Quantum Bitcoin: An Anonymous and Distributed Currency Secured by the No-Cloning Theorem of Quantum Mechanics

Jonathan Jogenfors*

Information Coding Group,
Department of Electrical Engineering,
Linköping University, Sweden

April 27, 2016

Abstract

The digital currency Bitcoin has had remarkable growth since it was first proposed in 2008. Its distributed nature allows currency transactions without a central authority by using cryptographic methods and a data structure called the blockchain. In this paper we use the no-cloning theorem of quantum mechanics to introduce Quantum Bitcoin, a Bitcoin-like currency that runs on a quantum computer. We show that our construction of quantum shards and two blockchains allows untrusted peers to mint quantum money without risking the integrity of the currency. The Quantum Bitcoin protocol has several advantages over classical Bitcoin, including immediate local verification of transactions. This is a major improvement since we no longer need the computationally intensive and time-consuming method Bitcoin uses to record all transactions in the blockchain. Instead, Quantum Bitcoin only records newly minted currency which drastically reduces the footprint and increases efficiency. We present formal security proofs for counterfeiting resistance and show that a quantum bitcoin can be re-used a large number of times before wearing out - just like ordinary coins and banknotes. Quantum Bitcoin is the first distributed quantum money system and we show that the lack of a paper trail implies full anonymity for the users. In addition, there are no transaction fees and the system can scale to any transaction volume.

*Electronic address: jonathan.jogenfors@liu.se

The digital currency Bitcoin was a revolutionary concept when it was published in 2008 [1]. It challenged our conceptions of how what actually constitutes a currency as it needs no central authority to function. Instead, Bitcoin transactions are verified by a distributed voting process where participants, "miners", spend computing power to participate. Central to the Bitcoin protocol is the blockchain, a data structure that enforces consensus across a network.

Classical information can be copied at will. On the other hand, a currency unit of currency must not be copied or the system will fail to work. In Bitcoin, this is called *double-spending*, and a large part of the complexity of the Bitcoin protocol is used to prevent it. Bitcoin exist only as transactions that are added to the end of the blockchain, and a user can compute his or her account balance by summing over all transaction to and from the account.

Double-spending is prevented in Bitcoin by waiting for confirmation by third parties, called miners. These verify the correctness of the transaction details and ensure that no double-spending occurs. In order to add this new transaction to the blockchain, however, they must compete with other miners to add their confirmation to the end of the blockchain. This competition is called a *proof-of-work puzzle*, where they spend computing power to receive a reward. Even though miners are untrusted, this expenditure of energy allows Bitcoin users to trust their confirmations.

However, this protocol comes with a cost. Transactions cannot be finalized immediately and instead, users have to wait roughly 60 minutes [2] before they are sure the transaction was successful. In addition, the sheer size of the ever-growing blockchain (approaching 70 GB as of April 2016) makes it increasingly difficult to store and manage.

Therefore we turn to quantum mechanics. Does quantum physics allow us to create something that prevents double-spending on a more fundamental level? The answer is yes in the form of the no-cloning theorem [3]. This is a peculiar result of quantum mechanics which states that an unknown quantum state cannot be copied. In other words we could use the no-cloning theorem as a copy-protection mechanism on which we then build a currency.

As early as 1970, Wiesner [4] proposed a scheme for quantum cheques, where a bank can create and verify unclonable money tokens. In Wiesner's scheme, the bank prepares a number of qubits in a secret basis. If a counterfeiter wants to create a copy, he or she will not know the correct basis and must measure randomly, which creates errors in both the original and copied cheque. With large probability, this cheque will not pass the verification algorithm. Since Wiesner's original idea, there have been a number of developments into quantum money, including Bennett et al. [5], Lutomirski et al. [6], Farhi et al. [7], and Aaronson and Christiano [8].

In our paper [9] we build a novel payment system: Quantum Bitcoin. In many ways this is *the* ideal currency system as it has advantages over traditional currencies, Bitcoin and previous quantum money proposals. Due to the no-cloning theorem, quantum bitcoin are (almost) self-contained with no need for the complicated transaction list found in classical Bitcoin. Instead, the no-cloning theorem prevents double-spending, and we give a polynomial-time algorithm that verifies a quantum bitcoin without waiting for external

confirmation.

The cornerstone of Quantum Bitcoin is the Hidden-Subspace Mini-Scheme introduced by Aaronson and Christiano [8]. Here, the quantum Bitcoin states are on the form

$$|A\rangle = \frac{1}{\sqrt{|A|}} \sum_{x \in A} |x\rangle \,, \tag{1}$$

where A is a subspace of $\mathbb{F}_2^n$. In our paper, $\mathbb{F}_2^n$ are bit strings of length n and the subspace A is randomly generated from a set of $n/2$ secret generators.

Quantum Bitcoin are minted by generating these quantum states together with a classical serial number s. In the mini-scheme, we can construct a polynomial-time verification algorithm that takes this serial number and quantum state and either accepts or rejects. New currency is generated by a minting process that resembles the classical Bitcoin protocol, where peers spend computing power in an attempt to solve a proof-of-work puzzle.

However, adopting the Bitcoin model straight away leads to something called the *reuse attack*. Quantum Bitcoin are minted by first generating a random, secret "seed" which is then used to generate the quantum bitcoin state using Equation (1). The seed should be safely discarded after the quantum bitcoin can be generated, otherwise it is possible to create new, counterfeit quantum bitcoin. However, we can not trust all minters to really throw away the seed, so we have to assume the existence of dishonest minters.

We prevent the reuse attack by a construction where we add a secondary blockchain to the minting process. Assuming that a majority of the minters are honest and erase their seeds, a minority of malicious minters will not be able to disrupt the system. The primary blockchain now contains descriptors to "quantum shards", which, when assembled in the secondary blockchain, become quantum bitcoin. In this method, a quantum bitcoin consists of many independently-generated shards, so that a majority of minters will have to collude in order to perform a reuse attack.

In our paper we show that the double-blockchain construction can make the probability of reuse attack exponentially small in the security parameters. We also show that counterfeiting is computationally infeasible, i.e. it requires $\Omega(2^{n/4})$ oracle queries for a security parameter n.

If we compare Quantum Bitcoin to traditional money and previous quantum money proposals we note the following: Quantum Bitcoin requires no central point of authority, so new currency can be minted without needing to trust the decisions of a central bank. Instead, policies are enforced by transparent, verifiable algorithms according to a predefined ruleset.

The interesting comparison, however, is the comparison to classical Bitcoin. Compared to the 60-minute transaction times of Bitcoin, Quantum Bitcoin transactions finalize immediately. No interactive network access is needed, except for the receiving party who only needs read access to the blockchain. The blockchain only needs to be recent enough to include the description of the quantum bitcoin being received. In addition, Quantum Bitcoin transactions are free and has a much smaller blockchain.

Another performance advantage is scalability. According to Garzik [10], Bitcoin as originally proposed by Nakamoto [1] has an estimated global limit of seven transactions per second. In comparison, the local transactions of Quantum Bitcoin implies that there is no upper limit to the transaction rate. It should be noted, however, that the minting rate is limited by the capacity of the Quantum Shard and Quantum Bitcoin blockchains. By placing the performance restriction only in the minting procedure, the bottleneck should be much less noticeable than if it were in the transaction rate as well.

Local transactions also mean anonymity, since only the sender and receiver are aware of the transaction even occurring. No record, and therefore no paper trail, is created. In essence, a Quantum Bitcoin transaction is similar to that of ordinary banknotes and coins, except no central point of authority has to be trusted. Bitcoin, on the other hand, records all transactions in the blockchain which allows anybody with a copy to trace transaction flows, even well after the fact. This has been used by several authors [11–16] to de-anonymize Bitcoin users.

To conclude, Quantum Bitcoin is a tangible application of quantum mechanics where we construct the ideal distributed, publicly-verifiable payment system. The currency works on its own without a central authority, and can begin to function as soon as it is experimentally possible to prepare, store, measure and reconstruct quantum states with low enough noise. The no-cloning theorem provides the foundation of copy-protection, and the addition of a blockchain allows us to produce currency in a distributed and democratic fashion. Quantum Bitcoin is the first example of a secure, distributed payment system with local transactions and can provide the basis for a new paradigm for money, just like Bitcoin did in 2008.

References

[1] S. Nakamoto. “Bitcoin: A peer-to-peer electronic cash system”. In: *Consulted* (2008).

[2] G. O. Karame, E. Androulaki, and S. Capkun. “Double-spending Fast Payments in Bitcoin”. In: *Proceedings of the 2012 ACM Conference on Computer and Communications Security*. CCS ’12. New York, NY, USA: ACM, 2012, pp. 906–917. ISBN: 978-1-4503-1651-4. DOI: 10.1145/2382196.2382292.

[3] W. K. Wootters and W. H. Zurek. “A single quantum cannot be cloned”. In: *Nature* 299.5886 (Oct. 28, 1982), pp. 802–803. DOI: 10.1038/299802a0.

[4] S. Wiesner. “Conjugate Coding”. In: *SIGACT News* 15.1 (Jan. 1983), pp. 78–88. ISSN: 0163-5700. DOI: 10.1145/1008908.1008920.

[5] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner. “Quantum Cryptography, or Unforgeable Subway Tokens”. In: *Advances in Cryptology*. Ed. by D. Chaum, R. L. Rivest, and A. T. Sherman. Boston, MA: Springer US, 1983, pp. 267–275. ISBN: 978-1-4757-0604-8 978-1-4757-0602-4. DOI: 10.1007/978-1-4757-0602-4_26.

[6] A. Lutomirski, S. Aaronson, E. Farhi, D. Gosset, A. Hassidim, J. Kelner, and P. Shor. "Breaking and making quantum money: toward a new quantum cryptographic protocol". In: (Dec. 20, 2009). arXiv: 0912.3825.

[7] E. Farhi, D. Gosset, A. Hassidim, A. Lutomirski, and P. Shor. "Quantum money from knots". In: (Apr. 28, 2010). arXiv: 1004.5127.

[8] S. Aaronson and P. Christiano. "Quantum Money from Hidden Subspaces". In: (Mar. 21, 2012). arXiv: 1203.4740.

[9] J. Jogenfors. "Quantum Bitcoin: An Anonymous and Distributed Currency Secured by the No-Cloning Theorem of Quantum Mechanics". In: *arXiv:1604.01383 [quant-ph]* (Apr. 5, 2016).

[10] J. Garzik. *Making Decentralized Economic Policy*. BIP 100 - Theory and Discussion, v0.8.1. June 15, 2015.

[11] F. Reid and M. Harrigan. "An Analysis of Anonymity in the Bitcoin System". en. In: *Security and Privacy in Social Networks*. Ed. by Y. Altshuler, Y. Elovici, A. B. Cremers, N. Aharony, and A. Pentland. New York, NY: Springer New York, 2013, pp. 197–223. ISBN: 978-1-4614-4138-0 978-1-4614-4139-7.

[12] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage. "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names". In: *Proceedings of the 2013 Conference on Internet Measurement Conference*. IMC '13. New York, NY, USA: ACM, 2013, pp. 127–140. ISBN: 978-1-4503-1953-9. DOI: 10.1145/2504730.2504747.

[13] M. Moser, R. Bohme, and D. Breuker. "An inquiry into money laundering tools in the Bitcoin ecosystem". In: IEEE, Sept. 2013, pp. 1–14. ISBN: 978-1-4799-1158-5. DOI: 10.1109/eCRS.2013.6805780.

[14] "BitIodine: Extracting Intelligence from the Bitcoin Network". en. PhD thesis. Aug. 2013.

[15] D. Kondor, M. Pósfai, I. Csabai, and G. Vattay. "Do the Rich Get Richer? An Empirical Analysis of the Bitcoin Transaction Network". en. In: *PLoS ONE* 9.2 (Feb. 2014). Ed. by M. Perc, e86197. ISSN: 1932-6203. DOI: 10.1371/journal.pone.0086197.

[16] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun. "Evaluating User Privacy in Bitcoin". en. In: *Financial Cryptography and Data Security*. Ed. by A.-R. Sadeghi. Lecture Notes in Computer Science 7859. Springer Berlin Heidelberg, Apr. 2013, pp. 34–51. ISBN: 978-3-642-39883-4 978-3-642-39884-1. DOI: 10.1007/978-3-642-39884-1_4.