iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** X **Month of publication:** October 2021

DOI: https://doi.org/10.22214/ijraset.2021.38510

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue X Oct 2021- Available at www.ijraset.com

A Review on the Impact of Quantum Computing on Blockchain Technology

Roman B. Shrestha[1], Ramika Pandey[2]
[1, 2]*Department of Computer Science, Kathmandu Model Secondary School, Kathmandu, Nepal*

Abstract: ***Blockchain is a promising revolutionary technology and is scalable for countless applications. The use of mathematically complex algorithms and hashes secure a blockchain from the risk of potential attacks and forgery. Advanced quantum computing algorithms like Shor's and Grover's are at the heart of breaking many known asymmetric cyphers and pose a severe threat to blockchain systems. Although a fully functional quantum computer capable of performing these attacks might not be developed until the next decade or century, we need to rethink designing the blockchain resistant to these threats. This paper discusses the potential impacts of quantum computing on blockchain technology and suggests remedies for making blockchain technology more secure and resistant to such technological advances.***
Keywords: Quantum Computing, Blockchain, Shor's Algorithm, Grover's Algorithm, Cryptography

I. INTRODUCTION

A. Classical Computation

The classical stack has been developing for a long time. From the invention of the transistor in 1953, the evolution of classical computers has been 70+ years in the making. These computers use bits(i.e. either 0 or 1) to solve the problems. These are electrical pulses that flow throughout the circuit to complete tasks. It seems the most significant breakthrough in technology, but still, it does not explore all the possibilities of nature.

B. Quantum Computation

We have been building the quantum stack for about 20 years, and it is not as sophisticated as the classical stack yet. In quantum computing, unusual properties of quantum physics are used to create an entirely new type of computation. A qubit(combination of 0s and 1s) is the fundamental unit of information on a quantum computer. Quantum computers can solve some types of problems much faster than regular computers. Just like classical computers did, quantum computers are evolving by asking questions, making improvements, and discovering new technologies. Quantum computers have an advantage over classical computers in:

1) Problems that involve too much searching or testing for regular computers to do quickly.
2) Problems that require secure encryption
3) Problems that involve simulating quantum mechanical systems

C. Blockchain Technology

A blockchain is a chain of blocks linked to each other by a cryptographic hash. It is an open, distributed digital public ledger that is duplicated and distributed across the network of computers on the blockchain. Blockchain is a promising revolutionary technology as it helps reduce risk, eradicate fraud, and makes it transparent and scalable for countless applications. Characteristics such as decentralization, persistency, anonymity and auditability form the backbone of blockchain technology. Although blockchain technology developed with its application for bitcoin [1], its applications go far beyond cryptocurrencies and bitcoins, ranging from how contracts are enforced to making government work more efficiently.

Blockchain technology is based on a digital, public, distributed ledger that is not controlled and monitored by any central authority and can be viewed by all users on the network. Blockchain comprises blocks of data, each of which contains a cryptographic hash of the previous block, a timestamp and transaction data. When users want to add transactions to the ledger, other computers encrypt and verify the data using cryptographic algorithms. If a majority consensus is reached, a new block of data is added to the chain of transactions. Blockchains are resistant to data modification because once recorded, the data in any given block cannot be changed without changing all subsequent blocks. The use of advanced cryptographic algorithms makes it almost impossible for someone to hack into a blockchain network.

©IJRASET: All Rights are Reserved

II. QUANTUM COMPUTING ALGORITHMS

Blockchain technology is based on cryptographic algorithms that are hard to decipher. These algorithms are based on the use of complex mathematical hashes and limitations of the computation power of classical computers. For example, RSA encryption works on the principle that it is challenging to factorize large numbers. This case, however, might not always hold. Shor, in 1994 invented his famous prime factorization algorithm [2]. Later in 1996, Grover developed a quantum search algorithm that solves the problem of unsorted databases [3]. These are at the heart of breaking many known asymmetric cyphers and thus are relevant to breaking things like public-key cryptography and digital signatures. In conclusion, both of these quantum algorithms pose a severe threat to blockchain systems.

A. Shor's Algorithm

Your In 1994, Peter Shor developed a quantum computing-based algorithm for factoring large numbers. The difficulty in factoring large numbers was the base of many complex cryptographic algorithms shielding the blockchain from potential hacking threats. If Shor's algorithm worked in real life, all of these present cryptographic systems would be useless. While only a few people were conducting quantum computing research in the past, this discovery significantly drew the attention of many researchers towards advancements in quantum computing.

Shor's algorithm results from number theory: the function $F(a) = x^a \bmod n$ is a periodic function when x is an integer coprime to n. In the context of Shor's algorithm, n will be the number we want to factor. When two numbers are coprime, it means that their greatest common divisor is 1. Calculating this function for an exponential number of a's would take exponential time on a classical computer. Shor's algorithm utilizes quantum parallelism to perform the exponential number of operations in one step.[4] Shor's algorithms can provide the solution to problems like the discrete logarithm problem, which in turn makes such cryptographic algorithms as ElGamal encryption, Diffie-Helman key exchange, the Digital Signature Algorithm, and elliptic curve cryptography insecure. The existence of Shor's algorithm demonstrates that a quantum computer opens vulnerabilities to the existing blockchain ecosystem.

B. Grover's Algorithm

Grover's algorithm [3] is one of the best quantum algorithms that can search an unsorted database quadratically faster than any known classical search. Blockchain relies on the calculation of hashes to ensure security against modification of previous blocks. Modifying a single block is secured by the difficulty of finding a hash collision with the existing hash, which amounts to the problem of inverting the hash function. Grover's algorithm is specifically a solution to the problem of finding a preimage of a value of a function that is difficult to invert. If we are given a signature that is the hash value of some data s=H(d), and the function H(d) can be implemented on a quantum computer, then Grover's algorithm allows us to find d for a given s in a time of order $O(\sqrt{n})$ where n is the size of the space of valid hashes. In other words, it allows us to generate hash collisions more efficiently than brute force search, which would be O(n).[5] While Groove's algorithm does not provide exponential speedup as Shor's algorithm, it can significantly improve almost any other quantum algorithm.

III.THREAT TO BLOCKCHAIN

The promises of blockchain can be invalidated easily with the two quantum computing algorithms we talked about previously. Shor's algorithm thus potentially breaks most of the currently implemented cryptographic algorithms and with them all the public-key cryptography mechanisms deployed on the Internet. Groove's algorithm can be used to search for hash collisions and replace the blocks without breaking the integrity of the chain. It can also be used to increase the speed to generate nonsense, potentially up to the point that it can recreate the entire chain with modified hashes consistently without breaking its integrity. We will now discuss a few possible attacks that can be carried out with these two algorithms.

A. Grover's Full Collision Attack

In order to modify a block in a chain, one will need to generate a full collision of a hash value. Generating a full collision hash value, however, is computationally expensive. This requires iterating over the possible inputs with enough extra bits to exhaust the hash space until a case is found that matches the known hash value [5]. An ideal hash requires linear time in the size of a hash space. However, Groover's algorithm reduces the time complexity to $O(\sqrt{n})$ and would have a 150% speedup compared to classical computing algorithms. This could make it possible to search for hash collisions in half the number of bits than in the hash. So, in any case, where attackers get a hold of quantum computing technology before the defenders (a worst-case scenario), it might be possible to modify a given block and hash and add trivial data to it.

©IJRASET: All Rights are Reserved

B. Effect on Mining time

The calculation nonces during blockchain mining are computationally expensive and necessary for rewriting the chain finding a pre-image to a partially defined hash. However, with increased computational power due to quantum computers and Grover's algorithm, calculating nonces and reconstructing chains from a modified block can be fast. So, quantum computing miners have a higher advantage while mining blockchains. In crypto mining, the attackers will have a higher edge over classical miners, and they can obtain currency faster by mining faster. In other cases, the fastest miners will dominate the generation of new blocks and take control of the blockchain's content. This can even lead to the recreation of a whole new blockchain and dominating and substituting the history of the actual chain. Since the longest chain is traditionally the accepted truth, a faster-growing chain will dominate the blockchain, successfully rewriting history [5].

C. Shor's Algorithm attack

Shor's algorithm is considered one of the significant scientific achievements of the 20th century. Shor's algorithm can easily break existing algorithms and systems such as the RSA, TLS, DSA and all the public-key cryptography mechanisms deployed on the Internet [6].

While this threat is not directly related to the structure of linked chains or hashes or generation of new blocks, breaking the encryption can easily allow the attacks to forge messages and signed content, which further passes to the main blockchain and gains legitimacy of being a part of publicly available, distributed verified record. All the encrypted communications will be vulnerable with the implementation of Shor's algorithm. We will need to seriously reconsider encryption methodologies to prevent the risk of such attacks in the coming future.

IV. POST-QUANTUM CRYPTOGRAPHY

Blockchain is now taking over the Internet. The implications on the blockchain are now limited not only to cryptocurrency but also to different fields such as health, education and even secret services. The mathematically complex algorithms and hashes secure a blockchain from the risk of potential attacks and forgery. However, a few quantum computing algorithms pose a real threat to the blockchain architecture. Although a fully functional quantum computer capable of performing these attacks might not be developed until the next decade or century, we need to rethink designing the blockchain resistant to these threats. Post Quantum cryptography (also known as quantum-resistant cryptography) aims to develop cryptographic systems that are secure against both quantum and conventional computers and can interoperate with existing communication protocols and networks. The cryptographic algorithms presented in this section do not rely on the hidden subgroup problem (HSP), such as factoring integers or computing discrete logarithms, but different complex mathematical problems.

A. Quantum Distribution Key

Quantum Key Distribution (QKD) challenges securely exchanging a cryptographic key between two parties over an unsecured channel. QKD is based on the basic characteristics of quantum mechanics that are invulnerable to increased computational power and can be achieved using the quantum properties of light, lasers, fibre optics and transmission technology.[7] This security, in particular, derives from the Quantum No-cloning theorem [8], a consequence of Heisenberg's uncertainty principle, which states that a signal made of a single quantum particle cannot be copied without introducing an observable error, preventing the interceptor from evading detection. The encrypted message is considered cryptographically secure once a random key is established between two parties via the QKD protocol.

B. Mathematics Based Solutions

There are many alternative mathematical problems to those used in RSA, DH and ECDSA that have already been implemented as public-key cryptographic schemes, and for which the Hidden Subgroup Problem (HSP) [9] does not apply; therefore, they appear to be quantum-resistant.

1) Lattice-based Cryptography: The construction of lattice-based cryptography [10] relies on the assumed hardness of lattice problems, the most basic of which is the shortest vector problem (SVP). This is a form of public-key cryptography that avoids the weaknesses of RSA. Rather than multiplying prime numbers, lattice-based encryption schemes involve matrix multiplication.
2) *Multivariate-based Cryptography*: The security of this public key scheme is based on the difficulty of solving systems of multivariate polynomials over finite fields. Multivariate cryptosystems can be used for both encryption and digital signatures.[11]

©IJRASET: All Rights are Reserved

3) Hash-based signatures: Hash-based signature schemes use one-time signature schemes as their building block. A given one-time signing key can only be used to sign a single message securely. Indeed, signatures reveal part of the signing key. The security of (hash-based) one-time signature schemes are based solely on the security of an underlying hash function.[12]

4) *Code-based Cryptography*: Code-based cryptography [13] refers to cryptographic systems that use error correction codes. The algorithms are based on the difficulty of decoding linear codes and are considered robust against quantum attacks when the key sizes are increased by the factor of 4.

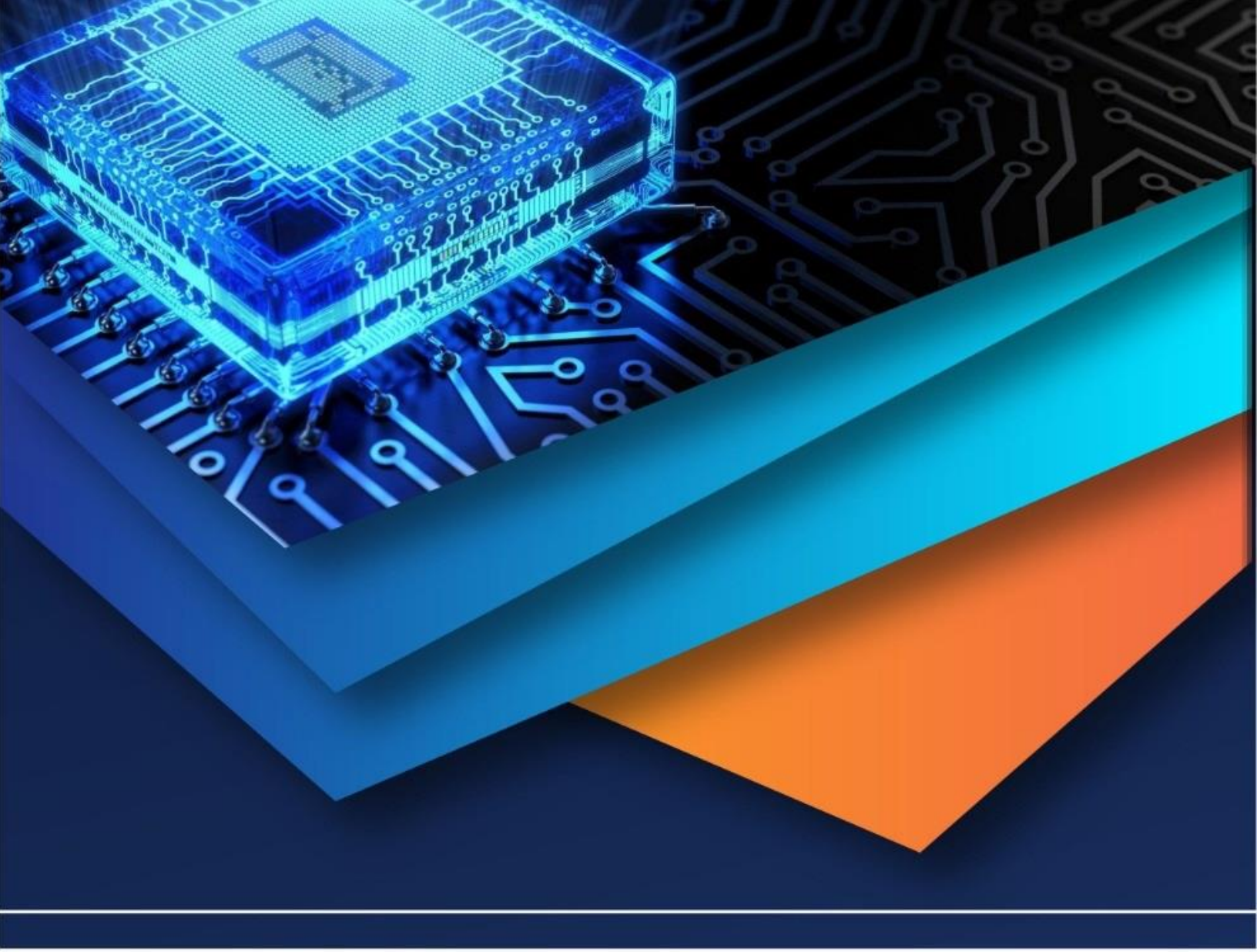
V. CONCLUSIONS

Emerging technologies such as quantum computing pose a real threat to the security of information of data. Some of the quantum computing algorithms can easily break today's most advanced cryptographic algorithms. However, the development of such advanced computers might take a decade or even a century. Building a scalable and fault-tolerant quantum computer is a moonshot effort and while today's best efforts are about a dozen qubits kept stable for a few microseconds, we would need millions of qubits stable for at least hours in order to make anything useful with quantum computers [6]. The consequence of this technical advancement can lead to the collapse of current methods and algorithms that are widely used for securing data and transactions. So, more research is needed in developing quantum-resistant cryptographic measures and possibly a quantum-based cryptography algorithm such as the QDK. We need to move forward in developing such a cryptographic system that is very secure and efficient.

REFERENCES

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Bitcoin.org. Retrieved October 10, 2021, from https://bitcoin.org/bitcoin.pdf.
[2] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484–1509. https://doi.org/10.1137/s0097539795293172
[3] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing - STOC '96. https://doi.org/10.1145/237814.237866
[4] Hayward, M. (1999). Quantum Computing and Shor's Algorithm. CiteSeerX. Retrieved October 10, 2021, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.121.1509&rep=rep1&type=pdf.
[5] Rodenburg, B., & Pappas, S. P. (2017). Blockchain and Quantum Computing. Mitre Corporation. Retrieved October 10, 2021, from https://www.mitre.org/sites/default/files/publications/17-4039-blockchain-and-quantum-computing.pdf.
[6] Aumasson, J.-P. (2017). The Impact of Quantum Computing on Cryptography. Computer Fraud & Security, 2017(6), 8–11. https://doi.org/10.1016/s1361-3723(17)30051-9
[7] Mavroeidis, V., Vishi, K., D., M., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. International Journal of Advanced Computer Science and Applications, 9(3). https://doi.org/10.14569/ijacsa.2018.090354
[8] Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. Nature, 299(5886), 802–803. https://doi.org/10.1038/299802a0
[9] Lomonaco, S. J., & Kauffman, L. H. (2002, June 17). Quantum hidden subgroup problems: A mathematical perspective. arXiv.org. Retrieved October 10, 2021, from https://arxiv.org/abs/quant-ph/0201095.
[10] Micciancio, D., & Regev, O. (2008). Lattice-based cryptography. Retrieved October 10, 2021, from https://cseweb.ucsd.edu/~daniele/papers/PostQuantum.pdf.
[11] Ding, J., & Yang, B.-Y. (2009). Multivariate public key cryptography. Post-Quantum Cryptography, 193–241. https://doi.org/10.1007/978-3-540-88702-7_6
[12] Dods, C., Smart, N. P., & Stam, M. (2005). Hash based digital signature schemes. Cryptography and Coding, 96–115. https://doi.org/10.1007/11586821_8
[13] Overbeck, R., & Sendrier, N. (2009). Code-based cryptography. Post-Quantum Cryptography, 95–145. https://doi.org/10.1007/978-3-540-88702-7_4

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)