mathematics

MDPI

Article

Design of an Exchange Protocol for the Quantum Blockchain

Alexandru-Gabriel Tudorache

Department of Computer Science and Engineering, "Gheorghe Asachi" Technical University of Iasi, D. Mangeron Street, nr. 27A, 700050 Iasi, Romania; alexandru-gabriel.tudorache@academic.tuiasi.ro

Abstract: This paper explores the idea of a quantum exchange protocol between two entities, validated by (at least) a third one. Two entities, part of a greater system, decide they want to trade quantum goods: their exchange is configurable, and allows them to select the type of good, from a selected preset, and the desired quantity, up to a maximum value (one of the quantum goods can be interpreted as quantum money/a form of quantum currency). Certain qubits should also be used as a way of storing the details of the transfer, after it has been validated (acting in a similar way to a quantum ledger). The quantum circuits of the proposed design are implemented using the Python programming language with the help of Qiskit, IBM's open-source quantum framework.

Keywords: quantum algorithms; quantum blockchain; quantum information processing; quantum simulation

MSC: 81P68

1. Introduction

Over the last years, the quantum research field has become more and more important, as the available quantum processing power has been growing by the year (the article of [1] contains a list of companies that use quantum technology, and also mentions some of its advantages and disadvantages). The ideas and algorithms presented in this field must be approached theoretically and from a practical point of view, thus being correlated with the evolving quantum processors in order to obtain maximum performance, and helping to solve the issues that occur from designing and implementing protocols on such complex devices. We also notice the continuous development of the post-quantum cryptography initiative (see [2] for details), seen from a security perspective: its main objective is to find algorithms that can serve their security purpose when challenged by both classical and quantum devices.

The algorithm introduced in this paper is meant to use the quantum properties as a way of improving the future (quantum) blockchain. The Python implementation, quantum circuits and measurement results describe a concrete way of designing architectures that can be of use in the blockchain universe, and which also respect all of the already discussed properties.

The paper is structured as follows: After a brief introduction to the quantum field in the first section, the second one describes some of the innovations brought on by recent research papers. The third section conceptually presents the proposed algorithm, with the core ideas grouped into three stages, and shows the general diagram. The fourth section illustrates different solutions for the design of the transfer circuit, and analyzes some approaches for its components; it then offers details on the exchange circuit, for which it shows the proposed circuits and presents the measurement results (obtained after the implementation of the code written in the Python programming language and the Qiskit framework; see [3] for details). The fifth section evaluates some parameters of the scheme, simulated on the local machine, and discusses an alternative structure of the exchange circuit, with support for multiple transactions as part of the same exchange; the conclusion is drawn in the last section.

check for updates

Citation: Tudorache, A.-G. Design of an Exchange Protocol for the Quantum Blockchain. *Mathematics* **2022**, *10*, 3986. https://doi.org/10.3390/math10213986

Academic Editor: Dmitry Makarov

Received: 6 October 2022
Accepted: 24 October 2022
Published: 27 October 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

2. Related Work

The blockchain concept refers to a distributed ledger that contains all transactions made between various parties; a certain set of properties is imposed by design (such as security, privacy and transparency), in order to gain and keep the trust of the users. The development of various cryptocurrencies, such as Bitcoin, has made the blockchain more popular nowadays. However, digital currencies are not the only purpose of this technology: it is also used in finance, healthcare, smart contracts, voting and other fields (see [4] for more details regarding the blockchain, its advantages and uses). It is, therefore, of no surprise that, with the emergence of quantum technologies, researchers have approached the problem of how to design protocols that are better able to withstand attacks through the use of quantum properties. In our context, we analyze the quantum blockchain as representing the system that encompasses different free agents, giving them the possibility to execute various trading options; the purpose is to find a new way to design quantum circuits that allows multiple entities to securely trade forms of virtual currencies, which are regarded as quantum goods.

An overview of the cryptographic concepts that allow the blockchain to resist attacks is presented in paper [5], where the most recent post-quantum systems are described, together with their application in the distributed ledger technologies (DLTs); it offers a list of encryption algorithms, digital schemes and comparisons using different metrics. Paper [6] shows a survey that reveals on which layer should the analyzed blockchain solutions be classified: on the data, application and presentation, network, consensus, or infrastructure layer. It is also possible that the evaluated algorithms are not part of the mentioned categories, but present ideas on the DLT topic. Multiple blockchain proposals, together with an analysis of the issues that researchers must keep track of when discussing new algorithms, are presented in paper [7]; these ideas refer to the migration from the pre-quantum concepts to the post-quantum blockchain, the size of the algorithm keys, the energy impact and so on. An analysis of the vulnerabilities of different cryptocurrencies that are built using the blockchain technology is presented in paper [8], with the purpose of obtaining the associated risk in the context of quantum attacks.

The authors of paper [9] present a quantum blockchain that can withstand attacks generated using quantum technology; it is based on quantum asymmetric cryptography and a protocol regarding the stake vote consensus. The blocks are generated using the delegated proof of stake with the node behavior and Borda count; the security property of the transfers is fulfilled with the help of quantum signatures (using quantum one-way functions). Another protocol is presented in paper [10], where in order to achieve a secure way of transmitting data, concepts such as quantum hash, the quantum SWAP test and quantum teleportation are combined. It is resistant by design, and thus, the nature of the attackers' resources is irrelevant (classical and/or quantum). A different approach is considered in paper [11], where the quantum blockchain relies on the entanglement in time, using temporal entangled states, such as the GHZ (Greenberger–Horne–Zeilinger) state; an important advantage is justified by the fact that the physical (experimental) parts of the system have already been implemented for the proposed idea. A way of developing different blockchain techniques can be inspired by paper [12], where the authors describe how the idea from the B92 quantum protocol can be extended and applied to grayscale images; the paper shows how the proposed algorithm allows two entities, Alice and Bob, to select a secret message, and then use it (as a key) for different cryptographic protocols.

An algorithm called MatRiCT is introduced in paper [13], where the authors describe a new blockchain for confidential transactions, using lattice assumptions; this protocol includes a full implementation with the performance of the transactions on a simple computer. Another lattice-based signature scheme is proposed in paper [14], where the keys are obtained using Bonsai Trees with the RandBasis algorithm; the security is analyzed, followed by details for a post-quantum transaction. Other techniques and applications regarding the blockchain can be consulted in papers [15–18].

In terms of using the already existing infrastructure, we would like to mention one of the solutions that builds on the fiber networks in-place across cities in order to achieve secure authentication; this has implications for various applications (see [19] for details). The design of a post-quantum blockchain for smart cities is discussed in paper [20], with a new proof-of-work (PoW) consensus algorithm that can be used for different applications; the authors describe a post-quantum lightweight transaction. The idea of using the blockchain for a scalable smart city is also approached in paper [21], which presents a blockchain framework, and then analyzes multiple candidates of cryptography for the desired goal, such as lattice-based cryptography, quantum key distribution, and quantum entanglement in time. The Internet of Vehicles (IoV) topic is discussed in paper [22], where the authors propose a system based on blockchain technologies; a semi-quantum solution is illustrated, using two lightweight quantum-reflection protocols with unconditional security. The two proposed algorithms apply just two modular exponentiations as the main computational effort. More ideas on the interaction between the blockchain and the Internet of Things (IoT), as well as the IoV, can be found in papers [23–31].

3. Materials and Methods

The aim of the protocol introduced in this paper is to show a practical application of the available quantum tools by offering two parties, belonging to a general quantum system, the possibility to safely and securely trade two quantum goods (per transaction). We chose to use Qiskit, the open-source quantum framework from IBM, as it provides vast documentation for its available functions, as well as allowing the users to test their ideas by designing circuits that can be simulated on the local machine or tested remotely on real devices.

We consider the classical names for two entities, Alice and Bob, who want to engage in a fair trade of their quantum goods (which can be seen as digital assets); their transfer is supervised and validated by a third entity, Charlie, randomly chosen from the other parties. The concept of Charlie's validation as an entity, as well as its circuit implementation, can be extended to cover multiple transfer validators; here, one idea is the presence of multiple entities for each exchange, playing the role of the validators and all part of the system, with each transfer requiring the acceptance of the majority.

We assume that the system is designed for four types of quantum goods, to which we refer to as 0, 1, 2 and 3. Two qubits are needed for the representation of each one of these goods. The transfer between the parties can also be configurable in terms of quantity, allowing for values between 0 and 7; three qubits are required here. The type-0 good, together with the 0 quantity, could be selected as either a gift or as a solution for an exchange requiring multiple goods from at least one party (part of a more complex transaction, such as Alice exchanging 1 × type-1 + 3 × type-2 goods for Bob's 2 × type-3 goods); this idea would require at least one more field, such as a transfer ID, to be able to bind multiple exchanges as part of the same agreed transaction.

If we allocate 2 qubits to represent the type of goods, and 3 qubits for the quantity, then the quantum states of the corresponding qubits for the available types of goods can be mathematically written as:

- type-0, $|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$;
- type-1, $|01\rangle = |0\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$;

- type-2, $|10\rangle = |1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$;
- type-3, $|11\rangle = |1\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$.

The same applies to the quantum states that describe the available quantities; using 3 qubits, they are: $|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle$. The mentioned values (number of qubits for each property) are selected for demonstration purposes; generalized circuits can be created, depending on the properties and needs of the participants in each system.

The algorithm can be broken down into three main stages:

Stage 1/3

At first, Alice and Bob must signal their intention of a quantum exchange to the community (which can be interpreted as a public request to the system); then, randomly selected entities should be informed of an active transfer taking place on a certain shared communication infrastructure and tasked with overseeing the legitimacy of the transaction (therefore, special attention should be given to the state of certain qubits). For simplicity, we discuss the case of only a single validator, Charlie.

A dedicated qubit scheme can be used here, where all participants that want to trade, together with the validators, can be in control of qubits in shared systems; an entity can play either role for multiple trades, but only a single one in an exchange (either a trader or a validator).

A CCNOT gate is used, where the control qubits belong to the two entities that want to trade (Alice and Bob), and the target one belongs to the validator (Charlie). In order to prevent any sort of arrangement between one or both of the trading entities and the validator (basically cheating attempts or system exploits), it would be recommended for the trading parties to set the state of the validation qubits of multiple entities (validators), with the server only designating one (or a couple) for this purpose, unbeknownst to Alice and Bob.

Stage 2/3

The actual configuration of the exchange circuit takes multiple aspects into account, for all the involved entities, as mentioned below:

- To benefit from the choice of using the quantum solution, the qubits which map the actual values for the type of transferred goods, as well as the quantity, have to be first set up in superposition; this is carried out by applying a Hadamard gate on each one; then, NOT gates are added only for the qubits for which the desired state is $|0\rangle$, in order to bring them to the $|1\rangle$ state, which can be further used for CNOT-type gates.
- The system implies using a simple cross-validation mechanism (internal, relative to the trading parties), so that both Alice and Bob can validate the states corresponding to the other party's qubits (using CNOT and CCNOT gates), for the type of good received and its quantity; in other words, they check that their discussed arrangement is the same as the one represented in the quantum circuit, which can be carried out by adding a classical component (resulting in a hybrid system) using a system that publicly posts the NOT gates (and all the gates between the Hadamard gates and the CNOT/CCNOT gates) for that respective transaction. The main idea is for each party to know when the other one's configuration has matched the desired type and quantity (multiple qubits are used for this).
- The protocol uses a method for the system's validation (external, relative to the trading parties); after the circuit is completed, there is a control logic, which connects the internal validation qubits of Alice and Bob to Charlie's transfer validation qubit.

- If there is something wrong regarding the exchange (from Alice's and/or Bob's point of view), then the state of one of the internal validation qubits would be $|0\rangle$, which would further propagate to the external validation entity (and cancel the transfer); depending on the quantum infrastructure, Charlie can check other parameters, such as, for example, making sure that the exchanged goods are on the list of acceptable tradable goods (there could be a ban at a certain point) and, perhaps, are also within a limit (imposing a maximum value for various reasons). This restriction could be especially useful in the scenarios where more qubits are needed for both the type and quantity of the traded quantum goods, with the traders requiring a wider range of values in their exchanges.

Stage 3/3

If everything is in order, the transfer is marked as verified (and completed) to the community by the validator entity (Charlie), with the new (remaining) quantities being updated for the trading parties, and the details of the transfer saved in the public ledger. Alice and Bob are also notified that the transfer was successfully processed.

The algorithm is schematically presented in Figure 1.

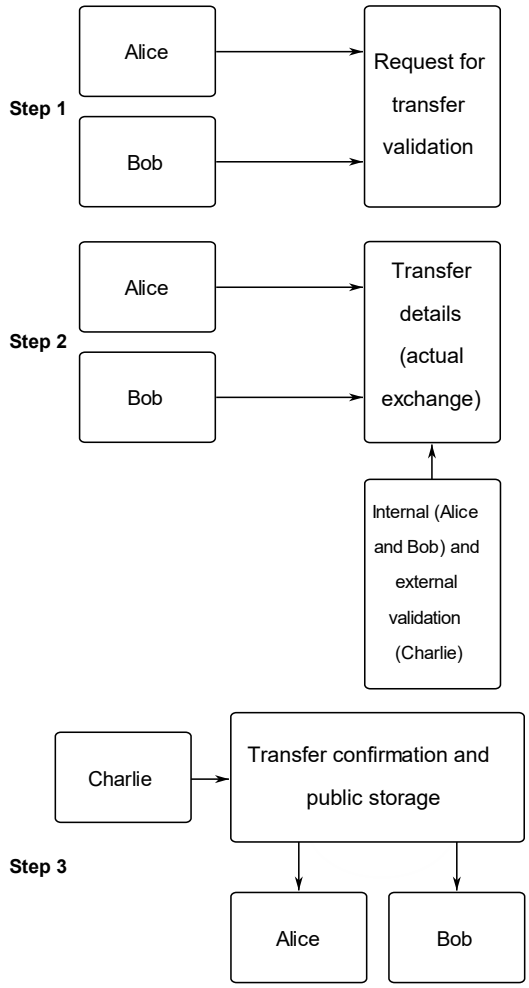

Figure 1. The proposed transfer scheme between Alice and Bob, for the scenario of a single validator (Charlie). *Step 1.* Alice and Bob announce their exchange intent, thus requiring an entity to validate the transfer. *Step 2.* The transfer details are mapped in a quantum circuit, together with the internal and external validation processes. *Step 3.* If everything is in order, the validator entity confirms the transfer details, merging the details into the public ledger.

After the three stages have been completed, the state of each party should be updated accordingly; the different solutions for quantum storage are not included in this paper. One idea for the update process is to use quantum increment and decrement circuits, therefore changing the state of the quantum memory registers of Alice and Bob.

The actual quantum methods used for representing the qubits and interacting with their states vary and depend on the selected quantum infrastructure.

4. Results

4.1. Design of the Transfer Validation Request

The first step in our design is using a gate or set of gates that can act as a validation request; one such relatively intuitive design, initiated by Alice and Bob, is simply simulated using a CCNOT gate, as shown in Figure 2. The circuit presented here, where the target qubit belongs to Charlie, can be extended to multiple validators (which is highly recommended for real applications), either directly or by first replicating this circuit and then adding a dedicated logic for the majority decider. This greatly contributes to the security component of the scheme, as the probability of multiple entities (at least half of the network members) being compromised is much lower than the error/compromise probability of a single member of the system.

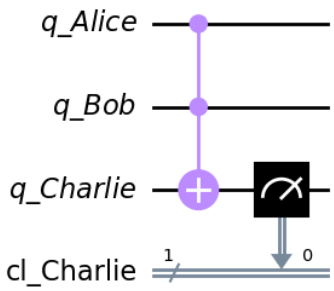

Figure 2. A simple validation circuit for the transfer request, using a CCNOT gate. The algorithm implies the existence of a dedicated quantum channel, which links Alice's and Bob's request qubits (*q_Alice* and *q_Bob*) to Charlie's qubit (*q_Charlie*), which is a generic party, randomly selected as validator.

Before going in depth regarding the actual transfer circuit, we describe the architecture of a potential validation solution with multiple users from the system.

We assume that our system has a total number of N users. In this scenario, it is necessary for each user to have qubits connected to all the other users (thus, $N-1$ qubits each) for the validation purpose. In each validation circuit, for the proposed notation, the indexes show the owner of the qubit and to whom it is addressed; for example, the $q\_user\_x_y$ qubit indicates that this qubit belongs to user x and is used in the validation circuit of user y.

We can, therefore, use the following notations to indicate the validation qubits:

- The first user, $user\_1$ shares the following $N-1$ validation qubits: $q\_user\_1_2$, $q\_user\_1_3, \ldots$ $q\_user\_1_N$
- The second user, $user\_2$, shares the following $N-1$ validation qubits: $q\_user\_2_1$, $q\_user\_2_3, \ldots q\_user\_2_N$ and so on for each user.

The output of each validation block—*q_Charlie* from Figure 2, to which we refer to generically as *q_val_i*, where *i* indicates the user who owns the validation qubit—is connected to a quantum addition circuit (paper [32] describes a solution for this goal). This circuit will take all the validation qubits as input, add them up and generate the total number of passed validations (the sum of their values). The resulting quantum state will be further used as input for a quantum comparator, alongside a quantum register corresponding to the value that indicates half of the users (rounded to $\left\lceil \frac{N}{2} \right\rceil$). A design for

the quantum comparator is proposed in paper [33]. The output of the comparator (we refer to this qubit as q_comp, which is initially set to the $|0\rangle$ state) can be interpreted as follows:

$$q\_comp = \begin{cases} |0\rangle, \ if \ less \ than \ \left\lceil \frac{N}{2} \right\rceil \ users \ validated \ the \ transfer; \\ |1\rangle, \ if \ at \ least \ \left\lceil \frac{N}{2} \right\rceil \ users \ validated \ the \ transfer. \end{cases}$$

The expressed ideas can be summarized in Figure 3, where we show the validation design of a transfer between two users, *user*_1 and *user*_2. Each validation block can be implemented using the circuit described in Figure 2. There are $(N-2)$ validation blocks, one for each of the other users, and these qubits serve as input to the quantum addition circuit. The result of this circuit is represented by p qubits, $res_{p-1}res_{p-2} \ \ldots \ res_0$, whereas the value of $\left\lceil \frac{N}{2} \right\rceil$ would require one less qubit (generically written on k qubits as $aux_{k-1}aux_{k-2} \ \ldots \ aux_0$) being used as the other input for the quantum comparator.

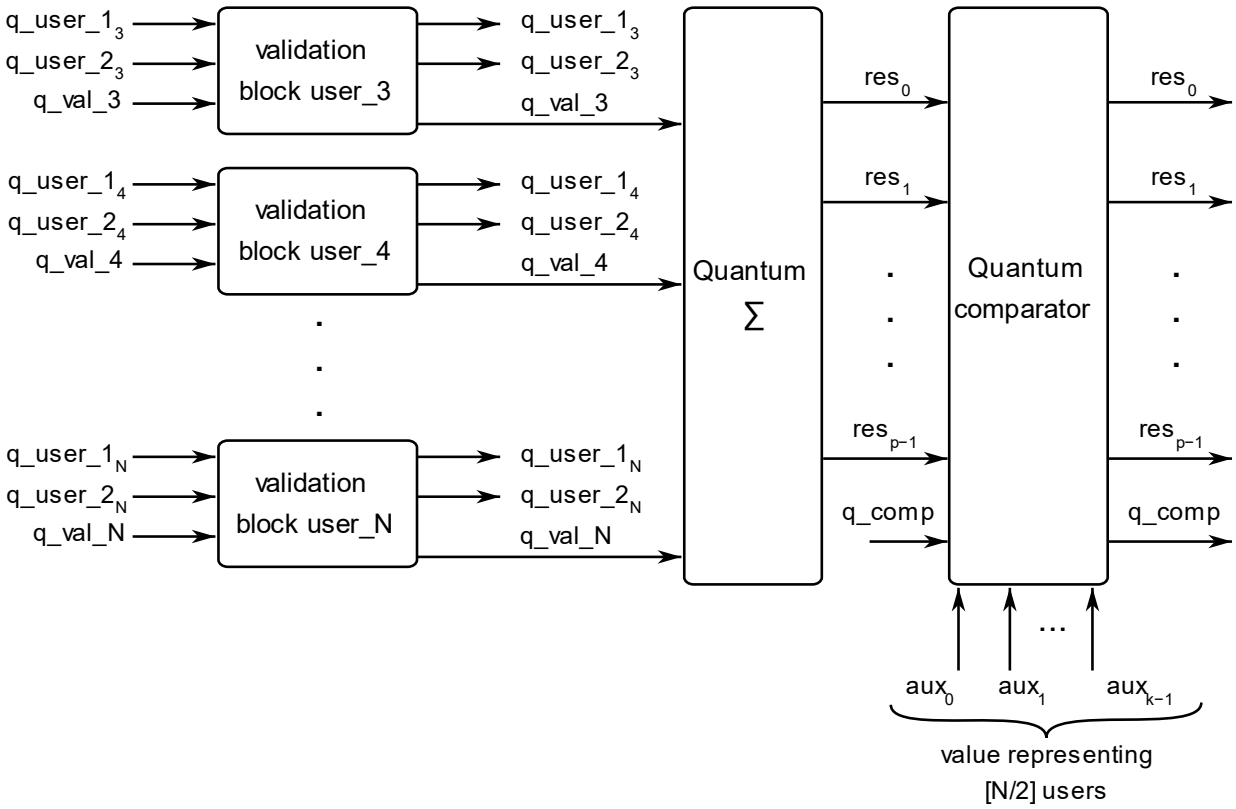

Figure 3. Schematic of the validation process for a transfer between *user_1* and *user_2*.

We also present the design of the quantum addition circuit, which is made up of multiple increment circuits; more specifically, we require a number of $(N-2)$ increment blocks, each one being controlled by the result of the validation block from the users (namely, the q_val_i qubits). After applying the addition block, the *res* vector will hold the sum of the q_val_i states, and this can be mathematically written as follows:

$$\sum_{i=3}^{N} q\_val\_i = res_{p-1}res_{p-2} \ \ldots \ res_0.$$

This is illustrated in Figure 4, where each qubit res_i, with $i = \overline{3, N}$, is initially set to $|0\rangle$ (the circuit is adapted from the one proposed in [32]); we are activating the increment option with each of the q_val_i qubits (if the validator agreed on the transfer).

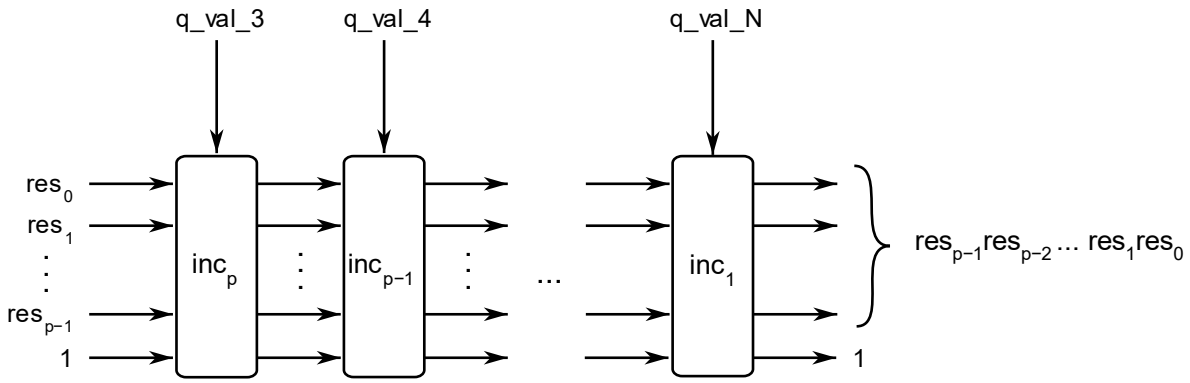

Figure 4. The design of the quantum addition circuit.

This validation solution has the advantage of taking into account the majority's opinion of the transaction; the more users the system has, the less likely there will be a compromise of any transfer. The validation blocks from Figure 3 can be improved (or changed), depending on the generalization of the system that is required. The architecture can also be modified to take into account the validation qubits from fewer users (or from randomly chosen users) for each transfer. Although a significant number of qubits is required to create connections between the validation qubits of all the participants, the proposed design provides a decent level of security; another option here is the configuration of multiple proxies that can perform the validation role for groups of users, thus reducing the qubit cost; in this case, we have to accept lowering the security component.

A different idea for the validation system can be explored by the voting algorithm described in paper [34], where the authors present a way in which grayscale images can be used to hide and decide a winner in a voting context, illustrating the necessary circuits and their measurement results. The mentioned article combines the least significant bit (LSB) technique with the novel enhanced quantum representation of images (NEQR, see [35] for details). This part of the architecture could be modified depending on the requirements and scale of the actual system and its implementation. A special algorithm can be used to randomly select only a certain number of users for the validation component, making sure the performance of the system is not affected; this implies the reconfiguration of the second input of the quantum comparator, in order to reflect this choice.

4.2. Design of the Exchange Circuit

In this section, we discuss the configuration of the exchange circuit: once the validator is informed of the transfer intent of Alice and Bob, Charlie takes note of the transfer details, presented in the circuit from Figure 5.

In this configuration, all qubits are at first in the $|0\rangle$ state. Then, we set the qubits indicating Alice's and Bob's type of goods and quantity in the superposition (a Hadamard gate is applied on each of them). Then, on each group of qubits we act with a potential set of NOT gates; the idea is that we want to obtain the desired (corresponding) values for the particular transfer. Another layer of NOT gates that mirrors the first one is applied at the end. We configure the qubits' state for the scenario of Alice transferring three goods of type-1 to Bob, who sends five goods of type-2; the NOT gates in the initial layer are added for the qubits that correspond to bits of 0 in the binary representation of each particular value.

The transfer circuit in this situation contains the following 16 qubits, some grouped into qubit registers:

- A 2-qubit register is used for the type of good that Alice trades (*q_AliceType*).
- A 3-qubit register indicates the quantity of Alice's good (*q_AliceQuantity*).
- A 2-qubit register is used for the type of good that Bob trades (*q_BobType*).
- A 3-qubit register indicates the quantity of Bob's good (*q_BobQuantity*).

- Then, 4 validation qubits are needed: *q_BobTypeVal*, *q_BobQtyVal*, *q_AliceTypeVal* and *q_AliceQtyVal*; for example, the validation qubit that indicates to Bob that he will receive the desired type of good from Alice is *q_BobTypeVal*, and its state is set using a CCNOT gate, where the control qubits are those indicating Alice's type. The same applies to all the validation qubits from the circuit.
- Finally, 2 auxiliary qubits are also present: when more than 2 qubits are needed to represent the actual value (for the quantity or type), auxiliary qubits are also used (the design requires CCNOT gates for the validation qubits); in our case, we need one ancilla qubit for each entity, called *q_BobAux* and *q_AliceAux*, since we need 3 qubits to represent each quantity for Alice and Bob.

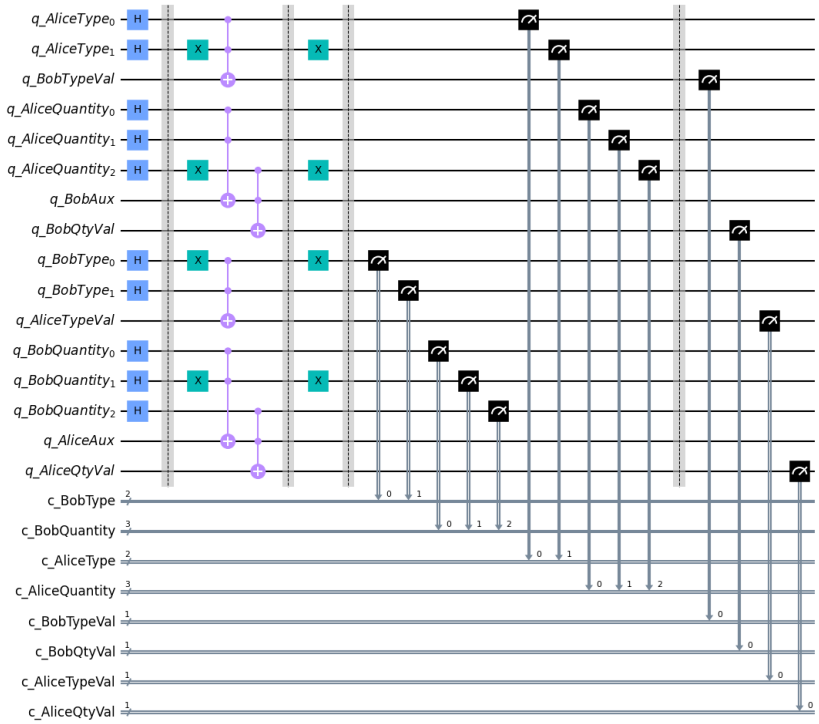

Figure 5. The quantum circuit that reflects the exchange between Alice and Bob. If Alice's qubits are in the $|1\rangle$ state (after the Hadamard and first layer of NOT gates), then the validation qubits of Bob will be set to $|1\rangle$, and vice versa.

The results obtained after simulating the circuit illustrated in Figure 5 are shown in the probability histogram from Figure 6, which contains the zoomed-in version of the results; the full version contains 2^{10} entries (there are 10 qubits in superposition), and thus, it is difficult to visualize all the results. The theoretical probability is $\frac{1}{2^{10}} = 0.00097$, and is also what we obtained in our experiment.

The main state to check here is the one collapsed in the last column, for which we can formally write as follows:

- $q\_AliceQtyVal\ q\_AliceTypeVal\ q\_BobQtyVal\ q\_BobTypeVal = 1111$;
- $q\_AliceQuantity = 011$ (three goods);
- $q\_AliceType = 01$ (type-1);
- $q\_BobQuantity = 101$ (five goods);
- $q\_BobType = 10$ (type-2).

This result confirms that the collapsed state of the validation qubits for Alice and Bob (both quantity and value) is 1111 only for the desired exchange: 3 $\times$ type-1 goods sent from Alice, who receives 5 $\times$ type-2 goods from Bob.

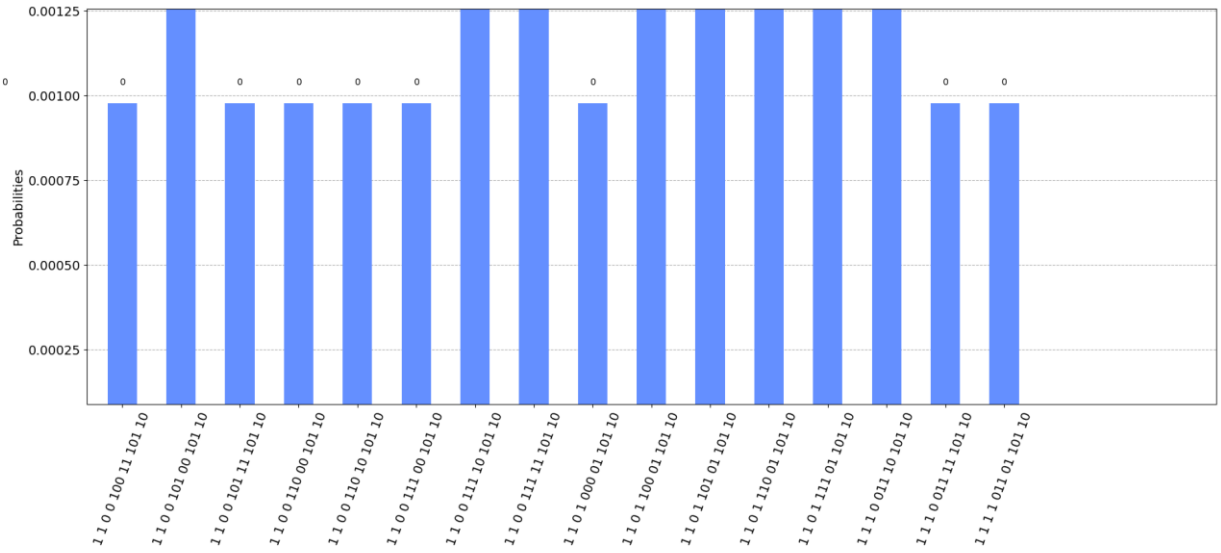

Figure 6. Probability histogram for the exchange circuit (zoomed-in).

5. Analysis and Discussion

For a circuit such as the one described in Figure 5, using 16 qubits, the following quantum gates are needed:

- Ten initial Hadamard gates (depending on the system, this number can obviously vary, as it is in direct correlation with the type and quantity of exchanged goods).
- Eight NOT gates (for the particular case of three type-1 goods traded for five type-2 goods); for a more complex scenario involving more trades between the same parties, the number of NOT gates will have to be selected according to the actual values).
- Six CCNOT gates; the more qubits that are used for the type and quantity, the more CCNOT gates will be needed to connect them to the validation qubits.

The number of auxiliary qubits also varies depending on the number of the types and maximum quantity.

The simulation was performed on the local machine, with an i9-9900K processor at a base speed of 3.60 GHz (and a maximum frequency during the simulation of 4.90 GHz), using 1024 shots (program runs). Using a public memory profiler tool (a module written in Python), we obtained the required memory needed to simulate the circuit and to represent the probability histogram: it is just above 200 MiB (206.2 MiB). The average simulation time on this machine is 0.914 s.

One important concept that should be noticed in the proposed algorithm is the way in which we use the quantum properties in order to improve the performance of the circuits.

The initial superposition of the users' type and quantity qubits could be used to allow us to configure multiple transfers using the same qubits, in a similar way to the quantum image representation technique called NEQR. This would work for transactions of different characteristics (at least a different type of a different quantity). Basically, each set of gates, such as the one described in Figure 5, represents one transfer between the entities and could be followed by subsequent exchanges, allowing for an increase in the actual items that are exchanged between the parties (another set of NOT gates is necessary for this purpose, mirroring the first one, after each transfer). This would also mean that the validation entities have to check not only one transaction at a time, but the whole group of exchanges between two entities, therefore allowing for a better structure and visibility regarding the ledger, as well as a way of keeping together the past transfers between two specific entities (around a certain timestamp).

Another solution (a variation on the ideas presented in Section 3) for the exchange circuit is the integration of a quantum transfer id in the circuit design, indicating either a global transaction identifier (and requiring a unique id, which poses its own problems in

terms of scaling), or just a local id between Alice and Bob for a series of minor exchanges, part of a group transfer of multiple items.

For demonstration purposes, we analyze the scenario of a maximum of four transactions per exchange; this means that 2 qubits will be required to indicate the transfer id local to Alice and Bob. In this case, the transfer id will serve the role of an index, rather than the one of a unique id. As a future extension idea, this id could be made global, but a much higher number of qubits (to represent it, together with auxiliary qubits) and connections (to link the final ancilla id qubit to all the other users) would be required. This circuit is shown in Figure 7.

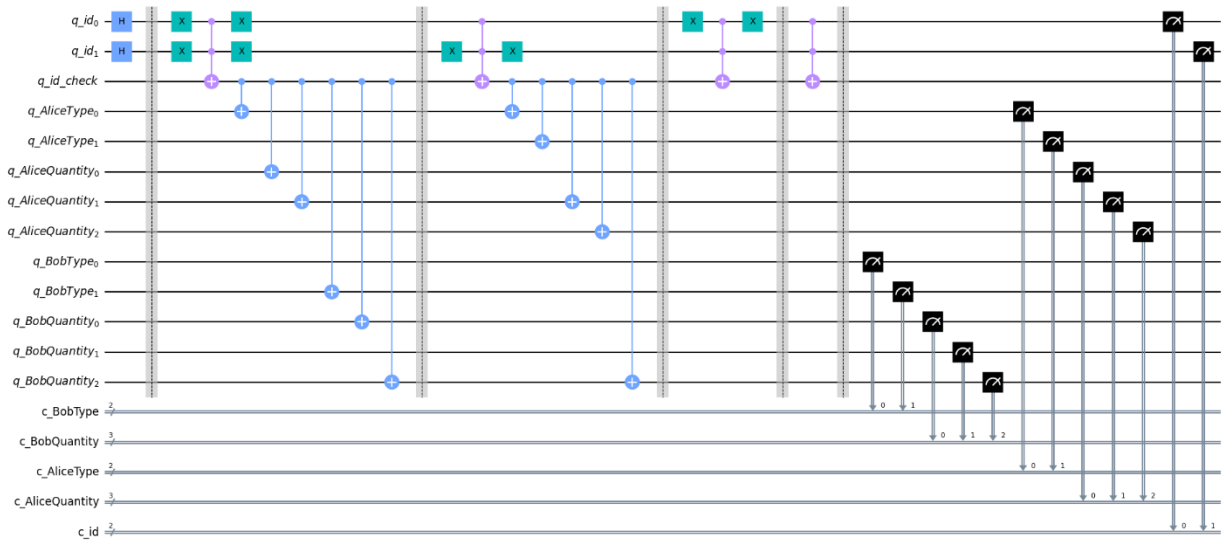

Figure 7. The alternative circuit for a series of transactions between Alice and Bob, using a local identifier.

For this circuit, we notice the fact that Alice's and Bob's type and quantity qubits are no longer set in superposition; the two identifier qubits (q_id_0 and q_id_1) are the only ones on which we apply Hadamard gates, in a similar way that we apply Hadamard gates on the position qubits in the NEQR representation. A single ancilla qubit, *q_id_check*, is set to the $|1\rangle$ state using a CCNOT gate when the id qubits are in the $|1\rangle$ state (thus, NOT gates are applied on them for the $|0\rangle$ state). This qubit sets the corresponding state for Alice's and Bob's qubits for each particular transaction. Each section between the barriers represents a transaction, and by measuring, we know the transfer id in relation to the actual configuration of the exchanged goods. The exchange circuit from Figure 7 contains two transactions:

- For the first transaction, with the collapsed id state of $q\_id_1 q\_id_0 = 00$, Alice trades three goods of type-1 for Bob's five goods of type-2;
- For the second transaction, with the collapsed id state of $q\_id_1 q\_id_0 = 01$, Alice trades six goods of type-3 for Bob's four goods of type-0;
- The other two transactions are left blank.

The measurement results are shown in the probability histogram from Figure 8. We notice the expected results, each with a probability of 25%. After simulating the circuit, a third entity (validator) can easily see the transferred goods for each transaction. The issue for this scenario is finding a secure way to configure the links between the *q_id_check* qubit and the other qubits. Unlike the first proposed method, where the parties can set the states for their qubits and have a validation qubit for each of the other party's data, here there would have to be a way for Alice and Bob to link their qubits to the *q_id_check* qubit; a solution for this problem should be searched at a physical level of the quantum infrastructure and is beyond the scope of this article.

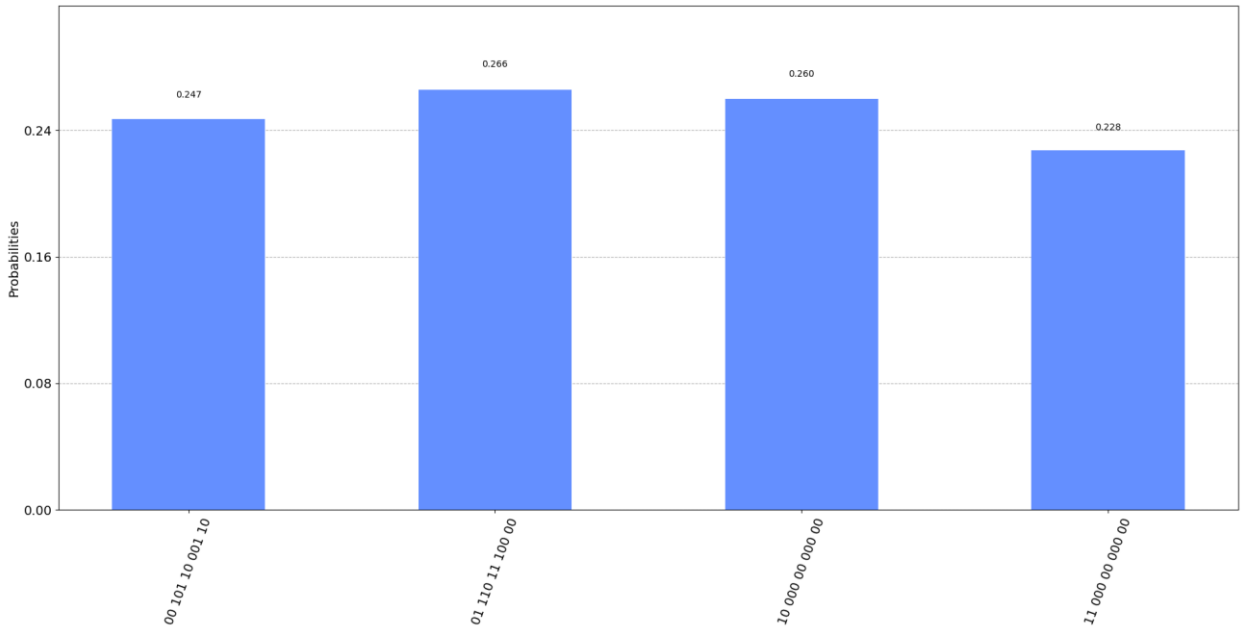

Figure 8. The probability histogram for the alternative exchange circuit.

6. Conclusions

This paper shows a new way in which quantum technologies can be used in the quantum blockchain context. A protocol is proposed, which shows how two entities, Alice and Bob, can exchange virtual goods; the described quantum circuits present the required qubits and operations, allowing for the transfer to be configurable in terms of quantity and type of selected goods. The algorithm has two parts; the first approaches a general architecture for the validation request, using a comparator and a quantum addition circuit, together with multiple validation subcircuits. The second part focuses on the actual exchange circuit, and analyzes its performance. An alternative version, inspired by the ideas from the NEQR image representation, is also presented and simulated; the circuits are implemented using the Qiskit framework and their simulation results are illustrated and discussed. The ideas described in this paper can be used in a future implementation of the quantum blockchain, which will add another layer of security and speed up the classical versions by utilizing the rapid development of the quantum processors.

Potential applications of the presented ideas can be targeted toward society constructs that require clear and public (transparent) exchanges between different entities, such as cryptocurrency platforms, internal banking validations, voting systems, distributed processing algorithms (using the cloud for logging and data management), various applications on the topic of smart cities and so on.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Dungey, T.; Abdelgaber, Y.; Casto, C.; Mills, J.; Fazea, Y. Quantum Computing: Current Progress and Future Directions. EDUCAUSE. 2022. Available online: https://er.educause.edu/articles/2022/7/quantum-computing-current-progress-and-future-directions (accessed on 1 October 2022).
2. Post-Quantum Cryptography PQC | CSRC, NIST. Available online: https://csrc.nist.gov/Projects/post-quantum-cryptography (accessed on 1 October 2022).
3. Qiskit, Open-Source Quantum Development. Available online: https://qiskit.org (accessed on 1 October 2022).
4. Hayes, A. What Is a Blockchain? Investopedia. 2022. Available online: https://www.investopedia.com/terms/b/blockchain.asp (accessed on 1 October 2022).

5. Fernández-Caramès, T.M.; Fraga-Lamas, P. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access* **2020**, *8*, 21091–21116. [CrossRef]
6. Faridi, A.R.; Masood, F.; Shamsan, A.H.T.; Luqman, M.; Salmony, M.Y. Blockchain in the Quantum World. *arXiv* **2022**, arXiv:2202.00224. [CrossRef]
7. Khalid, Z.M.; Askar, S. Resistant Blockchain Cryptography. *Int. J. Sci. Bus.* **2021**, *5*, 116–125.
8. Kearney, J.J.; Perez-Delgado, C.A. Vulnerability of blockchain technologies to quantum attacks. *Array* **2021**, *10*, 100065. [CrossRef]
9. Wang, W.; Yu, Y.; Du, L. Quantum blockchain based on asymmetric quantum encryption and a stake vote consensus algorithm. *Sci. Rep.* **2022**, *12*, 8606. [CrossRef]
10. Wen, X.J.; Chen, Y.Z.; Fan, X.C.; Yi, Z.Z.; Jiang, Z.L.; Fang, J.B. Quantum blockchain system. *Mod. Phys. Lett. B* **2021**, *35*, 2150343. [CrossRef]
11. Rajan, D.; Visser, M. Quantum Blockchain Using Entanglement in Time. *Quantum Rep.* **2019**, *1*, 3–11. [CrossRef]
12. Tudorache, A.-G.; Manta, V.; Caraiman, S. Quantum steganography based on the B92 quantum protocol. *Mathematics* **2022**, *10*, 2870. [CrossRef]
13. Esgin, M.F.; Zhao, R.K.; Steinfeld, R.; Liu, J.K.; Liu, D. MatRiCT: Efficient, scalable and post-quantum blockchain confidential transactions protocol. In Proceedings of the ACM Conference on Computer and Communications Security 2019, London, UK, 11–15 November 2019; pp. 567–584.
14. Li, C.-Y.; Chen, X.-B.; Chen, Y.-L.; Hou, Y.-Y.; Li, J. A New Lattice-Based Signature Scheme in Post-Quantum Blockchain Network. *IEEE Access* **2019**, *7*, 2026–2033. [CrossRef]
15. Banerjee, S.; Mukherjee, A.; Panigrahi, P.K. Quantum blockchain using weighted hypergraph states. *Phys. Rev. Res.* **2020**, *2*, 013322. [CrossRef]
16. Sharma, P.; Bhatia, V.; Prakash, S. Securing Optical Networks using Quantum-secured Blockchain: An Overview. *arXiv* **2021**, arXiv:2105.10663.
17. Abulkasim, H.; Mashatan, A.; Ghose, S. Quantum-based privacy-preserving sealed-bid auction on the blockchain. *Optik* **2021**, *242*, 167039. [CrossRef]
18. Azzaoui, A.E.; Sharma, P.K.; Park, J.H. Blockchain-based delegated Quantum Cloud architecture for medical big data security. *J. Netw. Comput. Appl.* **2022**, *198*, 103304. [CrossRef]
19. Kiktenko, E.O.; Pozhar, N.O.; Anufriev, M.N.; Trushechkin, A.S.; Yunusov, R.R.; Kurochkin, Y.V.; Lvovsky, A.; Fedorov, A.K. Quantum-secured blockchain. *Quantum Sci. Technol.* **2018**, *3*, 035004. [CrossRef]
20. Chen, J.; Gan, W.; Hu, M.; Chen, C.M. On the construction of a post-quantum blockchain for smart city. *J. Inf. Secur. Appl.* **2021**, *58*, 102780. [CrossRef]
21. Azzaoui, A.E.; Park, J.H. Post-quantum blockchain for a scalable smart city. *J. Internet Technol.* **2020**, *21*, 1171–1178.
22. Zhu, H.; Wang, X.; Chen, C.M.; Kumari, S. Two novel semi-quantum-reflection protocols applied in connected vehicle systems with blockchain. *Comput. Electr. Eng.* **2020**, *86*, 106714. [CrossRef]
23. Yi, H. Secure Social Internet of Things Based on Post-Quantum Blockchain. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 950–957. [CrossRef]
24. Gupta, D.S.; Karati, A.; Saad, W.; da Costa, D.B. Quantum-Defended Blockchain-Assisted Data Authentication Protocol for Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2022**, *71*, 3255–3266. [CrossRef]
25. Younan, M.; Elhoseny, M.; Ali, A.A.; Houssein, E.H. Quantum Chain of Things (QCoT): A New Paradigm for Integrating Quantum Computing, Blockchain, and Internet of Things. In Proceedings of the 2021 17th International Computer Engineering Conference (ICENCO), Cairo, Egypt, 29–30 December 2021; pp. 101–106.
26. Shahid, F.; Khan, A.; Jeon, G. Post-quantum distributed ledger for internet of things. *Comput. Electr. Eng.* **2020**, *83*, 106581. [CrossRef]
27. Zhu, Q.; Loke, S.W.; Trujillo-Rasua, R.; Jiang, F.; Xiang, Y. Applications of distributed ledger technologies to the internet of things: A survey. *ACM Comput. Surv.* **2019**, *52*, 1–34. [CrossRef]
28. Suhail, S.; Hussain, R.; Khan, A.; Hong, C.S. On the Role of Hash-Based Signatures in Quantum-Safe Internet of Things: Current Solutions and Future Directions. *IEEE Internet Things J.* **2021**, *8*, 1–17. [CrossRef]
29. Stebila, D.; Mosca, M. Post-quantum key exchange for the internet and the open quantum safe project. In *Selected Areas in Cryptography—SAC 2016*; Avanzi, R., Heys, H., Eds.; Springer: Cham, Switzerland, 2017; Volume 10532, pp. 14–37.
30. Nguyen, T.; Tran, N.; Loven, L.; Partala, J.; Kechadi, M.T.; Pirttikangas, S. Privacy-aware blockchain innovation for 6G: Challenges and opportunities. In Proceedings of the 2020 2nd 6G Wireless Summit (6G SUMMIT), Levi, Finland, 17–20 March 2020; pp. 1–5.
31. Suhail, S.; Hussain, R.; Jurdak, R.; Hong, C.S. Trustworthy digital twins in the industrial internet of things with blockchain. *IEEE Internet Comput.* **2022**, *26*, 58–67. [CrossRef]
32. Kaye, P. Reversible addition circuit using one ancillary bit with application to quantum computing. *arXiv* **2004**, arXiv:quant-ph/0408173v2.
33. Xia, H.; Li, H.; Zhang, H.; Liang, Y.; Xin, J. Novel multi-bit quantum comparators and their application in image binarization. *Quantum Inf. Process.* **2019**, *18*, 229. [CrossRef]

34. Tudorache, A.-G.; Manta, V.; Caraiman, S. Integration of a Quantum Voting Scheme into Grayscale Images Using the Novel Enhanced Quantum Representation and Qiskit Framework. *Model. Simul. Eng.* **2022**, *2022*, 8128754. [CrossRef]
35. Zhang, Y.; Lu, K.; Gao, Y.; Wang, M. NEQR: A novel enhanced quantum representation of digital images. *Quantum Inf. Process.* **2013**, *12*, 2833–2860. [CrossRef]