ledgerjournal.org

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2018.127

Quantum Attacks on Bitcoin, and How to Protect Against Them: Open Review

Divesh Aggarwal,[*][†] Gavin Brennen,[‡] Troy Lee,[§] Miklos Santha,[**] Marco Tomamichel[††]

Reviewers: Reviewer A, Reviewer B

Abstract. The final version of the paper "Quantum Attacks on Bitcoin, and How to Protect Against Them" can be found in Ledger Vol. 3 (2018) 68-90, DOI 10.5915/ LEDGER.2018.127. There were two reviewers involved in the review process, none of whom have requested to waive their anonymity at present, and are thus listed as A and B. After initial review by Reviewers A and B (1), it was determined that the submission should be accepted with minor revisions. The authors made subsequent revisions and the changes were accepted by the reviewers, thus completing the peer-review process.

1. Review

Reviewer A:

Does this paper represent a novel contribution to cryptocurrency or blockchain scholarship?:

Yes

[*] 3KNzjxAUuA199FbmWaA7ide4PvhVcKobCd

[†] D. Aggarwal (dcsdiva@nus.edu.sg) is an Assistant Professor in the Department of Computer Science and Principal Investigator at the Centre for Quantum Technologies at NUS, Singapore.

[‡] G. K. Brennen (gavin.brennen@mq.edu.au) is an Associate Professor at Macquarie University.

[§] T. Lee (troyjlee@gmail.com) is an Associate Professor at the University of Technology Sydney.

[**] M. Santha (miklos.santha@gmail.com) is Senior Researcher at the CNRS, IRIF, Université Paris Diderot and Principal Investigator at the Centre for Quantum Technologies at NUS, Singapore.

[††] M. Tomamichel (marco.tomamichel@uts.edu.au) is Senior Lecturer in Quantum Information at the University of Technology Sydney.

If you answered "yes" to the previous question, in one sentence, describe in your own words the novel contribution made by this paper:

This paper uses prior work on quantum computing and assumes a "universal quantum computer" combined with two known quantum algorithms, Grover's and Shor's, to estimate the difficulty of breaking the PoW and signature scheme used in Bitcoin. It also considers some alternative schemes that may be more quantum computing resistant.

Is the research framed within its scholarly context and does the paper cite appropriate prior works?:

Yes.

Please assess the article's level of academic rigor:

High.

Please assess the article's quality of presentation:

High.

How does the quality of this paper compare to other papers in this field?:

High.

Please provide your free-form review for the author in this section:

The authors of this paper discuss various quantum computing attack vectors on Bitcoin's PoW scheme as well as its ECDSA used for signing transactions. The paper is very well written, and presented, and I highly recommend it for publication.

That being said, I have a few relatively minor suggestions to further improve the paper:

- Despite leading the reader clearly through all of the details in the first four pages, on page five the use of unexplained jargon ramps up rather significantly. The following are all very mysterious to a reader without a background in quantum computing.
--- T gates vs. Toffoli gates
--- "surface code"
--- "magic states"

- Although the authors can't be expected to include a "quantum computing 101" guide as part of their paper, I believe that adding one extra sentence for each of the above bullets that sheds slightly more light on what these terms mean (and explicitly point readers to references where they can find more information on the topics) would significantly help in the readability of the paper (which is already very good).

- On pg 8 "are posed" should be "are poised"

Reviewer B:

Does this paper represent a novel contribution to cryptocurrency or blockchain scholarship?:

Yes

If you answered "yes" to the previous question, in one sentence, describe in your own words the novel contribution made by this paper:

The paper provides an analysis of possible quantum attacks and mitigations for such attacks going forward.

Is the research framed within its scholarly context and does the paper cite appropriate prior works?:

Yes

Please assess the article's level of academic rigor:

Excellent (terms are well defined, proofs/derivations are included for theoretical work, statistical tests are included for empirical studies, etc.)

Please assess the article's quality of presentation:

Excellent (the motivation for the work is clear, the prose is fluid and correct grammar is used, the main ideas are communicated concisely, and highly-technical details are relegated to appendixes).

How does the quality of this paper compare to other papers in this field?:

Top 10%

Please provide your free-form review for the author in this section:

This was an extremely interesting and valuable paper that clarifies many of the questions about quantum computing as applied to Bitcoin, as well as providing well-grounded speculation as to the future of such attacks on Bitcoin. The paper analyzes several of these attacks, as well as providing analysis on possible mitigations for such attacks.

The paper is well-organized and explains concepts well. I did not see any errors in reasoning or foundational issues. I strongly recommend it for publication. However, I did have several suggestions for improvement to improve its readability, and several other suggestions for improving understanding for those with a computer science background who may not have a background specifically in quantum computing.

In regards to the sentence including "However, such a development is unlikely in the next decade..." Section 3.1 (Page 4) – On first reading, this seems like a rather broad and unsupported statement, until I realized that it was discussed further in Appendix I. I would recommend adding a pointer (e.g., "(See Appendix I)" to the end of this sentence.

In Appendix I, in the table labeled "number of qubits per year" (page 21), there are two references to "IBM" with no further information – I would like to see a more specific reference to where these values originated.

I assume this is paper is intended to be read by those who may not have a background in quantum computing. As such, it may be useful to provide several references at the beginning of Section 3.1 in order to help comprehension on the topic. For example, on page 5, the superposition equation (right after "i.e., perform the mapping…"), those not familiar with quantum computing may not know the |x> symbol indicates superposition. Adding a reference to an overview of the field (e.g., Yanosky's "An Introduction to Quantum Computing" - https://arxiv.org/abs/0708.0261v1) somewhere at the beginning of this section may be useful.

I found several minor typographical issues, as well, enumerated below:

Section 3.1 (page 6 - footnote) - The correct capitalization is "Antminer", not "AntMiner" (according to Bitmain's product description page - https://shop.bitmain.com/antminer_s9_asic_bitcoin_miner.htm)

Section 3.1 (page 9) - "This reduces the effecting mining power" - I believe this should be "effective mining power".

Section 3.3 (page 11) "While each each such query..." - This should be "While each such query..." ("each" was doubled)

Section 4.2 (page 13) "Looking at Table 2, with respect the sum of..." This should be "with respect to the sum of..."

Notes and References (page 16) – In reference 33, there is a reference to "Cryptographers? Track at the RSA Conference". This should be "Cryptographers' Track at the RSA Conference".

Is there a reason that the Appendices start at "Appendix G" instead of "Appendix A"?

ISSN 2379-5980 (online)
DOI 10.5915/LEDGER.2018.127