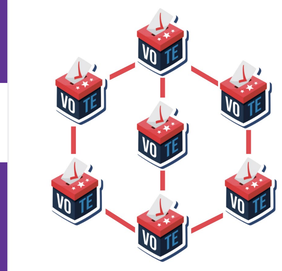
The Cloud Miners: Decentralized Autonomous Voting Using Blockchain

Department of Computer Science, Stephen F. Austin State University

[1]Juliette Marroquin Garcia, Faculty Mentor: [2*]Dr. Ivancic Christopher

[1]Email: garciajm31@jacks.sfasu.edu, [2*]Email: ivancic@sfasu.edu



ABSTRACT

In an era where democratic elections face increasing challenges from security vulnerabilities and accessibility barriers, this project explores innovative solutions to enhance the integrity, transparency, and inclusivity of voting systems.

The project leverages emerging technologies, including blockchain for secure, immutable voting records; IoT devices to increase accessibility and autonomy in voting processes; and smart contracts to decentralize control and enforce data ownership.

By addressing critical issues such as transparency, availability, cybersecurity, and voter education, the project aims to design a secure, scalable, and efficient voting framework.

INTRODUCTION

Traditional voting methods rely on centralized authorities, which can be hacked, tampered with, or mismanaged, making elections vulnerable and less trustworthy.

This project proposes a Web3-based voting system, which moves away from centralized control and instead uses blockchain, smart contracts, and IoT devices to create a more secure, transparent, and accessible election process.

This solution empowers voters, increases trust in elections, and lays the groundwork for a new era of democratic engagement.

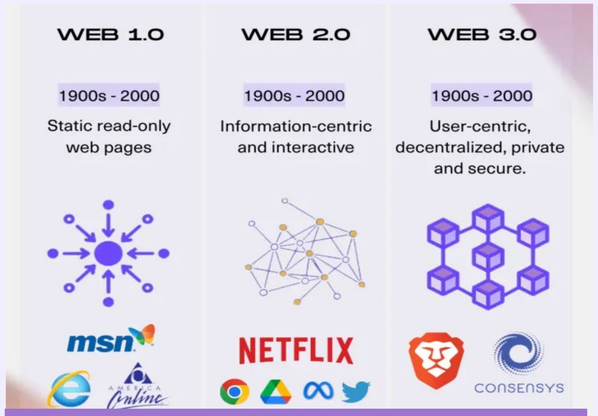


Figure 1. Web Iterations

KEYWORDS

- **Blockchain** is like a digital notebook that no one can erase — every vote is recorded permanently and cannot be changed.
- **Web3** means people control their own data and interact directly with systems, like voting apps, without needing to trust a central authority.
- **Smart contracts** are automated rules written in code. They count votes, manage access, and enforce security — all without needing a middleman.
- **IoT voting devices** make it possible for people to vote securely from different locations, including rural or underserved areas.
- **Decentralized** – no single party controls the election.
- **Transparent** – anyone can verify the results.
- **Secure & Private** – votes are encrypted and tamper-proof.
- **Accessible** – voters can cast ballots via smart devices, enabling broader participation.

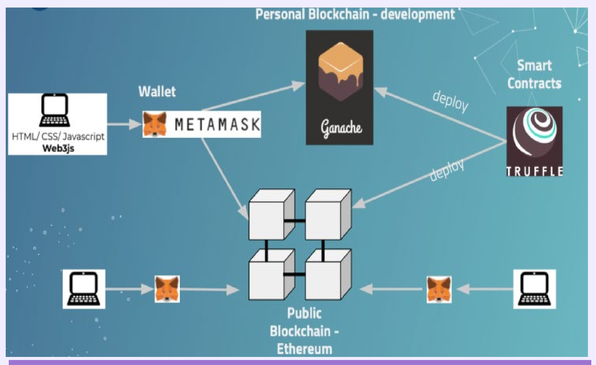


Figure 2. Web3 Network System Diagram

METHODOLOGY

To build a secure and decentralized voting system, this project was developed on the Ethereum blockchain, enabling transparent and immutable vote recording through smart contracts written in Solidity, a programming language designed for blockchain logic and automation.

The development environment was powered by Ganache, a personal Ethereum blockchain used for local testing and simulation of the voting system. Truffle, a blockchain development framework, was used to compile, deploy, and test the smart contracts, providing structure and repeatability during the development process.

For user interaction, the system integrates with MetaMask, a browser extension that acts as a digital wallet and Web3 gateway. MetaMask allows voters to connect securely to the blockchain, authenticate themselves, and cast their vote directly through a decentralized interface without relying on a central server.

This stack—Ganache, Truffle, Ethereum, Solidity, and MetaMask—enabled the creation of a prototype voting system that is self-verifiable, transparent, and tamper-resistant, reflecting the principles of Web3 and decentralized governance.

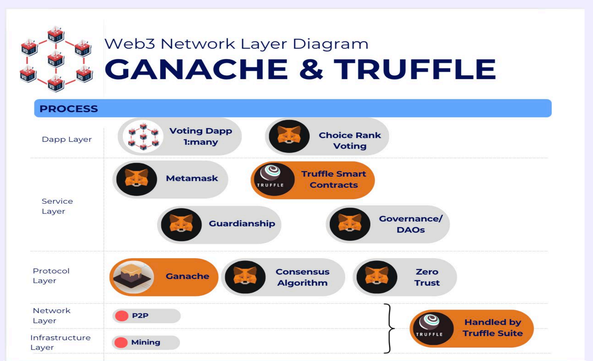


Figure 3. Web3 Network Layer Diagram

ANALYSIS

This project set out to investigate whether blockchain technology could support the core requirements of a general government election—namely, security, transparency, accessibility, and verifiability. Unlike many blockchain voting experiments focused on small-scale or internal applications, this research specifically targeted the feasibility of a public, large-scale election system suitable for civic use. Through iterative development and testing, a functional minimum viable product (MVP) was successfully implemented using Ethereum, smart contracts, and decentralized identity mechanisms. The MVP demonstrated the ability to cast and record votes immutably, verify results transparently, and operate without centralized control.

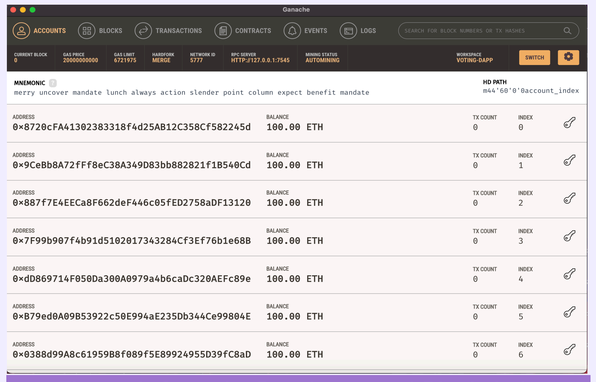


Figure 4. Ganache Developmental Blockchain

CONCLUSION

This project demonstrates that blockchain technology, when combined with smart contracts and decentralized tools, offers a viable foundation for secure, transparent, and autonomous voting systems. By successfully developing a minimum viable product tailored to the requirements of a general election, this work affirms the potential of Web3 infrastructure to address longstanding challenges in electoral integrity and accessibility.

However, the path to full-scale adoption requires more than technological innovation—it demands supportive legislation, regulatory frameworks, and proactive government engagement. Only through institutional collaboration can this approach be properly built out, standardized, and trusted by the public. With such support, blockchain-based voting systems have the potential to help restore faith in democratic processes and safeguard the future of free and fair elections.

FUTURE WORK

Future phases of this research will explore alternative blockchain platforms or consensus mechanisms that eliminate the need for monetary transactions, enabling more equitable and cost-effective election deployment. Additionally, the system will undergo adversarial testing to evaluate its resilience against vote manipulation, including simulated attempts to overturn election outcomes through smart contract exploitation or blockchain-level attacks. Further investigation will also assess the security of IoT-based voting interfaces by identifying vulnerabilities that could allow unauthorized or fraudulent vote submission. These efforts aim to strengthen the platform's integrity, validate its security posture, and develop best-practice recommendations for safeguarding decentralized election technologies.

Contact

Juliette Marroquin Garcia
Department of Computer Science
1936 North St.
Nacogdoches, Texas 75964
Juliette.Marroquin.Garcia@gmail.com

Acknowledgments

This research was supported by the College of Sciences and Mathematics as part of the 2025 Practicum in Cyber Security Research at Stephen F. Austin State University. I would like to extend my sincere thanks to Stephen F. Austin State University for the opportunity to pursue this work. I am especially grateful to my faculty advisors — Dr. Ivancic, Dr. Zheng, and Dr. Ogale — for their mentorship, guidance, and continued support throughout the duration of this project. Their insights were invaluable in shaping the research and development process.

References

1. **Kurt, E. (2022, August 18). Testing strategies for Web3 DApps. Medium. https://ekremkurt1907.medium.com/testing-strategies-for-web3-dapps-dbbf9ad0a388**
2. **Lunar Strategy. (2024, January 24). The best Web3 social media platforms of 2024. Lunar Strategy. https://www.lunarstrategy.com/article/the-best-web3-social-media-platforms-of-2024**