LEDGER
ledgerjournal.org

ISSN 2379-5980 (online)
associated article DOI 10.5915/LEDGER.2021.199

Enhanced Electronic Voting with a Dual-Blockchain Architecture: Open Review

Kees Leune,* Jai Punjwani†

Reviewers: Reviewer A, Reviewer B, Reviewer C

Abstract. The final version of the paper "Enhanced Electronic Voting with a Dual-Blockchain Architecture" can be found in Ledger Vol. 6 (2021) 42-57, DOI 10.5915/LEDGER.2021.199. There were three reviewers involved in the review process, neither of whom has requested to waive their anonymity at present, and are thus listed as Reviewers A, B, and C. After initial review by Reviewers A and B, the submission was returned to the authors with feedback for revision (1A). The authors responded (1B) and resubmitted their work. A third reviewer, Reviewer C, was added to the review process. After another round of revisions (2A), the authors again responded with revisions (2B). Reviewers B and C then agreed that their concerns had been adequately handled, thus ending the peer review process. Responses have been formatted for clarity.

1A. Review

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:

The paper describes a solution where we can apply blockchain to voting machines to increase the ability to audit and enhance transparency.

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

* K. Leune (leune@adelphi.edu) is a faculty member in the Department of Mathematics and Computer Science at Adelphi University.
† J. Punjwani (jaipunjwani@mail.adelphi.edu) is an alumnus, who graduated from Adelphi University with a B.S. in Computer Science in 2018.

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.

I was impressed with the concept of applying blockchain to an existing voting infrastructure instead of proposing a new one. The largest problem in election infrastructure is the voter registration system giving providence to voters in the first place. If this proof-of-concept were to be implemented in a real environment I would add one step further and add a third piece of the infrastructure that includes the entire voter registration system. This suggestion aside, adding blockchain into the voting machines would assist with creating a publicly available audit trail to increase confidence in the public.

Reviewer B

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

No

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

Important references are missing

Please assess the article's level of academic rigor.

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

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2021.199

Please assess the article's quality of presentation.

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

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

Bottom 50%

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

The use of blockchains in electronic voting is not novel, and the paper fails to establish precisely the requirements that the block chain will meet.

It states that it will use "blockchain technology in order to ensure voter secrecy, vote correctness, and equal voting rights." But, these informal concepts are not rigorously defined/specified. What do they mean by secrecy? What is their definition of correctness - they refer to "tamper-resistant" later in the paper? What do they mean by "equal voting rights"?

The papers high level objective is stated as - "We ask the following research question: In what way can a blockchain-based electronic voting process provide election integrity while maintaining voter secrecy?" However, there is no specific answer to this question.

The use of 2 blockchains (one for the electronic urn and one for the electoral list) is not particularly novel and the separation of the 2 by a ballot claim ticket is a fairly standard approach.

Figure 1 is missing in the paper - so it i hard to validate the proposed architecture against the voting process being proposed.

The "introduction of a new consensus algorithm that is specific to electronic voting." is a minor contribution as the paper fails to explicitly identify the advantages of the proposed algorithm over other algorithms/approches.

The testing scenarios in table 1 hardcoded in the main python program rather than in configurable separate test files. It is not clear that the implemented tests cover all different scenario executions completely (in terms of requirements checking, and in terms of test code coverage).

(The code in this repository is poorly documented and its structure is not obviously coherent with the architecture design.)

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2021.199

The paper claims that " The readability of Python code also served as documentation for our voting process." ... this is poorly justified and the code does not provide adequate documentation.

The conclusions state: "While the use of blockchain technology is not a solution to all election-related issues, it can address some problems. Unfortunately, it may also introduce new ones." The paper fails to provide much insight into the +s and -s with respect to using different blockchain architectures/protocols for e-voting.

The authors are encouraged to provide a much more detailed state-of-the-art in the use of blockchain technologies for e-voting.

They are missing many of the key references to published academic work, and fail to reference many alternative approaches that exist (commercial and non-commercial)

The citations in notes 4,7,9,11 and 12 are to on-line material; but they are cited inconsistently and incompletely.

1B. Author Response

We thank the reviewers for their detailed comments, and have endeavored to address their concerns. A summary of our responses is included below.

Reviewer A

I was impressed with the concept of applying blockchain to an existing voting infrastructure instead of proposing a new one. The largest problem in election infrastructure is the voter registration system giving providence to voters in the first place. If this proof-of-concept were to be implemented in a real environment I would add one step further and add a third piece of the infrastructure that includes the entire voter registration system. This suggestion aside, adding blockchain into the voting machines would assist with creating a publicly available audit trail to increase confidence in the public.

- Unfortunately, field-testing in a life environment is out-of-scope for this phase of the research. Given the current COVID-19 pandemic, we are unsure at what point in time we would be able to perform such a test.

Reviewer B

Important references are missing.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2021.199

- We have included additional references as the result of an additional literature review.

The use of blockchains in electronic voting is not novel, and the paper fails to establish precisely the requirements that the block chain will meet.

- We have taken additional steps to clearly identify the assumptions on which our approach is based, and what requirements we aim to solve.

While the use of blockchains in electronic voting is indeed not new, we have 1) included citations to related work and 2) attempted to clarify the areas in which our work is different from that work.

- It states that it will use “blockchain technology in order to ensure voter secrecy, vote correctness, and equal voting rights.” But, these informal concepts are not rigorously defined/specified.

- In the original paper, we included a reference to other locations in which these concepts are rigorously defined. To ensure that our paper is readable as a self-contained unit, we have incorporated more definitions into the text of our work.

The paper’s high level objective is stated as “We ask the following research question: In what way can a blockchain-based electronic voting process provide election integrity while maintaining voter secrecy?" However, there is no specific answer to this question.

- We extended the answer to this question in the Conclusions section.

The use of 2 blockchains (one for the electronic urn and one for the electoral list) is not particularly novel and the separation of the 2 by a ballot claim ticket is a fairly standard approach.

- We acknowledge this and extended our work by citing a number of appropriate sources.

Figure 1 is missing in the paper - so it is hard to validate the proposed architecture against the voting process being proposed.

- The version of the paper uploaded to Ledger journal did in fact contain Figure 1. We apologize for any possible incompatibility issues and will strive to produce the Final PDF in a more reliable format.

The “introduction of a new consensus algorithm that is specific to electronic voting.” is a minor contribution as the paper fails to explicitly identify the advantages of the proposed algorithm over other algorithms/approaches.

- We stand by our contribution as a valuable one. However, we have, hopefully, improved our argument.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2021.199

The testing scenarios in table 1 hardcoded in the main python program rather than in configurable separate test files. It is not clear that the implemented tests cover all different scenario executions completely (in terms of requirements checking, and in terms of test code coverage).

- The referenced code is meant as a proof-of-concept, rather than as a functional system. It is not intended to be a scalable prototype. However, in response to the reviewer's comments, we have improved the codebase, and will continue to do so as this work evolves.

The paper claims that “The readability of Python code also served as documentation for our voting process.” . . . this is poorly justified and the code does not provide adequate documentation.

- Additional comments have been added to the code.

The conclusions state: “While the use of blockchain technology is not a solution to all election-related issues, it can address some problems. Unfortunately, it may also introduce new ones.” The paper fails to provide much insight into the +s and -s with respect to using different blockchain architectures/protocols for e-voting.

- The author guidelines limit the size of our contribution, and encourage authors to focus their contributions on a single topic of research. While conducting a broad evaluation of blockchain architectures and protocols for use in e-voting is certainly a worthwhile endeavor, it is not contained in the scope of this paper.

The authors are encouraged to provide a much more detailed state-of-the-art in the use of blockchain technologies for e-voting.

- See above.

They are missing many of the key references to published academic work, and fail to reference many alternative approaches that exist (commercial and non-commercial)

- We have endeavored to include such references. Without specific details, we are unable to respond to the reviewer's comments in order to explain why certain references were omitted.

The citations in notes 4,7,9,11 and 12 are to on-line material; but they are cited inconsistently and incompletely.

- Citations are automatically formatted by LaTeX using the Ledger bibliography style. If desired, we will manually override these citations.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2021.199

We thank the reviewers for their insightful comments, and we are confident by incorporating their suggestions, we have improved the overall quality of our work.

2A. Second Round Review

Reviewer B

My review of this updated submission is based upon whether the issues I brought up with the first submission.

Important references are missing.

- We have included additional references as the result of an additional literature review.

The additional up to date references on e-voting using blockchains are appreciated.

The use of blockchains in electronic voting is not novel, and the paper fails to establish precisely the requirements that the block chain will meet.

- We have taken additional steps to clearly identify the assumptions on which our approach is based, and what requirements we aim to solve. While the use of blockchains in electronic voting is indeed not new, we have 1) included citations to related work and 2) attempted to clarify the areas in which our work is different from that work.

Now that the assumptions are explicitly stated, it is clear that the use of blockchain is to provide a trustworthy (immutable) audit. There has been much previously published research on audit trails in voting systems. The submitted paper would be greatly improved by referring to this work, and making a comparison between blockchain and other audit systems such as voter-verifiable audit trails (VVAT). Many of these systems meet the specific audit requirements that your paper specifies without using a blockchain, so the paper needs to clarify what makes the blockchain different/better

It states that it will use "blockchain technology in order to ensure voter secrecy, vote correctness, and equal voting rights." But, these informal concepts are not rigorously defined/specified.

- In the original paper, we included a reference to other locations in which these concepts are rigorously defined. To ensure that our paper is read- able as a self-contained unit, we have incorporated more definitions into the text of our work.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2021.199

OK

The paper's high level objective is stated as "We ask the following research question: In what way can a blockchain-based electronic voting process provide election integrity while maintaining voter secrecy?" However, there is no specific answer to this question.

- We extended the answer to this question in the Conclusions section.

OK

The use of 2 blockchains (one for the electronic urn and one for the electoral list) is not particularly novel and the separation of the 2 by a ballot claim ticket is a fairly standard approach.

- We acknowledge this and extended our work by citing a number of appropriate sources.

OK

Figure 1 is missing in the paper - so it is hard to validate the proposed architecture against the voting process being proposed.

- The version of the paper uploaded to Ledger journal did in fact contain figure 1. We apologize for any possible incompatibility issues and will strive to produce the final PDF in a more reliable format.

OK

The "introduction of a new consensus algorithm that is specific to ele tronic voting." is a minor contribution as the paper fails to explicitly identify the advantages of the proposed algorithm over other algorithms/approaches.

- We stand by our contribution as a valuable one. However, we have, hopefully, improved our argument.

The explanation of the difference from the VoteBook algorithm is appreciated.

The testing scenarios in table 1 hardcoded in the main python program rather than in configurable separate test files. It is not clear that the implemented tests cover all different scenario executions completely (in terms of requirements checking, and in terms of test code coverage).

- The referenced code is meant as a proof-of-concept, rather than as a functional system. It is not intended to be a scalable prototype. However, in response to the reviewer's comments, we have improved the codebase, and will continue to do so as this work evolves.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2021.199

As a proof-of-concept, it is important that you demonstrate that the prototype does function correctly for the small number of scenarios that you have identified. It is acknowledged that you cannot test exhaustive, but the paper should explicitly show which tests correspond to which specific scenarios. As the tests are implemented as simulations, it is important to show how well the simulations explore the possible behaviours of the system. It is good that you have tested 7 scenarios, but how well do these scenarios cover the requirements?

The paper claims that "The readability of Python code also served as documentation for our voting process." . . . this is poorly justified and the code does not provide adequate documentation.

- Additional comments have been added to the code.

OK

The conclusions state: "While the use of blockchain technology is not a solution to all election-related issues, it can address some problems. Unfortunately, it may also introduce new ones." The paper fails to provide much insight into the +s and -s with respect to using different blockchain architectures/protocols for e-voting.

- The author guidelines limit the size of our contribution, and encourage authors to focus their contributions on a single topic of research. While conducting a broad evaluation of blockchain architectures and protocols for use in e-voting is certainly a worthwhile endeavor, it is not contained in the scope of this paper.

OK - but the paper should specifically address the weaknesses/potential problems of the blockcahin architecture that it proposes.

The authors are encouraged to provide a much more detailed state-of- the-art in the use of blockchain technologies for e-voting.

- See above.

The comment was that the paper should better explain the novelty of the proposed approach wrt the wide range of alternative proposals for using blockchain in e-voting. This is certainly something which is in the scope of the submitted paper.

They are missing many of the key references to published academic work, and fail to reference many alternative approaches that exist (commercial and non-commercial)

- We have endeavored to include such references. Without specific details, we are unable to respond to the reviewer's comments in order to explain why certain references were omitted.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2021.199

OK - The additional references to recently published work on blockchain for e-voting address this issue

The citations in notes 4,7,9,11 and 12 are to on-line material; but they are cited inconsistently and incompletely.

- Citations are automatically formatted by LaTeX using the Ledger bibliography style. If desired, we will manually override these citations.

Please check that the bibtex entries are as complete as possible.

Reviewer C

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

Not sure

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?

Bottom 50%

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

It seems the real contribution here compared to other papers in the literature is the consensus algorithm. As the authors reference, dual blockchain architectures are not new. Personally, I don't feel the individual transaction details (for 'claim' and 'cast') constitute enough adequate original material for a paper. However, the consensus algorithm might. But I think the authors should be very clear with the specifics of other dual blockchain architectures and why the consensus algorithm proposed in the paper is necessary. Should the authors present a rigorous argument in favor of their consensus algorithm as a candidate for dual blockchain voting architectures, I think this would be a good paper and would be more than adequate for acceptance in an academic journal. I have a few suggestions and notes below on how the authors may be able to achieve this, but I do want to note that I quite liked the experiment and implementation made public on GitHub; I thought the code was good to illustrate the themes

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2021.199

of the paper.

* To truly illustrate why a "specialized" or original consensus algorithm is necessary for voting, it would be useful if the authors very clearly articulate where other proposals are lacking or why existing consensus algorithms are inadequate. It isn't entirely clear why the proposed consensus algorithm is particularly necessary / superior for voting purposes. For example, it isn't clear why the authors build off the Ripple consensus protocol especially since, presumably, all nodes will be known and authenticated ahead of time by the voting authority.

* It is necessary to completely specify the network and fault models considered for a proper security analysis. For example, it is mentioned "Nodes that disagree with the state of the blockchain, as well as their transactions, areexcluded from consensus-building. The presence of excluded nodes should be exceptional..." Because the network (or at least my understanding of the network assumptions) is assumed to be reliable (i.e. no dropped messages) and all nodes are synchronized, then my guess would be there are two types of problems we might encounter, a node crashing and a node exhibiting (honest or dishonest) Byzantine behavior. For the former problem, comparing hash values of blocks isn't strictly necessary and to fully account for the latter problem it's worth discussing the Byzantine faults that might occur under the model. Making these specifications will also be important to distinguish why a blockchain consensus algorithm is needed as opposed to a traditional (Byzantine or not) consensus algorithm.

* Although the experiment was a good contribution to the work, I think it would be necessary to conduct a security analysis.

* Proofs or arguments of correctness should be provided.

* I don't believe the consensus algorithm is entirely specified, and there is a potential attack in the protocol. The bug is a race condition on the Voter Blockchain when voters try to get their ballot claim ticket. Suppose Mallory is an adversary. At time t0 Mallory could attempt to claim a ticket at two distinct polling places. Since the Authentication Machines at both polling places will have the same synchronized state at t0, they will both issue Mallory a ticket at time t1 since she has not voted yet at that time. It is not clear how the algorithm would proceed and validate the transaction at the next time step. This concurrency problem is akin to "write skew" when you have two or more writable databases. You need some transaction or locking mechanism that the databases could participate in to ensure some invariant (like Mallory can claim one and only one claim ticket at any polling place at any given time). Something like two-phase locking (appropriately analyzed within the security model) could prevent more than one machine from issuing a valid ticket to the same person. Although one could argue that the Authentication Machine can be assumed perfect (i.e., it's impossible for Mallory to perform such an attack), the problem is in theory solvable at the database level and should very much be a consideration in the design of the algorithm, especially since voting security is of utmost importance. At the very least attacks like this --- and how they can be mitigated --- should be mentioned in the manuscript.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2021.199

2A. Second Round Authors' Response

We thank the reviewers for their detailed comments, and have endeavored to address their concerns. A summary of our responses is included below.

Editor's Comments

Most specifically, both reviewers commented that the submission needs a more detailed review of the state of the field (with specific reference to dual-chain architectures), and a more detailed and convincing explanation of what benefits it has over other established audit methods for e-voting.

- Additional literature review has been included throughout the paper and additional references are included. Specifically, the Introduction now includes explicit discussion of concerns imposed by the use of Direct Recording Electronic voting machines, and of voter-verifiable audit trails. Section 3 includes discussion of the use of Dualchain Network Architectures.

Reviewer B

The submitted paper would be greatly improved by referring to this work, and making a comparison between blockchain and other audit systems such as voter-verifiable audit trails (VVAT). Many of these systems meet the specific audit requirements that your paper specifies without using a blockchain, so the paper needs to clarify what makes the blockchain different/better

- This has been addressed by extending the Introduction section, in which we position our work more clearly.

It is good that you have tested 7 scenarios, but how well do these scenarios cover the requirements?

- We extended the discussion in the section describing the proof of concept, and have clarified the relationship between the requirements, the scenarios and the method of implementation.

The paper should specifically address the weaknesses/potential problems of the blockcahin architecture that it proposes.

- We have endeavored to make the limitations of our approach more explicit throughout the paper, and revisit the scoping decisions in the Future Work section.

Please check that the bibtex entries are as complete as possible.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2021.199

- We have done so.

Reviewer C

The authors should be very clear with the specifics of other dual blockchain architectures and why the consensus algorithm proposed in the paper is necessary.

- We have included additional discussion to address this comment. Most of that discussion takes place in the Introduction section.

To truly illustrate why a "specialized" or original consensus algorithm is necessary for voting, it would be useful if the authors very clearly articulate where other proposals are lacking or why existing consensus algorithms are inadequate.

- We have included specific arguments why proof-of-work is not sufficient for e-voting, and we have made more explicit comparisons with the Ripple approach.

It is necessary to completely specify the network and fault models considered for a proper security analysis.

- Agreed. We have made the preliminary argument that this is addressed by our assumptions, and by the expectation that we are practically Byzantine fault tolerant. Our Future Work section acknowledges this comment and we hope to provide more in-depth analysis then.

Although the experiment was a good contribution to the work, I think it would be necessary to conduct a security analysis. Proofs or arguments of correctness should be provided.

- The adversarial scenarios discussed are the result of initial threat modeling and initial arguments of the correctness of our approach are included. We will extend on this in future work and mention so explicitly.

I don't believe the consensus algorithm is entirely specified, and there is a potential attack in the protocol.

- We have extended the discussion of the protocol and proposed a resolution for such situations.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2021.199