International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 06 | June 2021 www.irjet.net p-ISSN: 2395-0072

Juxtaposition of Blockchain Technology with Emerging Quantum Computing

G. T. Thampi[1], Vinayak Mhatre[2], Sarvesh Pande[3], Jay Shah[4]

[1]*Principal, Thadomal Shahani Engineering College, Maharashtra, India*
[2,3,4]*Student, Information Technology Department, Thadomal Shahani Engineering College, Maharashtra, India*

Abstract – *Quantum computing is an emerging technology that brings massive computational speed to the table. It has been proven that modern day quantum computers can solve the most complex problems in a jiffy when compared to the present day supercomputers. Blockchain is another technology that has gained momentum in the previous decade. With the emergence of Bitcoin and other cryptocurrencies, blockchain seems to provide a promising future for safe and secure transactions. Hashing, which is essentially a complex mathematical problem, is an integral part of blockchain. Hashing is the concept that makes a blockchain so secure and immutable. With the advent of quantum computers, blockchain's security is rendered questionable. This paper aims to provide an overview of the current scenario between these two technologies, essentially a juxtaposition of blockchain and quantum computers.*

Key Words: **Quantum Computing, Blockchain, Hashing, Cryptocurrency**

1. INTRODUCTION

Juxtaposition means placing two things close to each other that have divergant effects. Here, the two things that are being put into juxtaposition are blockchain and quantum computers and their two contrasting properties are the complex cryptography and the rapid computation speed. Blockchain implements complex cryptography through one-way functions called hashes. They are called one-way functions because computing the factors of these hashes is extremely difficult. The present day cryptographic algorithms such as RSA, Elliptic Curve Digital Signature Algorithm, Elliptic Curve Diffie-Hellman and Digital Signature Algorithm all help blockchain to produce hash values. These algorithms were proven effective evenagainst the most powerful present day supercomputers. However, they may not stand against the test of quantum computers. Quantum computers are fundamentally different than classical computers. They can compute exponentially more states at the same time when compared to a classical computer. Due to this ability of quantum computers, the security of cryptographic algorithms is in jeopardy, and eventually blockchain's too. There are various factors that influence quantum computers to crack these cryptographic functions such as Grover's search algorithm and Shor's algorithm. Attempts have been made to secure blockchain from attacks of quantum computers and the same are discussed in the following sections of this paper.

1.1 Blockchain

The renowned cryptocurrency Bitcoin gave birth to the blockchain technology[1]. Blockchain in essence is a new method of maintaining records. Every recorded transaction is considered as a block. Each block contains data pertaining to that transaction along with a timestamp and a hash value of the previously occurring block. It is the hash value in the block that provides immutability to a blockchain. Depending on the algorithm used, every string of data will have its unique hash value. No two different strings of data can have the same hash value. Since hash values are very difficult to factorize, it becomes nearly impossible to tamper with the contents of a block. This is because any change in the contents of a block will change its hash value significantly eventually leading to a break in the chain. Anyone who wishes to make changes to a block will have to make changes to each and every block in the blockchain in order to show its authenticity. Even if someone manages to change contents of every block in the blockchain, it cannot persist as an authentic blockchain because of the distributed ledger.

Every participant in the blockchain network has a register of occurring transactions called as a distributed ledger. This ledger keeps on updating itself with every occurring transaction. For a transaction to persist in the blockchain, it must have the consensus of the participating members of the blockchain. Consensus is achieved through an algorithm called the consensus algorithm. Depending on the blockchain, the consensus algorithm may be different. In some cases, a transaction is only added to the blockchain if and only if more than 50% of the members have verified that transaction.

Due to such a rigorous procedure, blockchain to provide platforms for secure communications, unambiguity, privacy of data, and durability[2]. Due to the popularity that it has gained, blockchain has been recommended as a prominent technology for multidisciplinary applications like supply chain and logistics, smart manufacturing units

and e-voting[3].

1.2 Quantum computing

Quantum computers are machines that use quantum phenomena such as superposition and entanglement to perform computation. The laws of quantum mechanics drive the concept of quantum computation. Due to this, quantum computers present a massive speed in computation. Quantum computers are fundamentally different in nature. Unlike classical computers that store and read information in the form of binary bits, quantum computers make the use of qubits. Also known as quantum bits, qubits are able to encode information as 1s, 0s or both at the same time. The ability to store multiple states together is what makes a quantum computer so fast.

1.3 Threat to Blockchain

Quantum computers can solve mathematical problems such as integer factorization dramatically faster when compared to classical computers. Because of such computational ability, evolving quantum computers pose a threat to the classical cryptographic algorithms such as RSA, ECDSA (Elliptic Curve Digital Signature Algorithm), ECDH (Elliptic Curve Diffie-Hellman), and DSA (Digital Signature Algorithm) that help blockchain to generate hashvalues.

The main threat is Grovers algorithm[4], which can excellently fasten the inversion of functions. The problem of finding an image of a value before going through a function that is difficult to invert can be solved specifically using Grover's algorithm. Brandon Rodenburg and Stephen P. Pappas[5] have mentioned that the rapidity due to Grovers algorithm happens to be a factor of the square root of the number of possibly occurring hashes. It means, a hash value that is subjected to an attack from a quantum computer, would not have adequate security when compared to a hash value that has 50% of the bits when subjected to an attack from a classical computer. If we havea signature which is obtained after hashing the value of data $s = H(d)$ and if the function $H(d)$ is implementable on a quantum computer, then using Grover's algorithm we can find d for a given s in time of order $O(\sqrt{n})$ where n is the size of the space of valid hashes.

Another threat that blockchain's security faces is through the Shor's algorithm[6]. Shor's algorithm drastically boosts the efficiency of factorization of very large numbers. Thus, asymmetric key cryptographic algorithms such as RSA and similar algorithms can be broken using Shor's algorithm. Ifa blockchain relies on asymmetric key cryptography, then it's security is at risk.

Brandon Rodenburg and Stephen P. Pappas[5] have mentioned that in a pragmatic approach, this generates RSA keys of 4096 bits in implementation resistant to classical computation, but not resistant to quantum computer attacks.

Thus, RSA or similar algorithms would be vulnerable to attacks from quantum computers and so would be the aspects of blockchain that implement them.

2. QUANTUM-SECURED BLOCKCHAIN

In the research paper by Kiktenko, et al.[7] a blockchain protocol has been proposed. A secure authentication based on a network in which each pair of nodes is connected via a quantum key distribution (QKD) link. Here, the blockchain protocol consists of two layers and the network consists of n nodes. The first layer communicates private keys securely for each pair of nodes in the QKD network. The second layer is used to transmit messages with authentication tags securely that are created using the private keys obtained from the first layer. The chaining process proposed here is different than usual. In the proposed Quantum-secured blockchain, the unconfirmed transactions are aggregated together to avoid quantum computer attacks. This ensures protection from attacks of quantum computer in minimum two number of ways. First, the digital signatures would not rig the transactions. Second, a node equipped with quantum computing capabilities is able to generate new blocks colossally faster than another node without quantum computing capabilities.

It is also emphasized that the protocol intensively focuses on the data. Quantum channels are only used for the purpose of producing private keys. This protocol appears to be resistant to quantum computer attacks on newly generated blocks and distribution of transactions. The only drawback is that the database still remains vulnerable. This protocol has been tested in Moscow experimentally.

3. POST-QUANTUM CRYPTOGRAPHY

The following algorithms can be utilized to prevent a threat to Blockchain:

3.1 Code-based cryptography

As Overbeck R., Sendrier N.[8] have explained, code-based cryptography are the cryptosystems that use error correcting codes C in the algorithmic primitive. The algorithmic primitive is the underlying one-way function. This primitive may consist in adding an error to a word of C or in computing a syndrome relative to a parity check matrix of C.

The initail versions of the cryptosystems is a public key encryption scheme and it was proposed by Robert J. McEliece[9]. The public key is a random generator matrix.

This matrix is the arbitrarily permuted variation of theGoppa

code. The private key is an arbitrary binary Goppa code that is irreducible. Cipher text is gained after the addition of errors to the code word. These errors can be removed only by the owner of the Goppa code which is the private key. When some parameter adjustments were made three decades later, no attack was known to represent a serious threat on the system, even on a quantum computer[9].

After the first proposal of a code based cryptosystem by Robert J. McEliece, all other proposals suffered a common problem: they all had large memory requirements. A similar performance problem was observed in Jean-Bernard Fischer and Jacques Stern's[10] pseudo-random generator. Various proposals were made to modify McEliece's scheme in order to reduce the key size, however, most of them turned out to be insecure or inefficient. Code-based cryptography, however, is a potential candidate for post-quantum cryptography.

3.2 Lattice-based cryptography

As Micciancio and Regev (2008) have explained in their paper, a lattice is a set of points in n-dimensional space with a periodic structure[11], such as the one illustrated in Figure 1. Given 'n' linearly independent vectors b1,b2,b3 bn, with each vector containing m entries, the lattice generated by them is defined as all possibleweighted sums of these vectors when scaled by integers. To create a 2D vector we choose two points for e.g (4,2) & (2,4) and choosing another random number such as a=6,b=-3 and multiplying a with 1st point and b with 2nd which would compute to (24,12) & (-6,-12) and byunceasing this process would generate a lattice with the basis containing vectors (4,2) & (2,4). Depending on these a short vector, long vector, and closest vector problem.

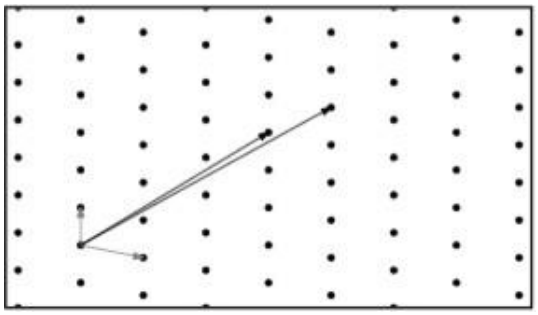

Fig -1: A two-dimensional lattice and two possible bases[11].

A short basis lattice problem can be explained as, given a long basis for some lattice "L", find the short basis for L. The advantage of the lattice is that no efficient algorithm, classical or quantum, can solve these problems in better than exponential time. It includes the generation of cryptographic primitive that involves lattice in underpinning security or security proofing.

Lattice-based cryptographic constructions are quite appealing for post-quantum cryptography, as they ensure robust security proofs, even for worst-case hardness, relatively impressive implementations while keeping things simple. Lattice-based cryptography is believed to be secure against quantum computers.

3.3 Multivariate-based cryptography

According to Ding, Jintai & Yang, Bo-Yin (2009), the foundation of Multivariate Cryptography schemes is the challenge of computing non-linear equation structures over finite fields[12]. As Asif, Rameez. (2021) has explained in his paper titled Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms, seeking a solution for such structures is called an NP-complete/NP-hard problem. All Multivariate Public-Key Cryptosystems (MPKC) use the same basic architecture, since they all rely on the use of multivariate polynomials over a finite field. The degree of polynomial is two in most cases which results in multivariate quadratic polynomials. These are still credited with being solved as NP-hard[13]. The Shor's algorithm does not seem to crack the MQPKC more easily with a classical computer. This is because it does not rely on any of the complex problems that Shor's algorithm can solve when compared to various other versions of public-key cryptography. It is also a potential candidate group for, a quantum-resistant encryption scheme[14].

When compared to other encryption schemes, multivariate offers various advantages. Multivariate schemes outperform most of it's competitors with regard to speed and can be implemented efficiently. What makes multivariate schemes attractive is the fact taht they are quick and demand only modest computational resources. [15].

Multivariate schemes employ simple arithmetic operations such as multiplication and addition and thus can be utilized on cheap devices like RFID chips. Also, signatures in Multivariate schemes are very short, upto a few hundred bits. However, the major disadvantage of multivariate schemes is that it has a large size of public keys. The public key size is typically about 10 to 100kB which are much larger than that of RSA like classical schemes.

4. COMPARISION OF POST-QUANTUM CRYPTOGRAPHIC ALGORITHMS

The following table shows a comparison of above mentioned three post-quantum cryptography approaches. The basis of comparison are the size of public and private keys and claimed quantum and classical security. The figures are adopted from the works of Tiago M. Fernandez-Carames and Paula Fraga-Lamas on Post-Quantum

Blockchain[16]. The authors have very meticulously mentioned the efficacy of these post-quantum cryptosystems on various processors. The figures in the following table are an aggregated representation of the figures mentioned in the original paper by Tiago M. Fernandez-Carames and Paula Fraga-Lamas.

Table -1: Comparison of Post-Quantum Cryptographic algorithms

Comparison of post-quantum cryptography algorithms				
Name of the algorithm	**Claimed Quantum Security**	**Claimed Classical Security**	**Public Key Size**	**Private Key Size**
Code-based Cryptography	64 bits, 96 bits,128 bits	128 bits, 192 bits, 256 bits	6,824 ~ 10,862,529 bits	320 ~ 159,376 bits
Lattice-based Cryptography	100 bits, 101 bits, 164 bits, 230 bits, 233 bits, 128 bits ~ 308 bits	128 bits, 192 bits, 256 bits, 153 bits ~ 368 bits	6400 bits ~ 172,160 bits	320 ~ 25,344 bits
Multivariate-based Cryptography	128, 192, 256 bits	46 bytes ~ 7106 Kbytes	93 Kbytes ~ 122701 KBytes	N.A

5. BLOCKCHAIN BASED E-VOTING SYSTEMS:

In their paper, Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson[17] have introduced a blockchain based e-voting system that is unique in nature. The system makes use of smart contracts for lower cost and safe election that ensures voter privacy. The design, vulnerability analysis and the system architecture has been outlined. Blockchain technology has been presented that provides new possibilities for democracies to transition from traditional election systems to a more timely and low cost system. While being time efficient, it also augments the security practices of present day election schemes. Ethereum[18], which is another renowned cryptocurrency is used in the private blockchain where it is possible to execute numerous transactions on the blockchain. This utilizes every virtue of smart contract to reduce the processing pressure on the blockchain.

However, Ethereum uses ECDSA (Elliptic Curve Digital Signature Algorithm) for its public-key cryptography. If e-voting systems based in Ethereum are to be implemented, the cryptographic algorithm must undergo a change so that the system is quantum resistant.

6. CONCLUSION

Thus, this paper gives a brief idea about two of the most significant technologies that define the future of engineering science; blockchain & quantum computing. This paper provides us with the current scenario of these two technologies and how quantum computing is posing a threat to blockchain. A comparative study has been done on various Post Quantum Cryptography Algorithms and based on the analysis, we determine which algorithm suits the best for the new iterated e-voting which shall be conducted in the future.

Table -2: Performance comparison of Post-Quantum Cryptographic algorithms

Performance comparison of post-quantum cryptography algorithms			
Name of the algorithm	**Speed of the algorithm**	**Resistance against quantum attacks**	**Size of the key exchange**
Lattice-based cryptography	Fast	Resistant against quantum attacks	1Kb
Code-based cryptography	Slower than Lattice-based cryptography	Resistant against quantum attacks	1Mb
Multivariate-based cryptography	Slow	Limited resistance against quantum attacks	Not Applicable

REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] M. Swan, “Blockchain: blueprint for a new economy”. First Edition, O’Reilly Media, Jan. 2015.

[3] T. M. Fernández-Caramés, O. Blanco-Novoa, I. Froiz-Míguez and P. Fraga-Lamas, "Towards an Autonomous Industry 4.0 Warehouse: A UAV and Blockchain-Based System for Inventory and Traceability Applica tions in Big Data-Driven Supply Chain Management," Sensors, vol. 19, no. 10, p. 2394, May 2019.

[4] L. K. Grover, "A fast quantum mechanical algorithm for database search". In Proc. 28th Annual ACM Symposium on the Theory of Computing, Philadelphia, USA, May 1996.

[5] Brandon Rodenburg, PhD Stephen P. Pappas, PhD, "Blockchain and Quantum Computing" MITRE Technical Report, June 2017.

[6] P. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM Journal on Computing, vol. 26, no. 5, pp. 1484-1509, Oct. 1997.

[7] Kiktenko, et al. "Quantum-secured Blockchain", June 5, 2018.

[8] Overbeck R., Sendrier N. (2009) Code-based cryptography. In: Bernstein D.J., Buchmann J., Dahmen E. (eds) Post-Quantum Cryptography. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-88702-7_4

[9] McEliece, R.: A public key cryptosystem based on algebraic coding theory.DSN progress report, 42–44:114–116 (1978).

[10] Fischer JB., Stern J. (1996) An Efficient Pseudo-Random Generator Provably as Secure as Syndrome Decoding. In: Maurer U. (eds) Advances in Cryptology — EUROCRYPT '96. EUROCRYPT 1996. Lecture Notes in Computer Science, vol 1070. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-68339-9_22

[11] Micciancio D., Regev O. (2009) Lattice-based Cryptography. In: Bernstein D.J., Buchmann J., Dahmen E. (eds) Post-Quantum Cryptography. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-88702-7_5

[12] Ding, Jintai & Yang, Bo-Yin. (2009). Multivariate Public Key Cryptography. 10.1007/978-3-540-88702-7_6.

[13] Ding, Jintai & Petzoldt, Albrecht. (2017). Current State of Multivariate Cryptography. IEEE Security & Privacy. 15. 28-36. 10.1109/MSP.2017.3151328.

[14] Asif, Rameez. (2021). Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms. IoT. 2. 71-91. 10.3390/iot2010005.

[15] Ding J., Petzoldt A., Wang L. (2014) The Cubic Simple Matrix Encryption Scheme. In: Mosca M. (eds) Post-Quantum Cryptography. PQCrypto 2014. Lecture Notes in Computer Science, vol 8772. Springer, Cham. https://doi.org/10.1007/978-3-319-11659-4_5

[16] T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks," in IEEE Access, vol. 8, pp. 21091-21116, 2020, doi: 10.1109/ACCESS.2020.2968985.

[17] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain-Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018, pp. 983-986, doi: 10.1109/CLOUD.2018.00151.

[18] Vujičić, Dejan & Jagodic, Dijana & Ranđić, Siniša. (2018). Blockchain technology, bitcoin, and Ethereum: A brief overview. 1-6. 10.1109/INFOTEH.2018.8345547.