2022 2nd International Conference on Intelligent Technologies (CONIT)
Karnataka, India. June 24-26, 2022

Utilization of Blockchain in E-Voting System

G.Pranitha
Dept. of CSE
Koneru Lakshmaiah Education Foundation,
Guntur, AP
pranithagummadi@gmail.com

T. Rukmini
Dept. of CSE
Koneru Lakshmaiah Education Foundation ,
Guntur, AP
rukminithummallapalli@gmail.com

T. N. Shankar
Dept. of CSE
Koneru Lakshmaiah Education Foundation
Vaddeswaram, Guntur, AP
tnshankar2004@kluniversity,in

Basant Sah
Dept. of CSE
Koneru Lakshmaiah Education Foundation,
Guntur, AP
basantbitmtech2008@kluniversity.in

Naween Kumar
Dept. of CSE
Koneru Lakshmaiah Education Foundation,
Guntur, AP
naween@kluniversity.in

Sasmita Padhy
School. of Computing Science and Engg, VIT
Bhopal University, MP
sasmita.padhy@vitbhopal.ac.in

***Abstract*-This paper is based on a voting system that's widely used in elections known as electronic voting machines and has the potential to conduct the process securely by blockchain technology. The prime aim of this system for ensuring security, integrity as well as transparency. Voter privacy is one of the prime factors in the electronic voting portal that presents a blockchain-based voting system to overcome several drawbacks of current voting methods by proposing a simple, reliable, fast and inexpensive e-voting system. The election data can be arranged in a chain with several blocks with the best security level for this process that employs for any election to ensure flawless counting.**

Keywords - EVM, E-Voting, Blockchain, Hashing algorithm, Winner, Authentication

I. INTRODUCTION

Electronic voting machines cannot provide the same level of security and integrity as internet-based voting systems [1]-[5]. It also safeguards the users by storing the mandate of eligible voters in a designated pattern. It encourages the voters to confirm their choice through electronic web-based gadgets by referring to an open system. Blockchain is a decentralized peer-to-peer(P2P) network. The prime goal of blockchain is to prevent third-party access over the network that was introduced for the bitcoin with the various levels of safety measures and is transformed as the industry for the extensive use [2]. Often, the paper-based electoral system is manipulation prone, because fraudulent ballot papers can be used to cast the mandate. It is quite impossible for anyone to refer the malpractice through the electronic voting machine (EVM) that can ensure a flawless process by pressing electronic the buttons. Any unexpected tampering can be possible by the techies in favor of impersonating candidates by breaching the security policies that affect the entire system with a declaration of fraud. Customarily, the database is managed by a single entity or central authority that has complete control over it and can modify the desire with direct interference.

The authority that maintains the database is usually the same as that produced one and can be used for data preservation of the respective organization that is intended to thwart the misinterpretation or manipulation of its own statistics. On the other hand, permission to the group of exclusive owners of the database such as voting is perilous by creating many odds. In this regard, the company cannot insure against the fraudulent changes [6]-[10]. With the recent advancement, blockchain is one of the most secure, highly reliable, and prompt alternatives to conventional voting in the establishment of a strong blockchain-based voting system, by addressing multiple issues. The first component of such a system is citizens whose intervention is strictly prohibited for the free and fair election [12]-[20].

Online elections with electronic voting systems can assist in making important decisions by collecting the input of several groups in a systematic and verifiable manner. Internet voting is commonly used by corporations and organizations to elect official leaders and board members.

Using a blockchain voting system can be advantageous in the following aspects:

Choose the leaders: For instance, the board of directors' election in several chairs can be conducted in a fair manner. The listed positions must be available with all the information during the election to the participant employees for selection of their favourite one.

Accept new members into your group: This helps you maintain a consistent, fair assessment process and provides candidates an idea of what to expect.

Vote on yearly budgets: Budget optimization is one of the prime ambitions in the online voting system that can handle the entire system with limited options.

Above all, an online voting system can allow users to make better and justifiable firm decisions in the selection of the best candidate.

II. AUTHENTICATION

There are several strategies for voter verification where authentication must be done by using cryptographic private keys that provide accessibility to the voters in an election process. Voters must be registered by an authority, while voter registration keys must be generated and distributed to voters on hand. It's a difficult task to verify and authenticate the voters based on the specified conditions. Biometric solutions such as face comparisons, fingerprints, irises, and retinal scans have been used in some research, but they are flawed and easily regenerated or stolen. However, we believe that using complicated algorithms that are difficult to crack is one way to protect stolen biometric data [5]-[7]. You can hash the biometric data instead of recording it as binary data and store it as a reference string using any hashing method. During the validation and identification process, the sample model must be transformed to a hash value before being compared to the reference value.

2022 International Conference on Intelligent Technologies (CONIT) | 978-1-6654-8407-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/CONIT55038.2022.9847995

Authorized licensed use limited to: ULAKBIM UASL - DOKUZ EYLUL UNIVERSITESI. Downloaded on November 08,2022 at 05:42:05 UTC from IEEE Xplore. Restrictions apply.

III. BLOCKCHAIN AND EVM

Blockchain technology is a peer-to-peer network of nodes that tracks public transaction data, also known as blocks, in several databases, also known as the "chain." This sort of storage is also known as a 'digital ledger.' The transactions that are exposed as part of the blockchain network's normal operation cannot be modified. A blockchain has several benefits that make it a reliable and secure database alternative:

Decentralization: In a traditional centralized transaction system, every transaction must be affirmed by a trusted central entity. As a result, decentralization necessitates trust, which is the most pressing issue, as well as increased resilience, availability, and failover, which the decentralized peer-to-peer blockchain infrastructure may be ideally adapted for.

Persistence: Blockchain provides the framework for measuring truth and allowing both producers and consumers to show their data is authentic and not manipulated. **Anonymity**: Blockchain networks can be connected using the unique address generation called Pseudorandom addresses. To protect his identity, a user in a Blockchain network can have multiple addresses. As blockchain is not a centralized technology the data cannot access or modified by anyone.

Auditability: The digital distributed ledger of the blockchain network consists of each and every transaction that is connected with each other. Because of this, previous records can be audited and traced using any network node.

IV. ETHEREUM

Ethereum is managed and tracked using a decentralized computer network, or distributed ledger, known as a blockchain. It's helpful to think of a blockchain as a continuous record of all cryptocurrency transactions. As smart contracts are used only when the specific conditions are satisfied and it works based on a particular distributed manner. Blockchain Ethereum is one of the most widely used technology as it developed on smart contracts. When code is requested, a peer-to-peer network of nodes that are mutually distrustful of one another keeps track of the global state and executes it. The data is stored in a blockchain, which is secured by a proof-of-work consensus method like that used by Bitcoin. The main selling point of Ethereum is that it is a full-featured programming language capable of creating complex business logic [21]-[25].

V. SMART CONTRACTS

Smart contracts are basically programs that run once predetermined conditions are met and are stored on a blockchain. They're built on the blockchain, which means they're stored in a public database and can't be altered. A smart contract is a work based on the specific conditions written in the programs, which are executed when the conditions are satisfied and these are processed without the help of any third-party users as once it is recorded will not be able to modify.

With the advent of smart contracts, two or more parties can now exchange blockchain assets without the involvement of a trusted third party as shown in figure 1. Smart contracts are developed by eliminating the limitations of the previous versions of traditional contracts i.e. it has more advantages than the previous one:

Fig. 1. Smart Contracts

Reducing risks: Because of immutability, it is nearly impossible to be turned at will after they've been registered. Furthermore, all transactions stored and duplicated across the entire distributed blockchain system can be traced and audited.

Reduce the costs of administration and service: Blockchains ensure system trust without the use of a central broker or intermediary by using distributed consensus mechanisms. Smart contracts stored in blockchain systems can indeed be activated in what seems like a decentralized way. As a result of the third-party intervention, administration and service costs can be significantly reduced.

Processes are considered well-organized structures: The efficiency of business processes can be dramatically improved by eliminating intermediary dependency.

TABLE I. SMART CONTRACTS VS TRADITIONAL CONTRACTS

Smart Contracts	**Traditional Contracts**
Fast and efficient	Time-consuming
Immutable	Can be changed by anyone
No need for the authority of a third party	Requires a third-party authentication
Cost-effective	Expensive
Automatic payment	Manual payment
Virtual presence(digital signature)	Physical presence(wet signature)
Pseudonymous	Legal Identity

VI. EXISTING WORKS

Electronic voting methods have already been adopted in certain countries and are used in parliamentary elections. Estonia, for example, has a long history in this subject and employs electronic voting in all of its elections with success [26-30]. Other projects came up, however, they all had major security flaws and were frequently canceled. Owing the Estonian E-Voting system is still in operation does not imply that the system is secure. Some community states and nations are using network-based voting systems through the internet confidentially whereas some nations like Switzerland, the USA, UK are using them publicly. In some provinces in Canada, online voting has been used at the municipal level where municipalities have been given the authority to do so. In 2003, France began testing the use of online voting for overseas voters, and in 2012, it made it available to all citizens living abroad for the first time during parliamentary elections. Online voting became the preferred method of voting for more than half of voters living abroad shortly after it became available. Nowadays there are many countries that allow the voters to vote through the voting system based on the blockchain through internet The countries like Brazil, the United States, and India allow the voters to use the internet-

Authorized licensed use limited to: ULAKBIM UASL - DOKUZ EYLUL UNIVERSITESI. Downloaded on November 08,2022 at 05:42:05 UTC from IEEE Xplore. Restrictions apply.

based voting system to cast their votes and there are many states and countries which doesn't allow this voting system as it has many concerns and high chances of frauds and security issues and cyber frauds compared to the traditional paper-based voting system.

VII. Proposed Work

After the candidate's identification has been ascertained, the voter can use the recommended e-voting platform to exercise their right to vote. The voter will be led to the voting portal in the e-voting system, where they can cast their vote by picking a candidate and hitting the submit button. If the same voter votes again, following verification and candidate selection, the electronic voting system will show that the person has already voted, implying that each voter has just voted once. To view the results, the administrator of the electronic voting system must call the process end method, which, like the start method, within the span of seconds shows the results, with the highest vote contender will be elected.

Fig. 2. E-Voting Process

The E-voting system is shown in figure 2. The admin must use the start process method in the background to initiate the selection procedure. The voter and candidate lists will be sent to the electronic voting system, where the voter casts his or her vote. When a voter casts a vote by selecting candidates, the votes are encrypted and sent to the start process method in the background, where it checks whether the vote is valid or not by checking the voter's verification, communicating with Ethereum to check the validity of votes, and sending smart contracts to the blockchain, allowing the voter to cast only one vote. Azure is used for background and front-end services, and they communicate with each other via GitHub accounts, where they validate votes and verify voters' identities for real-time deployment. They communicate with each other via encrypted calls that take advantage of the Azure Blockchain's scaling capabilities. In the background, the background talks with the blockchain, which is where the vote is cast. As the blockchain is more secure than other technologies the casting votes and smart contracts are deployed securely.

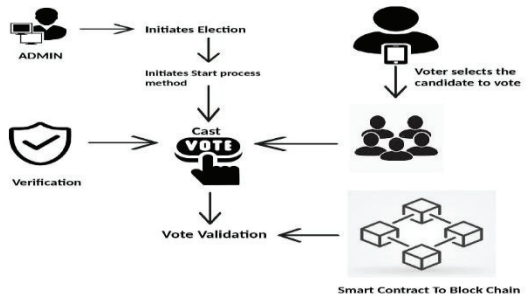

Fig. 3. Workflow of the proposed system

E-voting system can make the work easier and increase the comfort level of the voters but it also has a vulnerability that it may compromise the voter's data and voting results.so we use the blockchain technology to enhance the security issues any risks in voters' information and it helps in casting and counting the votes within limited time. The advantages are as follows for a voting system based on blockchain:

The blockchain-based E-voting system can enhance many important factors that will help the voters to use the voting system more easily. Blockchain can also help in storing the voter personal information safely and identities of voters' reliability and casting votes. The voting systems and data storing is more secure than others by this chain system. Last year United States Government used an online app for voting based on Hyperledger Fabric and the Thai Government used an online voting system based on blockchain coins and it has a database to store the voter's data and votes in an encrypted format. Switzerland's government allowed voters to use the Ethereum-based voting system to register the voters and use their voting rights as the government's online voters identity services and from 2018 onwards many governments are widely using blockchain-based voting systems in government elections to cast the votes securely.

Fig. 4. Advantages of E-Voting Systems.

VIII. Algorithm

After the registration of the voters the election process starts to register, voters must provide some basic information. The administrator will have to verify the information provided by the voters before allowing them to vote. All of the smart contract codes will be deployed on the local blockchain, and the test blockchain will be used to test apps. The reason for not directly deploying the code into the live blockchain is that they are immutable. It will be impossible to change a smart contract that has not been fully programmed once it has been stored in the live blockchain. As a result, before being deployed on the live blockchain, codes must be thoroughly tested. The smart contract is written now to prevent users from voting twice.

Step 1. All the registered voters will be having exactly one token in their Metamask wallet accounts.

Step 2. If the voter enters the voting portal then the vote cast method is used to check whether the vote has voted or not. If not, the voting option will be given to that voter.

Step 3. Every time the voter takes part in the process of the election then the process of calling the voting method starts.

Step 4. Every time a person vote with a token that transfers to the candidate to whoever intended to cast the vote.

Once the election is completed the winner will be declared by counting the tokens they have received. The

Authorized licensed use limited to: ULAKBIM UASL - DOKUZ EYLUL UNIVERSITESI. Downloaded on November 08,2022 at 05:42:05 UTC from IEEE Xplore. Restrictions apply.

result will be generated within a span of seconds, and it shows the candidate with the respective number of votes acquired the highest will be elected.

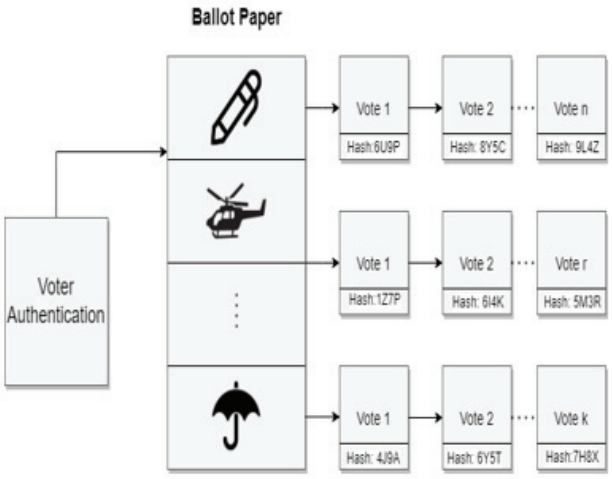

Fig. 5. Blockchain in E-Voting

Figure 5 depicts the authentication system of a voter and the blockchain to store the votes of the respective person in a chain. The hash function has a vital role in terms of security to defend against any type of tampering. Most of the papers stress SHA-256 for the higher level of security, but in work, MD-5 is introduced for fast processing.

Algorithm-1 (*Creation of Blockchain by the votes*)

Step 1. Permission is granted to cast the vote after ascertaining of voter's authenticity.

Step 2. Push ith button on *EVM*.

Step 3. Read the ith symbol to create the ith block (Where $1< i <m$)

Step 4. Creation of block chain for ith block

H (*i*) ←SHA-256 (vote (*j*-1)) // $1<j<n$

hash ← *H*(*i*)

Vote ←*new* ->*Vote*

Vote->*hash* ← *Vote*

null ← *Vote*->*hash*

Step 5. Repeat *Step* 3 till a number of votes are cast on the candidate.

Algorithm-2 (*Evaluation of winner from the blockchains*)

Step 1: Access the system and cast the vote.

Step 2: Push the button from *EVM*.

Step 3: Votes are stored as the nodes of the respective symbol by forming a chain.

Step 4: Go to *Step* 1 till the end of the Voters.

Step 5: Count the # of chains

Step 6: # of votes ← # of nodes in a chain

Step 7: Max ← 0.

Step 8: *If* # of votes > Max then Max ← # of votes

Step 9: Winner ← Max.

Output and analysis

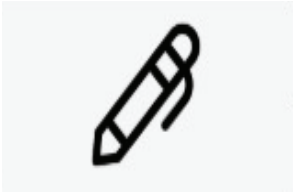

Fig. 6. The output of the voting system.

The hexadecimal output of Figure 6 is

MD-5: 57EDF4A22BE3C955AC49DA2E2107B67A

SHA-256: F371BC4A311F2B009EEF952DD83CA80E2B60026C8E935592D0F9C308453C813E

Difference between hash algorithms MD-5 and SHA-256.

TABLE II. COMPARISON OF MD-5 AND SHA-256

	Input	No of rounds	Message digest output
SHA-256	512	64	256
MD-5	512	64	128

From Table.2 it is obvious that both the algorithms are different from each other in terms of output. MD-5 is faster than SHA-256 for the generation of output. MD-5 utilizes less time than other one for the production of message digest output.

Security strength: MD-5 security strength is lesser than SHA-256 for the XOR operations as shown in Figure 7.

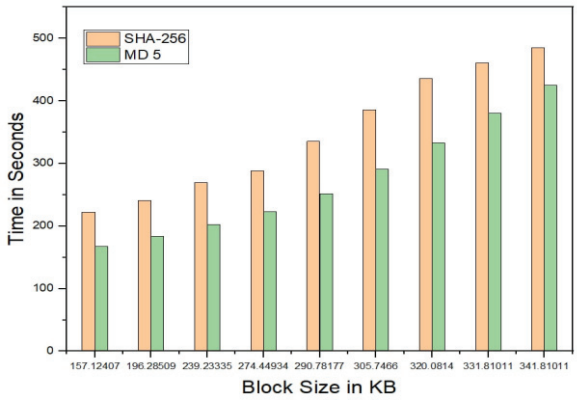

Fig. 7. block size with respect to time for SHA-256 and MD 5

IX. CONCLUSION

Electronic voting systems are evolved to ensure a secure and transparent technological aspect to provide the qualitative service to the voters. The voting system must be reusable, so it doesn't need to procure again and again for this process. Nowadays so many countries have employed electronic voting systems to conduct elections. In the future, it can completely replace the manual voting system to perform the voting process perfectly. Of course, blockchain technology is a little bit more complex than the existing systems with high-level security by challenging several security issues at present and in the future. An attempt has been made to overcome the flawless counting through the number of nodes focus on in this paper. The voting system has a process to collect and secure the voter's identities and

Authorized licensed use limited to: ULAKBIM UASL - DOKUZ EYLUL UNIVERSITESI. Downloaded on November 08,2022 at 05:42:05 UTC from IEEE Xplore. Restrictions apply.

information. The registered users can vote only once as a voter, and the votes can store in the respective queues to elect the winner within a short span of time. The candidate with the highest margin can be elected to the designated post. All the data can preserve on a server database by the chain which is secure forever and can recount at any moment to face any challenge. As blockchain technology becomes more extensively utilized and advanced, it will bring many changes to business and our way of life. Blockchain and identity, currently, identity systems are flawed in a variety of ways. They are porous, operate alone, and are prone to error. Blockchain systems can solve these issues by providing a centralized source for verifying identity and assets. Blockchain identity can also provide a form of "self-sovereignty" that did not previously exist with greater transparency between industries, there will most likely be a single blockchain that is shared by multiple industries. Having a single system, rather than multiple ones for different companies and industries, makes it easier and more accessible to the public, while also providing greater transparency and the inherent security of blockchain.

REFERENCES

[1] Ahmed Afif Monrat, PhD Student, LTU, Olov Schelen, Karl Andersson, A Survey of Blockchain from the Perspectives of Applications, Challenges and Opportunities

[2] Amara Devendra Dinesh; Chirra Durga Prasad Reddy; Govada Venkata Gopi; Rishab Jain; T. N. Shankar, A Durable Biometric Authentication Scheme via Blockchain, 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), 06 April 2021, **DOI:** 10.1109/ICAECT 49130. 2021.9392415.

[3] C. Meter, "Design of Distributed Voting Systems," Master's thesis, Heinrich-Heine-Universitt Dsseldorf, 2017.

[4] C.D. Clack, V.A. Bakshi, and L. Braine, "Smart contract templates: foundations, design landscape and research directions", Mar 2017, arXiv:1608.00771.

[5] D. Khader, B. Smyth, P. Y. Ryan, and F. Hao, "A fair and robust voting system by broadcast", in 5th International Conference on Electronic Voting, Vol. 205, pp 285-299, 2012.

[6] E. Maaten, "Towards remote e-voting: Estonian case." in Proceedings of the 1st Conference on Electronic Voting, 01 2004, pp. 83–100.

[7] Francesco Restuccia, Salvatore D'Oro, Salil S. Kanhere, TommasoMelodia, 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.

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

[9] G. Wood, "Ethereum: a secure decentralised generalised transaction ledger", Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014.

[10] Jonathan Alexander, Steven Landers and Ben Howerton, "Netvote: A Decentralized Voting Network", https://netvote.io/wpcontent/ uploads/2018/02/Netvote-White-Paper-v7.pdf, 2018.

[11] K Abdul Basith, T.N. Shankar, Hybrid Routing Topology Control for Node Energy Minimization for WSN, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 13, No. 2, March,2022, pp.468- 476.

[12] K. A. Basith, T.N.Shankar, Hybrid state analysis with improved firefly optimized linear congestion models of WSNs for DDOS & CRA attacks, Volume 8, Feb. 2022, Article number e845, PeerJ Computer Science, DOI: 10.7717/PEERJ-CS.845.

[13] K.Spurthy, T.N.Shankar, A HYBRID ENERGY EFFICIENT SECURED ATTRIBUTE BASED ZRP AIDING AUTHENTIC DATA TRANSMISSION, JSIR, SCIE, Vol.81(1), pp. 69-71, Feb.2022.

[14] Komal Kundan Sharma, Jyoti Raghatwan, Mrunalinee Patole, Vina M. Lomte, "Voting System Using Multichain Blockchain and Fingerprint Verification.

[15] Komal Kundan Sharma, Prof. Mrunalinee Patole, Prof. Vina M. Lomte, Securing Voting System Using Blockchain and Fingerprint Verication, International Research Journal of Engineering and Technology(IRJET)

[16] Krisna Adiputra, Rikard Hjort, Hiroyuki Sato A Proposal of Blockchain-based Electronic Voting System Cosmas Dept. of Electrical Engineering and Information Systems The University of Tokyo Tokyo, Japan

[17] Kriti Patidar, Swapnil Jain, 2019, Decentralized E-Voting Portal Using Blockchain 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT).

[18] Mrunal Pathak1 , Amol Suradkar2 , Ajinkya Kadam2 , Akansha Ghodeswar2 , Prashant Parde2, A Review on Blockchain Based E-Voting System.

[19] P. A. Azocar, Youth voter participation: involving today's young in tomorrow's democracy. International IDEA, Stockholm, 1999.

[20] R. Hanifatunnisa and B. Rahardjo, "Blockchain based e-voting recording system design," 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), Lombok, 2017.

[21] Sasmita Padhy, Sachikanta Dash, Prince Priya Malla, Sidheswar Routray and Yinan Qi, "An Energy-Efficient Node Localization Algorithm for Wireless Sensor Network", *2021 IEEE 2nd International Conference on Applied Electromagnetics, Signal Processing, & Communication (AESPC).*

[22] Rumeysa Bulut, Alperen Kantarcı, Safa Keskin, Şerif Bahtiyar Blockchain-Based Electronic Voting System for Elections in Turkey

[23] S. Nakamoto, "Bitcoin : A Peer-to-Peer Electronic Cash System," White Paper, pp. 1–9, 2008.

[24] S.-I. Kang and I.-Y. Lee, "A study on the electronic voting system using blind signature for anonymity," 2006 International Conference on Hybrid Information Technology, vol. 2, pp. 660–663, 2006.

[25] Shankar, T., N., Sahoo, G., Niranjan, S 'Using the Digital Signature of a Fingerprint by an Elliptic Curve Cryptosystem for Enhanced Authentication' , Information Security Journal , A Global Perspective, Taylor and Francis, Vol.21, No. 5, pp. 242-254.

[26] Dash, S., Panda, R., & Padhy, S. (2021). Blockchain-based intelligent medical IoT healthcare system. SPAST *Abstracts*, 1(01).

[27] T. M. Roopak and R. Sumathi, "Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology," 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, 2020, pp.

[28] T. N. Shankar; P Rakesh; T Bhargawa Rao; L Hari Bharadwaj; Ch Rakesh; M. Lakshmi Madhuri, Providing Security to Land Record with the computation of Iris, Blockchain, and One Time Password 2021, International Conference on Computing, Communication, and Intelligent Systems (ICCCIS).

[29] U.C. abuk, A. avdar, and E. Demir, "E-Democracy-The-Next-GenerationDirectDemocracy-and-Applicability-in-Turkey."

[30] What Are Smart Contracts? A Beginner's Guide to Smart Contracts. Retrieved 26 8, 2018, from https://blockgeeks. com/guides/smart-contracts/https://theinfinitekitchen.com/guide/quick-answer-what-is-difference-between-sha-and-md5/

Authorized licensed use limited to: ULAKBIM UASL - DOKUZ EYLUL UNIVERSITESI. Downloaded on November 08,2022 at 05:42:05 UTC from IEEE Xplore. Restrictions apply.