Preprints.org

Article

Not peer-reviewed version

QUMA: Quantum Unified Medical Architecture using Blockchain

Akoramurthy B * and Surendiran Balasubramanian

Posted Date: 8 February 2024

doi: 10.20944/preprints202402.0529.v1

Keywords: Health Informatics; Blockchain; Quantum Hash; Electronic Medical Record; M-IoT

Preprints.org is a free multidiscipline platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2024 doi:10.20944/preprints202402.0529.v1

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

Article

QUMA: Quantum Unified Medical Architecture using Blockchain

Akoramurthy Balasubramaniam * and B. Surendiran

National Institute of Technology, Puducherry, Karaikal,609609, India; surendiran@gmail.com
* Correspondence: akor.theanchor@gmail.com, cs22d1005@nitpy.ac.in

Abstract: A substantial spike in the need for quality healthcare has resulted from people being more cognizant of health issues. With blockchain, healthcare providers may safely share patient information electronically, which is especially important given the sensitive nature of the data contained inside them. However, flaws in the current blockchain design have surfaced since the dawn of quantum computing systems. The study proposes a novel quantum inspired blockchain system (Qchain) and constructs a unique entangled quantum medical record (EQMR)system with an emphasis on privacy and security. This Qchain relies on entangled states to connect its blocks. Automated production of the chronology indicator reduces storage capacity requirements by connecting entangled BloQ (blocks with quantum properties) with controlled activities. One qubit is used to store the hash value of each block. A lot of information regarding quantum internet is included in the protocol for the entangled quantum medical record (EQMR). EQMR can be accessed in Medical Internet of Things (M-IoT) systems may be kept private and secure, and their whereabouts can be monitored in the event of an emergency. The protocol also uses quantum authentication in place of more conventional methods like encryption and digital signatures. Mathematical research shows that the quantum converged blockchain (QCB) is highly safe against attacks such as the External attack, Intercept-Measure-Repeat attack, and Entanglement-Measure attack. The reliability and auditability evaluations of the entangled BloQ, as well as the quantum circuit design for computing the hash value, are presented. There's also a comparison between the suggested approach and several other quantum blockchain designs.

Keywords: health informatics; blockchain; quantum hash; electronic medical record; M-IoT

1. Introduction

Thanks to Satoshi Nakamoto who introduced the world to the concept of Bitcoin in 2008 [1], and with it came a novel method of conducting financial transactions. Bitcoin was the first fully decentralized electronic cash method that can be relied upon. Because of the brilliant blockchain system that underlies it, Bitcoin is secure even without any kind of centralized administration. The distributed ledger technology known as blockchain records transactions in an immutable ledger of ever-expanding blocks. In multi-party environments, it may provide a novel cooperative trust paradigm[2]. There has been an increase in the number of use cases for blockchain in the IoT related to public health [3]. In order to intelligently identify, track the location of, monitor, and operate a wide range of things, including humans, the Internet of Things [4] enables their connection and collaboration over the Internet. The Internet of Medical Things (IoMT) [5] connects sensor devices such as health gadgets, integrated healthcare equipment's, fixed medical apparatus, and networks that track patients' vitals and to access varied patient medical records to provide valuable data for later treatment. Sensing, networking, and actions all make up the M-IoT's three-tiered architecture. Figure 1 depicts a light weight version of the IoMT network model.

© 2024 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2024 doi:10.20944/preprints202402.0529.v1

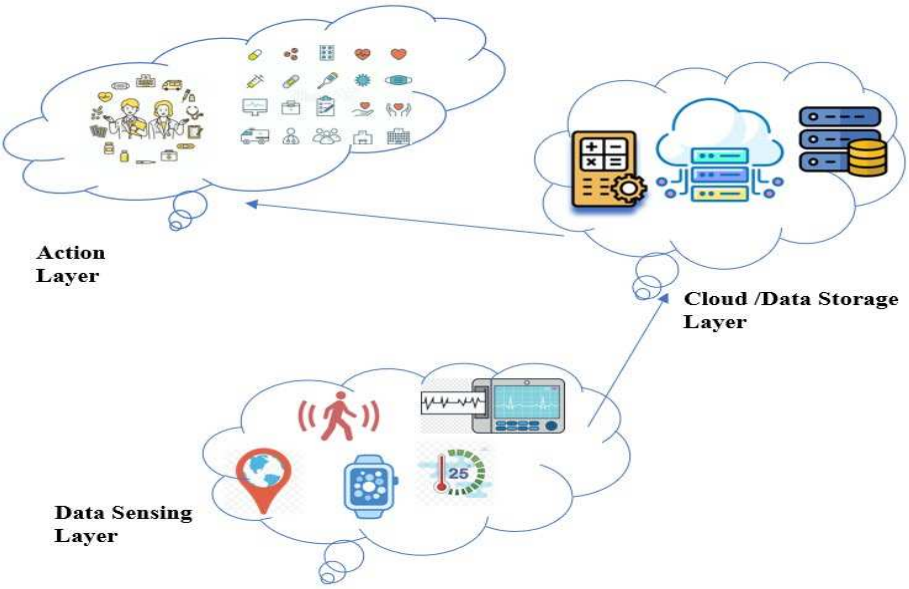


Figure 1. Conceptualization of M-IoT systems as a layer.

Multiple sorts of decentralized healthcare facilities generate massive amounts of health records every day. When patients need to relocate to medical institutions, they sometimes have to undergo additional testing, making the exchange of electronic medical information between such hospitals essential. Electronic medical records (EMRs) are incredibly confidential due to their diagnostic and therapeutic implications [6]. Since information leakage happens throughout the flow of information among EMRs [7], keeping EMRs private and secure is a major concern. These difficulties with huge data can be overcome, according to the literature review [8], thanks to the special characteristics such as distributed storing and immutableness. The following advantages are gained by combining blockchain with big data: Blockchain's decentralized storage is well suited for data exchange between different medical organizations, and its one-of-a-kind data encoding techniques, which leads to the difficulty for accessing by unauthorized user. EMRs saved on the blockchain network are protected and trustworthy because of blockchain's immutable data format, which prevents unauthorized changes to the records. Third, avoiding fraud: current big data can't help with spotting phony communications. Blockchain technology allows hospitals and clinics to instantly check the legitimacy of electronic medical records that may have been tampered with. In the here and now, health care organizations can use data from multiple sources to provide comprehensive and methodical diagnoses with the use of analytics that monitor data in real time. Integrating blockchain technology with IoMT systems (BIoMT) can guarantee anonymity, security, and authenticity of every electronic medical record. Electronic medical records (EMRs) are transferable across hospitals and clinics, and their history may be retrieved at any time to check for tampering [9]. Digital signatures and elliptic curve cryptography [10] are two examples of the traditional cryptographic techniques on which blockchain technology depends; both have their own security flaws [11]. Current blockchain systems are susceptible to assaults from quantum computing devices [14], which have been developed alongside quantum information processing [13] and quantum machines [12]. Shor and Grover algorithm [15] have such high computational requirements that malevolent medical organizations will monopolize block generation. By all above means, it is obvious that blockchain is in quantum danger [16], and so necessary to migrate to a quantum mechanics properties exploiting blockchain and entangled quantum health records (EQHR) by using the new security features of quantum cryptography [17].

In order to protect blockchain networks against quantum computer attacks, this research proposes a new physics inspired blockchain network. An overview of the features and contributions is provided below.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2024

doi:10.20944/preprints202402.0529.v1

1. A whole new network of Quantum Mechanics-based Chain for Highly Advanced Medical Information Networking (QMEDCHAIN) is developed. Entangled states are used to link the quantum blockchain nodes together. Hash values for individual blocks are stored in a single qubit, and time stamps are created automatically during the regulated actions required to combine quantum blocks.

2. An innovative protocol for entangled quantum medical records (EQMR) is proposed, and the data flow and processing in the network is explained in detail. This protocol implements a quantum authentication technique. New EQMR protocol feasibility is explained by linked simulations, and its security aspects are fully realizable, also the mechanism of information processing in the network is elucidated via an example.

3.This study provides an in-depth evaluation of security measures. Security research, derived from theory, shows that the EQMR protocol is secure against three common types of attacks: external attacks, measurement replay attacks, and entanglement attacks. Correctness and traceability analyses of the BloQ, are well presented. The suggested QMEDCHAIN is also compared to many current blockchain models, in particular quantum blockchain systems, in this study.

The following is the outline for this paper. The theoretical underpinnings of quantum mechanics postulates, as well as the quantum hash generation, quantum embeddings are described in Section 2. The data format of the proposed system and the EQMR protocol are described in Section 3. The protocol's viability is demonstrated by concrete examples and experimental simulations. The robustness, safety, and verifiability of BloQ in detail are dissected in Section 4 along with the theoretical underpinnings. In addition, parallels are drawn to various versions of blockchain technology now in use. The paper comes to a close in Section 5.

2. Prelude

This section will go through some of the core principles pertinent to this study, such as recent related papers, the theoretical underpinning of quantum mechanics. The quantum hash generation and embeddings has been described in the section 4.2 and 4.3 respectively.

2.1. Postulates of Quantum Mechanics, and its Application to Qubits

Quantum physics is built on an entirely new mathematical context. Following that, we will introduce the postulates that form the underpinning of quantum theory. These postulates serve as a bridge between the physical world and quantum mechanics' mathematical formalism. Generally, it is not necessary to learn the theories of quantum electrodynamics and field theory, to understand quantum information.

Pos1: The Current Quantum State: A Description

A quantum system in comparison with any isolated system will be called a Hilbert space or state space of the QSystem, which exhibits a complex vector space along with an inner product. Here, the unit vector is used to define the state of the QSystem in its state space itself.

Pos2: Describing the Operators of the Quantum System

There exists an operator for each physical quantity that may be seen conventionally. This operator should exhibit Hermitian and linear behavior, as anticipated.

Pos3: Describing the Measurement of the Quantum System

For any measurement $\boldsymbol{\widehat{M}}$ of the Hermitian operator, the only value will be seen as eigen values, which is represented as

$$\boldsymbol{\widehat{M}\phi} = \mathrm{e}\boldsymbol{\phi} \tag{1}$$

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2024 doi:10.20944/preprints202402.0529.v1

Pos4: Describing the Probability Estimates and Wave Function Failure

In the case where a system is being defined by a normalized wave function $\boldsymbol{\varphi}$, the average value of the observed values associated with $\widehat{\boldsymbol{M}}$ can be found via:

$$|\boldsymbol{M}\rangle = \int_{-\infty}^{\infty} \boldsymbol{\varphi}^{*} \widehat{\boldsymbol{M}}\ \boldsymbol{\varphi}\ \mathbf{d\tau} \tag{2}$$

Pos5: Describing the Changing Face of Time

The formula proposed by Schrödinger, which relies on the clock, describes the evolution of a system's wave function:

$$\widehat{\boldsymbol{H}}\boldsymbol{\varphi}(\boldsymbol{t},\boldsymbol{r}) = \frac{\partial\varphi}{\partial t}\ \mathrm{i}^{*}\hbar \tag{3}$$

Pos6: Describing the antisymmetric principle

Regarding the reversal of all fermion locations, the whole wavefunction has to be antisymmetric. Incorporating electronic spin into these positions is essential.

2.2. Concerns About Blockchain's Security in Light of Forthcoming Quantum Computing

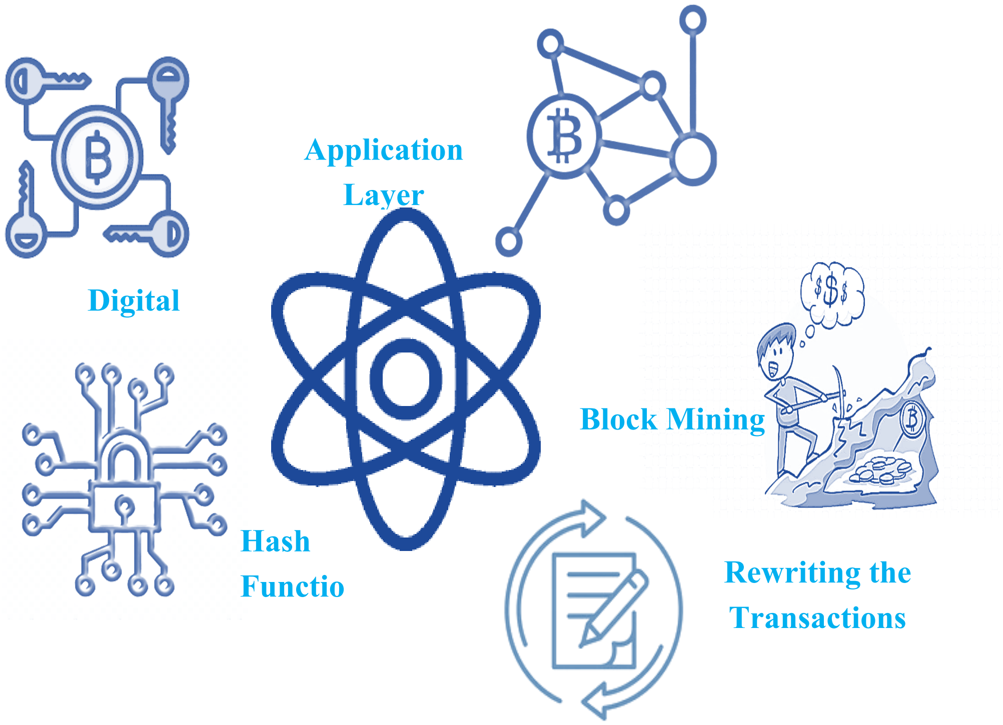


Figure 2. Quantum Threats to Blockchain.

There will be possibilities and threats to digital technology in the new paradigm that quantum computing ushers in. When powerful quantum computers crack a number of crucial encryption techniques in use today, there will be a plethora of new threats. Since blockchain is primarily a cryptographic system, it is vulnerable to these kinds of attacks. The above five threats have been identified as when blockchain technology and quantum computing meet, according to research [18–20]:

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2024 doi:10.20944/preprints202402.0529.v1

3. Associated Works

Ever since the Internal Report 8105[21] from NIST in 2016, the fact that contemporary encryption is vulnerable to quantum attacks has been widely recognized. As the blockchain system is based on the classical cryptographic algorithms, the quantum computations have become the scourge to the blockchain system. Considering the famous blockchain system Ethereum has introduced an account abstraction (ERC-4337) [22] for their users account to be quantum resistant. Having the advantage of plug and play or modular architecture concept in Hyperledger fabric, will be able to replace the quantum resistant system in place according to the situation need. Among blockchain experts, this is the consensus view. Many are aware of the impending arrival of quantum computers, but no pressing need to act on this information just yet. Additionally, the consequences of quantum computers' attacking capabilities on blockchain platforms are not yet completely understood. Few of the most prominent blockchain technology summits in the world even touch on the subject. Although the study is more fascinating from an academic point of view than an empirical perspective, it is nevertheless worth discussing.

Consistent with our presentation in "Concerns about blockchain's security in light of forthcoming quantum computing," the literatures [23–25] has appropriately addressed the big picture of the threat that quantum computers pose to blockchain technology. In order to decipher blockchain network encryption, several researchers have been building models to estimate how many qubits would be required. Based on the literature [26] If the surface code, code cycle time, response time, and physical gate error were to be used to crack the encryption in one hour, it would need 317 × 106 physical qubits. On the other hand, thirteen million physical qubits would be needed to decrypt the encryption in a single day. Though many researchers claim different qubits to decrypt, the exact number of physical qubits required for this function remains unknown. In August 2023, Ed Gerck a researcher claimed that RSA -2048 key has been broken, which stirred the entire research community. There is some prior research that suggests ways to protect blockchain networks and protocols against quantum computer assaults. There are two main schools of thought when it comes to blockchain technology proposals: quantum blockchain (QUAB) and post-quantum (PQB). Using quantum phenomena, such as quantum key distribution (QKD) to secure interaction among nodes and entangled property to enable no-tampering of transactions and avoid double spending, quantum blockchain (QUAB) networks are able to withstand quantum attacks [27–30]. Scientists created a blockchain system that is both permissive and secure against quantum attacks [31] to combat the threat that quantum computing brings to blockchain technology. The developed one uses a voting-based consensus algorithm and a digital signature mechanism based on QKD to obtain consensus on the blockchain. Due to the vulnerability of digital signatures to quantum computer assaults, the paper [32] used Quantum Key Distribution (QKD) networks the same year to enable safe authentication on blockchain networks. Also, they employed an information-theoretic broadcast system in which everyone on the network agreed on fresh blocks on equal conditions, as opposed to leaving the creation of new blocks up to a single miner. In 2018, the necessary hash and nonce were obtained by using the quantum Grover search method [33]. In 2021, [34] suggested a protocol for building a blockchain infrastructure that would allow for safe data transfer between Internet of Things devices, which would use quantum walk technology for identification and encoding. Coupling quantum infant with a conventional blockchain that can process stateful smart contracts, [35] constructed a simple hybrid classical-quantum payment system. In order to circumvent the issue of quantum banknotes' lack of trustworthiness, they utilized blockchain technology to create a public-key quantum money system that utilized quantum states as currency. Actually, the paper doesn't give an explanation of the structure of quantum blockchain; it just builds a quantum money system using conventional blockchain. Based on their theoretical framework, [36] conducted a qualitative study of American EHR users in 2020 and investigated the potential commercial and academic applications of blockchain technology for EHR, security, and storage. An innovative blockchain-based credibility score-based approach (CSA) was proposed in the study article [37]to guarantee the integrity and confidentiality of electronic health records. There are still major practical concerns with quantum blockchain and electronic health records, despite numerous academic achievements in both areas.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2024 doi:10.20944/preprints202402.0529.v1

Traditional blockchain-based EHRs are susceptible to quantum computing assaults, which makes security maintenance a challenge. While studies on quantum blockchain's exact data structure and information processing are still in their infancy, what little there is shows promise. Another group offers a fascinating method for hash chain-based digital signatures. Whilst these post-quantum blockchain projects show great promise, they do not yet offer comprehensive solutions for blockchain networks that are resilient to quantum technologies; at present, these outlines are limited to safeguarding digital signatures and assets. Furthermore, every single proposal does not aim to improve upon any preexisting blockchain network; the only exception to this is the Matri CT protocol, which is relevant to the Monero coin. Hence, safeguarding the present assets held in existing blockchain networks, totaling thousands of millions of dollars, does not directly follow from this.

4. QUMEDCHAIN - Quantum Mechanics-based Chain for Highly Advanced Medical Information Networking

This part provides an overview of the suggested quantum mechanics based blockchain (QMEDCHAIN), explains how the entangled quantum health record (EQHR)protocol works, and provides an illustrative case supported by relevant simulations. The layer-based approach has been followed and the complete description included in as the supplementary data in Appendix A.

4.1. The Data Structure of Classical Blockchain Vs Quantum Blockchain

Table 1 demonstrates that data structures of quantum blocks include both a header and a body in comparison with classical blockchain. The header of a block contains data necessary for mining. The current block's body contains a directory of hospital records it contains. As we are engaging in medical records information, which is very sensitive, and if the qubits get into the superposition, we may tend to lose the information. The Qblocks (quantum register) created will be connected together with the help of the Z gate operating on a single qubit since it is a unitary gate.

Table 1. QMEDCHAIN Vs Classical Blockchain Data Structures.

Blockchain		**QMEDCHAIN**	
Block Header	Block Body	Quantum Header	Quantum Body
Version	List of Medical Records	MQubits	QMedical Records
Hash and timestamp			
Merkle root		Qhash	
Difficulty target			
Nonce		Quantum State	

More specifically, it changes the value of 1 to -1 while leaving 0 unmodified. This is accomplished via a 180-degree (radians) rotation about the qubit's Z axis. The qubit's phase is changed as a result. The preceding array describes the functioning of Z-gates: In the case of qubits, two braket vectors stand in for the computational base of 0 and 1.

$$|1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \qquad |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \tag{4}$$

$$Z = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix} \tag{5}$$

In the above matrix, the computational base of 1 has been flipped to -1, which shows that when the qubit is $|0\rangle$, no action will be done. Once the qubit is measured, it won’t change the state and avoids the superposition state.

4.1.1. Measurement

Here, we use a Hermitian operator H on the measurement quantum block. 'a' is the amplitude of the eigenvector, and the likelihood of the register collapsing into one of its eigenvectors in operator is proportional to $|a|2$. If that were the case, the probability of $|y|2$ and $|x|2$ would cause our qubit $|qb1\rangle = y|0\rangle + x|1\rangle$ to collapse to $|0\rangle$ and $|1\rangle$, respectively as illustrated in figure 3. It is standard practice in quantum computing to use the aforementioned matrix while measuring. In the computational basis, this reduces our qubits to a binary value of $|0\rangle$ or $|1\rangle$. What this clearly shows us is that our qubit's behavior is further complicated:

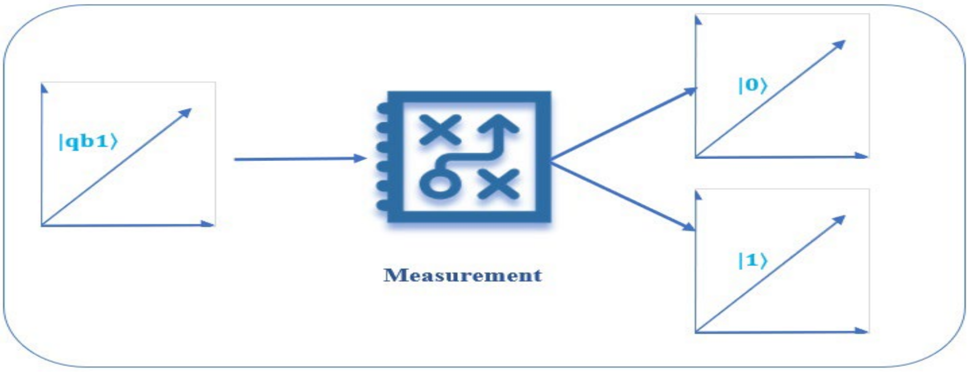


Figure 3. Collapse of $|qb1\rangle$ into $|0\rangle$ and $|1\rangle$.

To begin, our qubit vector's magnitude must always be calibrated to 1 as the likelihood of getting a measurement is 1. Also, when we measure, our qubit's superposition is broken, and the data held in its amplitudes is lost. The fact that we can only receive a yes/no response in spite of all the details stored in these qubit states is a disappointing limitation of quantum computer science.

4.2. Quantum Hash Generation

The development of a QHF via refinements to the 1-D discrete-time Quantum Walk on a sphere for two particles. The Quantum Walk of two walkers whose paths are constrained to the circle is described by a 1-D 2-particle discrete-time Quantum Walk on a circle. Then the operators $\widehat{\boldsymbol{x_1}}$and $\widehat{\boldsymbol{x_2}}$ becomes

$$\widehat{x_1} = \begin{cases} |2,0\rangle\langle 1,1| \; + |\mathrm{m},1\rangle\langle 1,0|, \text{when a } = 1 \\ |1,0\rangle\langle \mathrm{m},0| \; + |\mathrm{m}-1,1\rangle\langle \mathrm{m},1|, \text{when a } = \mathrm{m} \\ |a+1,0\rangle\langle \mathrm{a},0| \; + |\mathrm{a}-1,1\rangle\langle \mathrm{a},1|, \text{when a } \neq 1, \mathrm{m} \end{cases} \tag{6}$$

In this case, $\widehat{x_2}$ is analogous to $\widehat{x_1}$. For the full conditional shift operator $\hat{x}$, we have $\widehat{x_1} \otimes \widehat{x_2}$. For each step of the walk, if the last 4-bits of the message that is sent is 10(11), then the interaction will be $W_0W_1(W_2W_3)$.

For instance, if the input is ‘011111011’, then the last state of the walk is represented as

$$|\psi\rangle_9 = \hat{A}_0 \, \hat{A}_1 \, \hat{A}_2 \, \hat{A}_3 \, \hat{A}_4 \, \hat{A}_5 \, \hat{A}_6 \;\; \hat{A}_7 \, \hat{A}_8 \, \hat{A}_9 \, |\psi\rangle_0 \tag{7}$$

where $\hat{A}_0 = \hat{x} \; (\hat{I} \; \otimes \widehat{W}_0)$, $\hat{A}_1 = \hat{x} \; (\hat{I} \; \otimes \widehat{W}_1)$ and so on. Then the initial condition of the entire quantum system $|\psi\rangle$ is described by

$$|\psi\rangle_0 = |a, b\rangle \otimes |c_1, c_2\rangle \tag{8}$$

$|c_1, c_2\rangle \quad = (\alpha|000\rangle + \beta|001\rangle + \Upsilon|010\rangle + \delta|011\rangle + \varepsilon|100\rangle + \zeta|101\rangle + \eta|110\rangle + \theta|111\rangle$

Where, $|\alpha|^2+|\beta|^2+|\Upsilon|^2+|\delta|^2+|\varepsilon|^2+|\zeta|^2+|\eta|^2+|\theta|^2=1$

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2024 doi:10.20944/preprints202402.0529.v1

4.3. Quantum Embedding

A quantum embedding (QE) utilizes a quantum feature map to visualize bits as states of quantum matter (Qubits)in a Hilbert space. Using conventional datapoint 'i', it generates a quantum state $|\boldsymbol{\psi}_i\rangle$by adjusting the settings of a quantum circuit's gates The abstract representation of conversion of classical blockchain to quantumized blockchain is shown following figure 4.

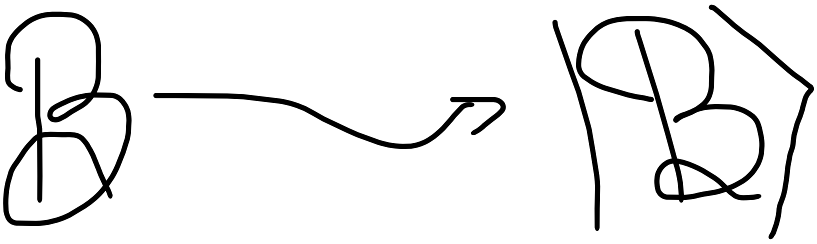


Figure 4. Abstract representation of conversion of classical blockchain to quantumized blockchain.

Consider traditional input data(bits), which consists of K instances, each of which has L attributes**.**

$$\text{QE}= i^1, \quad i^2, \quad i^3,\ldots\ldots\ldots\ldots\ldots, \; i^k,\ldots\ldots\ldots \quad i^K, \tag{9}$$

where i^k, is L-dimensional vector for k=1,2,3………K. In order to incorporate this data into quantum subsystems, namely qubits or qblocs, there are several embedding approaches that can be employed. A quick explanation of technique called basis embedding is provided below.

The process of basis embedding (BE) involves the association of every data point with a computing ground state within a quantum-bit system. Hence, traditional information must be represented as a sequence of 0s and 1s. The embedded quantum state refers to the conversion of a string of bits into the equivalent states of the quantum layer, where each bit is represented by a specific quantum state. As an illustration, the value of i, which is equal to 110111, is denoted by the quantum state of a 6-qubit system, specifically denoted as |110111⟩. Therefore, each quantum layer corresponds to a single unit of traditional bits.

Let us examine the traditional dataset health records denoted as H, which has been discussed before. In the context of basis embedding (BE), it is required that each instance is represented as a binary string composed of N bits. Specifically, an example x^N is denoted as (x_1, ..., x_N), where each x_i is either 0 or 1 for i = 1, ..., N. Given that every attribute is encoded using unitary bits (a single bit), it is possible to unambiguously associate each input example $i^k$with the corresponding quantum state $|i^k\rangle$.

This implies that the minimum requirement for the number of quantum components, denoted as n, is that it must be equal to or greater than N. Superpositions of every base states are a useful way to represent the full dataset as

$$|\text{H}\rangle= \frac{1}{\sqrt{K}} \sum_{k=1}^{K} |i^k\rangle. \tag{9}$$

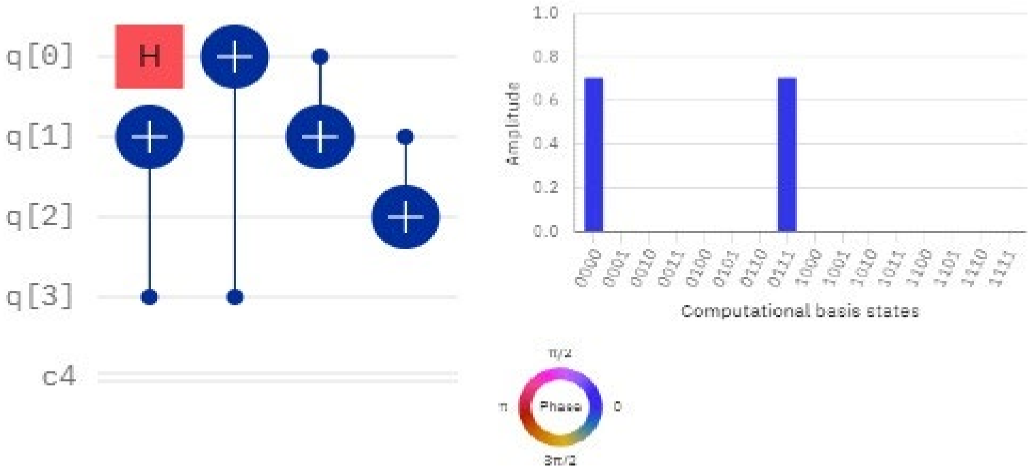
As an illustration, consider a classical dataset consisting of four examples, denoted as i^1 = 0000 and i^2 = 0111. The basic encoding method in (9) utilizes a pair of qubits to represent the states $|i^1\rangle$ = |0000⟩ and $|i^2\rangle$ = |0111⟩, leading to

$$|\text{H}\rangle= \frac{1}{\sqrt{2}} \; |0000\rangle + \frac{1}{\sqrt{2}} \; |0111\rangle. \tag{10}$$

Now, that the above dataset has been embedded as qubits (8), the state of the four Qblocks can be represented as

$$|\text{B}\rangle= \frac{1}{\sqrt{2}} \; |0000\rangle + \frac{1}{\sqrt{2}} \; |0111\rangle. \tag{11}$$

It is evident that a sequence of n bits can be stored using only one quantum bit, resulting in a significant reduction in resource use. The subsequent passage serves as a tangible illustration of Figure 5.



Output State: [0.707+0j, 0+0j, 0+0j, 0+0j, 0+0j, 0+0j, 0+0j, 0.707+0j, 0+0j, 0+0j, 0+0j, 0+0j, 0+0j, 0+0j, 0+0j, 0+0j]

Figure 5. A tangible illustration of Quantum Embedding with 4 qubits and its computational basis states.

4.4. *Representations of Qblocks*

From the equation (11), clearly, only one quantum bit is needed to store a sequence of 'n' bits, which greatly reduces resource use. The fine-grained form of equation (11) will be representing the Qblocks as follows:

Table 2. Representation of Qblocks.

When x=1 for $|B_x\rangle$	$|B_1\rangle= \frac{1}{\sqrt{2}}\ |0\rangle + \frac{1}{\sqrt{2}}\ |1\rangle.$
When x=2	$|B_2\rangle= \frac{1}{\sqrt{2}}\ |00\rangle + \frac{1}{\sqrt{2}}\ |01\rangle+ \frac{1}{\sqrt{2}}\ |10\rangle + \frac{1}{\sqrt{2}}\ |11\rangle.$
When x=3	$|B_3\rangle= \frac{1}{\sqrt{2}}\ |000\rangle + \frac{1}{\sqrt{2}}\ |001\rangle+ \frac{1}{\sqrt{2}}\ |010\rangle + \frac{1}{\sqrt{2}}\ |011\rangle + \frac{1}{\sqrt{2}}\ |100\rangle + \frac{1}{\sqrt{2}}\ |101\rangle+ \frac{1}{\sqrt{2}}\ |110\rangle + \frac{1}{\sqrt{2}}|111\rangle$
When x=4	$|B_4\rangle= \frac{1}{\sqrt{2}}\ |0000\rangle + \frac{1}{\sqrt{2}}\ |0001\rangle+ \frac{1}{\sqrt{2}}\ |0010\rangle + \frac{1}{\sqrt{2}}\ |0011\rangle + \frac{1}{\sqrt{2}}\ |0100\rangle + \frac{1}{\sqrt{2}}\ |0101\rangle+ \frac{1}{\sqrt{2}}\ |0110\rangle + \frac{1}{\sqrt{2}}|0111\rangle+\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.\frac{1}{\sqrt{2}}|1111\rangle$
When x=n	$|B_n\rangle= \frac{1}{\sqrt{2}}\ |0000\ldots.000\rangle + \frac{1}{\sqrt{2}}\ |00\ldots0001\rangle+ \frac{1}{\sqrt{2}}\ |00\ldots0010\rangle + \frac{1}{\sqrt{2}}\ |000\ldots0011\rangle + \frac{1}{\sqrt{2}}\ |000\ldots0100\rangle + \frac{1}{\sqrt{2}}\ |000\ldots0101\rangle+ \frac{1}{\sqrt{2}}$

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2024 doi:10.20944/preprints202402.0529.v1

$$|0000\ldots.0110\rangle + \frac{1}{\sqrt{2}}|0000\ldots.0111\rangle + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.\frac{1}{\sqrt{2}}|11\ldots1111\rangle$$

5. Quantum Entangled Medical Record (EQMR)Protocol

With the help of information sensing technologies, the Internet of Health Things (IoHT) aims to intelligently identify, area or location, track, manage, and monitor healthcare amenities. The proposed blockchain-based quantum health record system keeps a public health record management (HRM) across numerous healthcare providers to provide better healthcare management for patients. By allowing doctors to access one other's notes, patients will be able to monitor and ensure that all treatment procedures are being carried out correctly. The use of shared health records facilitates transparency throughout the treatment process, enabling effective supervision and monitoring of each step of treatment. In order to keep up a quantum blockchain system, a quantum-based hospital network was created. As soon as the arrangement is live, instruments begin producing raw health data for patients, and doctors begin entering the data as a health records. A group of hospitals and other medical facilities have banded together to create a quantum network and keep a quantum blockchain up and running. When the system is live, sensors collect raw patient health data, to which doctors and nurses then add those data as treatment records. The patient's identification will be attached to these records. These data, along with the time they were generated and the places they came from, make up a patient's health record. The procedure's schematic and QHR protocol's flowchart is depicted in Figure 6. depicts the. The procedure's detailed steps are as follows.

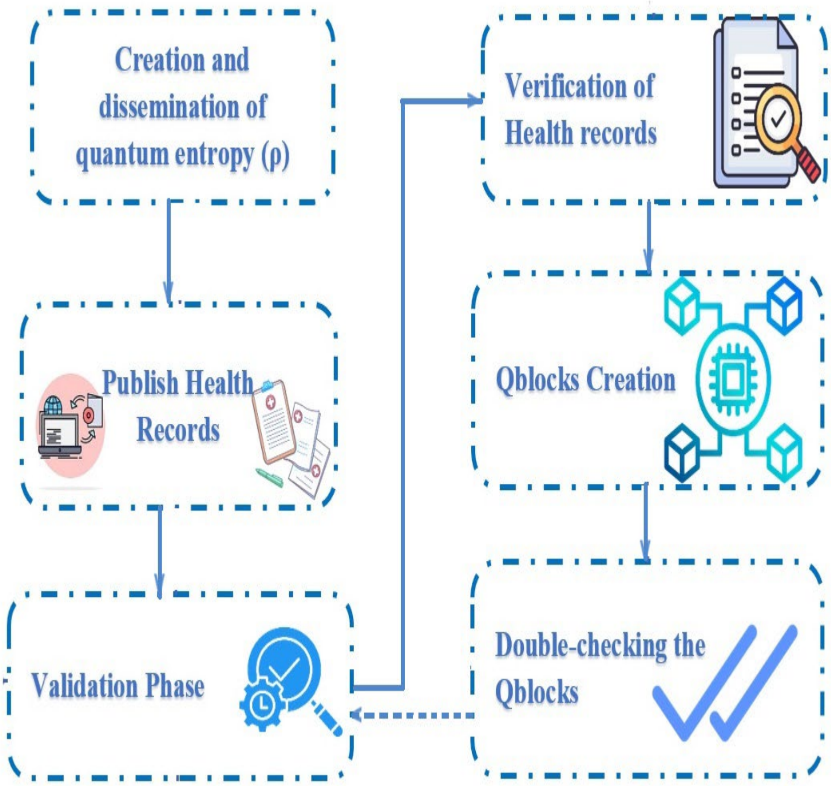

Creation and dissemination of quantum entropy (ρ)
Publish Health Records
Validation Phase
Verification of Health records
Qblocks Creation
Double-checking the Qblocks

Figure 6. A Process flow of the EQHR protocol's procedure.

5.1. Creation and Dissemination of Quantum Entropy

Multiple branches of hospital collaborate to establish a secure quantum information network. All of the nodes are trustworthy and can reliably exchange quantum and classical data, as well as

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2024 doi:10.20944/preprints202402.0529.v1

prepare, store, and measure quantum states. Let each node have access to quantum entropy so that post-quantum keys may be created using quantum pure randomness. In the event that individual nodes are unable to generate enough quantum entropy, a central source may be accessed over a quantum-resistant link. Each pair of quantum nodes in a quantum network uses the same N-key string, which is distributed in an unconditionally secure manner.

Take, for instance, the six-node quantum network seen in Figure 7 A, B, C, D, E, and F are the six nodes, and any two of them can have a conversation with the others. Quantum states can be stored, prepared, and sent at each node. Each pair of nodes communicates with each other using a mix of quantum and classical channels, and they use the same set of keys, each of length 20, for example key_{BF} = 10101100010101010111110. The EQHR protocol is responsible for key distribution.

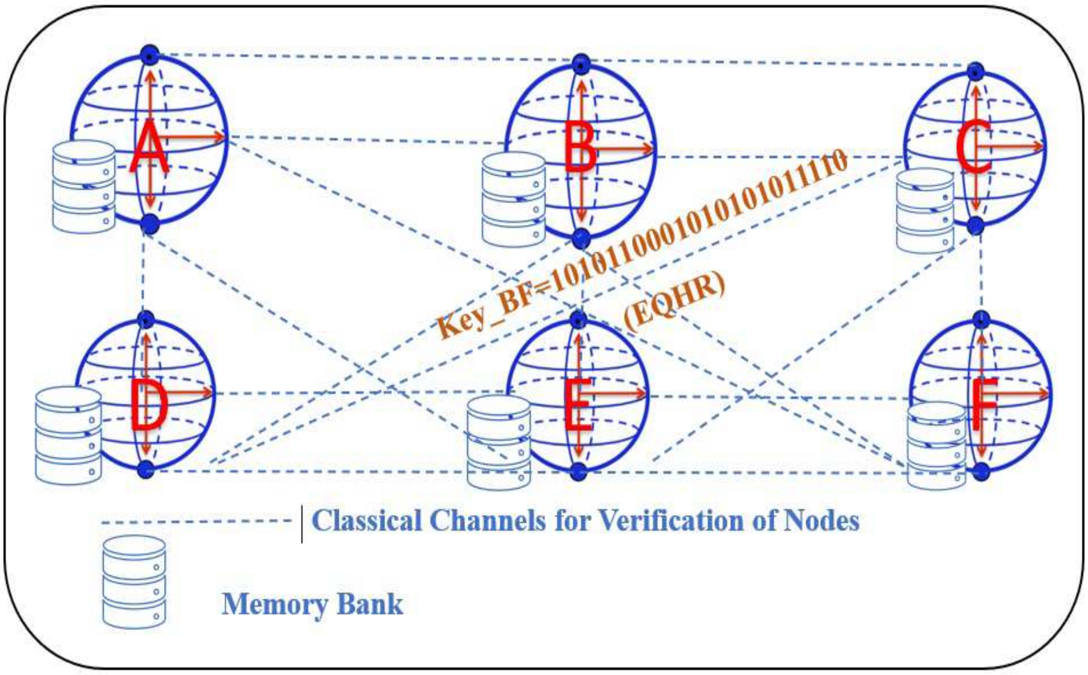

A
B
C
D
E
F
Key_BF=10101100010101010111110
(EQHR)
Classical Channels for Verification of Nodes
Memory Bank

Figure 7. A six-node quantum network for verification process.

Following the dissemination of the health record data, nodes D, E, and F will send requests for verification to node A, while nodes A, B and C will send verification calls to node D. Here, we'll pretend that node D has decided to send node A, a validation request.

Assuming that all 20 Bell states prepared by Node D′ are "$\mathscr{B}$," the network will use these states to authenticate users. Node D delivers the sequence S2 to node A, who picks particles at locations 2, 4, 6, 10 13,15, 17 and 19 for measurement. Table 4 displays the underlying measurements and the resulting values.

5.2. Publish Health Records

Now, let's say that node "A" in the quantum network is interested in making its health records public. Programming on the "A" Network to other nodes in the qnet the hash of the health record. Assuming that there are two health records are produced during the period, nodes B and F would each make available a health record (health record B, HB) and node F's health record (health record F, HF). All the other nodes get details about the health record, including the patient's identifier, the data's origins, a timestamp, and the hash of the data.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2024 doi:10.20944/preprints202402.0529.v1

Table 3. Equivalent bits in the hash value and the ratio to $\boldsymbol{B_{init}}$ & $\boldsymbol{F_{init}}$.

Root Hash	0x1c9d15000aaa03e75b0449bd0b638d09ac6f5ce75201c657
H_B	1010111100110101100010101100011110100
H_F	0101011100100001001111010110110100101110
hash$_B$	0x356fc60a20190c462e08e4fe05d8650a2d5413b984201c34
hash$_F$	0xef2eb1bff1708434918a38d3a86a2064b4304bba8073017

Table 4. Measurement of base input and its corresponding output of particles at positions 2, 4, 6, 10, 13,15 ,17 and 19.

	Pos_2	Pos_ 4	Pos_ 6	Pos_10	Pos_ 13	Pos_15	Pos_17	Pos_19
BI	{∣0⟩, ∣1⟩}	{∣↑⟩,∣↓⟩}	{∣+⟩, ∣-⟩}	{∣∈⟩,∣∉⟩}	{∣u⟩, ∣v⟩}	{∣x⟩, ∣y⟩}	{∣∱⟩,∣∲⟩}	{|α⟩,∣β⟩}
Output	∣1⟩	∣↑⟩	∣-⟩	∣∉⟩	∣v⟩	∣y⟩	∣∲⟩	|α⟩

5.3. Validation Phase

To counteract attacks from near-term computing, the QUAB network employs quantum authentication in place of conventional digital signature and cryptography algorithms. After obtaining A's health data, each node will issue a validation request to her. To better illustrate the steps involved in the validation process, we'll use the subsequent scenario, in which D sends a validation request to A. The following flowchart provides a representation of the identity validation process.

5.4. Verification of Health Records

After establishing A's identity, the remaining nodes in the network check the hash to ensure the health record is accurate. If there are no problems, the health record is added to the bank of health records to be compiled.

5.5. Qblocks Creation

The intervals of block production are managed approximately ten minutes utilising the uncertainty of getting arbitrary numbers and every healthcare organization spends their savings by fighting for recordkeeping privileges. In view of that, node "B" has been given access to the books, he will now package the health records in the health records bank that are due to be packed into blocks during the time period and send them out to the other nodes.

5.6. Double-Checking the Qblocks

Once the remainder of the nodes get the Qblock information broadcasted by "B," they verify the Qblock hash value, the adherence of the hardness objective and nonce related to mining, and the truthfulness of the health record list in the block. Each of the nodes in the Qnet adds the qblock to its private replica of the QUAB if all data contained in the qblock is accurate; elsewhere, the block is deleted. Each Qblock's hash values establish entangled states with the others.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2024 doi:10.20944/preprints202402.0529.v1

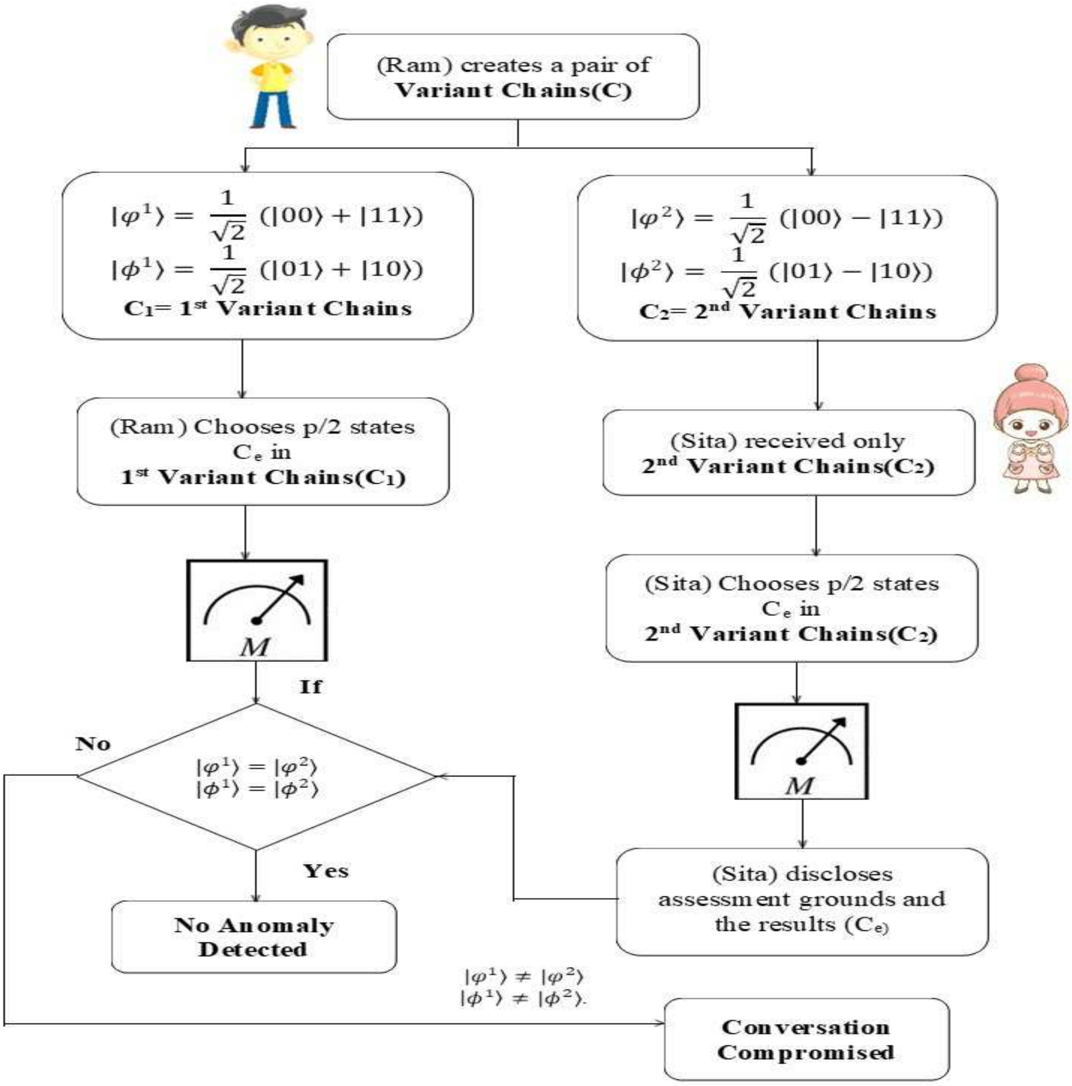

(Ram) creates a pair of Variant Chains(C)
$|\varphi^1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
$|\phi^1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
C1= 1st Variant Chains
$|\varphi^2\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$
$|\phi^2\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$
C2= 2nd Variant Chains
(Ram) Chooses p/2 states Ce in 1st Variant Chains(C1)
(Sita) received only 2nd Variant Chains(C2)
(Sita) Chooses p/2 states Ce in 2nd Variant Chains(C2)
M
If
No
$|\varphi^1\rangle = |\varphi^2\rangle$
$|\phi^1\rangle = |\phi^2\rangle$
M
Yes
No Anomaly Detected
(Sita) discloses assessment grounds and the results (Ce)
$|\varphi^1\rangle \neq |\varphi^2\rangle$
$|\phi^1\rangle \neq |\phi^2\rangle$.
Conversation Compromised

Figure 8. A Flowchart for 'Ram' seeks validation from 'Sita'.

5.7. Validation Process and its Descriptions

S1: (Ram) selects and prepares himself a chain from the following equations (12,13,14,15), C = {|ψ1⟩, |ψ2⟩.... |ψ (n/2) ⟩} while also recording his various states. Here the equations (12,13) are the C1 which is the 1st variant chains and the equations (14,15) are 2nd variant chains.

$$|\varphi^1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{12}$$

$$|\phi^1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{13}$$

$$|\varphi^2\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{14}$$

$$|\phi^2\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{15}$$

S2: With each phase or positions in C, (Ram) retains the first variant to create chain C1, and (Sita) receives the second variant to form chain C2. (Sita) To identify anomalies, she chooses p/2 states Ce in

C_2. Afterwards, she discloses both the assessment grounds and the results after recording the states of C_e and arbitrarily choosing assessment grounds to detect variants in C_e. When measuring the C_e variations, (Ram) uses the same evaluation criteria and then correlates the findings. Both variables' performance on the state's evaluation are related; the following table 5 exhibits the same.

Table 5. Selected Variant Chains Assessment Values.

	$\|\varphi^1\rangle$	$\|\phi^1\rangle$	$\|\varphi^2\rangle$	$\|\phi^2\rangle$
$\{\|0\rangle, \|1\rangle\}$	00	01	00	01
	11	10	11	10
Anomalies can be easily detected if the values are different.			$\|\varphi^1\rangle = \|\varphi^2\rangle$ $\|\phi^1\rangle = \|\phi^2\rangle$	

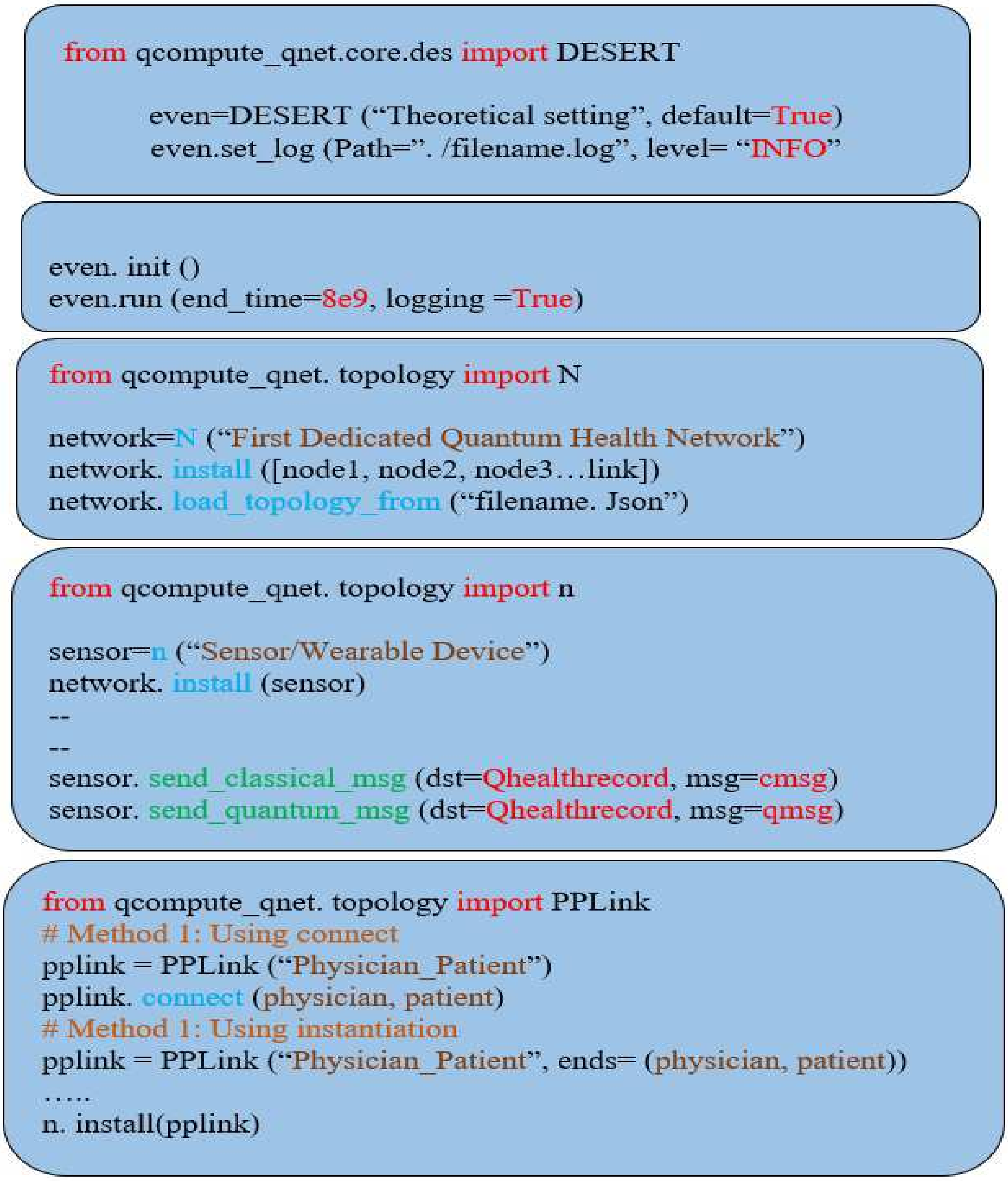
When the error probability is below the specified limit, (Ram) and (Sita) proceed to (**S3**). If not, they discard the selected variants, when $|\varphi^1\rangle \neq |\varphi^2\rangle \quad and \quad |\phi^1\rangle \neq |\phi^2\rangle$. If it's not, it's deemed an eavesdropping attempt, and the conversation ends.

S3: Both (Ram) and (Sita) prefers Unitary transformations, which preserves the inner product of the selected chain variants, which is more powerful than the operation used in (**S1**). Based upon the type of information, that (Ram) wants to send to (Sita), he will apply the quantum gates to his qubit.

For instance, (Ram) just transmits (Sita) the value '00' without touching his qubit if he wishes to do so. To convey the number '01', Ram modifies his qubit by applying the phase flip Z, which changes its quantum state to equation (14) . (Ram) uses the NOT gate to communicate the integer '10', providing the result equation (13). The equation (15) is the result of applying NOT and Z to send'11'. Then based on the assessment of the different selected chain variants, validation can be done.

6. Theoretical Setting

The theoretical setting will serve as our starting point here. A DES environment (DESERT) must be built beforehand, as it will serve as the simulation's driver for the entire network. Furthermore, we may allow the entities to automatically attach to the default environment by setting the simulation environment to default (i.e., setting the option default=True). The set default env method can also be used for this purpose. In addition, there is a logging feature built into the simulation environment for keeping track of data as it becomes available. Set log allows us to modify logging behaviour by adjusting things like the log level and the location of the log file. Figure 9 is an example of some code.



```
from qcompute_qnet.core.des import DESERT

        even=DESERT (“Theoretical setting”, default=True)
        even.set_log (Path=”. /filename.log”, level= “INFO”


even. init ()
even.run (end_time=8e9, logging =True)

from qcompute_qnet. topology import N

network=N (“First Dedicated Quantum Health Network”)
network. install ([node1, node2, node3…link])
network. load_topology_from (“filename. Json”)

from qcompute_qnet. topology import n

sensor=n (“Sensor/Wearable Device”)
network. install (sensor)
--
--
sensor. send_classical_msg (dst=Qhealthrecord, msg=cmsg)
sensor. send_quantum_msg (dst=Qhealthrecord, msg=qmsg)

from qcompute_qnet. topology import PPLink
# Method 1: Using connect
pplink = PPLink (“Physician_Patient”)
pplink. connect (physician, patient)
# Method 1: Using instantiation
pplink = PPLink (“Physician_Patient”, ends= (physician, patient))
…..
n. install(pplink)
```

Figure 9. Sample code for the Simulated Environment(DESERT).

7. Results & Discussion

In this analysis, we take a look at the findings from the simulation and assess the reliability and safety of the proposed system and EQHR protocol. In addition, parallels are drawn to existing blockchain schemes.

7.1. Multi Hash Collision Resistance Analysis

Collision resistance in the hash function is essential for creating a blockchain that cannot be altered and can be tracked back to its source. Core to the operation of the proposed system is the Markov chain with memory-based hash function.

The quantum hash function's security is ensured not by solving difficult mathematical problems, but by the limitless possibilities of the beginning state and its immutable nature of assessment. The acquired normal distribution or Bell curve provides no beneficial data without knowledge of the beginning states. Modulo operators are then used to convert the hash value from the normal distribution. Due to the one-to-many nature of this relationship, it cannot be undone. It's quite difficult to reverse-engineer a hash value into its original normal distribution. The robustness of the hash algorithm against collisions is evaluated here. All it takes to run the test is changing a single bit in a sequence of message and far-sighted what happens to the hash created. Here, the generated 256-bit hashes are based on a total of 1000 Quantum walks. The following figure 10 exhibits the Quantum walk with one step forward (4 cycle node). Pick an arbitrary value M value at random, and then swap the message's first, final, 100th bits and 1000th bits to arrive at Mfirst, Mlast, M100 and M1000.

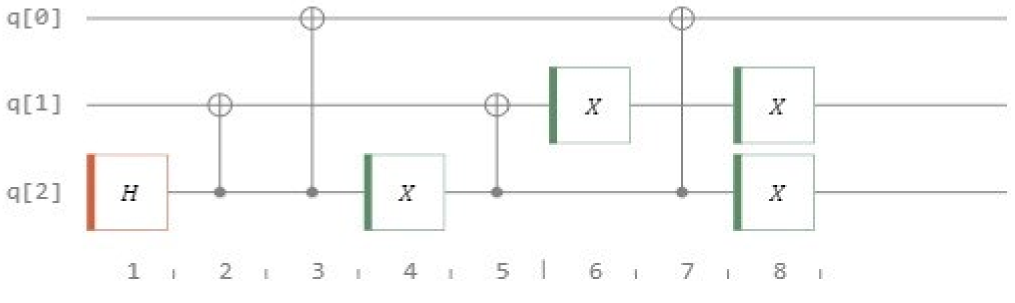
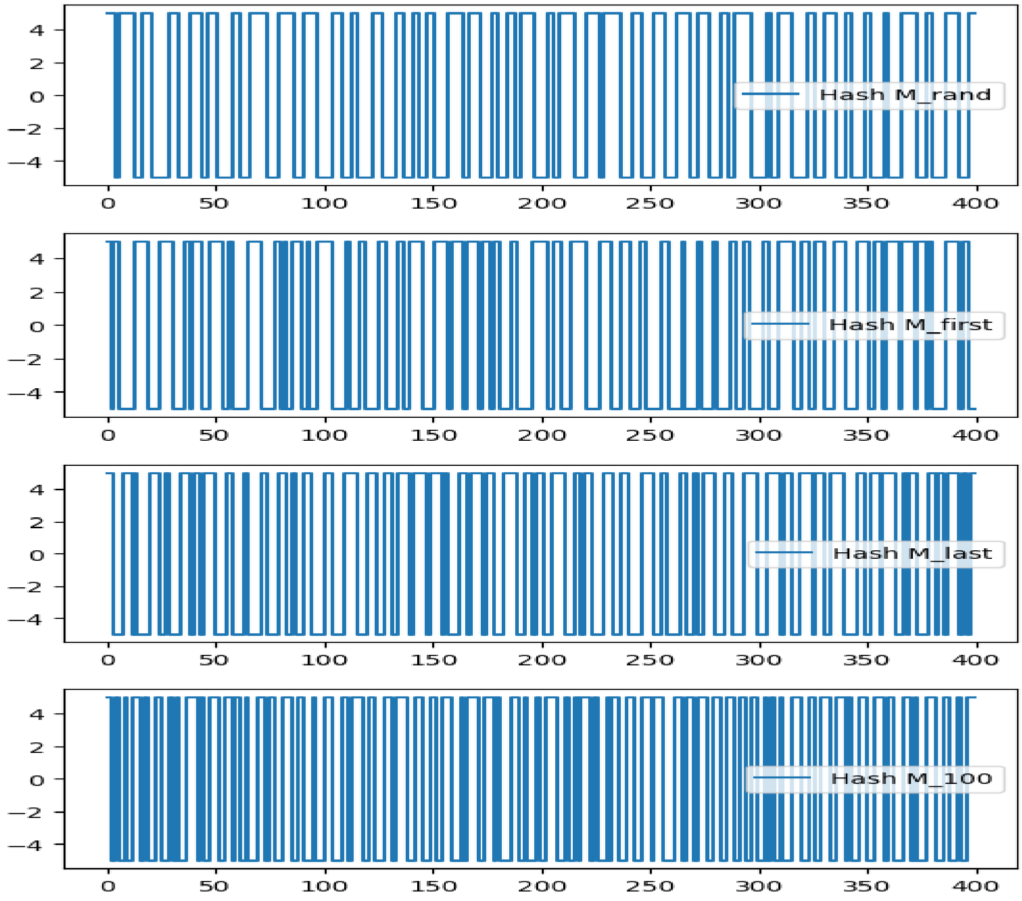


Figure 10. Quantum Walk- One Step Forward, On a 4-Noded Cycle.

In Figure 11, we can see how five slightly altered hash values compare to the original message. A hash variance of at least 35% is possible with a modification of just 0.25 percent in the randomly chosen message string. As a result, the hash value produced by the little modified message is very different from the one that was initially sent. Because of its strong statistical features and ability to prevent data corruption or manipulation, the so-called hash value constructed using Markov chain with memory makes the blockchain network extremely valuable.



Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2024 doi:10.20944/preprints202402.0529.v1

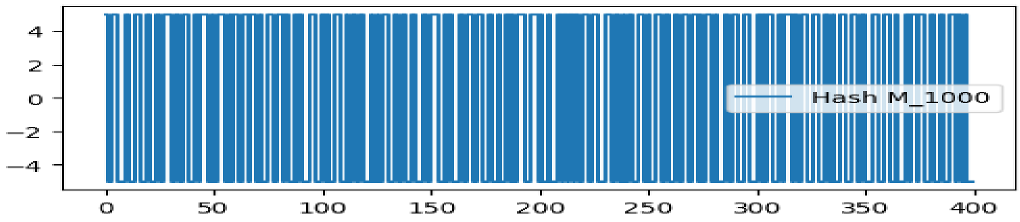


Figure 11. Plots of Various Quantum Hash Values (Mrand, Mfirst, Mlast, M100, M1000).

7.2. Attacks and Analysis

We conduct a thorough analysis of our protocol's safety here. For the EQHR protocol, it is important to think about both external assaults from snoopers and inside attacks from deceitful players. As a result, EQHR protocols require a more involved security evaluation than QKD methods.

7.2.1 Outside Attack

Let's pretend that an adversary node is introduced into the network. Ravana plans to distribute a bogus health record externally of the restricted quantum network in order to disrupt the patient's regular care. The other nodes will need to send a request for identification to Ravana after they have received this health data. Since the blocs in the proposed system implement quantum key distribution (QKD), which necessitates knowledge of the key's information, Ravana is unable to finish the validation stage and illicitly leak the fake health file. Therefore, this QUAB network can ensure the safe and effective functioning of the EQHR protocol by discouraging malevolent players from disseminating false health information.

7.2.2. A Simple Intercept-Resend Attack

For the sake of argument, let's say Ravana desires to seize the key among Sita and the remaining ones, so she may publish a bogus health file and disrupt the patient's regular treatment by means of an Intercept-Resend attack. Consider the scenario where Rama sends a request for identification to Sita. In such a scenario, if some 'X' intercepts the transmitted particle sequence R_2 (second step of the algorithm 1), and 'X' started measuring the original transmitted particle based on the $\{|+\rangle, |-\rangle\}$, then the Bell state of the particle sequence R_2 produces a new vector space, in which all the states related with will be in different space and in entangled position. Following the measurement, 'Ravana' will prepare the element sequencing RX and transmit it to 'Rama' together with the intercepted sequence.

If only Ram(A)' suspects the particle sequence received, then there is a 50% probability that R_X, may hold a same value of R_1. i.e., in other sense $R_1 \neq R_X$. The following figure exhibits the entire scenario of the Intercept- Resend attack of the system.

Since 'X' will be immediately exposed if he/she attempts an IR attack on the process of verification between two quantum blocks, he/she will be unable to steal any confidential information. On this Medical quantum blockchain (MQB) network, IR attacks are impossible to pull off. The entire scenario has been illustrated in figure 12.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2024 doi:10.20944/preprints202402.0529.v1

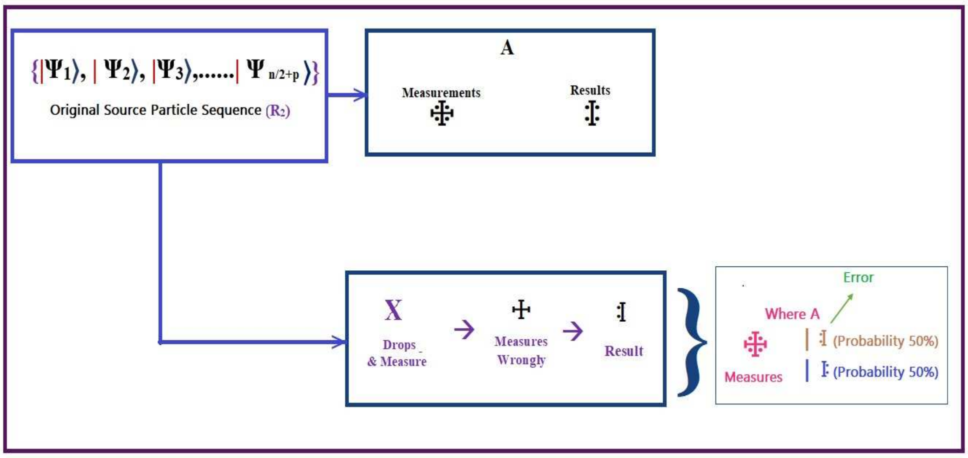


Figure 12. Intercept- Resend attack of the system.

7.2.3. Entanglement Measure Attack (ENMA)

Let's say Ravana(X) is attempting to publish a bogus health report by stealing the key that links node Rama to the other nodes in the network via an Entanglement Measure attack. Consider the scenario when Rama seeks Sita's approval for authentication. Ravana must use isomorphism to entangle the electron in transport with the supplementary atom in her hands with the goal of obtaining the knowledge of the particle that is being targeted. The definition of isomorphism is as follows.

$$\mathrm{U}\,|-\rangle|X\rangle = \sigma_-\,|\text{-}\rangle\,|X_0\rangle \;+\tau_-\,|+\rangle\,|X_1\rangle \tag{16}$$

$$\mathrm{U}\,|+\rangle|X\rangle = \sigma_+\,|\text{-}\rangle\,|X_2\rangle \;+\tau_+\,|+\rangle\,|X_3\rangle \tag{17}$$

Here, $|\sigma_-|^2 + |\tau_-|^2 = 1$ and $|\sigma_+|^2 + |\tau_+|^2 = 1$. $|X\rangle$ is obviously the supplementaty particle of the 'X'- The intruder.

Because of this, to prevent the espionage process from being uncovered, the algorithm must account for isomorphism. We refrain from performing standard logical or arithmetic operations on qubits as we would in traditional computers. The concepts of "while statement" and "branching statement" do not exist in quantum computing. To handle qubits using the interference principle of quantum physics, we substitute unitary operators. Look sophisticated yet are in fact simple to use.

$$(\psi|-\rangle|X\rangle\langle X|\langle -|\psi^{\dagger}) = |\text{-}\rangle|\text{-}\rangle \tag{18}$$

$$(\psi|+\rangle|X\rangle\langle X|\langle +|\psi^{\dagger}) = |+\rangle|+\rangle \tag{19}$$

$$(\psi|0\rangle|X\rangle\langle X|\langle 0|\psi^{\dagger}) \;=\; |0\rangle|0\rangle \tag{20}$$

$$(\psi|1\rangle|X\rangle\langle X|\langle 1|\psi^{\dagger}) \;=\; |1\rangle|1\rangle \tag{21}$$

Here, τ_- and $\sigma_+ = 0$ and $\tau_+|+\rangle|X_3\rangle - \sigma_-|\text{-}\rangle|X_0\rangle = 0$. When all of those things line up, it's clear that the surjective bounded operation will be of:

$$\mathrm{U}\,|\psi\rangle|X\rangle = \;\sigma_-\,|\psi\rangle\,|X_0\rangle \tag{22}$$

Since the surjective bounded operator places the apprehended and additional particles in separate quantum spaces, the extra photons cannot provide Ravana with reliable information. So, there's no way for Ravana to exploit the algorithm using an ENMA and learn anything. If Ravana is able to intercept the R2 sequence transmitted in algorithmic fashion and then carry out the surjective bounded operation with the particles in his control, we have a working version of the algorithm. After a surjective bounded operation, the states of the qblocks are shown in the above equation.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2024 doi:10.20944/preprints202402.0529.v1

Consider the Bell state $|\Phi^{\dagger}\rangle$; following the surjective bounded operation, the additional particle $|\boldsymbol{X}\rangle$acquires a state of entanglement with the Bell state.

$$\mathrm{U}|\Phi^{\dagger}\rangle|X\rangle = 0.5\begin{cases}|\Phi^{\dagger}\rangle(\sigma_{-}|X_0\rangle + \tau_{+}|X_3\rangle + |\Phi^{\dagger}\rangle(\sigma_{-}|X_0\rangle - \tau_{+}|X_3\rangle) \\ |\psi^{\dagger}\rangle(\tau_{-}|X_1\rangle + \sigma_{+}|X_2\rangle + |\psi^{\dagger}\tau_{-}|X_1\rangle - \sigma_{+}|X_2\rangle)\end{cases} \tag{23}$$

Since Rama now has a 0.25 percent chance of determining the proper Bell state, it is likely that the eavesdropping procedure will pick up on Ravan's presence. If Ravan attempts an ENMA attack on the verification process between two quantum spaces, Ravan will undoubtedly be exposed and rendered impossible to get any sensitive data.

7.3. Validity and Auditability of Quantum Blocks

Even if Ravana were to desire to alter the contents of a qblock, she would be unlikely to achieve, due to the fact that she could not alter the hash value of both current and subsequent blocks simultaneously. By storing the verified information in the qblock, the DQHR protocol can guarantee the secrecy and correctness of the data in the qblock.

If data from a specific block in a chain of blocks linked by entangled states has to be located and audited, the relative phase of the timestamp associated with that block can be determined using the quantum phase estimation (QPE) procedure. The phase value may be precisely retrieved by employing an adequate number of additional particles. We need to find the phase factors in the quantum state that corresponds to the time $|t\rangle$, taking into account that 'a' is the quantity of additional particles. The chronology indicator of the data to be mined allows us to set the quantum state time 't'. If k= 1, 2, 3, ..., a-1, then it is possible to do an oracle operation with controlled $|\psi^{4}|\rangle$. The above finding suggests that the quantum blockchain suggested in this article can guarantee the precision of the data included inside the qblock and accomplish data tracking by retrieving the hash of the every data at the proper moment. The relative phase at time $|t\rangle$ may be extracted using the quantum circuit diagram shown in Figure 13.

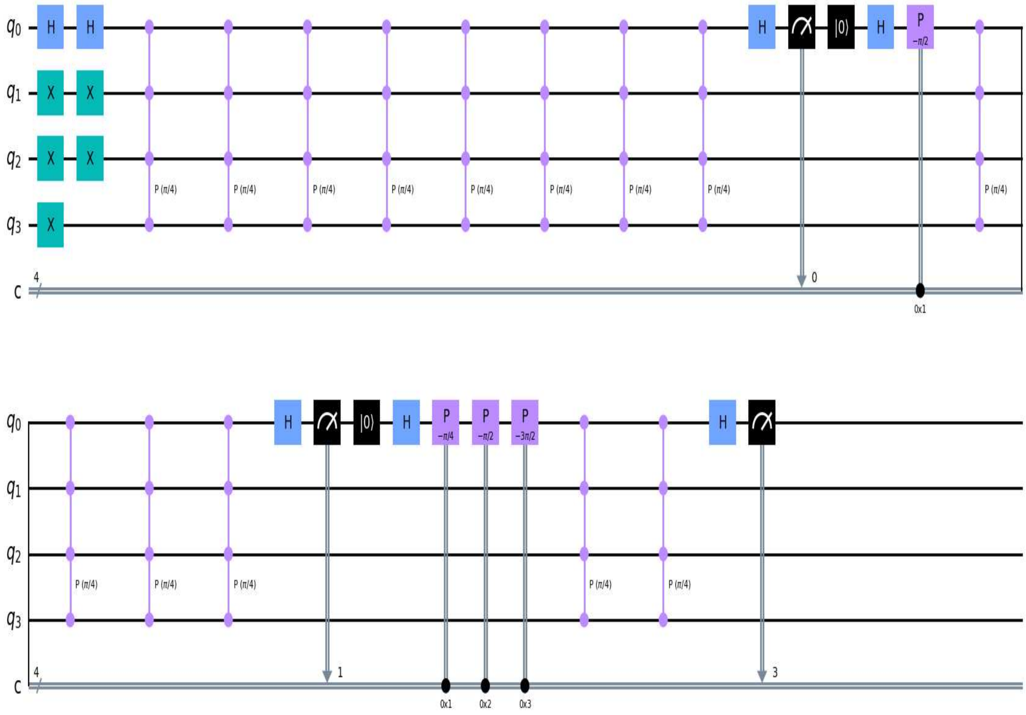


Figure 13. The schematic representation of the quantum circuit to determine the phase distribution of a quantum state.

7.4. A Review of Accomplishment

Here, we take a look at various current blockchain models and compare them to the proposed quantum blockchain. Table 6 displays the pertinent comparisons among the references [39–41].

Improving upon previous designs, this article [39] suggests an NTRU lattice-based postquantum blockchain architecture for the Internet of Things. Thanks to its efficient underlying lattice structure, the technique narrows down transaction sizes from hundreds of gigabytes to few kilobytes. To provide a broad foundation for future performance enhancement, the authors also proposed an aggregate signature across the NTRU lattice and segregated witnesses.

An overview of recent advances in the construction of quantum-safe systems, an examination of the vulnerabilities of existing cryptographic methods to computational and innovations in technology, and possible remedies to these vulnerabilities are the primary takeaways from the article [40].

The study [41] goes over the well-known area of quantum computing, how present encryption is threatened by it, and how algorithms are being developed to estimate how many qubits would be needed to crack the system of blockchain security.

Table 6. Pertinent comparisons with existing systems.

Review	**Information traceability**	**Quantum Block structure**	**Resist quantum computer attacks**	**QKD**	**Quantum walk**	**Quantum Embedding**	**Quantum Entropy**
NTRU lattice [39]	Yes	Yes	Yes	No	No	No	No
Hybrid Quantum [40]	Yes	No	Yes	Yes	No	No	No
Quantum-resistant blockchain networks [41]	Yes	No	Yes	Yes	No	No	Yes
QUAB (Proposed)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

8. Conclusions

Sharing electronic medical records between healthcare professionals is essential, but this information is extremely private and must be treated as such. Blockchain technology can facilitate a multi-party trust model by providing accessible, immutable, and transparent electronic health records. Nevertheless, with the progress of near term quantum computing techniques, vulnerabilities in the current blockchain architecture have emerged. This study offers a physics inspired blockchain network which is actually a quantum computing and creates a new entangled quantum health record (EQHR) protocol with privacy and security at the forefront of their respective architectures. The data blocks that make up this physics inspired blockchain are linked via states(bloQ) of entanglemts. The protocol for the Quantumized Health Record (QHR) goes into great detail about quantum information processing. Health information stored in IoMT systems can be kept secure and private, and their whereabouts can be traced at all times. In light of the findings from the computational study, the QUAB network is impenetrable to quantum computer attacks. The quantum block's precision and audit trail are evaluated. In addition, several competing QUAB models are contrasted with the one put forward in this article.

In order to improve safety and effectiveness, QUAB makes use of quantum entanglement, a feature that is absent from standard blockchain. This paper's suggested framework for quantum blockchains provides more detail about the information processing mechanism of the health record protocol and the data structure of quantum blockchains than previous research has found. There are, however, still restrictions on the work. To what extent the EMR procedure should be implemented in practice is not specified in this study. Due to logistical limitations, it has yet to be tested in a genuine experimental context. As technology develops further, quantum information processing and its networking will be able to be fully integrated into world wide web (WWW). Eventually, the quantum Internet will incorporate not only QKD but also other information security technologies. Conversely,

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2024 doi:10.20944/preprints202402.0529.v1

the present system for quantum information transfer is still in its early stages and is being expanded at the moment. Unfortunately, a quantum blockchain cannot be implemented without a special kind of quantum network. The QUAB architecture and EQHR protocol proposed in this paper need to overcome the first obstacle—noise interference—before they can be tested in a real quantum system. It is also important to solve the problem of sustaining 'Q'states over a prolonged amount of time. The real-world difficulty lies in solving the problem of maintaining the stability of quantum states carried by block carriers. The improved methodology and practical applications of quantum blockchain should be the focus of future studies. Additional work is required to create a working quantum blockchain with a transport layer that can run on a real quantum computer, is easy to implement, and offers great security and scalability.

Author Contributions: Conceptualization, AB.; methodology, AB.; software, BS.; validation, BS.; formal analysis, AB.; investigation, AB.; resources, AB.; data curation, AB.; writing—AB, X.X.; writing—review and editing, BS.; visualization, AB.; supervision, BS; project administration, BS.; funding acquisition, BS. All authors contributed to the final version of the manuscript and gave their final approval of the version to be published.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

Acknowledgments: The work was supported by Visvesvaraya PhD Scheme-Phase-II, Ministry of Electronics & Information Technology, India.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf.
2. Junfeng Miao, Zhaoshun Wang, Zeqing Wu, Xin Ning, Prayag Tiwari (2024). A blockchain-enabled privacy-preserving authentication management protocol for Internet of Medical Things, Expert Systems with Applications, Volume 237, Part A,121329, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2023.121329.
3. Gupta, S., Sharma, H.K., Kapoor, M. (2023). Integration of IoMT and Blockchain in Smart Healthcare System. In: Blockchain for Secure Healthcare Using Internet of Medical Things (IoMT). Springer, Cham. https://doi.org/10.1007/978-3-031-18896-1_7
4. Kumar, S., Tiwari, P. & Zymbler, M. Internet of Things is a revolutionary approach for future technology enhancement: a review. J Big Data 6, 111 (2019). https://doi.org/10.1186/s40537-019-0268-2
5. Kamalov F, Pourghebleh B, Gheisari M, Liu Y, Moussa S. Internet of Medical Things Privacy and Security: Challenges, Solutions, and Future Trends from a New Perspective. Sustainability. 2023; 15(4):3317. https://doi.org/10.3390/su15043317.
6. Beasley JW, Holden RJ, Sullivan F. Electronic health records: research into design and implementation. Br J Gen Pract. 2011 Oct;61(591):604-5. doi: 10.3399/bjgp11X601244. PMID: 22152827; PMCID: PMC3177114.
7. Yeo LH, Banfield J. Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. Perspect Health Inf Manag. 2022 Mar 15;19(Spring):1i. PMID: 35692854; PMCID: PMC9123525.
8. Habib G, Sharma S, Ibrahim S, Ahmad I, Qureshi S, Ishfaq M. Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. Future Internet. 2022; 14(11):341. https://doi.org/10.3390/fi14110341
9. Virtual Mentor. 2012;14(9):712-719. doi: 10.1001/virtualmentor.2012.14.9.stas1-1209.
10. S. Lamba and M. Sharma, "An Efficient Elliptic Curve Digital Signature Algorithm (ECDSA)," 2013 International Conference on Machine Intelligence and Research Advancement, Katra, India, 2013, pp. 179-183, doi: 10.1109/ICMIRA.2013.41.
11. Kalra, S., Sood, S.K. (2011). Elliptic Curve Cryptography: Current Status and Research Challenges. In: Mantri, A., Nandi, S., Kumar, G., Kumar, S. (eds) High Performance Architecture and Grid Computing. HPAGC 2011. Communications in Computer and Information Science, vol 169. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-22577-2_62
12. R. Raussendorf, H. Briegel, A one-way quantum computer, Physical Review Letters 86 (22) (2001) 5188–5191, https://doi.org/10.1103/ PhysRevLett.86.5188.
13. T. P. Spiller, "Quantum information processing: cryptography, computation, and teleportation," in Proceedings of the IEEE, vol. 84, no. 12, pp. 1719-1746, Dec. 1996, doi: 10.1109/5.546399.

14. Abdelrahman Abuarqoub. 2021. Security Challenges Posed by Quantum Computing on Emerging Technologies. In Proceedings of the 4th International Conference on Future Networks and Distributed Systems (ICFNDS '20). Association for Computing Machinery, New York, NY, USA, Article 44, 1. https://doi.org/10.1145/3440749.3442651
15. D. K. Kumar, E. H. Venkata Krishna, R. Ushasri, V. Jahnavi, K. B. Prakash and S. Imambi, "Implementation of Grover's and Shor's Algorithms In Quantum Machine Learning," 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bengaluru, India, 2023, pp. 967-972, doi: 10.1109/IITCEE57236.2023.10091029.
16. Fedorov, A. K., Kiktenko, E. O., & Lvovsky, A. I. (2018). Quantum computers put blockchain security at risk. Nature, 563(7729), 465+. https://link.gale.com/apps/doc/A573163765/AONE?
17. S. K. Sehgal and R. Gupta, "Quantum Cryptography and Quantum Key," 2021 International Conference on Industrial Electronics Research and Applications (ICIERA), New Delhi, India, 2021, pp. 1-5, doi: 10.1109/ICIERA53202.2021.9726722.
18. Mavroeidis, V., Vishi, K., Zych, M. D. & Jøsang, A. he impact of quantum computing on present cryptography. Int. J. Adv. Comput. Sci. Appl. 9(3), 1–10 (2018).
19. Allende-Lopez, M. & Da Silva, M.M. Quantum Technologies: Digital Transformation, Social Impact, and Cross-sector Disruption. 1–94 (Inter-American Bank, 2019).
20. Punathumkandi, S. & Boscovic, D. A survey on quantum-safe blockchain system. in Annual Computer Security Applications Conference, Austin TX USA (2022).
21. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R. & Smith-Tone, D. NIST Report on Post-Quantum Cryptography (2026). https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf.
22. Ethereum’s pathway of handling quantum -https://www.erc4337.io/
23. Mavroeidis, V., Vishi, K., Zych, M. D. & Jøsang, A. The impact of quantum computing on present cryptography. Int. J. Adv. Comput. Sci. Appl. 9(3), 1–10 (2018).
24. Khalid, Z. M. & Askar, S. Resistant blockchain cryptography to quantum computing attacks. Int. J. Sci. Bus. 5(3), 116–125 (2021).
25. Punathumkandi, S. & Boscovic, D. A survey on quantum-safe blockchain system. in Annual Computer Security Applications, Conference, Austin TX USA (2022).
26. Webber, M., Elfving, V., Weidt, S., & Hensinger, W. K. (2022). The impact of hardware specifications on reaching quantum advantage in the fault tolerant regime. AVS Quantum Science, 4(1).
27. Kiktenko, E. O. et al. Quantum-secured blockchain. Quantum Sci. Technol. 3(3), 035004 (2018).
28. Cai, Z., Qu, J., Liu, P. & Yu, J. A blockchain smart contract based on light- weighted quantum blind signature. IEEE Access 7, 138657–138668 (2019).
29. Rajan, D. & Visser, M. Quantum blockchain using entanglement in time. Quantum Rep. 1(1), 3–11 (2019).
30. Chen, H. Quantum relay blockchain and its applications in key service. in Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy. 95–99 (2020).
31. Gao, Y.-L. et al. A novel quantum blockchain scheme base on quantum entanglement and DPoS. Quantum Inf. Process 19, 420 (2020).
32. X. Sun, M. Sopek, Q. Wang, P. Kulicki, Towards quantum-secured permissioned blockchain: signature, consensus, and logic, Entropy 21 (9) (2019) 1–15, https://doi.org/10.3390/e21090887.
33. E. Kiktenko, N. Pozhar, M. Anufriev, A. Trushechkin, R. Yunusov, Quantum-secured blockchain, Quantum, Science & Technology 3 (3) (2018) 035004, https://doi.org/10.1088/2058-9565/aabc6b.
34. F. Ablayev, D. Bulychkov, D. Sapaev, A. Vasiliev, M. Ziatdinov, Quantum-assisted blockchain, Lobachevskii Journal of Mathematics 39 (7) (2018) 957– 960, https://doi.org/10.1134/S1995080218070028.
35. A. El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, J. Peng, Quantum-inspired blockchain-based cybersecurity: Securing smart edge utilities in iotbased smart cities, Information Processing & Management 58 (4) (2021) 102549, https://doi.org/10.1016/j.ipm.2021.102549.
36. A. Coladangelo, O. Sattath, A quantum money solution to the blockchain scalability problem, Quantum 4 (2020) 297–340, https://doi.org/10.22331/q-2020-07-16-297.
37. T. Stafford, H. Treiblmaier, Characteristics of a blockchain ecosystem for secure and sharable electronic medical records, IEEE Transactions on Engineering Management 67 (4) (2020) 1340–1362, https://doi.org/10.1109/TEM.2020.2973095.
38. S. Krishnan, M. Manoj, T. Gadekallu, N. Kumar, P. Maddikunta, S. Bhattacharya, D. Suh, M. Piran, A blockchain-based credibility scoring framework for electronic medical records (2020) 1–6doi:10.1109/GCWkshps50303.2020.9367459.
39. Yuan B, Wu F, Zheng Z. Post quantum blockchain architecture for internet of things over NTRU lattice. PLoS One. 2023 Feb 1;18(2):e0279429. doi: 10.1371/journal.pone.0279429. PMID: 36724147; PMCID: PMC9891535.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 February 2024

doi:10.20944/preprints202402.0529.v1

40. Fedorov, A. K. (2023). Deploying hybrid quantum-secured infrastructure for applications: When quantum and post-quantum can work together. Frontiers in Quantum Science and Technology, 2, 1164428. https://doi.org/10.3389/frqst.2023.1164428
41. Allende M, León DL, Cerón S, et al. Quantum-resistance in blockchain networks. Scientific Reports. 2023 Apr;13(1):5664. DOI: 10.1038/s41598-023-32701-6. PMID: 37024656; PMCID: PMC10079930

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.