The Implementation of a Blockchain-Based E-voting System for Clubs at the University of Guelph

Myron Ladyjenko and Eric Buys.
University of Guelph, Guelph, ON, Canada.
mladyjen@uoguelph.ca, ebuys@uoguelph.ca

ABSTRACT

In a World where transparency and trust are paramount, a visionary solution emerges – a Blockchain-Based E-Voting System tailored to the needs of university clubs. The project aims to study the up-to-date state of blockchain-based e-voting research along with associated possible challenges while aiming to forecast future directions. We aim to create a solution that encompasses the advantages of blockchain technology while keeping voters' identities private. To perform our research and implementation we will follow the literature review and modelling methodologies combined with the Agile paradigm of software development. Our solution aims to provide a transparent e-voting system that fosters trust among student communities.

ACM Reference Format:
Myron Ladyjenko and Eric Buys.. 2024. The Implementation of a Blockchain-Based E-voting System for Clubs at the University of Guelph. In *Proceedings of , 2024, Introduction to Cryptography (Introduction to Cryptography),* 4 pages.
https://doi.org/10.475/123_4

1 INTRODUCTION

Voting today relies on the credibility and truthfulness of the central managing government/organization to be honest about electoral results. While this system has been in place for many years, it still suffers from the inherent weaknesses of a trust-based model. This can be seen in examples like the 2020 Belarusian Presidential Election [6]. Voters must be able to trust the central organization to accurately and fairly count every valid vote. However, implementing a decentralized blockchain-based electronic voting system takes away the reliance on a central authority to be truthful in their statements on the outcome of an election.

Our project is related to Blockchain Technologies with a focus on the application of electronic voting systems, specifically for the University of Guelphs' club elections. The current voting system in place involves casting a vote in an online form and being presented the results by the clubs themselves. As a voter, there is no way to verify the results of the election using this system. The primary objective of our proposal is to create a transparent and secure voting mechanism for clubs, while also ensuring voters' privacy using existing cryptographic methods. This will be done by utilizing the decentralization, transparency and immutability benefits of blockchain solutions [2].

This system addresses various challenges in traditional voting systems like fraud, corruption, lack of transparency, counting inaccuracies and time consumption for counting votes. However, some challenges with a blockchain-based approach include throughput (measured as the number of successful transactions per second), privacy and authentication [2].

2 PRELIMINARY LITERATURE REVIEW

A preliminary literature review reveals that implementing a blockchain-based electronic voting system is an idea that has intrigued many people. There are various cases around the world where a blockchain-based voting system has been trialled. One example of this can be seen in Japan where it was used for an online voting validation test. Another key example can be seen in the small town of Zug in Switzerland, where the first municipal vote in Switzerland using blockchain was held. This town has now become one of the world's leaders in integrating blockchain technologies [2].

The major strengths associated with blockchain can be seen through its built-in transparency, immutability and security [2]. The properties of immutability and security are exemplified through concepts like proof-of-work which ensure that blocks cannot be changed without redoing a lot of work [5]. Additionally, the inherent transparency is only available due to the distributed ledger available in blockchains like Bitcoin [3].

One critical weakness with current blockchain solutions is the lack of transactions per second that they can process [2]. In addition to this, voter anonymity needs to be addressed when casting votes, however there have been various avenues of research delving into this topic like the Blind Signature Protocol, ring signature and group signature [1][2].

Based on all this, our research will focus on some existing blockchain technologies like Bitcoin and Ethereum, implementing key components of these to create a blockchain-based voting system from scratch. Additionally, this project aims to combine some of the existing research done related to the weaknesses of blockchain.

3 PROJECT OBJECTIVES

The primary objectives of our research project revolve around analyzing, modelling and implementing Blockchain-Based E-Voting Systems and its application for University Clubs. The questions that our research project seeks to answer are:

1. What are the building blocks that are required to implement a blockchain-based e-voting system?
2. How can the privacy of voters be ensured?

Introduction to Cryptography, 2024

ACM ISBN 123-4567-24-567/08/06.
https://doi.org/10.475/123_4

3. How can a voter be prevented from voting with multiple accounts or multiple times within the same account?
4. How can the vote which was cast become public information to allow the transparency of the election?
5. What type of Blockchain would be suitable for Universities clubs' elections?

The primary objectives of our research projects are:

1. Implement the key features of the Bitcoint-based blockchain (tailoring to be a consortium blockchain to more precisely follow the use case of University clubs).
   a. Miners and mining algorithms.
   b. Private/public keys, hashing and chaining algorithms.
   c. Setup a peer-to-peer(P2P) network.
2. Implement a front-end application to allow users to log in to the system and participate in the election.
3. Implement a system where voters can cast their votes while maintaining their identity private at any point in time.
4. Implement a system where a voter is only able to cast a single vote per election.
5. Implement a system where all votes are visible and each person can verify their vote is counted.

In summary, our research project aims to investigate, model, and implement Blockchain-Based E-Voting Systems tailored for University Clubs. Our study will include the identification of essential building blocks for implementing such a system, ensuring voter privacy, preventing multiple voting instances and establishing transparency in election results. Combining all of the results, we will be able to build a blockchain-based e-voting system that is applicable to University clubs.

4 METHODOLOGY

The two primary research methodologies for this study are literature review and modeling. The implementation for this project will plan to follow an Agile development process [4]. The first phase will consist of a literature review to gain an understanding of attempted techniques, current issues with feasibility and the current best practices. Based on this understanding, a model for a blockchain-based e-voting system will iteratively be built by applying an agile development process.

A literature review is pivotal to gaining a broader understanding of the topic at hand. Without it, much time would be wasted investigating avenues that have already been deeply investigated. Modelling is crucial in verifying proposed ideas found through literature review. It will also give room to adapt and make changes where needed.

5 RESOURCES AND MATERIALS

Hardware

- 3 personal computers

Software

- Visual Studio Code, Github, Discord, Trello

Languages and Frameworks

- Python, Flask, HTML, CSS, JavaScript

6 TIMELINE & IMPLEMENTATION PLAN

For the research project involving modelling a Blockchain-Based E-Voting System for a University, 12 weeks have been allocated. In order to create a realistic timeline, a thorough analysis and breakdown of the objectives and expected outcomes into smaller tasks was performed.

Week 1-2 (January 8, 2024): Initial Research

- Research topics in cryptography and agree on an idea

Week 3-4: Planning and Research

Project Proposal: Friday, January 26, 2024.

- Define the scope, requirements, and constraints of the project.
- Finalize the project plan and create a research proposal.
- Research existing blockchain technologies and e-voting systems.

Week 5: Setting up mining and Blockchain blocks

Objective 1a: Implement a single miner.

- Set up a basic blockchain structure.
- Implement a basic mining algorithm.

Objective 1b: Creating a block and storing transactions in it.

- Develop functionality to create a block.
- Implement transaction storage within blocks.

Week 6-7: Blockchain Implementation

Midterm Project Discussion: Tuesday, February 27, 2024.

Objective 1c: Chaining blocks based on the previous hashes.

- Develop logic for linking blocks using hash pointers.
- Implement validation checks for the blockchain.

Objective 1d: Encryption using private/public key pairs.

- Implement key pair generation and management.
- Integrate encryption into transaction handling.

Week 8-9: Transparent and Auditable Results

Objective 2a: Ability to count all votes without revealing private voters' information.

- Design a secure mechanism for vote counting.
- Implement cryptographic techniques to protect voter privacy.

Objective 2b: Ensuring a person is only allowed to vote once per election.

- Implement user authentication.
- Develop mechanisms to prevent duplicate voting.

Week 10: Front-end Application

Pre-recorded Presentation & Demo Video: Friday, April 5, 2024.

Objective 3a: Hosted front-end application.

- Develop a user interface for voters.
- Integrate the front end with a blockchain backend.
- Record a demo to present the model.

Week 11-12 (April 12, 2024): Stretch Goals

Final Report Code: Friday, April 12, 2024.

Goal 1: Final Review.

- Create a final report and clean code for submission.

Stretch Goal 1a: Implement a P2P network with multiple miners.

- Extend the blockchain to support multiple miners.
- Implement basic peer-to-peer networking.

Stretch Goal 1b: Broadcasting a transaction (vote) to the network.

- Task: Develop a mechanism for broadcasting transactions.
- Task: Ensure synchronization across the P2P network.

While the provided timeline serves as our initial plan for the project's progress, some adjustments may be necessary due to factors such as the complexity of the development and unforeseen challenges that may arise during implementation. Before each major milestone, a buffer time was incorporated into the schedule in order to allow for the accommodation of unexpected hurdles or the need for additional refinement. The use of the Agile methodology, biweekly instructor reviews and visible progress will help to ensure that milestones are achieved effectively and that the final solution aligns with the project's expected objectives. To ensure that our project meets the expected outcomes, we will perform unit and system integration testing to verify the functionality.

7 POTENTIAL CHALLENGES AND SOLUTIONS

Some of the key potential challenges facing this project are outlined below as well as a solution which may help to address the issue.

Challenge: Implementing a blockchain from the ground up
Solution: Existing research papers and tutorials can be referenced.

Challenge: Ensuring the privacy of a voter casting a vote and ensuring only one vote is allowed per election
Solution: There are some topics related to this issue and some proposed solutions include the Blind Signature Protocol [1], ring signature, group signature and the mix network concept [2].

Challenge: Indicating the start and end of an election
Solution: Using a blockchain for a singular election and publishing the public/private key pair to send votes to at the corresponding beginning and end of the election [1].

Challenge: Linking a student's University of Guelph email to a specific account
Solution: Existing research papers and tutorials can be referenced for setting up a blockchain wallet or similar solution [8].

Challenge: Implementing a peer-to-peer network [7]
Solution: Investigate how to perform communication across the network by reading research papers and analyzing existing solutions (technologies used).

8 EXPECTED OUTCOMES

For our research project, we decided to model a Blockchain-Based E-Voting System for University Clubs. The full solution offers to deliver a comprehensive and innovative solution for University club elections. In our research project, we will focus on several key expected outcomes (these expectations are based on time available for the duration of this project):

Expected outcomes

1. Implementation of a Blockchain
   a. Single miner
   b. Creating a block and storing transactions (votes) in it
   c. Chaining blocks based on the previous hashes
   d. Encryption using private/public key pairs
2. Transparent and Auditable Results
   a. Ability to count all of the votes without revealing private voters' information
   b. Ensuring a person is only allowed to vote once per election
3. Hosted front-end application
   a. Enabling voters to log in using their University of Guelph emails and vote for an election

Stretch Goals:

1. Peer-to-peer (P2P) network.
   a. Multiple miners
   b. Broadcasting a transaction (vote) to the network to be put into a block.

The successful accomplishment of these outcomes will serve as a proof of concept for implementing a blockchain-based e-voting system for university clubs at the University of Guelph. Expanding the designed and implemented system will allow the creation of a comprehensive system that will enable a reliable, secure, and transparent e-voting system tailored for university club elections, fostering a more inclusive and democratic structure.

9 CONCLUSION

The research project addresses a vital need for a blockchain-based transparent e-voting system tailored for University clubs. By investigating existing solutions for blockchain-based e-voting systems and creating a system for transparent elections the lack of trust in the electoral process of the club elections at the University of Guelph can be addressed. The proposed research topic aims to not only establish a secure blockchain infrastructure for storing and validating votes but also to ensure voter privacy and prevent duplication of votes. By incorporating features inspired by Bitcoin and leveraging a peer-to-peer network within the consortium, our solution seeks to provide a robust and innovative platform for conducting University Club elections.

Ultimately, the project's main purpose is to contribute to the enhancement of democratic processes within university communities through the application of cutting-edge blockchain technology.

REFERENCES

[1] Julio César Perez Carcia, Abderrahim Benslimane, and Samia Boutalbi. 2021. Blockchain-based system for e-voting using Blind Signature Protocol. In *2021 IEEE Global Communications Conference (GLOBECOM)*. 01–06.

[2] Jun Huang, Debiao He, Mohammad S. Obaidat, Pandi Vijayakumar, Min Luo, and Kim-Kwang Raymond Choo. 2021. The Application of the Blockchain Technology in Voting Systems: A Review. 54, 3 (2021).
[3] Suvarna Kadam. 2018. Review of Distributed Ledgers: The technological Advances behind cryptocurrency.
[4] Peng Xu Lan Cao1, Kannan Mohan and Balasubramaniam Ramesh. 2009. A framework for adapting agile developmentmethodologies. *European Journal of Information Systems* 18, 4 (2009), 332–343.
[5] Satoshi Nakamoto. 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. *Cryptography Mailing list at https://metzdowd.com* (03 2009).
[6] Olga Onuch and Gwendolyn Sasse. 2022. The Belarus crisis: people, protest, and political dispositions. *Post-Soviet Affairs* 38, 1-2 (2022), 1–8.
[7] R. Schollmeier. 2001. A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In *Proceedings First International Conference on Peer-to-Peer Computing*. 101–102. https://doi.org/10.1109/P2P.2001.990434
[8] Saurabh Suratkar, Mahesh Shirole, and Sunil Bhirud. 2020. Cryptocurrency Wallet: A Review. In *2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*. 1–7.