Lottery and Auction on Quantum Blockchain

Xin Sun [1], **Piotr Kulicki** [1,*] and **Mirek Sopek** [2]

[1] Department of the Foundations of Computer Science, John Paul II Catholic University of Lublin, 20-950 Lublin, Poland; xin.sun@kul.pl
[2] MakoLab SA, 91-062 Lodz, Poland; sopek@makolab.com
* Correspondence: kulicki@kul.pl

Abstract: This paper proposes a protocol for lottery and a protocol for auction on quantum Blockchain. Our protocol of lottery satisfies randomness, unpredictability, unforgeability, verifiability, decentralization and unconditional security. Our protocol of auction satisfies bid privacy, posterior privacy, bids' binding, decentralization and unconditional security. Except quantum Blockchain, the main technique involved in both protocols is quantum bit commitment.

1. Introduction

A blockchain is a distributed, transparent and append-only ledger of cryptographically linked units of data (blocks). Information is stored in a blockchain in a large decentralized network of parties that do not have to trust one another. The system is distributed in the sense that all nodes of the network, that are in charge of updating the ledger (usually called miners), have separated, identical copies of the ledger. To add a new block to the ledger, the nodes storing the information need to achieve consensus over the content of the ledger.

Cryptocurrencies such as Bitcoin [1] are the best-known applications of blockchain technology. Smart contracts [2], which are enforceable, irrefutable agreements among mutually distrusting peers are another important type of applications. The crucial feature of smart contracts is that they do not require a trusted third party for their administration and enforcement.

Almost all existing blockchain implementations deeply rely on the public-key digital signatures. For that reason, the developments in the field of quantum computing generate a serious threat to them. The factorization tasks, on which the cryptographical power of the public-key digital signatures is based, are hard to solve for traditional computers, but can be easily solved by quantum computers due to quantum algorithms [3]. Quantum computers, discussed for several decades as a theoretical concept, and being in an experimental phase right now, are expected to be ready for wider use quite soon. The current predictions [4] assume that by 2026 the chance of their practical availability is about 15% and by 2031 the chance grows to 50%. As blockchain-based systems are used for the transfer of value, they are particularly vulnerable to an attack. Thus, as pointed out in [5], blockchain technology as we know it today may founder unless it integrates quantum technologies.

There is a significant number of publications related to the quantum-safe blockchain immune to attacks of quantum computers [6–10]. One of the most prominent proposals is the Quantum-secured Blockchain (QB) [6]. It is based on quantum key distribution (QKD) technology that enables an unconditionally secure message authentication. The major limitation of QB is that the consensus protocol it adopts is not efficient, because it becomes exponentially data-intensive if a large number of cheating parties is present. This limitation is overcome in [9], where a new consensus protocol is proposed, with only quadratic dependence of resources on the number of miners.

Quantum-secured Blockchain, as well as other quantum-safe blockchain systems, gives us a general scheme of a distributed ledger, but does not offer protocols for specific tasks like voting, lottery or auction that may be built on top of them. In [10] a simple voting protocol based quantum blockchain is defined. In the present paper, in order to further demonstrate the power and application potential of quantum blockchain, we present protocols for lottery and auction.

While the auction protocol we propose is the first one of the kind, a lottery protocol for quantum blockchain was already mentioned in [9]. The lottery protocol presented there is, however, defined for only two parties and for that reason cannot be applied to the majority of lotteries. In contrast, the protocol we present in the present paper is designed for any number of players and is secured by a group of miners. The main technique that we will use for our lottery and auction protocols, except for quantum blockchain, is quantum bit commitment.

The lottery business is a huge industry of a multi-billion dollar turnover [11]. A lottery is organized by a trusted authority for a usually large number of players. To participate in the game players buy tickets from the organizer. Then, a random process determines the winning tickets. Since revenue is often huge, so is the incentive to cheat. In order to ensure fair play and the trust of players, a lottery protocol should satisfy the following requirements [12–17]:

1. Randomness. All tickets are equally likely to win.
2. Unpredictability. No player can predict the winning ticket.
3. Unforgeability. Tickets cannot be forged. Especially, it is impossible to create a winning ticket after the outcome of the random process is known.
4. Verifiablity. The number and the revenue of winning tickets are publicly verifiable.
5. Decentralization. The random process does not rely on a single authority.

Lottery protocols that satisfy the above requirements already exist [12,16]. With the threat from prospective quantum computers, it is reasonable to require that lottery protocols also satisfy another property:

6. Unconditional security. Even an adversary with an unlimited power of computation cannot rig the lottery.

Although quantum coin flipping [18–25], a specific form of lottery, has been researched in the past 20 years, only randomness and the unconditional security has been studied in those works, while other properties of a lottery have rarely been addressed in this context. In this paper, we design a lottery protocol that satisfies all the above requirements appropriate for multiple players.

Auction is an even more important business in the sense that trillions of dollars are transferred by auctions. An auction is a process of buying and selling goods by offering them up for bid, taking bids, and then selling the item to the buyer who offers the highest bid. In general, there are two types of auctions: sealed-bid auction and non-sealed-bid auction. The main advantage of the sealed-bid auction lies in the fact that no buyer gets to know the bids offered by other buyers. In the literature [26–28] it is acknowledged that an ideal sealed-bid auction must satisfy the following properties:

1. Bid privacy. The submitted bids are not visible to other buyers during the bidding phase.
2. Posterior privacy. The losing bids are not revealed to the public. In other words, only the seller knows all losing bids and their corresponding buyers.
3. Bids' binding. Buyers cannot deny or change their bids once they are committed.

In the setting of quantum blockchain, it is reasonable to require that the auction protocol further satisfies the following properties:

4. Decentralization. The process of the auction does not rely on a single trusted third party.
5. Unconditional security. Even an adversary with an unlimited power of computation cannot manipulate the process of auction.

While blockchain-based auction [29,30] does satisfy decentralization and quantum auction [31,32] does satisfy unconditional security, no existing auction protocol satisfies both of these properties. The auction protocol we are going to propose satisfies all the above properties.

The rest of the paper is organized as follows. In Section 2 we review some background knowledge of quantum blockchain and quantum bit commitment. In Section 3 we present our lottery protocol and in Section 4 our auction protocol. In Section 5 we present conclusions and remarks on the future work.

2. Background

2.1. Quantum Blockchain

The concept of quantum blockchain was presented in [6,9,10]. We are using this general framework to specify lottery and auction protocols. We assume that each pair of nodes is connected by a quantum channel and a classical channel. Every pair of nodes can establish a sequence of secret keys by using the quantum key distribution [33] mechanisms. Those keys will later be used for secure communication.

New transactions or new messages (updates) on the blockchain are initiated by the nodes that wish to append some new data to the chain. Each miner checks the consistency of the update with respect to their local copy of the ledger and works out a judgment regarding the update's admissibility. Then, all the miners apply a consensus algorithm to the update, arriving at a consensus regarding the correct version of the update.

In this paper, we will consider quantum blockchain on a high level, omitting its detailed structure and mechanism, and taking advantage of its following desired properties:

1. Every node is a (small scale) quantum computer which can run some quantum computation on a small number of qubits. More specifically, nodes are capable of performing the quantum computation involved in at least one quantum bit commitment protocol.
2. The communication between different nodes is unconditionally secure.
3. There is a consensus algorithm which can be used by all miners to achieve consensus. The consensus mechanism is immune to attacks. A general definition of the consensus algorithm is given as the following.

Definition 1 (consensus algorithm)**.** *An algorithm among n parties, in which every party p holds an input value $x_p \in D$ (for some finite domain D) and eventually, decide on an output value in $y_p \in D$, is said to achieve consensus if the algorithm guarantees that the output values of all honest parties are the same.*

2.2. Quantum Bit Commitment

Bit commitment typically consists of two phases, namely: commitment and opening. In the commitment phase, a sender chooses a bit a ($a = 0$ or 1) and presents to a receiver some evidence about it. In the opening phase, the sender discloses more information to the receiver. That information enables the receiver to reconstruct the initial bit. Let us use a' to call the reconstructed bit. A useful bit commitment should be correct, concealing and binding. A correct bit commitment protocol will ensure that the initial bit is equal to the reconstructed one: $a = a'$. A protocol is concealing if a receiver cannot get to know the bit before the opening phase, and is binding if a sender cannot change the bit after the commitment phase.

The design of the first quantum bit commitment (QBC) protocol can be attributed to Bennett and Brassard [33]. A number of QBC protocols have been designed to achieve unconditional security (see e.g., [34,35]). Although according to the Mayers-Lo-Chau (MLC) no-go theorem [36–38], unconditionally secure QBC cannot be achieved within the theory of quantum mechanics, scientists have found ways to overcome this negative result in the past two decades. Among them, let us mention cheat-sensitive quantum bit commitment (CSQBC) [39–43] and relativistic QBC [44–49] protocols. Accompanied by well-designed punishment mechanisms the CSQBC can be useful in practice and resilient to the attack of quantum computers. Relativistic QBC protocols make use of

relativity theory and also achieve unconditional security (see [49], where a protocol is presented in which a bit is concealed for 24 hours). Another practically useful QBC can be found in He [50,51], who proposed a QBC protocol based on the use of Mach-Zehnder interferometer.

The following is an abstract yet rigorous definition of QBC, which can be found in Sun et al. [38] and will be used in this paper.

Definition 2 (quantum bit commitment). *A quantum bit commitment protocol consists of the following:*

(1) Two finite-dimensional Hilbert spaces A and B.

(2) A function commit : $\{0,1\} \mapsto A \otimes B$.

(3) Two pure states $|c_0\rangle, |c_1\rangle \in A \otimes B$, in which $|c_i\rangle = commit(i)$ is the commitment of i.

(4) A quantum operation (i.e., completely positive, trace-preserving super operator) Open on $A \otimes B$ such that $Open(|c_0\rangle\langle c_0|) \neq Open(|c_1\rangle\langle c_1|)$.

This QBC protocol is concealing if $Tr_A(|c_0\rangle\langle c_0|) = Tr_A(|c_1\rangle\langle c_1|)$. It is binding if there is no unitary U on A such that $(U \otimes I_B)|c_0\rangle = |c_1\rangle$.

3. Lottery on Quantum Blockchain

Now let us present our lottery protocol. In the setting of the lottery, we assume there are n players and every ticket of the lottery is an m-bit string. Our lottery protocol consists of three phases: the ticket purchasing phase, the ticket agreement phase and the winner determination phase. Figure 1 presents a simplified visualization of our protocol.
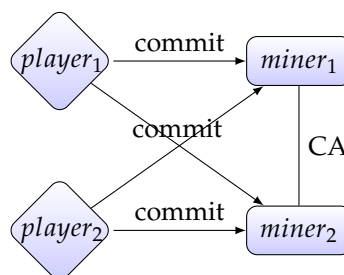

Figure 1. A network of players and miners: players commit their tickets to miners. Miners use a consensus algorithm (CA) to achieve consensus about the players' tickets.

1. Ticket purchasing:

   (a) For every player $p_i \in \{p_1, \ldots, p_n\}$, to purchase a ticket T_i, p_i uses QBC to commit T_i to all miners. At the end of this phase, every miner possesses a list of commitments $(commit(T_1), \ldots, commit(T_n))$.

2. Ticket agreement:

   (a) Every player opens his commitment to every miner, so that the commitments in every miner's possession change to $(Open(commit(T_1)), \ldots, Open(commit(T_n)))$, which essentially equals to $(T_1, \ldots, T_n)$.

   (b) All the miners run a consensus algorithm to achieve a consensus on the tickets $(T_1, \ldots, T_n)$ purchased by players. Every miner adds $(T_1, \ldots, T_n)$ to his local copy of the blockchain.

3. Winner determination:

   (a) The winning ticket is calculated by bit-wise XOR: $T = T_1 \oplus \ldots \oplus T_n$.
   (b) A player's revenue is determined by the Hamming distance between his ticket and the winning ticket T. The closer his ticket is to the winning ticket, the higher is his revenue (a specific rule of revenue which satisfies this principle is beyond the scope of this paper and is left for future work).

Analysis

Our lottery protocol satisfies the following requirements:

1. **Randomness**.

   The winning ticket is calculated by bit-wise XOR. For every index $j \in \{1, \ldots, m\}$ in the winning ticket, $T[j] = 1$ iff $T_1[j] \oplus \ldots \oplus T_n[j] = 1$. Therefore, the probability of $T[j] = 1$ is the same as $T[j] = 0$.

2. **Unpredictability**.

   To predict the winning ticket a player has to know all tickets before they are opened. The concealing property of QBC ensures that even miners cannot know the players' tickets before they are opened. Since tickets are only sent to the miners by QBC, the probability that a player knows all tickets is even lower than the probability that a miner knows them.

3. **Unforgeability**.

   The binding property of QBC ensures that it is impossible to change a ticket after the ticket purchasing phase.

4. **Verifiablity**.

   This is because the quantum blockchain is a transparent database. After the ticket agreement phase, the list $(T_1, \ldots T_n)$ is added to the blockchain. Every player can read all the other players' tickets and calculate the winning ticket by himself.

5. **Decentralization**.

   The random process does not rely on a single authority. Every player's ticket essentially affects the calculation of the winning ticket.Moreover, the calculation of the winning ticket does not rely on a single miner, but on all miners.

6. **Unconditional security**.

   Even an adversary with an unlimited power of computation cannot manipulate the lottery protocol. The concealing and binding property of QBC does not rely on any computational assumption. Nor does the security of the consensus algorithm. The unconditional security of the ledger is further guaranteed by the unconditional security of the digital signature schemes adopted by quantum Blockchain.

4. Auction on Quantum Blockchain

In our protocol of auction, we assume three types of participants: one seller S, m buyers $\{B_1, \ldots, B_m\}$ and n miners $\{M_1, \ldots, M_n\}$. Our protocol works as follows: First all buyers send their bids to the seller. Then the seller calculates which buyer is the winner. Finally, all miners verify the seller's calculation. Figure 2 is a brief visualization of the process of auction. There are five phases in our protocol.
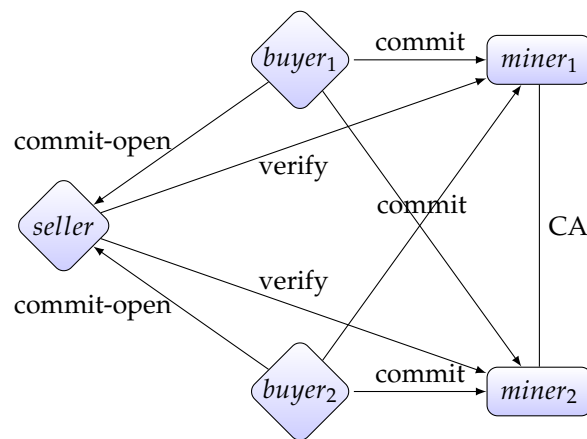
Figure 2. A network of the seller, buyers and miners.

1. The bidding phase: Every buyer B_i commits his bid b_i to the seller and to all miners M_j, where b_i is a positive integer.
2. The opening phase: Every buyer opens his bid to the seller.
3. Decision phase: The seller calculates the winning bid, which is the highest bid (if there is a tie, then one of the maximal bids is chosen randomly), and the winning buyer, who has offered the winning bid.
4. Verification phase: In this phase, the seller S and every miner M_j ($1 \leq j \leq n$) run the following procedure to convince M_j that S has chosen the valid winner:

    (a) S sends the information about the winning buyer B_w and his bid b_w to the miner M_j.
    (b) S permutes losing bids to obtain a new list of $m-1$ bids $(b'_1, \ldots, b'_{m-1})$.
    (c) S sends $b'_1, \ldots, b'_{m-1}$ to M_j.
    (d) M_j first checks if $b_w \geq b'_k$ for all $k \in \{1, \ldots, m-1\}$. If yes, then M_j sends $(b_w, b'_1, \ldots, b'_{m-1})$ to all buyers. Otherwise, M_j sets S as a cheater by setting output to $\perp$.
    (e) After receiving $(b_w, b'_1, \ldots, b'_{m-1})$, every buyer B_i checks if his bid is in the list, i.e., there is some $b'_k = b_i$. If yes, then B_i sends the message "valid" to M_j. Otherwise B_i opens b_i to M_j. M_j then sets S as a cheater by setting output to $\perp$.
    (f) If M_j does not output $\perp$, then the seller passes the verification phase. The output of M_j is now $(b_w, b'_1, \ldots, b'_{m-1}, B_w)$

5. Publication phase: All miners run the consensus algorithm to achieve consensus on the output of the verification phase. The consensus is then added to the blockchain.

Analysis

Our auction protocol satisfies the following requirements:

1. **Bid privacy**.

   Every buyer only commits and opens his bids to the seller. Therefore, no buyer knows other buyers' bids.

2. **Posterior privacy**.

   What is added to the blockchain is the winning buyer and his bid, as well as a permuted list of losing bids. Therefore, no losing buyer's bid is revealed.

3. **Bids' binding**.

   The binding property of quantum bit commitment ensures that buyers cannot deny or change their bids once they are committed.

4. **Decentralization**.

   There are in total n miners. The process of the auction does not rely on a single miner.

5. **Unconditional security**.

   As in the case of our lottery protocol, even an adversary with an unlimited power of computation cannot manipulate the auction protocol because the security of the quantum bit commitment and consensus algorithm does not depend on computational complexity. The unconditional security of the ledger relies on quantum Blockchain properties.

5. Conclusions and Future Work

This paper proposes a lottery protocol and an auction protocol based on quantum bit commitment and quantum blockchain. These protocols satisfy all the important properties of distributed lottery/auction and are implementable by the current technology.

In the future, we are interested in applying quantum blockchain to the general field of multi-party computation. We believe that quantum blockchain will provide new insights into these interesting tasks. We estimate that in the future more complicated protocols (smart contracts) on the quantum blockchain will be designed. Developing a formal tool for the specification and verification of smart contracts on the quantum blockchain is on our agenda. The recently developed categorical logic of quantum programs [52] seems to be a good starting point.

Author Contributions: Conceptualization, X.S., P.K. and M.S; formal analysis, X.S. and P.K.; methodology, X.S.; project administration, P.K.; funding acquisition, P.K.; supervision, P.K.; validation, P.K. and M.S.;writing—original draft, X.S.; writing—review & editing, P.K. and M.S. All authors have read and agreed to the published version of the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 19 November 2020).
2. Szabo, N. The Idea of Smart Contracts. 1997. Available online: https://nakamotoinstitute.org/the-idea-of-smart-contracts/ (accessed on 19 November 2020).
3. Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.* **1997**, *26*, 1484–1509. [CrossRef]
4. Mosca, M. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *IEEE Secur. Priv.* **2018**, *16*, 38–41. [CrossRef]
5. Fedorov, A.K.; Kiktenko, E.O.; Lvovsky, A.I. Quantum computers put blockchain security at risk. *Nature* **2018**, *563*, 465–467. [CrossRef]
6. 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. *Quantum Sci. Technol.* **2018**, *3*, 035004. [CrossRef]
7. Aggarwal, D.; Brennen, G.; Lee, T.; Santha, M.; Tomamichel, M. Quantum Attacks on Bitcoin, and How to Protect Against Them. *Ledger* **2018**, *3*. [CrossRef]
8. Stewart, I.; Ilie, D.; Zamyatin, A.; Werner, S.; Torshizi, M.; Knottenbelt, W. Committing to quantum resistance: a slow defence for Bitcoin against a fast quantum computing attack. *R. Soc. Open Sci.* **2018**, *5*, 180410. [CrossRef] [PubMed]

9. Sun, X.; Sopek, M.; Wang, Q.; Kulicki, P. Towards Quantum-Secured Permissioned Blockchain: Signature, Consensus, and Logic. *Entropy* **2019**, *21*, 887. [CrossRef]
10. Sun, X.; Wang, Q.; Kulicki, P.; Sopek, M. A Simple Voting Protocol on Quantum Blockchain. *Int. J. Theor. Phys.* **2019**, *58*, 275–281. [CrossRef]
11. Isidore, C. Americans Spend More on the Lottery Than on. Available online: https://money.cnn.com/2015/02/11/news/companies/lottery-spending/ (accessed on 19 November 2020).
12. Chow, S.S.M.; Hui, L.C.K.; Yiu, S.; Chow, K.P. An e-Lottery Scheme Using Verifiable Random Function. In Proceedings of the International Conference on Computational Science and its Applications, Singapore, 9–12 May 2005; pp. 651–660. [CrossRef]
13. Bentov, I.; Kumaresan, R. How to Use Bitcoin to Design Fair Protocols. In Proceedings of the Advances in Cryptology—CRYPTO 2014—34th Annual Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 2014; pp. 421–439. [CrossRef]
14. Andrychowicz, M.; Dziembowski, S.; Malinowski, D.; Mazurek, L. Secure Multiparty Computations on Bitcoin. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, SP 2014, Berkeley, CA, USA, 18–21 May 2014; IEEE Computer Society: Washington, DC, USA, 2014; pp. 443–458. [CrossRef]
15. Bartoletti, M.; Zunino, R. Constant-Deposit Multiparty Lotteries on Bitcoin. In *International Conference on Financial Cryptography and Data Security*; Springer: Cham, Switzerland, 2017, Volume 10323, pp. 231–247. [CrossRef]
16. Grumbach, S.; Riemann, R. Distributed Random Process for a Large-Scale Peer-to-Peer Lottery. In *Distributed Applications and Interoperable Systems*; Chen, L.Y., Reiser, H.P., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 34–48.
17. Miller, A.; Bentov, I. Zero-Collateral Lotteries in Bitcoin and Ethereum. In Proceedings of the 2017 IEEE European Symposium on Security and Privacy Workshops, EuroS&P Workshops 2017, Paris, France, 26–28 April 2017; pp. 4–13. [CrossRef]
18. Goldenberg, L.; Vaidman, L.; Wiesner, S. Quantum Gambling. *Phys. Rev. Lett.* **1999**, *82*, 3356–3359. [CrossRef]
19. Spekkens, R.W.; Rudolph, T. Quantum Protocol for Cheat-Sensitive Weak Coin Flipping. *Phys. Rev. Lett.* **2002**, *89*, 227901. [CrossRef]
20. Nayak, A.; Shor, P. Bit-commitment-based quantum coin flipping. *Phys. Rev. A* **2003**, *67*, 012304. [CrossRef]
21. Ambainis, A.; Buhrman, H.; Dodis, Y.; Rohrig, H. Multiparty Quantum Coin Flipping. In Proceedings of the 19th IEEE Annual Conference on Computational Complexity, Amherst, MA, USA, 24 June 2004; IEEE Computer Society: Washington, DC, USA, 2004; pp. 250–259. [CrossRef]
22. Nguyen, A.T.; Frison, J.; Huy, K.P.; Massar, S. Experimental quantum tossing of a single coin. *New J. Phys.* **2008**, *10*, 083037. [CrossRef]
23. Silman, J.; Chailloux, A.; Aharon, N.; Kerenidis, I.; Pironio, S.; Massar, S. Fully Distrustful Quantum Bit Commitment and Coin Flipping. *Phys. Rev. Lett.* **2011**, *106*, 220501. [CrossRef] [PubMed]
24. Hänggi, E.; Wullschleger, J. *Tight Bounds for Classical and Quantum Coin Flipping. Theory of Cryptography*; Ishai, Y., Ed.; Springer: Berlin/Heidelberg, Germany, 2011; pp. 468–485.
25. Nayak, A.; Sikora, J.; Tunçel, L. A search for quantum coin-flipping protocols using optimization techniques. *Math. Program.* **2016**, *156*, 581–613. [CrossRef]
26. Brandt, F. Fully Private Auctions in a Constant Number of Rounds. In *Financial Cryptography, Proceedings of the International Conference on Financial Cryptography, Guadeloupe, France, 27–30 January 2003*; Springer: Berlin/Heidelberg, Germany, 2003; Volume 2742, pp. 223–238. [CrossRef]
27. Brandt, F. How to obtain full privacy in auctions. *Int. J. Inf. Secur.* **2006**, *5*, 201–216. [CrossRef]
28. Montenegro, J.A.; Fischer, M.J.; Lopez, J.; Peralta, R. Secure sealed-bid online auctions using discreet cryptographic proofs. *Math. Comput. Model.* **2013**, *57*, 2583–2595. doi:10.1016/j.mcm.2011.07.027. [CrossRef]
29. Blass, E.O.; Kerschbaum, F. Strain: A Secure Auction for Blockchains. In *Computer Security*; Lopez, J., Zhou, J., Soriano, M., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 87–110.
30. Galal, H.S.; Youssef, A.M. Succinctly Verifiable Sealed-Bid Auction Smart Contract. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*; Garcia-Alfaro, J., Herrera-Joancomartí, J., Livraga, G., Rios, R., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 3–19.
31. Liu, W.; Wang, H.; Yuan, G.; Xu, Y.; Chen, Z.; An, X.; Ji, F.; Gnitou, G.T. Multiparty quantum sealed-bid auction using single photons as message carrier. *Quantum Inf. Process.* **2016**, *15*, 869–879. [CrossRef]

32. Zhang, R.; Shi, R.; Qin, J.; Peng, Z. An economic and feasible Quantum Sealed-bid Auction protocol. *Quantum Inf. Process.* **2018**, *17*, 35. [CrossRef]

33. Bennetta, C.; GillesBrassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 9–12 December 1984, pp. 175–179.

34. Brassard, G.; Crépeau, C. Quantum Bit Commitment and Coin Tossing Protocols. In *Conference on the Theory and Application of Cryptography*; Menezes, A., Vanstone, S.A., Eds;. Springer: Berlin/Heidelberg, Germany, 1990; pp. 49–61.

35. Brassard, G.; Crépeau, C.; Jozsa, R.; Langlois, D. A Quantum Bit Commitment Scheme Provably Unbreakable by both Parties. In Proceedings of the 34th Annual Symposium on Foundations of Computer Science, Palo Alto, CA, USA, 3–5 November 1993; IEEE Computer Society: Washington, DC, USA, 1993; pp. 362–371. [CrossRef]

36. Mayers, D. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.* **1997**, *78*, 3414–3417. [CrossRef]

37. Lo, H.K.; Chau, H.F. Is Quantum Bit Commitment Really Possible? *Phys. Rev. Lett.* **1997**, *78*, 3410–3413. [CrossRef]

38. Sun, X.; He, F.; Wang, Q. Impossibility of Quantum Bit Commitment, a Categorical Perspective. *Axioms* **2020**, *9*, 28. [CrossRef]

39. Hardy, L.; Kent, A. Cheat Sensitive Quantum Bit Commitment. *Phys. Rev. Lett.* **2004**, *92*, 1–4. [CrossRef] [PubMed]

40. Buhrman, H.; Christandl, M.; Hayden, P.; Lo, H.K.; Wehner, S. Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment. *Phys. Rev. A* **2008**, *78*, 1–10. [CrossRef]

41. Shimizu, K.; Fukasaka, H.; Tamaki, K.; Imoto, N. Cheat-sensitive commitment of a classical bit coded in a block of m × n round-trip qubits. *Phys. Rev. A* **2011**, *84*, 1–14. [CrossRef]

42. Li, Y.; Wen, Q.; Li, Z.; Qin, S.; Yang, Y. Cheat sensitive quantum bit commitment via pre- and post-selected quantum states. *Quantum Inf. Process.* **2014**, *13*, 141–149. [CrossRef]

43. Zhou, L.; Sun, X.; Su, C.; Liu, Z.; Choo, K.R. Game theoretic security of quantum bit commitment. *Inf. Sci.* **2019**, *479*, 503–514. [CrossRef]

44. Kent, A. Unconditionally secure bit commitment with flying qudits. *New J. Phys.* **2011**, *13*, 1–16. [CrossRef]

45. Kent, A. Unconditionally Secure Bit Commitment by Transmitting Measurement Outcomes. *Phys. Rev. Lett.* **2012**, *109*, 130501. [CrossRef]

46. Lunghi, T.; Kaniewski, J.; Bussières, F.; Houlmann, R.; Tomamichel, M.; Kent, A.; Gisin, N.; Wehner, S.; Zbinden, H. Experimental Bit Commitment Based on Quantum Communication and Special Relativity. *Phys. Rev. Lett.* **2013**, *111*, 180504. [CrossRef]

47. Adlam, E.; Kent, A. Device-independent relativistic quantum bit commitment. *Phys. Rev. A* **2015**, *92*, 1–9. [CrossRef]

48. Lunghi, T.; Kaniewski, J.; Bussières, F.; Houlmann, R.; Tomamichel, M.; Wehner, S.; Zbinden, H. Practical Relativistic Bit Commitment. *Phys. Rev. Lett.* **2015**, *115*, 030502. [CrossRef] [PubMed]

49. Verbanis, E.; Martin, A.; Houlmann, R.; Boso, G.; Bussières, F.; Zbinden, H. 24-Hour Relativistic Bit Commitment. *Phys. Rev. Lett.* **2016**, *117*, 140506. [CrossRef] [PubMed]

50. He, G.P. Quantum key distribution based on orthogonal states allows secure quantum bit commitment. *J. Phys. A Math. Theor.* **2011**, *44*, 445305. [CrossRef]

51. He, G.P. Simplified quantum bit commitment using single photon nonlocality. *Quantum Inf. Process.* **2014**, *13*, 2195–2211. [CrossRef]

52. Sun, X.; He, F. A First Step to the Categorical Logic of Quantum Programs. *Entropy* **2020**, *22*, 144. [CrossRef]