Universität Zürich[UZH]

UZH Blockchain Center

VoteCrypt: Transparent Blockchain Voting System

Anurag Moyde (Ashoka University), Francis Waweru (University of Nairobi), Loubna Ezakani (ENCG Casablanca), Quan Sirui (University of Macau), Felix Ritzi (University of Zurich)

Summer School: Deep Dive into Blockchain 2024

18.07.2024

ABSTRACT

One of the key trends in the anonymous voting software market is the integration of blockchain technology to enhance security and transparency. Blockchain-based voting solutions provide immutable and decentralized platforms for recording and verifying votes, making it extremely difficult to falsify or manipulate the voting process. Additionally, there is a growing focus on improving the user experience and accessibility of anonymous voting software, with providers investing in intuitive interfaces, mobile responsiveness, and cross-platform compatibility to ensure smooth voting experiences for diverse demographics and user preferences. With VoteCrypt, we have engineered a solution that implements a blockchain-based voting system that utilizes Hedera as a high-throughput solution.

1. INTRODUCTION

VoteCrypt is suitable for simple voting processes such as polls, elections, or referendums. Simple voting, weighted voting, anonymous voting, and encrypted results are all supported. There is no trustless way to know what happens within a vote when using centralized solutions. With our blockchain, everything happens in the open, so anyone can verify the execution of the voting processes and the integrity of the votes.

2. MARKET ANALYSIS

A. MARKET OVERVIEW:

Blockchain-based voting systems have gained attention due to their potential to enhance transparency, security, and accessibility in elections and voting processes. This technology leverages the decentralized nature of blockchain to address several challenges faced by traditional voting systems, such as fraud, manipulation, and logistical inefficiencies.

B. MARKET SEGMENTATION:

- **By Type**

Depending on the type, the market can be classified into on-premises and cloud categories.

On-Premises:

- Installed and operated on the organization's local servers or infrastructure.
- Allows complete control and customization.
- Favored by organizations with strict confidentiality and security requirements.

Cloud:

- Hosted and managed by third-party providers on remote servers accessible via the Internet.
- Offers scalability, flexibility, and cost-effectiveness.

- Accessible without the need for extensive infrastructure investment.

- **By Application:**

Depending on the applications, the market can be classified into government, company, and school.

- **Government**: Voting software for government programs must comply with criminal rules, electoral laws, and international requirements to guarantee the integrity and legitimacy of the voting technique.

- **Enterprise**: Voting software recognition enterprise applications streamline decision-making processes, improve transparency, and promote stakeholder participation.

- **School**: The school voting software packages aim to allow students and school participants to participate in democratic strategies, express their criticism, and select representatives.

C. SWOT ANALYSIS:

Analyzing the strengths, weaknesses, opportunities, and threats (SWOT) of voting software using the Ethereum blockchain can provide an overview of its benefits and potential challenges. Here is a detailed SWOT analysis for such software:

Strengths	**Weaknesses**
Increased security: The Ethereum blockchain provides robust security through its decentralized and cryptographic infrastructure, reducing the risks of fraud and manipulation. Transparency: Every vote is recorded transparently on the blockchain, allowing public verification and increasing trust in the electoral process. Immutability: Once recorded, votes cannot be changed, ensuring the integrity of election results. Availability: Decentralized applications (dApps) operate without interruption thanks to the distributed nature of the Ethereum blockchain, ensuring continuous availability of the voting system.	Technical complexity: Implementing and managing an Ethereum-based voting system requires considerable technical expertise, which can be a barrier for some organizations. Scalability: The Ethereum blockchain may experience scalability issues, especially during high transaction volumes, which may affect the performance of the voting system. Transaction costs: Gas fees on Ethereum can fluctuate, leading to potentially high transaction costs during periods of high network activity. Adoption and trust: Users may be reluctant to adopt a new blockchain-based voting system due to a lack of understanding or trust in the technology.
Opportunities	**Threats**
Innovation and leadership: By adopting blockchain for voting, an organization can position itself as an innovative leader in election technology. Market expansion: Blockchain technology can be used for various types of elections and decision-making processes, opening up new market opportunities. Partnerships and collaborations: Collaboration with blockchain experts and technology institutions can strengthen the credibility and capabilities of the voting system. Continuous improvement: The continued evolution of blockchain technology, with updates like Ethereum 2.0, can improve the scalability and performance of the voting system.	Regulations and compliance: Government regulations on blockchain technology and elections can pose legal and compliance challenges. Security from cyberattacks: Although secure, the Ethereum blockchain is not immune to sophisticated cyberattacks, and system security must be constantly updated. Competition: Other e-voting or blockchain technologies could emerge and compete for market share. Public perception: Negative incidents or misperceptions regarding the security or reliability of blockchain can harm the adoption of the voting system.

D. MARKET SIZE & COMPETITORS:

a. Market size:

The global online voting system market size was worth around USD 301 million in 2022 and is predicted to grow to around USD 622 million by 2030 with a compound annual growth rate (CAGR) of roughly 9.5% between 2023 and 2030.

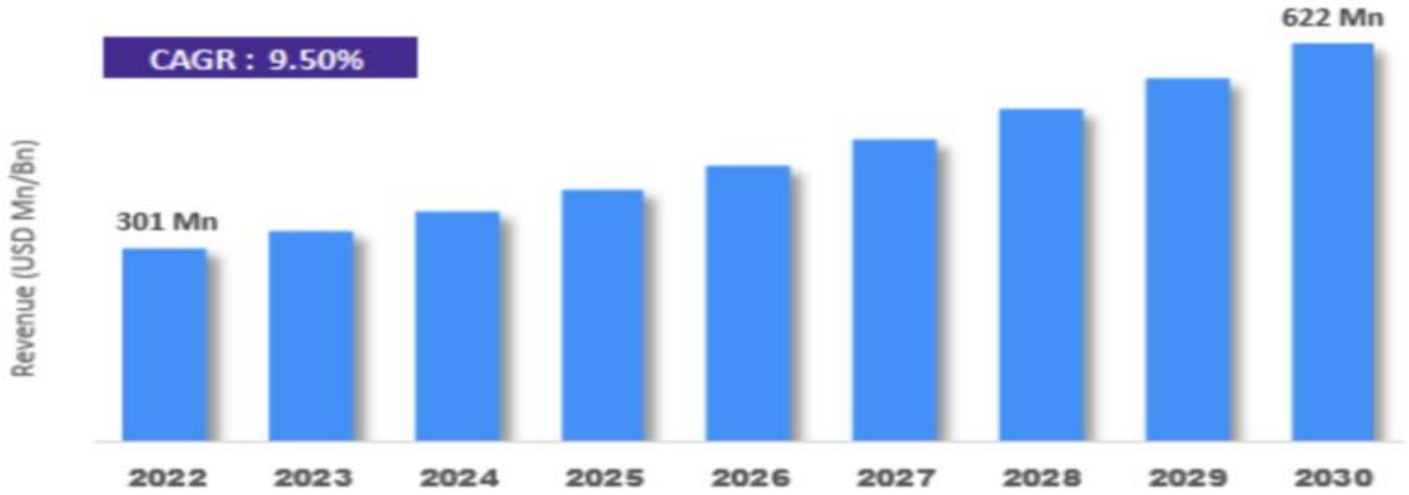

Fig. 1: INSERT DESCRIPTION: The global online voting system market size.

According to the latest research, done by Business Reach insights, the global Blockchain in Voting System market looks promising in the next 5 years. As of 2022, the global voting system market was estimated at 301 USD million, and it's anticipated to reach 622 USD million in 2028, with a CAGR of 9,5% during the forecast years.

b. Competitors:

The Major Key Players Listed in Voting System Market Report are:

- Simply Voting: Specializes in providing secure online voting solutions for elections, referendums, and surveys.
- ELECTION SYSTEMS & Software: Focuses on creating comprehensive election management systems, including voting machines and software for election officials.
- Smartmatic: Provides advanced electronic voting technology and services for elections, including secure voting machines and software.
- Voatz : Specializes in mobile voting solutions, using blockchain technology to ensure secure and accessible voting via smartphones.
- Honest Ballot Association (HBA): Offers a range of election services, including traditional paper ballots, online voting, and election management consulting.
- YesElections : Provides comprehensive election services, including online voting, vote-by-mail, and in-person election management.
- eBallot : Specializes in online voting solutions for organizations and corporations, offering secure and user-friendly voting platforms.

- Dominion Voting Systems: Develops and supplies electronic voting hardware and software, offering a range of voting solutions for government elections.

The above mentioned voting systems are well designed but remain to have a few weaknesses that VoteCrypt platform aims to address. It is important to note that VoteCrypt is a blockchain-based e-voting system, that ensures security and accessibility.... Its unique feature is the ability to customize according to user needs, catering to clients such as governments, businesses, and international organizations, utilizing the Ethereum blockchain, which is secure but requires regular updates to defend against sophisticated cyberattacks, VoteCrypt proactively manages these challenges, as discussed in the following section.

3. TECHNICAL SOLUTION

BLOCKCHAIN AND TECH STACK

The Hedera blockchain was chosen due to its significant transaction processing capabilities. Using Hedera makes the voting process scalable and financially feasible for any election. Hedera's KYC and DID capabilities (flags) could further enhance the voter experience, making it seamless for the end user. While the validator set of Hedera is limited to approved validators (large companies), the access to the blockchain is permissionless. As the companies are domiciled in various nation states across the globe, there is no risk of a specific state influencing or colluding with all companies and therefore the system is decentralized.

The MerkleVoting smart contract was written using Solidity code and deployed on the UZH Ethereum blockchain for simplicity purposes. The smart contract code and the deployment addresses may be found in the appendix of this document. The contract will be deployed to Hedera at some point in the future. The contract utilizes two main structs, a Voter struct and a Candidate struct. The smart contract has an owner that can add candidates and administer the election phases.

ELECTION PROCESS

The election process looks as follows:

1. The contract owner (election committee) deploys the smart contract onto the Hedera blockchain.
2. The contract owner distributes access to wallet addresses to each person eligible to vote, either by mail or directly at the voting booth.
3. The eligible voters will use a user interface where they perform a facial recognition identification to ensure they are eligible. Once done, they receive access to the blockchain address that was sent to them.
4. In the user interface, the merkle proof is generated and once the candidate has been selected, submitted to the smart contract within a transaction. The selected candidate is encrypted with a secret only known to the election committee.
5. After the voting ends, the encrypted votes may be decrypted with the secret (which is published by the election committee.
6. The votes may then be counted by running an event filter on the VoteSubmitted event that was emitted by the smart contract for each vote that was recorded. This is publicly visible and entirely transparent.

MERKLE TREES

By utilizing merkle trees for voter eligibility verification, the smart contract provides for an efficient way of handling large amounts of voter data. Using the setMerkleRoot function, the contract owner can set the merkle root (generated offline) for the merkle proofs to be checked against:

```
function setMerkleRoot(bytes32 _merkleRoot) public onlyOwner {
        merkleRoot = _merkleRoot;
}
```

Fig. 2: setMerkleRoot Function of the Smart Contract

When voting, the voter has to submit the merkle proof (to be generated in the UI backend) together with the candidate number that should receive the vote. The merkle proof is then checked against the merkle root using OpenZeppelin's MerkleProof contract:

```
function vote(bytes32[] memory _merkleProof, bytes memory _encryptedVote) public {
   require(electionActive, "Election is not active");
   require(electionEnd <= block.timestamp, "Election is over");
   require(!voters[msg.sender].voted, "You have already voted");
   bytes32 merkleLeaf = keccak256(abi.encodePacked(msg.sender));
   require(MerkleProof.verify(_merkleProof, merkleRoot, merkleLeaf), "You are not eligible to vote");
   voters[msg.sender].voted = true;
   voters[msg.sender].encryptedVote = _encryptedVote;
   emit VoteSubmitted(msg.sender, _encryptedVote);
   }
```

Fig. 3: vote Function of the Smart Contract

ELECTION PHASES

The smart contract implements three election phases: pre-election, voting and post-election For various functions, there are "require" statements in place to ensure that they may only be called in the appropriate phase (to ensure data integrity). The pre-election phase starts upon deployment of the contract and is used for setting up candidates and eligible voters. At any time, the contract owner may then trigger "startElection(uint256 _electionDuration)" to start the voting phase:

```
function startElection(uint256 _electionDuration) public onlyOwner {
   require(!electionActive);
   require(merkleRoot != 0, "Merkle root is not set");
   require(candidates.length > 0, "No candidates added");
   electionActive = true;
   electionStart = block.timestamp;
   electionDuration = _electionDuration;
   electionEnd = electionStart + _electionDuration;
}
```

Fig. 4: startElection Function of the Smart Contract

Once started, the election will last for the duration (in seconds) that was specified by the owner. Once this time has passed, anybody will be able to call "endElection()" to end the election period and reset the period data:

```
function endElection() public {
   require(block.timestamp >= electionEnd, "Election is still ongoing");
   require(electionActive, "Election has not started");
   electionActive = false;
   electionStart = 0;
   electionDuration = 0;
   electionEnd = 0;
}
```

Fig. 5: endElection Function of the Smart Contract

Once the election has ended, the election results (votes per candidate) can be retrieved by anybody that has the secret key (which needs to be made public by the contract owner) by decrypting all "VoteSubmitted" events that were emitted during the voting phase:

```
event VoteSubmitted(address voter, bytes encryptedVote);
```

Fig. 6: VoteSubmitted Event of the Smart Contract

ELECTION PRIVACY

As the mapping from an address to a voter identity is not present, the voters stay anonymous. Furthermore, with the encryption of the contents of the vote, there is no possibility of having real-time election results before the voting phase is finished, therefore keeping the voting secrecy in place. The "VoteSubmitted" event will provide

clarity on who won the election only after the secret key used for encrypting the votes has been published. The encryption should be handled by the UI in a way that the secret key may not be accessed by the voter but used for encrypting the data.

4. BUSINESS MODEL

VALUE PROPOSITION

Our blockchain-based voting system leverages EVM smart contracts and Hedera for robust security, transparency, and efficiency. We employ advanced technologies, including Merkle trees for hashing voter addresses and two-factor authentication with face ID verification, to deliver a state-of-the-art electoral platform. Below are the core elements of our value proposition:

- **Security and Integrity:** Tamper-proof blockchain with Ethereum smart contracts and Merkle tree hashing for anonymized, immutable votes.
- **Efficiency and Cost Reduction:** Automated processes reduce administrative overhead, human errors, and operational costs, speeding up tallying and reporting.
- **Privacy:** Advanced cryptographic techniques protect voter identities and choices, ensuring confidentiality while maintaining transparent, auditable data.

CUSTOMER SEGMENTS

We've selected these customer segments as our main target market, and we aim to develop a completely customizable smart contract that considers the distinct political and legislative systems of each country/state/organization.

- **Governments and Municipalities**: National and local governments seeking secure and transparent voting solutions.
- **International Organizations**: Entities like the United Nations or the European Union interested in promoting democratic processes in developing regions.
- **Corporations and Associations**: Private sector companies and member organizations need secure voting for shareholder meetings, board elections, and member voting.

REVENUE STREAMS

A. **Licensing Fees:**
   a. Charge governments and institutions annual licensing fees for using the platform.
   b. Offer tiered pricing based on the size and complexity of the elections.

B. **Consulting and Customization Services:**
   c. Provide consulting services to customize and integrate the voting system with existing infrastructure.
   d. Offer premium support and maintenance contracts.

C. **Grants and Subsidies:**
   e. Seek grants from international organizations and non-profits focused on improving democratic processes.
   f. Explore public-private partnerships to fund the deployment in underdeveloped regions.

COST STRUCTURE

A general cost structure for the coming few steps for our startup are:

- **Development and Maintenance**: Costs associated with developing and maintaining the blockchain infrastructure on the Hedera platform.
- **Marketing and Sales**: Expenses for marketing campaigns, sales personnel, and promotional activities.
- **Regulatory Compliance**: Legal and compliance costs to ensure adherence to electoral laws.

MARKETING AND DIRECT SALES GROWTH CHANNELS

- **Direct Sales**: Employ a sales team to engage with potential clients directly.

- **Online Platform**: Maintain an informative and user-friendly website for marketing and client engagement.
- **Conferences and Expos**: Participate in global tech and democracy conferences to showcase the platform.

5. LEGAL ANALYSIS

The blockchain-based voting system has the unique advantage of transparency and efficiency. However, implementing blockchain-based voting systems requires a thorough legal analysis to address critical issues of data privacy and protection, security, and integrity.

DATA PRIVACY AND PROTECTION

EXISTING DATA PROTECTION LAWS REQUIREMENTS

- **General Data Protection Regulation (GDPR) - European Union:** Requires strict protection of personal data, mandating transparency, consent, data minimization, and the right to be forgotten.
- **California Consumer Privacy Act (CCPA) - United States (California):** Emphasizes consumer's rights regarding access to personal information, the right to delete data, and the right to opt-out of data sales.

LEGAL ANALYSIS

- **Anonymization**: Our systems ensure that voter identities are anonymized as the distribution of private keys and addresses are randomized so that no one can tell one another.
- **Data Minimization and Modification**: Only essential voter information like private keys and their vote can be collected and processed. However, Blockchain's immutability makes compliance with data rectification regulations difficult.
- **Data Security**: Before the result is announced, the whole system is encrypted, only limited access is provided to the election authorities. Unauthorized data access or breaches are not possible, aligning with GDPR and CCPA requirements. However, all data (shows only distributed randomized private keys) will be open to the public once the election is finished.

ELECTION SECURITY AND INTEGRITY

ELECTION SECURITY STANDARDS AND LEGAL REQUIREMENTS

- **Federal Election Commission (FEC)- United States**
  Provide comprehensive guidelines on maintaining the electoral process's integrity, transparency, and security, including implementing cybersecurity measures to protect Post-Election Audits.

LEGAL ANALYSIS

- **Cryptographic Safeguards and Resilience**:
  The blockchain-based voting system is great at resilience through decentralized consensus mechanisms, making it difficult for a single entity to alter the voting data. Which perfectly meets the legal standards requirements of the system to be resilient against hacking, fraud, and tampering.
- **Auditability**: Our system allows for an immutable audit trail, which can be used to verify the integrity of the election process. All details of the vote can be open to the public after the voting phase ensuring the auditability of the whole election.

Our blockchain-based voting system has significant advantages in security, transparency, and auditability. However, it must navigate complex legal landscapes concerning data privacy, and security. Current legal frameworks will also need to evolve to address the unique challenges posed by blockchain technology, ensuring that these systems can be legally and effectively integrated into the electoral process.

6. CONCLUSIONS

VoteCrypt voting system has the unique advantage of transparency and efficiency by leveraging on blockchain technology that provides for an efficient way of handling large amounts of voter data. Using the setMerkleRoot function, the contract owner can set the merkle root (generated offline) for the merkle proofs to be checked against. When voting, the voter must submit the merkle proof (to be generated in the UI backend) together with the candidate number that should receive the vote. The merkle proof is then checked against the merkle root

using OpenZeppelin's MerkleProof contract. The business model of the blockchain-based voting system leverages EVM smart contracts and Hedera for robust security, transparency, and efficiency. We employ advanced technologies, including Merkle trees for hashing voter addresses and two-factor authentication with face ID verification, to deliver a state-of-the-art electoral platform. The core elements of our value proposition include; security & integrity, transparency, efficiency & cost reduction, privacy, trust & accountability. The revenue streams for the project would be from licensing fee, consultations & customization, data analytics & SaaS Model for smaller elections.

7. AUTHOR CONTRIBUTIONS

All authors conceived and designed the project idea. Anurag Moyde and Loubna Ezakani developed and wrote the business model and performed the market analysis. Quan Sirui worked on the regulatory implications. Felix Ritzi and Francis Waweru developed the technical implementation and wrote the technical section. Felix Ritzi wrote the critical overview of the platform selected. All authors revised and accepted the final version of this document.

8. REFERENCES

- https://www.researchnester.com/fr/reports/voting-system-market/2518
- https://www.zionmarketresearch.com/report/online-voting-system-market
- https://www.linkedin.com/pulse/blockchain-voting-system-market-dynamics-mxbnf/
- https://www.alyra.fr/post/election-vote-et-blockchain
- https://chaum.com/votexx/
- Electronics | Free Full-Text | Blockchain-Based E-Voting Systems: A Technology Review (mdpi.com)
- https://gdpr-info.eu/
- https://oag.ca.gov/privacy/ccpa

9. APPENDICES

APPENDIX A: SMART CONTRACT CODE

The source code of the MerkleVoting smart contract is available on GitHub:

https://github.com/xdecentralix/votecrypt