Quantum blockchain using weighted hypergraph states

Shreya Banerjee,[1,*] Arghya Mukherjee,[2,†] and Prasanta K. Panigrahi[1,‡]
[1]*Department of Physical Sciences, Indian Institute of Science Education and Research Kolkata, Mohanpur-741246, West Bengal, India*
[2]*Department of Mathematical Sciences, Indian Institute of Science Education and Research Kolkata, Mohanpur-741246, West Bengal, India*

(Received 20 December 2019; accepted 24 February 2020; published 16 March 2020)

Using the multiparty entanglement of quantum weighted hypergraph states, we built a protocol to build a quantum blockchain. In this protocol, the information contained by the classical blocks is initialized at a single qubit that acts as a vertex of the corresponding hypergraph and the entanglement of the hypergraph state serves the purpose of the "chain." The security and effectiveness of the protocol are then outlined. We further provide a quantum circuit and implement it on IBM's five-qubit computer with single- and two-qubit quantum gates as components.

DOI: 10.1103/PhysRevResearch.2.013322

I. INTRODUCTION

A. Classical blockchain technology

The classical blockchain is the most popular distributed ledger technology (DLT) [1], used by the famous cryptocurrency network bitcoin [2]. The distributed ledger technology eliminates the necessity of a third party settling any transactions between two parties and keeps multiple records of one transaction. This makes a transaction impossible to alter once it is recorded and entered into the ledger. Blockchain is an example of this technology and many cryptocurrencies, e.g., bitcoin, etherium, litecoin, ripple, are based on the blockchain technology. This technology has found use in biomedical domains [3], preventing fake news in social media [4], as well as in public administration [5]. The blockchain technology aims to preserve and secure information in worldwide-distributed ledgers. It is essentially a trustless peer-to-peer network [2,6], where time-stamped information (transactions in case of a cryptocurrency) is drawn from a pool of transactions and encrypted in a block by one of the nodes of the network. This node is one of the few nodes ("miners" in case of bitcoin) which is selected by a process called "proof of work" [2]. The proof of work (PoW) algorithm is an NP hard problem that requires to guess a value (nonce) and solve a prescribed problem (generation of the cryptographic hash function) which generates the "hash" for a particular block [7]. Once a hash is successfully generated, as a security measure the block is also given the hash of the previous block. The peer that made the block transmits it to all the nodes in the network. For bitcoin there is a publicly available ledger [8]. The nodes accept the block after verifying it based on a mutually agreed upon consensus and acknowledge the block by applying its hash to the next block of the chain. The security of the classical blockchain thus lies on two major key points. The computation complexity of the proof of work (PoW) algorithm and addition of the previous hash function in the next block formation. The PoW, being an NP hard problem, takes a significant amount of computational power and time to solve for a potential hacker Eve [9]. The inclusion of the previous hash function makes the job of Eve more difficult. If Eve wants to change one transaction, she has to change the hash of the block in which that transaction is added (say, block m). Then, to cover her track, she has to change the hash of every block that is added to the chain after the mth block. Figure 1 provides a graphical flowchart to explain the classical blockchain workflow [10].

The recent advances of quantum computation [11] have severely threatened the security of classical blockchain [6,10,12]. As an example, we can consider the Grover's Search algorithm [13], which can provide a quadratic speedup in the PoW process. Thus, if Eve possesses a quantum computer, it gives her an unfair advantage over the miners. Several protocols have been proposed making use of quantum cryptographic and key distribution algorithms to defend the quantum attacks on classical blockchain in recent years [10,12,14]. The need to have a protocol for the blockchain technology using quantum tools is thus evident in recent times. Previously, using the temporal Greenberger-Horne-Zeilinger (GHZ) states a theoretical concept has been provided [6,15], where each block is made up of n qubits. In this work, we outline a protocol to make a quantum blockchain encoding information of each block in a single qubit using the multiparty entanglement of quantum weighted hypergraph states [16–18]. In this protocol, the information contained by the classical blocks is initialized at a single qubit that acts as a vertex of the corresponding hypergraph and the entanglement of the hypergraph state serves the purpose of the "chain." We briefly describe the hypergraph states and the weighted hypergraph states in the following subsection. The protocol is outlined in Sec. II.

*shreya93ban@gmail.com
†arghyabzs@gmail.com
‡pprasanta@iiserkol.ac.in

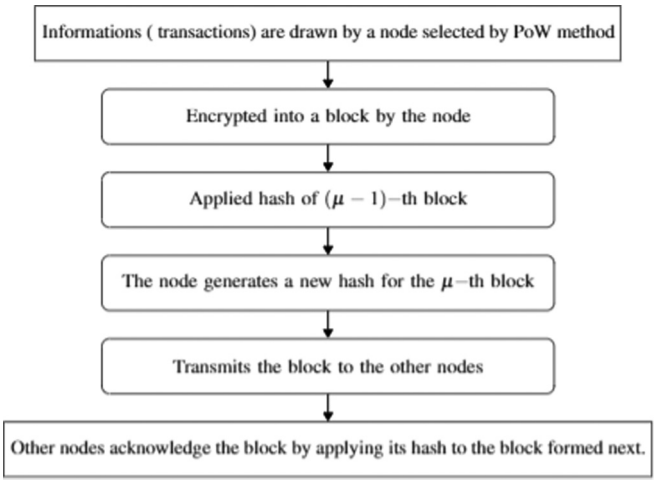

FIG. 1. Flowchart representing workflow of the formation of the classical blockchain.

Section III discusses the security and effectiveness of the protocol. A quantum circuit to prepare quantum blockchain explicated using IBM quantum experience with single- and two-qubit quantum gates as components is provided in Sec. IV along with fidelity analysis for a 2-blockchain prepared in "ibmqx2" quantum processor. We conclude in Sec. V with future directions.

B. Quantum hypergraph states and weighted hypergraph states

The quantum hypergraph states are a group of highly entangled multipartite quantum states that are constructed on the mathematical hypergraph [16]. The quantum states are localized on the vertices of the hypergraph, the edges of which show connections with the other qubits which together represent a nonseparable many-body quantum state. We use the entanglement of these states as a tool to replace the classical ledger and hash functions and propose a protocol to make a blockchain which is intrinsically quantum. Below, we present a brief description of a hypergraph state following [16]. Given a mathematical hypergraph with k hyperedge (i.e., a hyperedge connecting k qubits) and n vertices, a corresponding quantum state can be prepared [16]. The number of vertices of the hypergraph are equal to n, the number of qubits in the quantum system. All of the n qubits are initiated in the state $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$. A controlled-$Z$ operation is then performed for each k-hyperedge. Figure 2 represents a mathematical hypergraph with five vertices, 1, 2, 3, 4, and, 5, a 3-hyperedge connecting vertices 1, 2, and 3; and a 5-hyperedge connecting all five vertices. This hypergraph represents a quantum state that can be formed by using the circuit provided in Fig. 3.

From Figs. 2 and 3, it is evident that for each hyperedge, a controlled-Z operation has been performed on the connecting qubits. The output state of the circuit in Fig. 3 is the quantum state corresponding to the hypergraph in Fig. 2, and is given by

$$|\psi\rangle = C^2{}_{(1,2,3,4,5)} Z C^2{}_{(1,2,3)} Z\, |+\rangle^{\otimes 5}\,.$$

The entanglement of a hypergraph state has been discussed in [16,19,20] as well as many of its properties. As is well known, local unitary operations carried through classical communication (LOCC) does not alter the entanglement of the state under consideration. These LOCC equivalent classes need to be identified when considering the application of the states for applications of the state for quantum communications and cryptographical protocols. A singular LOCC equivalent class has been identified for a three-qubit hypergraph state and 27 LOCC equivalent classes have been found for four-qubit hypergraph states [19]. It has been also shown in [19] that using local applications of unitary Pauli operations on the kth qubit one can remove all the $(N-1)$ edges for the special case where an n-qubit hypergraph state contains only an n edge.

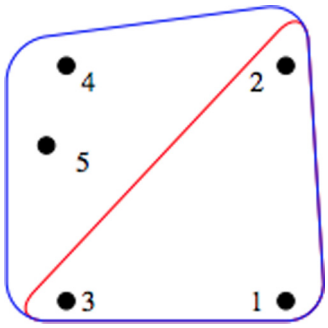

FIG. 2. A mathematical hypergraph with five vertices, a 3-hyperedge, and a 5-hyperedge.

An equivalence between the real equally weighted (REW) states and the hypergraph states was first drawn in [16]. In [18,21], the weighted hypergraph states were introduced as a locally maximally entanglable (LME) state. As described in [17,18], a weighted hypergraph state can be represented by a hypergraph where each hyperedge carries a weight [17], i.e.,

$$|\psi\rangle = \frac{1}{\sqrt{2^N}} \sum_{x\in(0,1)^N} e^{\iota\pi f(x)}\, |x\rangle\,.$$

Here, $|x\rangle$ represents the computational basis state and $f(x)$ corresponds to any real number. For hypergraph states described before, $f(x) \in \{0, 1\}$ [17].

II. PROTOCOL TO MAKE QUANTUM BLOCKCHAIN

We present our protocol to prepare a decentralized, quantum, and cost-effective blockchain. Our protocol replaces the classical ledger-based network and cryptographic hash

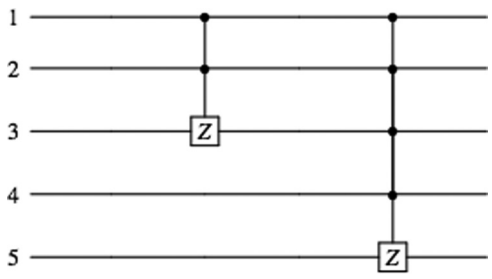

FIG. 3. Circuit to prepare quantum hypergraph state corresponding to the mathematical hypergraph as presented in Fig. 2. Each qubit in the circuit is initiated in the state $|+\rangle$.

functions with the entanglement of a weighted hypergraph state, where the creation of block remains analogous to that in the classical case. We use the "weights," i.e., the phases carried by the hyperedges of the weighted hypergraph states to encode the classical information in the hypergraph state. The protocol accommodates infinite number of quantum blocks added by trustless peers. The peers use only local operations and classical communications over a quantum secure channel (using any quantum key distribution protocol of their choice) to build the chain according to a mutually agreed upon consensus. In this section we first present the protocol and then discuss the security and effectiveness of the quantum blockchain formed.

(i) *Encoding the classical information of the blocks in qubits*. In the proposed quantum block chain, we consider each classical block to be represented by a binary string, which will have a decimal equivalent p. The peer that made the block first initiates his qubit at state $|\psi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, and introduces the p value in the relative phase of the system as

$$|\psi_1\rangle = S(p)\,|\psi\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0\\ 0 & e^{\iota\theta_p}\end{bmatrix}|\psi\rangle = \frac{|0\rangle + e^{\iota\theta_p}\,|1\rangle}{\sqrt{2}},$$

where $\theta_p \in (0, \frac{\pi}{2})$ is a function of p, $f(p)$, any bijective function chosen by and known to only the peer who creates the block, and $\sum_i \theta_{p_i} < \frac{\pi}{2}\ \forall\ i$. Here, i represents the number of the block added to the chain. Qubit $|\psi_1\rangle$ now carries the information of the classical block. Ensuring the conditions on θ_p is crucial in this protocol as these conditions ensure the entanglement of the state prepared. The peers can address this issue by using a mutually agreed upon consensus, which ensures that these conditions are met.

(ii) *Consensus.* The mutually agreed upon consensus between the peers is a very crucial part of this protocol. The consensus to be followed for the efficient work of this algorithm should be such that each $0 < \theta_{p_i} < \frac{\pi}{2}$ as well as $\sum_i \theta_{p_i} < \frac{\pi}{2}\ \forall\ i$. First, we provide an example of such a consensus.

According to this consensus, the peers agree to encode the classical information of the blocks they are forming in their qubit in a way so that the relative phase of the ith qubit, prepared by the ith peer, is given as

$$\theta_{p_i} = \frac{1}{2^{(i-1)}}\theta_{p_1},$$

where θ_{p_1} is the phase initiated by the first peer in his qubit.

We consider the infinite sum

$$\sum_{i=1}^{\infty}\theta_{p_i} = \sum_{i=1}^{\infty}\frac{1}{2^{i-1}}\theta_{p_1}.$$

The infinite series $\sum_{i=1}^{\infty}\frac{1}{2^{i-1}}$ is a geometric progression series of constant ratio $\frac{1}{2}$ and initial number θ_{p_1} that converges to $2\theta_{p_1}$. Thus, to ensure that $\sum_{i=1}^{\infty}\theta_{p_i} < \frac{\pi}{2}$, the phase θ_{p_1} initiated by the first peer in his qubit should be fixed at a value less than $\frac{\pi}{4}$.

One can formulate infinitely many such infinite series. We consider the infinite series

$$\sum_{i=1}^{\infty}\theta_{p_i} = \sum_{i=1}^{\infty}\frac{1}{n^{i-1}}\theta_{p_1},$$

where $n \in N/\{1\}$, and N is the set of all positive integers. The infinite series converges to $(\frac{n}{n-1})\theta_{p_1}$, and is upper bounded by $2\theta_{p_1}$. Thus, the peers can choose any such infinite series to build up their quantum ledger with an appropriate choice of θ_{p_1}.

The consensus provided here is an example. Any such consensus that ensures the conditions on the relative phase θ_{p_i} are met is agreeable with the protocol.

To address the question of trust amongst peers, a verification step is required to check if the phase encoded in each block is per the consensus. This step demands the first peer to openly broadcast θ_{p_1} to all other peers using the quantum secure channel established between them.

(iii) *Formation of the quantum blockchain.* The multiparty entanglement of the weighted hypergraph states is used to form the quantum blockchain, replacing the classical ledger database. The chain of n blocks is a quantum weighted hypergraph of n qubits having each qubit encoded with the information of a classical block as above. Once the classical information of a block is encoded in a qubit, the peer sends a copy of the state to all other peers in the network. Since (s)he exactly knows the state of the qubit, this does not violate the no-cloning theorem. Each of the peers verifies the qubit based on the consensus and adds it to their local copy of the chain making use of multiple controlled-Z gates, and thus forming an n-qubit weighted hypergraph. If a peer is going to add the nth block to the chain, (s)he uses $C^{(n-1)}Z$ gate to add it to the previously made $(n-1)$-blockchain, which effectively is a $(n-1)$-qubit weighted hypergraph state. The peers then remove the previous $(n-1)$ edge from the n-qubit hypergraph using a local Pauli-X gate on the nth qubit. The removal of the $(n-1)$ edge is not mandatory to form the quantum ledger, yet useful to enhance security of the protocol. Further discussions on the security of the protocol against potential attacks are provided in Sec. III.

(iv) *Verification of the blocks.* To check if the blocks are added according to the consensus, and maintain the entanglement of the weighted hypergraph state formed a step of verification of each block is needed prior adding them in the chain. According to the proposed consensus, (a) the peer who creates the first block openly broadcasts the relative phase θ_{p_1} initiated in his/her qubit, (b) the peers prepare their qubits by encoding the classical information of their blocks in the relative phase of their respective qubits following a geometric progression series of the form $(\frac{1}{n^{i-1}})\theta_{p_1}$, where $n \in N/\{1\}$, N being the set of all positive integers, and i is number of the block being added to the chain. The constant ratio of the geometric progression series $\frac{1}{n}$ is known to all the peers.

Effectively, the relative phase of each qubit is known to each peer building the chain. The peer who creates the mth block prepares his/her qubit as

$$|\psi_m\rangle = \frac{|0\rangle + e^{\iota\theta_{p_m}}\,|1\rangle}{\sqrt{2}},$$

where the relative phase should be $\theta_{p_m} = (\frac{1}{n^{m-1}})\theta_{p_1}$. (S)he sends one copy of the state to each peer in the system. The peers, upon receiving the qubit, measure it in a basis $|\pm_{\theta_m}\rangle = \frac{|0\rangle \pm e^{\iota\theta_{pm}}\,|1\rangle}{\sqrt{2}}$. If the measurement outcome is 1, then they add the state in their local copy using the $m-1$ controlled-Z gate.

FIG. 4. Circuit diagram for quantum blockchain with two blocks. Here, $R(\theta_p)$ represents the phase gate. The output is a weighted graph state with two qubits.

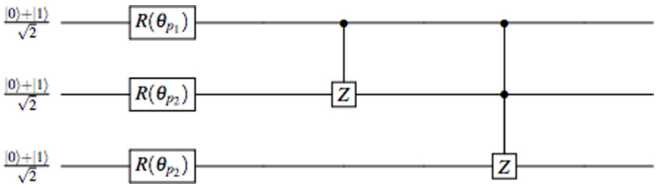

FIG. 5. Simplistic circuit diagram to prepare quantum blockchain with three blocks.

For any other measurement outcome, the protocol is aborted, and the peer is identified as untrustworthy. Inclusion of this verification step in the protocol ensures that the proposed quantum blockchain can be built by completely trustless peers. It also frees the protocol from the need of any "proof of work" or "proof of stake" to select the peers who can build the chain.

(v) *Example.* We provide the construction of a general n-blockchain as an example.

(a) In this example, we consider the blocks to be represented by decimal numbers p_1, p_2, p_3, ..., p_n. After encoding, the qubits representing the blocks are

$$|\psi_1\rangle = \frac{|0\rangle + e^{\iota\theta_{p_1}}|1\rangle}{\sqrt{2}}, \quad |\psi_2\rangle = \frac{|0\rangle + e^{\iota\theta_{p_2}}|1\rangle}{\sqrt{2}},$$
$$|\psi_3\rangle = \frac{|0\rangle + e^{\iota\theta_{p_3}}|1\rangle}{\sqrt{2}}, \ldots, \quad |\psi_n\rangle = \frac{|0\rangle + e^{\iota\theta_{p_n}}|1\rangle}{\sqrt{2}},$$

... up to infinity, where $\theta_{p_i} = (\frac{1}{n^{i-1}})\theta_{p_1}$; $n \in N/\{1\}$, N being the set of all positive integers, and i is number of the block being added to the chain.

(b) Peer 1 prepares the first qubit in state $|\psi_1\rangle$, broadcasts the value of θ_{p_1} as well as shares copies of his state with each peer in the network via a secure quantum channel for verification. As mentioned earlier, peer 1 exactly knows the state thus making multiple copies of it will not violate the no-cloning theorem.

(c) The other peers in the system measure the qubit in a basis $|\pm_{\theta_1}\rangle = \frac{|0\rangle \pm e^{\iota\theta_{p_1}}|1\rangle}{\sqrt{2}}$. If measurement outcome turns out to be 1, they prepare their own local qubit in the same state.

(d) The peer who adds the second block initiates his qubit in $|\psi_2\rangle$ and shares n copies of it to all the peers. Everyone upon verifying the authenticity of the qubit entangles it with the first qubit using controlled-Z gate, with the target on the second qubit as shown in Fig. 4. The blockchain with two blocks is given by

$$|\psi_{12}\rangle = C_{1,2}Z(|\psi_1\rangle \otimes |\psi_2\rangle)$$
$$= \tfrac{1}{2}(|00\rangle + e^{\iota\theta_{p_2}}|01\rangle + e^{\iota\theta_{p_1}}|10\rangle - e^{\iota(\theta_{p_1}+\theta_{p_2})}|11\rangle)$$

representing a two-qubit entangled weighted graph state.

(e) Peer 3 prepares his qubit at $|\psi_3\rangle$ and shares copies of it to everyone in the network. After the verification of the authenticity of the qubit, the qubit is then entangled with state prepared by peer 1 and peer 2 using a C^2Z gate, with two controls on qubits 1 and 2, and target on the third qubit. The simplistic circuit diagram is shown in Fig. 5.

The chain now can be represented as

$$C^2_{12,3}Z(|\psi_{12}\rangle \otimes |\psi_3\rangle)$$
$$= \frac{1}{2\sqrt{2}}(|000\rangle + e^{\iota\theta_{p_3}}|001\rangle$$
$$+ e^{\iota\theta_{p_2}}|010\rangle + e^{\iota(\theta_{p_2}+\theta_{p_3})}|011\rangle$$
$$+ e^{\iota\theta_{p_1}}|100\rangle + e^{\iota(\theta_{p_1}+\theta_{p_3})}|101\rangle$$
$$- e^{\iota(\theta_{p_1}+\theta_{p_2})}|110\rangle + e^{\iota(\theta_{p_1}+\theta_{p_2}+\theta_{p_3})}|111\rangle).$$

As one can see, $|\psi_{123}\rangle$ is a three-qubit entangled weighted hypergraph state that can be represented by the hypergraph in Fig. 6. To make this state more secure, the peers can operate unitary Pauli operations (in this case Pauli-X gate) locally on this qubit (qubit 3), thus making the state an entangled 3-edge hypergraph as depicted in Fig. 7. According to [19], the hypergraph in Fig. 6 and the hypergraph state in Fig. 7 are LOCC equivalent. The application of the Pauli-x gate on the third qubit thus does not affect the entanglement of the state, but the state of the system changes to

$$|\psi_{123}\rangle = X_3C^2_{12,3}Z(|\psi_{12}\rangle \otimes |\psi_3\rangle)$$
$$= \frac{1}{2\sqrt{2}}(e^{\iota\theta_{p_3}}|000\rangle + |001\rangle + e^{\iota(\theta_{p_2}+\theta_{p_3})}|010\rangle$$
$$+ e^{\iota\theta_{p_2}}|011\rangle + e^{\iota(\theta_{p_1}+\theta_{p_3})}|100\rangle + e^{\iota\theta_{p_1}}|101\rangle$$
$$+ e^{\iota(\theta_{p_1}+\theta_{p_2}+\theta_{p_3})}|110\rangle - e^{\iota(\theta_{p_1}+\theta_{p_2})}|111\rangle),$$

creating a single 3-edge three-qubit hypergraph.

(f) The blockchain after addition of the nth block can thus be represented as a weighted hypergraph with a single n edge; further blocks can be added to the chain following the protocol.

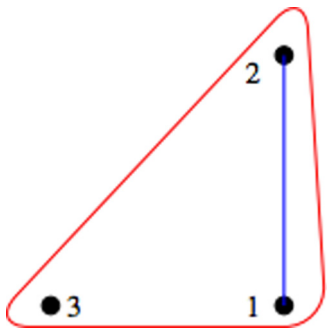

FIG. 6. The weighted hypergraph state that represents the quantum 3-blockchain.

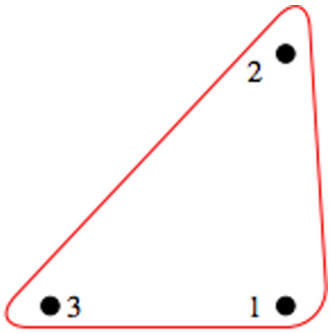

FIG. 7. The three-qubit weighted hypergraph state representing the quantum 3-blockchain after removal of the 2-edge by the local Pauli operations.

We provide a flowchart representing the protocol herewith (Fig. 8).

III. SECURITY AND EFFECTIVENESS OF THE QUANTUM BLOCKCHAIN

In our protocol, the entanglement of the weighted hypergraph state acts as the chain as well as ensures the security of the blockchain. It deals with the security of the blockchain only after a block is added to the chain by a peer. The authenticity of the blocks is checked by the verification step provided by in Sec. II, which also takes care of the untrustworthy peer scenario. If a block fails to meet the verification criterion, the corresponding peer who made the block is marked as untrustworthy. Below, we discuss the security of information after adding a block to the chain against potential attacks on the blockchain from the outside.

In the classical case, each block is assigned to two cryptographic hash functions, one belonging to the previous block and other designated to the current block. Thus, if an attacker Eve tampers with a particular block m in the chain, she will need to change the hash belonging to all subsequent blocks that has been added to the chain after block m. The probability of her catching up is significantly low if she uses a classical computer, although is high if she uses a quantum computer. In our protocol, the blockchain is represented by an entangled state, where the information is stored in the phases of the corresponding qubits and there are n copies of the same state shared amongst n peers. In our protocol, there is no publicly shared "hash function" or any shared ledger-based database; only the relative phase of the first qubit θ_{p_1} is shared amongst the peers with the help of a quantum secure channel established between them. Thus, if Eve wants to tamper one particular after it is added to the chain, she needs to perform a measurement on that particular qubit of the chain. The chain being a entangled state, any measurement on any of the qubits will lead to a collapse of the entire local copy she was attacking, negating her efforts.

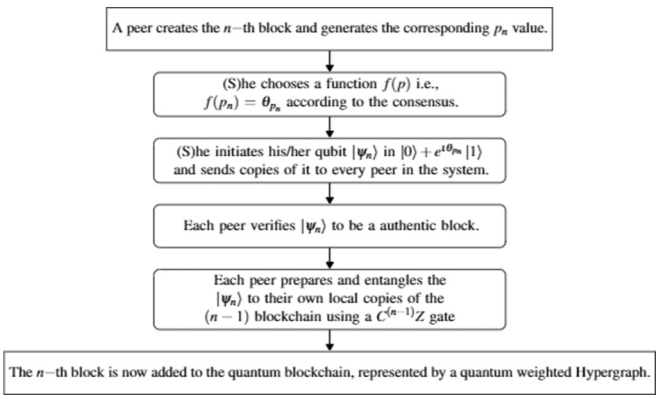

FIG. 8. Flowchart describing the workflow of the proposed quantum blockchain.

We consider another case where Eve wants to change a transaction that has been included in the mth block with corresponding phase factor θ_{p_m}, she then needs to adjust the relative phase of the mth qubit to θ_q. In order to do so, she needs to operate a unitary operation on the mth qubit, to add a relative phase $(\theta_q - \theta p_m)$ to the corresponding qubit. The consensus of the quantum blockchain prevents Eve in doing so, as the relative phase of each qubit is predefined and can be checked by performing a simple measurement on the correct basis on that particular qubit anytime. The peer whose local copy of the chain has been compromised can identify the compromise and rebuild his/her blockchain as (s)he knows the exact quantum state without violating no-cloning theorem.

Moreover, weighted hypergraph states are a class of states that fall under the locally maximally entanglable (LME) [17,21] class of states. Hence, the peers can apply local unitary operations on the states to change it to a different state of the same SLOCC class which can also increase the entanglement in the system. Quantum operations being reversible, this will not affect a trusted party to retrieve the information, although it will prevent any attacker who does not know what operations have been performed on the state.

The key effectiveness of the quantum blockchain proposed lies in the fact that each qubit in this protocol represents a block. Previously in [6], another protocol of creating quantum blockchain was shown using temporal GHZ states, where each block is an n-qubit state. Our protocol is more cost effective as it uses a single qubit to represent a block.

As each peer shares a local copy of the prepared state at each step, the distributive nature of the blockchain technology is maintained whereas the need of cryptographic hash function and commonly shared ledger is eradicated. The function $f(p_n)$ that converts the classical information to the relative phase of the corresponding qubit is chosen by and known only to the peer who creates the nth block, which adds another layer of security to the stored information. The stored information is also retrievable as each quantum operation is reversible and $f(p)$ is a bijective function.

In the next section, we present an example of a quantum 3-blockchain prepared in IBM five-qubit computer.

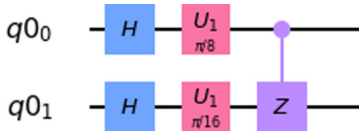

FIG. 9. Circuit for quantum 2-blockchain prepared in IBM quantum experience.

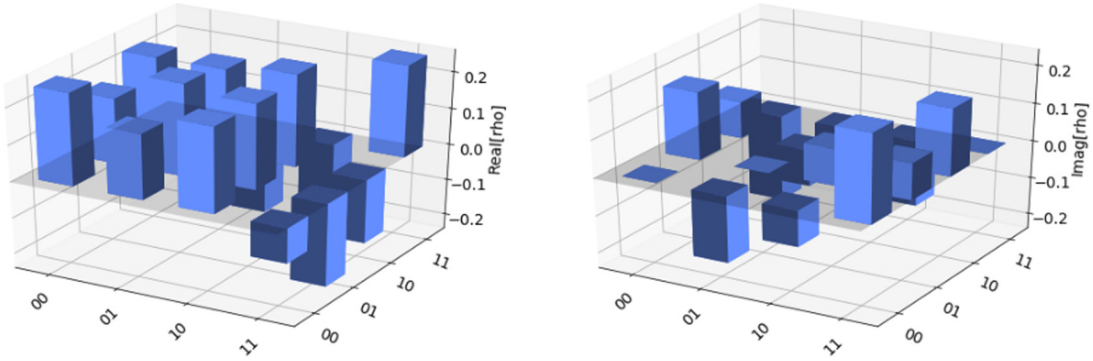

FIG. 10. Real (Real[rho]) and Imaginary (imag[rho]) parts of the theoretical density matrix representing the quantum 2-blockchain.

IV. QUANTUM BLOCKCHAIN PREPARED IN IBM FIVE-QUBIT QUANTUM COMPUTER

In this section we present two quantum blockchains with two and three blocks prepared in IBM Quantum Experience. Although IBM Quantum Experience is a cloud-based platform and this protocol is based on a distributive ledger technology, we present the construction of the blockchains in the IBM quantum computer as a proof of concept. To construct the quantum blockchain, we have mutually agreed upon a general consensus that the function $f(p_i)$ that converts the decimal number p_i containing the binary bit information of the block i (here index i represents the chronological number of the block) to θ_{p_i}, the weight of the weighted hypergraph state as described in Sec. II is selected individually by peer i (the peer who creates the ith block) in such a way that $\theta_{p_i} = \frac{1}{2^{i-1}}\theta_{p_1}$. The conditions on θ_{p_i} described in Sec. II are met by enforcing this condition.

A. Quantum 2-blockchain

We consider the phase added to the first block to be $\theta_{p_1} = \frac{\pi}{8}$, and it is being broadcasted to all the peers in the network. So, the relative phase added to the second block is $\theta_{p_2} = \frac{\pi}{16}$. The circuit prepared in IBM quantum experience representing the quantum 2-blockchain is given in Fig. 9. The circuit has been designed on "ibmqx2" quantum processor. The verification of the quantum state sent by the first and second peers can be done by initiating the state on an ancilla and measuring it on the suitable basis, which we did not show here. The density matrix for theoretical quantum blockchain with 2-blocks is plotted in Fig. 10, whereas Fig. 11 represents the reconstructed density matrix obtained after running the circuit in "ibmqx2" quantum processor with 8192 shots. The state fidelity of the results is found be 0.9548 (up to 4 decimal places).

B. Quantum 3-blockchain

The phase of the third block will be $\theta_{p_3} = \frac{\pi}{32}$ as per the consensus and prepare the circuit in IBM quantum experience making use of the available gates. The corresponding circuit diagram is presented in Fig. 12. Here, we have used four qubits to make a 3-blockchain, using the last qubit as an ancilla to create the C^2Z gate using two CX gates and one CZ gate [22]. Running this circuit in IBM "quasm simulator," we found the state fidelity between the original density matrix and the reconstructed matrix postmeasurement to be 0.9948. To prepare a $C^{(n-1)}Z$ gate using only C^2X gate and CZ gate, one needs to use $2(n-1)$ qubits [$(n-1)$ control qubits, $(n-2)$ ancillas, and 1 target qubit] [22]. It is thus possible to make a quantum n-blockchain with $2(n-1)$ qubits using IBM Quantum Experience. One can prepare a quantum blockchain with 8 blocks using the publicly accessible 14-qubit processor of IBM (7 control qubits, 6 ancillas to prepare the C^7Z gate, and one target qubit) using the method prescribed here at this very moment.

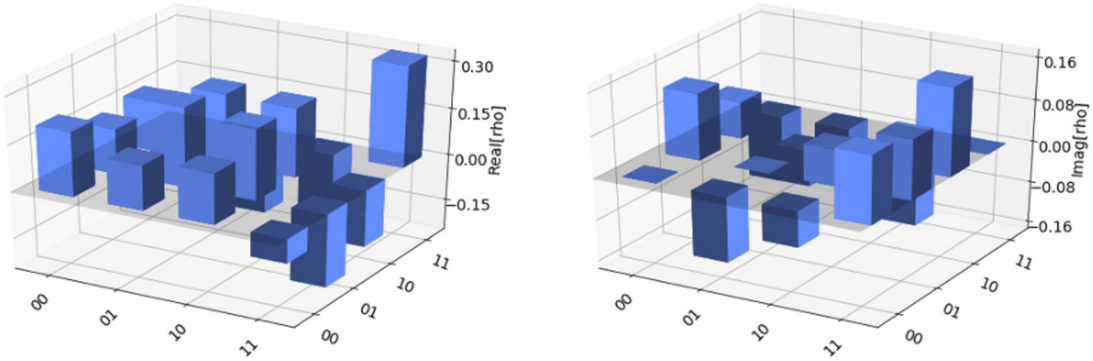

FIG. 11. Real (Real[rho]) and Imaginary (imag[rho]) part of the reconstructed density matrix after running the circuit in Fig. 9 representing the quantum 2-blockchain in "ibmqx2" quantum processor with 8192 shots.

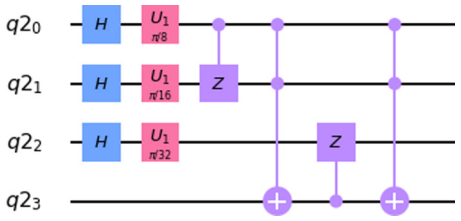

FIG. 12. Circuit for 3-blockchain as prepared in IBM quantum experience.

V. CONCLUSION

In summary, a protocol to prepare a quantum blockchain has been presented using weighted hypergraph states where the classical ledger-based network and cryptographic hash functions have been replaced with the entanglement of the weighted hypergraph state. The security and effectiveness of the protocol have been discussed against an attacker possessing a quantum computer. A prescription to prepare a quantum blockchain using publicly accessible IBM quantum computer. A quantum 2-blockchain prepared in IBM five-qubit processor "ibmqx2" is presented as a proof of concept, which has a fidelity of 0.9548. We hope that this protocol finds significant applications in various fields as the classical blockchain technology is threatened by the recent quantum advancements. Quantum money [23,24] and attacks against it [25,26] have been a point of interest of quantum information research since it was first proposed by Wisner [23]. Previously, the idea of a quantum check scheme has been proposed by Moulick and Panigrahi [27], which is unconditionally secure. This proposed quantum money transaction via quantum check has been realized experimentally in a quantum computer using IBM quantum experience [28]. The idea of a quantum blockchain provides a secured quantum ledger to keep unalterable records of such quantum as well as several classical transactions. This is a step forward to the direction of establishing a secure and completely quantum currency transaction system.

ACKNOWLEDGMENT

The authors acknowledge IBM Quantum Experience for providing the support to the IBM quantum processors and thank Professor F. Nori at Riken, Japan, and Dr. A. Dasgupta and A. Acharya at Indian Institute of Science Education and Research Kolkata for valuable comments and discussions.

[1] M. Rauchs, A. Glidden, B. Gordon, G. C. Pieters, M. Recanatini, F. Rostand, K. Vagneur, B. Zheng Zhang, Available at SSRN: https://ssrn.com/abstract=3230013.
[2] S. Nakamoto, available at http://www.bitcoin.org/bitcoin.pdf.
[3] G. Drosatos and E. Kaldoudi, Comput. Struct. Biotechnol. J. **17**, 229 (2019).
[4] W. J. Tee and R. K. Murugesan, *Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA)* (IEEE, Piscataway, NJ, 2018).
[5] N. Kossow and V. Dykes, doi: 10.13140/RG.2.2.16340.76162.
[6] D. Rajan and M. Visser, Quantum Rep. **1**, 3 (2019).
[7] J. Katz and Y. Lindell, *Introduction to Modern Cryptography* (Chapman and Hall/CRC, Boca Raton, FL, 2014).
[8] bitcoin-publicly accessible ledger: Available at https://www.blockchain.com/explorer.
[9] C. G. Oliver, A. Ricottone, and P. Philippopoulos, arXiv:1708.09419.
[10] 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 Sci. Technol. **3**, 035004 (2018).
[11] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler *et al.*, Nature (London) **574**, 505 (2019).
[12] Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu, and Y.-X. Yang, IEEE Access **6**, 27205 (2018).
[13] L. K. Grover, arXiv:quant-ph/9605043.
[14] W. Yin, Q. Wen, W. Li, H. Zhang, and Z. Jin, IEEE Access **6**, 5393 (2018).
[15] C. Li, Y. Xu, J. Tang, and W. Liu, J. Quantum Comput. **1**, 49 (2019).
[16] M. Rossi, M. Huber, D. Bruß, and C. Macchiavello, New J. Phys. **15**, 113022 (2013).
[17] N. Tsimakuridze and O. Gühne, J. Phys. A: Math. Theor. **50**, 195302 (2017).
[18] R. Qu, J. Wang, Z.-S. Li, and Y.-R. Bao, Phys. Rev. A **87**, 022311 (2013).
[19] O. Gühne, M. Cuquet, F. E. S. Steinhoff, T. Moroder, M. Rossi, D. Bruß, B. Kraus, and C. Macchiavello, J. Phys. A: Math. Theor. **47**, 335303 (2014).
[20] S. Dutta, R. Sarkar, and P. K. Panigrahi, Int. J. Theor. Phys. **58**, 3927 (2019).
[21] C. Kruszynska and B. Kraus, Phys. Rev. A **79**, 052304 (2009).
[22] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, New York, 2011).
[23] S. Wiesner, ACM Sigact News **15**, 78 (1983).
[24] A. Lutomirski, S. Aaronson, E. Farhi, D. Gosset, A. Hassidim, J. Kelner, and P. Shor, arXiv:0912.3825.
[25] K. Bartkiewicz, A. Cernoch, G. Chimczak, K. Lemr, A. Miranowicz, and F. Nori, NPJ Quantum Inf. **3**, 7 (2017).
[26] A. Molina, T. Vidick, and J. Watrous, *Conference on Quantum Computation, Communication, and Cryptography* (Springer, Berlin, 2012), pp. 45–64.
[27] S. R. Moulick and P. K. Panigrahi, Quantum Inf. Process. **15**, 2475 (2016).
[28] B. K. Behera, A. Banerjee, and P. K. Panigrahi, Quantum Inf. Process. **16**, 312 (2017).