International Journal of Theoretical Physics (2019) 58: 275–281
https://doi.org/10.1007/s10773-018-3929-6

A Simple Voting Protocol on Quantum Blockchain

Xin Sun[1] · **Quanlong Wang**[2] · **Piotr Kulicki**[1] · **Mirek Sopek**[3]

Received: 4 June 2018 / Accepted: 10 October 2018 / Published online: 18 October 2018

Abstract
This paper proposes a simple voting protocol based on Quantum Blockchain. Despite its simplicity, our protocol satisfies the most important properties of secure voting protocols: is anonymous, binding, non-reusable, verifiable, eligible, fair and self-tallying. The protocol could also be implemented using presently available technology.

Keywords Electronic voting · Quantum computation · Blockchain

1 Introduction

Many voting protocols based on classical cryptography have been developed and successfully applied since Chaum et al. [9]. However, the security of protocols based on classical cryptography is based on the unproven complexity of some computational algorithms, such as the factoring of large numbers. The research in quantum computation shows that quantum computers are able to factor large numbers in a short time, which means that classical protocols based on such algorithms are already insecure. To react to the risk posed by forthcoming quantum computers, a number of quantum voting protocols have been developed in the last decade [3, 15, 16, 18, 24, 25, 38, 40, 41, 43].

To be reliable and useful in practice, voting protocols should satisfy some essential requirements, such as:

1. Anonymity. Only the voter knows how he or she voted.
2. Binding. Nobody can change the ballot after its submission.
3. Non-reusability. Every voter can vote only once.
4. Verifiability. Every voter can verify whether his or her ballot has been counted properly.
5. Eligibility. Only eligible voters can vote.
6. Fairness. Nobody can obtain a partial tally of ballots before the tallying phase.

✉ Xin Sun
xin.sun.logic@gmail.com

[1] Department of the Foundations of Computer Science, The John Paul II Catholic University of Lublin, Lublin, Poland

[2] Department of Computer Science, University of Oxford, Oxford, UK

[3] MakoLab S A, Lodz, Poland

7. Self-tallying. Everyone who is interested in the voting result can tally ballots by himself or herself.

To the best of our knowledge, among all existing quantum voting protocols, only the protocol proposed by Wang et al. [43] satisfies all of the above requirements. However, their protocol is difficult to implement using available technology. Our aim, presented in this paper, was to develop a voting protocol that satisfies all of the above requirements, and in addition, can be implemented by presently available technology.

The key feature of our protocol is its utilization of the Quantum Blockchain developed and described in [21, 34]. It turns out that Blockchain can significantly simplify the design of the protocol for electronic voting. A quantum bit commitment protocol is also needed to ensure some essential properties of voting. There are quantum bit commitment protocols in existence, which are both highly secure and implementable by the current technology. See, for example [14, 33, 42]. Either of these solutions can be used in our voting protocol.

We first review some background knowledge on the Quantum Blockchain and the quantum bit commitment (Section 2). Then, in Section 3, we present our voting protocol based on Quantum Blockchain. We finish this paper in Section 4, with conclusions and remarks on the future work.

2 Background

2.1 Quantum Blockchain

Blockchain is a distributed, transparent and append-only database technology which incorporates the mechanisms for achieving consensus over data in a large decentralised network of agents who do not trust each other. It is distributed in the sense that each of its nodes and every miner (an agent in charge of updating the database) have an identical copy of the database. One of the most prominent applications of Blockchain technology is to enable the creation and existence of cryptocurrencies, such as Bitcoin [30]. Another important application is the implementation of self-executable "smart contracts" [2, 35] - computational protocols for execution of trustworthy transactions without involvement of any third party.

The concept of the Quantum Blockchain presented in [21, 34], which we are going to explore for our voting protocol, assumes that each pair of nodes (agents) is connected by an authenticated quantum channel and by a classical channel which does not need to be fully authenticated. Every pair of nodes can establish a sequence of secret keys by using Quantum Key Distribution [5] mechanisms. Those keys will later be used for message authentication.

Updates (new transactions or new messages) on Blockchain are initiated by those nodes who wish to append some new data to the chain. The classical data of an update is sent via classical channels to all miners, while the quantum data of the update is sent via quantum channels. Each miner checks the consistency of the update with respect to their local copy of the database and works out a judgement regarding the update's admissibility.

Then all the miners apply a (quantum) Byzantine agreement protocol [4, 10, 11, 17, 22, 31, 37] to the update, arriving at a consensus regarding the correct version of the update and whether the update is admissible. Finally, if at least half of the miners agree that the update is admissible, the update is added to the copies of the database of every node.

2.2 Quantum Bit Commitment

Bit commitment, used in a wide range of cryptographic protocols (e.g. zero-knowledge proof, multiparty secure computation, and oblivious transfer), typically consists of two phases, namely: commitment and opening. In the commitment phase, Alice the sender, chooses a bit a ($a = 0$ or 1) which she wishes to commit to Bob, the receiver. Then Alice presents Bob some evidence about the bit. The committed bit cannot be known by Bob prior to the opening phase. Later, in the opening phase, Alice discloses some information needed for the reconstruction of a. Then, Bob reconstructs a bit a' using Alice's evidence and the disclosure. A correct bit commitment protocol will ensure that $a' = a$. A bit commitment protocol is concealing if Bob cannot know the bit Alice committed before the opening phase, and is binding if Alice cannot change the bit she committed after the commitment phase.

The first quantum bit commitment (QBC) protocol was proposed in 1984 by Bennett and Brassard [5]. A QBC protocol is unconditionally secure if any cheating can be detected with a probability arbitrarily close to 1. Here, Alice is cheating if she changes the committed bit after the commitment phase, while Bob is cheating when he learns about the committed bit before the opening phase. A number of QBC protocols have been designed to achieve unconditional security, such as those of [6, 7]. However, according to the Mayers-Lo-Chau (MLC) no-go theorem [26, 29], unconditionally secure QBC in principle can never be achieved.

Although unconditionally secure QBC seems to be impossible, several QBC protocols satisfy some other notions of security, such as cheat-sensitivity. For example, cheat-sensitive quantum bit commitment (CSQBC) protocols [8, 12, 23, 32, 45] and relativistic QBC protocols [1, 19, 20, 27, 28, 42] have been developed. In CSQBC protocols, the probability of detecting cheating is merely required to be non-zero. According to this less stringent security requirement, many QBC protocols which are not unconditional secure are regarded as secure within the notion of cheat-sensitivity. With well-designed mechanisms of punishment, the CSQBC protocols can be useful in practice and resilient to an attack of quantum computers.

In Sun and Wang [33] a CSQBC protocol is proposed which is more secure and efficient than all other existing CSQBC protocols. According to Tatar et al. [36], this protocol is also practically resilient to the entanglement attack, which damages the unconditional security of many QBC protocols [26, 29]. Moreover, this protocol is implementable by the current technology.

Relativistic QBC protocols achieve unconditional security by making use of the power of relativity theory. In [42], the authors implemented a relativistic QBC protocol in which the bit is concealed for 24 hours.

He [13, 14] proposed a QBC protocol based on the use of Mach-Zehnder interferometer. His protocol is immune to the cheating strategy in the light of MLC no-go theorem, because the density matrices of the committed states in his protocol do not satisfy an important condition required by the MLC no-go theorem. He's protocol is also implementable by the current technology.

To sum up, practically useful QBC protocols are already available and are ready for applications to other computational tasks.

3 Voting on Quantum Blockchain

In the simplest setting for voting, n voters vote on an issue. Every voter V_i has a private binary value $v_i \in \{0, 1\}$, where $v_i = 0$ means disagreement, and $v_i = 1$ means agreement,

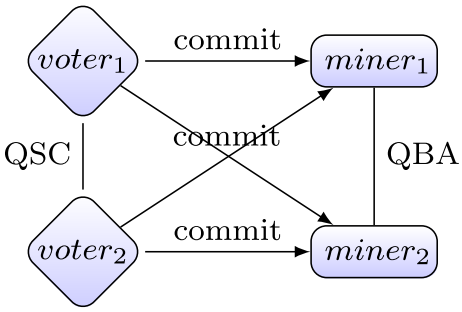

Fig. 1 A network of voters and miners: Voters use quantum secure communication (QSC) to distribute matrix. Voters commit their masked ballots to miners. Miners use quantum Byzantine agreement (QBA) to achieve consensus about voters' masked ballot

with the issue. Our protocol for simple voting, of which the structure is similar to (and simpler than) the voting protocol on the Bitcoin blockchain [39, 44], consists of two phases: the ballot commitment phase and the ballot tallying phase. Figure 1 presents simplified visualization of our protocol.

1. Ballot commitment.
   (a) For every $i \in \{1, \ldots, n\}$, voter V_i generates the i-th row of an $n \times n$ matrix of integers $r_{i,1}, \ldots r_{i,n}$, of which the sum $\sum_j r_{i,j}$ and 0 are congruent modulo $n+1$. That is, $\sum_j r_{i,j} \equiv 0 \ (mod\ n+1)$.
   (b) For every i and j, voter V_i sends $r_{i,j}$ to V_j via quantum secure communication [5, 46].
   (c) Now for every i, voter V_i knows the i-th column $r_{1,i}, \ldots, r_{n,i}$. Then he computes his masked ballot $\widehat{v_i} \equiv v_i + \sum_j r_{j,i} \ (mod\ n+1)$. V_i commits $\widehat{v_i}$ to every miner of the blockchain by a QBC protocol.
2. Ballot tallying by decommitment.
   (a) For each i, V_i reveal $\widehat{v_i}$ to every miner of the blockchain by opening his commitment.
   (b) All the miners run the quantum honest-success Byzantine agreement protocol [34] to achieve a consensus of on the masked ballot $\widehat{v_1}, \ldots, \widehat{v_n}$.
   (c) The result of voting is obtained by calculating $\sum_i \widehat{v_i}$, which equals to $\sum_i v_i$ because $\sum_i \widehat{v_i} \equiv \sum_i (v_i + \sum_j r_{j,i}) \equiv \sum_i v_i + \sum_{i,j} r_{j,i} \equiv \sum_i (v_i + \sum_j r_{i,j}) \equiv \sum_i v_i \ (mod\ n+1)$.

Example 1 Assume there are 3 voters $\{V_1, V_2, V_3\}$ with $v_1 = v_2 = 1$, $v_3 = 0$ and the matrix generated by those voters is

$$\begin{pmatrix} 2 & 0 & 2 \\ 1 & 1 & 2 \\ 3 & 0 & 1 \end{pmatrix}.$$

Then $\widehat{v_1} = 1 + (2 + 1 + 3) = 7 \equiv 3 \ (mod\ 4)$, $\widehat{v_2} = 1 + (0 + 1 + 0) = 2 \equiv 2 \ (mod\ 4)$, $\widehat{v_3} = 0 + (2 + 2 + 1) = 5 \equiv 1 \ (mod\ 4)$. Then we have $\widehat{v_1} + \widehat{v_2} + \widehat{v_3} = 3 + 2 + 1 \equiv 2 \ (mod\ 4)$, which equals to $v_1 + v_2 + v_3 = 2$.

3.1 Security Analysis

Our voting protocol satisfies the following security requirements:

1. Anonymity.
   The anonymity is guaranteed because the quantum secure communication prohibits other voters to know the entire matrix. Therefore, other voters can only know the masked ballot, while the original ballot stays unknown.
2. Binding.
   Other voters cannot change a voter's ballot because of the authentication procedure of the quantum blockchain, while the success of authentication on the quantum blockchain is guaranteed by Quantum Key Distribution. The voter himself cannot change his submitted ballot because of the binding property of Quantum Bit Commitment.
3. Non-reusability.
   Non-reusability would be violated if a voter could successfully append two different ballots to the blockchain. This is exactly the same as the double-spending attack on Blockchain, which will not be achieved on Quantum Blockchain [34].
4. Verifiability.
   Every voter can easily check if his masked ballot is successfully uploaded to the blockchain because by design it is a transparent database.
5. Eligibility.
   This can be ensured by the authentication procedure of the blockchain: only authenticated voters can successfully communicate to the miners.
6. Fairness.
   Fairness will be destroyed if somebody can partially tally the ballots before the ballot tallying phase. To achieve this, he or she have to know some masked ballots before the ballot tallying phase. Note that according to the concealing property of quantum bit commitment, even the miners cannot know a single masked ballot before the tally phase. Therefore fairness is ensured.
7. Self-tallying.
   This requirement is satisfied because of the transparency of the blockchain. All data on the blockchain is accessible to every interested user. Users can tally ballots simply by calculating the sum of masked ballots.

4 Conclusion and Future Work

This paper proposes a simple voting protocol based on Quantum Blockchain. Besides of being simple, our protocol offers anonymous, binding, non-reusable, verifiable, eligible, fair and self-tallying voting. Besides Quantum Blockchain, other quantum techniques used in our protocol include quantum secure communication and quantum bit commitment. All these techniques are realizable by the current technology.

We have demonstrated that Quantum Blockchain can significantly simplify the task of electronic voting. In the future, we are interested in applying Quantum Blockchain to other fields such as quantum auction and quantum lottery. We believe that Quantum Blockchain will also simplify these interesting tasks.

References

1. Adlam, E., Kent, A.: Device-independent relativistic quantum bit commitment. Phys. Rev. A **92**(022315), 1–9 (2015)
2. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., Caro, A.D., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolic, M., Cocco, S.W., Yellick, J.: Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Oliveira, R., Felber, P., Hu, Y.C. (eds.) Proceedings of the Thirteenth Eurosys Conference, EuroSys 2018, Porto, Portugal, April 23–26, 2018, pp. 30:1–30:15. ACM (2018). https://doi.org/10.1145/3190508.3190538
3. Bao, N., Yunger Halpern, N.: Quantum voting and violation of arrow's impossibility theorem. Phys. Rev. A **95**, 062306 (2017). https://doi.org/10.1103/PhysRevA.95.062306
4. Ben-Or, M., Hassidim, A.: Fast quantum byzantine agreement. In: Proceedings of the Thirty-Seventh Annual Acm Symposium on Theory of Computing, STOC '05, pp. 481–485. ACM, New York, NY, USA (2005). https://doi.org/10.1145/1060590.1060662
5. Bennetta, C., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179 (1984)
6. Brassard, G., Crépeau, C.: Quantum bit commitment and coin tossing protocols. In: Menezes, A., Vanstone, S.A. (eds.) Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, pp. 49–61. Springer (1990)
7. Brassard, G., Crépeau, C., Jozsa, R., Langlois, D.: A quantum bit commitment scheme provably unbreakable by both parties. In: 34th Annual Symposium on Foundations of Computer Science, Palo Alto, California, USA, 3–5 November 1993, pp. 362–371. IEEE Computer Society (1993). https://doi.org/10.1109/SFCS.1993.366851
8. Buhrman, H., Christandl, M., Hayden, P., Lo, H.K., Wehner, S.: Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment. Phys. Rev. A **78**(022316), 1–10 (2008)
9. Chaum, D., Crépeau, C., Damgård, I.: Multiparty unconditionally secure protocols (extended abstract). In: Simon, J. (ed.) Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2–4, 1988, Chicago, Illinois, USA, pp. 11–19. ACM (1988). https://doi.org/10.1145/62212.62214
10. Fitzi, M., Gisin, N., Maurer, U.: Quantum solution to the byzantine agreement problem. Phys. Rev. Lett. **87**(21, No. 217901), 1–4 (2001)
11. Gaertner, S., Bourennane, M., Kurtsiefer, C., Cabello, A., Weinfurter, H.: Experimental demonstration of a quantum protocol for byzantine agreement and liar detection. Phys. Rev. Lett. **100**(7, No. 070504), 1–4 (2008)
12. Hardy, L., Kent, A.: Cheat sensitive quantum bit commitment. Phys. Rev. Lett. **92**(15), 1–4 (2004)
13. He, G.P.: Quantum key distribution based on orthogonal states allows secure quantum bit commitment. J. Phys. A Math. Theor. **44**(44), 445305 (2011). http://stacks.iop.org/1751-8121/44/i=44/a=445305
14. He, G.P.: Simplified quantum bit commitment using single photon nonlocality. Quantum Inf. Process **13**(10), 2195–2211 (2014). https://doi.org/10.1007/s11128-014-0728-8
15. Hillery, M., Ziman, M., Buek, V., Bieliková, M.: Towards quantum-based privacy and voting. Phys. Lett. A **349**(1), 75–81 (2006). https://doi.org/10.1016/j.physleta.2005.09.010. http://www.sciencedirect.com/science/article/pii/S0375960105014738
16. Horoshko, D., Kilin, S.: Quantum anonymous voting with anonymity check. Phys. Lett. A **375**(8), 1172–1175 (2011)
17. Iblisdir, S., Gisin, N.: Byzantine agreement with two quantum-key-distribution setups. Phys. Rev. A **70**(3, No. 034306), 1–2 (2004)
18. Jiang, L., He, G., Nie, D., Xiong, J., Zeng, G.: Quantum anonymous voting for continuous variables. Phys. Rev. A **85**, 042309 (2012). https://doi.org/10.1103/PhysRevA.85.042309
19. Kent, A.: Unconditionally secure bit commitment with flying qudits. New J. Phys. **13**(113015), 1–16 (2011)
20. Kent, A.: Unconditionally secure bit commitment by transmitting measurement outcomes. Phys. Rev. Lett. **109**, 130501 (2012)

21. 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. **3**(3, No. 035004), 1–8 (2018). http://stacks.iop.org/2058-9565/3/i=3/a=035004
22. Lamport, L., Shostak, R.E., Pease, M.C.: The byzantine generals problem. ACM Trans. Program. Lang. Syst. **4**(3), 382–401 (1982). https://doi.org/10.1145/357172.357176
23. 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 **13**(1), 141–149 (2014)
24. Li, Y., Zeng, G.: Quantum anonymous voting systems based on entangled state. Opt. Rev. **15**(5), 219–223 (2008). https://doi.org/10.1007/s10043-008-0034-8
25. Li, Y., Zeng, G.: Anonymous quantum network voting scheme. Opt. Rev. **19**(3), 121–124 (2012). https://doi.org/10.1007/s10043-012-0021-y
26. Lo, H.K., Chau, H.F.: Is quantum bit commitment really possible? Phys. Rev. Lett. **78**(17), 3410–3413 (1997)
27. 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. **111**, 180504 (2013)
28. Lunghi, T., Kaniewski, J., Bussières, F., Houlmann, R., Tomamichel, M., Wehner, S., Zbinden, H.: Practical relativistic bit commitment. Phys. Rev. Lett. **115**, 030502 (2015)
29. Mayers, D.: Unconditionally secure quantum bit commitment is impossible. Phys. Rev. Lett. **78**(17), 3414–3417 (1997)
30. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf (2008)
31. Pease, M.C., Shostak, R.E., Lamport, L.: Reaching agreement in the presence of faults. J. ACM **27**(2), 228–234 (1980). https://doi.org/10.1145/322186.322188
32. 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 **84**(022308), 1–14 (2011)
33. Sun, X., Wang, Q.: Bit commitment in categorical quantum mechanics. Submitted to quantum information processing (2018)
34. Sun, X., Wang, Q., Kulicki, P., Zhao, X.: Quantum-enhanced logic-based Blockchain I: Quantum honest-success byzantine agreement and Qulogicoin. arXiv:1805.06768
35. Szabo, N.: The idea of smart contracts (1997)
36. Tatar, A.E., Nagy, M., Nagy, N.: The cost of breaking a quantum bit commitment protocol on equivalence classes. Parallel Processing Letters. Accepted (2018)
37. Tavakoli1, A., Cabello, A., Zukowski, M., Bourennane, M.: Quantum clock synchronization with a single qudit. Sci. Rep. **5**(7982), 1–4 (2015)
38. Thapliyal, K., Sharma, R.D., Pathak, A.: Protocols for quantum binary voting. Int. J. Quant. Inf. **15**(01), 1750007 (2017). https://doi.org/10.1142/S0219749917500071
39. Tian, H., Fu, L., He, J.: A simpler bitcoin voting protocol. In: Chen, X., Lin, D., Yung, M. (eds.) Information Security and Cryptology, pp. 81-98. Springer International Publishing, Cham (2018)
40. Tian, J.H., Zhang, J.Z., Li, Y.P.: A voting protocol based on the controlled quantum operation teleportation. Int. J. Theor. Phys. **55**(5), 2303–2310 (2016). https://doi.org/10.1007/s10773-015-2868-8
41. Vaccaro, J.A., Spring, J., Chefles, A.: Quantum protocols for anonymous voting and surveying. Phys. Rev. A **75**, 012333 (2007). https://doi.org/10.1103/PhysRevA.75.012333
42. Verbanis, E., Martin, A., Houlmann, R., Boso, G., Bussières, F., Zbinden, H.: 24-hour relativistic bit commitment. Phys. Rev. Lett. **117**, 140506 (2016)
43. Wang, Q., Yu, C., Gao, F., Qi, H., Wen, Q.: Self-tallying quantum anonymous voting. Phys. Rev. A **94**, 022333 (2016). https://doi.org/10.1103/PhysRevA.94.022333
44. Zhao, Z., Chan, T.H.: How to vote privately using bitcoin. In: Qing, S., Okamoto, E., Kim, K., Liu, D. (eds.) Information and Communications Security - 17Th International Conference, ICICS 2015, Beijing, China, December 9-11, 2015, Revised Selected Papers, Lecture Notes in Computer Science, vol. 9543, pp. 82–96. Springer (2015). https://doi.org/10.1007/978-3-319-29814-6
45. Zhou, L., Sun, X., Su, C., Liu, Z., Choo, K.K.R.: Game theoretic security of quantum bit commitment. Information Sciences. https://doi.org/10.1016/j.ins.2018.03.046, http://www.sciencedirect.com/science/article/pii/S0020025518302263 (2018)
46. Zhou, L., Wang, Q., Sun, X., Kulicki, P., Castiglione, A.: Quantum technique for access control in cloud computing II: encryption and key distribution. J. Netw. Comput. Appl. **103**, 178–184 (2018). https://doi.org/10.1016/j.jnca.2017.11.012