SCHOOL OF COMPUTER SCIENCE (SCSE)

VIT®
BHOPAL

Blockchain Ballot: Revolutionizing Voting

Faculty Supervisor :Dr.S.Vairachillai

COURSE CODE -DSN2099

Team Members

- Akshat Agrawal 21MIP10022
- Suman Bhandari 21MIP10028
- Naman Mishra 21MIP10007

Table of Contents

- Objective
- · Literature Review
- · Proposed work
- · Real time usage
- · Hardware & software requirements
- · Overall system architecture diagram
- · List out the modules & Explanation
- · Project timeline chart
- · References

Introduction

What is Blockchain ?

Blockchain is a decentralized, distributed, and transparent digital ledger that is used to record transactions across multiple parties in a secure and immutable way. It consists of a chain of blocks, where each block contains a set of transactions, and each block is linked to the previous block using cryptographic techniques, creating a chain of blocks.This makes it resistant to tampering and provides transparency, as all participants in the network can verify the integrity of the transactions.

What is blockchain voting ?

- Blockchain voting refers to the use of blockchain technology as a platform for conducting secure and transparent voting processes. In traditional voting systems, votes are typically recorded and stored in centralized databases.

- In a blockchain voting system, each vote is recorded as a transaction on a blockchain, which is a distributed ledger that is maintained by a network of computers known as nodes. These transactions are encrypted and linked together in blocks using complex cryptographic algorithms, and once a block is added to the chain, it cannot be altered or deleted without consensus from the network. This makes the system highly secure and resistant to tampering.

Objective

Blockchain technology is leveraged to enhance the integrity, efficiency, and accessibility of voting processes, with the following key objectives:

- **Security:** Blockchain are encrypted and linked together in blocks using cryptographic algorithms, making it extremely difficult to alter or delete votes without consensus from the network.

- **Transparency**: Blockchain voting promotes transparency by providing a verifiable and auditable trail of all votes. Once a vote is recorded on the blockchain, it becomes a permanent and immutable part of the distributed ledger, which can be independently verified by voters, election observers, and other stakeholders. This helps build trust in the integrity of the voting process.

Objective

- **Decentralization**: Blockchain voting seeks to eliminate the need for intermediaries, such as electoral commissions or third-party auditors, by leveraging the decentralized nature of blockchain technology.

- **Efficiency:** Smart contracts, which are self-executing programs on the blockchain, can be used to automate vote counting, result tabulation, and other administrative tasks, potentially making the process more efficient and reducing costs.

- **Accessibility**: Blockchain voting has the potential to increase accessibility by enabling remote and online voting, which can make it more convenient for voters, especially those who face physical, geographical, or other barriers to in-person voting. This can potentially increase voter participation and engagement in the democratic process.

Literature Review

- **Open vote network (OVN) :** It was presented by McCorry, Shahandashti, which is the first deployment of a transparent and self-tallying internet voting protocol with total user privacy by using Ethereum.

- **decentralized anonymous transparent electronic voting system (DATE) :** Lai, Hsieh proposed it. This system is suitable only for small scales because of the limitation of the platform

- **BSJC proof :** Shahzad and Crowcroft says On a large scale, generating and sealing the block may cause the polling process to be delayed.

Literature Review

- **Anti-quantum electronic voting protocol :** Gao, Zheng proposed Key Generation Center (KGC) is a certificateless cryptosystem that serves as a regulator. It not only recognizes the voter's anonymity but also facilitates the audit's functioning.

- **blockchain-based electronic voting Scheme (BES) :** A BES is based on the distributed ledger (DLT) may be employed to avoid vote falsification.

- **block-based e-voting architecture (BEA):** conducted strict experimentation with permissioned and permissionless blockchain architectures through different scenarios

Literature Review

Table 3. Comparison of selected electronic voting schemes based on blockchain.

Authors	Voting Scheme	BC Type	Consensus Algorithm	Framework	Cryptographic Algorithm	Hashing Algorithm	Counting Method	Security Requirements (Measuring on a Large Scale)							
								Anonymity	Audit	Accuracy/Correctness	Accessibility	Integrity	Scalability	Affordability	Verifiability by Voter
Shahzad and Crowcroft [2]	BSJC	Private	PoW	Bitcoin	Not specified	SHA-256	3rd Party	✓	✓	✗	✓	✓	✗	✓	✗
Gao, Zheng [8]	Anti-Quantum	Public	PBFT	Bitcoin	Certificateless Traceable Ring Signature, Code-Based, ECC	Double SHA-256	Self-tally	✓	✓	✗	✓	✓	✗	✓	✗
McCorry, Shahandashti [76]	OVN	Public	2 Round-zero Knowledge Proof	Ethereum	ECC	Not specified	Self-tally	✓	✗	✗	✓	✗	✗	✓	✓
Lai, Hsieh [81]	DATE	Public	PoW	Ethereum	Ring Signature, ECC, Diffie-Hellman	SHA-3	Self-tally	✓	✗	✗	✓	✗	✓	✓	✓
Yi [83]	BES	Public	PoW	Bitcoin	ECC	SHA-256	NA	✓	✓	✗	✓	✗	✗	✓	✓
Khan, K.M. [86]	BEA	Private/Public	PoW	Multichain	Not specified	Not specified	NA	✗	✓	✗	✓	✗	✓	✓	✗

Literature Review

Author	Hashing Algorithm	Framework	BC Type	link
Ahmed Ben Ayed	SSHA256	Bitcoin	Private/public	Ayed-4/publication/341498272_A_CONCEPTUAL_SECURE_B
Francesco Fusco	Not Specified	Bitcoin and Ethereum	public	https://www.researchgate.net/profile/Andrea-Pinna-6/publication/327907758_Crypto-voting_a_Blockchain_based_e-Voting_System/links/5cb8de2da6fdcc1d499ef07a/Cry
Maria-Victoria Vladucu	Not Specified	Bitcoin and Ethereum	public/private/ hybrid	https://ieeexplore.ieee.org/abstract/document/10061373
Gautham Srivastav, Mhd.Baza	Not Specified	Ethereum	Private/public	https://www.mdpi.com/article/10.3390/app13021096
Mustafizur Rahaman	Not Specified	Ethereum	Private	https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/blc2.12021
Adel Khelifi	cryptographic hash	bitcoin	Private	https://ieeexplore.ieee.org/abstract/document/9787540
Dylan Weiss	Not Specified	Bitcoin and Ethereum	Public	https://ieeexplore.ieee.org/abstract/document/10025096
R. Hansarandi Adithya Rathnayake	SHA-256	bitcoin	Private	https://www.researchgate.net/profile/Hansarandi-Adithya/publication/368282306_Electronic_Voting_System_based_on_Blockchain_for_Sri_Lanka_Concept
Zarina Shukur	cryptographic	Ethereum	Private/public	https://www.mdpi.com/1424-8220/21/17/5874

Purpose Work

Some of the key areas of proposed work in blockchain voting include:

- Security Enhancements: Researchers and developers are constantly working on developing advanced cryptographic algorithms, implementing multi-factor authentication, and addressing potential vulnerabilities in the system to ensure that votes are securely recorded and stored on the blockchain.

- Privacy Solutions: Privacy is a critical consideration in voting, and proposed work in blockchain voting often involves finding ways to protect voter privacy while maintaining transparency.

- Usability and Accessibility: Ensuring that blockchain voting systems are user-friendly and accessible to all voters is an important area of proposed work.

Purpose Work

- Real-world Pilot Projects: These pilot projects are typically conducted in controlled environments, such as local elections or community-based decision-making processes, to gather data and insights on the feasibility, benefits, and limitations of blockchain voting in practice.

CHALLENGES

While a voting system using blockchain offers many advantages, there are also some challenges that need to be addressed.

- One of the main challenges is scalability. Blockchain technology is still in its early stages, and current systems may not be able to handle the volume of transactions required during a large-scale election.

- Another challenge is ensuring that the system is accessible to everyone, regardless of their technological literacy. This may require additional resources and support to ensure that everyone can participate in the election.

REAL WORLD EXAMPLES

Despite the challenges, several countries have already implemented blockchain-based voting systems.

- Estonia, has been using a blockchain-based system for remote voting since 2014, which has been praised for its security and efficiency.

- Other countries, such as Sierra Leone and West Virginia, have also experimented with blockchain-based voting systems, with mixed results. While these systems have shown promise, more research and development are needed to address the challenges and ensure that they can be scaled up for use in larger elections.

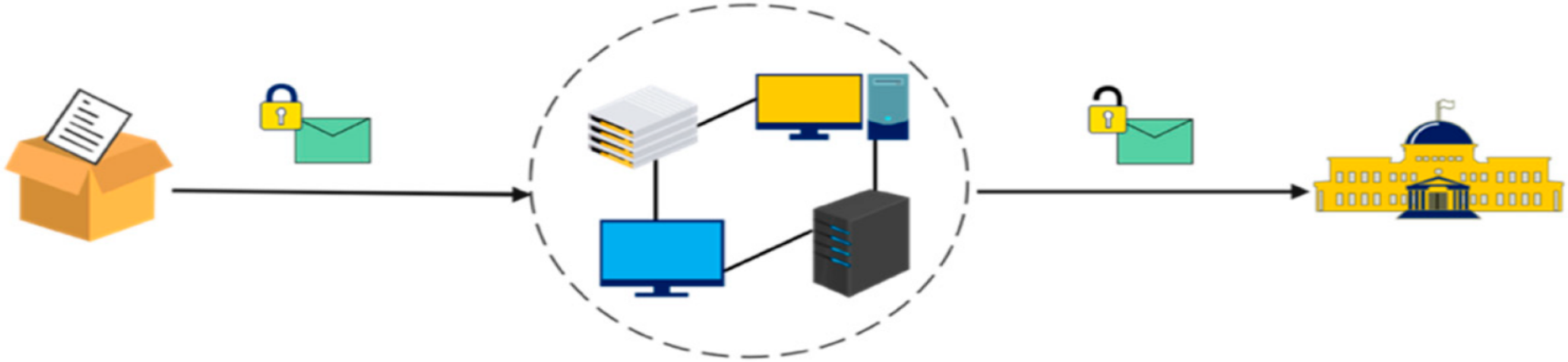
Hardware & software requirements

. For a simple proof of concept project, a basic computer or laptop with a minimum of 4GB RAM, an internet connection, and a web browser would be sufficient.

. Blockchain platform, smart contract language, front-end and back-end development tools, database, development environment, security tools.

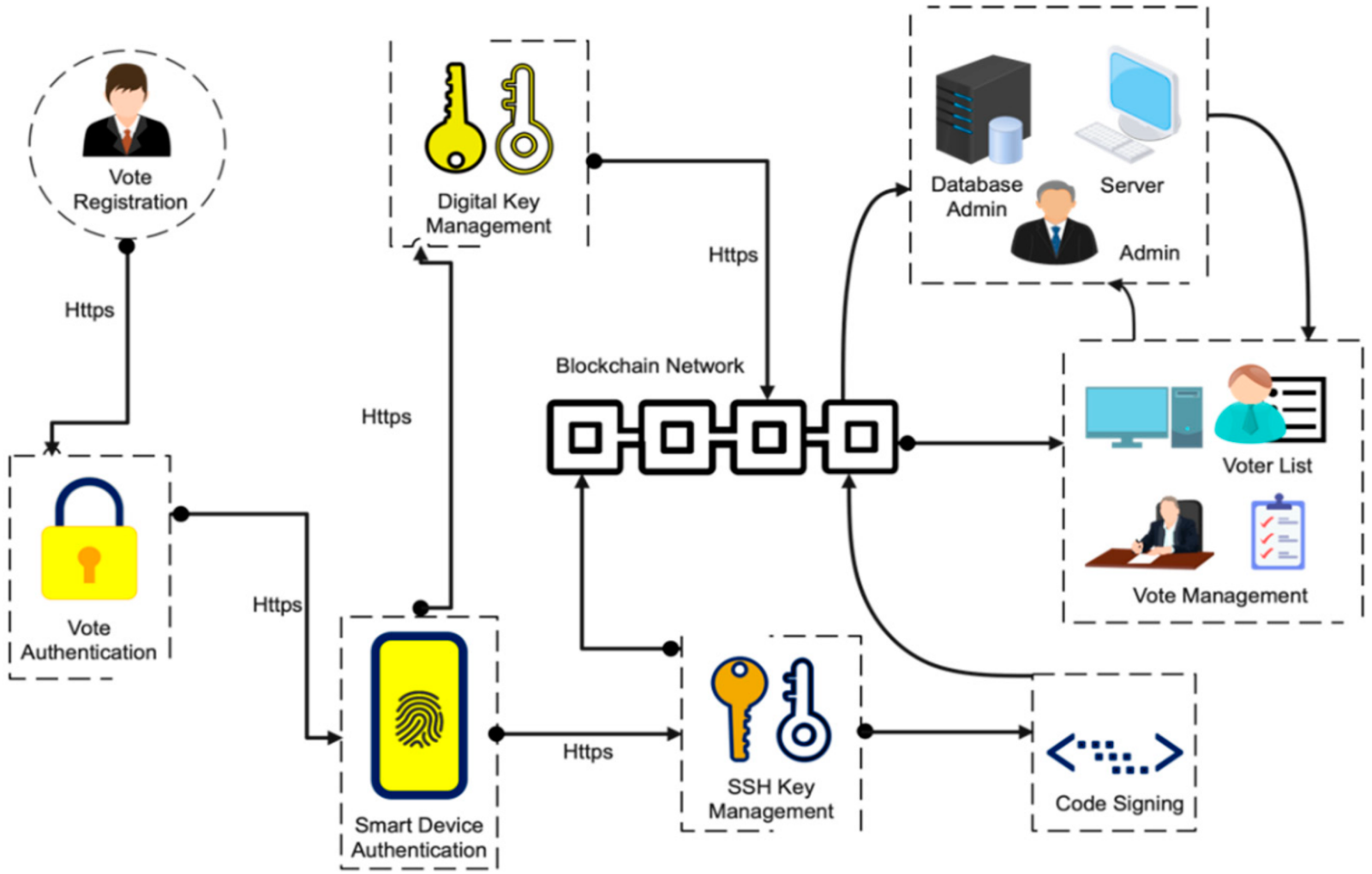
Overall system architecture diagram

Traditional Voting System



Blockchain Voting System

Overall system architecture diagram



References

https://www.mdpi.com/1424-8220/21/17/5874

https://core.ac.uk/download/pdf/155779036.pdf

THANKYOU !