IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.11703

Towards a Scalable and Secure Blockchain Based on Post-Quantum Cryptography.

Betty O. Ahubele[1] and Martha O. Musa[2]

[1,2]Department of Computer Science, University of Port-Harcourt, Rivers State, Nigeria.

Abstract: Blockchain systems rely on classical cryptography of public key encryption and hash functions for its security. These security mechanisms of the distributed technology is made possible by complex mathematical computations, integer factorization and discrete logarithm problems. The emergence of quantum technology is expected to reduce the security of current cryptographic systems. As a result, companies adopting blockchain-based solutions, becomes prone to quantum attack in long-term strategic planning. Grover's and Shor's quantum algorithms, which attack the cryptographic principles on which the blockchain is built, currently pose the biggest threat to the blockchain. To counter these threats, the post-quantum cryptography was proposed. The main aim of this study is to critically analyzed the security of classical blockchain and present some post-quantum implementation algorithms in developing a quantum-based blockchain system that would be able to withstand any attacks using quantum technology.

Keywords: Blockchain system, Classical computers, Quantum Technology, Post-Quantum Cryptography.

I. INTRODUCTION

Distributed Ledger Technologies (DLTs) most especially blockchain has evolved over the years as highly accepted, open and decentralized data structure that provides data transparency, tamper-resistance, privacy, decentralization, immutability etc, based on cryptographic mechanisms of public key encryption and hash functions. Blockchain users leverage the various public key cryptographic primitives to validate block of transactions and linking a new block with the previous blocks using the hash functions. These hash functions generates digital signatures and create records of transactions in the form of block that do not need to trust each other for effective transaction processing and execution. Conventional information technology and blockchain-based systems are provided with security countermeasures using several public (asymmetric) and private (symmetric) cryptographic algorithms [1].

The Public key cryptographic algorithms used in those systems are Rivest Shamir Adleman (RSA) [14] encryption, Elliptic Curve Digital Signature Algorithm (ECDSA) [15], Elliptic Curve Diffe Hellman (ECDH) algorithm [16] and Edwards-curve Digital Signature (EdDSA) Algorithm, which utilizes hard mathematical problems like discrete logarithm and large integer factorization in providing the underlying security. Alternatively, the private key cryptographic algorithms include; Data Encryption Standard (DES), Triple DES (TDES) and Advanced Encryption Standard (AES) which utilizes the block cipher protocol for generating both encryption and decryption symmetric keys. Since the security of blockchain systems are based on the computational structure of high computing powers, many standard classical cryptography systems are known to be vulnerable against the advent of quantum computers [2].

Quantum computing is the use of quantum physics properties of superposition and entanglement to perform computation using quantum computers [20]. Unlike the digital classical computers, quantum computers makes use of specific algorithms designed for a specific problem for simulating complicated, large, and uncertain systems, where a lot of potential outcomes are considered [4]. Recently, quantum computing is like a metaphorical elephant due to its potentials in altering the time and space complexity algorithms in classical computers such as a solution to a linear system of equations. However, the invention of quantum computers poses threat to classical cryptography [20].

Therefore, it has become urgent to develop new methods to protect against the threat of quantum computing. An effective approach is to develop quantum cryptography mechanisms based on the unique properties of quantum physics. For instance, the quantum signature technology based on quantum state computational distinguishability with fully-flipped permutations (QSCDff) problem, utilizing the complexity of QSCDff problem for quantum computation, can guarantee the security of the blockchain-based signature process. This study analyze the classical blockchains, their cryptography algorithms and the impact of quantum algorithms (based on Shor and Grover) on the security of blockchain and the attacks on classical systems. To guide the researchers on the development of quantum-blockchain in mitigating the attacks, the study discussed the post-quantum implementation algorithms on enhancing the security of distributed ledgers.

DOI: 10.17148/IJARCCE.2022.11703

II. RELATED WORKS

Various studies have been carried out on blockchain ranging from applications, challenges and issues and the implementation of the distributed ledger platform in industries such as supply chain, drug distribution, e-voting, decentralized governance, NFTs etc. In Ahubele et al. [23], the on-blockchain distributed ledger platform was implemented using the etnereum operating system for pharmaceutical drug distribution. The authors provided a transparent, secure and distributed platform for tracking pharmaceutical products from the manufacturing to the final clients (patients). Blockchain is a decentralized database that is cryptographically protected against manipulation using digital signatures. Cryptographic hash functions that are used in preparing new blocks, any node with access to quantum computer would procure mining rewards to himself. In a study by [3], a quantum safe blockchain system that uses the quantum key distribution (QKD) across an urban fibre network for secure authentication was proposed.

Wang et al., [25] proposed a quantum blockchain algorithm that utilizes the DPoSB to generate block and signs the transaction information with a quantum one-way function. By the stake vote and distracting the malicious behaviours of DPoSB and asymmetric quantum encryption, the fairness, efficiency and security of the blockchain system can be improved. The study also demonstrated blockchain security and compared with quantum algorithms. Our quantum blockchains provide a safe platform that could decrease the costs of various operations and transaction activities.

However, recent developers have increased their interests in distributed ledger systems where public key infrastructure and hashing technology functions. As a result, Tiago et al., [24] studied the state of the art on current post-quantum cryptosystems, its applicability to blockchains and distributed ledger technologies and their challenges. The study also analyzed the impact of computing attacks based on Shor and Grover's algorithms on blockchain and how to apply post-quantum cryptosystems to mitigate such attacks. In addition, the study provided a broad view on blockchain with useful guidelines for researchers and developers who wants to become the next developers of the quantum-resistant blockchains generation.

A. Classical Blockchain Systems

Blockchain technology will be deeply threaten by the quantum era as its main safety is the integrity of public key infrastructure, consensus mechanism and hash technology. The distributed database enable any user to transfer and receive digital currency or assets from another user. In the decentralized network, records are stored as blocks, validated, maintained by several network of computers and sent across several nodes. The underlying technology is the basic structure of all cryptocurrencies. Without the shared database, no cryptocurrency exists. Classical blockchain system replaces the single central authority in such that the records are supervised by a large community and no individual person can control or manipulate any stored transactions [12].

In a blockchain, every generated block contains a timestamp, data (sender, recipient and the amount of bitcoin sent), hash, and hash of the previous block. The hash represents a unique QR or finger print which identifies the block and its content. If a hacker attempt to make changes to a block in the chain, the hash will change, affecting all the blocks succeeding it. This is almost impossible as the hacker will have to recalculate the hash of the blocks and gain 51% consensus of the entire network. In addition, the Proof-of-Work mechanism makes forgery very complicated and almost impossible. [7] highlighted the key features offered by the blockchain as a promising technology for transacting and executing decentralization of transactions without the need for a third party trust (See figure 1).

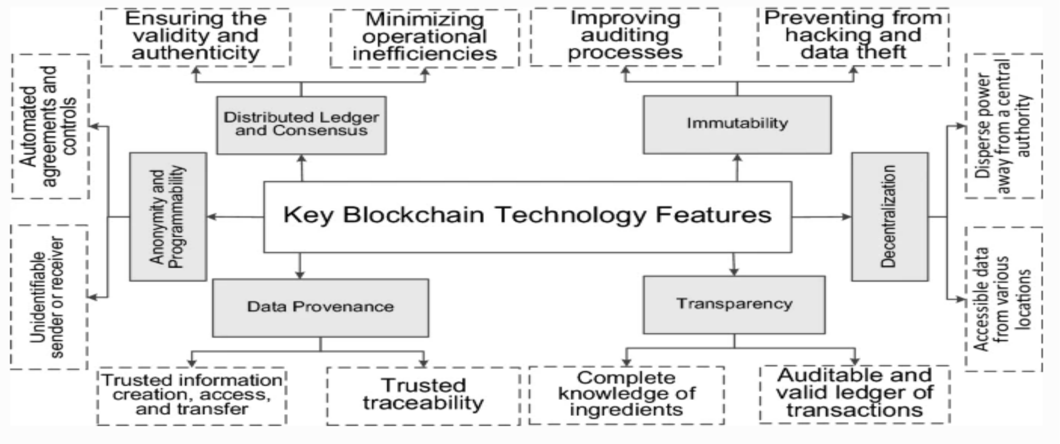
Ensuring the validity and authenticity
Minimizing operational inefficiencies
Improving auditing processes
Preventing from hacking and data theft
Automated agreements and controls
Distributed Ledger and Consensus
Immutability
Disperse power away from a central authority
Anonymity and Programmability
Key Blockchain Technology Features
Decentralization
Unidentifiable sender or receiver
Data Provenance
Transparency
Accessible data from various locations
Trusted information creation, access, and transfer
Trusted traceability
Complete knowledge of ingredients
Auditable and valid ledger of transactions

Figure 1: Key Features of Classical Blockchain [7]

B. Blockchain Issues and Challenges

The concept of blockchain started with Nakamoto in 2008 [1], where it was described as a peer-to-peer cash payment system. The initial blockchain “Bitcoin” consist mainly of the block header and the body. As time progresses, blockchain technology became necessary for integrating other industries such as health, supply chain, insurance, education, etc. The distributed network provides the transparency and security of transactional information. Despite the potential benefits of integrating the distributed ledger technology in various business domains, some enterprises who require high performance legacy transaction processing speed, find it very unappealing to integrate blockchain into their business solutions. The most vital factors in the core of the technology are consensus algorithms and digital signatures. Various consensus algorithms are utilized to generate blocks while the digital signatures provide security of the transaction information.
In the Bitcoin blockchain, the PoW (Proof-of-Work) consensus mechanism enable miners to compete by calculating the hash value of the block using high computing power. The miner with higher hash power tends to discover the accurate hash solution, and the first miner that finds the accurate hash value will generate a new block and be rewarded with bitcoin. Other consensus algorithms include Proof-of-Stack (PoS), Delegated-Proof-of-Stack (DPoS), and Delegated-Proof-of-Stake with node’s behaviour and Borda count (DPoSB). These algorithms does not rely on computing power and this reduces power consumption. Byzantine algorithm also helps to achieve consensus in communication in the presence of malicious nodes. However, digital signatures uses the public-key encryption (Rivest Shirma Adleman (RSA) and Elliptic Curve Ccryptography (ECC)) methods for implementing security on the blockchain. These encryption methods were well-developed and complicated for classical computers to crack, facilitating the security of the digital signatures. However, Shor’s and Grover’s quantum algorithm threaten the security of blockchain by its ability to effectively solve the integer decomposition problem and the discrete logarithmic problem of the blockchain encryption methods. Consequently, the security of blockchain technology based on the digital signatures is vulnerable to quantum computation.
Forging issues of the blockchain can occur in two approaches; first, the attacker can forge signatures by **using** the transaction information of the signers and second by **forging** the transaction information of the signers. The challenge of repudiation where the attackers can repudiate signatures that makes the signers fail in the information signing process can be seen on the blockchain. Similarly, the blockchain systems are comparatively slow. Scalability in blockchain can account for delay in bitcoin transfer, high transaction cost in bitcoin network and traffic congestion in the decentralized transactions based ethereum blockchain [26], Cryptocurrencies are decentralized money based on blockchain which uses public key cryptography algorithms like ECDSA (Elliptic-curve Digital Signature Algorithm) for its security.
With the advent of quantum technology, ECDSA are vulnerable to quantum attacks. Cryptocurrency worth over 2trillion market capitalization will face huge risk in the quantum era [27]. With the prevalence of large scale quantum computers, recent cryptographic algorithms would be hacked. It becomes very pertinent to develop a quantum-based blockchain framework in order to scale up to the level of digital computers and resist attacks from both digital and quantum computers [26].

C. Quantum Computing

Quantum computing is an emerging that utilizes the properties of quantum physics to store data and perform computations. Quantum computers will be able to change the data in a block without changing the hashing function. When such happens, all the blocks will remain valid. Quantum computers can be extremely advantageous for certain tasks where they could vastly outperform even our best supercomputers. Quantum computers differs from classical computers as the former utilizes qubits while the later uses regular bits. These qubits can be represented by any quantum particle with two important quantum properties [10].

Qubits are made using physical systems, such as the spin of an electron or the orientation of a photon. These systems utilizes the superposition, entanglement and tunneling principles of quantum physics to break the cryptographic safety of the blockchain. Just like the regular bits, a qubit can be in the state of 0 and 1 but also occur in a state between the two with probabilities for each state. This is called superposition. The superposition of a qubit makes its state unknown and with this, the quantum computer can handle calculations on both states simultaneously. This remains so until the qubit is put into a controlled state for measurement, which causes its quantum state to collapse to either 0 or 1 [30]. Due to entanglement and superposition properties, a quantum computer can process various inputs in parallel, which allows it to compute all possible states, given by 2^n where n is the number of qubits, at the same time. With the combined properties of superposition and entanglement, quantum computers can perform huge problems and tasks simultaneously [28].

Quantum computers will redefine cryptography on all distributed ledger platforms [28]. Significant research must be carried out to mitigate the effects of this quantum computers and move all classical cryptography to the post-quantum cryptography. Since the quantum computers will not be able to break the hashing code of the blockchain but will go through the cryptographic safety and gain access to the data in the blocks, do anyone think it is ideal to consider the quantum computers which is just being speculated or on the blockchain which is already in use today?. The answer is: it is advisable to add the blockchain to quantum cryptography and turning the entire blockchain to quantum phenomena.

D. Quantum Threats on Classical Public Key Blockchain Cryptography

Quantum computer utilizes a particular quantum algorithm to solve a particular problem efficiently, unlike classical computers that handles a wide range of tasks with a single algorithm. The Shor and Grover's algorithms are the two quantum algorithms that threaten the security of blockchain systems.

1) Shor's Threat on RSA (Rivest Shimar Addleman) Algorithm

In a typical blockchain system, the user sends his public key to the server in request for some confidential information using the RSA public key encryption. The server uses the sender's public key to encrypt the information and send the encrypted message to the user. Then the users utilizes its corresponding private key to gain access by decryption. In a similar fashion, blockchains utilizes the procedure of RSA for creating and encrypting the e-wallets [14]. Whenever any blockchain user creates e-wallet, a public address and its corresponding private key pair is generated. The cryptocurrencies on the blockchain are transacted using the public address of the user [21], while the user's private key is used in correspondence with the public key to access and spend the user's crypto. Mathematically, RSA is a one-way trapdoor function where public information is made up of two large prime numbers (p,q) and their product (mod p,q) for encryption and decryption. With an improved RSA, the algorithm can also be used to solve the discrete logarithm problem [5], allowing an attacker to break asymmetric cryptography and the blockchain digital signature [6].

With the advent of quantum computers, an attacker will implements the Shor's algorithm to compute the private key based on the information from the public key that was published together with a transaction. Then the malicious entity can transact using the victim's private key. A study by [22] described a transaction hacking scenario where the attacker utilized the computed private key to publish conflicting transactions before the original transaction will be finally verified and validated in a block, spending the same currency which the victim has already spent, but with a higher fee to manipulate miners including the attacker's transaction instead of the original transaction.

2) The Shor's Threat on Elliptic Curve Cryptography and Elliptic Curve Digital Signature Algorithm (ECDSA).

Elliptic curve-based algorithms generates a 256-bit private key standards for creating for e-wallet and signing e-transactions. Classically with ECDSA, it is almost impossible to determine the random value for a given generated public key. The randomly generated private key is used to sign transactions while the public key is the corresponding key pair to prove the usage of the private key. However, Shor's algorithm can compromise the private key for any public address and gain total access to a person's e-wallet. From a security point of view, it is a known fact that ECDSA provides a better security level than RSA and a 224-bit sized public key ECDSA provides a 112bit security level. Although, for RSA to achieve the same 112-bit security level, a 2048-bit sized public key is required but the presence of post-quantum resistance will put ECDSA under more threat than the conventional RSA [14].

3) Shor's Threat on Elliptic Curve Diffe Hellman (ECDH) Algorithm.

The elliptic curve Diffie Hellman key agreement protocol rely on the discrete logarithm problem to allow two parties establish a shared secret over an unsecure communication channel. The bitcoin receiver utilizes this concept to publish some ECDH information which the sender require for computing a shared secret like the bitcoin or stealth address, reusable payment codes, reusable address, and payments to which a sender sends his money [16]. The receiver calculates the corresponding private key to gain access to the money. The aim is to determine a unique integer that can be the order of the generator element of a finite cyclic group. For general elliptic curves, DLP seems to be extremely computationally hard as best known classical algorithms for DLP on elliptic curves are the generic algorithms with running times exponential to the number of bits necessary to describe the problem. Modified Shor's algorithm can break the 'thought to be' irreversible and intractable one-way trapdoor function.

4) Shor's Threat on Digital Signature Algorithm

Blockchain technology utilizes digital signature algorithm to ensure non-repudiation and integrity of data. Once a message is digitally signed, the sender will not deny its authenticity in sending the message and the sent message cannot be manipulated. This unique feature of blockchain makes the system vulnerable to quantum computer-aided attacks. Due to the advent of quantum technology, the classical computers are not safe in the near future as they rely of complex integer factorization and discrete logarithm for their security [17].

5) Grover’s Threat on Classical Blockchain Cryptography.

Blockchain uses the hash functions to prevent alterations of previous blocks and guarantees the blocks integrity. This provides the security of transactions on the distributed architecture as it requires huge computational efforts in calculating the inverse of a hash, finding a hash collision with existing hash and changing the transactions in a single block. However, with Grover’s algorithm this security feature of blockchain will be broken as the inverse hash value can be determine. This poses a threat mainly to hash functions using symmetric cryptography as it facilitates a quadratic speedup in calculating the inverse of a hash function [6]. Consequently, with this algorithm, a quantum computer can infiltrate a hash function with a length of k bits in just 2k/2 iterations [9], and this affects its security-level by half in a post-quantum setting [11].

With Grover’s algorithm, two main attacks can occur on the blockchain; firstly, the algorithm can be used to search for hash collisions in order to replace blocks without breaking the integrity of the chain [5] [6]. For instance, if an attacker wants to change a transaction contained in a block, he has to make sure that the block’s hash remains unchanged, so the previous-block-pointer stays valid in the next block. If a collision is found, the modified content combined with other data of the block will give the same hash as before. The attacker can alter transactions stored in the block without disrupting the blockchain [3]. Secondly, the speedup through Grover’s algorithm allows a miner equipped with a quantum computer, to mine blocks significantly faster than a classical computer [9]. In a so-called 51%-attack, where one instance controls more than half of the network’s computing power, an attacker could monopolize the block creation to afford him the verified opportunity to add data to blockchain [3].

E. Quantum-Based Blockchain

Blockchain and quantum computing are new technologies that will optimize information and communication security in the future and revolutionize the information industry. While Blockchain provides specific properties (public key infrastructure, consensus protocols and hashing functions) that make hacking impossible, quantum computers will take advantage of quantum phenomena to threaten the security of the Blockchain. The study in [13] has shown that quantum properties are especially useful when it comes to cryptocurrencies, because these properties could ensure the safety of the created currency when represented by a quantum state. While it might work for certain local blockchains due to scalability restrictions as the technologies required to realize quantum networks over great distances are yet to be developed. Since quantum computers can quadratically perform a wide and exhaustive search faster than classical computers, it is necessary to utilize the modified Grover's algorithms to perform mining on a quantum computer.

F. Security Analysis of the Blockchain.

The security models used in information theory and cryptography include; semi-honest adversary model: which assumes that some adversaries in the system are semi-honest and would maintain the protocol correctly but restrict some information to pose a threat later; malicious adversary model: which assumes that some malicious adversaries in a system may break the existing protocol for additional information and would keep the necessary information to infer additional information. When generating the block, a semi-honest adversary will only keep public information of the block header and block body. This will prevent him from interfering in any useful additional information, because the public information does not keep the secrets. In the signing process, a semi-honest adversary can attempt to infiltrate the signer’s private (the only secret) which is not feasible based on the security of the private keys. Therefore, the blockchain can guarantee security in the semi-honest adversary model. In this study, we would expound on the security in the malicious adversary model by breaking blockchain security into two sections which include:

1) Security of the generation of blocks

Existing blockchains utilizes the consensus algorithms in the generation of blocks and different consensus mechanisms have different levels of security. The malicious adversary model can be envisaged by launching three main protocol attacks in this process; double-spending attacks; hash value attacks and the nodes that attacks the blocks generation. Similarly, attacker nodes can secretly and successfully forge another blockchain to forge information in blocks with large computing power, which is termed double-spending attacks. The success rate is 100% when the computing force of one node is larger compared to the total computing force of the entire blockchain system. However, this attack can be avoided in our proposed blockchain because it rely on the computing power which is not included in our algorithm. Based on quantum computer, an attack can crack the hash value in a short time. With the Grover's algorithm, the quantum computer can use quadratic acceleration to crack the hash value, which gives the nodes that have quantum computers to dominate the entire.

2) Security of the signing process.

In any distributed system, the security of the private keys which is used in signing the transactions cannot be overlooked. The malicious attacks which can occur during this process are eavesdropping, forging, repudiation and interception. In this study, we explained how the blockchain can be robust in the signing process to avoid the launch of these attacks in the malicious adversary model. The security of private keys is in two ways: firstly, it has been proven that the private keys of signers cannot be cracked by quantum algorithm in polynomial time when there is no private key π [29]. Hence, no one can differentiate the cyphertexts signatures β^{+}_{π} (n) from β^{-}_{π}(n) efficiently. Secondly, because private keys are selected from κ_n and $|\kappa_n| = n^{!}/ \sqrt{2}^{n}$, the attacker only has a chance of $\sqrt{2}^{n}/n^{!}$. Since the divergence of $n^{!}$ is far greater than $\sqrt{2}^{n}$, it becomes difficult to generate the private keys. This makes the success rate of the brute attacks minimal, which means that the success rate of by which the attackers can randomly generate signatures is negligible.

III. PROPOSED QUANTUM INFORMATION SECURITY.

In quantum asymmetric encryption, an encryption is said to have a quantum information security if the quantum cyphertexts are computational indistinguishability. Here, we can claim that two quantum ensembles β_1 and β_2 are computationally indistinguishable, if for every polynomial probabilistic algorithm B, every positive polynomial P(.) and sufficiently large positive integer (n), the following equation can be satisfied:
$[P_r(B\text{-}(\beta_1) = 1) - P_r(B\ (\beta_2) = 1)] < 1/P(n)$ such that $P_r(.)$ represents the probability.

In this study algorithm, the cyphertexts are β^{+}_{π} (n) and β^{-}_{π}(n). Then $\beta1 = \beta^{+}_{\pi}\ (n)^{\otimes P(n)}$, $\beta2 = \beta^{-}_{\pi}(n)^{\otimes P(n)}$
We prove that:

$$[P_r(B(\beta^{+}_{\pi}\ (n)^{\otimes P(n)}) = 1) - P_r(B\ \beta^{-}_{\pi}(n)^{\otimes P(n)}) = 1)] < 1/P(n).$$

We assumed a probabilistic polynomial algorithm Bl, such that:

$$[P_r(B(\beta^{+}_{\pi}\ (n)^{\otimes P(n)}) = 1) - P_r(B\ \beta^{-}_{\pi}(n)^{\otimes P(n)}) = 1)] \geq 1/P(n).$$

Therefore, we have an efficient algorithm to differentiate the signature cyphertexts β^{+}_{π} (n) from β^{-}_{π}(n) efficiently, corresponding to solving the QSCDff (Quantum state computational distinguishability with fully fipped) permutations problem. However, the problem cannot be solved in polynomial time due to the hardness of the QSCDff problem but our study was able to obtain the quantum information security.

The proposed quantum-blockchain platform also implemented a quantum algorithm for the two forging attacks on the classical blockchain. In the first attack where the signer generates transaction information T_A and public key $[P_K]$ and then uses the private key to generate signature [β1]. An attacker wants to forge a signature with T_A and the signer's private key, which makes [β1]≠ [β2]. Based on the signature algorithm in transaction signing and verification process where the nodes signs transactions using a quantum one-way function based on the quantum state computational distinguishability with fully flipped permutations (QSCDff) problem and the uniqueness of the output, β^{+}_{π} (n), in generating algorithm, we envisaged that [β1]=[[β2] and thus, the signatures cannot be forged. In the second approach, a signer generates transaction information T_A1 and public key P_K. An attacker attempts to forge the signer's transaction information by ensuring $T_A2 \neq T_A1$, so that T_A2 signature can escape the verification process. Based on the private keys security, the attackers will not be able to generate a valid signature when they cannot access the signers' private keys. In conclusion, the transaction cannot be forged and the attackers forging method will not work.

IV. CONCLUSION

The only way to achieve a secure and scalable decentralized system in the long run seems to be quantum cryptography. Due to the laws of quantum physics, data can be secured in such a way that nobody is able to read or modify it without being noticed. Also, a quantum computer cannot break it, because quantum cryptography does not depend on classical computations. Blockchains are more likely to keep evolving with quantum computing than quantum computing alone, which will make the entire blockchain existence a past history. However, including the two technologies will birth the ultimate quantum-blockchain so that any existing transaction will remain tamper-proof and permanently secured. The

DOI: 10.17148/IJARCCE.2022.11703

only drawback is that quantum cryptography requires expensive quantum hardware. Therefore, in the future this might only be practical in cases where security has the highest priority and costs are not particularly important, for example for government or financial data. Although due to the inexistence of the quantum internet that requires a network of quantum routers to transmit quantum information and still retain their properties, this wonderful idea may not be achieved now but with time enhanced security for unforeseen attacks which can destroy the power-housed distributed technology will be a revolution.

REFERENCES

[1] Mavroeidis, V., Vishi, K., D., M., and Jøsang, A. 2018. The Impact of Quantum Computing on Present Cryptography. International Journal of Advanced Computer Science and Applications 9(3). Doi: 10.14569/IJACSA.2018.090354.

[2] Ikedia, K. Security and Privacy of Blockchain and Quantum Computation. Advances in Computers. 111(2018. 199-228.

[3] Kiktenko, E. O., Pozhar, N. O., Anufriev, M. N., Trushechkin, A. S., Yunusov, R. R., Kurochkin, Y.V., Lvovsky, A. I., and Fedorov, A. K. Quantum-secured blockchain; Quantum Science and Technology. 2018. 3(3).35004. Doi: 10.1088/2058-9565/aabc6b.

[4] Katwala, A. Quantum computing and quantum supremacy explained. 2020. https://www.wired.co.uk/article/quantum-computing-explained. Retrieved 09/06/2022.

[5] Cui, W., Dou, T., and Yan, S. Threats and Opportunities: Blockchain meets Quantum Computation. 39th Chinese Control Conference (CCC). Shenyang, China. IEEE. 2020. 5822-5824.

[6] Fernandez, V., Orue, A. B., and Arroyo, D. Securing Blockchain with Quantum Safe Cryptography: When and How? 2021. 13th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2020)

[7] Yaqoob, I., Salah, K., Jayaraman, R. and Al-Hammadi,Y. Blockchain for healthcare data management:Opportunities, Challenges and future recommendations. 2020. Neural Computing and Applications.

[8] Nakamoto, S. A peer-to-peer electronic cash system. Decentralized Bus. Rev. 21260 (2008).

[9] Rodenburg, B. V., and Pappas, S. P. Blockchain and Quantum Computing. 2017. MITRE Technical Report.

[10] Donna Lu. https://www.newscientist.com/question/what-is-a-quantum-computer/

[11] Amy, M., Di Matteo, O., Gheorghiu, V., Mosca, M., Parent, A., and Schanck, J. Estimating the Cost of Generic Quantum Pre-image Attacks on SHA-2 and SHA-3 in Selected Areas in Cryptography. 2017. R. Avanzi and H. Heys (eds.), Cham: Springer International Publishing. 317-337.

[12] Sarmah, S.S. Understanding Blockchain Technology. 2018. Computer Science and Engineering 2018. 8(2). 23-29. Business Intelligence Architect, Alpha Clinical Systems, USA. DOI:10.5923/j.computer.20180802.02.

[13] Jogenfors, J. 2019. Quantum Bitcoin: An Anonymous, Distributed, and Secure Currency Secured by the No Cloning Theorem of Quantum Mechanics. In 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea (South). 14.05(17.05). 245-252.

[14] Rivest, R.L., Shamir, A. and Adleman, L. A method for obtaining digital signatures and public- key cryptosystems. 1983. Commun. ACM. 26(1). 96–99.

[15] Koblitz, N. Elliptic curve cryptosystems. 1987. Mathematics Comput. 48(17).203–209.

[16] Diffie, W. and Hellman, M. New directions in cryptography.1976. IEEE Trans. Inf. Theory. 22(6).644–654.

[17] Digital Signature Standard (DSS). Standard FIPS 186-2. 2000. NIST.

[18] Crypto Forum Research Group. Available: https://irtf.org/cfrg. Retrieved 10/06/2022.

[19] Grover, L.K. A fast quantum mechanical algorithm for database search. 1996. In Proc. 28th Annual ACM Symp. Theory Comput., Philadelphia, PA, USA. 212–219.

[20] Hassija, V., Chamola, V., Goyal, A., Salil, S. and Guizani, N. Forthcoming applications of quantum computing: Peeking into the future institutions of Engineering and Technology. https://doi.org/10.1049/iet-qtc.2020.0026.

[21] Mosca, M. Cybersecurity in an era with quantum computers: Will we be ready?. 2018. IEEE Secure- Privacy. 16(5). 38–41.

[22] Stewart, I., Ilie, D., Zamyatin, A., Werner, S., Torshizi, M. F., and Knottenbelt, W. J. Committing to quantum resistance: a slow defence for Bitcoin against a fast quantum computing attack. 2018. Royal Society open Science. 5(6). 180410. Doi: 10.1098/rsos.180410.

[23] Ahubele, B.O, Eke, B.O. and Onuodu, F.E. On-Blockchain Validation Smart Contract Model on Ethereum Distributed Ledger System for Pharmaceutical Products Distribution. IOSR Journal of computer Engineering (IOSR-JCR). 23(2), 10-22.

[24] Fernandez-Carames, T. M., and Fraga-Lamas, P. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. 2020. IEEE Access (8).21091-21116. Doi: 10.1109/ACCESS.2020.2968985.

DOI: 10.17148/IJARCCE.2022.11703

[25] Wang, W., Yang, Yu and Lingjie, Du. Quantum Blockchain Based on asymmetric quantum encryption and a stake vote consensus algorithm. 2022. School of Physics and National Laboratory of Solid State Microstructures, Nanjing University, Nanjing 210093, China. Email: ljdu@nju.edu.cn

[26] Ahmed, A., El-Latif, A., Bassan, A., Mehwood, I., Muhammad, K., Salvador, E. and Peng, J. Quantum-Inspired Blockchain based cybersecurity: Securing Smart Edge Utilities in IoT-Based Smart Cities. 2021. Information Processing Management. 58(4).

[27] Alghamdi, S. and Almuhammadi, S. The future of cryptocurrency in the quantum era. 2021. IEEE.

[28] Raychev, N. Quantum Blockchain. 2020. Quantum Review Letters. 15-47. https://www.scholarchain.eu/qrl. DOI: 10.37686/qrl.v1i2.61

[29] Kawachi, A. et al. Computational indistinguishability between quantum states and its cryptographic application. 2012. J. Cryptol. 25. 528–555.

ABOUT AUTHORS

Dr. Betty Osamegbe Ahubele received Ph.D. degree in Computer Science in the Faculty of Sciences in 2021 from the University of Port Harcourt, Rivers State, Nigeria. She was awarded the best graduated student in the Department of Computer Science, Faculty of Natural Sciences, Ambrose Alli University (AAU), Edo State, Nigeria, in the year 2005. She obtained her M.Sc (Computer Science) from University of Port-Harcourt, Rivers State, Nigeria, in the year 2012. She is currently working as a Lecturer in the Department of Physical Sciences, Benson Idahosa University, Benin, Edo State. Her current research is focused on Blockchain Technology and Cyber Security. She has published several papers in International Journals.

Dr. Martha Ozohu Musa is a Lecturer in the Department of Computer Science, Faculty of Science, University of Port Harcourt, Nigeria. She obtained her first degree in Computer Science from University of Ilorin, Kwara State, Nigeria, her second degree (M.Sc. Computer Science) and her third degree (PhD. Computer Science) from the University of Port Harcourt where she presently works. Her research focuses on Human Activity Recognition (using sensors and actuators) and User Behavior Analysis using Machine Learning Algorithms and methods and also on Cyber security.

She was born in Lafiagi, Kwara State in Nigeria to an incredibly loving and supportive family and has being passionate about science from her elementary days and has always being interested in improving the human life with it. She influences others with her vision and serves as a role model to many, having taught many students and supervised their projects. Amongst her recent publications are; Internet Threats and Mitigation Methods in Electronic Businesses Post Covid-19, Improved Hybrid Machine Learning User Behavioural Model for Secured Smart Homes, Gaussian Naïve Sensor-Based Approach for Activity Recognition and Smart System for detecting Anomalies in Crude Oil Prices using Long Short-Term Memory.

She enjoys the work she does as she loves to solve problems and be of help to others and also see them succeed. She derives tremendous satisfaction from this. She hopes to make connections through research collaborations and networking opportunities.

In her free time, she enjoys spending time with her family, walking and listening to good music.