# Quantum Computing Threats and Opportunities to Blockchain Security

Ahmed Elarabyi[1], Javed Ahmed[2]

***Abstract*- Knapsack is a combinational optimization problem which is based on selection of the best possible collection of values and weights capacity. Selection of values varies and depends on the social and environmental situations. The research work is focused on practical approach of the Multidimensional Knapsack problem (MKP). This paper comprises an introductory part of Genetic Algorithm and understanding towards Knapsack problem. The program is developed in Python programming language using the pyEasyGa libraries. The MKP program Genetic Algorithm class is initialized within defined population size. Fitness function is defined to evaluate best solutions in .shape of best values to maximize the beneficial point**

***Keywords: Multidimensional Knapsack Problem (MKP); Genetic Algorithm; Python, Fitness Function***

## INTRODUCTION

Computing has revolutionized data processing and management. The advancements of technology lead to the development of computers that process data with quantum mechanics, not with the mechanism of classical physics. The laws of physics relevant to the data processing are fundamental to understanding the computation limitations. The classical computing devices are thus referred to as "classical computers" utilizing classical mechanics laws. The quantum computers depend on quantum mechanics laws, resulting in a dramatic change in the computational capacity [1- 3]. The modern technology that considers a computational data framework called a blockchain provides an open, public, distributed ledger with various applications in different fields. The potential power of quantum technology will overcome blockchain's security, which relies on the difficulty of solving particular elliptic curve cryptography. Specifically, hashes, as used in signing the ledger blocks, can be compromised. A quantum computer can forge an elliptic curve signature that underpins every transaction security in blockchain by using Shor's algorithm variant [4]. In the organizations looking to utilizing blockchain technology, after completing a migration to a blockchain-based system, unless you are solving this challenge upfront, you will need to move again to a system that can resist quantum computers [5, 6]. This article discusses how quantum technology makes blockchain technology vulnerable and how it could make it more secure.

### *A. Principles of Blockchain Technology*

Blockchain is being described as the fifth disruptive innovation technology in computing [7, 8]. In the simplest way, it is a distributed ledger of records that is verifiable and immutable. Since, it was developed in 2008, the technology of blockchain has been utilized in different ways. The most significant application or impact of blockchain is seen as plenty of cryptocurrencies that have developed and sprung up. However, with time, blockchain technology gains an impact much broader than just the cryptocurrency scope and distributed ledger storage. Recently, cryptocurrency has gained full attention from both academia and industry. Bitcoin, usually called the first cryptocurrency, had earned tremendous success with the capital market attaining 10 billion dollars in 2016. The blockchain is the essential Bitcoin mechanism, and it was suggested in 2008 and implemented in 2009. Blockchain can be considered as a public ledger, in which all obliged transactions are stored in blocks of chain. This chain continuously increases when new blocks are added to it. Blockchain technology has main characteristics like decentralization, persistence, auditability, and anonymity [9]. The blockchain structure can describe as blocks sequences that are stored on and copied among publicly accessible servers. Each block has four main elements: a) the preceding block hash; b) the block data content; c) the nonce that is utilized to make a particular form to the hash; d) the block hash. The operation of blockchain can be described in Fig. 1

.

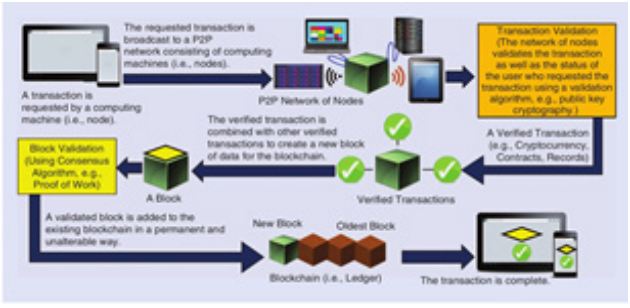


Fig. 1. Operations of Blockchain[10].

## QUANTUM THREATS TO BLOCKCHAIN

The security of blockchain relies on cryptographic algorithms to function. Some of the essential cryptography types used for blockchain security are hash functions, public-key

[1] South Valley University Qena, Egypt
[2] Sukkur IBA University

cryptography, and elliptic curve cryptography (ECC). The hash function has the property of one-way computation, which implies that it cannot be reversed and easy to implement on the classical computer. For example, multiplying two large prime numbers is simple to perform on the classical computer, but obtaining the prime factors for a particular product is challenging since it requires substantive computing power and time to achieve by the classical computer. The functions mentioned above are employed to create digital signatures that the blockchain participants order to verify themselves. It isn't easy to fabricate and simple to check. One-way functions are also applied to authorize the transaction records in the blockchain ledger. The resulting hash of the current block is obtained from the previous block's hash, the current one's associated data, and nonce. It results in a chain of blocks connected by an immutable link. If the attacker wants to hack a block N successfully, he has to change the previous block's hash. Again, finding the block's hash is relatively easy, but hard to select the nonce that would generate a particular hash value. That would require reversing the method to acquire the information that created the hash, which is useless since it is a one-way function. For example, to add a block into the chain toward Bitcoin, powerful computers called miners have to solve the required difficulty level to achieve the desired hash. This process will require a substantive computational capability for searching for the corresponding nonce to succeed that condition. The mining process delays new blocks' addition since it provides time for each to check every transaction and record it. In case of the proof of work, which is widely used for the blockchain's mining process, any node with sufficient computational power can work for the mining operation and add blocks to the chain. When we have a quick look at the history of security protocols, we can observe the sequence of attacks that broken them. For example, Allies broke the German military's Enigma code for encrypting the transmitted messages during the Second World War. Also, the Data Encryption Standard algorithm used for encrypting the transferred electronic messages is broken in 1997. It will be the same situation for blockchain technology in the advent of a quantum computer [11]. It will threaten the security of blockchain and search for the nonce quickly compared to the classical system. Hence, it can calculate the hash functions and hack the transmitted transactions over the blockchain. Therefore, one-way encryption will immediately become outdated. So, it is necessary to propose secure quantum protocols for protecting data and communications capabilities of resisting the tremendous power of the quantum computer in the environment of blockchain.

The operation of quantum computers relies on physics characteristics like superposition and entanglement. Indeed, quantum computing proved it has powerful computational abilities for various applications, especially communication and cryptography, compared to classical ones. For example, it is breaking the security protocols based on classical cryptographic algorithms. A blockchain is especially at risk because one-way functions are its single line of generating the digital signature and user's protection against eavesdropping. If a node in the blockchain implemented with a quantum computer could apply Shor's algorithm to produce any digital signature, mimic that node, and allocate their digital assets [4]. Most experts and professionals in the field estimate that this achievement would need a universal quantum computer, which is not available and will take time to achieve it. However, other researchers inform that this could occur earlier, adopting advanced quantum computational devices that possess different limited abilities, such as those being developed by IBM, DWave, Google, and others [12, 13].

The primary goal of Quantum computers is to get solutions for the hash difficulty problem quickly. It will facilitate the few enabled quantum nodes to control the transmitted transactions and manage the addition of blocks to the Bitcoin ledger. Furthermore, these nodes could destroy transactions, block their own from being recorded, or double-spend. These types of attacks, along with its impact on blockchain technology, have been highlighted by citeaggarwal 2017. It also summarized the potential consequences of quantum computers' evolution on Bitcoin, and the suggestion for the transition from the Bitcoin to the quantum-resistant is discussed in [14]. If nothing is done to update the protocols, cryptocurrencies will reveal once quantum computers are available.

## IMPROVING SECURITY OF BLOCKCHAIN

Fortunately, apart from posing a serious threat to blockchain technology, quantum computing offers some of the opportunities to enhance its security [6], [15- 18]. We can divide the problem of quantum-proofing the blockchain into two scenarios. In the first scenario, we deal with designing a quantum-resistant blockchain from scratch. The second scenario refers to quantum proofing the existing blockchain. It is significantly harder patching existing blockchain against quantum computing attacks than designing quantum-safe blockchain from scratch. Replacing the existing deployed cryptosystem with a post-quantum one makes the existing blockchain resistant against quantum computing attacks. Extensive research is currently being carried out in post-quantum cryptography. A number of post-quantum schemes are introduced, such as lattice-based schemes, codebased schemes, super singular isogenies schemes, multivariate polynomial schemes, and Merkle tree-based signatures, etc. But all these competing proprietary schemes are under-tested due to the absence of international standards. Fortunately, a long term standardization project was initiated by NIST in 2016 to identify candidate quantum-resistant cryptosystems. Some of the limitations of post-quantum cryptosystems are larger key sizes, signature size, a significant decrease in computational speed, etc. Post-quantum cryptosystems trade off efficiency for security. To design efficient quantum-resistant blockchain, there is a need for further research that

facilitates a significant reduction in signature size and key size. This approach of patching existing blockchain resistance against quantum computing attacks provides security for future transactions. However, the earlier transactions signed with pre-quantum signature schemes may be compromised to reveal public/private key pairs, which result in the theft of funds. The strategy to deal with such a quantum attack is either never reuse the public key or make sure to spend/ transfer all available funds from the address for which the public key has been revealed. Another major problem of patching existing blockchain is the high vulnerability of proof of work system against quantum adversaries. An asymmetric quantum adversary can solve the cryptographic puzzle significantly faster than the rest of the network. It gives rise to the possibility of rewriting the history of blockchain and launching a double spending attack.

Several researchers put forward the idea of classical blockchain with added quantum features. One of the exciting proposals is from Kiktenko et al. [19]. The authors combine a QKD (Quantum Key Distribution) layer to the classical blockchain, which protects the relevant sub-algorithms against a quantum computing attack. QKD is among very few mature technologies that have resulted from quantum cryptography. Using QKD, a random bit stream can be generated between parties. This secret shared key distribution approach is based on quantum physics laws instead of using mathematical complexity for security. The basis for the security of this approach is the Quantum No-cloning theorem. The QKD protocol facilitates the exchange of cryptographically secured encrypted messages if the random key has been successfully established between two parties. The advantage of using QKD over postquantum schemes is that it is resilient to cryptanalysis. In contrast, post-quantum schemes are based on computational assumptions and thus come with future cryptanalysis risk.

Rajan et al. [20] put forward the conceptual design for an intrinsically quantum blockchain using entanglement in time. Quantum blockchain is designed using quantum information principles, and its design is fully integrated into a quantum network. In the proposed conceptual design, classical blockchain's data structure component is replaced with a quantum system, whereas the classical consensus network with quantum network. The design's innovation is encoding the blockchain into a temporal GHZ(Greenberger-HorneZeilinger) states of photons that do not simultaneously coexist.

## CONCLUSION

The focus of the work presented in this paper is quantum computing threats to blockchain security. The article describes how classical blockchain applications can be compromised in the presence of asymmetric quantum adversaries. This research work paves the way to open new research frontiers in quantum information science. Quantum computing research is in its infancy stage and still has a long way to go to realize quantum computing hardware. Nevertheless, researchers working in blockchain technology consider the problem of quantum proofing the classical blockchain either by replacing pre-quantum cryptography with post-quantum cryptography or designing quantum blockchain, which is based on the principles of quantum information science.

## ACKNOWLEDGMENT

This work was carried out at the department of information security and communication technology, Norwegian University of Science and Technology, Gjovik, Norway during the tenure of an ERCIM 'Alain Bensoussan' Fellowship Programme.

## REFERENCES

[1] Lov K Grover. A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pages 212–219, 1996.

[2] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review, 41(2):303– 332, 1999.

[3] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Technical report, Manubot, 2019.

[4] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science, pages 124–134. Ieee, 1994.

[5] L Chen, S Jordan, YK Liu, D Moody, R Peralta, R Perlner, and D SmithTone. Report on post-quantum cryptography," national institute of standards and technology. US Department of Commerce, 2016.

[6] Daniel J Bernstein and Tanja Lange. Post-quantum cryptography. Nature, 549(7671):188–194, 2017.

[7] Bernard Marr. How blockchain technology could change the world. Forbes, May, 27, 2016.

[8] George Foroglou and Anna-Lali Tsilidou. Further applications of the blockchain. In 12th student conference on managerial science and technology, pages 1–8, 2015.

[9] Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone. Blockchain technology overview. arXiv preprint arXiv:1906.11078, 2019.

[10] Deepak Puthal, Nisha Malik, Saraju P Mohanty, Elias Kougianos, and Gautam Das. Everything you wanted to

know about the blockchain: Its promise, components, processes, and problems. IEEE Consumer Electronics Magazine, 7(4):6–14, 2018.

[11] Tiago M Fernandez-Caram´ es and Paula Fraga-Lamas.` Towards postquantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE Access, 8:21091–21116, 2020.

[12] Xinhua Peng, Zeyang Liao, Nanyang Xu, Gan Qin, Xianyi Zhou, Dieter Suter, and Jiangfeng Du. Quantum adiabatic algorithm for factorization and its experimental implementation. Physical review letters, 101(22):220405, 2008.

[13] Eric Anschuetz, Jonathan Olson, Alan Aspuru-Guzik, and Yudong Cao.´ Variational quantum factoring. In International Workshop on Quantum Technology and Optimization Problems, pages 74–85. Springer, 2019.

[14] Iain Stewart, Daniel Ilie, Alexei Zamyatin, Sam Werner, MF Torshizi, and William J Knottenbelt. Committing to quantum resistance: A slow defence for bitcoin against a fast quantum computing attack. Royal Society open science, 5(6):180410, 2018.

[15] H Jeff Kimble. The quantum internet. Nature, 453(7198):1023–1030, 2008.

[16] Anne Broadbent and Christian Schaffner. Quantum cryptography beyond quantum key distribution. Designs, Codes and Cryptography, 78(1):351– 382, 2016.

[17] Vlad Gheorghiu, Sergey Gorbunov, Michele Mosca, Bill Munson, et al. Quantum-proofing the blockchain. Blockchain Research Institute: University of Waterloo, 2017.

[18] Guillaume Chapron. The environment needs cryptogovernance. Nature, 545(7655):403–405, 2017.

[19] Evgeniy O Kiktenko, Nikolay O Pozhar, Maxim N Anufriev, Anton S Trushechkin, Ruslan R Yunusov, Yuri V Kurochkin, AI Lvovsky, and AK Fedorov. Quantum-secured blockchain. Quantum Science and Technology, 3(3):035004, 2018.

[20] Del Rajan and Matt Visser. Quantum blockchain using entanglement in time. Quantum Reports, 1(1):3–11, 2019.