LEDGER
ledgerjournal.org

ISSN 2379-5980 (online)
associated article DOI 10.5915/LEDGER.2019.143

Energy-Efficient Mining on a Quantum-Enabled Blockchain Using Light: Open Review

Authors: Adam J. Bennet, [*†] Shakib Daryanoosh[‡]

Reviewers: Reviewer A, Reviewer B, Reviewer C

Abstract. The final version of the paper "Energy-Efficient Mining on a Quantum-Enabled Blockchain Using Light" can be found in Ledger Vol. 4 (2019) 82-107, DOI 10.5915/LEDGER.2019.143. There were three reviewers involved in the review process, none of whom have requested to waive their anonymity at present, and are thus listed as A, B, and C. After initial review by Reviewers A, B, and C (1A), the Author responded (1B) and submitted a revised manuscript. Reviewers A, B, and C then reviewed the submission a second time (2A), and the authors responded once again (2B), after which it was deemed acceptable for publication with minor revisions, thus ending the peer review process. *Nota bene*: In section 1B, the Authors mention "blue," "green," and "red" text, which refer to color-coded sections of their resubmitted manuscript. As Ledger does not publish sequential drafts, these references are of limited usefulness, but have been retained for the sake of transparency.

1. Review (First Round)

Reviewer A

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

Not sure.

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

[*] 1MsJx7YNiMCQzYPSidQbK3EgbW2zzMqk1Q

[†] A. J. Bennet (adam.bennet@alumni.griffithuni.edu.au) is an independent researcher in Melbourne, Australia.

[‡] S. Daryanoosh (shakib.daryanoosh@alumni.griffithuni.edu.au) is a post-doctoral researcher at Macquarie University, Department of Physics and Astronomy, and the Australian Research Council Centre of Excellence for Engineered Quantum Systems, Sydney, Australia.

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:

Good (not excellent but a long way from poor)

Please assess the article's quality of presentation:

Good (not excellent but a long way from poor)

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

Top 20%

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

The authors propose a way to use a quantum effect, namely bipartite quantum entanglement between optical modes, shared between so-to-speak miners and a new kind of actor which they deem quantum nodes, to generate randomness that would have the same role as PoW protocols, which are the cornerstone of trust in the blockchain.

The article is well written overall, despite some inconsistencies in the headers and some typos in the text. Whereas the topic is sufficiently interesting and definitely timely, I cannot support publication of this work in its current form. In particular, I recommend that the authors address three critical issues before publication:

- The outlined protocols rely heavily on a trusted source of time stamps, for instance in order to close the no-signaling loophole, but not only. How can this protocol deal with adversarial time-stamping? It is a well known fact that trust in the blockchain does not rely on time-stamping.

- Both in the local and the non-local approaches, I was not able to understand how the miners verifiers are selected to connect to the prover and eventually mint a block. If they are selected accordingly to some distribution, they should make sure that the protocol is robust against adversarial noise. Another way of putting it: how does this protocol deal with forks? More generally, how does this protocol deal with known exploits?

- Finally, I do not understand how PoE can substitute PoW as a source of trust. Usually, a block is minted by someone with high stakes in the good associated to the ledger. This is not true for PoE, as far as I can see. This has serious consequences for its interest as a source of consensus.

The rest of my remarks can be found as comments in the attached pdf. Regarding the bibliography, I believe that the discussion of previous work relevant to this article is sound

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2019.143

and exhaustive.

Some minor comments:

- The use of capital letters in the headers is not consistent.
- The appendices are numbered in a somewhat strange way.
- There are a few typos in the text.

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 describes a novel variant of proof for securing the blockchain, proof-of-entanglement.

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:

Good (not excellent but a long way from poor)

Please assess the article's quality of presentation:

Good (not excellent but a long way from poor)

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

Top 20%

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

This was paper explores a novel way of securing proof-of-work on a blockchain, namely, via proof-of-entanglement. This paper was generally well-written and I believe provides valuable insight into possible future blockchain development and security. This paper describes a possible system for using nonlocal resource generation for securing proof-of-work on a blockchain system which is similar to, but distinct in several ways from, a traditional blockchain data structure as used by, e.g., Bitcoin.

While I recommend this paper for publication, there are several issues which I feel must be

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2019.143

addressed before publishing. I will go through these roughly in order from the beginning of the document to the end (although I will discuss minor typographical errors in one section at the end).

In Section 1 (page 2), the list of emerging quantum technologies such as integrated photonic devices, micropillar quantum dots, etc. seems superfluous. Simply ending the Introduction with "...quantum-compatible with the suite of newly emerging quantum technologies. [23,24,25,26,27]" would be a stronger and more relevant while still including information about said technologies in the references. That being said, this is mostly a stylistic observation.

In Section 2 (page 2), the first paragraph states that the technology for entanglement generation is "the primary candidate for unequivocally addressing the issue of post-quantum security" with a reference to Chen et al's "Report on Post-Quantum Security". However, this strong statement is not supported by the reference. The referenced paper specifically mentions use of new algorithms and increased key lengths for encryption using classical mechanisms. It does not mention entanglement, and even states that "[w]hen standards for quantum-resistant public key cryptography become available, NIST will reassess the imminence of the threat of quantum computers to existing standards, and may decide to deprecate or withdraw the affected standards thereafter as a result." This is a far cry from an "unequivocal" endorsement of entanglement as a solution to the challenges of quantum computing applied to cryptography.

Further in Section 2 (page 3), in the third paragraph, there is talk of the prover being "synonymous with the role of Alice..." There should be a reference here (either to Appendix I, if it is kept, or somewhere else where the roles are defined and specified).

The first paragraph in Section 2.1 (page 3). raises a few questions which I feel should be addressed. First, how does the strict time stamping work? This is a known issue in distributed systems, and one of the reasons that there is a two-hour window in the Bitcoin protocol in terms of valid timestamps. This also becomes relevant in Step 8 for the protocol for local mining (page 5). Second, in regards to "the properties of nonlocal systems force the provers into trustworthy behaviors", this seems unsupported based on the information already provided. I believe a reference would be appropriate here or at least a phrase such as "as we shall see" and explain it later.

The penultimate paragraph of Section 2.1 (on page 4), states that the communication channel "will be secured using ... RLWE-SRP". Is this because using RLWE-SRP is a necessary condition, or are there other communication protocols which are post-quantum secure? If so, are there reasons why this particular scheme was chosen over others? It notes post-quantum security and perfect forward secrecy, are these only available via RLWE-SRP?

In Section 2.1. (page 5), step 9, how are nodes which consistently fail to certify the generation of nonlocal resources removed/blacklisted from the network? Are there protections against Sybil attacks or other identify forging attacks to get around this?

In Section 3 (pp 8-9), the second paragraph, perhaps the writing is a bit unclear, but I fail to

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2019.143

see how proof-of-entanglement prevents a mining arms race, at least in terms of block rewards. Since the incentive of miners is to generate tokens (of whatever kind) for themselves, it seems that they would be able to increase their chances of winning by creating more q-nodes. In an ad absurdum example, if there is only 1 miner, they have a 100% win probability; if there are 1,000 miners, then each individual miner has a 0.1% win probability. What is to prevent a mining conglomerate to then an additional 1,000 q-nodes on-line, giving them now a 50.1% winning probability? I did not notice any identification scheme to prevent this, so it seems like simple game theory means that miners will continue to bring more q-nodes online to increase their winning probability relative to others, thus bringing about the same arms race as we see in traditional proof-of-work mining schemes.

I believe this paper would be even stronger if there was a section dedicated particularly to possible weaknesses or drawbacks to using proof-of-entanglement versus traditional proof-of-work (and possibly including variants such as proof-of-stake, proof-of-space, etc.).

The Appendices seem to be mostly overview of basic concepts in various fields. Appendix H may be useful despite it being a primer on nonlocal correlations, Bell's inequality, etc., as these will most likely not be familiar to many readers of Ledger. As quantum computing becomes more important in dealing with the security challenges of blockchain technology, this may change in the future, but we are certainly not at that point now. This could be left as-is or replaced with a reference to a good primer on the topic.

However, I certainly question the inclusion of Appendices I and J. In regards to Appendix I, any reader of Ledger is going to be familiar with the basics of blockchain technology and I do not see a reason for a basic primer on it.

In regards to Appendix J, the steps for setting up a Sagnac interferometer seem to be implementation details rather than strictly relevant to the paper. Additionally, these implementation details (in an apparently more comprehensive form) are available in Ref. 59, "An Ultrafast Source of Polarisation Entangled Photon Pairs based on a Sagnac Interferometer". I believe removing Appendix J and simply adding a reference to Smith's thesis when first discussing the Sagnac interferometer would be sufficient (perhaps with wording such as "Sagnac interferometers were constructed and calibrated using the instructions found in Ref. 59").

Finally, there were several typographical errors I would like to bring to the authors' attention, although some or all of these may be obviated by any changes made by updating the paper as described above.

In Section 1, "...designed for a blockchain, namely;" the semicolon should be removed or replaced with a comma.

In Section 2, third paragraph, "psuedo" is incorrect and should be spelled "pseudo".

In Section 2.2., under the steps for the protocol for remote mining with EPR steering inequalities, Step 5 has "...q-node verifier reports the the measurement output...". The redundant "the" should be eliminated.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2019.143

In Notes and References, Ref. 25 contains "Bell?s Theorem" which should be "Bell's Theorem".

In Appendix H, Section 8.1, first paragraph, "resepctively" should be spelled "respectively".

Reviewer C

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:

A consensus mechanism for quantum computer operated - or at least consolidated - blockchains

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:

Unsatisfactory (better than poor but a long way from excellent)

Please assess the article's quality of presentation:

Good (not excellent but a long way from poor)

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

Top 50%

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

The paper introduces into an interesting topic of new research - quantum computed blockchains and consensus. But it seems more written for - or even better: extracted from - quantum computer experts interested in blockchains. Hardly any satisfactory background on quantum computing is given, but a lot of information about blockchains, consensus in Bitcoin, ...

According to my expectation, the ledger journal's target group is just the opposite: A lot of knowledge about blockchains, but hardly any knowledge in quantum computing.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2019.143

Therefore the style and the content of the article should be vice-versa: Skip the deep introductions and annexes explaining blockchains, but explain more on quantum computing and the role in blockchains.

More comments in the paper.

1B Author's Responses

Reviewer A

- Referee A (and Referee B) asked how the protocol deals with a) adversarial time-stamping and b) mechanisms for closing the no-signaling loophole, noting that trust in the blockchain does not rely on timestamping. We have removed the requirement for strict timestamping, instead requiring only that clients accept server announcements after performing their measurement. We deliver a more detailed analysis of adversarial strategies on the part of a dishonest quantum server (page 12-13, blue text), which allows for falsified timestamps, false announcements, and falsified qubit encodings, finding that the PoE protocol remains secure as long as the adversary cannot predict a secret QRNG result or send signals backwards in time. No-signalling is enforced by assuming no information leaks form the clients device (a standard cryptographic assumption), which is further supported through the introduction of a quantum secure authentication protocol which affords tamper detection of devices.

- Referee A noted it remained unclear on how the miner—verifiers (now simply termed `clients') are selected to connect to the prover (now termed `quantum server') and eventually mint a block, asking also how the protocol deal with forks and known exploits. We have elaborated on the selection criteria for mining pools, with flexibility in selecting clients, allowing for random selection, optimized selections, or restricted elections based upon accumulated reputations, detection efficiencies, transmission losses, coupling efficiencies, measurement strategies, and measurement speed. We have included a formal consensus mechanism based upon Byzantine Fault Tolerance to circumvent chain forks whilst retaining the ability to mine through public election of voting servers (page 6-7, red text). This allows us to address other vulnerabilities like double spend, pre-mine, and Sybil attacks (page 13-14, green text).

- Referee A enquired how PoE can substitute PoW as a source of trust, stating that "Usually, a block is minted by someone with high stakes in the good associated to the ledger. This is not true for PoE, as far as I can see." To address this, we have adjusted the interactive PoE mining protocol to act as an access gate into a consensus round. This ensures that servers must interact honestly with clients if they wish to generate and commit entanglement towards securing the blockchain. Servers are thus publicly accountable and incentivized to act honestly, with provision to earn reputational rewards or deficits depending on their actions (page 6, green text).

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2019.143

Reviewer B

- We have implemented Referee B's suggestion to simplify the end of the introduction, using "... mapping traditional scientific computing technologies onto newly emerging quantum technologies. [57, 58, 59, 60, 61, 62]" (page 3, blue text).

- We have removed the strong statement and incorrect reference claiming that "entanglement generation is the primary candidate for unequivocally addressing the issue of post-quantum security"

- We have removed the statement declaring the prover (now quantum server) as being "synonymous with the role of Alice…" and implemented the Referee's suggestion to more clearly define and specify roles (page 4, blue text).

- Referee B also raised the issue of strict time stamping, As mentioned above, we have removed the requirement for strict time stamping, instead requiring only that clients accept server announcements after performing their measurement. We deliver a more detailed analysis of adversarial strategies on the part of a dishonest quantum server (page 12-13 blue text), which considers falsified timestamps, false announcements, and falsified qubit encodings, finding that the PoE protocol remains secure as long as the adversary cannot predict a secret QRNG result or send signals backwards in time. As the Referee points out, the statement "the properties of nonlocal systems force the provers into trustworthy behaviors" is unsupported, and has been removed. Incentives for trustworthy behaviors are now reward and reputation based, with honest interactions rewarded through admission to consensus round (page 6, red text). An in-depth discussion on incentives for trustworthiness are given on page 14-15 (blue text).

- Referee B asked "whether RLWE-SRP is a necessary condition for the protocol, or if there other communication protocols which are postquantum secure?". We have since removed this requirement, however included references to this and other post—quantum secure (or "quantum—resistant") schemes for encryption to highlight alternative approaches to blockchain design (page 3, green text).

- Referee B asked "how nodes which consistently fail to certify the generation of nonlocal resources are removed/blacklisted from the network? Are there protections against Sybil attacks or other identify forging attacks to get around this?". To address this we have utilized the features of a consortium blockchain which makes the identities of nodes (now quantum servers) known to the network and accountable to honesty through incentives and reputation (page 13-14, green text). Sybil attacks are addressed on the part of quantum servers, who may collude with pools of clients. The likelihood of a Sybil attack is diminished by identity management and infrastructure cost through inclusion of the quantum secure authentication protocol (page 5-6, blue text).

- Referee B noted that if the incentive of miners is to generate tokens (of whatever kind) for themselves, it seems that they would be able to increase their chances of winning by creating more q-nodes (now quantum servers), potentially resulting in an arms race. We have addressed this by moving away from an emergent consensus mechanism, opting instead for a

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2019.143

modified BFT consensus mechanism based upon a consortium blockchain architecture and election into voting through interactive mining.

- Referee B recommended the paper may be made stronger if there was a section dedicated particularly to possible weaknesses or drawbacks to using proof-of-entanglement versus traditional proof-of-work (and possibly including variants such as proof-of-stake, proof-of-space, etc.). While we have eluded to but not directly compared PoE with other mechanisms, we have highlighted drawbacks to PoE in the form of infrastructure requirements, and included preliminary analysis of energy efficiency and scalability based upon results from proof-in-principle experiments (page 11-12, blue text). We have included a paragraph in the conclusion to address areas for improvement and future exploration (page 15, blue text).

- Appendices have been removed and renamed, now containing material relevant to quantum secure authentication and experimental loopholes. All other necessary material has been moved to references.

- We have observed and amended Referee B's indications of typos and misspellings.

2A Review (Second Round)

Reviewer A

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:

It has the potential to help solve the energy consumption problem.

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:

Good (not excellent but a long way from poor)

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).

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2019.143

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:

I believe the second version of this paper is a substantial improvement over the first one. Most of my remarks have been addressed.

However I still do not what is the advantage of PoE over an equivalent protocol in which server and clients would follow the rules in section 5.2 using only classical correlations. In other words, the creation of bi-partite entanglement seems to me like a fungible resource very similar to a classical or quantum randomness reservoir.

I would recommend publication after authors have addressed this point.

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 use of entanglement as proof for a blockchain

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%

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2019.143

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

This paper explores a novel way of securing proof-of-work on a blockchain, namely, via proof-of-entanglement. This paper was generally well-written and I believe provides valuable insight into possible future blockchain development and security. This paper describes a possible system for using nonlocal resource generation for securing proof-of-work on a blockchain system which is similar to, but distinct in several ways from, a traditional blockchain data structure as used by, e.g., Bitcoin. Additionally, it describes a "proof-in-principle" implementation using a Sagnac interferometer and fiber optic communications. I believe that this paper represents a novel and useful addition to the field of blockchain technology and it should be accepted.

This paper was revised dramatically since the first revision, making it a much stronger paper. All of the points that I brought up in my initial review were addressed thoroughly (specifically: the reduction and improvement of the appendices, a better explanation of the setup, the addition of a section on possible attack vectors and weaknesses, the description of protections against Sybil attacks and addition of more detail on resource trust, details on timestamping, and several better descriptions of the scope of security provided). The section on potential attack vectors was especially well-done and appreciated.

There are several questions which it raises which I feel would are valuable prompts for further research, including different consensus algorithms and the ability to fork the chain. The authors indicated that they are already working on such experiments and I look forward to reading about them in future papers.

I have a few very minor comments and errata, but I do not think that any of these are roadblocks to acceptance.

1. With the caveat that I am not a physicist, let alone a quantum physicist, I think that in Section 3, the phrase "... and today, entanglement is placed as the 'missing link' for the unification of quantum theory and gravity' is rather strong. According to this, it sounds as though it is settled science. My understanding is that the hypothesis in Raamsdonk's "Building up spacetime with quantum entanglement" has led to many promising avenues of theory and research, it is not yet universally considered the "Theory of Everything". Perhaps replace "placed as" with "proposed as"?

2. Should the phrase "physically unclonable key" be "physical unclonable key"? This seems to be the standard phrase, used in e.g., Goorden et al.'s "Quantum-secure authentication of a physical unclonable key" and Uppu et al.'s "Asymmetric Cryptography with Physical Unclonable Keys".

A minor typo that I noticed as well:

Reference 106 misspells "Trezor" as "Tresor". Additionally, the link is incorrect - it should be https://wiki.trezor.io/Cryptocurrency_Standards (there are two unnecessary $ signs in the original)

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2019.143

Reviewer C

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:

Using quantum mechanics of photons creates a new concept of uncopyable identities - elementary for use of blockchains.

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:

Good (not excellent but a long way from poor)

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:

The authors have accepted and considered nearly all comments from the reviewers. This improved the quality of the content and its understanding significantly.

The paper itself is still very (too) long, but there is also no significant section which can be shortened without reducing the general understanding

2B. Author's Responses

Reviewer A

1) Reviewer A noted that they were not sure on "what the advantage of PoE is over an equivalent protocol in which server and clients would follow the rules in section 5.2 using only classical correlations." To address this comment, we have elaborated on paragraph 4 in

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2019.143

the “Discussion and analysis of vulnerabilities” section, highlighting that classical correlations formally belong to a weaker class of correlation, and subsequently will not provide the degree of correlation required for successful mining and security in a consortium of untrusted servers.

2) Reviewer A also made the interesting comment that “in other words, the creation of bi-partite entanglement seems to me like a fungible resource very similar to a classical or quantum randomness reservoir.” Paragraph 4 has been expanded slightly to incorporate this insight by posing an open question as to whether trust--tests (in particular, device--independent certification) may connect with or inform the formalism describing entanglement as a fungible resource. Relevant references have been included.

Reviewer B

1) Reviewer B noted that the statement “... entanglement is placed as the 'missing link' for the unification of quantum theory and gravity” is rather strong. We have amended this statement as per the reviewer’s suggestion to “... entanglement is proposed as being the `missing link' for the unification of quantum theory and gravity”.

2) As per Reviewer B’s suggestion, throughout the work, "physically unclonable key" has been changed to "physical unclonable key". 3) The typos in reference 106 have been updated as per Reviewer B’s recommendation (Tresor -> Trezor, and removal of ‘$’ symbols).

Reviewer C

1) Reviewer C notes that the paper is quite long, yet notes that it is challenging to shorten the work without sacrificing general understanding. The authors tend to agree on this point.

Miscellaneous

1) In several places, phrasing in the main text referring to experimental work has been adjusted slightly to make it clear that our energy cost analysis and feasibility arguments rely upon previous experimental demonstrations performed by the author (Adam Bennet). The author has obtained permission from the academic group (of Prof. Geoff J. Pryde) where the experiments were conducted in order to authorize the use of these previous experimental outcomes and subsequent datasets in the context of this publication. The authors will be happy to share these confirmations at the necessary time, in accordance with Ledger’s publication policies. Below are some examples of the phrasing adjustments from the abstract and main text:

Abstract (before): “To demonstrate the energy efficiency of the mining protocol, we deliver the results of two proof--in--principle experiments (one performed over 1km of optical fibre)”

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2019.143

Abstract (after): “To demonstrate the energy efficiency of the mining protocol, we elaborate upon the results of two previous experiments (one performed over 1km of optical fibre) as applied to this work.”

Main text (before): “In this work, we elaborate upon recent results from two proof--in--principle experiments which demonstrate how the PoE mining protocol can be implemented with a Sagnac interferometer.”

Main text (after): “In this work, we elaborate upon results from two previous proof--in--principle experiments, and explore how the PoE mining protocol may be readily implemented with a Sagnac interferometer, functioning, in this case, as a quantum server.”

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2019.143