its popularity from the aspect of providing competent and optimal security to Bitcoin, one of the most popular and highly valued cryptocurrency around the world [23][24][25].

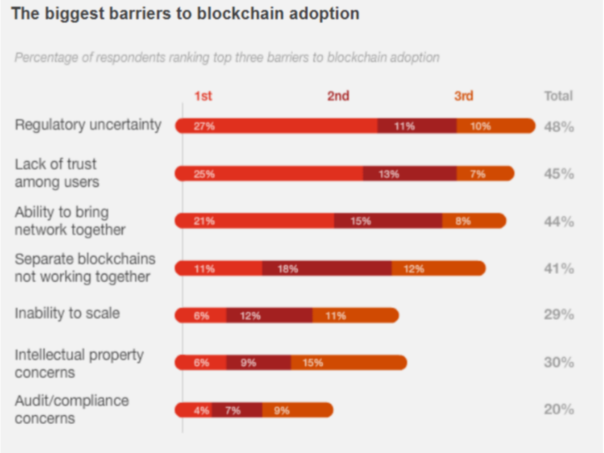


Figure 4: Barriers to Blockchain Adoption [23]

In the attempt to cope with audit or compliance concerns, blockchain is designed with the immutable feature that distributes its ledger to allow users to audit transactions effectively. Blockchain has to fuse both public and private addresses via a 5-layer spectrum of trust, particularly to cope with the issue of mistrust from users and those who transact online.

3. IDENTIFIED GAPS IN BLOCKCHAIN FOR FUTURE CYBERSECURITY

As discussed in the review of literature and thorough analysis of blockchain in this paper, the technology is competent enough in providing cybersecurity depending on current computing technology. But, the technology is advancing fast, and one major challenge that exists is high computation power that could be capable of reverse-engineering hashing and cryptographic algorithms used in confiscating user identity, keeping transactions trackable, and ensuring that transactions are indelible. Also, the incoming high computer power may have great power that could allow them to fake a transaction and therefore facilitate fraud.

Nonetheless, due to the aspect of blockchain providing competent security, particularly to cryptocurrency such as bitcoin [4]. It has been identified to create a haven for fraudsters particularly because an individual's full identity cannot be revealed. This makes blockchain contribute more to insecurity in the cyberspace rather than promote security. Already, there are alarming losses and incidences of theft and scamming done via cryptocurrency [26]. Chavez-Dreyfuss (2019) reported to *New York Reuters* that fraud-related activities based on cryptocurrency have already yielded $1.2 billion losses which are 70 percent of what was recorded in 2018. A total loss of $1.7 billion was recorded in 2018, but the crime is continuing to balloon as the cryptocurrency market is continually slowing down [24]. Already, scam and fraud activities are totaling more than the amount being exchanged genuinely in the cryptocurrency network. These huge losses are being blamed on weak security systems and lack of effective and outstanding governmental regulations.

Another major gap identified in implementation of blockchain for future cybersecurity is the undeniably growing computing power. Quantum computing is being associated with having great abilities to break codes, algorithms, and various cryptographies in place. Therefore, it is being feared to become a cybersecurity threat to the future. From the analysis, it is known that blockchain heavily relies on cryptography and use of algorithms [28][30]. Particularly, blockchain makes use of the public key. Technically, the most basic and straightforward way to break code is by using trial and error method where one tries multiple keys until they find one that works efficiently. In looking at some known past cases, a 64-bit key was launched by a group of developers in 2002. To achieve this, it took 300,000 developers almost half a decade to achieve it. It would take a very powerful computer to decode the 2^{128} possible trials to decode an encrypted key. This would surely take long such that the world's strongest computer could take millions of years to decrypt. But, with quantum computing, tables are turning. The Grover's algorithm has a speed that could take shorter time to decode a 128-bit key, but on the other hand, quantum computing can achieve creation of a 256-bit key which is stronger and has greater ability to resist quantum attach [25] [28]. So, on the one hand, blockchain could take advantage of quantum computing by creating a stronger cryptographic resistance, but on the other hand, the attack on cryptography is significantly increased by blockchain.

However, as much as quantum computing can provide blockchain with highly resistant cryptography, this does not imply that blockchain would be entirely secure. Cryptography is one piece of the larger pie as far as blockchain is concerned. The fact that blockchain is decentralized creates loopholes for attacks, especially to persons who cannot effectively and confidently secure their systems. Also, blockchain is gaining larger popularity, which implies that it is becoming more and more usable. In the mix, there are users who might not have the right experience that is usable in ensuring that the transact safely without making themselves easy target for attackers.

4. RESOLVING THE IDENTIFIED GAPS IN BLOCKCHAIN FOR FUTURE CYBERSECURITY

There are a variety of strategies that blockchain could use to remain effective in the future with the aim of addressing the various gaps identified in this model. The solutions would address cybersecurity issues related to users' malpractice or inability to take proper caution. Another solution would be aimed at coping with the increasing computation power that could increase chances of reverse-engineering blockchain security technologies and breaking cryptographies that are used as principal security requirement in blockchain as well as protecting user identity. Moreover, one essential requirement is to cope with the conflicting interests associated with hiding users' real identity particularly in online transactions, especially in cryptocurrency, which promotes fraudulent activities. Blockchain needs to come up with a way through which the identity may be revealed in case a transaction is suspected to be fraudulent with the aim of countering fraud. The many problems here is the aspect of conflicting interests. Below is a lengthy discussion of how blockchain may resolve the issues or gaps identified herein. It is commendable that blockchain facilitates tracking all transactions and there is none that can be deleted from systems, but having the user identity hidden keeps information on adversaries hidden. In fact, cryptocurrency is identified as one currency that is supporting fraud, especially through scamming inexperienced users [24][27].

4.1 Coping with Threats from Quantum Computing

As illustrated earlier, quantum computing will create a problem and a solution as well—it will have the capability to create a higher key of higher bit number that is harder to decipher, and on the other hand, it will have the ability to crack keys with lower bit number within a shorter time than expected. So, blockchain will need to capitalize on creating and implementing cryptography systems with at least 256-bit public key that would take an adversary a lengthy amount of time to crack even while using quantum computing. Like web hosting packages where a member can choose a package that suits them best depending on the features, blockchain could implement different packages for users of different preferences depending on the level of security they need. For example, a package with 64-bit cryptography system could be termed as 'basic' its price could be relatively low. A 128-bit system could be termed as 'standard' since it has stronger security and perseverance to crackers, and it is almost impossible. 256-bit systems would be termed as 'premium' since it has the strongest security systems {14][16].

Technically, implementing the packages above would help organizations and cyberspace users to have a better understanding of blockchain and therefore have a clear mind of what they want to use depending on what they want to protect. This would also make blockchain more popular, and users would upgrade their cybersecurity to their security expectations. However, other security systems, strategies, and For instance, phishers, spammers, botnet attackers, and other types of hackers could steal the authentication details of legit users, which is one thing that blockchain needs to address, apparently. But, this is one issue that is hard to solve using algorithms since it involves user activities and, in some cases, the users may be reckless or not experienced in security practices [30]. Below is an overview of how these issues may be solved in the future by advancing blockchain further. protocols such as 2-step verification, 2-factor authentication, use of biometrics, and others should not be ignored [31][32]. These could act as reinforcements to blockchain.

4.2 Coping with Threats from Inexperienced or Careless Users

To keep users from being tricked, to give up their authentication or authentication or even the key to accessing blockchain systems, they need to be continually trained on the essence of security and how they could achieve it. Apart from thorough training, more algorithms should be implemented to cope with issues associated with users being tricked into giving away their verification details [31]. As much as fast and convenient instant access is required, it could be safer to involve two or three verification and authentication steps before allowing users to access systems or data in the cyberspace. Another workable solution that blockchain can implement is to track transactions using network features and alerting users as well as requiring them to confirm their access to their systems. In case it is not them who are accessing the systems, this could have them take steps immediately. This is a futuristic solution that could competently work on blockchain in enhancing the future of cybersecurity [31][32].

4.3 Coping with Conflicting Interests of Hiding Users Identities

In looking at a solution that would pose lesser conflicts, regulations would be applied to authorize investigation or probing of transactions that may be fraudulent. This would require the blockchain to keep a user's identity that is associated with the public key. Thus, when a public key gets flagged, it will be possible to track the user associated with it. But, this tracing will only be authorized to the government agencies that deal with cybersecurity. Also, regulation that governs how much these bodies can dig into knowing about transactions should be limited to only the authority, perhaps the FBI, CIA, or any bodies associated with Homeland security or devoted to protecting the national grid and they should be authorized [33][34]. This could bring hope for reducing fraud since people may fear that the protection or cover provided to them by blockchain is no longer applicable in protecting or covering them.

5. CONCLUSION

In conclusion, it is evident that there are a few very essential elements that make blockchain one of the most reliable cybersecurity provider. It is capable of providing security for supply chain and any financial transactions such as those of cryptocurrency. Some of the features that make blockchain much reliable include decentralization, immutability, and transparency. Any transactions done publicly can be traced using public key. Also, all transactions are indelible—they cannot be deleted. Blockchain implements various cryptographic algorithms, most of which are complex to decode. But, with the invention and development of quantum computing, it might be possible to decode or break the cryptographies implemented in blockchain. Some of the gaps identified in blockchain include threats from quantum computing, conflicting interests; blockchain promotes fraud and errors associated with human users. Regulations are also not effectively implemented. To cope with these errors. There are various ways through which these issues could be coped with which include training users in solving issues associated with user interactions in the cyberspace; introduction of regulations to cope with fraud; changing the anonymity in blockchain by ensuring that user's original identity can be revealed in order to reduce fraud, and to the create different packages for blockchain users, which could help in understanding its concepts better. These steps could help improve blockchain to become come effectively for use in the future.

6. FUTURE WORK

The future work associated with this research will be focused on evaluating the algorithms that can be added to the blockchain to ensure that the real user details remain confiscated unless needed by the authorities. Of course, anybody can try to mimic and deceive blockchain while impersonating authorities, and therefore, an algorithm that may implement machine learning and artificial intelligence concepts may be used to differentiate between these users. This possibility is treated as future research.

7. REFERENCES

[1] Revolution B. How the Technology Behind Bitcoin is Changing Money. Business and the World, page. 2016;324.

[2] Fortney, Luke. "Blockchain Explained." Investopedia. Investopedia, June 25, 2019. https://www.investopedia.com/terms/b/blockchain.asp.

[3] A. Rosic, "What is Blockchain Technology? A Step-by-Step Guide For Beginners," *Blockgeeks*, 20-Aug-2019. [Online]. Available: https://blockgeeks.com/guides/what-is-blockchain-technology/. [Accessed: 13-Sep-2019].

[4] Crosby M, Pattanayak P, Verma S, Kalyanaraman V. Blockchain technology: Beyond bitcoin. Applied Innovation. 2016 Jun;2(6-10):71.

[5] A. Wright, De Filippi P. Decentralized blockchain technology and the rise of lex cryptographia. Available at SSRN 2580664. 2015 Mar 10.

[6] LISK.io, "Blockchain Use Cases " Real World Application: Lisk Academy," *Lisk*, 2019. [Online]. Available: https://lisk.io/academy/blockchain-basics/use-cases. [Accessed: 13-Sep-2019].

[7] Hbus, "The How and Why of Blockchain Transparency," *Medium*, 19-Dec-2018. [Online]. Available: https://medium.com/hbus-official/the-how-and-why-of-blockchain-transparency-b3f3465f6989. [Accessed: 13-Sep-2019].

[8] Nugent T, Upton D, Cimpoesu M. Improving data transparency in clinical trials using blockchain smart contracts. F1000Research. 2016;5.

[9] Benchoufi M, Porcher R, Ravaud P. Blockchain protocols in clinical trials: Transparency and traceability of consent. F1000Research. 2017;6.

[10] Bashir I. Mastering blockchain. Packt Publishing Ltd; 2017 Mar 17.

[11] Swan M. Anticipating the economic benefits of blockchain. Technology innovation management review. 2017 Oct 1;7(10):6-13.

[12] A. Rosic, "What is Blockchain Technology? A Step-by-Step Guide For Beginners," *Blockgeeks*, 20-Aug-2019. [Online]. Available: https://blockgeeks.com/guides/what-is-blockchain-technology/. [Accessed: 13-Sep-2019].

[13] L. Fortney, "Blockchain Explained," *Investopedia*, 25-Jun-2019. [Online]. Available: https://www.investopedia.com/terms/b/blockchain.asp. [Accessed: 13-Sep-2019].

[14] LISK.io, "Cryptography Explained," *Lisk*, 2019. [Online]. Available: https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/blockchain-cryptography-explained. [Accessed: 13-Sep-2019].

[15] Blockgenic, "Asymmetric Cryptography In Blockchains," *By Blockgenic*, 22-Nov-2018. [Online]. Available: https://hackernoon.com/asymmetric-cryptography-in-blockchains-d1a4c1654a71. [Accessed: 13-Sep-2019].

[16] Kosba A, Miller A, Shi E, Wen Z, Papamanthou C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In2016 IEEE symposium on security and privacy (SP) 2016 May 22 (pp. 839-858). IEEE.

[17] Nofer M, Gomber P, Hinz O, Schiereck D. Blockchain. Business & Information Systems Engineering. 2017 Jun 1;59(3):183-7.

[18] Banafa A. IoT and blockchain convergence: benefits and challenges. IEEE Internet of Things. 2017 Jan 10.

[19] Baliga A. Understanding blockchain consensus models. InPersistent 2017 Apr.

[20] Hussein AF, ArunKumar N, Ramirez-Gonzalez G, Abdulhay E, Tavares JM, de Albuquerque VH. A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform. Cognitive Systems Research. 2018 Dec 1;52:1-1.

[21] Mingxiao D, Xiaofeng M, Zhe Z, Xiangwei W, Qijun C. A review on consensus algorithm of blockchain. In2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC) 2017 Oct 5 (pp. 2567-2572). IEEE.

[22] J. Cordero, "Solving the Biggest Barriers to Blockchain Adoption; Today.," *Medium*, 03-Sep-2018. [Online]. Available: https://medium.com/@jonelcordero/solving-the-biggest-barriers-to-blockchain-adoption-today-8350bebb5102. [Accessed: 13-Sep-2019].

[23] G. Chavez-Dreyfuss, "Cryptocurrency thefts, fraud hit $1.2 billion in first quarter: report," *Reuters*, 30-Apr-2019. [Online]. Available: https://www.reuters.com/article/us-crypto-currency-fraud/cryptocurrency-thefts-fraud-hit-1-2-billion-in-first-quarter-report-idUSKCN1S62P3. [Accessed: 14-Sep-2019].

[24] P. Blockchain, "Blockchain Algorithms 101: A Introduction to Consensus Protocols," *By Professor Blockchain*, 03-Jul-2019. [Online]. Available: https://hackernoon.com/blockchain-algorithms-101-a-introduction-to-consensus-protocols-c00f884a01fb. [Accessed: 13-Sep-2019].

[25] Trautman LJ. Is disruptive blockchain technology the

future of financial services?

[26] Yeoh P. Regulatory issues in blockchain technology. Journal of Financial Regulation and Compliance. 2017 May 8;25(2):196-208.

[27] Z. Ali, “A Simple Introduction to Blockchain Algorithms,” *Medium*, 17-Mar-2019. [Online]. Available: https://blog.goodaudience.com/a-simple-introduction-to-blockchain-algorithms-ca05b9bcc32f. [Accessed: 13-Sep-2019].

[28] Mylrea M, Gourisetti SN. Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In2017 Resilience Week (RWS) 2017 Sep 18 (pp. 18-23). IEEE.

[29] Patel, “Consensus Algorithms in Blockchain,” *GeeksforGeeks*, 25-Apr-2019. [Online]. Available: https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/. [Accessed: 13-Sep-2019].

[30] Fanning K, Centers DP. Blockchain and its coming impact on financial services. Journal of Corporate Accounting & Finance. 2016 Jul;27(5):53-7.

[31] Mylrea M, Gourisetti SN. Blockchain: A path to grid modernization and cyber resiliency. In2017 North American Power Symposium (NAPS) 2017 Sep 17 (pp. 1-5). IEEE.

[32] N. Bauerle and M. Kuznetsov, “What is Blockchain Technology?,” *CoinDesk*, 2019. [Online]. Available: https://www.coindesk.com/information/what-is-blockchain-technology. [Accessed: 13-Sep-2019].

[33] Kshetri N. Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy. 2017 Nov 1;41(10):1027-38.