2023 Congress in Computer Science, Computer Engineering, &amp; Applied Computing (CSCE) | 979-8-3503-2759-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/CSCE60160.2023.00273

A Quantum Teleportation Protocol Secured by a Blockchain Technology

Jaylin Butts
Department of Computer Science
Winston-Salem State University
Winston-Salem, NC, USA
jbutts120@rams.wssu.edu

Emmanuel White
Department of Computer Science
Winston-Salem State University
Winston-Salem, NC, USA
ewhite123@rams.wssu.edu

Jinsuk Baek
Department of Computer Science
Winston-Salem State University
Winston-Salem, NC, USA
baekj@wssu.edu

***Abstract*—A quantum computer can be defined as a computer that implements high-speed calculations by actively utilizing the unique physical states of quantum mechanics. The unique physical states include superposition and quantum entanglement. Quantum computing takes advantage of these states to achieve greater computational power than traditional computing. One important application of quantum computing is quantum teleportation, which enables the transmission of a quantum bit (qubit) between communication entities using measurement-based calculations. However, since the transmission of measured data still relies on traditional communication channels, there can be a security issue, which could pose a potential obstacle to the widespread use of quantum teleportation in the future. In our paper, we propose enhancing the security of legacy quantum teleportation protocol by incorporating blockchain technology.**

Keywords— quantum computing, teleportation, blockchain, entanglement

I. Introduction

In recent years, quantum computing has emerged as a groundbreaking development in the computational sciences. Among the many fascinating aspects of quantum computing, quantum teleportation demonstrates a unique position. It showcases the impressive potential of quantum communication by employing the fundamental principles of quantum mechanics for transmitting quantum states over vast distances.

However, quantum systems are easily disrupted by environmental influences and the measurement process itself. Ensuring the integrity of the transferred quantum state, a key requirement for successful quantum teleportation, remains a significant hurdle. Traditional security approaches, while effective in classical contexts, are often inadequate for protecting quantum information. This deficiency highlights the need for a more resilient security solution.

We consider blockchain technology as an innovative and promising candidate for strengthening the security aspects of quantum teleportation. The inherent security attributes of blockchain, a decentralized, tamper-proof ledger system, could be applied to enhance the reliability and authenticity of quantum teleportation procedures. In this paper, we propose a novel approach of integrating blockchain technology into quantum teleportation to improve the security and verification processes of quantum state transfers.

We believe this pioneering work can help address current security weaknesses in quantum teleportation and contribute to the development of more secure quantum networks. The following sections will provide an in-depth understanding of quantum teleportation mechanics, explore the motivations for incorporating blockchain technology into quantum teleportation, and demonstrate how this technology can be practically applied. We will conclude with potential future research directions to continue this innovative work.

II. Quantum Teleportation

In quantum computing, the elementary unit of information is a qubit, a quantum system that can exist in a superposition of |0> and |1> states simultaneously. The state of a qubit, $|\Psi>$, is represented as follows using complex numbers α and β.

$$|\Psi> = \alpha|0> + \beta|1> = \begin{pmatrix}\alpha \\ \beta\end{pmatrix} \tag{1}$$

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2}$$

That is, the state of a qubit, $|\Psi>$, can be represented as a linear combination of two basis vectors, |0> and |1>, which is called a superposition state. Here, the complex numbers α and β are subjected to the condition that the sum of the squares of their absolute values is 1 since they are considered as complex amplitudes. Also, $|\alpha|^2$ and $|\beta|^2$ represent the measurement probabilities of |0> and |1>, respectively, according to Born's rule [1]. An equal superposition state of |0> and |1> can be represented as

$$|\Psi> = \frac{1}{\sqrt{2}}|0> + \frac{1}{\sqrt{2}}|1> = \begin{pmatrix}\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}}\end{pmatrix} \tag{3}$$

In Equation (3), the measurement probabilities of |0> and |1> are equally 50%. The squared magnitudes of their corresponding complex amplitudes are equal to 1/2.

Let us now examine the scenario setup for quantum teleportation [2], as illustrated by the quantum circuit in Fig. 1. There are two communication entities, *A* and *B*, both initially in state |0>. Entity *A* possesses a superposition quantum state, $|\Psi>$, which it wishes to transmit to *B*.

Since multiple qubits are typically represented using the tensor product, $\otimes$, the initial state of the three qubits can be denoted as:

$$|\text{state } 0> = |\Psi> \otimes |0> \otimes |0>$$

979-8-3503-2759-5/23/$31.00 ©2023 IEEE
DOI 10.1109/CSCE60160.2023.00273

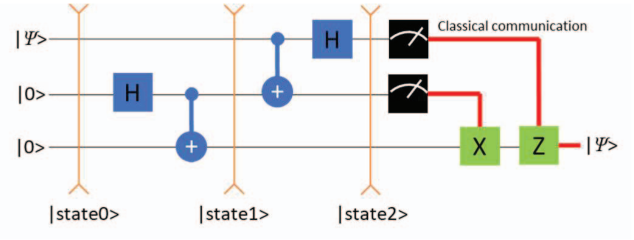

Fig. 1. Quantum circuit for quantum teleportation

To enable the transmission of |*Ψ*>, *A* and *B* shares a quantum entanglement state [3] created through the application of an Hadamard (H) gate to *A*'s initial state, followed by a CNOT gate for *A* and *B*. In other words, the outputs of the H gate serve as the control bit for the CNOT gate. This entanglement state can be established directly by *A* and *B*, or created and distributed to them by a trusted third party. After this step, *A* and *B* can be separated by any distance. The overall quantum state, |state 1>, at this point is as follows:

$$
\begin{aligned}
|\text{state } 1> &= \mathrm{CNOT}_{2,3}\ \mathrm{H}_2\ |\text{state } 0> \\
&= \mathrm{CNOT}_{2,3}\ \mathrm{H}_2\ (|\mathit{\Psi}> \otimes |0> \otimes |0>) \\
&= \mathrm{CNOT}_{2,3}\ (|\mathit{\Psi}> \otimes \mathrm{H}|0> \otimes |0>) \\
&= \mathrm{CNOT}_{2,3}\ (|\mathit{\Psi}> \otimes \frac{|0> +|1>}{\sqrt{2}} \otimes |0>) \\
&= \mathrm{CNOT}(|\mathit{\Psi}> \otimes \frac{|00> +|10>}{\sqrt{2}}) \\
&= |\mathit{\Psi}> \otimes (\mathrm{CNOT}\ \frac{|00> +|10>}{\sqrt{2}}) \\
&= |\mathit{\Psi}> \otimes \frac{|00> +|11>}{\sqrt{2}} \\
&= \frac{\alpha|0> \otimes (|00> +|11>) + \beta|1> \otimes (|00>+|11>)}{\sqrt{2}} \\
&= \frac{\alpha(|000> + |011>) + \beta(|100> + |111>)}{\sqrt{2}}
\end{aligned}
$$

Note that the subscript of the quantum gate indicates which qubit it is applied to. It now applies CNOT gate to the first and second qubits, and apply the H gate to the first qubit as shown in Fig. 1. After this step, we can have a new overall quantum state, |state 2>.

$$
\begin{aligned}
|\text{state } 2> &= \mathrm{H}_1\mathrm{CNOT}_{1,2}|\text{state } 1> \\
&= \mathrm{H}_1\mathrm{CNOT}_{1,2}\ \frac{\alpha(|000> + |011>) + \beta(|100> + |111>)}{\sqrt{2}} \\
&= \mathrm{H}_1\ \frac{\alpha(|000> + |011>) + \beta(|110> + |101>)}{\sqrt{2}} \\
&= \frac{\alpha(\frac{|0>+|1>}{\sqrt{2}}|00> + \frac{|0>+|1>}{\sqrt{2}}|11>) + \beta(\frac{|0>-|1>}{\sqrt{2}}|10> + \frac{|0>-|1>}{\sqrt{2}}|01>)}{\sqrt{2}} \\
&= \alpha\left(\frac{|000>+|100>}{2} + \frac{|011>+|111>}{2}\right) \\
&\quad +\beta(\frac{|010>-|110>}{2} + \frac{|001>-|101>}{2}) \\
&= \frac{1}{2}|00>(\alpha|0> + \beta|1>) + \frac{1}{2}|01>(\alpha|1> + \beta|0>) \\
&\quad + \frac{1}{2}|10>(\alpha|0> - \beta|1>) + \frac{1}{2}|11>(\alpha|1> - \beta|0>)
\end{aligned}
$$

In |state 2>, the following observations can be made. First, if *A* measures the first two qubits, there are four possible outcomes: |00>, |01>, |10>, and |11>. Second, each outcome has an equal probability of 0.25, which is the square of ½. Finally, upon *A* making such measurements, it can be observed that *B*'s qubit will also be collapse into one of the four possible superposition states, in accordance with the property of quantum entanglement. Therefore, *B* receives the measurement results of the first two qubits from *A* and performs the corresponding quantum gate operations to reproduce the original quantum state |*Ψ*> in all measurement results, thus completing the quantum teleportation.

TABLE I. B'S REPRODUCTION OF STATE |*Ψ*>

B's qubit state	Received	Gate	Final State
$\alpha|0> + \beta|1>$	00	I	$\alpha|0> + \beta|1>$
$\alpha|1> + \beta|0>$	01	X	$\alpha|0> + \beta|1>$
$\alpha|0> - \beta|1>$	10	Z	$\alpha|0> + \beta|1>$
$\alpha|1> - \beta|0>$	11	ZX	$\alpha|0> + \beta|1>$

As shown in Table I, if "00" is sent, *B* applies I gate to its state:

$$\mathrm{I}(\alpha|0> + \beta|1>) = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\begin{bmatrix}\alpha\\\beta\end{bmatrix} = \begin{bmatrix}\alpha\\\beta\end{bmatrix} = \alpha|0> + \beta|1>$$

If *A* sends "01", *B* has to interchange the constants, which can be done by applying a Pauli X gate.

$$\mathrm{X}(\alpha|1> + \beta|0>) = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}\beta\\\alpha\end{bmatrix} = \begin{bmatrix}\alpha\\\beta\end{bmatrix} = \alpha|0> + \beta|1>$$

If *A* sends "10", *B* has to remove the minus (–) sign, which can be done by applying a Pauli Z gate.

$$\mathrm{Z}(\alpha|0> - \beta|1>) = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}\begin{bmatrix}\alpha\\-\beta\end{bmatrix} = \begin{bmatrix}\alpha\\\beta\end{bmatrix} = \alpha|0> + \beta|1>$$

If *A* sends "11", *B* has to sequentially apply both the operations.

$$\mathrm{ZX}(\alpha|1> - \beta|0>) = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}-\beta\\\alpha\end{bmatrix} = \begin{bmatrix}\alpha\\\beta\end{bmatrix} = \alpha|0> + \beta|1>$$

Quantum teleportation is a phenomenon that demonstrates two important characteristics of quantum mechanics. First, it highlights the fact that quantum states cannot be copied. In the process of quantum teleportation, *A* measures the quantum state |*Ψ*>, and then sends the measurement result to *B*, who can use that information to reproduce the state |*Ψ*>. However, the act of measurement causes the state |*Ψ*> collapses, so the state |*Ψ*> does not exist simultaneously in *A* and *B* even for a moment. Since quantum states cannot be cloned or replicated (as per the no-cloning theorem), copy-and-paste operations are not allowed in quantum computing.

The second characteristics involves the use of entangles pairs of quantum bits to instantaneously determined the state of one qubit based on the measurement of another. This give us the impression of faster-than-light communication between A and B, as if the quantum state $|\Psi>$ is moving from A to B instantly.

However, we need to mention that in quantum teleportation, A must send the measurement result to B via classical communication channel before B can reproduce the state $|\Psi>$. Therefore, meaningful information cannot be transmitted faster than the speed of light, as this would violate the laws of physics [4].

III. Motivation of Adopting Blcokchain

Let us delve into a prominent security concern related to quantum teleportation. As per the mechanics of quantum teleportation, entity A can intercept the two classical bits meant for entity B, but it is incapable of creating the teleporting qubit $|\Psi>$ without another entangled qubit pair.

Even if a malicious actor manages to intercept the measurement results using a man-in-middle attack, it is unable to replicate the state $|\Psi>$ as it lacks the necessary entangled qubit pair. Importantly, this does not imply that A cannot pose a threat to the teleportation process. Entity A can indeed interfere with the teleportation process by intercepting the two qubits and supplying B with false bits.

Moreover, in the course of their journey, these classical bits need to traverse through a multitude of network nodes, such as repeaters, hubs, switches, and routers. This convoluted route exacerbates the complexity of the system.

As a result, a pure measurement-and-send quantum teleportation system employing traditional communication channels cannot ensure foolproof security. Therefore, we require highly reliable, efficient, and secure technology to implement a more secure and robust quantum teleportation protocol.

At this juncture, blockchain technology comes to the forefront as a promising solution. Blockchain, an immutable and shared ledger, facilitates the recording of transactions and tracking of assets in a network, including quantum networks. Through the application of blockchain technology, we can monitor and exchange almost anything of value in the network, thus mitigating risks and reducing overall costs.

In our revised quantum teleportation protocol, we necessitate that entity A records all the data generated during the measurement process into blocks before dispatching them to B. These blocks are chronologically linked together to form an immutable chain, enabling receivers to trace or retrieve any desired record detailing the process and recording of the measurement results.

Given that these blockchains represent a collective record of data, they also confer a high degree of trust. This use of trusted data offers a substantial impetus to the emerging domain of blockchain technology applications, promising significant enhancements in efficiency, reliability, and transparency in quantum teleportation processing.

IV. Application of Blcokchain Technology

After completing the measurement of two qubits, A performs data transmission tasks to B using blockchain as follows.

1. Entity A initiates the process by requesting a data transfer from B. This could be any quantum information that needs to be teleported. The request is communicated securely, with A ensuring it follows the protocol established for secure communication within the network.

2. A block containing the associated information is generated. The block encapsulates details regarding the measurement, including data about the state of the qubits and any other relevant metadata. The encapsulated information is then hashed, and this hash is stored in the block to ensure data integrity.

3. Once the block is ready, it is transmitted to all participants on the blockchain network. It is not just sent to B; it is broadcast to all the nodes in the network, ensuring transparency and reliability of the transaction. The process adheres to the blockchain's inherent decentralized architecture, adding an extra layer of security and robustness.

4. Participants in the network, upon receiving the block, mutually verify the validity of the information contained within it. This consensus protocol ensures that only verified and valid blocks are added to the chain. This property prevents fraudulent transactions and ensure the integrity of the data.

5. Once a block has been verified, it is linked to the previous block, creating a chain of blocks. The linkage is created by including the hash of the previous block in the current block, providing an audit trail. A copy of the updated blockchain is then distributed to each user's computer in a decentralized manner, maintaining the up-to-date and synchronized state of the blockchain across the network.

6. With the verified blocks linked and the blockchain updated, A completes the teleportation process by transferring the measurement data to B. This ensures that B receives the quantum information securely, verifying the same from the received block in the blockchain.

7. If necessary, B can further verify the validity of the transmitted data by accessing the blockchain network. This gives B the ability to cross-verify the received data with the recorded data in the blockchain, ensuring no tampering or misinformation.

Whenever measurement results are transmitted, a block containing the pertinent information is generated and persistently linked. The decentralized distribution of copies of these blocks to all participants' computers underscores the security and tamper-resistant nature of blockchain. Modifying information becomes practically impossible, as it would require altering the data held by a majority of the participants.

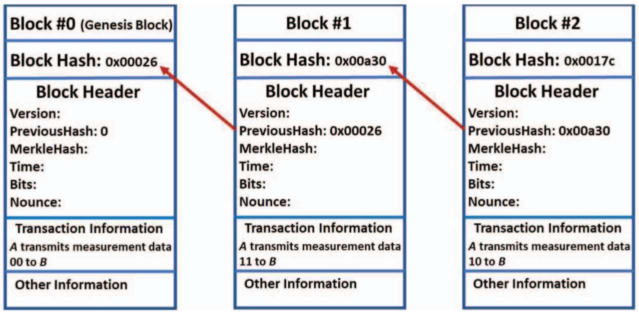

Fig. 2. Example of blockchain for quantum teleportation

The cryptographic technologies employed in blockchain, including hash functions, digital signatures, and public key encryption algorithms, provide robust security [5]. Hash functions convert arbitrary data into a hash value of a specific length, often termed as a 'fingerprint'. These hash values serve as powerful tools to verify the integrity of transmitted measurement data for quantum teleportation. By comparing the hash values of the original data with the transmitted data, any discrepancies or tampering can be easily detected.

Fig. 2 depicts a blockchain structure as an example. Data and the associated hash value are used to construct each individual block. The block's unique identification is formed by applying a hash function to the contents, signing it digitally, and adding the result to the block header.

We can see that the block header is composed of the following three components:

1. PreviousHash: indicates that the current block is linked to the previous block and identifies the block. It contains the hash value of the previous block.
2. MerkleHash: corresponds to the root of the Merkle tree and summarizes all the information in the block into a small-size data that exists in the block header.
3. Information related to miners' calculations for mining blocks, such as difficulty, timestamp, and nonce.

The hash of the previous block is incorporated into the next block. This interlinking structure forms a chain, where each block is connected to the preceding and following block via their hash values. It offers a chronological and tamper-evident structure where any changes in a block would alter its hash value, consequently affecting all the subsequent blocks in the chain due to their interconnectedness.

This feature adds a layer of security against data tampering since an adversary attempting to alter a specific block would need to change all the subsequent blocks in the chain – a computationally intensive and virtually impossible task considering the decentralized and consensus-based nature of the blockchain network.

As the network grows larger and more complex, manually verifying the integrity of transmitted measurement data by comparing information in the blockchain in a one-by-one manner becomes impractical for entity B. To ensure efficiency, B must be able to swiftly verify the authenticity of specific measurement results.

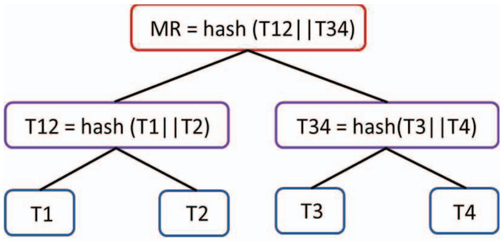

Fig. 3. Example of Merkle tree of a block with four dinstint transactions

This challenge can be overcome through the efficient structuring system inherent to blockchain technology known as the Merkle tree. Essentially a binary hash tree, the Merkle tree compiles all transactions or actions within a block. In the tree's construction, every leaf node embodies a hash representation of an individual transaction. Simultaneously, all non-leaf nodes signify hashes of their corresponding child nodes, effectively encapsulating the details of all their descendant transactions.

Crowning this tree structure is the Merkle root. This component is a unique hash derived from the combined data of all transactions in the block – or, in the context of our discussion, all the quantum measurement results. This single, comprehensive hash encapsulates the integrity of the entire block's data, presenting a summary that is then strategically positioned in the block header.

The Merkle root's existence in the block header allows any participant to verify the integrity of any single transaction (or measurement result) without needing to scrutinize every single transaction in the block. This efficient authentication system makes the Merkle tree an essential component of blockchain architecture, providing a scalable solution for data verification in expansive blockchain networks.

Hence, all hash values of the measurement results are consolidated in the Merkle root. The integrity of individual information within a block can be verified by comparing the original hash values against the hash values contained in the Merkle root. This allows for the quick and efficient verification of data integrity, without needing to comb through every single transaction in the block, providing a scalable solution for data authentication in large blockchain networks.

Fig. 3 depicts the Merkle tree for 4 transactions denoted as T1, T2, T3, and T4 and a Merkle Root (MR).

- H12 is the hash of the concatenation of T1 and T2.
  $H12 = hash(T1\|T2)$
- H34 is the hash of the concatenation of T3 and T4.
  $H34 = hash(T3\|T4)$
- MR is the hash of the concatenation of H12 and H34.
  $MR = hash(T12\|T34)$

Let us suppose that *B* receives transaction T2 from *A*, and wants to verify the integrity of T2. For the verification process, *B* needs the following information from the blockchain block:

- T2 (The transaction itself for verification)
- T1 (The sibling transaction to T2)
- H34 (The hash of T3 and T4)

Entity *B*, having obtained the necessary data, proceeds to perform two verification steps. The first step entails generating a hash from T1 concatenated with T2 (hash(T1||T2)) and comparing this computed value with H12 as recorded in the Merkle tree. Following this, *B* forms a hash by concatenating the just validated H12 with H34 (hash(H12||H34)) and compares this resultant value with the MR as given in the Merkle tree. If both steps yield a match, the integrity of T2 is successfully verified.

This procedure is renowned for its efficiency as it mandates only log(n) computations, with n symbolizing the total transactions recorded in the block. As demonstrated, entity *B* authenticated the integrity of transaction T2 using merely two hash computations, a feat achievable independent of the total transactions contained in the block.

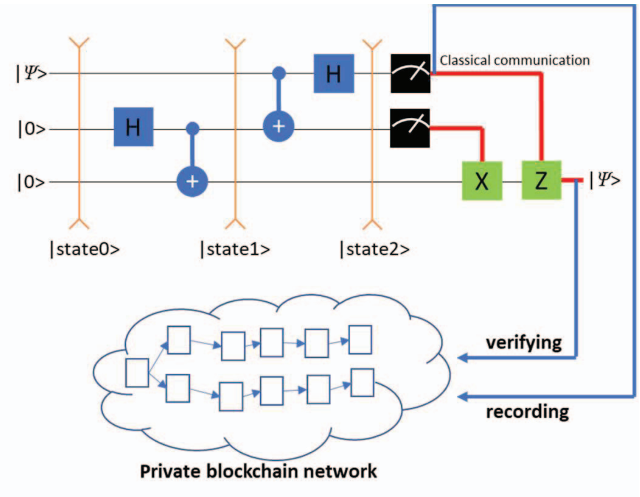

Fig. 4. Overall protocol for quantum teleportation with blockchain network

Fig. 4 shows the application of blockchain technology for quantum teleportation. Sender *A* records the measurement results to blockchain network and then sends them to receiver *B*, who can verify the data integrity by accessing the blockchain network.

V. Conclusion

Quantum teleportation cannot make a copy of a quantum state and transmit it to the receiver due to the no-cloning theorem. At the end of the teleportation, *A* no longer possesses its original qubit state, and its information appears on *B*'s side. Even though the quantum state seems to be teleported instantaneously, it is important to dispel the misconception that quantum teleportation provides faster than light communication. Although the qubit is teleported instantaneously, *A* must still send its measurement results to *B* through a classical communication channel, which is limited by the speed of light.

On top of these inherent characteristics, quantum teleportation can be threatened by potential security issues. For instance, the integrity of the measurement data could be compromised if *A* or a malicious attacker manipulates the measurement results before passing them on to *B*.

To bolster the security and data integrity of quantum teleportation, we proposed the utilization of blockchain technology. The specific form of blockchain implementation would be contingent on the intended application and context of quantum teleportation.

As of now, quantum computers are confined largely to research settings and are not yet accessible to the general public. Therefore, a private blockchain network, requiring validation from a sanctioned service provider, appears to be the most fitting choice for participants at this juncture.

Moving forward, as quantum computing technologies continue to advance and become more widely available, the implementation of a consortium or even a public blockchain could become viable options. Such progress would extend the potential for secure and efficient quantum teleportation into a wide range of applications and environments.

Moreover, it is important to note the growing prominence of quantum-resistant cryptographic algorithms that can provide additional layers of security for quantum communication and teleportation. Future work should include further exploration and application of these cryptographic measures within the blockchain context to further fortify the security of quantum teleportation.

Furthermore, studies on the integration of blockchain technology with quantum key distribution could also be a promising avenue to augment the security level of quantum teleportation. This will ultimately pave the way towards a more secure quantum internet, opening doors to countless applications in quantum computing and communication.

Acknowledgment

This work was supported by the U.S. Department of Energy Advanced Scientific Computing Research-Reaching a New Energy Sciences Workforce (DOE-ASCR-RENEW: DE-SC0023595).

References

[1] Born, Max (1926). "I.2". In Wheeler, J. A.; Zurek, W. H. (eds.). Zur Quantenmechanik der Stoßvorgänge [On the quantum mechanics of collisions]. Zeitschrift für Physik. Vol. 37. Princeton University Press (published 1983). pp. 863–867, doi:10.1007/BF01397477.

[2] Bennett, Charles H., et al., "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," Physical Review Letters, 70 (13): 1895–1899, March 1993.

[3] Hobson, M. P, et al. "Quantum Entanglement and Communication Complexity, SIAM J. Computing, 30 (6): 1829–1841, 1998.

[4] J. S. Bell, "On the Einstein Podolsky Rosen paradox", Physics Physique Fizika 1, pp 195–200, Nov 1964.

[5] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. https://bitcoin.org/bitcoin.pdf