Düzce University Journal of Science & Technology

Research Article

VOTEMAT: A Blockchain Based Voting System

Egemen BİROL [a], K. Tuğşat İSKENDER [a], Timur ÖZKUL [a], Ayça TOPALLI [a,*]

[a] *Department of Electrical and Electronics Eng., İzmir University of Economics, İzmir, TÜRKİYE*
** Corresponding author's e-mail address: ayca.topalli@ieu.edu.tr*
DOI: 10.29130/dubited.1451841

ABSTRACT

This study aims to show that a secure, trustable and immutable voting system can be established with Blockchain technology. Decentralized structure of the Blockchain excludes the central authority and provides transparency. Moreover, its cryptographic functions enable secure transactions. Therefore, the operation is prevented from potential frauds, such as multiple votes, fake vote attempts, and fraudulent vote counts. The proposed method, VOTEMAT, covers both electronic voting and paper ballot as a complete solution. A mobile application and a Web site, connected to Ethereum private Blockchain network, were developed for the voters who prefer to cast their votes remotely. It is also possible to vote in the voting centres via the mobile device or paper ballot placed in the vote boxes; but these votes are also recorded in the same Blockchain and equally secure. For the remote users, a two-step authentication is designed, based on the information on the national identity card and face recognition. An additional encryption based security measure is used to avoid hacking attempts, such as man in the middle attacks. Since the proposed system is more practical than the traditional voting methods, it can increase the participation and be utilized in all kinds of local or national elections.

Keywords: *Blockchain, Cryptography, Ethereum, Hyperledger Besu, Voting*

VOTEMAT: Blokzincir Tabanlı Oylama Sistemi

ÖZET

Bu çalışma Blokzincir teknolojisi ile güvenli, güvenilir ve değiştirilemez bir oylama sistemi kurulabileceğini göstermeyi amaçlamaktadır. Blokzincir'in merkeziyetsiz yapısı, merkezi otoriteyi sistemin dışında tutmakta ve şeffaflık sağlamaktadır. Ayrıca, uygulanan şifreleme işlemlerin güvenli bir şekilde gerçekleşmesini sağlamaktadır. Böylece birden fazla oy kullanılması, sahte oy pusulası kullanım girişimleri ve hileli oy sayımları gibi olası sahtekârlıkların önüne geçilebilecektir. Önerilen yöntem olan VOTEMAT, hem elektronik oylamayı hem de kâğıt oy pusulasını kapsadığı için eksiksiz bir çözüm sağlamaktadır. Oylarını sandığa gelmeden kullanmayı tercih eden seçmenler için Ethereum özel Blokzincir ağına bağlı bir mobil uygulama ve bir Web sitesi geliştirilmiştir. Sistem oy verme merkezlerinde, oy verme kabinlerine yerleştirilen mobil cihaz veya kâğıt oy pusulası aracılığıyla oy kullanmayı desteklemektedir; bu durumda da oylar aynı Blokzincir'e kaydedilmekte ve aynı derecede güvenli olarak saklanmaktadır. Oylarını sandık başına gelmeden kullanmak isteyenler için, ulusal kimlik kartındaki bilgilere ve yüz tanımaya dayalı iki adımlı bir kimlik doğrulama tasarlanmıştır. Ayrıca, ortadaki adam saldırıları gibi izinsiz erişim girişimlerini önlemek için şifreleme tabanlı bir güvenlik önlemi kullanılmıştır. Önerilen sistem geleneksel oylama yöntemlerine göre daha pratik olduğundan, katılımı artırabileceği ve her türlü yerel ya da ulusal seçimde kullanılabileceği düşünülmektedir.
Anahtar Kelimeler: *Blokzincir, Ethereum, Hyperledger Besu, Şifreleme, Oylama*

Received: 12/03/2024, Revised: 23/05/2024, Accepted: 30/05/2024

I. INTRODUCTION

Blockchain is a new topic that is open to research and development. With the popularity of cryptocurrencies, Blockchain has drawn a lot of attention, but its usage is not limited to cryptocurrencies [1-3]. Since data security and privacy are amongst the most sensitive and necessary issues of nowadays, Blockchain technology that provides this opportunity can be applied to many fields [4].

Election systems and voting protocols are one of the most suitable areas that can make use of the advantages of Blockchain. Conducting elections on paper poses many problems and threats such as lack of participation due to the process being hard for some people, costs required for the election process, high numbers of invalid vote counts due to voter faults, and sluggishness of the process of casting and counting votes.

In countries where no automated system of casting and vote counting exists, votes are usually recounted due to security concerns during political elections. When the recounting is done under the same governance, these concerns generally do not disappear [5]. Besides, having a single administrator that watches the whole process may cause fraud. Therefore, a decentralized network based on Blockchain technology could be a solution to cut the central authority out and may provide a secure and trustable voting system, satisfying data integrity and immutability [6].

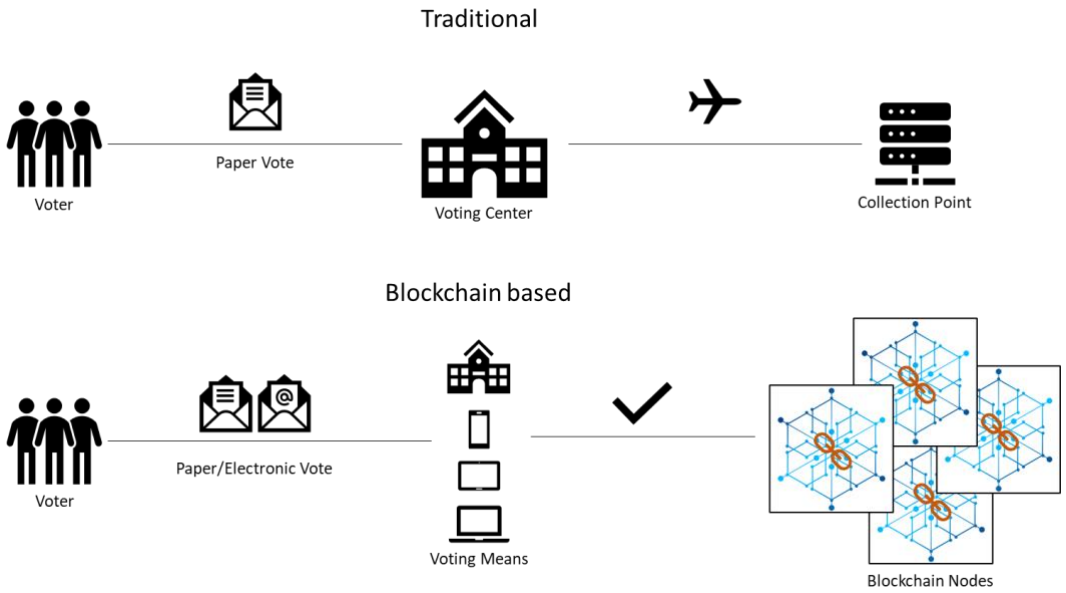


Figure 1. *Traditional vs Blockchain based voting systems*

The difference between traditional and Blockchain based voting systems is shown in Figure 1. In the former, voters must go to dedicated voting centers to cast their votes on paper. Then these votes must be counted and sent to a collection point. In the latter, on the other hand, the voters have the chance to cast their votes electronically without the need of going to the voting center. Furthermore, votes are stored instantly in all Blockchain nodes.

The system proposed here is named VOTEMAT and it combines these two voting methods. Voters can cast their votes remotely via their smartphones or computers to be stored in a Blockchain. But in any case, if a voter chooses to go to the voting center, their vote is also stored in the same Blockchain infrastructure in the proposed system; therefore, both ways are equally secure and private. Furthermore, it introduces additional security over the communication between client and server sides based on RSA encryption. The vulnerabilities of the classical voting system do not exist in the proposed method. In addition to the simplification of the process, the removal of the burden of going to and queueing in the

polling station is also increasing the practicality of the proposed system. Therefore, an increase in the participation can be expected.

In this study, Hyperledger Besu's (HB) Ethereum implementation is used as a private Blockchain network [7]. Although the system proof-of-concept makes use of Turkish ID cards thus making it suitable for elections in Turkey, it can be adapted to any election with or without the paper ballot part.

The rest of the paper is organized as follows: Section 2 gives a literature survey on the related studies and emphasizes the differences and novelties of the proposed system. The fundamentals of Blockchain technology are summarized in Section 3. Methodology is detailed in Section 4. Section 5 gives the results and discusses the findings. Conclusions and suggestions for the future work can be found in Section 6.

II. RELATED WORKS

A. LITERATURE SURVEY

Several works on voting systems with Blockchain technology have been proposed in recent years [8-27]. For example [9] focuses on the requirements of voting platforms such as transparency, provability, and authentication; and, tries to address these concepts using Ethereum Blockchain network and smart contracts. In [10], there is an administrator who creates and assigns individual authentication keys to the voters to avoid multiple casting issues. In this system, each vote is registered as a new block in the Blockchain. The authors of [11] introduce ABVS (Auditable Blockchain Voting System) for security improvements and verifiability in electronic voting protocols. They use the Paillier homomorphic encryption algorithm, which allows the system to read encrypted messages without decrypting them. With such a system, voters need to give their identification information but do not reveal their voting choices.

Garg et al. in [13], Al-Maaitah et al. in [14], and Singh et al. in [15] present literature surveys comparing different methodologies used in e-voting systems. They also emphasize the need for secure and reliable voting systems with increased transparency and minimal errors. The work in [16] as well gives a review of Blockchain-based electronic voting systems, exploring various Blockchain frameworks, consensus mechanisms, and cryptographic methods to address the challenges associated with traditional and digital e-voting systems.

Similarly, how to make elections more secure and reliable with Blockchain, and how Proof of Authority (POA) and smart contracts satisfy privacy issues are explained in [17]. But it is also stated that a separate measure is needed for a secure authentication since the Blockchain itself does not guarantee it. The paper presented in [18] proposes Blockchain usage in elections in order to reach the results instantly, which is another advantage of this technology. Malkawi et al. design an Ethereum-based electronic voting system for the Jordanian parliamentary elections in [19]. Their system uses a dual-smart contract structure where one smart contract deploys another to manage individual voting districts.

Tanwar et al. explore the implementation of a Blockchain-based electronic voting system utilizing Ethereum's smart contract functionalities in [20]. They outline a Decentralized Application (DApp) for voting, leveraging Ethereum's Blockchain to manage and secure electronic votes with a front-end user interface for accessibility. The system proposed by Hassan et al. utilizes the Ethereum Blockchain, Ganache as a local Blockchain environment, and Remix for deploying smart contracts in [21]. Their results indicate that while the system ensures voter anonymity and vote integrity, it faces challenges related to scalability and transaction costs, particularly under high network load. Bronco Vote [28] is an online voting system built for university events, such as ballots to guarantee easy access and wide-spread participation. It lies on top of Ethereum Blockchain infrastructure and uses smart contracts. There are also several Blockchain based mobile voting applications, such as FollowMyVote [29], Voatz [30], OVN [12], Agora [31], and Polys [32].

B. DIFFERENCES AND NOVELTIES OF THE PROPOSED SYSTEM

To the best of authors' knowledge, there is no study similar to the one presented here that combines both physical and remote voting in the same Blockchain infrastructure and adds extra security level based on RSA algorithm.

Traditional voting with paper ballot is highly familiar among voters, easy to perform especially by illiterate people. Moreover, people may not be accustomed to the Internet, may not have access to new technologies, or may have disabilities. Therefore, it is not possible to abandon the traditional voting at once. On the other hand, electronic voting brings advantages such as cost down, reusability, efficiency, remote area access, more voter turnout, etc. as compared to the traditional elections. On top of these advantages, Blockchain based voting is the most reliable, secure, transparent, decentralized, tamper and fraud free, fast, verifiable, and auditable electoral option as of today. Therefore, it should not be ignored. The proposed method embraces all categories of voters, modern or far from technology, by being interoperable with the existing traditional system, and introducing the Blockchain based new system. It allows paper balloting, online balloting in the vote center, and online balloting remotely. Regardless of the voting method, all votes are stored securely and immutably in the same Blockchain. This kind of complete solution has not been encountered in the literature, and in fact, it can be an intermediate solution until all parts of the society become ready for the online-only elections.

The proposed approach uses an RSA based encryption layer for the off-chain parts of the system, inspired by the Blockchain technology, in addition to the https connection. In this way, the sensitive data are transferred securely between front-end and back-end, as a measure to prevent hacking attempts. Moreover, a private Blockchain instead of a public one is configured to minimize attack risks and ensure security and data privacy.

Regarding the Blockchain platform, HB is a suitable one, although it has been used generally in finance area, and no example usage has been seen for voting [33]. The reason for this selection is because HB's sharding feature, a technique that divides the whole Blockchain network into smaller pieces [34]. Almost all studies point to the scalability issue that is Blockchain networks having difficulties to process growing number of transactions, especially in the case of national elections of highly populated countries. HB seems a proper alternative since it provides better scalability by sharding as compared to the others.

In the literature, some other Blockchain based voting systems suggest all voters to have their own accounts and Web3 interfaces. This is not a realistic requirement for a real-life scenario. Therefore, the system proposed here has an easy-to-use front-end with no prerequisite knowledge about the underlying technologies.

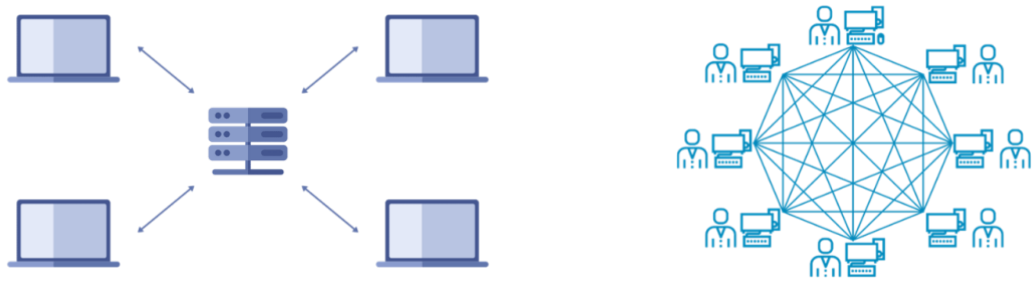
Another aspect is the voter's identity and eligibility confirmation. Blockchain does not provide a solution for this authentication part and every work provides its own solution. The proposed system's solution is a two-step authentication procedure involving ID number and face similarity checks using citizens' national cards and system's camera.

Overall, the proposed HB based Blockchain voting system meets eligibility, privacy, fairness, soundness, and completeness, which are the necessary criteria for a realistic solution.

III. BLOCKCHAIN TECHNOLOGY

Blockchain is a decentralized network of computer systems, different from the centralized model, which is operated by a single entity as shown in Figure 2.a. Blockchain models share and replicate a digital record of transactions (ledger) across the network as depicted in Figure 2.b. With the decentralized feature, data integrity is ensured and possibility of any fraud is eliminated. As compared to the classical

server usage for the data storage, which is more vulnerable to hacking attempts, it is nearly impossible to hack all of the nodes of a Blockchain.



(a) ***(b)***

Figure 2. (a) *Classical (centralized) server vs.* ***(b)*** *Blockchain (decentralized) model*

The decentralized and distributed nature of the ledger is one of the key features of Blockchain technology, and it is also often referred to as distributed ledger. Each participant's copy of the ledger is updated each time a new transaction is added to the Blockchain, and each block in the chain holds multiple transactions. Transactions are secured through encrypted messages, and each block in the chain is connected to the previous one by using a cryptographic hash. As shown in Figure 3, this creates an unchangeable and permanent record of all transactions that have ever happened on the Blockchain.

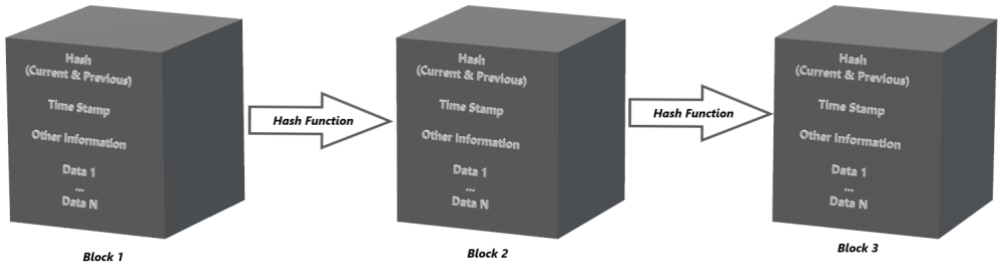


Figure. 3. *Blockchain structure*

It is crucial to distinguish between two fundamental elements within the Blockchain ecosystem: nodes and accounts. Nodes are individual computer systems that constitute the network. Their role includes validating and propagating transactions, as well as maintaining a copy of the entire Blockchain ledger. Nodes collaborate to ensure network security and consensus. They are integral to preserving the decentralized nature of the Blockchain. Accounts, on the other hand, are digital entities associated with specific users or entities on the Blockchain. They hold ownership of cryptocurrency tokens or assets and are used for initiating transactions. Accounts are distinct from nodes; while nodes collectively maintain the Blockchain, accounts interact with it by creating, sending, and receiving transactions.

Public networks are decentralized networks that are accessible to everyone and they do not have strict limitations on access in the context of the Blockchain. These networks' openness, inclusion, and decentralization make them stand out from other networks like the Ethereum main net. Bitcoin trading and dApps are two common activities carried out by users of public networks that call for a high level of security and openness.

Private networks, on the other hand, suggest a more limited and controlled Blockchain environment. Access to the Blockchain and its features is often restricted to a select number of authorized members in a private network. Private networks are appropriate for use cases where privacy, security, and controlled governance are crucial since these members are frequently screened and given permission to

join the network. Private networks are used by businesses and organizations for sensitive applications like voting systems, financial transactions, and supply chain management.

An important aspect of Blockchain is the use of consensus mechanisms to validate and record transactions. Rather than relying on a central authority to verify and process transactions, a consensus mechanism is utilized to ensure that all participants in the network agree on the validity of a particular transaction. Some of the most widely used consensus mechanisms are Proof of Work (PoW), Proof of Stake (PoS), and Proof of Authority (PoA). In private Ethereum networks, Istanbul Byzantine Fault Tolerance (IBFT 2.0), which is a PoA algorithm known for its high level of security and fault tolerance, is used. In an IBFT based Blockchain network, more than two third of the nodes are expected to validate transactions for an uninterrupted process. On top of that, IBFT has immediate finality which corresponds to preventing any formation of extra-chains and forks. Applications like VOTEMAT, where security, fault tolerance, and the integrity of transactions are of utmost concern, are particularly well suited for IBFT's strict consensus method. Therefore, IBFT is used as the consensus mechanism in this study.

Along with the advantages that come with using a decentralized network, multiple vote and fake vote attempts are also avoided in Blockchain based election systems. Furthermore, any potential fraudulent changes to the vote count are also prevented due to transactions being secured through cryptographic hash functions.

In this respect, Blockchain technology is a powerful tool that can be used to create decentralized systems that are more secure, transparent, and efficient than traditional centralized systems.

IV. METHODOLOGY

Overview of proposed VOTEMAT system is given in Figure 4. In this study, it is aimed to cover all possible voting schemes within a single system:

- via a mobile application (phone or tablet),
- via a Web site,
- via paper ballot.

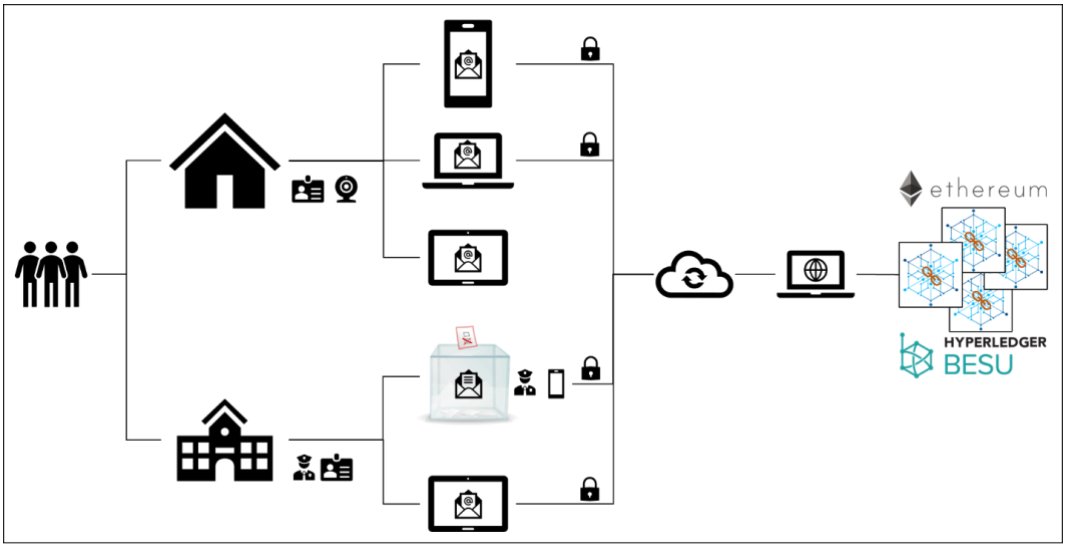


Figure 4. *Overview of proposed VOTEMAT system*

In the remote case, voters who prefer to stay at home and use either the mobile application or the Web site, are first authenticated by their identity numbers and face recognition to ensure that only one vote is cast by an eligible voter. The user's national ID card is captured by the camera of the mobile device or computer to extract ID number and ID photograph from the captured image. The ID number is sent to

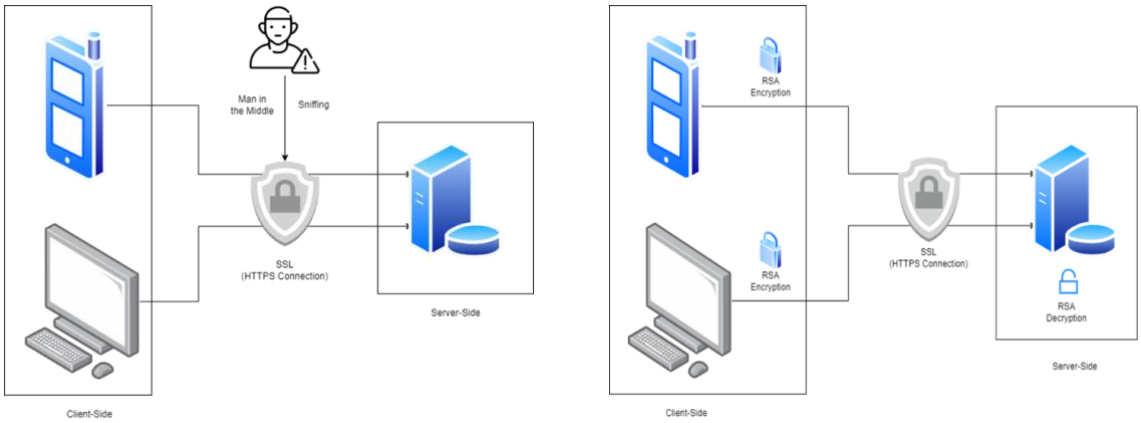
the server to ensure that it belongs to an eligible citizen and no vote has been cast yet with this number for the election. Then the voter's face is captured by the camera and compared with the ID photograph, seeking for a certain similarity. After the authentication has been established, they are presented with the election candidates and they can cast their votes.

In the physical voting, in which voters choose to go to the polling stations, the authentication task is performed by a person in charge. The ID number is recorded at the server, and the face similarity with the ID photograph is checked manually. Then the voting is done either via the mobile application installed on tablets in the voting kiosks, or via the classical paper ballot, depending on the voter's ability and preference.

In order to keep the information whether a citizen has cast their vote, there is an ID database placed in the server side. This database is different from the Blockchain part where votes are being kept; therefore, citizen's national ID and their vote cannot be associated.

Regardless of the way of voting, whether remote or physical, all votes are stored in the same Blockchain structure. Electronic votes are added directly by the mobile application or Web site; paper votes are added by authorized personnel via an interface application.

Before sending ID numbers and votes to the server, the mobile application and the Web site encrypt them by applying the RSA algorithm to add an extra security level during the transmission over the cloud. This is mostly done to prevent sniffing and data alteration attempts and protect this vulnerable information. As seen in Figure 5, even https connection is prone to the man in the middle attacks, and this can be avoided by introducing RSA ciphering.



(a) ***(b)***

Figure 5. (a) *SSL only HTTP connection vs* ***(b)*** *Secure communication with SSL & RSA*

The software on the Web server communicates with the Blockchain implementation via TLS-enabled cURL library and relays votes sent by the mobile application and the Web site. These votes are stored in the Blockchain in a secure and immutable way.

In this study, each Ethereum account created represents a candidate entered in the election. One more account is created and dedicated to the system administrator. Initial balances of the candidate accounts are all set to zero and each transaction from administrator to a candidate means a vote being cast to that candidate. At each transaction, the administrator's balance is decreased by one and the candidate's balance is increased by one. Transaction among candidate accounts is forbidden.

HB's Ethereum Blockchain implementation with IBFT consensus algorithm is used in this study [7]. The main reason behind this choice is that being widely used on the public Ethereum main net, it is tested intensively and well supported. Being licensed as open-source software under the Apache 2.0 terms is also another factor for our choice. It also supports private transactions, allowing two parties to perform a transaction on the network without the other members being able to work out the details. The

instance runs on the Ubuntu 22.10 environment, which is set up on Oracle VM VirtualBox software, as shown in Figure 6.

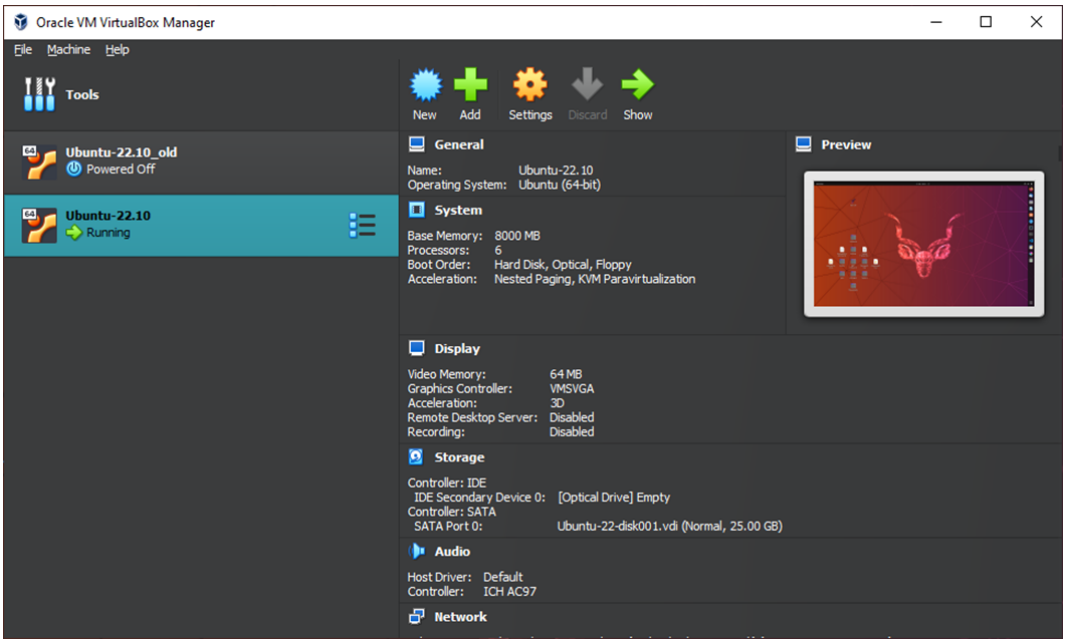


Figure 6. *Oracle VM VirtualBox*

HB is an open-source Ethereum client which runs on public and private networks. Private networks offer a controlled and secure environment, making them ideal for preserving the confidentiality and integrity of the voting procedure, two essential components of any democratic election system. Therefore, VOTEMAT is implemented utilizing a private network to meet the demanding criteria for security and data privacy that are inherent to the election process.

EthSigner [35], which is an Ethereum transaction signer module, is used to sign transactions using a private key. Tessera [36] is another module used to serve as a privacy manager for HB clients.

For the data files of the Blockchain, a main folder named IBFT-Network is created. In this folder, it is necessary to create files ibftConfigFile.json, genesis.json, and separate folders for the nodes. Inside each node folders, data and Tessera directories are to be generated to hold their public and private keys. Tree structures of IBTF-Network and Node folders can be seen in Figure 7.

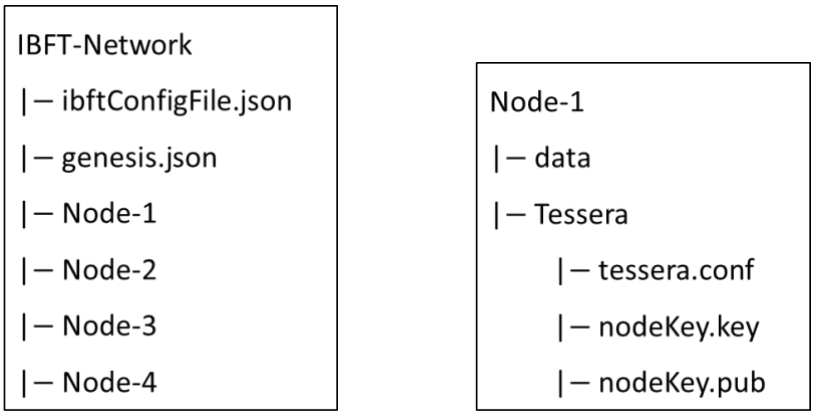


Figure 7. *Tree structures of IBTF-Network and Node folders*

In this study, the number of nodes is selected as four and nodes are created in the same machine for simulation purposes. In a real-life implementation, they need to run on different machines in accordance with the distributed nature of the Blockchain technology. Therefore, under the IBFT-Network folder,

normally there should be a single node directory. Among these nodes, one of them is called the boot node and it has special features. Node-1 is selected as the boot node in this study. The HB environment ensures synchronization of these nodes after any Blockchain operation.

The configuration file ibftConfigFile.json resides only in boot node's machine and holds Blockchain's identification number as 1337, the number of nodes as four, and names and balances of the accounts. Blockchain accounts along with their associated public and private keys are created by JavaScript language using web3.js library with the following code snippet:

```
const Web3EthAccounts = require('web3-eth-accounts');
const account = new Web3EthAccounts('ws://127.0.0.1:8591');
console.log(account.create());
```

The following command creates genesis.json file using the information stored in the configuration file ibftConfigFile.json:

```
besu operator generate-blockchain-config --config-
file=ibftConfigFile.json
```

The genesis.json file is a crucial configuration file that sets the initial state and parameters of a Blockchain network. It plays a pivotal role in establishing the network's starting conditions, including account setup and network identification.

In each Tessera directory, public and private key pairs are generated by the following command:

```
tessera -keygen -filename nodeKey
```

After the modules have been created, they need to be activated. First of all, the boot node, which is selected as Node-1, is started by running the following command under Node-1 folder:

```
besu --data-path=data --genesis-file=../genesis.json --rpc-http-
enabled --rpc-http-api=ETH,NET,IBFT,EEA,PRIV --host-allowlist="*" --
rpc-http-cors-origins="all" –rpc-http-port=8591 --privacy-enabled --
privacy-url=http://127.0.0.1:9101 --privacy-public-key-
file=Tessera/nodeKey.pub --min-gas-price=0
```

The above command returns boot node's Enode URL that is used to start other nodes. For example, Node-2 is started with the command below under Node-2 folder, using the Enode URL of Node-1:

```
besu --data-path=data --genesis-file=../genesis.json --rpc-http-
enabled --rpc-http-api=ETH,NET,IBFT,EEA,PRIV --host-allowlist="*" --
rpc-http-cors-origins="all" --rpc-http-port=8592 --privacy-enabled -
-privacy-url=http://127.0.0.1:9102 --privacy-public-key-
file=Tessera/nodeKey.pub --min-gas-price=0 --bootnodes=<Node-1 Enode
URL> --p2p-port=30302
```

Tessera module is started with the following command:

```
tessera -configfile tessera.conf
```

ETHSigner, which needs to run on the same machine with the boot node alone, is started with the following command:

```
ethsigner --chain-id=1337 --http-listen-host=http://127.0.0.1 --
downstream-http-port=8591 file-based-signer --key-file=keyFile --
password-file=passwordFile
```

where keyFile and passwordFile are generated using web3.js functions together with the private key and password of the administrator's Blockchain account.

When all modules are up and running, the system becomes ready to use. The main system components and their interactions are shown in Figure 8 for remote users.

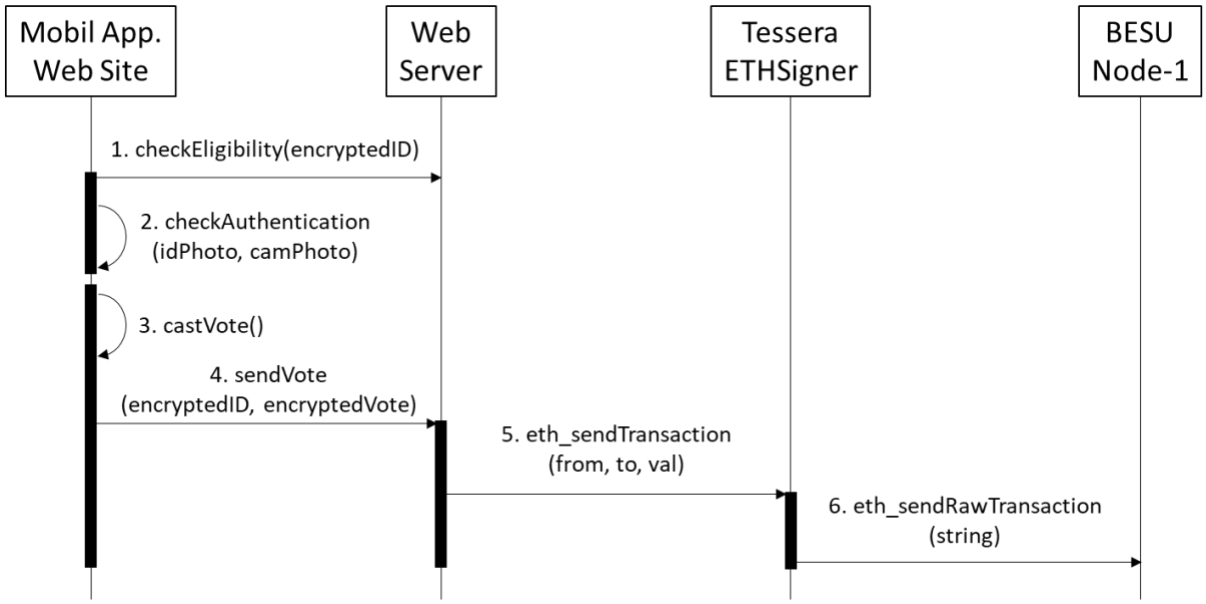


Figure 8. *Sequence diagram of the interactions*

As can be seen in Figure 8, the first interaction happens between the front-end and the Web server. Mobile application or Web site asks voter to enter their national ID and sends it to the Web server in encrypted format using application's private key. All the interactions between the front-end and the Web server are protected by the RSA algorithm, in addition to the https connection. Web server decrypts the ID number by the application's public key, checks the ID database stored off-chain, i.e., separately from the Blockchain and returns the result depending on the voter's status, if they are eligible and has not cast their vote yet.

For eligible voters, the second step is the authentication check in the front-end side by comparing the ID number given in the first step and the number on the national card captured via the camera. Similarity between the photo on the national card and voter's face shown to the camera is also checked in this step.

If the voter is authenticated, only then they can cast their vote as the third step. Their national ID number and vote are encrypted by the application's private key again and sent to the server in the fourth interaction. The server decrypts the incoming data by the application's public key, registers the ID as "vote cast finished" into the database. Since the ID database and the vote Blockchain are two independent entities, there is no way to associate the user's ID number and their vote.

In the fifth step, the Web server calls `eth_sendTransaction` function from ETHSigner by making a cURL request. Here, admin's Blockchain account address is given as "from" argument. Depending on the incoming vote, associated account address of the candidate or party is assigned as "to" argument. The last argument "val" is set to 1 ETH.

As the last interaction, ETHSigner encrypts these data using the admin's private key and sends as a hexadecimal string to the Blockchain via `eth_sendTransaction` function. After this step, the transaction is added to Node-1's Blockchain copy and other nodes are triggered for validation.

On the other hand, for the voters who prefer to go to the voting centers, eligibility and authenticity checks are performed by the people in charge. Then they can cast their votes either via paper ballot or via the mobile application installed on tablets in the kiosks. Paper votes are sent to the Blockchain via a special interface application developed for the authorized personnel after the election time has ended. Electronic votes are sent to the Blockchain from those tablets. For the voting center case, the process is the same as the remote voting case from the third step of Figure 8, ending at the same Blockchain for all cases.

In the proposed system, the Web server and HB Node-1, including Tessera and ETHSigner modules must reside on the same computer. This condition ensures that there is no network connection involved while calling `eth_sendTransaction` function. Moreover, the initialisation of ETHSigner limits the originator of this function to be only the localhost, hence no security issue. Otherwise, it would be necessary to deploy and trigger a smart contract to handle secure transaction of votes.

V. RESULTS AND DISCUSSION

Along with the HB Ethereum Blockchain infrastructure and a Web server setup, a mobile application and a Web site are designed and implemented to realize the proposed system. The welcome screens are shown in Figure 9.

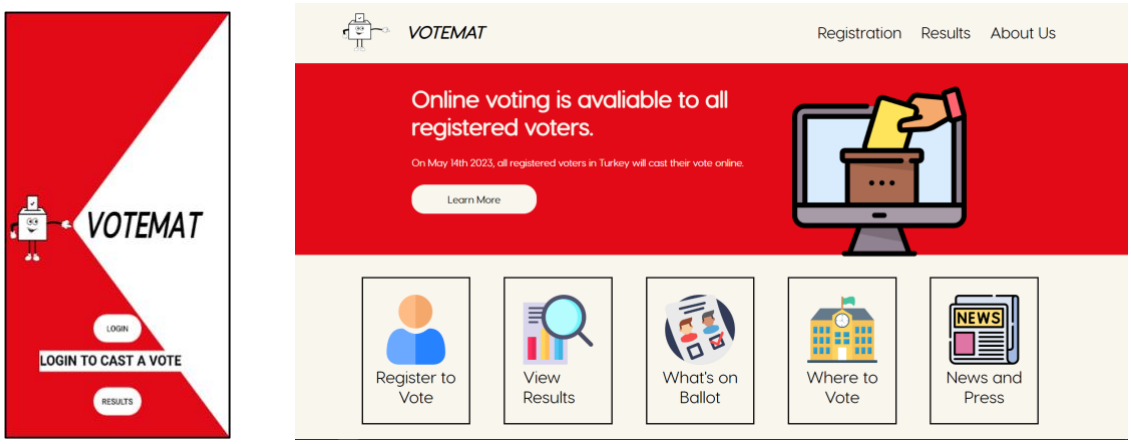


Figure 9. *The main screens of the mobile application and the Web site*

In order to cast a vote, the user has to register with their national ID number (Figure 10). The system checks its validity and whether a vote has already been cast associated with this number. In case of any violation, a message appears on the screen, such as "Invalid ID!" or "You have already cast your vote!".

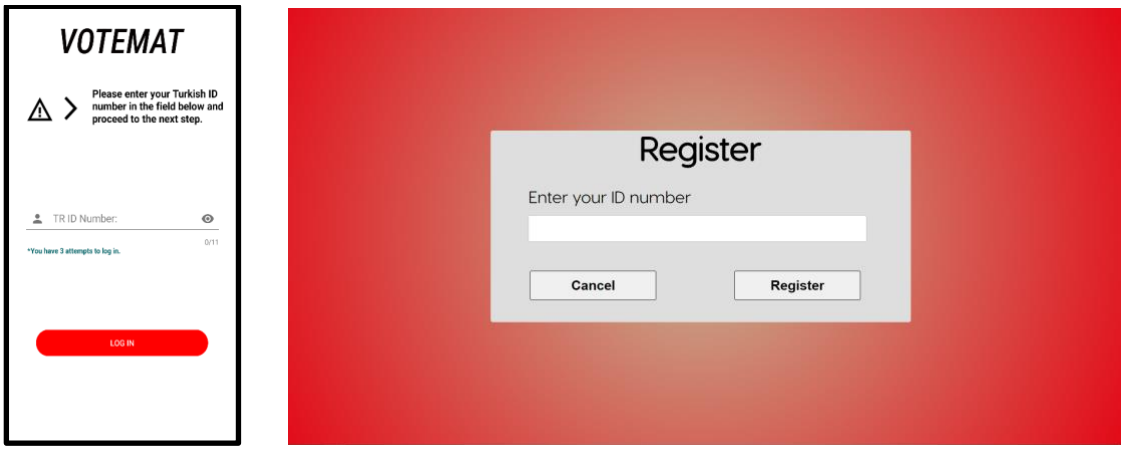


Figure 10. *Registration screens of the mobile application and the Web site*

After successful registration, the voter is directed to the authentication screen to ensure that the declared national ID number belongs to the user of the system. In this phase, there is a two-step authentication. First, the user is prompted to show their national ID card to the camera of the mobile device or computer so that the system can read the ID number from the card using optical character recognition (OCR) method and compare it with the one entered in the previous screen. If the number is matched, then in the second step, the user is asked to look at the camera for face recognition. The system captures the image from the camera and compares it with the photo on the national ID card. The structural similarity index (SSIM) between the ID photograph and the captured face is calculated and the system accepts 75% as the minimum score. For an efficient capture of the ID card and the face, guidelines appear on the screen, as shown in Figure 11. The authentication screens of the mobile application and the Web site can be seen in Figure 12.

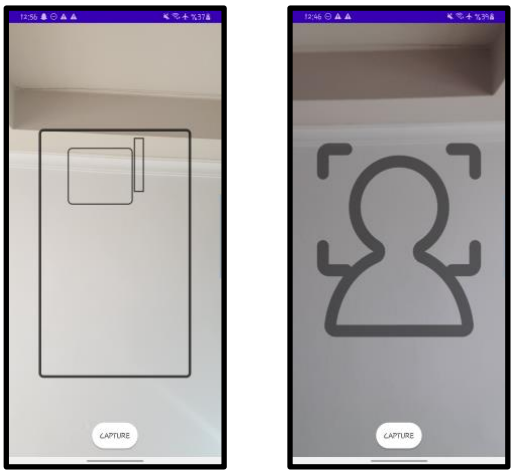


Figure 11. *Guidelines for the national ID card and face capture*

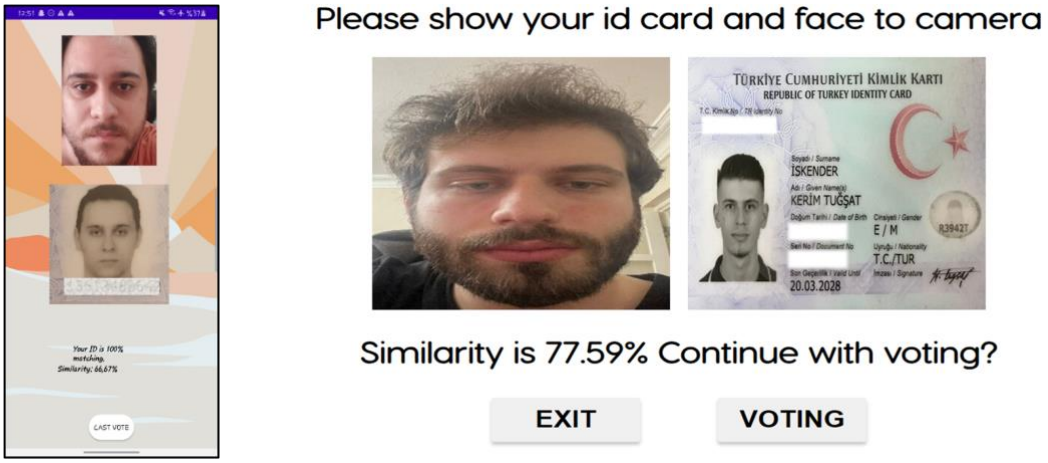


Figure 12. *Authentication screens on the mobile application and the Web site*

The voter who has completed the identification authentication phase either via the application remotely or via the authorized personnel in the voting center can proceed with the voting phase. Exemplary voting screens are given in Figure 13.

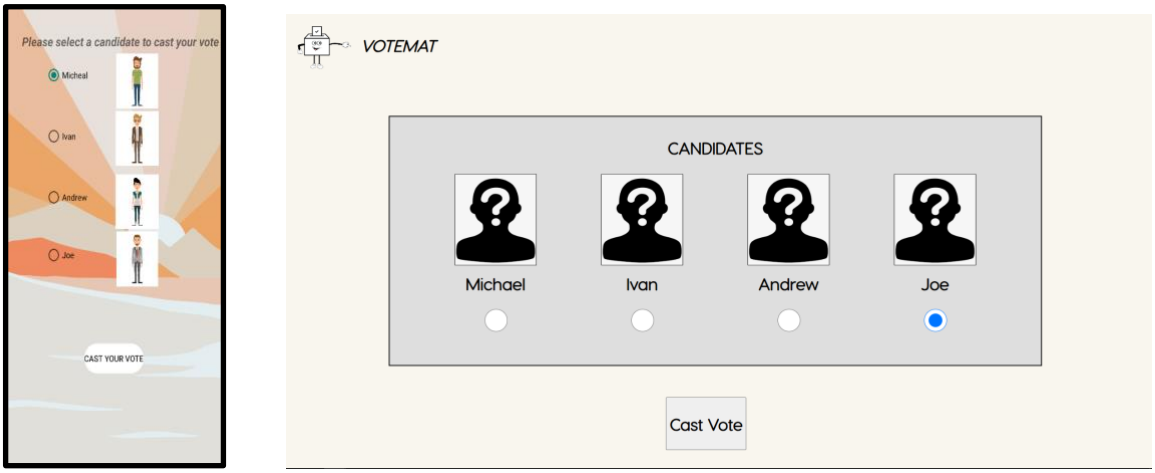


Figure 13. *Voting screens on the mobile application and the Web site.*

At this point the voter is prompted with their candidate selection and asked to confirm their vote. The successful voting ends with thank you screens as shown in Figure 14.

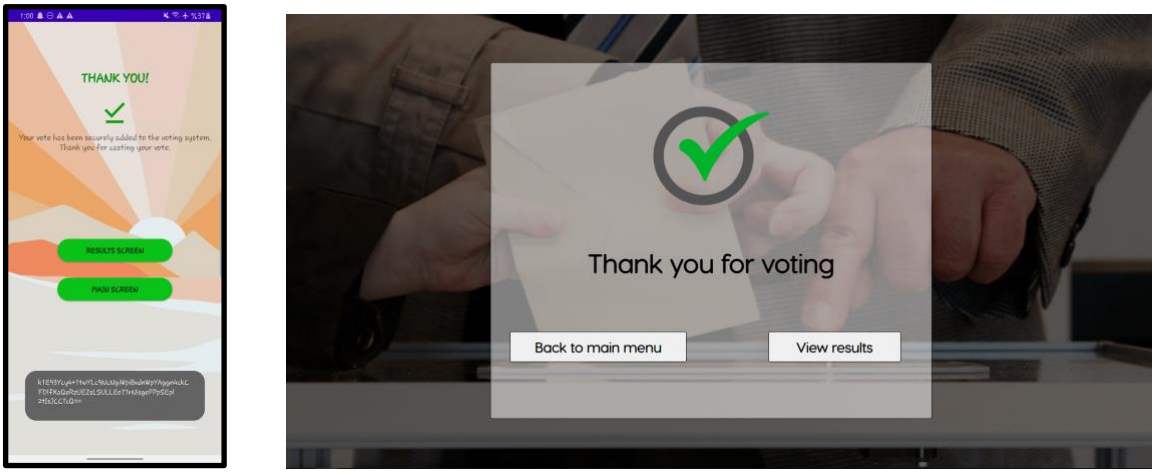


Figure 14. *Thank you screens on the mobile application and the Web site*

Paper ballots are also collected in sealed boxes in the voting centers. After the voting process is completed, these boxes are opened by trusted officials, and the votes are entered into the same Blockchain based system one by one.

When it is allowed to see the results, anybody can check them via the mobile application or the Web site (Figure 15). Depending on the election type, the results can be shown either after the voting time has ended or instantly. This would eliminate the issues such as loss of time during the transportation of votes to the center, disruptions on the way, and slowness in entering the votes into the main system.

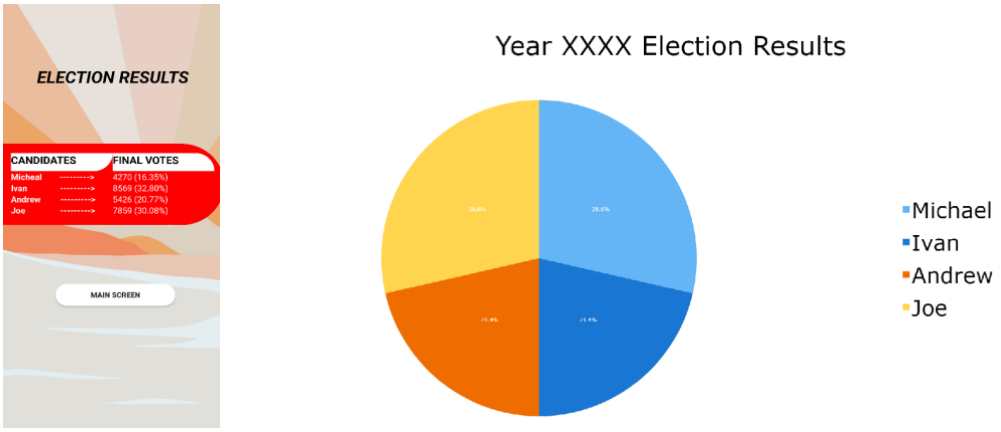


Figure 15. *Result screens on the mobile application and the Web site*

With this proposed system, it is shown that potential frauds are eliminated since it lays on a distributed network rather than a central single server. Hacking attempts are also prevented by the RSA based additional security procedure between the client and the server side. With the developed easy-to-use mobile and Web applications, voters are encouraged to participate in the elections. Even for the people who feel distant from using technology, the same Blockchain based security is still provided.

VI. CONCLUSION

In this study, VOTEMAT, a Blockchain based voting system, which covers both traditional paper ballot and electronic voting with additional RSA based security is proposed. An Ethereum private network implementation of HB is used as the Blockchain infrastructure.

The electronic voting part of the proposed system is more efficient, less costly, and faster than the traditional voting systems since it is composed of an easy-to-use mobile application or Web site. As there is no need to go to the polling station or there is no queuing at the polling station, people with mobility problems or time problems can also participate in the election which can increase the participation rates. The traditional part of the proposed system on the other hand, welcomes the voters who are not familiar or comfortable with the technology. Both of these ways of voting end up votes being stored securely and immutably in the same Blockchain; therefore, the known problems and threats that come with the election systems can be avoided.

The proposed Blockchain based system is nearly impossible to tamper with by nature because it consists of cryptographic chains of blocks that connect to the block that has come before them. Moreover, votes are encrypted by the RSA algorithm on the client side before being sent to the server side. This additional security measure protects the system from the man in the middle attacks. With the proposed system having a distributive ledger and decentralized network, a great deal of transparency is also provided which leads to a better traceability for the voting process as a whole.

Voter privacy and secrecy are essential to the integrity of the elections. Although voters have right to vote without intimidation or retaliation, in case of e-voting, there are some unavoidable risks. Coercion,

vote selling, and vote solicitation are among such risks. As mitigations, front-end application might require silence during the voting and stop working if there is a sound, and taking screenshots might be disabled, etc. However, fundamentally it should be the citizen's responsibility to protect their votes. Moreover, in many modern democracies, people vote by post, which has similar risks, but still used widely.

Blockchain technology is still a relatively new and rapidly evolving field, and it is not yet clear how it will be regulated and governed. This lack of legal certainty could create challenges for the implementation and acceptance of Blockchain based voting systems. To ensure legal and regulatory compliance, this kind of system needs to be developed with an understanding of existing laws and regulations and comply with them. A clear governance structure, risk management and compliance processes should be established and followed in the works to be performed in this field in the near future.

VII. REFERENCES

[1] M. Karakuş, "Implementation of blockchain-assisted source routing for traffic management in software-defined networks," *DÜBİTED*, vol. 11, no. 3, pp. 1250–1268, 2023, doi: 10.29130/dubited.1209656.

[2] N. Jam and K. Kalkan, "HungerHash: A distributed network for child-hunger relief based on Hedera Hashgraph," *DÜBİTED*, vol. 10, no. 3, pp. 1408–1422, 2022, doi: 10.29130/dubited.933171.

[3] K. Adıgüzel ve N. Krasnokutska, "Re-establishment and regarding trust and transparency, blockchain's contribution to the solution of a thousand-year problem," *DÜBİTED*, vol. 9, no. 4, pp. 1020–1040, 2021, doi: 10.29130/dubited.868598.

[4] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain: Research and Applications*, vol. 3, no. 2, 100067, 2022, doi: 10.1016/j.bcra.2022.100067.

[5] "Blockchain Technology for Voting Systems," All Answers Ltd., Nottingham, UK. Accessed: Mar. 10, 2024. [Online]. Available: https://www.ukessays.com/essays/information-technology/blockchain-technology-for-voting-systems.php.

[6] U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system-review and open research challenges," *Sensors*, vol. 21, no. 17, p. 5874, 2021, doi: 10.3390/s21175874.

[7] Hyperledger Besu Documentation, *Creating a Private Network with IBFT*. (2023). Accessed: Mar. 10, 2024. [Online]. Available: https://besu.hyperledger.org/en/stable/private-networks/tutorials/ibft/.

[8] M. Chaieb, S. Yousfi, P. Lafourcade, and R. Robbana, "Verify-Your-Vote: A verifiable blockchain-based online voting protocol," in *EMCIS 2018*, M. Themistocleous, P. Rupino da Cunha, Eds. 2019, pp. 16–30, doi: 10.1007/978-3-030-11395-7_2.

[9] E. Yavuz, A. K. Koç, U. C. Çabuk and G. Dalkılıç, "Towards secure e-voting using ethereum blockchain," in *6th International Symposium on Digital Forensic and Security (ISDFS)*, Antalya, Turkey, 2018, pp. 1-7, doi: 10.1109/ISDFS.2018.8355340.

[10] D. Pawar, P. Sarode, S. Santpure and P. Thore, "Secure voting system using blockchain," *International Journal of Engineering Research and Technology (IJERT)*, vol. 8, no. 11, pp. 817-819, 2019.

[11] M. Pawlak, A. Poniszewska-Maranda, and N. Kryvinska, “Towards the intelligent agents for blockchain e-voting system,” *Procedia Computer Science*, vol. 141, pp. 239-246, 2018, doi: 10.1016/j.procs.2018.10.177.
[12] P. McCorry, S. F. Shahandashti and F. Hao, “A smart contract for boardroom voting with maximum voter privacy,” in *Financial Cryptography and Data Security: 21st International Conference, FC 2017*, Sliema, Malta, April 3–7, 2017, pp. 357–375, doi: 10.1007/978-3-319-70972-7_20.

[13] K. Garg, P. Saraswat, S. Bisht, S. K. Aggarwal, S. K. Kothuri and S. Gupta, "A comparitive analysis on e-voting system using blockchain," in *4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, Ghaziabad, India, 2019, pp. 1-4, doi: 10.1109/IoT-SIU.2019.8777471.

[14] S. Al-Maaitah, M. Qatawneh, and A. Quzmar, “E-voting system based on blockchain technology: a survey,” in *2021 International Conference on Information Technology (ICIT)*, Jul. 14, 2021. doi: 10.1109/icit52682.2021.9491734.

[15] S. Singh, S. Bansal, and S. Semwal, “Blockchain based decentralized e-voting system : a survey,” *SSRN Electronic Journal*, 2024, doi: 10.2139/ssrn.4495873.

[16] M. Hajian Berenjestanaki, H. R. Barzegar, N. El Ioini, and C. Pahl, “Blockchain-based e-voting systems: a technology review,” *Electronics*, vol. 13, no. 1, p. 17, 2023, doi: 10.3390/ electronics13010017.

[17] A. K. Yadav, H. O. Patel and S. Kumar, “Blockchain-based e-voting system,” *International Journal of Innovative Science and Modern Engineering*, vol. 11, no. 7, pp. 1-5, 2023, doi: 10.35940/ijisme.b7801.0711723.

[18] R. Bulut, A. Kantarci, S. Keskin, and S. Bahtiyar, “Blockchain-based electronic voting system for elections in Turkey,” in *4th International Conference on Computer Science and Engineering (UBMK)*, Sep. 2019, doi: 10.1109/ubmk.2019.8907102.

[19] M. Malkawi, M. Bani Yaseen, and D. Habeebalah, “Ethereum blockchain based e-voting system for Jordan parliament elections,” *Applied Mathematics & Information Sciences*, vol. 17, no. 2, pp. 233-241, 2023, doi: 10.18576/amis/170206.

[20] S. Tanwar, N. Gupta, P. Kumar, and Y.-C. Hu, “Implementation of blockchain-based e-voting system,” *Multimedia Tools and Applications*, vol. 83, no. 1, pp. 1449-1480, 2023, doi: 10.1007/s11042-023-15401-1.

[21] H. Hassan, R. Hassan, and E. Gbashi, “E-voting system based on Ethereum blockchain technology using ganache and remix environments,” *Engineering and Technology Journal*, vol. 41, no. 4, pp. 1-16, 2023, doi: 10.30684/etj.2023.135464.1273.

[22] M. S. Farooq, U. Iftikhar and A. Khelifi. “A framework to make voting system transparent using blockchain technology”, *IEEE Access*, vol. 10, p. 59959, 2022, doi: 10.1109/ACCESS.2022.3180168.

[23] A. Ben Ayed, “A conceptual secure Blockchain-based electronic voting system”, *Int. J. Network Security & Its Applications*, vol.9, no. 3, 2017, doi: 10.5121/ijnsa.2017.9301.

[24] U. Jafar, M. J. Ab Aziz, and Z. Shukur, “Blockchain for electronic voting system - review and open research challenges,” *Sensors*, vol. 21, no. 17, p. 5874, 2021, doi: 0.3390/s21175874.

[25] A. Singh and K. Chatterjee, “SecEVS : Secure electronic voting system using blockchain technology,” in *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*, Sep. 2018, doi: 10.1109/gucon.2018.8675008.

[26] S. S. Gandhi, A. W. Kiwelekar, L. D. Netak, and H. S. Wankhede, “Security requirement analysis of blockchain-based e-voting systems,” arXiv, 2022, doi: 10.48550/ARXIV.2208.01277.
[27] İ. Sertkaya, P. Roenne, and P. Y. A. Ryan, “Estonian Internet voting with anonymous credentials,” *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 30, no. 2, pp. 420-435, 2022. doi: 10.3906/elk-2105-197.

[28] G. G. Dagher, P. B. Marella, M. Milojkovic, and J. Mohler, “Broncovote: secure voting system using Ethereum’s blockchain,” in *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 2018, doi: 10.5220/0006609700960107.

[29] “Secure Decentralized Application Development,” Follow My Vote. https://followmyvote.com/ (accessed Mar. 10, 2024).

[30] “Voatz Secure and Convenient Voting Anywhere,” Voatz. https://voatz.com (accessed Mar. 10, 2024).

[31] N. Gailly, P. Jovanovic, B. Ford, J. Lukasiewicz, L. Gammar, “Agora: Bringing our voting systems into the 21st century,” 2017. [Online]. Available: https://cryptopapers.info/agora/.

[32] “Polys-Online Voting System,” Polys Vote, https://polys.me (accessed Jan. 11, 2023).

[33] “Why Hyperledger Besu is a Top Choice for Financial Use Cases,” Hyperledger. https://www.hyperledger.org/blog/why-hyperledger-besu-is-a-top-choice-for-financial-use-cases (accessed Apr. 29, 2024).

[34] H. Dang, T. T. A. Dinh, , D. Loghin, E. C. Chang, Q, Lin, and B. C. Ooi, “Towards scaling blockchain systems via sharding,” in *Proceedings of the 2019 International Conference on Management of Data*, 2019, pp. 123-140.

[35] EthSigner Documentation. *Start EthSigner*. (2023). Accessed: Mar. 10, 2024. [Online]. Available: https://docs.ethsigner.consensys.net/Tutorials/Start-EthSigner.

[36] Hyperledger Besu Documentation. *Privacy in Hyperledger Besu*. (2023). Accessed: Mar. 10, 2024. [Online]. Available: https://besu.hyperledger.org/en/stable/private-networks/tutorials/privacy/.