Article

Quantum Blockchain Using Entanglement in Time

Del Rajan * and **Matt Visser**

School of Mathematics and Statistics, Victoria University of Wellington, PO Box 600,
Wellington 6140, New Zealand; matt.visser@sms.vuw.ac.nz
* Correspondence: del.rajan@sms.vuw.ac.nz

check for
updates

Abstract: We propose a conceptual design for a quantum blockchain. Our method involves encoding the blockchain into a temporal GHZ (Greenberger–Horne–Zeilinger) state of photons that do not simultaneously coexist. It is shown that the entanglement in time, as opposed to an entanglement in space, provides the crucial quantum advantage. All the subcomponents of this system have already been shown to be experimentally realized. Furthermore, our encoding procedure can be interpreted as nonclassically influencing the past.

1. Introduction

Entanglement is an intrinsically quantum effect that involves nonclassical correlations, usually between spatially separated quantum systems [1]. This phenomenon was described by Einstein as "spooky action at a distance", and yet it forms the basis of nearly all quantum information platforms, such as quantum computers and quantum networks. In particular, quantum networks distribute quantum information between any two nodes on the network [2,3]. This allows the distributed system to carry out valuable tasks such as quantum key distribution (QKD), which guarantees secure communication through the laws of physics [4,5]. Significant progress is currently being made towards the creation of a global quantum network [6], and it is becoming an increasing priority to find further applications that can be built on such a platform.

A blockchain is a type of classical database that contains records about the past, such as a history of financial (or other) transactions. Its unique design [7] makes it very difficult to tamper with, and it also does not require a centralised institution to maintain its ongoing accuracy. A notable result [8,9] is that scalable quantum computers could successfully break the cryptographic protocols that are used to secure (classical) blockchains, as well as the digital security of the modern world. With the advent of a quantum computing race [2,3], there have been various proposals for modified classical blockchains to protect against such an attack [10–12]. However, their reliability can be questioned, given the large research effort to find new quantum algorithms [13–15] which could potentially undermine such work. In addition to this, classical blockchains with added quantum features have also been put forward [16–21]. One in particular [9] adds a QKD network layer (which protects the relevant sub-algorithm against a quantum computing attack) to a classical blockchain. A more desirable solution would be an intrinsically quantum blockchain, which is constructed out of quantum information, and whose design is fully integrated into a quantum network. This would provide the benefit of a QKD layer as well other potential quantum advantages over a classical blockchain.

In this article, we propose a conceptual design for a quantum blockchain using entanglement in time [22–24]. Nonclassical correlations between temporally separated quantum systems have

manifested themselves through various physical settings; the particular case used in this work involves entanglement in time between photons that do not simultaneously coexist [25].

Our novel methodology encodes a blockchain into these temporally entangled states, which can then be integrated into a quantum network for further useful operations. We also show that entanglement in time, as opposed to entanglement in space, plays the pivotal role for the quantum benefit over a classical blockchain. As discussed below, all the subsystems of this design have already been shown to be experimentally realisable. Furthermore, if such a quantum blockchain were to be constructed, we would show that it could be viewed as a quantum networked time machine.

2. Classical Blockchain

The classical blockchain is composed of a blockchain data structure and a network consensus protocol; the former is the database, while the latter provides the decentralisation feature. The aim of a blockchain is to have a single database of records about the past that every node in the network can agree on. Furthermore, it should not require a centralised management node. It will be helpful to construct a physical model to describe this classical information system, i.e., its kinematic and dynamic properties.

We start with the kinematic features. Records about the past, which occurred at around the same time, are received and collected into a data block. These blocks are time-stamped to ensure that the data existed at the specified time. Furthermore, the blocks are linked in chronological order through cryptographic hash functions [26].

If an attacker tries to tamper with a particular block, these cryptographic hash functions can be used to ensure, with a high degree of confidence, the invalidation of all future blocks following the tampered block; this makes the classical blockchain extremely fragile, and thus sensitive to tampering. Hence, the older the time stamp on the block, the more secure it is in the blockchain. The key benefit to achieve through this sensitivity is that it should be very difficult to (successfully) tamper with a block without invalidating the blockchain.

Another way to achieve this benefit in the kinematic case is to have a large distributed network with each node hosting a local individual copy of the blockchain. If a dishonest node tampers with its local copy, it does not affect the other copies in the other nodes of the network.

In the dynamic case, we want to examine how a blockchain lengthens over time. The objective is to add valid blocks without a centralised institution; there are a number of ways this could be accomplished. One current classical design does this by invoking a node on the network to confirm the validity of records in a new block, and then broadcasting that block to other nodes. The different nodes accept the block if they can successfully link it to their own copy of the blockchain through the cryptographic hash functions. For this procedure to maintain ongoing accuracy, the validating node gets chosen at random for each block; this prevents preplanned node-specific attacks. Furthermore, the validating node is also incentivised through the network for carrying out these tasks. Despite some dishonest nodes, this is all achieved through consensus algorithms like proof-of-work or proof-of-stake [10].

From our analysis, we see that the relevant performance benefits are nontampering, and also maintaining ongoing accuracy in a decentralised manner. We aim to show that a fully quantum blockchain, at an abstract level, could provide an advantage over classical blockchain on these performance metrics.

3. Quantum Blockchain

In this section, our aim is to replace the data structure component of the classical blockchain with a quantum system. In quantum information theory, quantum systems are described as information carriers, with an encoding and decoding process. For the case of a blockchain, we capture the notion of the chain through the nonseparability (entanglement) of quantum systems (e.g., photons). For a bipartite system $|\psi\rangle_{AB}$, this means that:

$$|\psi\rangle_{AB} \neq |a\rangle_A |b\rangle_B , \tag{1}$$

for all single qubit states $|a\rangle$ and $|b\rangle$; the subscripts refer to the respective Hilbert spaces. In particular, multipartite GHZ (Greenberger–Horne–Zeilinger) states [27,28] are ones in which all subsystems contribute to the shared entangled property. This enables us to create the concept of a chain.

To create the appropriate code to utilise this chain, it is helpful to use a concept from superdense coding [5]. In this protocol, a code converts classical information into spatially entangled Bell states; two classical bits, xy, where $xy = 00, 01, 10$ or 11, are encoded to the state:

$$|\beta_{xy}\rangle = \frac{1}{\sqrt{2}}(|0\rangle |y\rangle + (-1)^x |1\rangle |\bar{y}\rangle), \tag{2}$$

where $\bar{y}$ is the negation of y. Given that Bell states are orthonormal, they can be distinguished by quantum measurements. This decoding process allows one to extract the classical bit string, xy, from $|\beta_{xy}\rangle$.

For our conceptual design, we temporarily simplified the data characterising the records in the classical block to a string of two bits. Our encoding procedure converted each block with its classical record, say $r_1 r_2$, into a temporal Bell state [25], generated at a particular time, say $t = 0$:

$$|\beta_{r_1 r_2}\rangle^{0,\tau} = \frac{1}{\sqrt{2}}(|0^0\rangle |r_2^\tau\rangle + (-1)^{r_1} |1^0\rangle |\bar{r_2}^\tau\rangle). \tag{3}$$

The superscripts in the kets signify the time at which the photon is absorbed; notice that the first photon of a block is absorbed immediately. For our purposes, this provides a way to do time stamps for each block.

Physically, such temporal Bell states were experimentally generated in the work by the authors of [25]. In their procedure, spatially entangled qubits were represented through polarized photons:

$$|\phi\pm\rangle = \frac{1}{\sqrt{2}}(|h_a h_b\rangle \pm |v_a v_b\rangle), \quad |\psi\pm\rangle = \frac{1}{\sqrt{2}}(|h_a v_b\rangle \pm |v_a h_b\rangle), \tag{4}$$

where h_a (v_a) represent the horizontal (vertical) polarization in spatial mode a (b). To create the temporally entangled states, consecutive pairs of spatially entangled pairs were generated at well-defined times separated by time interval τ:

$$|\psi-\rangle_{a,b}^{0,0} \otimes |\psi-\rangle_{a,b}^{\tau,\tau} = \frac{1}{2}(|h_a^0 v_b^0\rangle - |v_a^0 h_b^0\rangle) \otimes (|h_a^\tau v_b^\tau\rangle - |v_a^\tau h_b^\tau\rangle), \tag{5}$$

where the added superscripts provide the time labels for the photons. In the experiment, a delay line of time τ is introduced to one of the photons of each entangled pair. This resulting state equated to:

$$|\psi-\rangle_{a,b}^{0,\tau} |\psi-\rangle_{a,b}^{\tau,2\tau} = \frac{1}{2}(|\psi+\rangle_{a,b}^{0,2\tau} |\psi+\rangle_{a,b}^{\tau,\tau} - |\psi-\rangle_{a,b}^{0,2\tau} |\psi-\rangle_{a,b}^{\tau,\tau} - |\phi+\rangle_{a,b}^{0,2\tau} |\phi+\rangle_{a,b}^{\tau,\tau} + |\phi-\rangle_{a,b}^{0,2\tau} |\phi-\rangle_{a,b}^{\tau,\tau}). \tag{6}$$

When Bell projection was carried out on two photons at time $t = \tau$, entanglement was created between the photon absorbed at $t = 0$ and the photon absorbed at $t = 2\tau$; this is despite the fact that the latter two photons have never coexisted.

Going back to our design, as records are generated, the system encodes them as blocks into temporal Bell states; these photons are then created and absorbed at their respective times. A specific example of such blocks would be:

$$|\beta_{00}\rangle^{0,\tau}, \qquad |\beta_{10}\rangle^{\tau,2\tau}, \qquad |\beta_{11}\rangle^{2\tau,3\tau}, \tag{7}$$

and so forth. To create the desired quantum design, the system should chain the bit strings of the Bell states together in chronological order, through an entanglement in time [22–24].

Such a task can be accomplished using a fusion process [29] in which temporal Bell states are recursively projected into a growing temporal GHZ state. Physically, the fusion process is carried

out through the entangled photon-pair source, a delay line, and a polarising beam splitter (PBS). As an example, two Bell states can be fused into the following four-photon GHZ state:

$$
\begin{aligned}
|\psi+\rangle_{a,b}^{0,0} \otimes |\psi+\rangle_{a,b}^{\tau,\tau} \xrightarrow{delay} & |\psi+\rangle_{a,b}^{0,\tau} \otimes |\psi+\rangle_{a,b}^{\tau,2\tau} = \tfrac{1}{2}(|h_a^0 v_b^\tau\rangle + |v_a^0 h_b^\tau\rangle) \otimes (|h_a^\tau v_b^{2\tau}\rangle + |v_a^\tau h_b^{2\tau}\rangle) \\
\xrightarrow{PBS} & \tfrac{1}{2}(|h_a^0 v_b^\tau v_a^\tau h_b^{2\tau}\rangle + |v_a^0 h_b^\tau h_a^\tau v_b^{2\tau}\rangle) = |GHZ\rangle^{0,\tau,\tau,2\tau}.
\end{aligned}
\tag{8}
$$

In this GHZ state, entanglement exists between the four photons that propagate in different spatial modes and exist at different times.

Implementing this procedure in our design, the state of the quantum blockchain, at $t = n\tau$ (from $t = 0$) is given by:

$$
|GHZ_{r_1 r_2 \ldots r_{2n}}\rangle^{0,\tau,2\tau,2\tau\ldots,(n-1)\tau,(n-1)\tau,n\tau} = \frac{1}{\sqrt{2}}(|0^0 r_2^\tau r_3^\tau \ldots r_{2n}^{n\tau}\rangle + (-1)^{r_1} |1^0 \bar{r}_2^\tau \bar{r}_3^\tau \ldots \bar{r}_{2n}^{n\tau}\rangle). \tag{9}
$$

The subscripts on the left hand side of Equation (9) denote the concatenated string of all the blocks, while superscripts refer to the time stamps. The time stamps allow each blocks' bit string to be differentiated from the binary representation of the temporal GHZ basis state. Note that at $t = n\tau$, there is only one photon remaining.

The dynamics of this procedure can be illustrated with our example above. Out of the first two blocks, $|\beta_{00}\rangle^{0,\tau}$ and $|\beta_{10}\rangle^{\tau,2\tau}$, the system creates the (small) blockchain $|GHZ_{0010}\rangle^{0,\tau,\tau,2\tau}$. Concatenating the third block then produces $|GHZ_{001011}\rangle^{0,\tau,\tau,2\tau,2\tau,3\tau}$. The decoding process extracts the classical information, $r_1 r_2 \ldots r_{2n}$, from the state (Equation (9)). In recent work, it was shown how to characterise any such temporally generated GHZ state efficiently compared to standard tomography techniques. This can be accomplished without measuring the full photon statistics, or even detecting them [30]. Each of the operations above have been explicitly shown to be experimentally realisable, at least in simple cases [25,29,30].

The scalability of these temporally entangled systems was considered in Reference [25]. The key implication of their work is, and we quote, "any number of photons are generated with the same setup, solving the scalability problem caused by the previous need for extra resources. Consequently, entangled photon states of larger numbers than before are practically realizable". Our proposal certainly does not yet meet immediate engineering considerations for a quantum blockchain, but it shows a visible path forward towards scalability.

It is important to note that at this stage of development, we are advocating a conceptual mathematical design for a new quantum information technology. It should be viewed as analogous to early quantum algorithms (Deutsch's algorithm [31], Deutsch-Jozsa algorithms [32]). In the 1980s, the engineering considerations for quantum computers were not taken into account. In the 1990s, when Shor's algorithm and Grover's algorithm were developed, the experimental realisation of quantum computers was almost seen as an impossible project. Nonetheless, their work was certainly of interest to the wider community [33].

4. Quantum Network

Recall that a classical blockchain system has a number of different components: A blockchain data structure, a copy of this blockchain data structure at each node of a classical network, and a consensus network algorithm to verify the correctness of new blocks (before adding that new block to a blockchain).

In our design, we replaced the classical network with a quantum network. In addition, digital signatures would be covered by a QKD protocol as stated in Reference [8]. In fact, others have used this way of reasoning when introducing new quantum protocols. For example, in the paper that introduced the θ-protocol [34], the authors also simply assumed a QKD layer before moving onto their original work. We quote from their paper, "it is assumed that the verifier and each of the parties share a secure private channel for the communication. This can be achieved by using either a one-time pad or quantum key distribution".

Furthermore, each node on the quantum network would host a copy of the quantum blockchain (Equation (9)); hence, if a node tampers with its own local copy, it does not affect the copies at the other nodes analogous to the classical case. New blocks (that come from a sender) need to be verified for their correctness, before being copied and added to each node's blockchain. Since correct blocks are GHZ entangled states, one needs a verification test to do it.

At this stage of the design, we assumed that newly generated blocks are spatial GHZ states (converting this to the related temporal case is at this stage of the design process unnecessary and is left for future work). As in the classical case, the objective is to add valid blocks in a decentralised manner. The challenge is that the network can consist of dishonest nodes, and the generated blocks can come from a dishonest source. To solve this problem, the quantum network uses the θ-protocol [34], which is a consensus algorithm where a random node in the quantum network can verify that the untrusted source created a valid block (spatial GHZ state). More crucially, this is accomplished in a decentralised way using other network nodes, which may also be dishonest (Byzantine nodes).

To start off this verification protocol, we needed to pick a randomly chosen verifier node (analogous to proof-of-stake or proof-of-work); this can be accomplished through a low level sub-algorithm involving a quantum random number generator. The untrusted source shares a possible valid block, an n-qubit state. Since it knows the state, it can share as many copies of the block as is needed without running afoul of the no-cloning theorem. For verification, it distributes each of the qubits to each node, j. The verifying node generates random angles $\theta_j \in [0, \pi)$ such that $\sum_j \theta_j$ is a multiple of π. The (classical) angles are distributed to each node, including the verifier. They respectively measure their qubit using the basis:

$$|+_{\theta_j}\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\theta_j} |1\rangle \right), \tag{10}$$

$$|-_{\theta_j}\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle - e^{i\theta_j} |1\rangle \right). \tag{11}$$

The results, $Y_j = \{0, 1\}$, are sent to the verifier. If the n-qubit state was a valid block, i.e., a spatial GHZ state, the necessary condition:

$$\oplus_j Y_j = \frac{1}{\pi} \sum_j \theta_j \pmod 2, \tag{12}$$

is satisfied with probability 1.

The protocol links the verification test to the state that is used; Reference [34] explicitly mentions this, and we quote, "It is important to remark that our verification protocols go beyond merely detecting entanglement; they also link the outcome of the verification tests to the state that is actually used by the honest parties of the network with respect to their ideal target state. This is non trivial and of great importance in a realistic setting where such resources are subsequently used by the parties in distributed computation and communication applications executed over the network". Hence, the block can be copied and distributed to each node on the network to be added onto their blockchain. This θ-protocol has also been experimentally realised in simple cases, with quantitative analysis provided on cases involving dishonest nodes [34].

5. Discussion

For an analysis of the quantum benefit, we looked primarily at the blockchain's ability to be rendered tamper-proof. The classical blockchain data structure operates through time-stamped blocks with cryptographic hash functions linking them in a chronological order. If an attacker tampers with a particular block, all future blocks following the tampered block are invalidated. This sensitivity to such disturbances is the mechanism which makes it difficult to tamper with a blockchain without invalidating it.

For the quantum blockchain, we replaced the important functionality of time-stamped blocks and hash functions linking them with a temporal GHZ state with an entanglement in time. The quantum advantage is that the sensitivity towards tampering is significantly amplified, meaning that the full local copy of the blockchain is destroyed if one tampers with a single block (due to entanglement); on a classical blockchain, only the blocks after the tampered block are destroyed (due to cryptographic hash functions), which leaves it open to vulnerabilities. For the classical case, it is often stated that the farther back the block was time-stamped in, the more "secure" it is; this is precisely because of the above invalidation.

More specifically, with just a spatial GHZ state, the measurement correlations of these states are stronger than what a classical system could ever produce. In this spatial entanglement case, if an attacker tries to tamper with any photon, the full local copy of the blockchain would be invalidated immediately; this already provides a benefit over the classical case where only the future blocks of the tampered block are invalidated.

The temporal GHZ blockchain (Equation (9)) adds a far greater benefit in that the attacker cannot even attempt to access the previous photons, since they no longer exist. They can at best try to tamper with the last remaining photon, which would invalidate the full state. Hence, in this application of quantum information, we see that the entanglement in time provides a far greater security benefit than an entanglement in space.

There still needs to be a careful case-by-case analysis of potential tampering with the ultimately classical measurement results, but that would entail full security proofs, which is left for future work. It is important to distinguish between the classical case and quantum case like it was done for quantum algorithms with bounded probability for errors vs. classical deterministic algorithms. Showing such detailed security proofs would be a research paper in itself.

In terms of its network component, the classical blockchain's most important feature is time-stamped blocks with cryptographic hash functions linking them. Without this, the concept of a blockchain simply does not exist. However, with this concept, there are variations on various types of blockchain that can be considered. Some are public and some are "permissioned" with the extreme version being centralised. They have different consensus algorithms like proof of work or proof of stake. Some have Byzantine fault tolerance and others do not.

To be more specific, there are many well-known blockchains that do not provide Byzantine fault tolerance, such as earlier versions of hyperledger fabric [35]. Hence, this sets the precedent that one does not necessarily need Byzantine fault tolerance to present a novel blockchain design. Furthermore, it has been shown that Nakamoto's proof-of-work does not fulfil Byzantine fault tolerance. That is, no formal proof to this effect exists [36]; there is merely a probabilistic solution, and some argue that its probabilistic guarantees are not easy to relate to the consensus definitions given in traditional distributed computing literature [37,38]. Given this unclear situation even in the classical case, it seems unreasonable to demand full security proofs for Byzantine fault tolerance in our quantum design. Lastly, the θ-protocol which we harness in our design has been analysed quantitatively on uses in cases that involve dishonest (Byzantine) nodes [34]. It is indeed correct to say that our consensus algorithm needs further low-level detail, but that would entail providing a low-level design; at this stage, it would not add much to the main work of introducing a quantum blockchain data structure. Future work on quantum network consensus algorithms will build on this data structure.

The temporal GHZ state that we used in our design involves an entanglement between photons that do not share simultaneous coexistence, yet they share nonclassical measurement correlations. This temporal nonlocality between two entangled photons that existed at different times was interpreted in Reference [25] as follows: "*...measuring the last photon affects the physical description of the first photon in the past, before it has even been measured. Thus, the "spooky action" is steering the system's past*". Stated more boldly, in our quantum blockchain, we can interpret our encoding procedure as linking the current records in a block, not to a record *of* the past, but linking it to the actual record *in* the past, a record which does not exist anymore.

This research can be taken into various different directions. To enhance the realistic possibility of this design being implemented, one should note that quantum networks are currently being realised on space-based satellite links [4]; therefore, spacetime effects need to be taken into account [39,40]. This would entail extending this work into the regime of relativistic quantum information. We speculate that a blockchain can then be encoded into a different temporally entangled system, namely, the entanglement between the future and past in the quantum vacuum [41,42]. A realistic experimental proposal [43] suggests that it is possible to transfer this future past quantum correlation into qubits that do not simultaneously coexist, which is the resource needed for our current design.

For another direction, it is interesting to note that designs for classical blockchains have also advanced in various ways, some with nontrivial casual data [12]. One can look at combining such systems with other temporal quantum concepts, such as the work in quantum casual structures [44–46] or alternative temporal-based GHZ states [47,48]. This may provide variety of qualitatively different designs for a quantum blockchain.

An audacious direction of research stems from the view that at each node, our encoding procedure can be interpreted as influencing the past. With all such nodes connected through quantum channels, the blockchain can be viewed as a quantum networked time machine. On the theoretical front, the system design may be harnessed to invent other useful applications where the full network collectively influences the past in nonclassical ways; this may also lead a type of information–theoretic investigation into the nature of time [49,50]. Furthermore, unlike general relativistic time machines [51–54], all the subcomponents of this system have shown to be realisable [25,29,30,34]; this suggests the possibility to experimentally probe time travel paradoxes through quantum information. At the very least, such a system could lead to experimental probes of quantum causality [45,55] .

6. Conclusions

We have outlined a conceptual design for a quantum blockchain using entanglement in time. Our primary innovation was in encoding the blockchain into a temporal GHZ state. Furthermore, it was shown that entanglement in time, as opposed to entanglement in space, provides the crucial quantum benefit.

This paper is meant to serve as a conceptual design for a new quantum information technology. As such, a lot of detailed low level design gaps do exist, but the intention was to open up a novel area where at least the core functionalities are covered. In the most cited quantum computing textbook [1], it is mentioned that the primitive "Deutsch-Jozsa algorithm contains the seeds for more impressive quantum algorithms". Similarly, we believe that our conceptual quantum blockchain would be the seed for many detailed quantum blockchains that will build on our work. Given the rise of classical blockchains and the realistic development of a global quantum network, this work can potentially open the door to a new research frontier in quantum information science.

References

1.　Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information*; Cambridge University Press: Cambridge, UK, 2010.
2.　Castelvecchi, D. Quantum computers ready to leap out of the lab in 2017. *Nat. News* **2017**, *541*, 9. [CrossRef]
3.　Castelvecchi, D. The quantum internet has arrived (and it hasn't). *Nature* **2018**, *554*, 289. [CrossRef]

4. Bedington R.; Arrazola, J.M.; Ling, A. Progress in satellite quantum key distribution. *NPJ Quantum Inf.* **2017**, *3*, 30. [CrossRef]

5. Bennett, C.H.; Wiesner, S.J. Communication via one-and two-particle operators on Einstein–Podolsky–Rosen states. *Phys. Rev. Lett.* **1992**, *69*, 2881. [CrossRef] [PubMed]

6. Simon, C. Towards a global quantum network. *Nat. Photonics* **2017**, *11*, 678. [CrossRef]

7. Nakamoto, S. Bitcoin: A Peer-to-Peer electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 17 April 2019).

8. Aggarwal, D.; Brennen, G.K.; Lee, T.; Santha, M.; Tomamichel, M. Quantum attacks on Bitcoin, and how to protect against them. *arXiv* **2017**, arxiv:1710.10377.

9. Kiktenko, E.O.; Pozhar, N.O.; Anufriev, M.N.; Trushechkin, A.S.; Yunusov, R.R.; Kurochkin, Y.V.; Lvovsky, A.I.; Fedorov, A.K. Quantum-secured blockchain. *arXiv* **2017**, arxiv:1705.09258.

10. King, S.; Nadal, S. Ppcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. 2012. Available online: https://decred.org/research/king2012.pdf (accessed on 17 April 2019).

11. Witte, J.H. The Blockchain: A Gentle Four Page Introduction. *arXiv* **2016**, arxiv:1612.06244.

12. Buterin, V. Chain Interoperability. Available online: https://www.r3cev.com/s/Chain-Interoperability-8g6f.pdf (accessed on 17 April 2019).

13. McMahon, D. *Quantum Computing Explained*; John Wiley & Sons: Hoboken, NJ, USA, 2007.

14. Montananao, A. Quantum algorithms: An overview. *NPJ Quantum Inf.* **2016**, *2*, 15023. [CrossRef]

15. Zeng, W.; Johnson, B.; Smith, R.; Rubin, N.; Reagor, M.; Ryan, C.; Rigetti, C. First quantum computers need smart software. *Nature* **2017**, *549*, 149. [CrossRef] [PubMed]

16. Jogenfors, J. Quantum bitcoin: An anonymous and distributed currency secured by the no-cloning theorem of quantum mechanics. *arXiv* **2016**, arxiv:1604.01383.

17. Sapaev, D.; Bulychkov, D.; Ablayev, F.; Vasiliev, A.; Ziatdinov, M. Quantum-assisted Blockchain. *arXiv* **2018**, arxiv:1802.06763.

18. Behera, A.; Paul, G. Quantum to classical one way function and its applications in quantum money authentication. *arXiv* **2018**, arxiv:1801.01910.

19. Tessler, L.; Byrnes, T. Bitcoin and quantum computing. *arXiv* **2017**, arxiv:1711.04235.

20. Ikeda, K. qBitcoin: A Peer-to-Peer Quantum Cash System. *arXiv* **2017**, arxiv:1708.04955.

21. Kalinin, K.P.; Berloff, N.G. Blockchain platform with proof-of-work based on analog Hamiltonian optimisers. *arXiv* **2018**, arxiv:1802.10091.

22. Aharonov, Y.; Popescu, S.; Tollaksen, J.; Vaidman, L. Multiple-time states and multiple-time measurements in quantum mechanics. *Phys. Rev. A* **2009**, *79*, 052110, doi:10.1103/PhysRevA.79.052110. [CrossRef]

23. Brukner, Č.; Taylor, S.; Cheung, S.; Vedral, V. Quantum entanglement in time. *arXiv* **2004**, arxiv:quant-ph/0402127.

24. Ringbauer, M.; Costa, F.; Goggin, M.E.; White, A.G.; Fedrizzi, A. Multi-time quantum correlations with no spatial analog'. *NPJ Quantum Inf.* **2018**, *4*, 37. [CrossRef]

25. Megidish, E.; Halevy, A.; Shacham, T.; Dvir, T.; Dovrat, L.; Eisenberg, H.S. Entanglement swapping between photons that have never coexisted. *Phys. Rev. Lett.* **2013**, *110*, 210403. [CrossRef] [PubMed]

26. Katz, J.; Lindell, Y. *Introduction to Modern Cryptography*; CRC Press: Boca Raton, FL, USA, 2014.

27. Greenberger, D.; Horne, M.A.; Zeilinger, A. Going Beyond Bell's Theorem. *arXiv* **2007**, arxiv:0712.0921.

28. Carvacho, G.; Graffitti, F.; D'Ambrosio, V.; Hiesmayr, B.C.; Sciarrino, F. Experimental investigation on the geometry of GHZ states. *Sci. Rep.* **2017**, *7*, 13265. [CrossRef] [PubMed]

29. Megidish, E.; Shacham, T.; Halevy, A.; Dovrat, L.; Eisenberg, H.S. Resource efficient source of multiphoton polarization entanglement. *Phys. Rev. Lett.* **2012**, *109*, 080504. [CrossRef]

30. Megidish, E.; Halevy, A.; Pilnyak, Y.; Slapa, A.; Eisenberg, H.S. Quantum tomography of inductively-created large multiphoton states. *arXiv* **2017**, arxiv:1712.03633.

31. Deutsch, D. Quantum theory, the Church–Turing principle and the universal quantum computer. *Proc. R. Soc. Lond. A Math. Phys. Sci.* **1985**, *4*, 97. [CrossRef]

32. Deutsch, D.; Jozsa, R. Rapid solution of problems by quantum computation. *Proc. R. Soc. Lond. A Math. Phys. Sci.* **1992**, *439*, 553. [CrossRef]

33. Grover, L. Quantum Mechanics Helps in Searching for a Needle in a Haystack. *Phys. Rev. Lett.* **1997**, *79*, 325. [CrossRef]

34. McCutcheon, W.; Pappa, A.; Bell, B.A.; McMillan, A.; Chailloux, A.; Lawson, T.; Mafu, M.; Markham, D.; Diamanti, E.; Kerenidis, I.; et al. Experimental verification of multipartite entanglement in quantum networks. *Nat. Commun.* **2016**, *7*, 13251. [CrossRef]

35. Cachin, C.; Vukolić, M. Blockchain Consensus Protocols in the Wild. *arXiv* **2017**, arxiv:1707.01873.

36. Vukolić, M. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In Proceedings of the International Workshop on Open Problems in Network Security, Zurich, Switzerland, 29 October 2015.

37. Gramoli, V. From blockchain consensus back to Byzantine consensus. *Future Gener. Comput. Syst.* **2017**. [CrossRef]

38. Narayanan, A.; Clark, J. Bitcoin's academic pedigree. *Commun. ACM* **2017**, *15*, 36–45. [CrossRef]

39. Bruschi, D.E.; Ralph, T.; Fuentes, I.; Jennewein, T.; Razavi, M. Spacetime effects on satellite-based quantum communications. *Phys. Rev. D* **2014**, *90*, 045041. [CrossRef]

40. Bruschi, D.E.; Sabín, C.; White, A.; Baccetti, V.; Oi, D.K.L.; Fuentes, I. Testing the effects of gravity and motion on quantum entanglement in space-based experiments. *New J. Phys.* **2014**, *16*, 053041. [CrossRef]

41. Olson, J.S.; Ralph, T.C. Entanglement between the future and the past in the quantum vacuum. *Phys. Rev. Lett.* **2011**, *106*, 110404. [CrossRef] [PubMed]

42. Olson, J.S.; Ralph, T.C. Extraction of timelike entanglement from the quantum vacuum. *Phys. Rev. A* **2012**, *85*, 012306. [CrossRef]

43. Sabín, C.; Peropadre, B.; del Rey, M.; Martín-Martínez, E. Extracting past-future vacuum correlations using circuit QED. *Phys. Rev. Lett.* **2012**, *109*, 033602. [CrossRef]

44. Oreshkov, O.; Costa, F.; Brukner, Č. Quantum correlations with no causal order. *Nat. Commun.* **2012**, *3*, 1092. [CrossRef] [PubMed]

45. Brukner, Č. Quantum causality. *Nat. Phys.* **2014**, *10*, 259. [CrossRef]

46. Chaves, R.; Majenz, C.; Gross, D. Information–theoretic implications of quantum causal structures. *Nat. Commun.* **2015**, *6*, 5766. [CrossRef]

47. Nowakowski, M. Quantum entanglement in time. *AIP Conf. Proc.* **2017**, *1841*, 020007.

48. Nowakowski, M.; Cohen, E.; Horodecki, P. Entangled histories versus the two-state-vector formalism: Towards a better understanding of quantum temporal correlations. *Phys. Rev. A* **2018**, *98*, 032312. [CrossRef]

49. Lloyd, S.; Maccone, L.; Garcia-Patron, R.; Giovannetti, V.; Shikano, Y.; Pirandola, S.; Rozema, L.A.; Darabi, A.; Soudagar, Y.; Shalm, L.K.; et al. Closed timelike curves via post-selection: Theory and experimental demonstration. *Phys. Rev. Lett.* **2011**, *106*, 040403. [CrossRef] [PubMed]

50. Lloyd, S.; Maccone, L.; Garcia-Patron, R.; Giovannetti, V.; Shikano, Y. Quantum mechanics of time travel through post-selected teleportation. *Phys. Rev.* **2011**, *D84*, 025007. [CrossRef]

51. Visser, M. *Lorentzian Wormholes: From Einstein to Hawking*; Springer: Berlin, Germany, 1995.

52. Hawking, S.W. The chronology protection conjecture. *Phys. Rev.* **1992**, *D46*, 603–611. [CrossRef]

53. Visser, M. The quantum physics of chronology protection. In *The future of Theoretical Physics and Cosmology: Celebrating Stephen Hawking's 60th Birthday, Proceedings of the Workshop and Symposium, Cambridge, UK, 7–10 January 2002*; Cambridge University Press: Cambridge, UK, 2002; pp. 161–176.

54. Visser, M. From wormhole to time machine: Comments on Hawking's chronology protection conjecture. *Phys. Rev.* **1993**, *D47*, 554–565.

55. Ringbauer, M.; Giarmatzi, C.; Chaves, R.; Costa, F.; White, A.G.; Fedrizzi, A. Experimental test of nonlocal causality. *Sci. Adv.* **2016**, *2*, e1600162. [CrossRef] [PubMed]