Quantum Computing: A Threat to Blockchain?

Abstract

Blockchain is an open, public, decentralized system with an adequate safeguard against existing cyber threats that make it difficult or impossible to change, hack or cheat the system. However, this system is vulnerable to the advances in quantum technology and might not be able to protect itself against the future threats posed by large-scale quantum computers. Therefore, there is a need for post-quantum cryptography that would be impenetrable not only to future quantum attacks but also to classical attacks right now. This document, thereby, examines the shortcomings of Blockchain and how quantum computers could be used to enhance as well as exploit these vulnerabilities.

Keywords: Blockchain, Proof of Work, Quantum Computing, Superposition, Post-Quantum Cryptography

Introduction

Blockchain is an online cryptosystem of recording information using Distributed Ledger Technology that makes it difficult or impossible to change, hack, or cheat the system. Blockchain security relies on ‘one-way’ mathematical functions [1]. These are straightforward to run on a conventional computer and difficult to calculate in reverse. Hence, they use asymmetric encryption schemes: RSA cryptography for its difficulty of factoring or Elliptic Curve cryptography for its discrete logarithm problem. A blockchain is a chain of blocks that adds a new block whenever a transaction is requested and authenticated. A block in a blockchain contains

- Data (Depends on the type of blockchain)
- Hash of Block (Identifies a block and all of its contents and is always unique)
- Hash of the previous block

Hashes are very useful when you want to detect changes to blocks. The first block in a blockchain is a genesis block. Tampering with a block causes the hash of the block to change as well. In turn, that will make the next block and all the following blocks invalid because they no longer store a valid hash of the previous block. But using hashes is not enough to prevent tampering. So to mitigate this, blockchains have something called Proof of Work (PoW) [2]. It is a mechanism that slows down the creation of new blocks and prevents tampering since

tampering with one block will lead to recalculating the PoW of all other blocks in that blockchain. So the security of blockchain comes from its creative use of hashing and PoW.
One more way that blockchains secure themselves is by being distributed. A blockchain uses a peer-to-peer network and anyone is allowed to join. When someone joins this network, he gets the full copy of the blockchain. The node can use this to verify that everything is in order. Initially, a new block is created and sent to everyone on that network. Each node then verifies the block to make sure that it hasn't been tampered with. If everything checks out, each node adds this block to its own blockchain. Tampering with the new block would require tampering with all blocks on the chain, redoing the Proof of Work for each block, and taking control of more than 50% of the peer-to-peer network. This won't be easy to achieve and as a result, the blockchain will be secure against attackers.

Need for Quantum Computers

Conventional computer parts consist of chips made up of modules, which contain logic gates, which in turn contain transistors. The transistor is a switch that can either block or open the way for the information coming through. This information is in the form of bits (0s and 1s) and can be used to represent more complex data by combining several bits together. Many transistors combine to form logic gates. However, traditional computer parts are now approaching the size of an atom and as a result, quantum physics is making the process of building these computer parts more tricky. Today, a typical scale for transistors is 14nm which is less than the HIV virus diameter (100nm) as well as Red Blood Cells(10,000nm). As transistors are shrinking to the size of only a few atoms, electrons may just transfer themselves to the other side of a blocked passage via a process called Quantum Tunneling [3]. This type of tunneling is based on quantum physics where the wave function of an electron has some finite probability of tunneling through an electric field which otherwise would not have been possible in terms of classical physics where the electron particle is repelled by an electric field as long as the energy of that electron is below the energy level of the field.

This problem of physical barriers to technological progress needs to be solved with the help of quantum properties by building quantum computers. Unlike normal computers which use bits as the fundamental unit of information, quantum computers use qubits which can also be set to one of two values: 0 and 1. This qubit can be any 2-level quantum system such as spin and a magnetic field or a single photon. They also exhibit the superposition property [4] where they can exist in any proportions of both states at once. While 4 normal computer bits can represent any number from 16 possible combinations, 4 qubits in superposition can be in all 16 combinations at once. And this number only grows exponentially with each extra qubit. Another property that these qubits exhibit is Entanglement [4] which is a close connection that makes each of the qubits react to a change in the other's state instantaneously, no matter how far they are apart. This means when measuring just one entangled qubit, you can directly deduce the properties of its partners without having to look. A quantum computer also contains quantum gates that manipulate the input of superpositions, rotate probabilities, and produce another superposition as its output. So a quantum computer sets up some qubits, applies quantum gates to entangle them and manipulate probabilities, and finally, measures the outcome, collapsing superpositions to an actual sequence of 0s and 1s. Therefore, by cleverly exploiting superposition and entanglement, quantum computers can be exponentially more efficient than would ever be possible on a normal computer.

Quantum Computers: For Blockchain

The advances in quantum computing have raised serious questions about whether it will be the end or the beginning of blockchain technology. Quantum computers will have the capability to either break the encryption of the blockchain or replace blockchains to emerge as the most advanced method to secure the future of the data. Some experts believe that quantum computing could destroy blockchains while others believe that quantum computing could instead be used to combine with blockchains to create an exponentially more secure blockchain that would be highly resistant to quantum computer attacks as well. Furthermore, they feel that quantum keys could replace the asymmetric key algorithms and hash functions of blockchains. The use of quantum computers for blockchains may also provide node choice randomization [5], a quantum blockchain protocol that could pick a randomly chosen verifier node using a quantum random number generator. Additionally, quantum blockchains have the potential to replace the Byzantine agreement protocol of blockchain with a quantum-Byzantine agreement protocol, which could employ quantum encryption. Although this is theoretical, it could not only help in the creation of highly- secure quantum-encryption-based cryptocurrencies but also prevent 51% attacks.

Quantum Computers: Against Blockchain

A blockchain is secured using 1) encryption via asymmetric cryptography and 2) hashing. The former mechanism depends on computers being unable to find the prime factors of the enormous numbers used as public and private keys whereas the latter mechanism depends on computers being unable to break cryptographic hashing used in blockchain. They could be exploited by quantum computers by either breaking the security of the encryption or by compromising the authenticity of entries in the blockchain. Unlike encryption, hashing cannot be reversed, and hence, encryption will be more vulnerable to quantum computers than hashing will ever be.

Quantum Computations are significantly faster than the brute-forcing approaches that are often deployed in classical computations. They can easily solve complex problems at an accelerating pace and as a result, pose a threat to blockchain technology. These algorithms are of two types: Shor's Algorithm and Grover's Algorithm.

Shor's Algorithm

In classical computers, public key cryptography techniques like RSA use a public key which is a product of two large prime numbers that have been hashed into a series of smaller letters and numbers. Cracking this encryption is not an easy feat since it becomes time-consuming to decrypt the public key, especially with its increasing value. This makes classical computations completely tamper-proof, However, Shor's Algorithm will be able to perform these combinational calculations on larger numbers in fewer arithmetic steps, thus cracking RSA in polynomial time. It does so by exponentially increasing the speed while factoring integers. It can be applied to discrete logarithmic and hidden subgroup problems as well. Furthermore, it is a probabilistic algorithm that gives the correct answer with high probability. Therefore, this algorithm could be used to reduce the number of steps to factor big numbers in order to reveal the private key associated with a given public key easily and hence, challenging the asymmetric cryptography of blockchain that depends on the difficulty of factoring large numbers. It would be possible for an attacker to forge messages or signatures and pass them on to the blockchain where they will become a part of the publicly readable and verifiable record. Furthermore, the attacker would also be able to break the cryptographic security of the communications.

Grover's Algorithm

Grover's Algorithm is an input search algorithm. This quantum algorithm compromises the hash functions of insufficient length by finding a unique input to a black box function. It is highly effective for the purpose of searching through unstructured data since it does so in quadratic runtime and this is known as amplitude amplification [6]. This procedure increases the probability amplitude of the item to be searched while decreasing the probability amplitudes of the other irrelevant items. It also improves the search by utilizing superposition and phase interference which play a pivotal role in the computations. It takes an average of $\sqrt{N}$ steps to find the desired element which is far more effective than the classical computers that take N steps (worst case scenario) to find the same element. Here, N represents the total number of elements under consideration. As a result, Grover's Algorithm achieves a quadratic speedup for finding marked items in long lists. Therefore, this algorithm could be used to attempt to break cryptographic hashing and hence, challenge the hashing of blockchain.

Grover’s Algorithm can attack the blockchain in two ways:

- It can search for hash collisions that make it viable to add a modified block into the blockchain without compromising the consistency of the blocks. Trivial data can be added to the modified block content and the given hash to make it consistent with the block content.
- It can speed up the generation of nonces, to the point that entire chains of records can be recreated. This reconstruction of the chain from a modified block occurs much faster, thus, diminishing the computational effort of extension.

Post-Quantum Cryptography

Post-Quantum Cryptography or Quantum Resistant Cryptography is an evolving field that analyzes cryptographic algorithms and how quantum computers can be used to attack these algorithms. To implement this, “The American Innovation and Competitiveness Act” law was enacted in 2017 by Congress to urge the National Institute of Standards and Technology (NIST) to formulate future cybersecurity needs and quantum-resistant cryptography standards. This organization publicly posts updates to this process and works towards developing quantum-resistant algorithms. Balti, Santini, and Cancellieri (Baldi, Santini, & Cancellieri, 2017; Clupek, Malina, & Zeman, 2015) suggested blockchains for post-quantum or improvements to existing blockchains to counter quantum danger [7]. In 2018, Chao et al. (Li, Chen, Chen, Hou, & Li, 2018) demonstrated vulnerabilities existing against a quantum computer. In the same year, Geo et al.(Y.-L. Gao et al., 2018) demonstrated the post-quantum blockchain concept and even suggested a cryptocurrency scheme based on it. This scheme could withstand quantum computing assaults. In 2018, Stewart et al. (Stewart et al., 2018) proposed a commit delay protocol in Bitcoin that allows the safe movement of money from old products to those in a quantum digital signature structure. In 2019, Campbell and Robert (Campbell Sr, 2019) assessed cyber security risks in cryptographic algorithms such as Bitcoin, Ethereum, and Heart. Overall, the main aim is to develop cryptographic counter structures that form the basis of post-quantum algorithms based on NIST.

Conclusion

The essential question now is whether quantum computers will benefit or harm blockchain. The relationship between them may not necessarily be adversarial but it still may have the potential to hack blockchains. The answer to this will be determined by whether cryptographers are able to develop security solutions fast enough to protect themselves from quantum hacking.

Engineers and developers are not any closer to developing quantum computers capable enough to hack a blockchain. Quantum computers today are still in their primitive stage and will not be a challenge to the blockchain platform for at least another two decades.

However, if quantum computers ever do come into existence, they would not only put blockchain technology in grave danger but also become a major threat to core security mechanisms powering other digital security protocols such as encryption and cryptography securing traditional online banking. Therefore, there is a need to develop quantum-proof security protocols by updating the blockchain's existing software to use one-way cryptographic functions that are hard to reverse using quantum computers. Until these post-quantum solutions are implemented, the platforms must be capable enough to adapt themselves to different cryptographic algorithms on the fly.

References:

[1]Aleksey K. Fedorov, Evgeniy O. Kiktenko and Alexander I. Lvovsky, "Quantum computers put blockchain security at risk," 2018 Nature *doi:* https://doi.org/10.1038/d41586-018-07449-*z*

[2] I. G. A. K. Gemeliarana and R. F. Sari, "Evaluation of Proof of Work (POW) Blockchains Security Network on Selfish Mining," 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), 2018, pp. 126-130, doi: 10.1109/ISRITI.2018.8864381.

[3] Neil Turok 2014 New J. Phys. 16 063006

[4] Forcer, Tim & Hey, Tony & Ross, Douglas & Smith, Peter. (2002). Superposition, Entanglement, and Quantum Computation. Quantum Information & Computation. 2. 10.26421/QIC2.2-1.

[5] C. Li, Y. Xu, J. Tang and W. Liu, "Quantum blockchain: a decentralized, encrypted and distributed database based on quantum mechanics," *Journal of Quantum Computing*, vol. 1, no.2, pp. 49–63, 2019.

[6] Amit Nikhade. (2021, June 3). Grover's search algorithm | simplified [Blog Post]. https://towardsdatascience.com/grovers-search-algorithm-simplified-4d4266bae29e

[7] Khalid, Zhwan & Askar, Shavan. (2021). Resistant Blockchain Cryptography to Quantum Computing Attacks. 5. 116-125. 10.5281/zenodo.4497732.