Quantum Blockchain using entanglement in time

Del Rajan and Matt Visser
School of Mathematics and Statistics, Victoria University of Wellington, Wellington 6140, New Zealand.
(Dated: 17 April 2018; LaTeX-ed April 18, 2018)

A conceptual design for a quantum blockchain is proposed. 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. Perhaps more shockingly, our encoding procedure can be interpreted as non-classically influencing the past; hence this decentralized quantum blockchain can be viewed as a quantum networked time machine.

PACS numbers: 03.67.Bg, 03.67.Dd, 03.67.Hk,03.67.Mn
Keywords: entanglement in time, entanglement in space, blockchain, quantum blockchain

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 [6]. 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. Significant progress is currently being made towards the creation of a global quantum network [7], 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 [10] makes it very difficult to tamper with, and it also does not require a centralized institution to maintain its ongoing accuracy.

A notable result [14] 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 [5], there have been various proposals for modified classical blockchains to protect against such an attack. But their reliability can be questioned, given the large research effort to find new quantum algorithms [3, 4] 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 [15] 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.

In this Letter, we will propose a conceptual design for a quantum blockchain using entanglement in time. Non-classical correlations between temporally separated quantum systems have manifested itself through various physical settings; the particular case used in this work involves entanglement in time between photons that do not simultaneously coexist [22].

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 will 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 realized. Furthermore, if such a quantum blockchain were to be constructed, we will show that it could be viewed as a quantum networked time machine.

Classical blockchain: 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 centralized 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 will 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. Hence the older the time stamp on the block, the more secure it is in the blockchain. The key benefit to achieve is that it should be very difficult to (successfully) tamper with a block. Another way to achieve this benefit in the kinematic case is to have a large distributed network with each node hosting a copy of the blockchain. If a dishonest node tampers with its copy, it does not affect the other copies.

In the dynamic case, we want to examine how a blockchain lengthens over time. The objective is to add valid blocks without a centralized institution. The 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 pre-planned node-specific attacks. Furthermore, the validating node is also incentivized 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 [11].

From our analysis we see that the relevant performance benefits are non-tampering, and also maintaining on-going accuracy in a decentralized 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.

Quantum blockchain: In quantum information theory, quantum systems are described as information carriers, with an encoding and decoding process. For the case of a blockchain, we will capture the notion of the chain through the non-separability (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 [25] 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 utilize this chain, it is helpful to use a concept from superdense coding [9]. 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 simplify the data characterizing the records in the classical block to a string of two bits. Our encoding procedure converts each block with its classical record, say $r_1 r_2$, into a temporal Bell state [22], 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.

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:

$$|\beta_{00}\rangle^{0,\tau} , \qquad |\beta_{10}\rangle^{\tau,2\tau} , \qquad |\beta_{11}\rangle^{2\tau,3\tau} , \tag{4}$$

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.

Such a task can be accomplished by using a fusion process [23] in which temporal Bell states are recursively projected into a growing temporal GHZ state. Implementing this, the state of the quantum blockchain, at $t = n\tau$ (from $t = 0$) is given by

$$\begin{aligned} &|GHZ_{r_1 r_2 \ldots r_{2n}}\rangle^{0,\tau,\tau,2\tau,2\tau\ldots,(n-1)\tau,(n-1)\tau,n\tau} \\ &= \frac{1}{\sqrt{2}}(|0^0 r_2^\tau r_3^\tau \ldots r_{2n}^{n\tau}\rangle + (-1)^{r_1} |1^0 \bar{r}_2^\tau \bar{r}_3^\tau \ldots \bar{r}_{2n}^{n\tau}\rangle). \end{aligned} \tag{5}$$

The subscripts on the LHS of (5) 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 (5). In recent work, it was shown how to characterize 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 [24]. Each of the operations above have been explicitly shown to be experimentally realizable, at least in simple cases [22–24].

Quantum network: Each node in a quantum network would store a copy of the blockchain (5). At this stage of the design, we assume 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 decentralized 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 [27], where a random node in the network can verify that the untrusted source created a valid block (spatial GHZ state). More crucially, this is accomplished in a decentralized way by using other network nodes, who may also be dishonest.

To start off with, we need to pick a randomly chosen verifier node (analogous to proof-of-stake or proof-of-work); this can be accomplished through 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 in the basis,

$$|+_{\theta_j}\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\theta_j} |1\rangle \right), \tag{6}$$

$$|-_{\theta_j}\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle - e^{i\theta_j} |1\rangle \right). \tag{7}$$

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

$$\oplus_j \, Y_j = \frac{1}{\pi} \sum_j \theta_j \pmod 2, \tag{8}$$

is satisfied with probability 1. The protocol links the verification test to the state that is used. Hence the block can be added onto the blockchain. This θ-protocol has also been experimentally realized in simple cases [27].

Discussion: For an analysis of the quantum benefit, we look primarily at the blockchain's ability to be rendered tamper proof. 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 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 (5) 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.

The temporal GHZ state involves an entanglement between photons that do not share simultaneous coexistence, yet they share non-classical measurement correlations. This temporal non-locality, between two entangled photons that existed at different times, was interpreted in [22] 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 shockingly, 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, which does not exist anymore.

Future work: 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 realized on space-based satellite links [8]; therefore spacetime effects needs to be taken into account [34, 35]. 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 [28, 29]. A realistic experimental proposal [30] 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 a third direction, it is interesting to note that designs for classical blockchains have also advanced in various ways, some with non-trivial casual data [13]. One can look at combining such systems with other temporal quantum concepts, such as the work in quantum casual structures [31–33]. 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 non-classical ways; this may also lead a type of information-theoretic investigation into the nature of time [36, 37]. Furthermore, unlike general relativistic time machines [38–41], all the subcomponents of this system have shown to be realizable [22–24, 27]; this suggests the possibility to experimentally probe time travel paradoxes through quantum information. At the very least, this proposal would lead to direct experimental probes of quantum causality.

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. 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.

Acknowledgments: DR was indirectly supported by the Marsden fund, administered by the Royal Society of New Zealand. MV was directly supported by the Marsden fund, administered by the Royal Society of New Zealand.

[1] M.A. Nielsen and I.L Chuang, *Quantum computation and quantum information*. (Cambridge University Press, 2010).
[2] D. McMahon, *Quantum computing explained*. (John Wiley & Sons, 2007).
[3] A. Montananao, "Quantum algorithms: an overview", NPJ Quantum Information, **2**, 15023 (2016).
[4] W. Zeng, B. Johnson, R. Smith, N. Rubin, M. Reagor, C. Ryan, and C. Rigetti, "First quantum computers need smart software", Nature, **549**, 149 (2017).
[5] D. Castelvecchi, "Quantum computers ready to leap out of the lab in 2017", Nature News, **541**, 9 (2017).
[6] D. Castelvecchi, "The quantum internet has arrived (and it hasn't).", Nature, **554**, 289 (2018).
[7] C. Simon, "Towards a global quantum network", Nature Photonics, **11**, 678 (2017).
[8] R. Bedington, J.M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution", NPJ Quantum Information, **3**, 30 (2017).
[9] C.H. Bennett and S.J. Wiesner, "Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states", Physical Review Letters, **69**, 2881 (1992).
[10] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", https://bitcoin.org/bitcoin.pdf, (2008).
[11] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake", (2012). https://peercoin.net/assets/paper/peercoin-paper.pdf
[12] J.H. Witte, "The Blockchain: A Gentle Four Page Introduction", arXiv:1612.06244 [q-fin] (2016).
[13] V. Buterin, "Chain interoperability", https://www.r3cev.com/s/Chain-Interoperability-8g6f.pdf, (2016).
[14] D. Aggarwal, G.K. Brennen, T. Lee, M. Santha and M. Tomamichel, "Quantum attacks on Bitcoin, and how to protect against them", arXiv:1710.10377 [quant-ph] (2017).
[15] E.O. Kiktenko, N.O. Pozhar, M.N. Anufriev, A.S. Trushechkin, R.R. Yunusov, Y.V. Kurochkin, A.I. Lvovsky, and A.K. Fedorov, "Quantum-secured blockchain", arXiv:1705.09258 [quant-ph] (2017).
[16] K.P. Kalinin and N.G. Berloff, '"Blockchain platform with proof-of-work based on analog Hamiltonian optimisers", arXiv:1802.10091 [quant-ph] (2018).
[17] J. Jogenfors, "Quantum bitcoin: An anonymous and distributed currency secured by the no-cloning theorem of quantum mechanics", arXiv:1604.01383 [quant-ph] (2016).
[18] D. Sapaev, D. Bulychkov, F. Ablayev, A. Vasiliev, and M. Ziatdinov, "Quantum-assisted Blockchain", arXiv:1802.06763 [quant-ph] (2018).
[19] A. Behera and G. Paul, "Quantum to classical one way function and its applications in quantum money authentication", arXiv:1801.01910 [quant-ph] (2018).
[20] L. Tessler and T. Byrnes, "Bitcoin and quantum computing", arXiv:1711.04235 [quant-ph] (2017).
[21] K. Ikeda, "qBitcoin: A Peer-to-Peer Quantum Cash System", arXiv:1708.04955 [q-fin] (2017).
[22] E. Megidish, A. Halevy, T. Shacham, T. Dvir, L. Dovrat, and H. S. Eisenberg, "Entanglement swapping between photons that have never coexisted", Physical Review Letters, **110**, 210403 (2013).
[23] E. Megidish, T. Shacham, A. Halevy, L. Dovrat, and H. S. Eisenberg, "Resource efficient source of multiphoton polarization entanglement", Physical Review Letters, **109**, 080504 (2012).
[24] E. Megidish, A. Halevy, Y. Pilnyak, A. Slapa, and H. S. Eisenberg, "Quantum tomography of inductively-created large multiphoton states", arXiv:1712.03633 [quant-ph] (2017).
[25] G. Carvacho, F. Graffitti, V. D'Ambrosio, B.C. Hiesmayr, and F. Sciarrino, "Experimental investigation on the geometry of GHZ states", Scientific Reports, **7**, 13265 (2017).
[26] J. Katz and Y. Lindell, *Introduction to modern cryptography*. (CRC Press, 2014).
[27] W. McCutcheon, A. Pappa, B.A. Bell, A. McMillan, A. Chailloux, T. Lawson, M. Mafu, D. Markham, E. Diamanti, Kerenidis, J.G. Rarity1 and M.S. Tame "Experimental verification of multipartite entanglement in quantum networks", Nature Communications, **7**, 13251 (2016).
[28] J.S. Olson and T.C. Ralph, "Entanglement between the future and the past in the quantum vacuum", Physical Review Letters, **106**, 110404 (2011).
[29] J.S. Olson and T.C. Ralph, "Extraction of timelike entanglement from the quantum vacuum", Physical Review A, **85**, 012306 (2012).
[30] C. Sabín, B. Peropadre, M. del Rey, and E. Martín-Martínez, "Extracting past-future vacuum correlations using circuit QED", Physical Review Letters, **109**, 033602 (2012).
[31] O. Oreshkov, F. Costa, and Č. Brukner, "Quantum correlations with no causal order", Nature Communications, **3**, 1092 (2012).
[32] Č. Brukner, "Quantum causality", Nature Physics, **10**, 259 (2014).
[33] R. Chaves, C. Majenz, and D. Gross, "Information–theoretic implications of quantum causal structures", Nature Communications, **6**, 5766 (2015).
[34] D. E. Bruschi, T. Ralph, I. Fuentes, T. Jennewein, and M. Razavi, "Spacetime effects on satellite-based quantum communications", Physical Review D, **90**, 045041 (2014).
[35] D.E. Bruschi, C. Sabn, A. White, V. Baccetti, D.K.L. Oi, and I. Fuentes, "Testing the effects of gravity and motion on quantum entanglement in space-based experiments", New Journal of Physics, **16**, 053041 (2014).
[36] S. Lloyd *et al.*, "Closed timelike curves via post-selection:

Theory and experimental demonstration",
Physical Review Letters, **106**, 040403 (2011).

[37] S. Lloyd, L. Maccone, R. Garcia-Patron, V. Giovannetti, and Y. Shikano, "Quantum mechanics of time travel through post-selected teleportation",
Phys. Rev. **D84**, 025007 (2011).

[38] M. Visser, *Lorentzian wormholes: From Einstein to Hawking* (AIP Press, now Springer, 1995).

[39] S.W. Hawking, "The chronology protection conjecture",
Phys. Rev. **D46**, 603-611 (1992).

[40] M. Visser, "The quantum physics of chronology protection" in *The future of theoretical physics and cosmology: Celebrating Stephen Hawking's 60th birthday. Proceedings, Workshop and Symposium, Cambridge, UK, January 7-10, 2002* (2002) pp. 161-176, arXiv:gr-qc/0204022

[41] M. Visser, "From wormhole to time machine: Comments on Hawking's chronology protection conjecture",
Phys. Rev. **D47**, 554-565 (1993).