A new Security model for blockchain Using Quantum Computing

Sujith Kumar R
PG Scholar of Amal Jyothi College of Engineering,
Kanjirappally, Kerala
Sujithkumar.sk175@gmail.com

Sona Maria Sebastian
Asst. Professor of Amal Jyothi College of Engineering,
Kanjirappally, Kerala
sonasebastian@amaljyothi.ac.in

Abstract: **Quantum computing is the solution to many complex problems that technology facing today, like a replica of quantum computing systems and large number factorization. The concept of the quantum computing mechanism is pretty well accepted. Quantum computing is both boon and bane to our current blockchain technology which is fully established on encryption mechanism and hashing functions. Digital signatures in a blockchain may allow an attacker to fetch the identical key. Determining hash may be easy. So, ongoing blockchains also need their own resettling. We can achieve this by developing a new protocol or creating a post-quantum mechanism. Creating a quantum-based blockchain is a solution to this. Generating quantum-based replica of each block and maintaining that block in a superposition that can't be altered with normal computers. To alter a quantum-based block with the same quantum computing technology is also impossible or it takes more than 2000 years because to achieve this we need more than 50 qubit quantum computers, which is not created yet. The IBM-created quantum computer comes with only 27 qubit falcon processor.**

Keywords – Quantum Computing, blockchain, Superposition, Qubit, Quantum Entanglement.

I. INTRODUCTION

A Blockchain is a chain of blocks that hold a record of transactions. Every block is connected to each other. The blockchain is very difficult to meddle with only a single block because an attacker needs to change the block containing that ledger as well as those connected to it. This alone might not seem like much of a discouragement. Blockchain has some other distinctions that give extra security features. The record inside a blockchain is secured with the help of cryptography. Users have their own private keys that are allocated to the transactions they make and behave as distinctive digital signatures. If a transaction record in blockchain is altered, the digital signature will become baseless and the peer can detect that some alteration happened. Blockchains are decentralized across peer-to-peer networks, it doesn't have any chance of failure or it can't be changed with a single computing device. To make this possible we need an enormous amount of computing ability to approach every instance. As mentioned blockchains are immutable, but there are some challenges to blockchain security in the future, including 51 percent attack and quantum computing. Quantum computing can be used to make blockchain more secure and also it can be used as a threat. Quantum computing has the potential to reverse engineer the blockchain's public key, which can be used to find the private keys and break the system.

II. BlockChain

All chains in the blockchain has multiple blocks and every block has basically three elements.

- Data inside the block (transactions).
- A 32-bit number called the nonce. This whole number is randomly generated at the time of the creation of the block, this helps to create a block header hash.
- The header hash is a 256-bit number conjugal to the nonce, starting with a large number of zeros.

At the time of the initialization of the block, the nonce generates the hash. Transactions or the data inside the block is considered signed and always bond to the nonce and hash except it is mined. The miners are the users who fabricate new blocks to the chain through a process called mining. Every block has its own distinctive hash, but also has an instance of the previous block in the chain, so the process of mining is difficult, for larger chains.

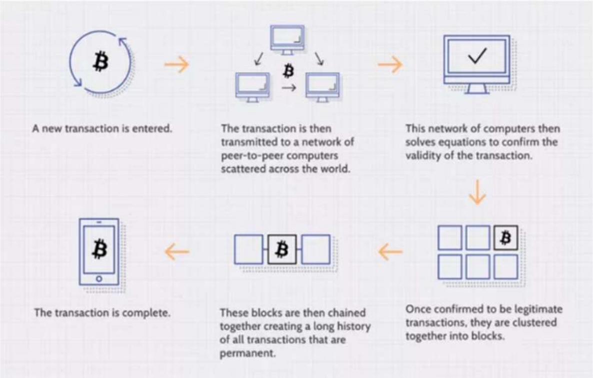
DOI: 10.5281/zenodo.6369652
ISBN: 978-93-5607-317-3@2022 MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam

An untimely change to any block requires re-mining not only the changed block but all of the blocks that come after. This is why it is exceedingly very difficult to exploit blockchain technology. After successful mining of a block, the difference is authorized by all the nodes on the network and also the miner is awarded financially.

Nodes are an important part of the blockchain and its decentralized behaviour. Nobody can own the chain rather, it is a distributed ledger via the nodes are linked to the chain. Nodes can be any kind of electronic device that keeps copies of each block and also makes the network functioning.

All the actions in the ledger can be checked and visible to everyone. Each node has its own copy and the network will approve newly mined block using special algorithms for the chain to be trusted and verified. Each miner has an identical alphanumeric ID that shows their transactions.

There are mainly two different types of blockchains, private and public. They differ in a couple of ways that can affect the level of security they contribute. The main difference is that public blockchains are always connected to public networks to certify transactions and assort them into blocks, which helps them to add new ledger. In a public blockchain, any computer connected to the public internet can join the party. On the other hand, private blockchains are different, they generally permit only known organizations and they form a private, users-only network. They are for business organizations.



A new transaction is entered.

The transaction is then transmitted to a network of peer-to-peer computers scattered across the world.

This network of computers then solves equations to confirm the validity of the transaction.

Once confirmed to be legitimate transactions, they are clustered together into blocks.

These blocks are then chained together creating a long history of all transactions that are permanent.

The transaction is complete.

Fig. 1 . Block chain basic working

III. Quantum Computing

Quantum computing is a technology of computing, entrenched in developing computer technology based on the principles of quantum theory that describes the conduct of energy and material on the subatomic level. Today's computer systems can only process with 0's and 1's, which limits their capacity. Quantum bits are used in quantum computers, also known as qubits. Which has the potentiality of subatomic particles that makes them endure in more than one state (between 1's and 0's).

A quantum bit or qubit is the quantum mechanical cognate of our classical bit. In our digital systems or computing, the data is encoded in the form of bits or like switch on or switch off the current in circuit board representing 0's and 1's. It is entirely different in quantum computing. In quantum computing, the data is encoded in qubits. A qubit can be in 0's or 1's or in a linear combination of both states. Before we measure a qubit, exists in a state called this superposition. Each qubit has some amplitude for being 0 and some amplitude for being 1. This is the reason that quantum computers can store and maintain a vast amount of data.

Orthogonal state x-basis

$|+\rangle = 2|0\rangle + |1\rangle \ / \ \sqrt{2}\ |-\rangle = |0\rangle - |1\rangle \ / \sqrt{2}$

Orthogonal y-basis state

$|R\rangle = |0\rangle + \imath|1\rangle \ / \sqrt{2}\ |L\rangle = |0\rangle - \imath|1\rangle \ / \sqrt{2}$

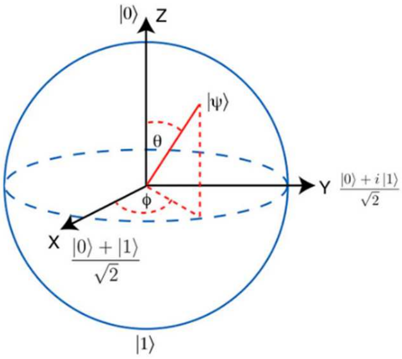

$|0\rangle$
Z
$|\psi\rangle$
θ
ϕ
Y
$\frac{|0\rangle + i|1\rangle}{\sqrt{2}}$
X
$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$
$|1\rangle$

Fig. 2 . A single qubit (*Bloch Sphere*).

a. *Amplitudes*

The main part of quantum physics is a concept called amplitudes. Here's what the classical rules of probability tells us about getting tails, if we toss 20, coin, we add up the probabilities for all the possible outcomes resulting in tails. Before we measure a subatomic particle, we can think about it as a wave of probability that exits in a kind of black box, a quantum system with many different chances of being in many different places. Quantum mechanics, as its code, is a chance to the rules of probability. These amplitudes are closely related to probability but they are not probabilities.

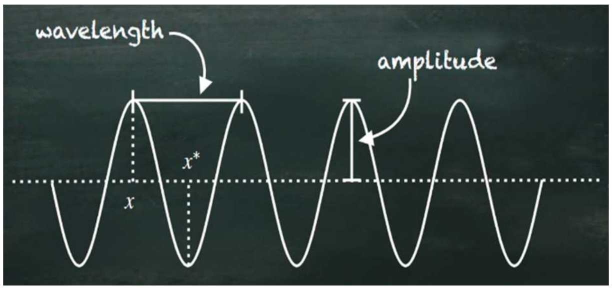


Fig. 2.1 positive and negative amplitude

A key difference is probability is always a number from zero to one. Amplitudes are complex numbers and what it means is that they obey different rules. So if we want to know the total amplitude for something to happen, we have to add up the amplitudes for all the different ways that it could have happened, we have to add up the amplitudes for all the different ways that it could have happened. But when we add up amplitudes, it seems different than a particle might reach a certain place one way with a positive amplitude and another way with a negative amplitude. If that happened, then those two amplitudes can cancel each other out so that the total amplitude would be zero, which would mean that the thing would never happen at all. This is the way that a physical system changes over time are by a linear transformation of these amplitudes.

b. *Quantum entanglement*

When two or more qubits are in a closed state of superposition, they relate to one another through the phenomenon called entanglement. This means that the final outcomes when we measure them, are mathematically related to each other. The key concept for understanding quantum computing is to understand quantum entanglement, this is used to correlate parts of a quantum system, which are entirely different from the correlations that we normally encounter in the classical world. Imagine that we have a 10 qubit computer it can store 2^10 values in parallel, which is 1024 values. To store this information in a classical computer we need 16 thousand bits. Any information, if it is 0's or 1's it is recorded in some radiation that's escaping from the quantum computer.

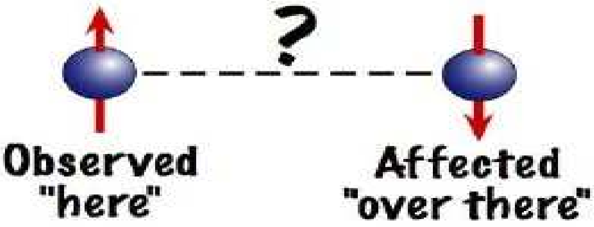


Fig. 2.2 Quantum Entanglement.

c. *Quantum Interference*

When waves in a pool hit each other, and one wave is above the surface and the other wave is below the surface, they hit each other and cancel each other. Interference is just what amplitudes do when we add them up. If something happens one way with an amplitude of a half and another way with an amplitude of minus a half, then the total amplitude for it to happen would be zero.

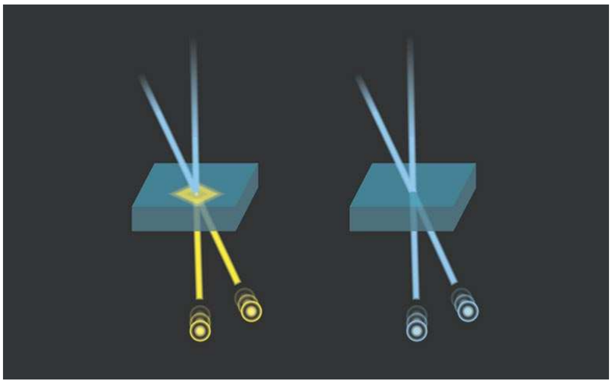


Fig. 2.3 Quantum Interference (*based on double slit experiment*).

d. *Quantum algorithm*

We can harness interference by creating a deterministic sequence of qubit gates. These gates cause the amplitudes to add up effectively. This means that they are mathematically guaranteed to boost the probability of seeing one of the right answers. This is a quantum algorithm. There is a question that, how could we possibly concentrate all this on the right answer when we don't know the answer in advance, which answer is the right one?. This is why designing a quantum algorithm is so difficult. scientists have been studying it for decades. Since 1994, there have been major findings in quantum algorithms, with theoretical applications in fields such as cyber security and search optimization.

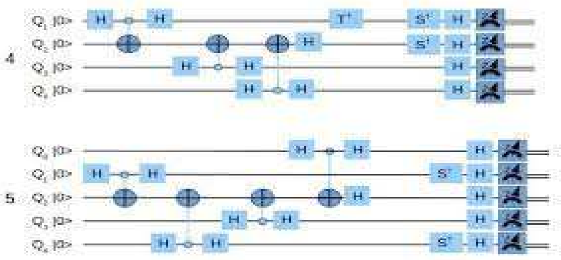


Fig. 2.4 Quantum algorithm.

IV. LITERATURE REVIEW

Haryono Soeparno et al [1] This cloud technology is a quantum computer that can be pervaded in a cloud environment using a network. Today, there are different quantum cloud computing services that are available to users. They are used to find solutions for complex problems that require more computing. Different quantum cloud computing services have different structures. In this research, he conducted this study on some services to evaluate the performances of different cloud quantum computing services and make connections out of them.

Sana Akbar et al [2] With the identification of large domains to social networks hike in the data created, and saved universally; the task of handling the uncertain, dynamic, and evolving nature of social networks has become backbreaking. In this regard, quantum computing (QC) has appeared as the most talented settler guaranteeing amazing storage capabilities by dynamic allocation of cluster size, quantum parallelism, reduced parameter dependency, etc.

Akshay Ajagekar et al [3] Quantum computing and machine learning techniques have got large acceptance in these years. QC-based machine learning methods for defect diagnosis that deed their singular potentiality to overcome the computational challenges faced by current data-based approaches carry out on classical computers. Deep acceptance networks are integrated into the proposed defect analysis model and are used to extract characteristics at different levels for normal processes.

Avinash Chalumuri et al [4] Training an ML model is an important task due to the size of a large amount of data. Also, a large number of domains are to be used in the network to find the patterns and analyze such data. QC is impending as an area that has a solution to this problem. A QC can mean data differently using qubits. Qubits in quantum computers are used to search the concealed patterns in data that are difficult for a classical computing system to find. Hence, there is a large area for application in artificial networks.

Payal Prajapati et al [5] Cryptography is very crucial in securing transactions, however, the digital signature process may be known to the attacker. Hence, the key can be compensated as a crucial part of any algorithm. With the symmetric key, researchers have developed concepts where the output of one process becomes an input to the next. Such a concept of modes of Cipher Chaining is unified into this article to generate multiple key blocks. The keys can be given to the unique block of plaintext for any encryption technique as per the demand.

V. PROBLEM DEFINITION

Quantum computing is a big challenge for all blockchain-based technologies like cryptocurrency. IBM has affirmed that quantum computing can reverse engineer the public key of blockchain network this helps to discover private keys to crash the network. This is an actual and valid threat. Which can be competent more than fifty percent of blockchain.

Solving this problem using three different techniques, they are:

- Developing a power full protocol and also using the concord algorithm.
- Incorporation of quantum cryptography into the core of blockchain.
- Creating a replication of newly created blocks and maintaining that replicated model in superposition using quantum technology, which makes it tamper-proof.

VI. IMPLEMENTATION

If data tampering happens in a blockchain the suspected block will check the next adjacent block and correct itself. If an attacker uses a quantum computer to modify data on a block, he can alter the entire or 50% of the blockchain without detection. To avoid this, we can replicate each block at the time of its creation and use a quantum computing mechanism to maintain this replicated block in a super-positioned state. When a data modification happens, the suspected block corrects itself or the corrections can be done with the help of miners.

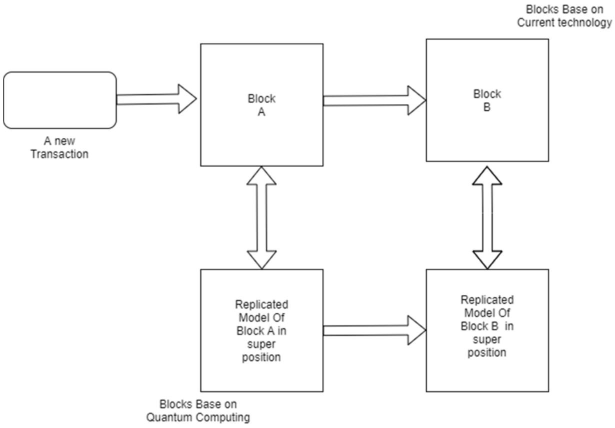


Fig. 3 Method of implementation.

VII. Grovers Algorithm

The grovers algorithm solves one of the multiplex plot in the field of quantum computing. This is also a solution for searching through unstructured data. This is also an important algorithm suggested for quantum computing. Consider a situation that we have a list of unsorted numbers N as shown in the diagram, we want to find value within the red box.

4	6	8			W			N=2^N

Fig. 4 list of n numbers.

We know the classical method for searching a value from a list. We need to check an average N/2 of these items in the list. We will require n steps that are O(N). if the list is pre-sorted, it needs a log(N). steps. However, using a quantum algorithm will take only √ N steps that is O(√ N) for finding the key value. For example, if we make a list of twenty-five elements, it will take only √25 which is 5 steps.

As above mentioned it uses superposition and interference to improve the required search. It's the amplitude amplification that plays this searching mechanism.

The amplitude amplification is a mechanism that increases the probability of the search value and reduces the probability amplitudes.

For example, there are k1, k2, k3….kn elements in a stabilized superposition, we need to find kw by using amplitude amplification when the elements are sent to the process, at the first time it flips the kw elements upside down to the negative phase from the probability which is the opposite of the previous state. It helps to disparate it from other elements.

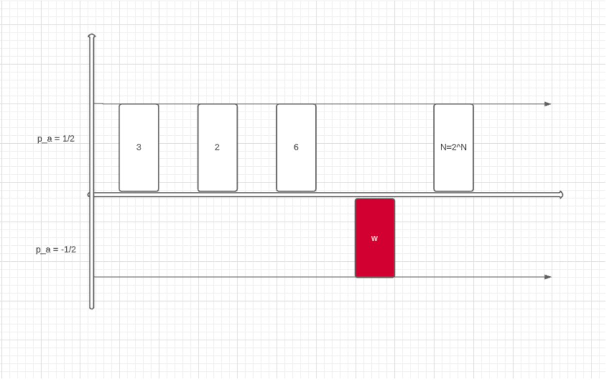


Fig. 4.1 negative phase of elements

At the next phase, it inverts all the amplitudes by finding its average. This results in the reduction of the amplitude and increases the elements Kw's ket such that the kw becomes 1 and the state of the rest will become 0's.

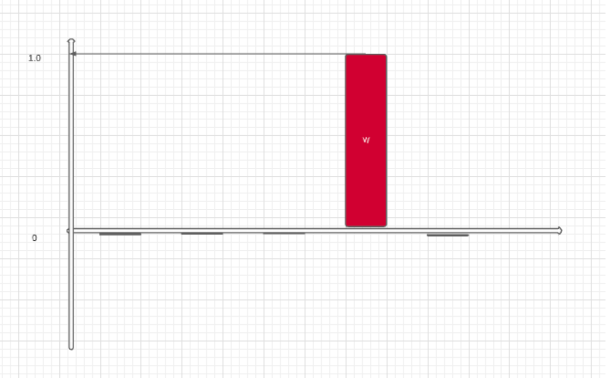


Fig 4.2 finding the ket

VIII. CONCLUSION

Quantum computers has the possibilities to transform computation by creating fixed types of classically intractable problem solvable. One of the most identical feature of blockchain is its immutable property, date hashes in a blockchain are habitual there forever. The signatures in a blockchain will help the attackers to retrieve the related private key. Hash calculations may be simplified. So today's blockchain needs its own resettling. Blockchain implementation to the post-quantum generation will require increased computing resources. Quantum computing technologies can be used to increase the security level of blockchains. This can be achieved in more than different ways.

IX. REFERENCES

[1] SanaAkbar and KhetwatSaritha, quantum computing based community detection, https://doi.org/10.1016/j.cosrev.2020.100313, on November 2020.

[2] Akshay Ajagekar, Quantum computing deep learning for fault detection in industrial process systems, India, on December 2020.

[3] AvinashChalumuri and RaghavendraKune, Modeling an Artificial Neural Network Using Qubits as Artificial Neurons: A QC Approach, July 2020.

[4] IEEE , Quantum computer structure, New Delhi, India,, 04 May 2015

[5] IEEE, Realizing QC Algorithms on Quantum Computing Devices, 10.23919/DATE48585.2020.9116240,Grenoble, France 15 June 2020

[6] Juri Mattila, Mika Pajarinen, and Timo Seppälä, Quantum computing is here – will cybersecurity be in threat? https://www.researchgate.net/publication/342437849_Digibarometer_2020_Quantum_computing_is_coming_-_will_cybersecurity_be_compromised, June 2020.

[7] Pradosh K. Roy , Quantum Computing, https://www.researchgate.net/publication/342439420_Fundamentals_Of_Quantum_Computing_Part_I_O_N_E_D_AY_I_N_T_E_R_N_A_T_I_O_N_A_L_W_E_B_I_N_A_R_O_N_Q_U_A_N_T_U_M_D_A_TA_A_N_D_A_L_G_O_R_I_T_H_M_S_2_8_J_u_n_e_2_0_2_0, 28 June , 2020.

[8] Xingtong Chen & Gang Kou , A systematic study of blockchain, 04 July 2019.

[9] Francis Asuncion, Adam Brickman, Dwanyne Cole, Connecting supplier and DoD blockchains for transparent part tracking,