Improving the implementation of quantum blockchain based on hypergraphs

Francisco Orts[1*†], Remigijus Paulavičius[1†] and Ernestas Filatovas[1†]

[1*]Institute of Data Science and Digital Technologies, Vilnius University, Vilnius, Lithuania.

*Corresponding author(s). E-mail(s): francisco.gomez@mif.vu.lt;
Contributing authors: remigijus.paulavicius@mif.vu.lt;
ernestas.filatovas@mif.vu.lt;
†These authors contributed equally to this work.

Abstract

In recent years, there has been a growing interest in the potential of quantum computing for enhancing the security and efficiency of blockchain technology. While quantum blockchain protocols offer improved security over their classical counterparts, implementing such protocols on present-day quantum computers poses difficulties due to the limited number of qubits and quantum gates and the significant effects of noise. In this paper, we propose a set of improvements for implementing a quantum blockchain protocol based on hypergraphs that aim to reduce the required resources and operations and increase noise tolerance. Specifically, we focus on enhancing the state-of-the-art quantum circuits that underpin the quantum blockchain by optimizing the so-called T-count and T-depth, which represent the number of quantum gates and the circuit depth, respectively. Our proposed implementations also leverage proven error detection and correction codes to improve noise tolerance. To evaluate the effectiveness of our proposed improvements, we tested them on real quantum devices. Our results demonstrate a significant reduction in the T-count and T-depth. Overall, our proposed improvements provide a promising direction for the practical implementation of quantum blockchain protocols on current quantum computers and lay a foundation for further research in this area.

Keywords: Quantum blockchain, Hypergraph states, Quantum circuit, Quantum Computing, Blockchain

1 Introduction

Quantum computing [1] and blockchain [2] are two disruptive technologies that are currently receiving a great deal of interest from the scientific community [3–6]. Although there is a great deal of literature on both topics, many works tend to concentrate on the potential risks that quantum computing could pose to the blockchain and cryptography as a whole [7–9]. The widespread approach is to talk about a blockchain aimed at resisting attacks carried out by exploiting the potential of quantum computing. As a rule, the goal is to avoid any cryptography that can be broken by Shor's quantum algorithm, allowing factoring numbers in polynomial time [10]. But Shor's algorithm is not the only threat from quantum computing. For instance, Grover's algorithm can also be used for more efficient attacks [11]. It is only a matter of time before a quantum computer is built with sufficient resources to put current cryptography in check [12].

However, as is usual in these cases, there are researchers who look for opportunities even in the face of the greatest threats. A growing and interesting variety of works in the literature do not treat quantum computing as a danger to the blockchain but as a potential source of advantages [13–16]. Such works try to build a quantum blockchain that benefits from the special features of quantum mechanics to achieve faster, cheaper, greener, and more secure results [17]. These benefits are especially useful when the blockchain faces scalability and efficiency issues [18].

The limitations of current quantum computers are the main obstacles to the aforementioned collaboration between quantum computing and blockchain. First, current quantum devices, commonly called Noisy Intermediate-Scale Quantum (NISQ) devices, are limited in resources [19]. With honorable exceptions, such devices typically do not exceed 100 qubits, which is insufficient for the largest problems. Secondly, these NISQ devices are heavily affected by internal and external noise [19]. Quantum circuits must consider the effects of noise, or else they will be unusable [20]. There are other problems that arise from these two, such as the strong need to adapt circuits to the topology of each quantum device [21], or to use only a subset of the infinite existing quantum gates if a given device requires so [22]. Nevertheless, such NISQ devices can already be successfully used to build interesting applications [23–25].

There is intense research to improve the hardware of quantum computers and achieve ever larger and more stable devices [19, 20]. In the meantime, any quantum algorithm must try to optimize resources and implement some noise tolerance. The quantum T gate is closely related to both concepts. First, it is part of the Clifford+T group, well known for (among other reasons) allowing the use of error detection and correction codes [20, 26]. Second, because its cost is up to 100 times the cost of other gates [26], reducing the number of T gates can greatly reduce the cost of a circuit. For these reasons, reducing the number of T gates to reduce costs and studying possible implementations based on Clifford+T gates are the central topics of this work.

This paper focuses on optimizing the implementation of currently available blockchain protocols for quantum computing based on hypergraphs in terms of T gates. The choice of why this type of quantum blockchain – based on hypergraphs – and not another is explained in a later section, as some concepts need to be introduced to justify this choice. The contribution is therefore related to improvements in the implementation of the protocols, and not in the other aspects of the protocols. We consider this topic vital in order to scale the protocols available in the literature to larger sizes on the available quantum devices.

The most important contributions of this paper are the following:

- It reviews state-of-the-art quantum blockchain construction protocols.
- It enhances the state-of-the-art quantum circuits that underpin the quantum blockchain and reduces the necessary resources. Specifically, significant reductions were achieved in both the so-called T-count and T-depth.
- It studies and proposes implementations using exclusively Clifford+T gates, thus allowing the resulting circuits to benefit from existing error detection and correction codes.

The rest of this paper is structured as follows. Section 2 provides an overview of the necessary background on blockchain and quantum computing that is essential to understand the work presented in this paper. In Section 3, we summarize the blockchain protocol used as a basis for this work. Building on this, in Section 4, we propose novel approaches to further optimize the implementation of the selected protocol in terms of T-count and T-depth while also exploring implementations based on Clifford+T gates. The results achieved through these improvements are presented and compared with the original implementations in Section 5. Finally, in Section 6, we present our concluding remarks and highlight potential avenues for future research in the field of quantum blockchain.

2 Background

This section will introduce some concepts that are necessary to understand the proposed implementations. First, we introduce the basic structure of blockchain. Secondly, an introduction to quantum circuits and their associated metrics is given. Next, an important algorithm from the literature is briefly introduced, allowing us to obtain a quantum circuit built exclusively using Clifford+T gates equivalent to any unitary gate (under certain assumptions). This algorithm obtains the equivalent in Clifford+T gates of some operations in our blockchain. Finally, the concept of a quantum hypergraph is explained since the implementation is based on the idea of a quantum hypergraph.

2.1 Blockchain fundamentals

The classical blockchain finds its foundation in key concepts introduced in a variety of influential works [27–29]. Notably, one of the earliest and most widely

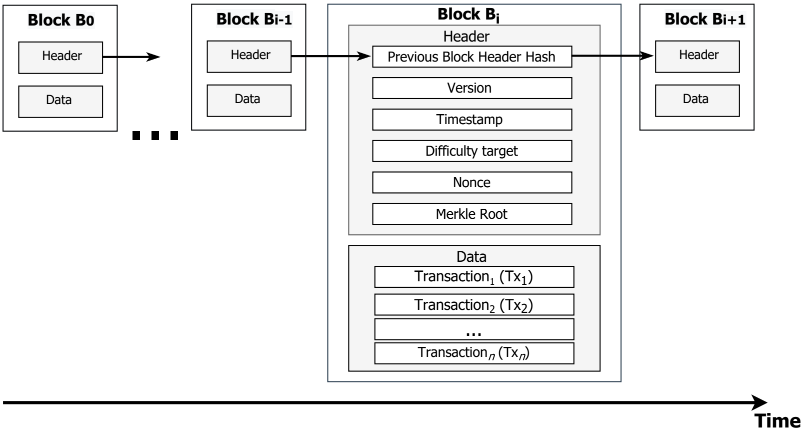


Fig. 1: The simplified Bitcoin blockchain data structure. The newly created block also contains a cryptographic hash of the previous block. As new blocks are added to the chain, the blockchain continues to grow in a continuous manner.

recognized implementations of a blockchain – Bitcoin [30] – is a distributed ledger that allows multiple parties to securely record, verify, and maintain a permanent and tamper-proof record of transactions without the control of a centralized authority. The ledger consists of a chain of blocks linked in chronological order using cryptographic hash functions. Each block contains data (usually a set of transactions) that have been verified and added to the chain by network participants (nodes). The simplified blockchain ledger is depicted in Fig. 1 using Bitcoin as an example.

The process of generating blocks on the blockchain is determined by a consensus mechanism that ensures agreement among network participants and facilitates the right to validate transactions and add them to the ledger. A wide range of blockchain consensus mechanisms have been designed with different concepts and properties (e.g., Prof-of-Work, Proof-of-Stake, etc.), and their selection depends on the blockchain system's purposes [31]. Typically, a node or peer is chosen to propose a block to the network using a specific method, such as voting or solving a computationally demanding cryptographic puzzle. Afterward, other nodes within the network must verify the proposed block to confirm its correctness and coherence with the current ledger. After the validating nodes reach a consensus, the block is appended to the chain and the local versions of all participants.

2.2 Quantum circuits and metrics

A quantum circuit consists of qubits and quantum gates that operate on the state of such qubits. Certain analogies can be drawn between classical and quantum circuits. In fact, for any classical circuit, an equivalent quantum circuit can be found [20]. However, there are important differences between the two types of circuits. The most obvious one is that classical circuits work on bits and quantum circuits on qubits. The bit can be worth 0 or 1, and the qubit has infinite possible values. Other differences include that quantum circuits do not allow feedback, must be reversible, and do not allow fan-in or fan-out [20, 32].

A common problem with quantum circuits is the difficulty in quantifying their degree of optimization. Given two quantum circuits, which one is better? Mohammadi et al. [33] established a metrics framework for measuring quantum circuits. They defined four important aspects: quantum cost, delay, number of qubits, and garbage qubits. These metrics allow a circuit to be accurately evaluated and compared and are widely used in the literature [34–36].

However, the four metrics described by Mohammadi et al. focus on describing the circuits and do not address a fundamental problem — noise. Noise is possibly the main problem quantum computers face nowadays [37, 38]. Any quantum circuit running on an NISQ device will suffer from noise and its results will be altered as a consequence. Medium to large circuits holds little to no value without a noise protection mechanism. A common approach in the literature is to build circuits using only Clifford+T gates [26, 39, 40]. This universal group (any quantum circuit can be approximated using only gates of this type) allows circuits to be compatible with proven error detection and correction codes [20]. Using such codes allows us to detect both amplitude and phase errors, making them a very useful tool to counteract the effects of noise [41]. Unfortunately, their use is only compatible with circuits built exclusively with transverse gates. Of the universal set of gates, the Clifford+T group meets this characteristic.

However, using the Clifford+T gate involves a new problem: the cost of the T gate. The cost of this gate is higher than the rest of the gates, making the cost of the others practically negligible [26]. Therefore, when this gate is used, circuits are usually measured not using quantum cost or delay but using two adaptations of such metrics called T-count and T-depth. T-count is the number of T-gates a circuit has, and T-depth is the number of T-gates the circuit has in its critical path [42]. For the sake of clarity, it should be mentioned that the T-gate is a core member of the Clifford+T group. Without this gate, the group would cease to be universal; thus, it cannot be easily replaced.

Reducing the number of T-gates (to reduce the T-count) is essential to prevent a circuit from reaching prohibitive costs. Also, to allow the use of error detection and correction codes, it is very useful to build circuits using only gates from the Clifford+T group [43, 44]. For these reasons, the objectives of this work are focused on achieving implementations with a reduced T-count, as well as trying to use only gates belonging to the Clifford+T group.

2.3 Approximation of unitaries operations by Clifford+T gates

Although the Clifford+T group is universal and can approximate any possible circuit, transforming an arbitrary circuit to an equivalent one using only Clifford+T gates is not trivial. This transformation is of great interest to the scientific community, and a wide variety of related works can be found in the literature [45–50]. In this paper, it is only required to obtain a Clifford+T circuit that implements the equivalent of a U_1 gate [20]. The U_1 gate is a diagonal gate which perform a (single) qubit rotation only around the Z axis [51]. To obtain the equivalent of an arbitrary U_1 gate in terms of Clifford+T gates is also not trivial, but it reduces the problem.

In 2015, Kliuchnikov et al. [45] proposed an algorithm to find the optimal implementation regarding the T-count of single-qubit unitaries using Clifford+T gates. Their algorithm outperformed (again, in terms of T-count) previous works in the literature. Since then, other works have been published that improve the implementation or some specific aspects of this algorithm [52–54]. However, none of them improves the obtained results by their algorithm in terms of T-count for the U_1 gate case. In addition, Kliuchnikov et al. freely offer software that automatically obtains such implementations. Therefore, in our work, the algorithm of Kliuchnikov et al. is used to obtain the equivalent circuits.

2.4 Definition of quantum hypergraph

A hypergraph is a special version of a graph. In a normal graph, an edge always connects two nodes. In a hypergraph, an edge can join two or more nodes. Such edges are usually called hyperedges to differentiate them from the classic edges that only join two nodes. A quantum hypergraph is the quantum version of a hypergraph, which can be defined as a set of highly entangled multipartite quantum qubits [55]. Therefore, in a quantum hypergraph, nodes correspond to quantum states, and (hyper)edges imply connections between such states. The way to represent the edges is by the entanglement of the qubits involved [56, 57].

An example of a hypergraph and its quantum equivalent is shown in Fig. 2. Controlled-Z quantum gates have been used to entangle the qubits corresponding to each edge (the implementation of the Controlled-Z gate is discussed in the next section). At the start of the circuit, the qubits must be in a $|+\rangle$-superposition state. The resulting quantum state of the circuit shown in Fig. 2 will then be:

$$|\psi\rangle = C^2_{(2,3,5)}ZC^2_{(4,5,6)}ZC^2_{(1,2,3)}Z\,|+\rangle^{\otimes 5}$$

The notion of hypergraph can be extended to that of a weighted hypergraph by assigning each edge a weight [55]. In quantum terms, a weighted hypergraph

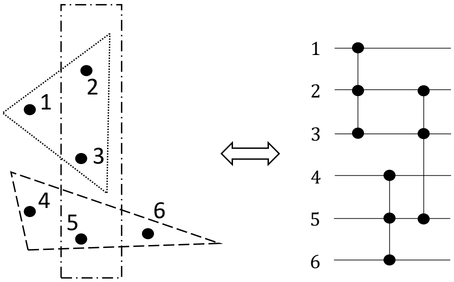


Fig. 2: Example of a hypergraph with six nodes, three hyperedges, and its associated quantum circuit. All qubits are assumed to be initially in the state $|+\rangle$.

state [58, 59] can be defined as:

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

where N is the number of edges, $|x\rangle$ the computational basis and $f(x) \in \{0,1\}$ [60].

2.5 State-of-the-art in quantum blockchain construction

The construction of a quantum blockchain is a relatively new topic [18]. However, several works in the literature address the implementation of a blockchain in a quantum network. In 2019, Rajan and Visser [61] proposed a quantum blockchain design based on the use of temporal GHZ states, being the first work of its kind to include a realistic analysis. However, despite its great conceptual contribution, this work is purely theoretical. It does not propose any implementation or designs of any kind that would allow the construction of prototypes in real quantum devices or simulators.

In the same year, Li et al. [62] extended Rajan and Visser's work by including important improvements in terms of security and efficiency. This article discusses the benefits and problems of building a quantum blockchain framework and even provides a complete conceptual algorithm of the necessary steps for its construction. But similar to the previous work, it does not address its implementation in quantum computers.

Other work focuses on specific aspects of building a quantum blockchain, often focusing on the quantum realization of one or more parts of a classical blockchain. Edwards et al. conducted a comprehensive review of all these articles published to date in 2020 and classified them into different categories depending on the part they studied (e.g., articles that propose or optimize a consensus) [18]. But once again, these works operate theoretically without going down to the level of implementations, or at least not in a complete way that allows the ideas provided to be reproduced within a fully functional protocol.

In 2020, Banerjee et al. [63] presented a protocol based on using quantum hypergraphs as substitutes for hash functions in a quantum environment. One of the biggest advantages of this protocol is its block optimization: only one qubit is dedicated to each block. And what is much more important: they propose an implementation for their protocol. Moreover, the proposed implementation is almost exclusively composed by gates from the Clifford+T group. Only one non-Clifford+T rotation gate is used per block. However, it is an incomplete protocol that does not meet all the needs of a blockchain. For instance, the proposed consensus has no real validity since only the first peer can send useful information.

In 2022 Li et al. [13] extended the proposal of Banerjee et al. by incorporating a Quantum Delegated Proof-of-Stake (QDPoS) consensus mechanism. Li et al. proposes significant conceptual improvements over the scheme of Banerjee et al. In addition, an implementation for the presented protocol is also proposed in their work. In fact, they use the implementation proposed by Banerjee et al. They also offer a second (own) implementation based on weighted graphs. However, this second implementation requires a larger number of gates that do not belong to the Clifford+T group than the one proposed by Banerjee et al.

Also in 2022, Nilesh and Panigraphi [16] presented a complete protocol with detailed definitions for the different phases of the protocol: transaction, verification, consensus, and block linking. As far as the authors are aware, this is the most complete protocol available today, improving on the others (which are still prototypical) in practically all aspects. However, precisely because of its completeness, it is not feasible on current quantum devices. But it is nonetheless the best quantum protocol currently available in the literature.

Among the works studied, two stand out with prototype-level implementations feasible in current quantum devices: the protocols of Banerjee et al. and Li et al. Our work builds upon the advancements made by Banerjee et al. by enhancing their circuits, thereby reducing the resources and operations required for constructing a quantum blockchain—a crucial consideration given the present state of quantum computing. It is important to emphasize that our focus lies solely on improving the implementation and not the protocol itself. Considering our objective of exploring the minimum cost for implementing a quantum protocol on currently available or near-term quantum devices, we chose the Banerjee et al. implementation over Li et al.'s. The former requires fewer conversions of non-Clifford+T gates, as discussed in Subsections 2.3 and 2.4. Nevertheless, we want to highlight the significance of Li et al.'s work and the notable advancements it offers, particularly in aspects like security and consensus. Although we use the Banerjee et al. protocol as the basis for our implementation in this paper, it is crucial to recognize that the proposed improvements are also applicable to the implementation of Li et al.'s protocol. In fact, we highly recommend adopting the Li et al. protocol, combining its comprehensive features with our proposed improvements.

3 Protocol to make quantum blockchains

This section summarizes the key points of the protocol presented by Banerjee et al. [63]. We highlight the most important points of the protocol for two reasons: first, we want to make it clear that the credit for the protocol goes to Banerjee et al. We have only identified it as the protocol with the most optimized implementation in terms of cost. Second, since our contribution is to improve the implementation of the protocol, it is necessary to know the protocol in order to make a proper comparison.

3.1 Definition of the protocol

The protocol proposed by Banerjee et al. [63] works with weighted hypergraph states and uses the weights to encode the information in the hypergraph state. The protocol consists of the following phases:

1. Encoding the information of the blocks: the information is a classical binary string with a decimal equivalent p. The peer who made the block initializes his qubit as $\psi = |+\rangle$ and introduces p as:

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

   being $\theta_p \in (0, \frac{\pi}{2})$ a function only known by the peer who creates the block. In this way, $|\psi_1\rangle$ contains the information corresponding to a classical block.
2. Consensus: the protocol of Banerjee et al. requires that $0 < \theta_{p_i} < \frac{\pi}{2}$ and $\sum_i \theta_{p_i} < \frac{\pi}{2}$, $\forall i$ (being i the number of blocks). The proposed consensus implies that the peers agree to form their blocks in such a way that the relative phase θ_p of each qubit i (belonging to peer i) is described as $\theta_{p_i} = \frac{1}{2^(i-1)}\theta_{p_1}$. Therefore, it is necessary for the first peer to broadcast its θ_{p_1} to all other peers. It is trivial to check that the first condition, $0 < \theta_{p_i} < \frac{\pi}{2}$, is always satisfied. Regarding the second condition, $\sum_i \theta_{p_i} < \frac{\pi}{2}$, note that the series $\sum_{i=1}^{\infty} \frac{1}{2^(i-1)}\theta_{p_1}$ converges to $2\theta_{p_1}$. To ensure that the condition is satisfied, it is important that the first peer initializes its qubit to a value less than $\frac{\pi}{4}$.
3. Formation of the quantum blockchain: the chain of N blocks is replaced by a hypergraph of N qubits, where each qubit encodes the information as it has been explained. Once a qubit contains the information, the peer sends a copy of the state to the rest of the peers. This is possible since the peer knows exactly the state of the qubit. Each peer verifies the conditions (see Consensus) and adds the qubit to their local copy of the chain using controlled-Z gates (creating a N-qubit weighted hypergraph).
4. Verification of the blocks: the peer who creates the m-th block prepares his qubit as

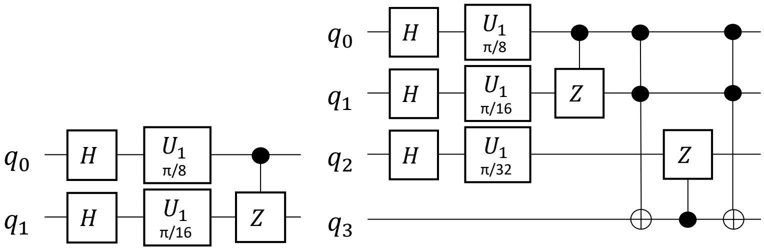
$$|\psi_m\rangle = \frac{|0\rangle + e^{i\theta_{p_m}}\,|1\rangle}{\sqrt{2}}$$

Here, $\theta_{p_m} = (\frac{1}{N^{m-1}})\theta_{p_1}$. The peers that receive a copy of this qubit can measure it using the basis $|\psi_m\rangle = \frac{|0\rangle + e^{i\theta_{p_m}}|2\rangle}{\sqrt{2}}$. If the result is 0, they abort the addition of this qubit in their local copy, and the peer is marked as untrustworthy.

3.2 Implementation of the protocol

Banerjee et al. [63] presented two real implementations with two and three blocks, respectively. Both implementations are reproduced in Fig. 3. In both cases, the phase of the first block is set to $\theta_{p_1} = \frac{\pi}{8}$, and the following added phases will be $\theta_{p_i} = \frac{1}{2^{i-1}}\theta_{p_1}$. The left side of Fig. 3 shows the blockchain for the two-block case. It can be seen how the two qubits are placed in a superposition. The first qubit introduces the θ_{p_1} phase. Then, the second block (with phase $\theta_{p_2} = \frac{\pi}{16}$) is then added, and both qubits are entangled using the Controlled-Z gate.

The same process is repeated in the 3-qubit version (right-hand side of Fig. 3). Subsequently, a third block with phase $\theta_{p_3} = \frac{\pi}{32}$ is introduced. However, a Controlled-Z gate with two control qubits would be needed to entangle the three qubits. Banerjee et al. implemented their circuits on the quantum computers available on the IBM Quantum platform. A version of the Controlled-Z gate with more than one control qubit is unavailable on such computers. In fact, it is hard to find a version with more than one control qubit for such a gate in any quantum device. However, the operation can be performed using a Toffoli gate acting on an auxiliary qubit and using that qubit as a control one in a Controlled-Z gate that (now) acts on the target qubit [20]. Although valid, the operation involves the use of an extra qubit. The machine used by Banerjee et al. to build and test the circuits was *ibmqx*2, which has a total of only 5 qubits. This is why even a single extra qubit for such an operation can be costly.



(a) 2-blockchain circuit

(b) 3-blockchain circuit

Fig. 3: Circuits for quantum blockchain proposed by Banerjee et al. [63].

Once the three qubits are entangled, a new Toffoli gate is applied on the auxiliary qubit to reset the auxiliary qubit and avoid garbage outputs, a highly recommended technique to free up the few available resources of quantum devices [64].

Banerjee et al. only implement these two blockchains but give the algorithm to build a blockchain for any block size. In this particular example, phase $\theta_{p_i} = \frac{1}{2^{i-1}}\theta_{p_1}$ should be introduced for the next blocks, and then Controlled-Z gates are used to entangle the qubits. The number of control qubits of such gates will depend on the number of blocks. For N blocks, $(N-1)$ Controlled-Z gates are needed, increasing their number of control qubits from 1 to $N-1$. Using the construction of the Controlled-Z gate based on Toffoli gates and auxiliary qubits requires adding, for each control qubit (except the first one), an ancilla qubit [65]. Therefore, for any blockchain of N blocks, N qubits will be required for the blocks, and $N-2$ ancilla qubits to perform the operations related to the entanglement. Also, $2(N-2)$ Toffoli gates and $N-1$ Controlled-Z gates (of one control qubit) are required. Trivially, it can be stated that N Hadamard gates and N U_1 gates are also required.

3.3 Limitations

The Banerjee et al. protocol offers a qubit-optimized implementation based on hypergraphs that allows prototypes to be implemented on even the smallest quantum devices. This is an advantage over other protocols in that it allows for tangible testing and is not limited to the purely theoretical. However, the Banerjee et al. protocol is an incomplete protocol that provides basic notions on the construction of a quantum blockchain but leaves several questions unaddressed compared to the (theoretical/conceptual) work of Nilesh and Panigraphi [16]:

- No clear way to identify whether the first message is valid or invalid is provided.
- No mechanism is indicated to resolve cases where two or more peers send their block at the same time.
- The indicated security proofs have no applicability in the offered implementation, or at least their applicability has not been developed in the paper.
- The proposed consensus is based on maintaining a difference in the relative phase of consecutive blocks. This only allows the first peer to send useful information. According to the consensus, the other peers have to send a qubit (a block) containing the agreed phase difference, which prevents them from including their own information. Otherwise, the agreed phase difference would no longer be maintained and it would not be possible to retrieve the information or check its integrity according to the mechanisms provided in the paper.

Despite these shortcomings, the hypergraph-based implementation is fully functional and remains the most optimized in terms of cubits. In this sense, the aforementioned work by Li et al. [13] uses this same implementation but offers a consensus with real utility and addresses some of the problems

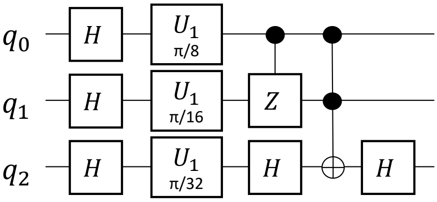


Fig. 4: Proposed implementation of a 3-blockchain circuit. It halves the T-count of the original circuit (Fig. 3 (b)) and also reduces the number of ancilla qubits.

of the protocol by Banerjee et al. This demonstrates the usefulness of this implementation regardless of the limitations of the protocol as the proposed improvements in implementation also apply to the protocol of Li et al. Therefore, we consider this implementation useful to advance the construction of quantum blockchains.

4 Proposed improvements for implementation

An optimized implementation in terms of qubits and T-count is presented in this section. In addition, the way to obtain circuits built exclusively using Clifford+T group gates is also addressed.

4.1 T-count optimized design

The first proposed improvement to the Banerjee et al. implementations is implementing a Controlled-Z gate of two control qubits using one Toffoli gate and two Hadamard gates. By using the well-known identity $HXH = Z$ [20] and controlling the X operation by a Toffoli gate, one auxiliary qubit can be saved. The 3-blockchain circuit can then be implemented as shown in Fig. 4. In addition to reducing the number of needed qubits by one, this operation also halves the T-count and T-depth as it allows us to reduce the number of Toffoli gates needed (a second one is not required to uncompute the garbage output). Although the improvement is simple at first glance, it allows the application of the problem to be extended to up to four blocks within a 5-qubit quantum computer like *ibmqx*2. On the other hand, the Hadamard gate has a markedly lower cost than the T gate [66, 67], so the extra Hadamard gates needed to be able to halve the T-count imply a lower cost than the presence of the T-gates.

This improvement is not limited to the 3-block case, but can be extended to all other sizes. However, it is still necessary to build extended versions of the Toffoli/ Controlled-Z gate for the following qubits. Nevertheless, the construction used to build the N-qubits Controlled-Z gate can be optimized. The Toffoli gates used in constructing these gates always act on qubits initialized to $|0\rangle$. The only purpose of such qubits is to store the partial control results temporarily. The second improvement is that such Toffoli gates can be replaced by

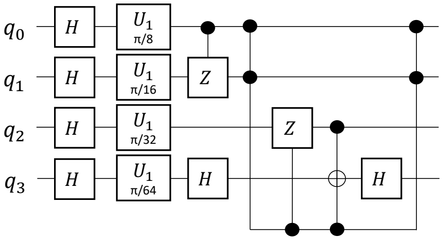


Fig. 5: Example of a hypergraph with six nodes, three hyperedges, and its associated quantum state. All qubits are assumed to be initially in the state $|+\rangle$.

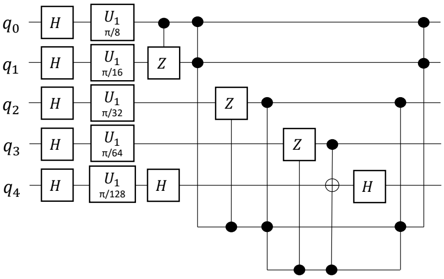


Fig. 6: Example of hypergraph with six nodes, three hyperedges, and its associated quantum state. All qubits are assumed to be initially in the state $|+\rangle$.

temporary logical-AND gates [68]. This gate requires acting on a qubit initialized in the state $\frac{1}{\sqrt{2}}(|0\rangle + e^{\frac{i\pi}{4}}\,|1\rangle)$ (a state that can be trivially set on a qubit using Clifford+T gates, with a T-count of 1). Following the same scheme as in the original work, $N-2$ temporary logical-AND gates and a single Controlled-Z gate are involved in constructing the equivalent of a Controlled-Z gate with N control qubits.

Putting these two ideas together - implementing the Z gate using H and X gates and replacing the expensive multi-qubit Toffoli gates with optimized versions of the Temporary logical-AND gate- results in a drastic reduction of the T-count and T-depth, as well as a reduction of one auxiliary qubit. The number of garbage outputs remains at zero, as in the original implementation. As examples, Figs. 5 and 6 show blockchain circuits for the case of 4 and 5 blocks, respectively.

For the sake of clarity, the steps involved in building the blockchain are outlined in simplified form:

1. The first peer prepares its block according to the chosen consensus. In particular, a Hadamard gate is used to put the cubit in superposition and a U_1 gate is used to encode its message in the relative phase.

2. The second peer prepares its block in a similar way to the first peer using a Hadamard gate and a U_1 gate to encode its message. This qubit is entangled with the previous one using a Controlled-Z, with the first peer's qubit acting as the control qubit, and the current qubit as the target one.
3. Peer i prepares its qubit like the two previous peers. Then, it is entangled with the blocks $i-1$ and $i-2$. To perform this action, a temporary logical-AND gate is applied using $i-1$ and $i-2$ as control qubits and an ancilla qubit (prepared in the state $\frac{1}{\sqrt{2}}(|0\rangle + e^{\frac{i\pi}{4}}|1\rangle)$) as a target one. The last one acts as a control qubit in a Controlled Z over the i qubit.
4. The last peer (if any) prepares its block. Then, a Toffoli gate is applied over this qubit, being the two previous blocks the control qubits.

4.2 Clifford+T circuit design

Although optimized, the circuit proposed in the previous subsection is not built exclusively with Clifford+T gates: the U_1 gate does not belong to such a group. Fortunately, the work of Kliuchnikov et al. [45] can approximate any single-qubit Z-rotation using Clifford+T gates. Furthermore, the algorithm proposed by Kliuchnikov et al. is optimized to achieve the lowest possible T-count for such an approximation.

The average number of T-gates needed to implement a U_1 gate is $3.067\log\left(\frac{1}{\epsilon}\right) - 4.322$, where ϵ is the desired approximation quality. It is trivial to point out that higher quality means more T gate. But it is worth mentioning that the algorithm guarantees that this T-count is optimal for any given quality. We will therefore use the value $3.067\log\left(\frac{1}{\epsilon}\right) - 4.322$ to define the T-count of each encoding of information in a block. Since this value will depend on the information to be encoded, it is not possible to give an exact value.

5 Results

Firstly, the results obtained by the optimised circuit will be analysed in terms of the T-count. Secondly, the results of the obtained circuit composed exclusively of Clifford+T group gates will be analysed.

5.1 Analysis of improvements in terms of T-counts

Of the gates used in the proposed circuit, only the Toffoli gate and the temporary logical-AND gate involve the use of T-gates. The Toffoli gate has a T-count of 7, while the temporary logical-AND gate has a T-count of 4 [68]. On the other hand, the Toffoli and temporary logical-AND gates have a T-depth of 3 and 2, respectively [26]. The T-count and T-depth of the circuit can be easily obtained by obtaining the number of Toffoli and temporary logical-AND gates in the circuit. For the general case of $N > 3$ blocks, the proposed circuit can be achieved as follows:

- To prepare N qubits, one qubit per block $(q_0, ...q_{N-1})$. Also, to prepare $N-3$ qubits for auxiliary tasks $(a_0, ...a_{N-4})$. **In total, $2N-3$ qubits will be required. T gates are not used in this step.**
- From the above qubits, to set N qubits in the $frac|0\rangle + |1\rangle\sqrt{2}$ state using N Hadamard gates (one per qubit). **T gates are not used in this step.**
- To set the remaining qubits in the $\frac{1}{\sqrt{2}}(|0\rangle + e^{\frac{i\pi}{4}}|1\rangle)$ state using an H gate and a T gate, to prepare them for later use of the temporary logical-AND gate. This step can be done initially, or just before the application of such gates. For simplicity, we assume here that the following are prepared initially. Therefore, $N-3$ **T gates are used in this step.**
- From $i = 1$ to N, to apply a U_1 gate to encode the value corresponding to the i block. **Again, T gates are not used in this step.**
- Apply a controlled Z-gate, where q_0 is the control qubit and q_1 is the target one. Also, to apply a temporary logical-AND gate with q_0 and q_1 as control qubits, and a_0 as the target one. 1 **temporary logical-AND gate (with a T-count of** 3**, deducting the one already used in step 3) is used in this step.**
- For $i = 2$ up to $N-3$, to apply a controlled Z-gate, with a_{i-2} as the control qubit and q_i as the target one. To apply a temporary logical-AND gate with a_{i-2} and q_i as target qubits, and a_{i-1} as the control qubit. $N-4$ **temporary logical-AND gates are involved here.**
- To apply an H gate on q_{N-1}, a Toffoli gate with q_{N-2} and a_{N-4} as control qubits and q_{N-1} as target one, and another H gate on q_{N-1}. 1 **Toffoli gate is applied.**
- Finally, for $i = N-3$ up to 1 to apply a uncomputation gate of the temporary logical-AND gate with a_{i-2} and q_i as target qubits, and a_{i-1} as the control qubit. **No T gates are involved in this step.**

Therefore, the circuit needs 1 Toffoli gate and $N-3$ temporary logical-AND gates. It has also been shown that it requires $2N-3$ qubits.

The original circuit of Banerjee et al. requires $2N-2$ qubits for the case of $N > 2$ blocks. Of the quantum gates used for its construction, only the Toffoli gate involves T-count. Knowing that the T-count of this gate is 7 and that the circuit consists of $2(N-2)$ Toffoli gates, we can establish that it has a total T-count of $14N-28$. The T-depth of the Toffoli gate is 3, so a blockchain of N blocks will also have a total T-depth of $6N-12$ since no Toffoli gate can be applied in parallel to others. On the other hand, our proposed circuit uses 1 Toffoli gate and $N-3$ temporary logical-AND gates, resulting in a T-count and T-depth of $4N-5$ and $2N-3$, respectively. Also, our proposed circuit needs $2N-3$ qubits.

Table 1 compares T-count, T-depth, and a number of qubits between the implementation proposed in Banerjee et al. and our proposal. The comparison is carried out for the case of several circuits with different numbers of blocks. Regarding qubits, our proposal only improves the original design in 1 qubit. However, in terms of T-count, the reduction is considerable. The T-count is halved for the smallest case, $N = 3$, while for the largest case, $N = 10000$,

Table 1: Comparison, in terms of T-count, T-depth, and number of qubits, between the proposed implementation and the original design of Banerjee et al. [63].

Number of blocks	Banerjee et al.			Proposal		
	T-count	**T-depth**	**Qubits**	**T-count**	**T-depth**	**Qubits**
3	14	6	4	7	3	3
4	28	12	6	11	5	5
5	42	18	8	15	7	7
10	112	48	18	35	17	17
15	182	78	28	55	27	27
20	252	108	38	75	37	37
30	392	168	58	115	57	57
40	532	228	78	155	77	77
50	672	288	98	195	97	97
100	1372	588	198	395	197	197
200	2772	1188	398	795	397	397
500	6972	2988	998	1995	997	997
1000	13972	5988	1998	3995	1997	1997
10000	139972	59988	19998	39995	19997	19997

it is reduced by an even larger factor. Significant reductions in T-depth have also been achieved, reducing the smallest case by half the original value and by almost three times for the largest size. Table 2 shows the percentage improvement of our proposal in the same cases as the previous table. It can be seen how the percentage improvement of both metrics improves as the size of the blockchain increases. T-count achieves an improvement of about 71% in the larger cases shown in the table, while T-depth improves by up to 66% in such cases. In the worst case, the smallest size, the improvement is 50% in both metrics.

Table 2: Percentages by which the proposed design improves on the original Banerjee et al. [63] design regarding T-count and T-depth for the indicated block sizes.

Number of blocks	% Improvement	
	T-count	**T-depth**
3	50.00	50.00
4	60.71	58.33
5	64.29	61.11
10	68.75	64.58
15	69.78	65.38
20	70.24	65.74
30	70.66	66.07
40	70.86	66.23
50	70.98	66.32
100	71.21	66.50
200	71.32	66.58
500	71.39	66.63
1000	71.41	66.65
10000	71.43	66.66

5.2 Analysis of the Clifford+T circuit design

More difficult is the analysis of the T-count associated with transforming U_1 rotations into Clifford+T group operations. First, It must be pointed out that such transformations are possible in both designs (Banerjee et al., and our proposal). Secondly, the cost will depend on each rotation and on the accuracy to be achieved. Using the Kliuchnikov et al. algorithm (their software is publicly available, the link is available at [45]) and setting it to an accuracy of about 10^{-16}, optimal approximations are achieved with a maximum of 155 T gates. We will use this maximum value as the upper bound of the T-count for such transformations. Thus, it can be established that the T-count for converting the designs into fully constructed circuits with Clifford+T gates will be $\leq 155N$. Of course, the corresponding value from Table 1 must be added to this value. Defining the T-depth would be too imprecise since the parallelism of these T gates depends entirely on each particular codification. Of course, the same upper limit can be set, but in this case it does not reflect the metric so faithfully.

It is clear that a T-count of $155N$ is impractical for a NISQ device even for a small number of blocks. However, the accuracy of the approximation can be reduced, which will lead to a reduction of the T-count. Of course, this implies that the blockchain is not realistically feasible as the information cannot be accurately encoded, but it will allow the implementation of prototypes for the smallest cases. Table 3 shows approximately the number of T gates needed to implement a U_1 rotation with the indicated accuracy.

Table 3: Average value of number of T gates involved in the approximation of a R_z rotation for a given approximation precision ϵ.

ϵ	**T-count**
10^{-1}	0
10^{-2}	1
10^{-3}	20
10^{-4}	25
10^{-5}	40
10^{-10}	100
10^{-15}	150

A maximum T-count of $155N$ can therefore be established for the conversion of the U_1 gates in a blockchain with N blocks. However, this value could be significantly reduced under certain assumptions, which basically involve limiting the rotations to certain assumptions in which the Kliuchnikov et al. algorithm achieves the optimal result (or the desired approximation) at the lowest cost. For instance, any rotation whose angle can be expressed as $\frac{2\pi k}{1000}$ (for any value of k between 1 and 1000) can be achieved using 109 T gates [45], which is a reduction of $46N$ with respect to the maximum value of the T-count used as reference. Of course, the reduction can be greater if precision is sacrificed. However, this would mean limiting the data to be encoded based on these rotations that can be computed more efficiently. Moreover, this possibility will be entirely linked to the degree of freedom that the chosen consensus allows.

6 Conclusions and future work

This paper has presented a review of the state-of-the-art protocols for building a quantum blockchain. Building upon a hypergraph-base blockchain protocol, we have introduced enhancements to the most optimized (in terms of qubits) implementation. By reducing the required resources, our proposed implementations have achieved significant improvements in T-count and T-depth. In the worst case, the proposed improvements halve such values. These results are important for reducing the cost and complexity of constructing a quantum blockchain and enabling the implementation of such protocols with fewer resources. The enhanced implementation has been introduced as part of a protocol that previously had significant limitations and can now be incorporated into more comprehensive protocols, like the one proposed by Li et al. Consequently, the proposed implementation holds considerable promise for future protocols, owing to its cost-effectiveness in terms of both qubits and T-gates. This advancement opens up new possibilities for the development of more efficient and robust quantum protocols.

In addition, we have calculated the cost of using exclusively Clifford+T gates for the implementation of the proposed circuits. While this approach offers the benefits of leveraging established error detection and correction codes, the current expense of converting non-Clifford operations into Clifford+T gates renders it impractical for NISQ (Noisy Intermediate-Scale Quantum) devices. However, by reducing precision, achievable T-count values can be reached that enable the implementation of prototypes of these circuits for reduced block numbers.

Future work will explore the use of rotations in specific ranges to optimize the T-count of the transformation of these rotations to Clifford+T operations. While limiting rotations to a certain range can pose significant safety issues, careful consideration and proper implementation can strike a balance between safety and cost as long as the consensus allows it. It will be essential to delve into the feasibility of such cases and thoroughly investigate the potential repercussions of this limitation. For instance, we need to address security concerns arising from the use of a protocol limited to encoding known sets of values. Can complementary measures strengthen security in such scenarios? Additionally, exploring methods to discretize data for suitable rotations will be an important aspect of our research, warranting further investigation that we leave for future exploration. Overall, our findings open up exciting new avenues for exploring the potential of quantum computing in blockchain technology and pave the way for developing more efficient and secure quantum blockchains in the future.

Declarations

Data Availability

Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Competing interests

The authors declare that they have no competing interests.

Funding

This research has received funding from the Research Council of Lithuania (LMTLT), agreement No. S-MIP-21-53.

References

[1] Orts, F., Ortega, G., Combarro, E.F., Garzón, E.M.: A review on reversible quantum adders. Journal of Network and Computer Applications **170**, 102810 (2020)

[2] Paulavičius, R., Grigaitis, S., Igumenov, A., Filatovas, E.: A decade of blockchain: Review of the current status, challenges, and future directions. Informatica **30**(4), 729–748 (2019)

[3] Wang, C., Li, X., Xu, H., Li, Z., Wang, J., Yang, Z., Mi, Z., Liang, X., Su, T., Yang, C., *et al.*: Towards practical quantum computers: transmon qubit with a lifetime approaching 0.5 milliseconds. npj Quantum Information **8**(1), 1–6 (2022)

[4] Anand, A., Schleich, P., Alperin-Lea, S., Jensen, P.W., Sim, S., Díaz-Tinoco, M., Kottmann, J.S., Degroote, M., Izmaylov, A.F., Aspuru-Guzik, A.: A quantum computing view on unitary coupled cluster theory. Chemical Society Reviews (2022)

[5] Yang, Q., Zhao, Y., Huang, H., Xiong, Z., Kang, J., Zheng, Z.: Fusing blockchain and AI with metaverse: A survey. IEEE Open Journal of the Computer Society **3**, 122–136 (2022)

[6] Sekar, S., Solayappan, A., Srimathi, J., Raja, S., Durga, S., Manoharan, P., Hamdi, M., Tunze, G.B.: Autonomous transaction model for

e-commerce management using blockchain technology. International Journal of Information Technology and Web Engineering (IJITWE) **17**(1), 1–14 (2022)

[7] Fernandez-Carames, T.M., Fraga-Lamas, P.: Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE access **8**, 21091–21116 (2020)

[8] Fedorov, A.K., Kiktenko, E.O., Lvovsky, A.I.: Quantum computers put blockchain security at risk. Nature Publishing Group (2018)

[9] Unogwu, O.J., Doshi, R., Hiran, K.K., Mijwil, M.M.: Introduction to quantum-resistant blockchain. In: Advancements in Quantum Blockchain With Real-Time Applications, pp. 36–55. IGI Global, Pennsylvania, USA (2022)

[10] Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review **41**(2), 303–332 (1999)

[11] Jaques, S., Naehrig, M., Roetteler, M., Virdia, F.: Implementing Grover oracles for quantum key search on AES and LowMC. In: Advances in Cryptology–EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part II 30, pp. 280–310 (2020). Springer

[12] Grimes, R.A.: Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto. John Wiley & Sons, Hoboken, USA (2019)

[13] Li, Q., Wu, J., Quan, J., Shi, J., Zhang, S.: Efficient quantum blockchain with a consensus mechanism QDPoS. IEEE Transactions on Information Forensics and Security **17**, 3264–3276 (2022)

[14] Qu, Z., Zhang, Z., Zheng, M.: A quantum blockchain-enabled framework for secure private electronic medical records in internet of medical things. Information Sciences **612**, 942–958 (2022)

[15] Wang, W., Yu, Y., Du, L.: Quantum blockchain based on asymmetric quantum encryption and a stake vote consensus algorithm. Scientific Reports **12**(1), 1–12 (2022)

[16] Nilesh, K., Panigrahi, P.K.: Quantum blockchain based on dimensional lifting generalized Gram-Schmidt procedure. IEEE Access **10**, 103212–103222 (2022)

[17] Krishnakumar, A.: Quantum Computing and Blockchain in Business: Exploring the Applications, Challenges, and Collision of Quantum Computing and Blockchain. Packt Publishing Birmingham (2020)

[18] Edwards, M., Mashatan, A., Ghose, S.: A review of quantum and hybrid quantum/classical blockchain protocols. Quantum Information Processing **19**(6), 1–22 (2020)

[19] Preskill, J.: Quantum computing in the NISQ era and beyond. Quantum **2**, 79 (2018)

[20] Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press, UK (2011)

[21] Pelofske, E., Bärtschi, A., Eidenbenz, S.: Quantum volume in practice: What users can expect from NISQ devices. arXiv preprint arXiv:2203.03816 (2022)

[22] De Luca, G.: A survey of NISQ era hybrid quantum-classical machine learning research. Journal of Artificial Intelligence and Technology **2**(1), 9–15 (2022)

[23] Wei, S., Chen, Y., Zhou, Z., Long, G.: A quantum convolutional neural network on NISQ devices. AAPPS Bulletin **32**(1), 1–11 (2022)

[24] Endo, S., Cai, Z., Benjamin, S.C., Yuan, X.: Hybrid quantum-classical algorithms and quantum error mitigation. Journal of the Physical Society of Japan **90**(3), 032001 (2021)

[25] Bharti, K., Cervera-Lierta, A., Kyaw, T.H., Haug, T., Alperin-Lea, S., Anand, A., Degroote, M., Heimonen, H., Kottmann, J.S., Menke, T., *et al.*: Noisy intermediate-scale quantum algorithms. Reviews of Modern Physics **94**(1), 015004 (2022)

[26] Thapliyal, H., Muñoz-Coreas, E., Khalus, V.: Quantum circuit designs of carry lookahead adder optimized for T-count, T-depth, and qubits. Sustainable Computing: Informatics and Systems **29**, 100457 (2021)

[27] Lamport, L., Shostak, R., Pease, M.: The byzantine generals problem. In: Concurrency: the Works of Leslie Lamport, pp. 203–226 (2019)

[28] Haber, S., Stornetta, W.S.: How to Time-Stamp a Digital Document. In: Menezes, A.J., Vanstone, S.A. (eds.) Advances in Cryptology-CRYPTO' 90, pp. 437–455. Springer, Berlin, Heidelberg (1991)

[29] Bayer, D., Haber, S., Stornetta, W.S.: Improving the efficiency and

reliability of digital time-stamping. In: Sequences II: Methods in Communication, Security, and Computer Science, pp. 329–334 (1993). Springer

[30] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf (2008)

[31] Filatovas, E., Marcozzi, M., Mostarda, L., Paulavičius, R.: A MCDM-based framework for blockchain consensus protocol selection. Expert Systems with Applications **204**, 117609 (2022)

[32] Bernhardt, C.: Quantum Computing for Everyone. Mit Press, US (2019)

[33] Mohammadi, M., Eshghi, M.: On figures of merit in reversible and quantum logic designs. Quantum Information Processing **8**(4), 297–318 (2009)

[34] Thapliyal, H., Ranganathan, N.: Design of reversible sequential circuits optimizing quantum cost, delay, and garbage outputs. ACM Journal on Emerging Technologies in Computing Systems (JETC) **6**(4), 1–31 (2010)

[35] Orts, F., Ortega, G., Garzón, E.M.: An optimized quantum circuit for converting from sign–magnitude to two's complement. Quantum Information Processing **18**(11), 1–14 (2019)

[36] Tan, Y.-y., Cheng, X.-y., Guan, Z.-j., Liu, Y., Ma, H.: Multi-strategy based quantum cost reduction of linear nearest-neighbor quantum circuit. Quantum Information Processing **17**(3), 1–14 (2018)

[37] Babukhin, D., Pogosov, W.: The effect of quantum noise on algorithmic perfect quantum state transfer on NISQ processors. Quantum Information Processing **21**(1), 1–18 (2022)

[38] Xue, C., Chen, Z.-Y., Wu, Y.-C., Guo, G.-P.: Effects of quantum noise on quantum approximate optimization algorithm. Chinese Physics Letters **38**(3), 030302 (2021)

[39] Orts, F., Ortega, G., Combarro, E.F., Rúa, I.F., Garzón, E.M.: Optimized quantum Leading Zero Detector circuits. Quantum Information Processing **22**(1), 1–17 (2023)

[40] Gayathri, S., Kumar, R., Dhanalakshmi, S., Dooly, G., Duraibabu, D.B.: T-count optimized quantum circuit designs for single-precision floating-point division. Electronics **10**(6), 703 (2021)

[41] Roffe, J.: Quantum error correction: an introductory guide. Contemporary Physics **60**(3), 226–245 (2019)

[42] Muñoz-Coreas, E., Thapliyal, H.: Quantum circuit design of a T-count

optimized integer multiplier. IEEE Transactions on Computers **68**(5), 729–739 (2018)

[43] Paler, A., Polian, I., Nemoto, K., Devitt, S.J.: Fault-tolerant, high-level quantum circuits: form, compilation and description. Quantum Science and Technology **2**(2), 025003 (2017)

[44] Zhou, X., Leung, D.W., Chuang, I.L.: Methodology for quantum logic gate construction. Physical Review A **62**(5), 052316 (2000)

[45] Kliuchnikov, V., Maslov, D., Mosca, M.: Practical approximation of single-qubit unitaries by single-qubit quantum Clifford and T circuits. IEEE Transactions on Computers **65**(1), 161–172 (2015)

[46] Paetznick, A., Svore, K.M.: Repeat-until-success: Non-deterministic decomposition of single-qubit unitaries. arXiv preprint arXiv:1311.1074 (2013)

[47] Forest, S., Gosset, D., Kliuchnikov, V., McKinnon, D.: Exact synthesis of single-qubit unitaries over Clifford-cyclotomic gate sets. Journal of Mathematical Physics **56**(8), 082201 (2015)

[48] Kliuchnikov, V., Maslov, D., Mosca, M.: Fast and efficient exact synthesis of single qubit unitaries generated by Clifford and T gates. arXiv preprint arXiv:1206.5236 (2012)

[49] Zhu, H.: Multiqubit Clifford groups are unitary 3-designs. Physical Review A **96**(6), 062336 (2017)

[50] Bocharov, A., Roetteler, M., Svore, K.M.: Efficient synthesis of universal repeat-until-success quantum circuits. Physical review letters **114**(8), 080502 (2015)

[51] Combaro, E.F., González-Castillo, S.: A Practical Guide to Quantum Machine Learning and Quantum Optimization: Hands-on Approach to Modern Quantum Algorithms. Packt Publishing, United Kingdom (2023)

[52] Younis, E., Sen, K., Yelick, K., Iancu, C.: Qfast: Conflating search and numerical optimization for scalable quantum circuit synthesis. In: 2021 IEEE International Conference on Quantum Computing and Engineering (QCE), pp. 232–243 (2021). IEEE

[53] Gheorghiu, V., Mosca, M., Mukhopadhyay, P.: T-count and T-depth of any multi-qubit unitary. npj Quantum Information **8**(1), 1–10 (2022)

[54] Gheorghiu, V., Mosca, M., Mukhopadhyay, P.: A (quasi-) polynomial time heuristic algorithm for synthesizing T-depth optimal circuits. npj

Quantum Information **8**(1), 1–11 (2022)

[55] Rossi, M., Huber, M., Bruß, D., Macchiavello, C.: Quantum hypergraph states. New Journal of Physics **15**(11), 113022 (2013)

[56] Gühne, O., Cuquet, M., Steinhoff, F.E., Moroder, T., Rossi, M., Bruß, D., Kraus, B., Macchiavello, C.: Entanglement and nonclassical properties of hypergraph states. Journal of Physics A: Mathematical and Theoretical **47**(33), 335303 (2014)

[57] Dutta, S., Sarkar, R., Panigrahi, P.K.: Permutation symmetric hypergraph states and multipartite quantum entanglement. International Journal of Theoretical Physics **58**(11), 3927–3944 (2019)

[58] Qu, R., Wang, J., Li, Z., Bao, Y.: Encoding hypergraphs into quantum states. Physical Review A **87**(2), 022311 (2013)

[59] Kruszynska, C., Kraus, B.: Local entanglability and multipartite entanglement. Physical Review A **79**(5), 052304 (2009)

[60] Tsimakuridze, N., Gühne, O.: Graph states and local unitary transformations beyond local Clifford operations. Journal of Physics A: Mathematical and Theoretical **50**(19), 195302 (2017)

[61] Rajan, D., Visser, M.: Quantum blockchain using entanglement in time. Quantum Reports **1**(1), 3–11 (2019)

[62] Li, C., Xu, Y., Tang, J., Liu, W.: Quantum blockchain: a decentralized, encrypted and distributed database based on quantum mechanics. Journal of Quantum Computing **1**(2), 49 (2019)

[63] Banerjee, S., Mukherjee, A., Panigrahi, P.: Quantum blockchain using weighted hypergraph states. Physical Review Research **2**(1), 013322 (2020)

[64] Mohammadi, M., Eshghi, M.: On figures of merit in reversible and quantum logic designs. Quantum Information Processing **8**(4), 297–318 (2009)

[65] Orts, F., Ortega, G., Garzón, E.M.: Studying the cost of N-qubit Toffoli gates. In: International Conference on Computational Science, pp. 122–128 (2022). Springer

[66] Amy, M., Maslov, D., Mosca, M.: Polynomial-time T-depth optimization of Clifford+ T circuits via matroid partitioning. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **33**(10), 1476–1489 (2014)

[67] Gosset, D., Kliuchnikov, V., Mosca, M., Russo, V.: An algorithm for the T-count. arXiv preprint arXiv:1308.4134 (2013)

[68] Gidney, C.: Halving the cost of quantum addition. Quantum **2**, 74 (2018)