Demonstration of quantum blockchain using theta protocol and different attacks on IBM QX

Preprint · April 2020

DOI: 10.13140/RG.2.2.24224.53761

Adrij Banik
Central University of Jharkhand
2 PUBLICATIONS **1** CITATION
SEE PROFILE

Khyati Supriya
Central University of Jharkhand
2 PUBLICATIONS **1** CITATION
SEE PROFILE

Hussein El Ghor
Lebanese University
34 PUBLICATIONS **120** CITATIONS
SEE PROFILE

Bikash K. Behera
Bikash's Quantum (OPC) Pvt. Ltd.
163 PUBLICATIONS **960** CITATIONS
SEE PROFILE

Demonstration of quantum blockchain using theta protocol and different attacks on IBM QX

Adrij Banik,[1, *] Khyati Supriya,[1, †] Hussein El GHOR,[2, ‡] Bikash K. Behera,[3, 4, §] and Prasanta K. Panigrahi[4, ¶]

[1] *Department of Physics, Central University of Jharkhand, Ranchi 835206, India*
[2] *Laboratory of Embedded and Networked Systems,*
Faculty of Technology, Lebanese University, B. P. 813, Saida, Lebanon
[3] *Bikash's Quantum (OPC) Pvt. Ltd., Balindi, Mohanpur 741246, West Bengal, India*
[4] *Department of Physical Sciences,*
Indian Institute of Science Education and Research Kolkata, Mohanpur 741246, West Bengal, India

Quantum blockchain, based on quantum computation and quantum information, and being a decentralized, encrypted and distributed database, provides utmost security. Here, we experimentally demonstrate a quantum circuit on the IBM quantum experience platform for a quantum blockchain by using a θ-protocol. The blockchains are encoded into a 3-qubit GHZ state and then CNOT and CZ attacks are performed in the experimental circuits and simulated illustrating an eavesdropping attack to steal the information. We also explicate the successful detection of eavesdropping action in the protocol. Our research helps to defend the security of quantum blockchain, which is more practical under the present technical conditions. We believe that the quantum blockchain using θ-protocol is very significant for other blockchain applications in the near future.

I. INTRODUCTION

Entanglement is the most unusual and fascinating phenomena of quantum mechanics [1–4] where the properties of two or more quantum systems can become correlated even after being spatially separated, which leads to the famous phrases given by Einstein "the spooky action at a distance" [1, 2, 5].

The entanglement itself becomes the basis of all quantum information theoretical models. Quantum networking and cryptography [6–8] is one of them. Quantum cryptography can be explained as a technique of key distribution [9–11] that depends upon the laws of quantum mechanics to generate a key. In general, cryptography is the problem of performing communication or computation including two or more parties who may not trust one another. The cryptography relies on the two major and unchanging blocks of quantum mechanics, the Heisenberg's uncertainty principle [12] and the principle of photon polarisation. The uncertainty principle states that no quantum states of a system can be measured simultaneously without disturbing the system.

Secondly, the photon polarisation principle expresses how light photons can be oriented or polarized in a particular direction. An important problem where cryptography is used is in the case of transmission of some secret message. Thus, for this type of problem, we need an electronic system that is based on cryptographic proof instead of some third parties.

The blockchain [13–16] is a sort of classical database that consists of data of the past, such as the history of economic transactions. It is a digital security system in this modern world. The idea of a blockchain (classical) was first given by a person (or group of people) named Nakamoto [17] in the year 2008. Further, keeping the idea of the classical blockchain in the year 2019 Rajan and Vieser first proposed a conceptual design of a quantum blockchain using entanglement in time [5].

The uniqueness of a blockchain is in its design which makes it very difficult to tamper [18]. In this century, quantum computing, the rising star will question the reliability of classical blockchain, as a quantum computer can easily hack the classical blockchain system [19, 20]. Since modern problems require an efficient solution, the most desirable solution is to develop quantum blockchain. Having the characteristics of decentralization, openness, and information storage the blockchain, which cannot be tampered easily, has a large range of applications in digital currency such as bitcoin, intelligence, information security agencies, and many more.

Previously, some works have been done on the quantum blockchain [5, 21] by using different protocols [22–24]. In this article, we outline how θ-protocol [25] is used to design a quantum blockchain in the IBM quantum computer. θ-protocol is more sensitive in detecting cheating. Also, we discussed the possible types of attacks [22, 27] on quantum blockchain such as CNOT attack, and CZ attack.

The rest of the paper is organized as follows. Sec. II describes the working of theta protocol. Sec. III introduces different types of attacks, such as CNOT and CZ attacks on a quantum blockchain. Finally, we conclude in Sec. IV discussing the future directions of the work.

[*] adrijbanik.007@gmail.com
[†] khyatisup27@gmail.com
[‡] hussein.elghor@ul.edu.lb
[§] bikash@bikashsquantum.com
[¶] pprasanta@iiserkol.ac.in

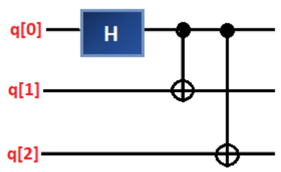

FIG. 1: The figure shows the constructed 3-qubit GHZ state with the quantum gates using Hadamard and controlled-NOT gates

II. DEVELOPING A QUANTUM BLOCKCHAIN USING THETA PROTOCOL

A. Preparation of GHZ state.

Greenberger-Horne-Zeilinger (GHZ) [28, 29] is a particular type of entangled quantum state which involves at least three subsystems (qubits). Three-qubit GHZ state is constructed by implementing a Hadamard gate and two CNOT gates as shown in Fig. 1.
Hadamard gate on 1^{st} qubit gives

$$\frac{|000\rangle + |100\rangle}{\sqrt{2}} \tag{1}$$

Now, applying two CNOT gates, one having control on 1^{st} qubit and target on 2^{nd} qubit and second having control on 1^{st} qubit and target on 3^{rd} qubit gives,

$$\frac{|000\rangle + |111\rangle}{\sqrt{2}} \tag{2}$$

And, this is the GHZ state for three qubit system.

B. The Theta Protocol

We consider a verification protocol [25] where,

- The source shares a n-qubit state ρ with n parties, where each party gets a qubit. Here, the shared state ρ is a GHZ state.
- Among these n parties, one will be called as Verifier. The Verifier will verify how close the shared GHZ state is to the ideal and whether it contains Genuine Multi-partite Entanglement (GME) [25, 26] or not.
- First, the Verifier will generate random angles θ_j for all parties including itself, such that $\sum_j \theta_j$ is a multiple of π. Then the angles will be sent to all the n parties.
- When the party j receives a random angle from the Verifier, it will measure in the basis, $\{|\theta_j\rangle, |\theta_-j\rangle\} = \{\frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta_j}|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - e^{i\theta_j}|1\rangle)\}$ and return the outcome Y_j.
- The Verifier will check whether it pass the following condition or not. $\oplus_j Y_j = \frac{1}{\pi}\sum_j \theta_j$

C. Circuit realization for quantum blockchain using theta protocol

Using the IBM Quantum Experience, we developed quantum circuits satisfying the above discussed θ protocol and simulate them to get a set of results. We implement the theory with the help of conventional quantum gates [1–3, 30] readily available in the IBM QE platform. Here, a 3-qubit GHZ state is being shared by a source to three parties say A, B, and C where B is the verifier. Now, B as a verifier will generate random angles using Hadamard gate and U_1 gate provided that $\theta \in [0, \pi)$ and $\sum_j \theta_j$= nπ. Here, we have considered θ to be θ_1 = 0, θ_2 = $\frac{\pi}{2}$, and θ_3 = $\frac{\pi}{2}$. So, verifier B generates an angle θ_1 = 0 using Hadamard gate and $U_1(\theta_1)$ gate and sends it to A using swap gate. Again, B will generate an angle θ_2 = $\frac{\pi}{2}$ using Hadamard gate and $U_1(\theta_2)$ gate and send it to c using swap gate. And then will generate angle θ_3 = $\frac{\pi}{2}$ using Hadamard gate and $U_1(\theta_3)$ gate and keep it to himself as shown in Figs. 2 and 3.
This is how the Theta-Protocol is used in a blockchain as it forms a chain interconnected to each other.

III. DIFFERENT TYPES OF ATTACKS ON QUANTUM BLOCKCHAIN

A. CNOT ATTACK

One of the most fundamental attacks in the field of quantum cryptography is called the CNOT attack [22, 32] that uses CNOT gate. Here, in our case, we show how the attacker will attack the shared qubits by keeping the control with its qubit and the target on the qubit the attacker wants to attack.
By measuring the qubits in Z-basis, the attacker will get the result.

1. *Circuit Realisation*

Here in the Fig., it has been clearly shown that a GHZ state is shared with A, B and C. Where the first qubit is with A, the second qubit is with B and the third qubit is with C. Let the 6^{th} qubit (i.e q[5]) belongs to the attacker as shown in Figs. 4 and 5. Suppose the attacker here performs a CNOT attack on the circuit, the explanation for the attacking action is explained in the next section. Here, the two ancilla qubits 3rd and 4th are used for the detection of the attack. Where the combination of 4 CNOT gates in a certain pattern is used for the detection circuit of the NOT attack. Now to know whether the circuit is attacked or not we measure both the ancilla qubits.

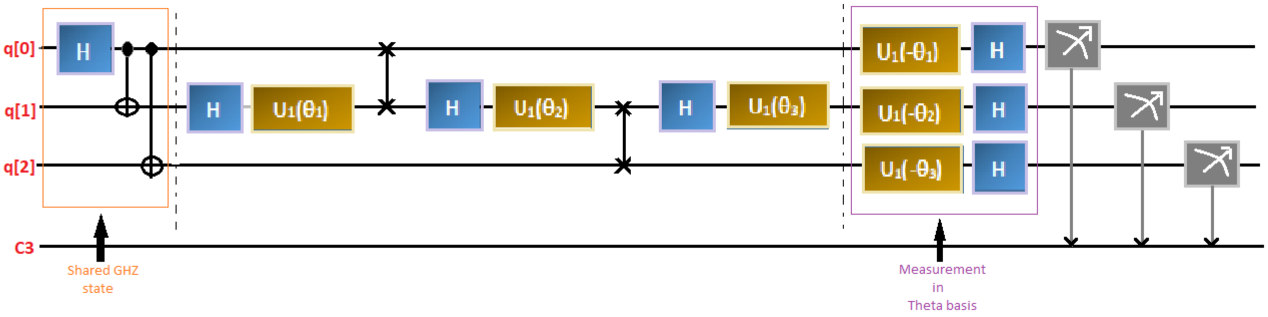

FIG. 2: the figure shows the Block diagram of circuit for quantum blockchain using theta protocol. In our original circuit we considered θ_1=0, θ_2=$\frac{\pi}{2}$ and θ_3=$\frac{\pi}{2}$ that satisfy the condition $\sum_j \theta_j$=$n\pi$ and the measurement is taken on θ basis.

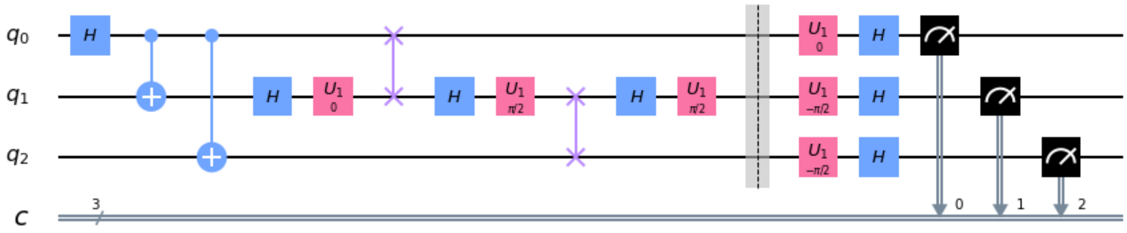

FIG. 3: The figure shows the constructed circuit as per the block diagram of quantum blockchain using theta protocol. The circuit is constructed on IBM QE platform. Here, the gates $U_1(0)$, $U_1(\frac{\pi}{2})$, $U_1(\frac{\pi}{2})$ shows the consideration of angle i.e., θ_1=0, θ_2 = $\frac{\pi}{2}$ and θ_3 = $\frac{\pi}{2}$ which further satisfy the condition $\sum_j \theta_j = n\pi$

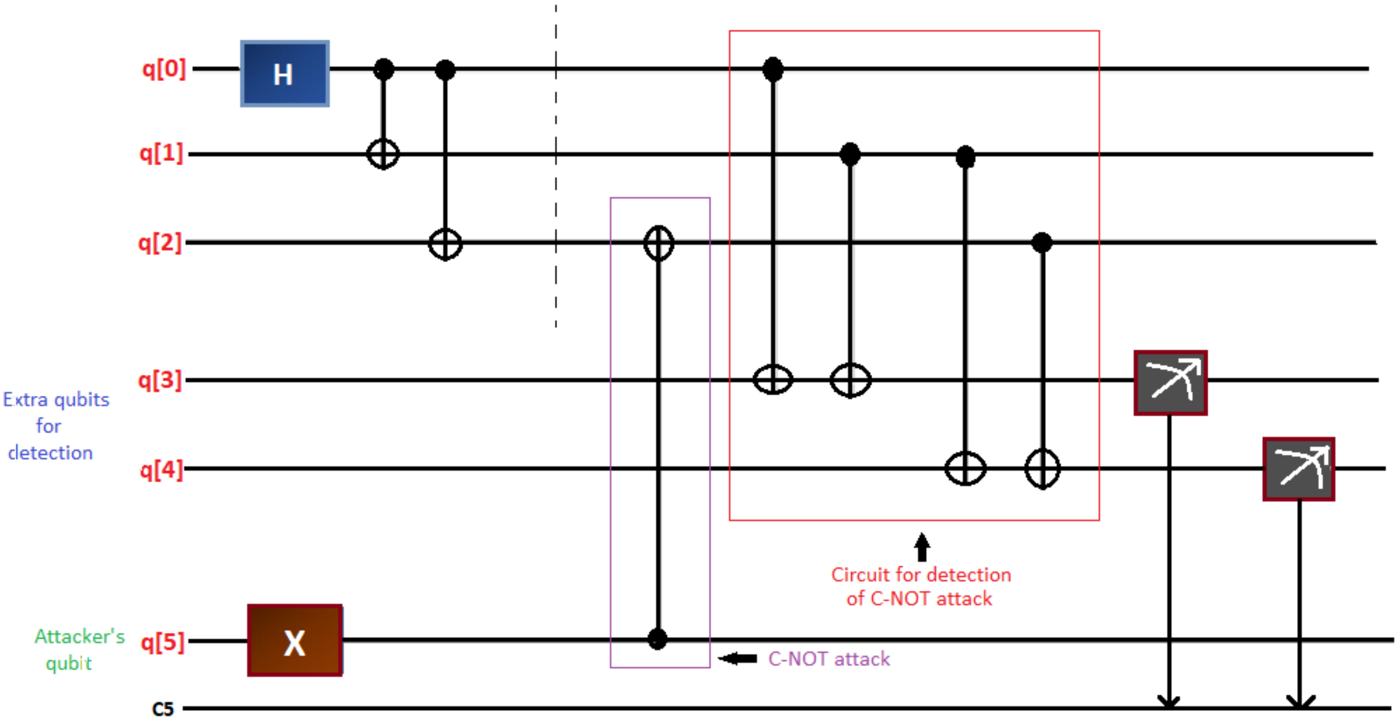
q[0]
q[1]
q[2]
q[3]
q[4]
q[5]
C5
H
X
Extra qubits for detection
Attacker's qubit
Circuit for detection of C-NOT attack
C-NOT attack

FIG. 4: The figure shows the block diagram of CNOT attack where q[5] qubit belongs to the attacker who can perform a CNOT operation on any of the shared qubits and q[3], q[4] qubits are used for the detection of the attack. Measurement is taken in Z- basis.

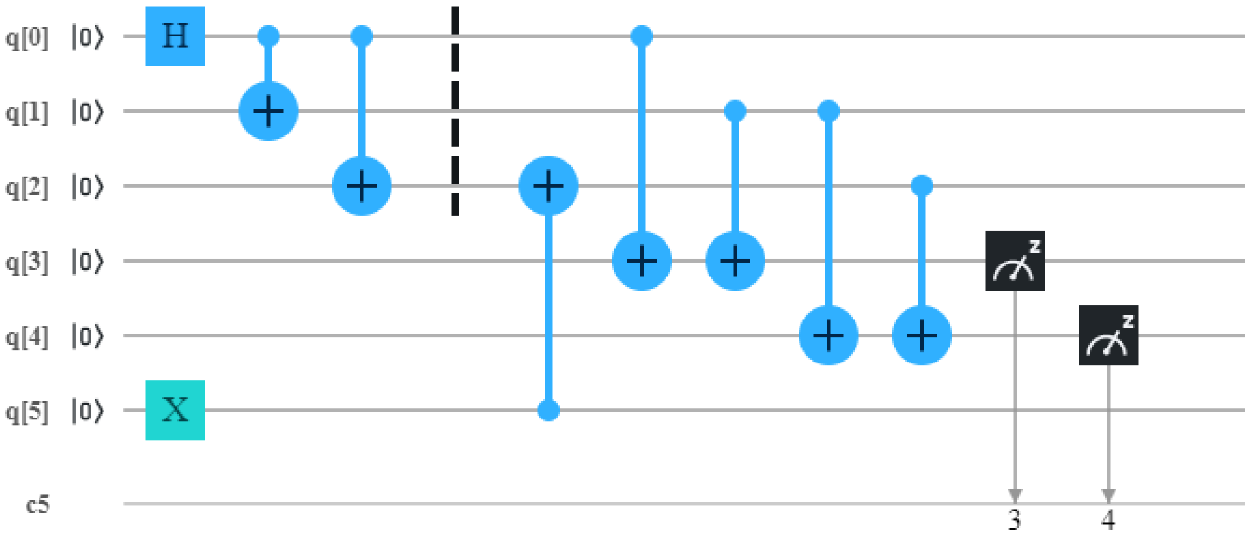

FIG. 5: The figure shows the constructed circuit as per the block diagram of CNOT attack on quantum blockchain. The circuit is constructed on IBM QE platform.

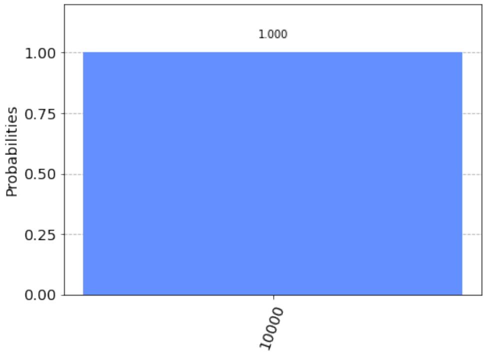

FIG. 6: Plot shows that when attacker performs a CNOT attack on the C's qubit then measurement of 4^{th} and 5^{th} qubits gives $|0\rangle \otimes |1\rangle$.

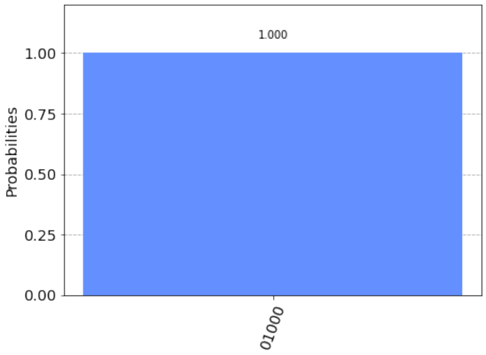

FIG. 7: Plot shows that when attacker performs a CNOT attack on the A's qubit then measurement of 4^{th} and 5^{th} qubits gives $|1\rangle \otimes |0\rangle$.

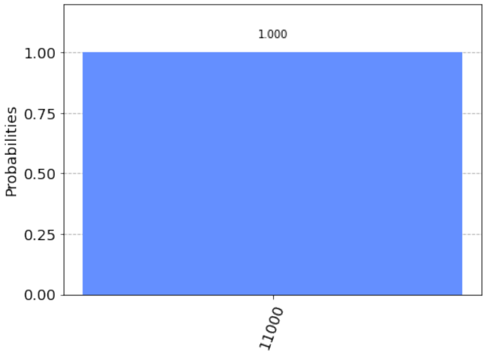

FIG. 8: Plot shows that when the attacker performs a CNOT attack on the B's qubit then measurement of 4^{th} and 5^{th} qubits gives $|1\rangle \otimes |1\rangle$.

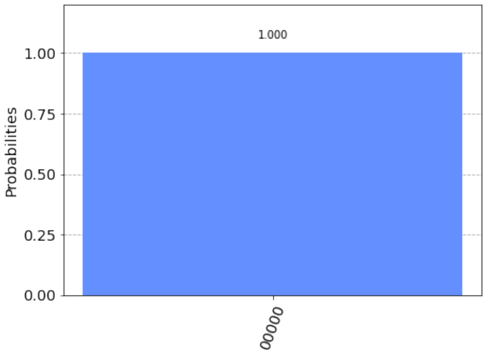

FIG. 9: Plot shows that when there is no CNOT attack on any of the qubit then measurement of 4^{th} and 5^{th} qubits gives $|0\rangle \otimes |0\rangle$.

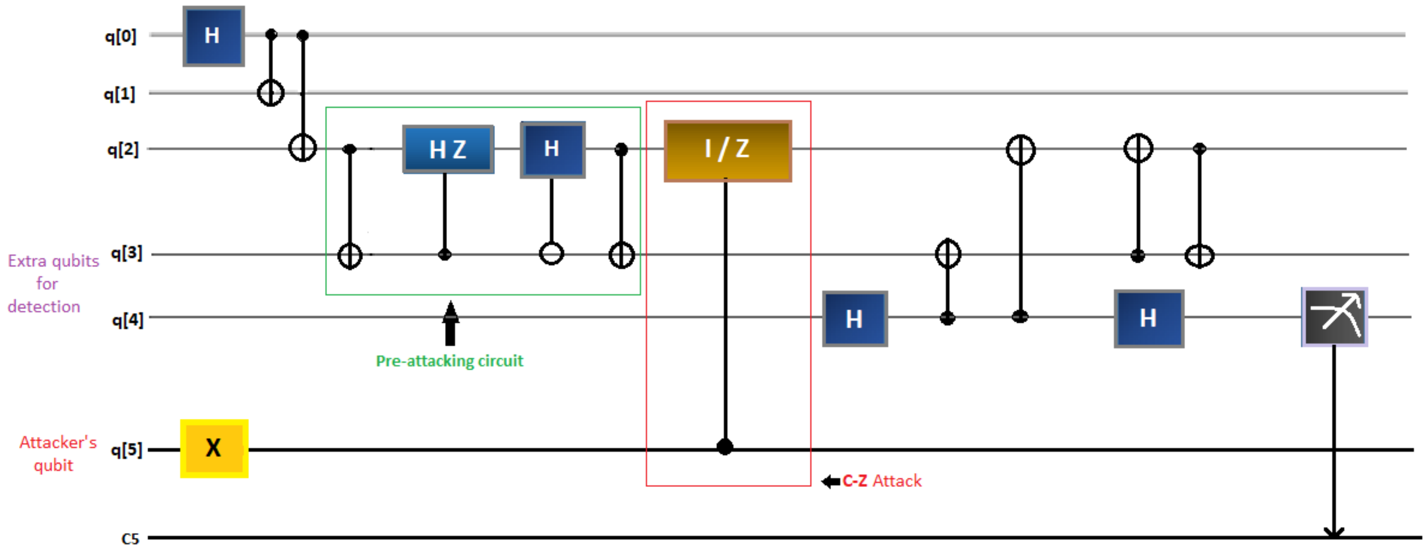

FIG. 10: The figure shows the block diagram of CZ attack where q[5] qubit belongs to the attacker who can perform a CZ operation on any of the shared qubits and q[3] qubit is used for the detection of the attack. Measurement is taken in Z-basis. Here the green marked box shows the pre-attacking circuit and the red marked box shows the operation of the attacker.

2. *Attacking action*

A GHZ state is shared with A, B, C which is shown in Fig. 4. Considering an attacker performs a CNOT attack in any of the three qubits, A, B, and C can detect whether there is a CNOT or not using following method as shown in the Fig. 4.

CASE-I:- If A's qubit got attacked.
GHZ state is shared within three qubits which are with A, B and C and there is no operation in the extra qubits.

$$\frac{|000\rangle + |111\rangle}{\sqrt{2}} \otimes |00\rangle = \frac{|00000\rangle + |11100\rangle}{\sqrt{2}} \qquad (3)$$

An Attacker performs NOT operation in the first qubit which belongs to A.

$$\frac{|10000\rangle + |01100\rangle}{\sqrt{2}} \qquad (4)$$

Here, we apply four CNOT gates, first having control on 1^{st} qubit and target on 4^{th} qubit, second having control on 2^{nd} qubit and target on 4^{th} qubit, third having control on 2^{nd} qubit and target on 5^{th} qubit and fourth having control on 3^{rd} qubit and target on 5^{th} qubit, the state becomes

$$\frac{|10010\rangle + |01110\rangle}{\sqrt{2}} \qquad (5)$$

CASE-II:- If B's qubit got attacked.
Same as the previous case, GHZ state is being shared with A, B and C and there is no operation in the extra qubits.

$$\frac{|000\rangle + |111\rangle}{\sqrt{2}} \otimes |00\rangle = \frac{|00000\rangle + |11100\rangle}{\sqrt{2}} \qquad (6)$$

In this case, the attacker performs NOT operation on the second qubit which belongs to B.

$$\frac{|01000\rangle + |10100\rangle}{\sqrt{2}} \qquad (7)$$

Here, we apply four CNOT gates, first having control on 1^{st} qubit and target on 4^{th} qubit, second having control on 2^{nd} qubit and target on 4^{th} qubit, third having control on 2^{nd} qubit and target on 5^{th} qubit and fourth having control on 3^{rd} qubit and target on 5^{th} qubit, the state becomes,

$$\frac{|01011\rangle + |10111\rangle}{\sqrt{2}} \qquad (8)$$

CASE-III:- If C's qubit got attacked.
Similar to case-I and case-II, GHZ state is being shared with A,B and C and there is no operation on the extra qubits.

$$\frac{|000\rangle + |111\rangle}{\sqrt{2}} \otimes |00\rangle = \frac{|00000\rangle + |11100\rangle}{\sqrt{2}} \qquad (9)$$

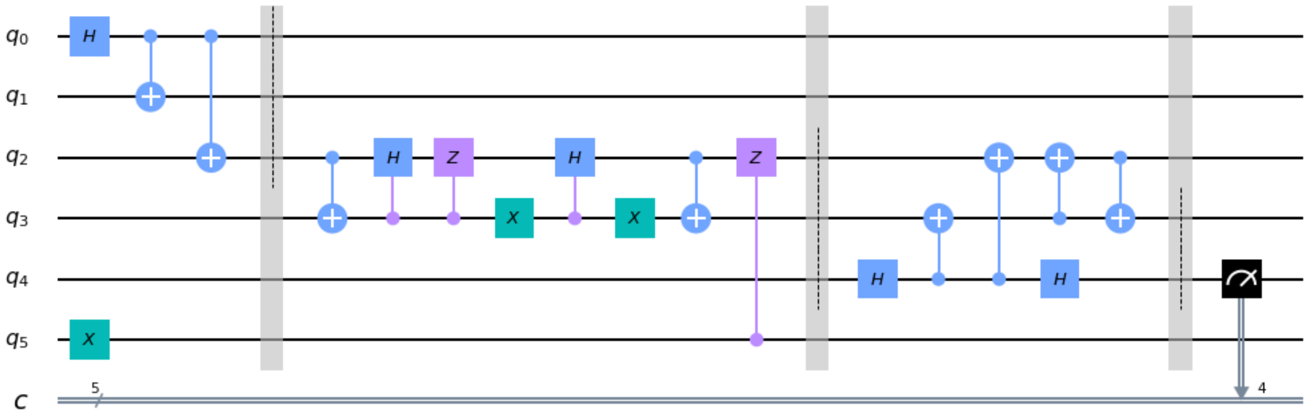

FIG. 11: The figure shows the constructed circuit as per the block diagram of CZ attack on quantum blockchain. The circuit is constructed on IBM QE platform.

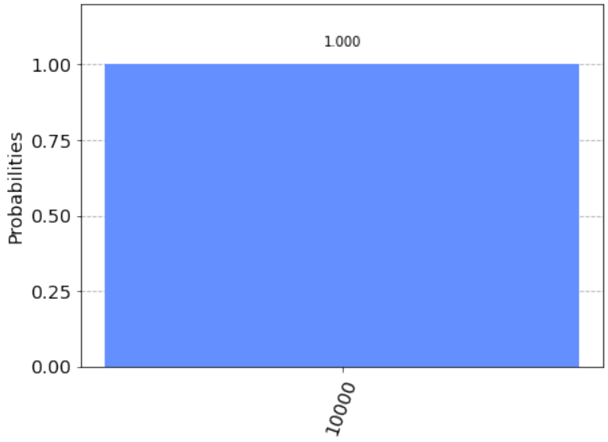

FIG. 12: Plot shows if the attacker performs a CZ attack on the 3^{rd} qubit then the measurement of 5^{th} qubit gives $|1\rangle$.

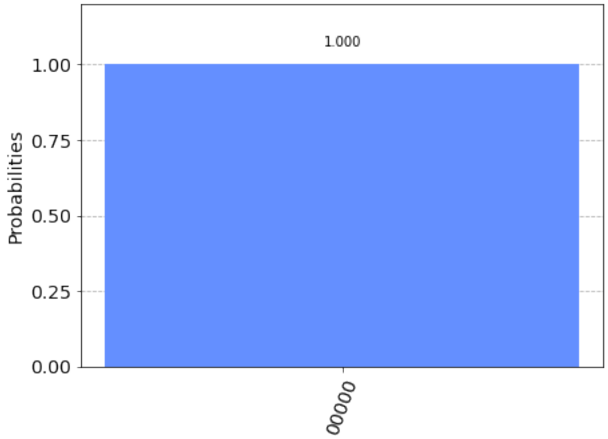

FIG. 13: Plot shows that if there is no CZ attack then the measurement of 5^{th} qubit gives $|0\rangle$

Now here, the attacker performs NOT operation on the third qubit which belongs to C. Same as previous when A,B,C applies a circuit for detection they would get,

$$\frac{|00100\rangle + |11000\rangle}{\sqrt{2}} \tag{10}$$

Here, we apply four CNOT gates, first having control on 1^{st} qubit and target on 4^{th} qubit, second having control on 2^{nd} qubit and target on 4^{th} qubit, third having control on 2^{nd} qubit and target on 5^{th} qubit and fourth having control on 3^{rd} qubit and target on 5^{th} qubit, the state becomes,

$$\frac{|00101\rangle + |11001\rangle}{\sqrt{2}} \tag{11}$$

CASE-IV:- If there is no attack on any of the three qubits

Similar to case-I and case-II and case-III, GHZ state is being shared with A, B and C and there is no operation on the extra qubits.

$$\frac{|000\rangle + |111\rangle}{\sqrt{2}} \otimes |00\rangle = \frac{|00000\rangle + |11100\rangle}{\sqrt{2}} \tag{12}$$

Since, there is no attack in any of the qubits the state will remain same.

Here, we apply four CNOT gates, first having control on 1^{st} qubit and target on 4^{th} qubit, second having control on 2^{nd} qubit and target on 4^{th} qubit, third having control on 2^{nd} qubit and target on 5^{th} qubit and fourth having control on 3^{rd} qubit and target on 5^{th} qubit, the state becomes

$$\frac{|00000\rangle + |11100\rangle}{\sqrt{2}} \tag{13}$$

3. *Results*

The theoretical results which we get on measuring both the ancilla qubits in order to detect the attack are as follows:

- $|1\rangle \otimes |0\rangle$ the attacker performs a CNOT attack on A's qubit, shown in Fig. 6.
- $|1\rangle \otimes |1\rangle$ the attacker performs a CNOT attack on B's qubit, shown in Fig. 7.
- $|0\rangle \otimes |1\rangle$ the attacker performs a CNOT attack on C's qubit, shown in Fig. 8.
- $|0\rangle \otimes |0\rangle$ there is no attack on the circuit, shown in Fig. 9.

We further satisfy the theoretical result with the experimented or simulated outcomes.

B. CZ ATTACK

Another type of attack that we introduce in the present paper is the CZ attack [22, 31] which uses a controlled-Z gate. When the attacker implements a controlled-Z attack in any of the shared qubits of A, B, and C by keeping the control with itself and the target (Z-gate) to the qubit which the attacker wants to attack and measuring the attacker's qubit gives the result as:

1. *Circuit realization*

As similar to the CNOT attack, in case of the CZ attack, the circuit is designed accordingly. Here a pre-attacking circuit by using the first ancilla qubit is introduced which is an arrangement of CNOT, CH, and CZ gates after the GHZ state is shared with A, B, and C as shown in Fig. 10. Here, we considered that the 6^{th} qubit belongs to the attacker who performs the CZ attack on the circuit by keeping the control with itself and the target (i.e. Z gate) to the qubit it wants to attack. Now, using the other ancilla qubit (i.e. q[4]) an attack checking circuit is designed and implemented here. These both pre attacking and attack checking circuits are used for detection of CZ attack. The more description of the attacking action is discussed in the next section.

2. *Attacking action*

As, GHZ state is shared with A, B, C. Considering attacker performs CZ attack in any of the three qubits, A, B, C can detect whether there is a CZ attack or not using following method as shown in Fig. 11

CASE-I:- If C's qubit got attacked.

GHZ state is shared with A, B, C and there is no operation in the extra qubits.

$$\frac{|000\rangle + |111\rangle}{\sqrt{2}} \otimes |00\rangle = \frac{|00000\rangle + |11100\rangle}{\sqrt{2}} \tag{14}$$

Applying CNOT gate having control on 3^{rd} qubit and target on 4^{th} qubit, controlled Hadamard gate having control on 4^{th} qubit and target on 3^{rd} qubit, CZ gate having control on 4^{th} qubit and target on 3^{rd} qubit, anti-controlled Hadamard gate having control on 4^{th} qubit and target on 3^{rd} qubit, CNOT gate having control on 3^{rd} qubit and target on 4^{th} qubit, the state becomes,

$$\frac{|00000\rangle + |00110\rangle + |11010\rangle + |11100\rangle}{2} \tag{15}$$

If the attacker applies Z gate on the third qubit

$$\frac{|00000\rangle - |00110\rangle + |11010\rangle - |11100\rangle}{2} \tag{16}$$

Applying Hadamard gate on fifth qubit, three CNOT gates, one having control on 5^{th} qubit and target on 4^{th} qubit and second having control on 5^{th} qubit and target on 3^{rd} qubit and third having control on 4^{th} qubit and target on 3^{rd} qubit, finally applying Hadamard gate on the fifth qubit we will get,

$$\frac{|000\rangle + |111\rangle \otimes (|-\rangle\,|1\rangle}{2\sqrt{2}} \tag{17}$$

Similarly, we can check the attacks for another two qubits, by putting the gates which were on the C's qubit to the qubits with A and B.

CASE-II:- If C's qubit got attacked.

GHZ state is shared with A, B, C and there is no operation in the extra qubits.

$$\frac{|000\rangle + |111\rangle}{\sqrt{2}} \otimes |00\rangle = \frac{|00000\rangle + |11100\rangle}{\sqrt{2}} \tag{18}$$

Applying CNOT gate having control on 3^{rd} qubit and target on 4^{th} qubit, controlled Hadamard gate having control on 4^{th} qubit and target on 3^{rd} qubit, CZ gate having control on 4^{th} qubit and target on 3^{rd} qubit, anti-controlled Hadamard gate having control on 4^{th} qubit and target on 3^{rd} qubit, CNOT gate having control on 3^{rd} qubit and target on 4^{th} qubit, the state becomes,

$$\frac{|00000\rangle + |11110\rangle}{\sqrt{2}} \tag{19}$$

If there is no attack, the further equation will remain same

Applying Hadamard gate on fifth qubit, three CNOT gates, one having control on 5^{th} qubit and target on 4^{th} qubit and second having control on 5^{th} qubit and target on 3^{rd} qubit and third having control on 4^{th} qubit and target on 3^{rd} qubit, finally, applying Hadamard gate on the fifth qubit we will get,

$$\frac{|000\rangle + |111\rangle \otimes (|+\rangle\,|0\rangle}{2\sqrt{2}} \tag{20}$$

3. *Result*

The theoretical results which we get on measuring both the ancilla qubits in order to detect the attack are as follows:

- $|1\rangle$ the attacker performs a CZ attack on A's, B's or C's qubit, shown in Fig. 12.
- $|0\rangle$ there is no attack on the circuit, shown in Fig. 13.

We further satisfy the theoretical result with the experimented or simulated outcomes.

IV. CONCLUSION

To conclude, we have constructed here a conceptual design of quantum blockchain using a 4-qubits system. Here, we focused to implement the blockchain using θ protocol that uses a shared entangled GHZ state. We have also constructed the circuits for CNOT and CZ attacks which is used for eavesdropping on the blockchain. The result after simulating over IBM quantum experience considerably proves the theoretically predicted results. We have proposed a strategy to visualize quantum blockchain which on further investigation can be implemented in quantum information processing in the near future.

ACKNOWLEDGEMENTS

A. B. and K. S. would like to acknowledge the hospitality of Bikash's Quantum (OPC) Pvt. Ltd. and IISER Kolkata during the project work. The authors thank Priyanka Dalei (Bikash's Quantum) for her contribution to the editing of the manuscript. B.K.B. acknowledges the prestigious Prime Minister's Research Fellowship awarded by DST, Govt. India. The authors would like to acknowledge QuEST initiative to DST/ICPS/QUST/THEME-1/2019 for the grant support. We acknowledge the support of IBM Quantum Experience for using the quantum processors. The views expressed are those of the authors and do not reflect the official position of IBM or the IBM quantum experience team.

[1] D. McMahon, Quantum Computing Explained, Wiley (2007).

[2] M. A. Nielsen, and I. L. Chuang, Quantum Computation and Quantum Information; Cambridge University Press: Cambridge, UK, 2010.

[3] A. Pathak, Elements of Quantum Computation and Quantum Communication, CRC Press (2013).

[4] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865-942 (2009).

[5] D. Ranjan, and M. Visser, Quantum Blockchain using entanglement in time, Quantum Rep. **1**(1), 3-11 (2019).

[6] A. Broadbent, and C. Schaffner, Quantum Cryptography Beyond Quantum Key Distribution, Designs, Codes and Cryptography **78**, 351-382 (2015).

[7] S. Bhandari, A New Era of Cryptography : Quantum Cryptography, Int. J. Crypt. Inf. Security (IJCIS), **6**, 3/4, (2016).

[8] J. Aditya, and P. Shankar Rao, Quantum Cryptography, Stanford Computer Science

[9] K. Inoue, Quantum key distribution technologies, IEEE J. Selected Topics in Quantum Elect. **12**, 4 (2006).

[10] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, Quantum Inf. Comput. **5**, 325-360 (2004).

[11] P. W. Shor and J. Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, Phys. Rev. Lett. **85**, 441 (2000).

[12] P. Busch, T. Heinonen, and P. Laht, Heiserberg's Uncertainty Principle, Phys. Rep. **452**, 155-176 (2007).

[13] D. Yaga, P. Mell, N. Roby, and K. Scarfone, Blockchain Technology Overview, National Institute of Standards and Technology (2018).

[14] M. Crosby, Nachiappan, P. Pattanayak, S. Verma, V. Kalyanaraman, BlockChain Technology: Beyond Bitcoin, Appl. Innov. Rev. (2016).

[15] M. Edwards, A. Mashatan, and S. Ghose, A Review of Quantum and Hybrid Quantum/ Classical Blockchain Protocols, arXiv:1912.09280v1 [cs.CR] (2019).

[16] D. Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps, Apress (2017)

[17] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on: December 17, 2019)

[18] C. Li, Y. Xu, J. Tang, and W. Liu, Quantum Blockchain: A Decentralized, Encrypted and Distributed Database Based on Quantum Mechanics, J. Quantum Comput. **1**, 49-63 (2019).

[19] D. Aggarwal, G. K. Brennen, T. Lee, M. Santha, and M. Tomamichel, Quantum attacks on Bitcoin, and how to protect against them, Ledger, [S.l.], v. 3, oct. (2018).

[20] A. K. Fedorov, E. O. Kiktenko, and A. I. Lvovsky, Quantum computers put blockchain security at risk, Nature **563**, 465-467 (2018).

[21] E.O. Kiktenko, N.O. Pozhar, M.N. Anufriev, A.S. Trushechkin, R.R. Yunusov, Y.V. Kurochkin, A.I. Lvovsky, and A.K. Fedorov, Quantum-secured blockchain, Quantum Sci. Technol. **3**, 035004 (2018).

[22] Md. Hasnain, A. Giri, B. K. Behera and P. K. Panigrahi, Demonstration of quantum blockchain, and therein CNOT and ping-pong attacks on IBM QX, DOI: 10.13140/RG.2.2.15582.38725 (2020).

[23] S. Banerjee, A. Mukherjee, and P. K. Panigrahi, Quantum blockchain using weighted hypergraph states, Phys. Rev. Research **2**, 013322 (2020).

[24] X. Sun, Q. Wang, P. Kulicki and M. Sopek, A Simple Voting Protocol on Quantum Blockchain, Int. J. Theor. Phys. **58**, 275-281 (2019).

[25] W. McCutcheon, A. Pappa, B. A. Bell, A. McMillan, A. Chailloux, T. Lawson, M. Mafu, D. Markham, E. Diamanti, I. Kerenidis, J.G. Rarity, and M.S. Tame, Experimental verification of multipartite entanglement in quantum networks, Nat. Commun. **7**, 13251 (2016).

[26] Yi Shen, Lin Chen, Construction of genuine multipartite entangled states, Journal of Physics A, **53**, (2020).

[27] T. M. Fernandez-Carames, and P. Fraga-Lamas, Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks, IEEE Access **8**, 21091 - 21116 (2020).

[28] M. Neeley, R. C. Bialczak, M. Lenander, E. Lucero, M. Mariantoni, A. D. O'Connell, D. Sank, H. Wang, M. Weides, J. Wenner, Y. Yin, T. Yamamoto, A. N. Cleland and J. M. Martinis, Generation of Three-Qubit Entangled States using Superconducting Phase Qubits, Nature **467**, 570-573 (2010).

[29] Y.-F. Huang, B.-H. Liu, L. Peng, Y.-H. Li, L. Li, C.-F. Li and G.-C. Guo, Experimental generation of an eight-photon Greenberger-Horne-Zeilinger state, Nat. Commun. **2**, 546 (2011).

[30] D. P. DiVincenzo, Quantum Gates and Circuits, Proc. R. Soc. Lond. A. **454**, 1969 (1998).

[31] V. Singh, B. K. Behera, and P. K. Panigrahi, Developing a New Quantum Circuit for Hacking in Ping-Pong Protocol: An IBM Quantum Experience, DOI: 10.13140/RG.2.2.12475.77607 (2019).

[32] Arpita Maitra, Third Party CNOT Attack on MDI QKD, arXiv:1208.5223 [quant-ph] (2012).