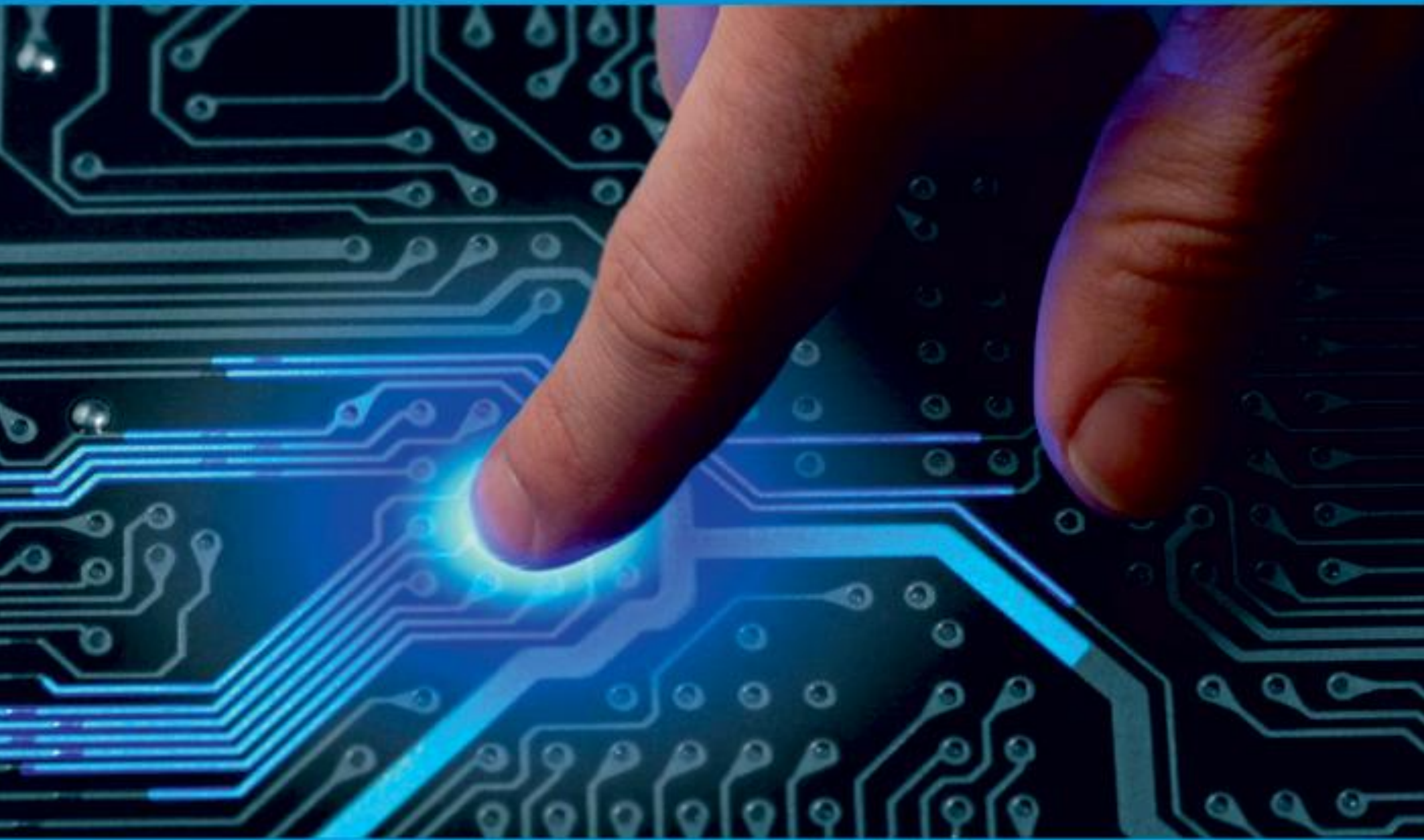
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 5, May 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105257 |

Online Electrol System Using Blockchain Technology With Machine Learning

Bhushan Nagare[1], Kartik Bhusal[2] ,Sanket Chaudhari[3] , Siddharth Dhokchaule[4] , Kiran Kharde[5]

UG Student, Dept. of I.T., PREC, SPPU University, Maharashtra , India

Assistant Professor, Dept. of I.T., PREC, SPPU University, Maharashtra , India

ABSTRACT: An electronic voting system that faithfully replicates real-world systems has been a longstanding aspiration. However, until recently, it was a challenge to fully address all the essential properties of a genuine voting scheme simultaneously. Fortunately, advancements in technology and research have ushered in a new era where not only can these crucial properties be effectively fulfilled, but also the anonymity and convenience of voting can be enhanced.In this work and presented in this dissertation, a decentralized and self-tallying electronic voting protocol has been developed, which significantly improves the privacy of voters and reduces centralization. This achievement is made possible through a synergistic relationship between the Ethereum Blockchain and the Portuguese electronic ID.
Distinguishing itself from previously proposed Blockchain e-voting protocols, this implementation stands out as the first one that closely aligns with most of the security requirements of a real-world voting scheme. Moreover, it surpasses existing e-Voting systems by incorporating a self-tallying protocol. As a result, each voting citizen retains the ability to compute the tally of the election and maintains complete control over their own vote. The execution of this protocol is enforced through the consensus mechanism, which ensures the integrity of the Ethereum Blockchain.

KEYWORDS: Blockchain, E-Voting, Face Recognition, Machine Learning.

I. INTRODUCTION

The motivation behind this project stems from the realization that electoral systems are governed by a set of rules that dictate how elections are conducted and their outcomes determined. These rules encompass various aspects of the voting process, including the timing of elections, eligibility criteria for voters and candidates, ballot labeling and casting procedures, vote counting methods, and result dissemination. For instance, in a traditional voting system, an eligible individual visits their designated polling location, presents their identification card to a polling agent, and receives a ballot paper featuring a list of candidates. The individual then proceeds to a private area, where they mark their chosen candidate(s) with a check mark. The completed ballot is then deposited into a ballot box and later counted by designated personnel. Finally, the aggregated results are announced by the government, making them accessible to the public.

The desire for an electronic voting system that faithfully emulates real-world systems has long been recognized. However, until now, it has been challenging to simultaneously address all the essential properties of a genuine voting scheme. These properties include security, anonymity, coercion resistance, and untraceability, among others. However, recent advancements in technology and research have made it not only feasible to meet these requirements but also to enhance the anonymity and convenience of the voting process. One promising technology that embodies these capabilities is the Ethereum Blockchain, which boasts the following characteristics:

Practical immutability: Modifying information on the blockchain would necessitate an impractical amount of computing power.**Transparency:** The data recorded on the blockchain is accessible to anyone.**Decentralization**: The absence of a central authority ensures the decentralized nature of the blockchain.Smart contracts and DApps: The Ethereum Blockchain facilitates the creation of intelligent contracts and decentralized applications..This Master's project aims to offer an elegant solution to electronic voting that harnesses the strengths of electronic identification systems in conjunction with the potential of blockchain technology. By doing so, it strives to minimize the reliance on centralization, a significant vulnerability of democratic systems. The project falls within the domains of computer security, digital transformation, and system design. According to the 2012 version of the ACM Computing Classification System, widely regarded as a de facto standard in computer science, the scope of this Master's project can be categorized as follows:

Applied Computing: Voting/election technologies
Security and Privacy: Usability in security and privacy

II. METHODOLOGY

The reason for using a private blockchain is that it’s inexpensive and a bit faster than a public. In addition, it does not pollute the public blockchain with raw data because it was designed to be used only for a digital currency, not for data storage, and it also holds the record of our desired transactions in a separate and filtered form, which can provide a great deal of assistance when auditing the voting system. Whereas, on the other hand, the public blockchain is used to share the root hash given by the Merkle tree to ensure the integrity of the data and distribute the final results of each polling station so that it is freely accessible to everyone. The project's primary goal is to find a way to increase voter participation in local, state, and national elections. As a result, we're working to create a voting system that allows people to cast their ballots from a distance, with their previously recorded picture face serving as proof of identity.

The system model for our proposed e-voting scheme.. It can be observed that the system contains multiple E-voting stations that are connected to the public blockchain. Other than that, we have a database that stores the citizen ’s record for the entire city to decide whether or not an elector is eligible to cast a vote at a particular polling station. In each E-voting station, we have servers (which can access data from the primary database if required), voters and voting machines. In our system, we use the concept of both public and private blockchain.The reason for using a private blockchain is that it’s inexpensive and a bit faster than the public. In addition, it does not pollute the public blockchain with raw data because it was designed to be used only for a digital currency, not for data storage, and it also holds the record of our desired transactions in a separate and filtered form, which can provide a great deal of assistance when auditing the voting system. Whereas, on the other hand, the public blockchain is used to share the root hash given by the Merkle tree in order to ensure the integrity of the data and distribute the final results of each polling station so that it is freely accessible to everyone. There are a few steps in our system to vote; first, an elector sends a request for registration to his / her corresponding E-voting station by submitting some personal information , e.g. name, CNIC, father’s name, place of birth and date of birth. When the registration server receives the information, it hashes the data and then requests the primary data center to provide the correspondence to the requested user. If hashes get the match , the elector must register and be entitled to cast a ballot on the election day. Until we delve deeply into the proposed methodology, we need to identify the design criteria for Evoting.

III. BACKGROUND AND RELATED WORKS

This chapter provides essential background information that serves as the foundation for this Master's project. It begins with a discussion on smart contracts and their association with Ethereum. Additionally, it introduces a thought experiment related to Zero Knowledge Proofs (ZKPs) in the context of this project. The chapter also explores the current state of electronic voting and its challenges.

Background: Smart Contracts and Ethereum:-In this section, the concept of smart contracts is introduced and its relationship with the Ethereum blockchain is explained. Smart contracts are self-executing agreements with predefined conditions and actions encoded within them. Ethereum, a decentralized blockchain platform, enables the execution of smart contracts and facilitates the development of decentralized applications (Dapps). The section provides an overview of how smart contracts function and their significance in the context of this research.

Current State of Electronic Voting:-This section focuses on the current state of electronic voting and the dilemmas associated with it. It examines the challenges faced by traditional voting systems and explores the potential benefits and drawbacks of electronic voting. The section delves into issues such as security, privacy, trust, and transparency in electronic voting systems. It also reviews existing electronic voting schemes and highlights their strengths and limitations.By exploring these topics in the background section, the reader gains a comprehensive understanding of the underlying technologies, namely smart contracts and Ethereum, and the current landscape of electronic voting. This knowledge sets the stage for the subsequent chapters, where the proposed electronic voting system and its implementation details willbe discussed.

IV. WORKING OF BLOCKCHAIN

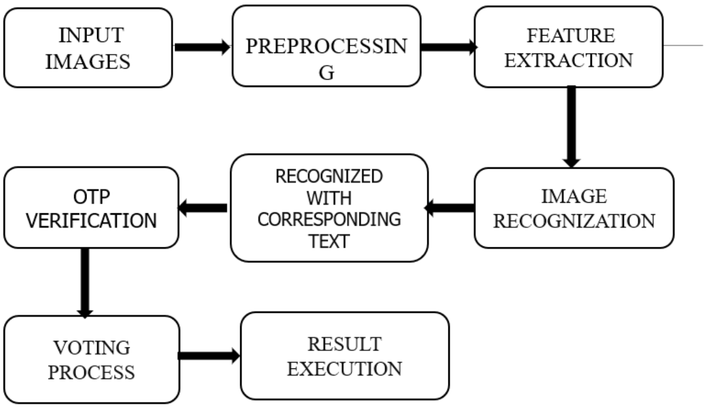
Voting System Registration process of voters and candidates is to be done in advance. Identity verification should be done before creating accounts. After identity verification, authorized person should authenticate eligible users by proving a coin or token. Using this coin or token each user can vote only once. Blockchain’s verification process will ensure that double spending of this token is not possible. So any user cannot vote multiple times. The e-voting system based on blockchain is decentralized. There is no central authority to conduct the elections.

Cryptography: is used to preserve privacy and transparency at the same time, economic incentives are used to encourage desired behaviour of network actors who do not trust or know each other, nor have any legally binding agreements with each other. Cryptography is the practice and study of techniques for secure communication in the presence of third parties. Cryptography literature often uses the name Alice "A" for the sender, Bob "B" for the intended recipient, and Eve "Eavesdropper" for the adversary. There are two kinds of cryptosystems: symmetric and asymmetric.

1. **Symmetric Cryptography**: Two parties agree on a secret key (private key) and use the same key for encryption and decryption. The problem with this approach is that this method does not scale. If you wanted to communicate privately with somebody you would need to physically meet and agree on a secret key. In the world of modern communications, where we need to coordinate with many actors, such methods would not be feasible. Furthermore. Data manipulation in symmetric systems is faster than asymmetric systems as they generally use shorter key lengths. On the other hand, encrypting files and messages with asymmetric algorithms might not always be practical. The main reason is performance. Symmetric key cryptography is much faster and handles better the encryption of big files and databases, therefore, is still widely used.

2.Asymmetric Cryptography (Public Key Cryptography): Asymmetric systems use a public key to encrypt a message and a private key to decrypt it. Use of asymmetric systems enhances the security of communication. Private keys should be kept secret and a public key could be freely distributed between parties. In an asymmetric encryption scenario, two parties would distribute their public keys and allow anyone to encrypt messages using their public keys. Because of how a key pair mathematically works it is impossible to decrypt a message which got encrypted with a public key.

E-voting System: E-voting currently widely used by some countries in the world, for example in Estonia. The country has been using the e-voting system since 2005 and in 2007 conducted online voting and was the first country in the world to conduct online voting. Since then, a legally binding online voting system has been implemented in various other organizations and countries such as the Austrian Federation of Students, Switzerland, the Netherlands, Norway, and so on . But it still has considerable security issues and the selection is often cancel.. Although getting a lot of attention, online voting system is still not widely done in various countries around the world. The traditional voting system has several problems encountered when managed by an organization that has full control over the system and database, therefore the organization can tamper with the database, and when the database changes the traces can be easily eliminated. The solution is to make the database public, the database owned by many users, which is useful to compare if there are any discrepancies. The solution to the e-voting system is compatible with using blockchain technology. Blockchain technology allows in support of e-voting applications. Each voter's vote serves as a transaction that can be created into blockchain that can work to track voice counting. In this way, everyone can approve the final calculation because of the open blockchain audit trail, the vote count can be verified that no data is altered or deleted nor is there any unauthorized data entered in the blockchain.



V. Conclusion and Future Work

In this paper, the principles of blockchain and machine learning to provide protection and integrity to the voting system are proposed to create a stable and efficient E-voting system architecture. This proposed system not only deals with the integrity of votes but also secures citizens' data as an E-voting station network. We used two machine learning models with different sets of settings. A comparison is made between these two classifiers by measuring their accuracy and AUC (area under the curve).ThisdissertationhaspresentedaBlockchaine-votingsystemthatsignificantlyimproves current schemes by making use of government-issued to authenticatecitizens and verify their eligibility to vote. The voting protocol used allows for E2Eauditability and maximum voter privacydue to the usage of zero-knowledge proofs andits execution being safeguarded by the same consensus mechanism that protects theEthereum Blockchain. Furthermore, and by virtue of the immutability of the Ethereum Blockchain, anyone can verify thattherulesoftheprotocolareenforcedjustly. The idea of a smart contract is used to register voters and to receive votes as well. Where the Merkle root algorithm has been used to get the root hash to ensure the integrity of the data stored at the citizen's data center. We believe that this voting architecture can be extended as an I (internet voting). where users can vote through a secure application or secure web servers. blockchain as a network as well as the database for storing voter's accounts, candidate details, and votes. It shows that blockchain technology can overcome limitations of centralized voting systems. In future work, the feasibility of blockchain based e-voting system for large-scale election should be analyzed.

References

[1] Francesco Restuccia, Salvatore D'Oro, Salil S. Kanhere, Tommaso Melodia, and Sajal K. Das, "Blockchain for the Internet of Things: Present and Future," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 1-8, January 2018.

[2] Yiyun Zhou, Meng Han, Liyuan Liu, and Wang Yan, "Improving IoT Services in Smart-Home Using Blockchain Smart Contract," in IEEE Confs. on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics, pp. 81-87, 2018.

[3] Nir Kshetri and Jeffrey Voas, "Blockchain-Enabled E-Voting," IEEE Software, pp. 95-99, 2018.

[4] Friorik P. Hjalmarsson, Gunnlaugur K. Hreioarsson, Mohammad Hamdaqa, and GisliHjalmtysson, "Blockchain-Based E-Voting System," in IEEE 11th International Conference on Cloud Computing, pp. 983-986, 2018.

[5] Bayu Adhi Tama, Bruno Joachim Kweka, Youngho Park, and Kyung-Hyune Rhee, "A Critical Review of Blockchain and Its Current Applications," in IEEE International Conference on Electrical Engineering and Computer Science (ICECOS) 2017, pp. 109-113, 2017.

[6] M. Hochstein, "Moscow's Blockchain Voting Platform Adds Service for High-Rise Neighbors," CoinDesk, 15 Mar. 2018; https://www.coindesk.com/moscows-blockchain-voting-platformadds-service-for-high-rise-neighbors, 2018.

[7] M.D. Castillo, "Russia Is Leading the Push for Blockchain Democracy," CoinDesk, 2018; https://www .coindesk.com/russiascapital -leading-charge-blockchain–democracy, 2018.

[8] "South Korea Uses Blockchain Technology for Elections," KryptoMoney, https://kryptomoney.com/south-korea-usesblockchain-technology-for-elections, 2017.

[9] Andrew Barnes, Christopher Brake and Thomas Perry, "Digital Voting with the use of Blockchain Technology", https://www.economist.com/sites/default/files/plymouth.pdf, 2016.

[10] Agora: Bringing our voting systems into the 21st century Available at: https://agora.vote/Agora_Whitepaper_v0.1.pdf, 2017

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.379

doi crossref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

Scan to save the contact details

www.ijircce.com