

DVO: A DECENTRALIZED VOTING SYSTEM

Olorunfemi Tayo

OT@ymx.com

ABSTRACT: DVO proposes a decentralized voting system leveraging blockchain technology and cryptography to enhance trust, transparency, and inclusivity in electoral processes. By integrating off-chain authentication and blockchain immutability, DVO prevents double voting and manipulation while ensuring user privacy and data security. The paper discusses adoption strategies, regulatory compliance, and security measures, highlighting DVO's potential to redefine electoral trust and promote decentralized decision-making for a more democratic society.

1. INTRODUCTION

Over the years, democracy has emerged as a cornerstone of governance, resonating across liberal and non-liberal societies worldwide. It's intricately woven into the fabric of political systems, defining the landscape of nations and shaping the aspirations of communities. Political systems are the set of formal legal instructions that constitutes a government. The most important type of political systems in the modern world is the nation-state (a territorial bounded sovereign polity i.e a state that is ruled in the name of a community of citizen who identify themselves as a nation). The world today is divided territorially into more than 190 countries, in which a nations government claims to exercise sovereignty or the power of final authority [1].

The economist group which publishes the democracy index (an index measuring the quality of democracy [2] across the world), categorizes each country into one of four regime types:

- 1) full democracies [3],
- 2) flawed democracies [4] ,
- 3) hybrid regimes, [5]
- 4) authoritarian regimes [6].











The democracy index produces a weighted average based on 60 questions, these questions are grouped into five categories

- 1) electoral process and pluralism
- 2) civil liberties
- 3) functioning government
- 4) political participation
- 5) political culture.

Likewise, there are a few questions considered so important:

- 1) whether elections are free and fair
- 2) the security of voters
- 3) the influence of foreign powers on government
- 4) the capabilities of civil servants to implement policies

The table below shows the number of nations and the percentage of World population for each type of regime as at year 2022:

Type of regime ↕	Score ↕	Countries		Proportion of World population (%) ↕
		Number ↕	(%) ↕	
Full democracies	 9.01–10.00	24	14.4%	8.0%
	 8.01–9.00			
Flawed democracies	 7.01–8.00	48	28.7%	37.3%
	 6.01–7.00			
Hybrid regimes	 5.01–6.00	36	21.6%	17.9%
	 4.01–5.00			
Authoritarian regimes	 3.01–4.00	59	35.3%	36.9%
	 2.01–3.00			
	 1.01–2.00			
	 0.00–1.00			

source: https://en.wikipedia.org/wiki/The_Economist_Democracy_Index

According to the data provided, flawed democracies accounted for 37.3% of the world's population in the year 2022. This indicates that a significant portion of the global population lived in countries that have significant faults due to poor political culture, low levels of participation in politics, and issues in the functioning of governance while on the other hybrid regimes, the data indicates that they accounted for 17.9% of the world's population in 2022. This means that a sizable portion of the

global population lived in countries where political systems exhibited regular electoral frauds preventing them from being fair and free democracies [7]. While the democracy index has experienced criticism, it underlines a flaw on the concept of democracy and factors responsible for it.

2. THE BLOCKCHAIN

According to IBM, the Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved [8].

Since the inception of the blockchain technology in 2009 by Satoshi Nakamoto we've seen the technology cut through various industries like finance, medicine, supply systems etc. A key feature of the blockchain is its transparency and data immutability which enables trust in a trust-less system, meaning its transparency ensures that actions carried out on it can be seen and verified by the general public (i.e we can verify that a particular action was carried out by a given user (*an address*) at a given time (*block time*)), in reality only the owner (*the signer*) of an account is able to carry out actions (*read and write functions*) on his/her account due to the decentralized nature of the blockchain although the identity of the user is anonymous to the public. Implementing the blockchain technology into traditional governance is one that is not root deep in society but its transparent and immutable nature instills trust in a trustless environment, as the words of the former and great American president Abraham Lincoln echoes: "*GOVERNMENT FOR THE PEOPLE AND BY THE PEOPLE*", the blockchain has the potential to empower citizens truly.

Citizens voting power can be retained and made immutable through the use of cryptography, and vote count can be easily verified and queried publicly in a decentralized manner, this in essence terminates the fear of vote count manipulations. However since the election of a particular candidate requires the use of off-chains data like a user voting-id it question how solid this method of approach can be.

3. DVO

One of the fundamental challenges of blockchain technology is its limited access to external, real-world data. Blockchain Oracles provide a way for the decentralized Web3 ecosystem to access existing data sources, legacy systems, and advanced computations [9]. Blockchain Oracles address this limitation by sourcing data from decentralized and centralized data providers, aggregating information from multiple sources to ensure reliability, accuracy, and resilience. This decentralization of data sources helps mitigate the risk of single points of failure and manipulation, enhancing the overall decentralization of blockchain applications. While oracles serve as a source for off-chain data, the accuracy and reliability of data provided by oracles depend on the quality and trustworthiness of the data sources. This therefore means that data like users' vote IDs and biometrics must be verified to ensure that only authorized users can participate in the voting process; this verification involves fetching data from a centralized entity, while using a blockchain oracle looks like the next possible option. Integrating blockchain oracles into decentralized applications can incur additional costs in terms of transaction fees, oracle fees, and operational overhead. Furthermore, as blockchain networks scale and process larger volumes of data, the cost and complexity of oracle operations may increase, posing scalability challenges for oracle networks and smart contract execution.

This system of retaining users' voting power is therefore a partly-decentralized solution where users' votes are stored on an immutable ledger and vote counts and other details associated to a user's public-key (address) can be queried on the blockchain, however other data like a user's vote ID can be persisted on a centralized database with optimal security and verified from external centralized entities, removing the task and cost of implementing a blockchain oracle.

User data can be persisted on a centralized database while the actual voting data is stored (and can be queried) on the blockchain publicly by anyone. Effectively, we can tie every user to a specific address on-chain, ensuring that users can't cast multiple votes. Once the data linking is confirmed, a user can then proceed to vote with his/her connected account. A step-by-step procedure is shown below:

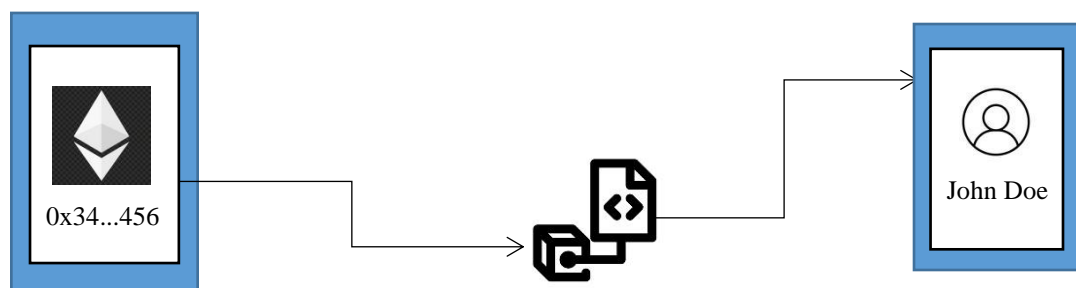
STEP 1: OFF-CHAIN AUTHENTICATION

Users must go through an off-chain verification process that proves their identity and eligibility as members of the specified voting group or institution in order to maintain secure access. Users provide identifying information (such as a government-issued ID, student ID, or membership ID) during the enrollment process, and it is compared to a safe, authorized database. This method provides a high level of trust and helps ensure only authorized individuals participate in the voting process.

Users' profiles are connected to their voter registration data after successful authentication, establishing a validated identity that will be utilized when voting takes place. By guaranteeing that only verified, qualified users may access the platform and cast votes, this off-chain verification is a crucial step in maintaining the integrity of the voting process.

STEP 2: SYNCHRONIZE USER VOTER ID TO A WALLET ADDRESS

This involves the authentication of a user's wallet account with their voter ID. To ensure security and integrity, robust authentication mechanisms such as cryptographic hashing and digital signatures is employed and the use of smart contracts on the blockchain can automate the synchronization process, ensuring accuracy and reliability.



STEP 3: OWNERSHIP VERIFICATION

Ownership verification is crucial for ensuring the authenticity of voters and preventing fraudulent activities such as identity theft or voter impersonation. Cryptographic techniques such as digital signatures is a method used to prove ownership of a wallet address, providing a secure and tamper-proof method of authentication

STEP 4: VOTE

Once ownership is verified, users can then proceed to cast their votes using their synchronized wallet addresses. Each vote is recorded on the blockchain, ensuring transparency and immutability. The scope is to use smart contracts to enforce rules such as one-person-one-vote and prevent double voting or tampering with the voting process. This further enables decentralized decision-making by empowering citizens to directly participate in the governance process. Combining biometric authentication with transparent and secure voting mechanisms, the voting process promotes democratic principles of inclusivity, fairness, and equality. Citizens can directly participate in governance processes with confidence, knowing that their votes are securely recorded and recorded on the blockchain.

STEP 5: RESULTS

Results from the voting system are readily accessible and transparent, thanks to the inherent nature of blockchain technology. The blockchain ensures that all voting transactions are securely recorded and publicly available for scrutiny. Users can query the blockchain at any time, from anywhere, to obtain real-time updates on voting results without relying on intermediaries or centralized authorities. This transparency fosters trust and confidence in the electoral process, as citizens can independently verify the integrity of the results. By providing a decentralized and auditable record of votes, this medium empowers citizens to actively engage in the governance process and ensures that their voices are accurately represented.

4. CONSIDERATIONS

Adoption and User Education

The success of every technological attempt still boils down to adoption and progressive development. The lifespan of bitcoin tells it all, since the inception of bitcoin in 2009 we've seen the emergence of various cryptocurrencies pushing forward the blockchain technology and the future of decentralization. The truth remains that not everyone will immediately accept a disruptive idea despite its obvious benefit. The Diffusion of innovations is a theory that seeks to explain how, why, and at what rate new ideas and technology spread [10]. The success of this concept relies heavily on widespread adoption by the voting population. Therefore, effective user

education and outreach programs must be implemented to familiarize voters with the new voting system and its benefits. This may include conducting awareness campaigns, providing training sessions, and distributing informational materials to ensure that voters understand how to use the system and trust its integrity.

Regulatory Compliance

To gain acceptance and legitimacy, complying with existing electoral laws and regulations is of much importance in each jurisdiction where it is deployed. Collaborating with election authorities and policymakers to ensure that legal requirements and standards for voting integrity, privacy protection, and accessibility is met. This may involve obtaining regulatory approvals, certifications, or endorsements from relevant government agencies.

Security and Privacy Measures

Protecting the security and privacy of voter data is paramount in any voting system. Implementing robust security measures, such as encryption, multi-factor authentication to safeguard against cyber threats, data breaches, and unauthorized access. Additionally, privacy-preserving technologies, such as zero-knowledge proofs or differential privacy, can help protect voter anonymity and confidentiality while still ensuring the integrity of the voting process.

5. CONCLUSION

In conclusion, we have proposed DVO, a decentralized voting system that redefines the concept of trust in electoral processes. Building upon the foundation of blockchain technology and cryptographic principles, DVO ensures strong control of voter ownership while addressing the critical challenge of preventing double voting. By leveraging a peer-to-peer network and employing biometric authentication, DVO establishes a transparent and secure public ledger of votes that is resistant to tampering and manipulation.

Similar to the robustness of blockchain networks, DVO operates with unstructured simplicity, this decentralized approach not only enhances the integrity of the voting process but also fosters inclusivity and accessibility, allowing citizens to directly

participate in governance with confidence. In essence, DVO represents a paradigm shift in electoral systems, offering a path towards a more democratic and participatory society. As we navigate the complexities of modern governance, DVO stands as a beacon of innovation, ushering in a new era of trustless and decentralized decision-making for the benefit of all.

REFERENCES

1. <https://www.britannica.com/topic/political-system/The-structure-of-government>
2. <https://en.wikipedia.org/wiki/Democracy>
3. https://en.wikipedia.org/wiki/Liberal_democracy
4. https://en.wikipedia.org/wiki/Illiberal_democracy
5. https://en.wikipedia.org/wiki/Hybrid_regime
6. https://en.wikipedia.org/wiki/Authoritarian_regimes
7. <http://www.yabiladi.com/img/content/EIU-Democracy-Index-2015.pdf>
8. <https://www.ibm.com/topics/blockchain>
9. <https://chain.link/education/blockchain-oracles>
10. https://en.wikipedia.org/wiki/Diffusion_of_innovations#CITEREFRogers1962_5th_ed