UniVote: A Paradigm Shift From Traditional Voting Methods

Abstract

Blockchain decentralized applications(Dapps) has been mainly involved in solving problems in the financial sector and upgrading the infrastructure of previous blockchain Dapps, but not too many interests have been mirrored in building real-world applications. UniVote plans to change that. Since the dawn of civilization, voting has been one of the most popular problems involving centralization. Every-time an election takes place there is always dissatisfaction mainly due to the lack of transparency involved in the voting process which can be linked to issues like unverifiable votes being approved, vote manipulation and data theft. This does not happen only in the high democracies but also at the grassroots level, universities being one of them. Using the Sui object-centric data model, dynamic scaling, Zkps, and the ability to track your vote and Election process in real-time, UniVote plans on making the whole process transparent and decentralized while keeping the Voters' data secure and to themselves.

Introduction.

Univote is a trustless voting platform created to fix the problem of traditional voting methods and their flaws, it plans on using SUI's object-centric data model and ZKps. Using SUI's object-centric model allows us to easily assign votes as objects that are tied to their respective owners (addresses), now this allows for the transfer of ownership of objects which in this case will be voting, we also plan on taking advantage of sui's low latency allowing for quicker voting times and a seamless voting experience, another thing we can't overlook is voters' privacy which is important in keeping voters' identity safe when votes are being released and can be reviewed— in real-time, we plan to do this by using zk methods to verify voters' identity all while keeping them private, this will be fully addressed later in this paper.

This whitepaper will be divided into three parts;

- The first is a brief overview of university voting methods and problems related to it.
- Secondly, the solution to these problems is addressed using our method.
- Finally, we will dive into the features we plan to use and how they work.

The problem with university voting methods.

Overview

The University of Benin(UNIBEN) recently introduced a new method of voting which was used in the just recently concluded elections, it is one of the safest so far of all the previously conducted elections ever done in the institution, voters were required to input a uniquely

generated code which could be found at every eligible student(voter)'s Kofa, also only duly matriculated and registered students for the current session are eligible to contest the election, except for final-year students, spillover students, direct-entry students, 100-level students, and diploma students. However, before election day, there was no concrete paper on how they planned to tally votes and the election process. We observed that after voters log into the terminal they cast their votes and then after the votes are tallied and results announced that same day, this might look like a secure and trustworthy process but it is full of flaws, the next section will address that.

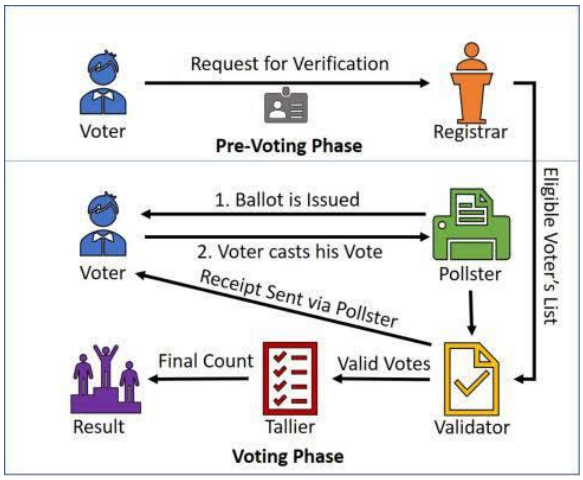


Fig 1.0(a simplified analogy of electronic voting)

Electronic Flaws

A sample survey was conducted after the election and it was brought to our notice that about 40% of students did not carry out the vote themselves and was done by someone else on their behalf, this stresses that there could have been a heightened activity of vote buying which will be our first flaw of UNIBEN electronic voting system—vote buying. We noticed that when those eligible users inputted the unique code to get access to the voting terminal there was no measure to make sure that it was those users who made the decisions on who they wanted to vote for. Another flaw we noted was the multiple voting which can be from a single device which indicates that there were no measures put in place to make sure there was no misuse of the system. Another flaw was the lack of user privacy as users were required to input their credentials to gain access to the terminal, this may seem small but it is a great threat to voters' data as we have seen data breaches happen before in the past if no appropriate measure put in place. In that same survey, a significant amount of people still did not feel satisfied with the voting process and this result will lead us to the final flaw we noticed—lack of trust, we've seen that there was no measure put in place for tracking and easily verifying votes in real-time, which will significantly decrease the trust in the voting process.

Solutions to the proposed Problem

The nature of the Sui blockchain enables objects to be mutable or immutable depending on how they are used. Using the Sui blockchain will negate candidates and third parties to avoid tampering with the results, as the ability for malicious candidates to carry out Sybil attacks on the blockchain in their favor is null and void due to the decentralized nature of the Sui blockchain. Transparency and trust in UniVote are possible because every transaction carried out on the Sui blockchain is not hidden but is available for all to view. This is done in anonymity while enabling only accredited voters to vote without revealing their Data, this will be made possible due to the advent of a method known as ZKps the full meaning being Zero-Knowledge proofs; ZKps is a cryptography method where a party(prover) proves to another party(The verifier) that something is true without revealing any information. So in this case the voter can prove that they are eligible to vote without revealing any of their personal information, the method as well, can compress lots of information into smaller pieces enabling

scalability and a smooth user experience. . UniVote will also ensure that those eligible voters can cast their vote once through the use of Device Binding which is the association of the voter's identity with their device–-removing almost all chances of Sybil, and these votes are transactions that will be validated on the Sui blockchain. The object-centric nature of the Sui blockchain enables very low latency and we will leverage this to build an optimal new way of voting therefore making easy, real-time viewing of votes whilst making the whole process private and secure. In addition, voters can view past elections because all transactions from previous blocks are stored—genesis block up until the current.

Candidates and their parties cannot manipulate votes because they do not have access to the credentials of an accredited voter because of this zk proof. In addition, this will eliminate the cases of over-voting in our electoral systems.

The Technological Aspect Of UniVote

Object-centric data model of Sui.

More classically designed account-based blockchains, like Ethereum, for example, rely on sharp structures that clearly make accounts and balances easy to distinguish. In contrast, the object-oriented approach proposed by Sui placed huge emphasis on "objects" with their own unique characteristics and particular ownership which together make them qualify as unique entities within the Sui blockchain ecosystem.
But this interesting approach is what enables us to consider each and every one of the votes about to get cast as an individual, separate object, complete with meaningful information on ownership of their respective owners. The end-to-end audit trail also plays a great role in making sure the whole process is highly documented and accounted for step by step, so everything can be traced. In the creation of Uni Vote we will use smart contracts created on the Sui Blockchain using the Move Language.
In Sui a smart contract is an object (called a Sui Move package), and these smart contracts manipulate objects on the Sui network, now these objects are addressable on-chain by unique IDs which can be easily tracked, when published the smart contract is immutable and can never be altered.This allows us to customize and build on how objects such as Voters,Votes,Ballot etc will interact with each other in the Sui Ecosystem.

Parallel Transaction Processing Of Sui.

A major problem faced when interacting with decentralized applications on traditional blockchain platforms are often a limitation to scale in the terms of transaction processing , for instance EVMs(The Ethereum Virtual Machine) processes transaction one at a time which can greatly hinder scalability, in the area of voting using this method will make it very difficult with processing requests(transactions) at peaks periods during voting, Sui overcomes these limitations by enabling concurrent processing of multiple transactions, known as transaction parallelization. Parallel execution methods has been used in many commercial spaces which includes companies like Google, Apple etc

This approach using parallel processing results in a tested rate of up to 297,000 transactions per second, in voting this will make near instantaneous verification and approval of votes while also keeping the transaction fees near 0 thus reducing cost. In line with Sui's object data model, those transactions involve changes to individual objects. Sometimes those changes simply mean ownership transfer, and sometimes a fundamental transformation, such as changing an object's appearance, Sui also allows only shared objects to go into consensus which is totally different from other traditional blockchains which requires every transaction to

go through consensus thus increasing latency, but for sui lower latency can be easily achieved.

This is an extended model in the usage of vote objects concerning the transfer of ownership to ensure that any required transfer is in a secure manner with full clarity. This shall not provide any opening for compromise or confusion but should instead ensure ownership rights remain intact. This would be ensured by one of the new concepts, namely zero-knowledge proof, which stands to provide voter anonymity.

Zero-knowledge proofs -ZKP

Zero-knowledge proof, sometimes referred to by their abbreviation ZKPs, really do realize this incredible capability wherein one party, known as the prover, convincingly proves to another party called the verifier, that a statement or claim being known to him, and the verifier approves of those claims after the prover successfully proves it to him, and during this the prover is able to keep the confidential information about claim in that he does not reveal any of the pieces of evidence or detailed information. In voters' verification using ZKPs, it will involve the process of proving his or her qualification without necessarily revealing any sensitive information, which includes the Person's name, Matric No etc.

In UniVote we plan on using ZK-SNARKs this abbreviation stands for **Z**ero-**K**nowledge **S**uccinct **N**on-Interactive **AR**gument of **K**nowledge. It is a form of ZK proof that requires no interaction between the prover and verifier. They are "succinct" because the proof size is small, and the verification is fast. Most ZK-SNARKS use elliptic curve cryptography and a trusted setup to generate parameters for the ZKPs.

This is going to be used in UniVote mainly in verification of voters.

Device Binding

To tackle one device, one vote in previous Electronic voting systems the use of device binding to ensure that there is no misuse of Votes and reduce the chances of vote buying.

Device binding is the process of associating a device as a credential to the mobile application. The authentication is considered trusted if it is initiated from the same device associated with the application.When a user logs into the app on a device for the first time. it creates a trusted link between the app on a specific mobile device and the backend server. This link is established through a 'handshake'.

Multi-Factor Authentication

To still fight against malicious attempts the use of different factor authentications will be used.

1. Email Verification of the eligible Voter to confirm the Voter's authenticity.
2. Phone Verification of the eligible Voter..
3. Biometrics Not compulsory, and fully dependent on the voters choice to improve security.

ROADMAP OF UNIVOTE

The Primary goal of UniVote has always been in line with fixing Nigeria's Electoral system but to do that we will have to first tackle grassroot and institutional voting challenges first, where we plan on growing and then expanding to a fully Nation Wide scale before then tackling Nigeria's Voting system using Blockchain.

Q4 2024.

- **Publish Whitepaper.**

Q1 2025.

- **MVP release (Minimum-Viable-Product).**

Q2 2025.

- **Beta testing.**

Q3 2025

- **App release**
- **Awareness and talks with UNIBEN board.**

Q4 2025.

- **Main Launch.**

This roadmap alligns with our current view of tackling institutional voting before going ahead into a national grade scale.

REFERENCES

https://docs.sui.io/paper/sui.pdf
https://blog.sui.io/all-about-directed-acyclic-graphs/
https://docs.sui.io/concepts/object-model?ref=blog.sui.io
https://blog.sui.io/transaction-processing/
https://medium.com/veridise/zero-knowledge-for-dummies-introduction-to-zk-proofs-29e3fe9604f1
The knowledge complexity of interactive proof systems
https://www.acjuniben.com/electoral-commission-rolls-out-guidelines-for-student-union-elections-2023-2024-academic-session/