Quantum Blockchain: A Persuasive Approach for Future Security

Hareram Giri[1], *Ravi Kumar Singh Pippal*[2]
[1]MTech Scholar, [2]Professor
[1]Department of Computer and Science Engineering, Vedica Institute of Technology, Bhopal, India
[2]Department of Computer and Science Engineering, Vedica Institute of Technology, Bhopal, India
harry3719@gmail.com[1] ravesingh@gmail.com[2]

Abstract: The term blockchain refers to the data which is scattered, crystalline and ledger of cryptographically linked. Publicly accessible servers store and copy sequence of blocks of data in blockchain terminology. The blocks are pointing to the previous block by hash pointer and all the transactions within the block are in the blockchain technology organized into a Merkel tree for the efficient proof of existence so it is a chain structure. For ensuring the unmodifiable data in redundant storage of multiple nodes, verifying and identity data digital signatures and hash functions are used in the Blockchain. In future for fast progress of quantum computing Grover's and Shor's algorithmic attacks performing possibilities are opened. Post-quantum or quantum-resistant cryptosystems are creating the algorithms that can be threaten for public-key cryptography and hash functions, forcing to redesign blockchains for the utilization of cryptosystems that withstand quantum attacks. This chapter is focused on post-quantum cryptosystems and the methods applied to blockchains. Moreover, post-quantum blockchain is studied along with their challenges faced by researchers. Along with that, this chapter is dedicated to provide comparative analysis of characteristics, performance measures as well as limitations of post quantum block chain techniques. So, this chapter is capable to give a broad view and useful guidelines to future blockchain researchers and developers. This chapter emphasize the drawbacks of blockchain after quantum computing attack and also helps to understand the characteristics and parameters. This chapter also presented the contribution of quantum key distribution to make blockchain more security and more efficient.

Keywords: Security Issues, Cryptography, Quantum computing, Blockchain

I. Introduction

As the need for network capacity rises for the existing data rate and the security and computational requirements together, the classical methods cease to provide both in the field of communication and computing a promising and efficient solution. This problem and the advancement of quantum mechanics contributed to the development of quantum communication and computing. Quantum mechanics have many phenomena in itself, which in classical domain do not have any counterpart like entanglement. Thus, if the concepts of quantum mechanics can be implemented in the fields of computation and communication, they can create Informatics already have jumped into a Nano-scale in which the action of quantum mechanics is regulated and computation and communication are entangled in the fields so that one needs improvement in the other. People like Richard Feynman, who were pioneers or leaders, said that, if information bits can be physically present, communication can use quantum mechanical properties[1]. better and more effective algorithms than what we are currently using. For information transmission decoding, electron spin, photon polarization or similar quantum properties can be used. This article includes the following details in order to achieve a deeper understanding. The fundamental premises of quantic mechanics, which govern quantum communication and computation, polarization and intertwining, and different applications such as teleporting, quantum cryptography, satellite communication, etc.

Scientists are preparing to develop a new form of machine called quantum computer because it has immense computing power that helps us to solve the difficult mathematical problems that hold back our advancement in various fields. A classical machine renders calculations using the 0 and 1 bits, of which 0 is off and 1 is on. The data is interpreted by transistors in the form of non- and zero-sequences. More computer power is given by the transistors. Two possible states are zero or one in classical machine bits. In Quantum Computing, Qubit is a knowledge unit. Qubit has unique features to solve the complex problem even more easily than conventional bits. Superposition is one property, which states that a Qubit can hold a combination of 0 and 1 simultaneously, not holding a value of either 0 or 1 like a classic bit. There are two possible zero and one states in Qubits, but these states are superimposed by zero and one. Qubit does not have to be one of those states in Quantum Universe. Any proportion of those states can be that.

II. Basics of Quantum Computing

Superposition of states: The basic theory of quantum mechanics is quantum superposition [2]-[5]. It's just like a wave as in classical physics, which leads to another true quantum state when overlapping two or more states.

Qubits Qubit: It is the fundamental unit of quantum data. Qubit is a description of a two-dimensional quantum system. Qubit can be in two states |0> and |1> or superposition from the two states. The difference between the qubit and the classic bit. In the classical bit, the bit is in a state of 0 or 1. Example: spin of an electron that can be seen as a drag and drop on two levels.

Quantum gates: The quantum gate is a fundamental quantum circuit running on a smaller number of qubits. The Quantum Circuits serve as a building block.

Quantum Entanglement: Quantum interconnection [6] is an effect which happens when the distribution of a number of substances is interacted in a way that does not allow the quantity status of each of the particles to appear separately, even if a large separation is present.

An electrical impulse is defined as either 1 or 0 in classical computation, where 1 indicates high current and 0 denotes voltage drop. Since the state of the quantum object is not understood until we observe it, in quantum computing. Therefore, the superposition of any possible state exists. Remember, for example, the spin of the electron to a bit that is spin up=0 and spin down=1. The exact spin of the electron can not be determined and the superposition of all possible spins is thus formed. "The respective generated bit is referred to as "qubit. In classical machine computation, the possible combinations are 00, 01, 10 and 11 if we take two bits of each digit, which can have a value of either 1 or 0. When you take the two electrons, their potential spin can be both 0 and 1 simultaneously, so they are much greater than the number of bits permitted by classical computing.

III. Ideal Characteristics of Blockchain Post-Quantum Schemes

A post-quantum cryptosystem would need to provide blockchain with the following main features in order to be efficient:
Tiny key sizes. In order to reduce the required storage space, the devices that interact with a blockchain need to ideally make use of small public and private keys. Furthermore, when managing them, tiny keys involve less complex computational activities. This is extremely significant for blockchain, which involve the ability to interact of IoT devices, usually limited by storage and computational power. There can be no doubt that IoT has experienced a significant growth in recent years, as with other advancing technology but IoT devices still face some important challenges, especially with regard to security.
Small and hash long signature. Data transactions, including user signatures and data/block hashes, are essentially stored by a blockchain. Therefore, the Blockchain size will also increase if signature/hash length increase.
Speedy Execution. In order to enable a blockchain to process a large number of transactions per second, post-quantum schemes need to be as fast as possible. Furthermore, a quick execution usually entails little computer complexity, which is necessary to avoid blockchain transactions by restricted devices with resource.
Low complexity in computing. This feature relates to rapid execution, although it is worth noting that rapid performance with other hardware does not imply computational simplicity in the post-quantum cryptosystem. For example, Intel microprocessors that use the Advanced Vector Extensions 2 (AVX2) instruction set can quickly execute some schemes, but when executed on ARM-based microcontrollers, the same schemes can be classified as slow. Therefore, a compromise between computational complexity, run-time and supported hardware devices must be sought.
Low energy consumption. Because of the energy required to execute its consensus protocol, some blockchain like Bitcoin are considered to be power hungry. Other factors have an impact on power consumption, such as the hardware used, the quantity of communications transactions performed and, obviously, the security schemes implemented, which, due to the complexity of the operations performed, can draw a relevant amount of current.

IV. Performance Comparison of Post-Quantum Cryptography

Lakshmi et al. [1] explained that for safe information sharing wherein two parties are actively engaged, cryptography is utilized. Transmitting sensitive information is the most common cryptographic challenge. Utilizing the cryptographic protocols confidentiality is retained. Instead of resolving, mathematical problems the protection of quantum cryptography depends mostly on physics, particularly quantum mechanics and statistics. Quantum key distribution which is utilized to build communication by producing cryptographic keys is a well-known usage of quantum cryptography. In addition, it is cantered on the theory of Heisenberg uncertainty, which assures protection and avoids privacy leakage. Essentially, in this work description and analysis of quantum cryptography with faint laser pulses, polarisation coding, phase coding, and frequency coding has been done.

Sharma et al. [2] discussed that while most IoT devices are designed without taking the security problem into account, IoT-based healthcare is particularly susceptible. Moreover, these smart devices can be linked to worldwide networking so that they can be instantly reached everywhere. Security problems such as mobility, device limitation, scalability, communication media, complex topology and, above everything else, privacy and confidentiality of information in storage or transmission are a few of them. Several other safety protocols and methodologies, such as steganography, AES cryptosystems, and RSA cryptographic technologies have been utilized in IoT-based healthcare services. As it is mandatory To ensure the confidentiality, safety, and authenticity of patient information collected and transferred from IoT-based healthcare systems, thus it is important to utilize the quantum cryptography technology. Quantum cryptography is a very interesting cyber security domain that uses quantum mechanics to expand a cryptosystem that is meant to be an impregnable protected device.

Kon et al. [3] discussed that the private Information Recovery (PIR) is a database query technique that offers consumer confidentiality by allowing the consumer to understand a given database record of their interests, but their query would be hided from the data centre. Symmetric recovery of personal information (SRPI) drives PIR even more by providing database confidentiality in advisement, where no new database entries can be learned by the consumer. unconditional protection of SPIR approaches with several databases are known conventionally, but are impractical since for protected connectivity and consensual unpredictability in the protocols, they need long shared confidential passwords among the parties. In this, rather than a realistic application, they suggest utilizing quantum key distribution (QKD) that could consider both the necessities of safe interaction and consensual unpredictability. They show that the protection of the SPIR protocols is maintained by QKD and that it is also protected against any external eavesdropper. They also illustrated that how such a classical-quantum framework can be applied realistically, utilizing the instance of a two-database SPIR protocol with passwords created by measuring device-independent QKD. They demonstrated via key rate calculations that such an application is possible with existing QKD technologies at the metropolitan stage.

Nath et al. [4] worked on smart grid is an extremely sustainable power infrastructure fitted with a cyber-physical structure for the sustainable generation, transmission and use of electricity. It is a designed network which utilizes information technology to safely and effectively deliver electricity. In the smart grid, flow of electricity is bidirectional, i.e. two-way communications with regulation. It can be utilized for surveillance of power automatically and secure delivery. It provides necessary heterogeneous power information interventions and the plausibility of multiple attacks on the shrewd system that negotiates the confidentiality and integrity of power records. The goal is to avoid digital attacks on the Smart Grid platform using quantum cryptography technique.

Sharma et al. [5] provides a comprehensive summary of the QKD technology is given in this article. The security key distribution between the two trusted entities is protected from unapproved accessibility utilizing this technology. In the subsequent stage, the structure of quantum cryptography is explained. Eventually, several major areas of use and drawbacks of this technology were addressed.

Kiselev et al. [6] discussed the function of chromatic dispersion in the subcarrier wave quantum key distribution network. Under the impact of chromatic dispersion, they developed a mathematical model of the shift in multi-mode weak coherent phase-coded conditions in a fibre channel and measured the asymptotic protected key rate. The lack of any reimbursement would restrict the overall span of the channel to 53 km. They suggested a method for minimising the impact of dispersion that greatly enhances the reach of the device. Every theory demonstrated is verified experimentally.

Pirandola et al. [7] provided both a basic overview and a state-of-the-art summary of the current developments in the area, both theoretically and experimentally. They started by analyzing quantum key distribution protocols based on discrete variable systems. First, we take into account aspects of computer independence, satellite problems, and continuous-variable systems-based protocols. They then addressed the ultimate restrictions of point-to-point personal communications and how these constraints can be resolved by quantum repeaters and networks. Eventually, they covered some aspects of quantum cryptography, such as quantum random number generators and quantum digital generators, besides regular quantum key distribution.

When elementary quantum protocols, like polarised photons, are utilized by **Bennett et al**. [8] to transfer digital data, the concept of uncertainty inevitably leads to novel cryptographic phenomena that are not feasible with conventional transmitting media such as a communication channel on which, it is difficult to pay attention without a significant likelihood of disrupting the transmission in a manner that can be observed. In comparison with regular vulnerable classical channels, a quantum channel may be utilized to transmit random important data between two consumers with the guarantee that it stays undisclosed to anybody else, though if the consumers at first disclose no confidential information. Through the exchange of quantum messages, they also presented a procedure for coin-tossing that is protected against typical ways of fraud, even by an adversary with infinite computing power, but can inevitably be corrupted through the utilization of an even more subtle quantum principle, the paradox of Einstein-Podolsky-Rosen.

Zoni et al. [9] presented an efficient and versatile design for the execution of the bit-flipping protocol addressing broad QC-LDPC codes for post-quantum cryptography. Researchers utilized the nine configurations of the LEDAcrypt cryptosystem as indicative application scenarios for QC-LDPC codes appropriate for post-quantum cryptography to show the usefulness of their approach. Their template design will provide a performance-optimized decoder application for all the FPGAs of the Xilinx Artix-7 mid-range group for every configuration. The experimental findings show that even on the smallest FPGA of the Xilinx Artix-7 family, their optimized design enables the deployment of large QC-LDPC codes. Taking into consideration the application of their decoder on the Xilinx Artix-7 200 FPGA, the experimental outcomes demonstrate an overall output speed of 5 times throughout all LEDAcrypt setups, in comparison to the approved improved software installation of the decoder that uses the Intel AVX2 extension, .

Cavaliere et al. [10] presented a description of Quantum Key Distribution (QKD) systems techniques and approaches addresses their safety risks and explores quality management practices for QKD networks. They also introduced quantum random number generators (QRNGs) as an essential key component for both classical and quantum encryption systems, and resolve the security threats raised by the emergence of quantum computers.

Bhatt et al. [11] examined the widespread security challenges in IoT and the currently existing solutions along with their disadvantages. And after that, quantum cryptography is discussed with some of its variants. And eventually, the assessment was performed with respect to the benefits and drawbacks of the implementation of quantum cryptography for Security measures.

Al Hasani et al. [12] performed the experimental and numerical analysis of optical important transmission quantum cryptography utilizing the BB84 method. They build a hidden quantum security code and examine the safety of the BB84 protocol by introducing Eve into the device, disrupting the synchronisation of qubits between Alice and Bob by the existence of Eve and leading to errors in bits. Eventually, they improved the safety of quantum cryptography utilizing one-time pad technology and chaotic signal produced by semiconductor laser with optical feedback. Integrating the quantum key with the chaotic signal will ensure the system's overall protection.

V. Conclusion

The development in quantum computing have attracted the attention of researchers and developers those who are contributing their efforts in the field of blockchain in which hash function and asymmetric encryption is important. This chapter is dedicated to analyze and discuss the impact of quantum-computing attacks on blockchain as well as postquantum cryptosystems to mitigate such attacks. The maximum relevant post-quantum schemes were re discussed their application to blockchain was analyzed, and their main challenges analyzed for that purpose. Extensive comparisons were provided on the characteristics and performance of the most promising post-quantum public-key encryption and digital-signature schemes in the addition. So by this review we will easily understand broad view on blockchain and useful guidelines for the researchers and developers of the next-generation of quantum-resistant blockchains.

References

[1] Lakshmi, S. Venkata, et al. "Quantum Cryptography: In Security Aspects." Limitations and Future Applications of Quantum Cryptography. IGI Global, 2021. 47-61.

[2] Sharma, Anand, and Alekha Parimal Bhatt. "Quantum Cryptography for Securing IoT-Based Healthcare Systems." Limitations and Future Applications of Quantum Cryptography. IGI Global, 2021. 124-147.

[3] Kon, Wen Yu, and Charles Ci Wen Lim. "Provably Secure Symmetric Private Information Retrieval with Quantum Cryptography." Entropy 23.1 (2021): 54.

[4] Nath, B. Kedar, et al. "Quantum Cryptography for Security of Data in Smart Grid System."

[5] Sharma, Meenakshi, and Sonia Thind. "A Quantum Key Distribution Technique Using Quantum Cryptography." Research Anthology on Blockchain Technology in Business, Healthcare, Education, and Government. IGI Global, 2021. 263-271.

[6] Kiselev, Fedor, Roman Goncharov, and Eduard Samsonov. "Chromatic Dispersion in Subcarrier Wave Quantum Cryptography." International Youth Conference on Electronics, Telecommunications and Information Technologies. Springer, Cham, 2021.

[7] Pirandola, Stefano, et al. "Advances in quantum cryptography." Advances in Optics and Photonics 12.4 (2020): 1012-1236.

[8] Bennett, Charles H., and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing." arXiv preprint arXiv:2003.06557 (2020).

[9] Zoni, Davide, Andrea Galimberti, and William Fornaciari. "Efficient and scalable fpga-oriented design of qc-ldpc bit-flipping decoders for post-quantum cryptography." IEEE Access 8 (2020): 163419-163433.

[10] Cavaliere, Fabio, John Mattsson, and Ben Smeets. "The security implications of quantum cryptography and quantum computing." Network Security 2020.9 (2020): 9-15.

[11] Bhatt, Alekha Parimal, and Anand Sharma. "Quantum cryptography for internet of things security." Journal of Electronic Science and Technology 17.3 (2019): 213-220.

[12] Al Hasani, Mahdi H., and Kais A. Al Naimee. "Impact security enhancement in chaotic quantum cryptography." Optics & Laser Technology 119 (2019): 105575.