ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL

BLOCKCHAIN BASED SECURE AND TRUSTWORTHY E-GOVERNMENT ARCHITECTURE

M.Sc. THESIS

Mustafa TOSUN

Department of Computer Engineering

Computer Engineering Programme

JUNE 2025

ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL

BLOCKCHAIN BASED SECURE AND TRUSTWORTHY E-GOVERNMENT ARCHITECTURE

M.Sc. THESIS

Mustafa TOSUN
(504221525)

Department of Computer Engineering

Computer Engineering Programme

Thesis Advisor: Prof. Dr. Şerif BAHTİYAR

JUNE 2025

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BLOCKCHAIN TABANLI GÜVENLİ VE GÜVENİLİR E-DEVLET MİMARİSİ

YÜKSEK LİSANS TEZİ

Mustafa TOSUN
(504221525)

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Programı

Tez Danışmanı: Prof. Dr. Şerif BAHTİYAR

HAZİRAN 2025

Mustafa TOSUN, a M.Sc. student of ITU Graduate School student ID 504221525 successfully defended the thesis entitled "BLOCKCHAIN BASED SECURE AND TRUSTWORTHY E-GOVERNMENT ARCHITECTURE", which he/she prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

Thesis Advisor :	**Prof. Dr. Şerif BAHTİYAR** Istanbul Technical University	.....
Jury Members :	**Prof. Dr. Sıddıka Berna ÖRS YALÇIN** Istanbul Technical University	.....
	Asst. Prof. Ebu Yusuf GÜVEN Istanbul University - Cerrahpaşa	.....

Date of Submission : **28 May 2025**
Date of Defense : **27 June 2025**

Aileme,

FOREWORD

I am very grateful to my advisor Prof. Dr. Şerif Bahtiyar for his support to me and help throughout my academic career.

I thank to my family for their unconditional support throughout my life. Thanks to them, I learned to pursue my dreams and fulfill my dreams in reality.

June 2025 Mustafa TOSUN

TABLE OF CONTENTS

ABBREVIATIONS

DID	**:** Decentralized identifier
ECDSA	**:** Elliptic Curve Digital Signature Algorithm
ID	**:** Identifier
P2P	**:** Peer-to-peer
PDF	**:** Portable Document Format
PoS	**:** Proof of Stake
PoW	**:** Proof of Work

SYMBOLS

E(ID) **:** Encrypted Identifier
H(ID) **:** Hashed Identifier

LIST OF FIGURES

BLOCKCHAIN BASED SECURE AND TRUSTWORTHY E-GOVERNMENT ARCHITECTURE

SUMMARY

One of the most transformative aspects of the digital age has been the migration of public services to online platforms. Over the past two decades, many countries have developed e-government infrastructures to allow their citizens to access state services through the internet. These services range from accessing official documents to applying for public benefits, and in some countries, even voting in elections. However, current e-government systems are largely built on centralized infrastructures. While this structure may offer simplicity in management, it also introduces several risks and limitations in terms of security, data integrity, transparency, and user privacy.

This thesis proposes a novel e-government system architecture that leverages blockchain technology to overcome the key challenges of conventional systems. Blockchain's decentralized, immutable, and transparent nature offers a solid foundation to rebuild trust between governments and citizens in the digital era. The proposed system consists of three main modules: Identity Management, Electronic Voting, and Credential Verification. Each module addresses one of the core functions of e-government and aims to provide a secure, privacy-respecting, and efficient public service model.

Motivation and Problem Definition Traditional e-government systems rely on centralized databases and servers. While this centralization enables easier administration and control, it also introduces several vulnerabilities:

- Single points of failure: A cyberattack or system malfunction could compromise the entire infrastructure.
- Data manipulation risk: Since data is managed by a central authority, there is a risk of unauthorized alteration, especially in sensitive operations like voting.
- Lack of user privacy: Personal information and activity logs are often stored without sufficient safeguards, potentially leading to surveillance or data misuse.
- Low transparency: Citizens generally have no means of independently verifying how the system operates or whether the data has been tampered with.

Therefore, a new paradigm is needed to ensure trust, security and transparency. Blockchain technology is uniquely positioned to meet these needs due to its decentralized consensus model, cryptographic security, and tamper-proof data storage.

The proposed blockchain-based e-government system is composed of three integrated modules, each responsible for a key public service area.

The first module in the proposed system is e-voting to run elections securely through online platforms. Voting is one of the most sensitive and foundational elements of democratic governance. However, the adoption of digital voting has been hampered by concerns over vote tampering, lack of transparency, and breach of ballot secrecy.

The e-voting module designed in this system provides a secure, transparent, and verifiable voting environment. Citizens cast encrypted votes, which are stored immutably on the blockchain. The encryption ensures that votes remain private, while the blockchain ensures that they cannot be altered or deleted.

Once the election period concludes, a secure decryption mechanism allows for public tallying of votes. This model ensures that all participants—and even third-party observers—can verify the election results independently, thereby increasing trust in the democratic process and removing the need for blind faith in centralized authorities.

The second module in the proposed system is credential verification which provides validation of documents such as diplomas, licenses, or certificates. Credential verification is a common requirement in public services. Currently, such validations depend on querying centralized databases or physical documents, both of which are inefficient and vulnerable to forgery.

In the credential verification module, each document is hashed and recorded on the blockchain during issuance. Later, when a user presents a credential, the system calculates its hash and compares it to the blockchain entry. If the hashes match, the document is validated.

This approach offers numerous advantages:

- Prevents forgery and tampering,
- Speeds up cross-institutional verification,
- Allows users to share proof of their credentials securely without disclosing unnecessary personal information.

The system proposed in this thesis introduces both technical and societal innovations:

- Decentralization eliminates single points of failure and enhances system resilience.
- Privacy-centric identity verification empowers citizens to control their own data.
- Transparent and verifiable digital elections improve democratic participation.
- Tamper-proof credential validation boosts trust in public institutions.

The modular architecture allows easy integration into existing infrastructures. Furthermore, the system is designed to be scalable and interoperable with international standards and regulations, making it adaptable across different governmental contexts.

This thesis presents a forward-thinking approach to modernizing e-government infrastructure through blockchain technology. The proposed system demonstrates that it is possible to offer secure, user-friendly, and trustworthy digital public services without compromising privacy or transparency.

Looking ahead, this system can be expanded with advanced technologies such as:

- Decentralized Identity (DID) management
- Smart contract-based public service automation,
- DAO-like citizen engagement platforms,

Thus, this study not only proposes a working technical framework but also lays the groundwork for rethinking governance in the age of decentralization.

BLOCKCHAIN TABANLI GÜVENLİ VE GÜVENİLİR E-DEVLET MİMARİSİ

ÖZET

Dijital çağın getirdiği en önemli dönüşümlerden biri, kamu hizmetlerinin dijital platformlar üzerinden sunulmasıdır. Özellikle son yirmi yılda birçok ülke, vatandaşlarının devlet hizmetlerine internet üzerinden erişebilmesi için çeşitli e-devlet sistemleri geliştirmiştir. Bu sistemler sayesinde bireyler resmi belgelere ulaşabilmekte, devlet kurumlarına başvuruda bulunabilmekte, hatta bazı ülkelerde oy kullanabilmektedir. Ancak mevcut e-devlet uygulamaları, büyük oranda merkezi altyapılar üzerine kuruludur. Bu durum, sistemlerin güvenliği, veri bütünlüğü ve kullanıcı gizliliği açısından önemli zaaflar doğurmakta; özellikle de devlet-vatandaş ilişkilerinde güven bunalımına neden olabilmektedir.

Bu tez çalışması, blockchain teknolojisinin merkeziyetsiz, şeffaf ve güvenilir yapısından faydalanarak, geleneksel e-devlet uygulamalarında karşılaşılan temel sorunlara çözüm sunmayı amaçlamaktadır. Tez kapsamında geliştirilen sistem, üç temel modülden oluşmaktadır: Kimlik Yönetimi, Elektronik Oylama ve Belge Doğrulama. Bu modüller, e-devlet işlevlerinin en temel alanlarını oluşturmaktadır ve her biri kamu hizmetlerinin daha güvenli, hızlı ve kullanıcı dostu hale gelmesine katkıda bulunacak şekilde yeniden tasarlanmıştır.

Mevcut e-devlet sistemleri genellikle merkezi veri tabanları üzerine kuruludur. Bu yapı, ilk bakışta yönetim kolaylığı sağlasa da birçok riski beraberinde getirmektedir:

- Veri güvenliği: Merkezi sistemler tekil arıza noktalarına sahiptir. Bu da, sistemin saldırıya uğraması durumunda tüm verilerin açığa çıkmasına veya kaybolmasına neden olabilir.
- Manipülasyon riski: Veriler belirli bir kurum veya otorite tarafından değiştirilebilir. Bu durum, özellikle oylama gibi kritik işlemlerde güven sorununa yol açmaktadır.
- Gizlilik eksikliği: Kullanıcıların kimlik bilgileri ve işlem geçmişi merkezi sistemlerde saklandığı için, bu verilerin üçüncü şahıslarla paylaşılması veya izinsiz kullanımı mümkündür.
- Şeffaflık eksikliği: Vatandaşlar, sistemin nasıl çalıştığını ve işlemlerin nasıl yürütüldüğünü doğrudan göremez. Bu da devlet-vatandaş ilişkisinde şeffaflık ilkesine zarar verir.

Bu nedenlerle, daha güvenli, şeffaf, merkeziyetsiz ve kullanıcı gizliliğini önceleyen yeni bir e-devlet mimarisine ihtiyaç duyulmaktadır. Blockchain teknolojisi, bu ihtiyaçlara doğrudan yanıt verebilecek niteliklere sahiptir.

Tezde geliştirilen sistem, iki ana modülden oluşmakta ve bu modüller birlikte çalışarak bütünsel bir e-devlet deneyimi sunmaktadır.

Demokratik toplumlarda oy kullanma, vatandaşların en temel haklarından biridir. Ancak dijital oylama sistemlerinin güvenliği, şeffaflığı ve gizliliği konusundaki endişeler nedeniyle birçok ülke bu teknolojilere temkinli yaklaşmaktadır. Mevcut oylama sistemlerinin çoğu, sonuçların doğrulanabilirliğini ve oy gizliliğini aynı anda sağlayamamaktadır.

Tez kapsamında geliştirilen elektronik oylama modülü, blockchain'in şeffaflık, değiştirilemezlik ve doğrulanabilirlik gibi avantajlarını kullanarak güvenli bir dijital seçim ortamı sunmaktadır. Seçmenler, sisteme giriş yaptıktan sonra kendilerine ait oylarını şifreleyerek ağ üzerinde yayınlamaktadır. Oyların şifreli şekilde blockchain'e kaydedilmesi, hem seçmenin tercihinin gizli kalmasını hem de sistem dışı müdahalelere karşı korunmasını sağlamaktadır.

Oylama süreci sona erdiğinde, sistem tarafından güvenli biçimde açılan oylar herkes tarafından doğrulanabilir şekilde sayılır. Bu sayede, seçim sonuçlarına olan güven artar, herhangi bir manipülasyon olasılığı ortadan kalkar ve sistem hem demokratik hem teknik açıdan güçlü bir altyapıya kavuşur.

Kamu hizmetlerinde sık karşılaşılan bir başka ihtiyaç da diploma, ruhsat, sertifika gibi belgelerin doğrulanmasıdır. Günümüzde bu belgeler genellikle kurumların veri tabanlarında saklanmakta ve bu veri tabanlarına erişim yoluyla doğrulama sağlanmaktadır. Ancak bu yaklaşım hem zaman kaybına neden olmakta hem de belge sahteciliğine açık bir zemin oluşturmaktadır.

Bu çalışmada sunulan belge doğrulama modülü, belgelerin doğrudan blockchain üzerinde doğrulanmasını mümkün kılmaktadır. Belgeler, zincir üzerine kaydedilmeden önce özetlenmekte ve bu özet değerler (hash'ler) zincire yazılmaktadır. Daha sonra, bir kullanıcı bir belge sunduğunda sistem, belgeye ait yeni bir özet hesaplayarak zincir üzerindeki kayıtla karşılaştırmaktadır. Eğer özet değerleri uyuşuyorsa, belgenin geçerli olduğu anlaşılmaktadır.

Bu sistem sayesinde:

- Belgelerin sahteciliği önlenir.
- Kurumlar arasında belge transferi ve onay süreci hızlanır.
- Vatandaşlar belgelerini üçüncü kişilere güvenli biçimde sunabilir.
- Ayrıca sistem, veri mahremiyetini korumak için yalnızca özet verilerle işlem yaptığından, herhangi bir özel belge içeriği kamuya açık hale getirilmeden doğrulama mümkün olmaktadır.

Tez kapsamında geliştirilen sistem, hem teknolojik hem de toplumsal açıdan birçok katkı sunmaktadır:

- Merkeziyetsizlik sayesinde tekil arıza noktaları ortadan kaldırılır; sistem, bir kurumun kontrolüne bağlı kalmadan çalışabilir.

- Gizlilik odaklı kimlik doğrulama ile vatandaşlar kişisel bilgilerini açıklamak zorunda kalmadan kamu hizmetlerinden yararlanabilir.
- Şeffaf ve güvenli seçim ortamı, dijital demokrasinin gelişmesine katkıda bulunur.
- Belge sahteciliğine karşı etkili koruma, kamu hizmetlerinde güveni artırır.

Bu tez çalışması, blockchain teknolojisinin e-devlet sistemlerine entegrasyonu konusunda bütüncül ve yenilikçi bir çözüm sunmaktadır. Geliştirilen modüller, geleneksel kamu hizmetlerinde karşılaşılan güvenlik ve şeffaflık problemlerini ortadan kaldırmakta; devlet-vatandaş ilişkisini daha eşit, güvenilir ve şeffaf bir temele oturtmaktadır.

Gelecekte bu sistemin;

- Merkeziyetsiz kimlik yönetimi (DID),
- Akıllı sözleşmelere dayalı otomatik kamu hizmetleri,
- Otonom vatandaş katılım platformları (DAO temelli altyapılar) ile entegre edilmesi mümkün gözükmektedir.

Bu yönüyle tez çalışması, sadece teknik bir sistem önerisi değil, aynı zamanda geleceğin dijital kamu yönetimi anlayışına dair vizyoner bir adım niteliği taşımaktadır.

1. INTRODUCTION

Governments around the world are increasingly adopting digital technologies to deliver public services more efficiently, securely, and transparently. These digital transformations, collectively referred to as e-government systems, aim to streamline administrative processes, reduce bureaucracy, and increase citizen participation. However, traditional e-government infrastructures often rely on centralized architectures, which pose significant challenges in terms of data privacy and trust.

Blockchain technology, with its inherent properties of decentralization, transparency, and immutability, offers promising solutions to the limitations of conventional e-government systems. By leveraging blockchain, it is possible to create tamper-resistant records, perform secure identity verification, and enable trustless interactions between citizens and institutions.

This study proposes a blockchain-based e-government framework that integrates multiple essential services, including secure identity management, electronic voting (e-voting), and document validation using digital signatures. The proposed system enables citizens to participate in elections anonymously while ensuring the authenticity and integrity of each vote. In addition, users can prove their eligibility for services (e.g., being part of a whitelist or above a certain age) without revealing sensitive personal information, and can present signed legal documents (e.g. diploma, certification) that are verifiable through blockchain.

By combining advanced cryptographic techniques with decentralized architectures, this study aims to contribute a secure and privacy-preserving e-government framework suitable for future digital democracies.

2. LITERATURE REVIEW AND BACKGROUND INFORMATION

2.1 Blockchain

Blockchain is a distributed ledger technology that enables the secure recording of transactions in a decentralized, tamper-resistant manner. It eliminates the need for a central trusted authority by allowing network participants to reach a consensus on the state of the data. This makes blockchain particularly suitable for applications that require transparency, auditability, and data integrity—key requirements in modern e-government systems.

At its core, a blockchain consists of a chain of blocks, where each block contains a batch of transactions and is cryptographically linked to the previous one. This structure ensures immutability and chronological order, meaning once a block is added to the chain, its contents cannot be altered without redoing the work for all subsequent blocks.

2.1.1 Structure of a block

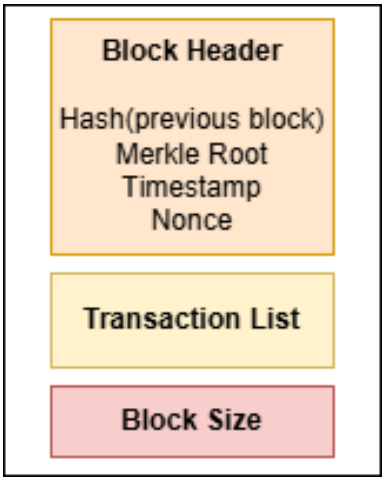

Figure 2.1: Structure of a Block

Structure of a block in a blockchain is shown in 2.1. Each block in a blockchain is composed of 3 main components which are block header, transaction list and the block size. These components are explained in details as follows:

- **Block Header:** Contains metadata about the block and is essential for maintaining the integrity and traceability of the blockchain. The block header typically includes:
  - Previous Block Hash: A cryptographic hash of the previous block's header, which links the current block to its predecessor.
  - Merkle Root: The root of a Merkle tree built from the hashes of all transactions in the block. This enables efficient and secure verification of individual transactions.
  - Timestamp: The time when the block was created.
  - Nonce: A number used once, which is varied during the mining process to satisfy the conditions of the consensus algorithm (e.g., proof of work).
- **Transaction List:** Contains all the transactions included in the block. Each transaction is digitally signed and may include information such as sender, receiver, amount, and additional metadata.
- **Block Size:** Specifies the size of the block, which can affect the number of transactions that can be stored and the speed of block propagation across the network.

2.1.2 Blockchain structure

A blockchain is essentially a linear, chronological chain of blocks as can be seen in 2.2. Each block references the hash of the previous one. This creates a secure and verifiable chain of records.

The first block in the blockchain is called the genesis block. It is hardcoded into the system and does not reference any previous block.

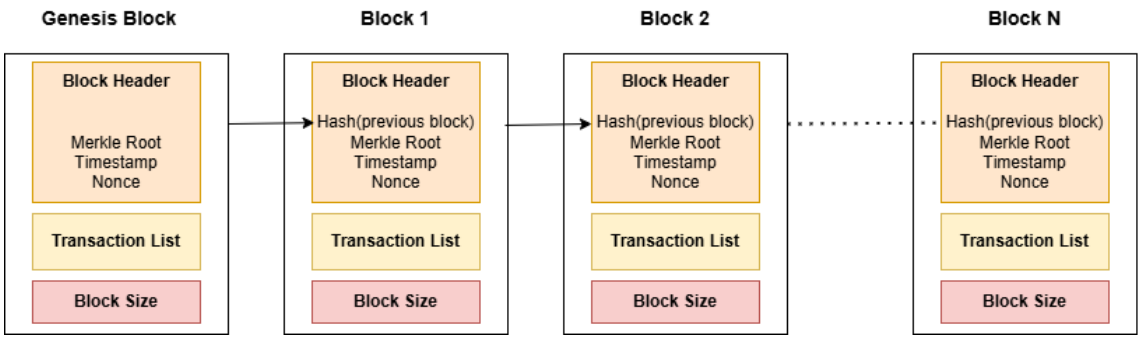

Figure 2.2: Structure of Blockchain

2.1.3 Hashing and immutability

Each block's hash is generated based on its content (including the previous block's hash), forming a unique digital fingerprint. If any data in a block is tampered with, its hash will change, breaking the chain unless every subsequent block is recalculated, which is computationally infeasible in large-scale networks. This cryptographic linking ensures immutability, which is critical in trustless environments such as decentralized voting systems and identity management in e-government applications.

2.1.4 Distributed and peer-to-peer architecture

In a blockchain network, each node in the network maintains a copy of the blockchain. These nodes operate in a peer-to-peer (P2P) manner.

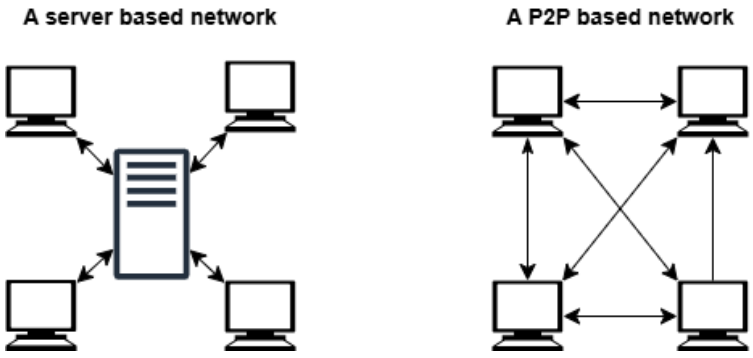

Figure 2.3: P2P Network

Instead of relying on a central server, as shown in Figure 2.3 each node has direct connections between them. With the help of that P2P connections, each node broadcasts new transactions and blocks to each other. Consensus algorithms which are explained in section 2.1.7 ensure that all honest nodes agree on the current state of the ledger, even in the presence of faults or malicious actors.

2.1.5 Smart contracts and programmability

Modern blockchains like Ethereum support smart contracts which are self-executing programs stored on the blockchain that automatically enforce rules and trigger actions based on predefined conditions.

Ethereum provides functionalities including smart contracts and decentralized applications [1]. Smart contracts have the capacity to create trust in no-trust contracting contexts [2,3]. In e-government systems, smart contracts can automate processes such as license renewals, tax payments, and eligibility checks, thereby improving efficiency and reducing bureaucracy.

2.1.6 Classification of blockchain networks

Blockchain networks can be classified into several types based on their accessibility.

2.1.6.1 Public blockchain

Public blockchains are open and permissionless networks where anyone can join, read, write, and participate in the consensus process. These blockchains are fully decentralized and provide high transparency and immutability. Examples include Bitcoin and Ethereum. However, their openness can lead to scalability and privacy concerns, making them less suitable for certain government applications.

2.1.6.2 Private blockchain

Private blockchains are permissioned networks controlled by a single organization. Only authorized participants can access and interact with the network. These

blockchains offer greater control, efficiency, and privacy compared to public blockchains, but they are less decentralized.

2.1.6.3 Consortium blockchain

Consortium blockchains are semi-decentralized networks where multiple organizations share control. Access and consensus responsibilities are distributed among a pre-selected group of nodes. This model combines elements of both public and private blockchains, offering a balance between transparency, scalability, and governance. For e-government, consortium blockchains are suitable for inter-agency cooperation and collaborative public services.

2.1.6.4 Hybrid blockchain

Hybrid blockchains integrate features of both public and private blockchains. They allow certain data to be made public while keeping other data private. This flexibility is advantageous in e-government systems, where some services require public transparency (e.g., voting results) while others demand privacy (e.g., citizen records).

2.1.7 Blockchain consensus mechanisms

Consensus mechanisms are protocols used by blockchain networks to achieve agreement on the state of the ledger. They ensure that all participants in the network validate transactions and blocks without relying on a central authority.

2.1.7.1 Proof of work

Proof of Work (PoW) is the original consensus algorithm introduced by Bitcoin. In PoW, participants known as miners solve complex cryptographic puzzles to validate transactions and add new blocks to the blockchain. The first miner to solve the puzzle is rewarded. While PoW offers high security and decentralization, it is computationally intensive and energy-consuming, making it less desirable for large-scale governmental applications.

2.1.7.2 Proof of stake

Proof of Stake (PoS) is an alternative consensus mechanism that selects validators based on the number of tokens they hold and are willing to "stake" as collateral. PoS significantly reduces energy consumption compared to PoW and improves transaction throughput. Variants such as Delegated Proof of Stake (DPoS) and Practical Byzantine Fault Tolerance (PBFT) further enhance efficiency and are often preferred for permissioned blockchain applications like e-government systems.

2.2 Merkle Tree

Merkle Tree is a binary tree structure. As can be seen in Figure 2.4, each non-leaf node contains the hash of it's children's data. Whenever a child node is tampered, since the parent node does not contain updated data, it will be detected from the Merkle Tree.

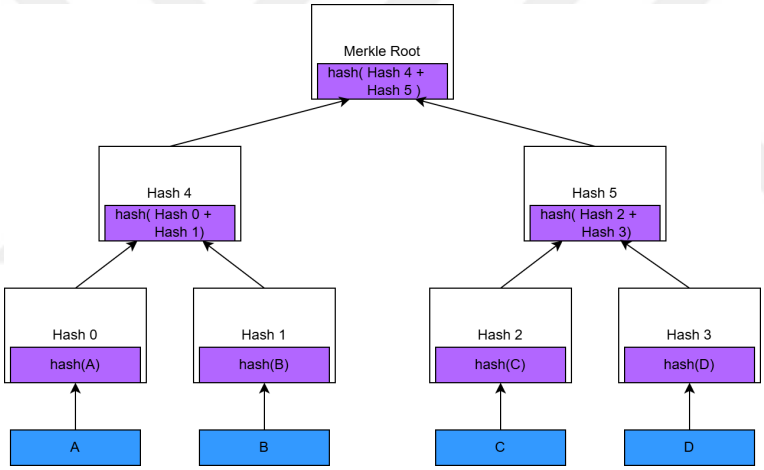

Figure 2.4: Merkle Tree

Merkle trees can be used in data verification. For verification, it required to know Merkle Root and Merkle Proof. For example if it is wanted to check Block C in the Tree in Figure 2.4, it is enough to know Hash 3 and Hash 4, which is the Merkle Proof. When we go up from down by hashing the blocks, we get a final hash. If this hash is equal to Merkle Root, than the data is verified.

2.3 Current E-Government Applications

E-government initiatives have been widely adopted to enhance the efficiency, transparency, and accessibility of public services. Countries like Estonia have pioneered digital governance, offering services such as online voting, digital identity verification, and electronic tax filing. However, traditional e-government systems often rely on centralized architectures, which can pose risks related to data security, single points of failure, and limited transparency. These challenges underscore the need for more secure and decentralized solutions in public administration.

2.4 Integration of Blockchain into E-Government Systems

Blockchain technology, characterized by its decentralized and immutable ledger, presents promising solutions to the limitations of conventional e-government systems. Recent studies have explored the application of blockchain in various governmental functions, including identity management, voting, and document verification.

For instance, Mansour et al. (2023) conducted a comprehensive survey on the status and challenges of blockchain in e-government services, highlighting its potential to enhance data integrity and trust in public [4]. Similarly, Chouhan and Sharma (2025) proposed a blockchain-based voting system that leverages digital identity verification and biometric authentication to ensure secure and transparent elections [5].

Blockchain based e-voting systems have been a hot research topic for many years due to ability of blockchain to enhance transparency, security, and integrity in digital voting. [6]. Kumar et al. proposed a secure decentralized E-Voting system with blockchain and smart contracts [7]. In this research, voter registration has been done by voters themselves using the application. After that, the admin can accept or discard the registration of users. The election result is sent to the voters via email. However, voters cannot verify their vote. Thus, transparency is not provided in this study.

In 2023, Malkawi et al. published a study which secures the e-voting using blockchain [8]. The system uses Ethereum based blockchain network with metamask wallets. After the election is finalized, results are tallied by smart contract. The contract

publishes results for each candidate publicly. Each candidate can check their wallet to learn how much votes they have obtained. However, votes cannot be verified by the voters in this system.

An architecture with blockchain for e-voting is proposed by Mullegowda et al. [9]. The system contains a side-chain network to increase the data security of the main blockchain network. In this system, a vote is encrypted by the public key of the election commissioner and the encrypted vote is stored in a side-chain. Main blockchain decrypts the encrypted vote. After the election is completed, the election commissioner enters his private key into system. Voting smart contract decrypts all encrypted votes. In this system, it is not possible to see votes during the election. Votes can be counted only with the private key of the election commissioner. Since transparency is not fully provided, it may reduce the trustworthiness of the system.

A blockchain based cryptographic algorithm for data protection in an e-voting system is proposed by Vinayachandra and Krishna [10]. To improve reliability and privacy, an e-voting system which combines AES and RSA encryption algorithms with blockchain is implemented. Credentials of the voter is encrypted with hybrid AES-RSA system and ciphertext is sent to the blockchain. Blockchain decrypts the ciphertext and it verifies the user. Since RSA is an asymmetric cryptography algorithm, it is important to securely store and distribute cryptographic keys for each voter. These researches show that existing blockchain based e-voting systems do not satisfy all requirements for having trustworthy and transparent voting.

Despite these advancements, challenges remain in integrating blockchain into e-government, such as ensuring legal compliance, scalability, and user privacy. Mustafa et al. (2025) emphasized the importance of developing comprehensive governance models that address legal, technical, ethical, and security considerations in blockchain-based e-government systems [11].

2.5 Contributions of the Proposed System

Building upon existing research, our proposed blockchain-based e-government system introduces several novel features:

- Decentralized Certificate Verification: By utilizing digital signatures and storing credentials on the blockchain, proposed system allows for the secure and tamper-proof verification of academic qualifications.
- Integrated E-Voting Mechanism: Proposed e-government architecture incorporates a secure e-voting module that ensures vote integrity and anonymity, addressing common concerns in electronic voting systems.

These features collectively contribute to a more secure, transparent, and user-centric e-government system, addressing the limitations of current applications and aligning with the evolving needs of digital governance.

3. SYSTEM DESIGN

This section describes the overall architecture and components of the proposed blockchain-based e-government system. The system is composed of two main components: E-Voting and Credential Verification. Both components leverages cryptographic primitives and blockchain technologies to ensure security, transparency, and user privacy.

3.1 E-Voting

Since elections has a huge impact on a community, they need to be organized in a trustworthy way. In addition to trust challenges about traditional voting systems, it is also expensive process to run an election for a state. The cost of an election may get higher according to several parameters. In 2019, elections in Canada cost $502.4 million. Two years later, in 2021 elections, the cost was $610 million [12].

An e-voting system may eliminate all these problems. However, the voting system, which is very important in the structure of society, needs to be regulated securely. In order to ensure security in the e-voting system, the following requirements must be satisfied:

- Eligibility: Only eligible people have the right to vote.
- Immutability: The submitted vote must not be changed in any way without the consent of the voter.
- Anonymity: The identity of the voter must remain confidential and the voter's decision must remain confidential.
- Transparency: All votes cast must be publicly visible. This ensures the reliability of the selection.

Blockchain is a pretty good solution to provide reliability of an election. Since the nature of a blockchain provide eligibility, transparency, anonymity, and integrity, it will fulfill the necessary requirements to organize an trustworthy election. Since blockchain is a decentralized network, it eliminates the need for a central authority for counting and validating the votes. Therefore, blockchain network prevents single point of failure and enhances the robustness of the system [13].

Proposed e-voting architecture provides a secure, anonymous, immutable and verifiable way for users to participate in digital elections which satisfies all the requirements for an elections with a reduced cost. The proposed system can be implemented according to requirements of different countries.

3.1.1 Eligibility

It is important in a voting system to provide an architecture that allows only eligible users to vote. To provide eligibility, the system needs an identity number and a password for each user to enable them to vote. In a real world application, the password must be randomly generated for eligible voters but this requires a physical environment. The person has to prove his/her identity in an authenticated institution, such as through the PTT (Post, Telegraph and Telephone service) in the Republic of Türkiye e-government system [14]. The election manager registers users by defining an identity number and a password of the voter. However, it is assumed that nobody knows the password of the voter other than oneself.

In this research, Firebase authentication system is used to provide authentication in the web application. Hence, the ID of the voter is encrypted to provide anonymity. Then, the encrypted ID and the password are send to Firebase authentication system. In this way, no additional hashing implementation is required for password security. This approach provides that any eligible user can login to system securely with a correct ID and a password combination.

In addition to authentication system in the web application, another authentication layer is provided in Blockchain side. The goal is to query the ID number of the voter to check eligibility. To do this, a Merkle Tree is constructed by the encrypted ID list of

eligible voters. This operation is done in the client side, therefore, it does not have any cost on Ethereum. After Merkle Tree is created, Merkle Root is used in the blockchain network to deploy the smart contract. Since designed smart contract has no function to change Merkle Root, it will remain constant. Whenever a voter sends a transaction to this contract, the H(ID) and Merkle Proof is also sent to the network. Then, the H(ID) is verified by Merkle Proof and Merkle Root. In this way, inside the smart contract, it is possible to check the eligibility of the voter.

3.1.2 Immutability

Immutability is another important requirement where the vote cast without the voter's consent must not be changed. In traditional to voting system, the voter has no right to change his/her vote after the submission. However, in an electronic environment, voters may have the right to change their votes. Thus, he/she has a chance to correct his/her wrong vote.

Blockchain technology naturally provides immutability because transactions are stored in a block and all blocks contain the hash of previous blocks [15]. If a transaction is modified by improperly, this transaction will not be accepted by the blockchain network [16]. As a result, the block's hash will change and it will not match the hash information in the next block. Thus, in a blockchain based e-voting system, the voter knows that the vote cannot be changed by anyone, since the transaction that contains the vote information cannot be deleted or modified.

A transaction hash is stored in database along with the encrypted ID (E(ID)) of the voter after vote is submitted to blockchain network. Since a password is used while encrypting the ID, it is not possible to obtain the same E(ID)without knowing the password. Since the user has been authenticated by Firebase with her/his E(ID), it is possible to find the linked transaction hash by searching this E(ID) in the database.

The transaction's input is stored as encoded information. After transaction hash is obtained, it is needed to decode the transaction. To achieve this, ABI of the smart contract is used. Then, the submitted vote of related person is obtained.

3.1.3 Anonymity

In a secure voting system, anonymity of voters must be ensured and a voter's decision must remain confidential. Ethereum Blockchain naturally provides anonymity since any transaction does not reveal the identity of the source [17]. Only the Ethereum address of the sender will be seen by the public. Anonymity is ensured as long as this address is not linked with the sender's real identity. In this research, a user who voted is allowed to query her vote at any time. Thus, all transactions are linked with the identity of voters in a secure way.

The ID number is encrypted by a symmetric key so that only the voter can decrypt it to provide the privacy of the system. The encryption process for a voter is done first time when the election manager identifies the ID number and the password of the voter to the system. First, 12 bytes are generated randomly as Initialization Vector (IV). Then, based on password, a key with the length of 32 bytes is generated, which is used in encryption of ID number. Password-Based Key Derivation Function 2 algorithm, which is a secure key generation algorithm, is used to generate a key from password [18]. Finally, by using IV and key, the ID number is encrypted with AES-256 algorithm.

The ID-IV pair is stored in the database after the encryption is completed. Whenever a user tries to login to system, encryption process will be run again. This time, IV is not randomly generated but it is obtained from the database. In this way, the ID is encrypted again and it is sent to firebase authentication with the password. If the user enters the correct ID and the password, he/she will be authenticated and can access to voting page. Even if an attacker gains access to the database and obtains this ID-IV pair, it is not possible to break the encryption since the password is still private. Thus, this encryption process is appropriate to Kerckhoffs' principle [19].

3.1.4 Transparency

Votes must be public for an election to be trustworthy. In this way, everyone can validate the voting. Since Ethereum is a public blockchain network, anyone with access to the network can see the transactions [20]. By decoding the input data of a transaction, everyone can see the votes. In this research, since Sepolia Test Network is used as Ethereum network. Any other Ethereum network will provide similar functionality which enables public to check the transactions. In this way, a selection can be validated.

3.1.5 E-Voting architecture

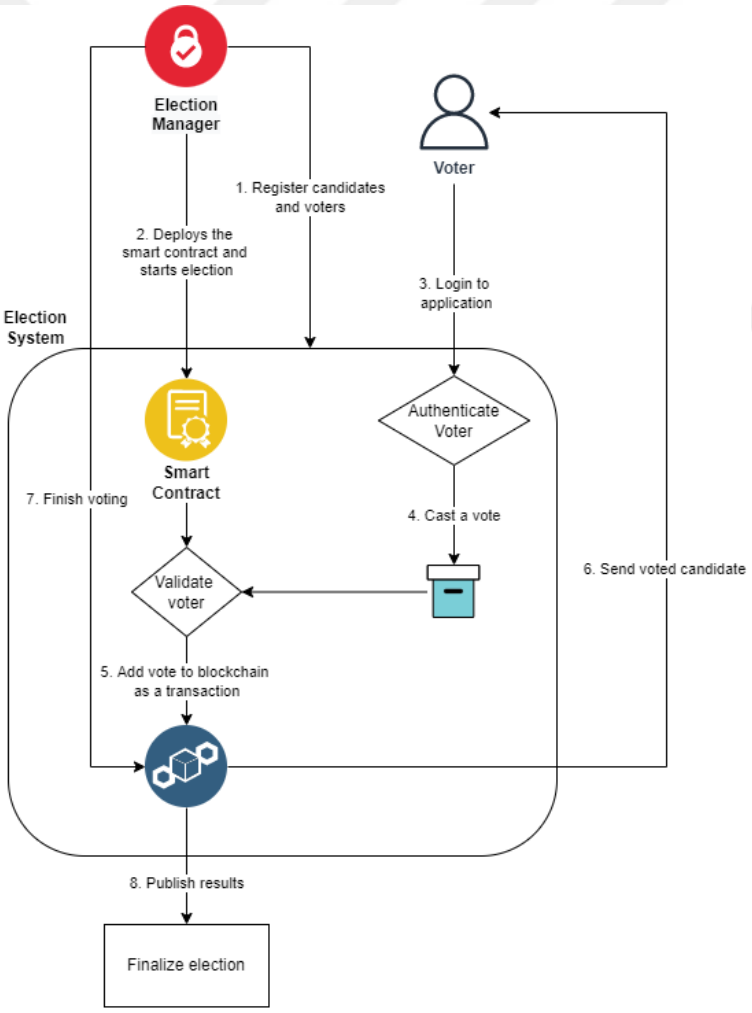

Figure 3.1: E-Voting Workflow

The proposed system consists of three phases in the architecture, namely initialization, voting, and resulting. Figure 3.1 shows the general workflow of the designed architecture.

3.1.5.1 Initialization

The election system requires an election manager to setup the system by defining voters and candidates.

- Election manager identifies voters and candidates in the initialization phase.
- Election manager deploys the smart contract. In this way, initialization phase is over and voting phase is started.

3.1.5.2 Voting

In voting phase, voters can cast their vote tho candidates.

- Voters can login to application with a correct identity number and a password combination, which is predefined.
- Authenticated voter is routed to the voting page, where the voter can vote by choosing one of the listed candidates. Then, the vote is sent to the smart contract as a transaction in the blockchain network.
- The smart contract validates the eligibility of the voter as a second authentication layer. After the validation, the vote is added into the blockchain as a transaction. The number of votes given to selected candidate is increased.
- After the vote is added to the blockchain, it returns voted candidate to voter. In this way, voters are able to validate their votes.

3.1.5.3 Resulting

The election manager's can finish the voting phase.

- After a certain amount of time, the election manager finishes the voting phase.
- After voting phase is ended, the election is finalized and results are published to the public.

3.1.6 Detailed e-voting workflow

The detailed sequence diagram of the system is explained in this section. The workflow explains how eligibility, immutability, anonymity, and transparency are satisfied in this research.

3.1.6.1 Adding voters and candidates

The election manager registers the voters in the authentication system as shown in Figure 3.2. It also adds voters and candidates to the database and initializes the election.

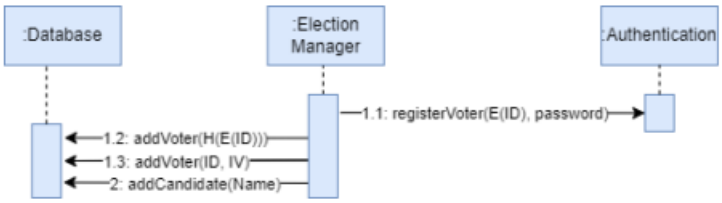

Figure 3.2: Adding voters and candidates.

3.1.6.2 Starting election

The election manager starts the voting phase after initialization. A Merkle Tree with hashed ID (H(ID)) list of voters is created. A smart contract is deployed with Merkle Root and the candidate list. ABI and the address of the smart contract are stored in the database. This phase is shown in Figure 3.3.

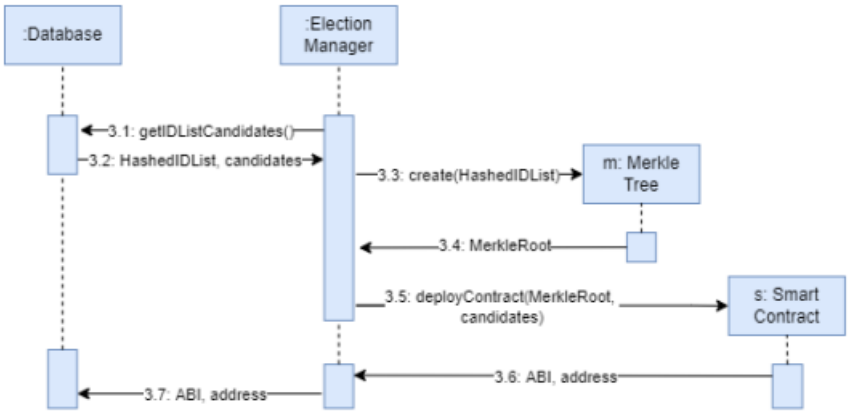

Figure 3.3: Starting the election.

3.1.6.3 Logging in

A voter enters an ID and a password combination when the election starts. The system gets IV from the database and the voter logs in to the system with the encrypted ID as in Figure 3.4.

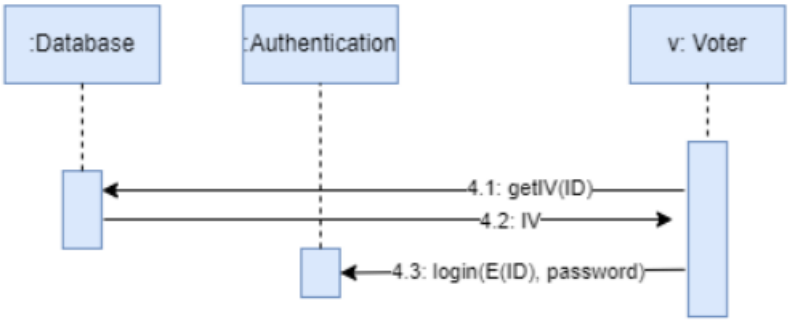

Figure 3.4: Logging in phase.

3.1.6.4 Obtaining credentials

After logged in the system, a voter sends its ID to Merkle Tree to obtain credentials. The voter gets Merkle Proof, ABI and the address of the smart contract as shown in Figure 3.5.

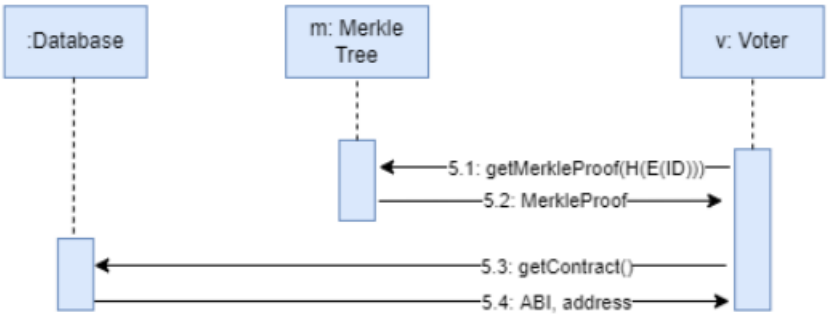

Figure 3.5: Obtaining credentials.

3.1.6.5 Voting

A voter sends the transaction to the smart contract as shown in Figure 3.6. The smart contract validates the voter with Merkle Tree. Then, the smart contract increases the vote count of the candidate. The voter gets the transaction hash and adds it to the database.

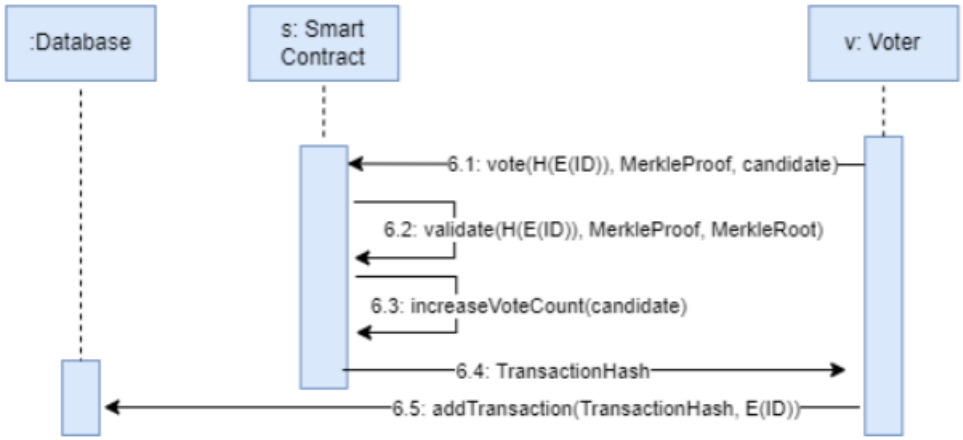

Figure 3.6: Voting process.

3.1.6.6 Querying a vote

During or after the election, a voter can query his/her casted vote from the blockchain to verify the election. The query process is shown in Figure 3.7. A voter gets the transaction hash from the database. By decoding the transaction, the voter can see the vote.

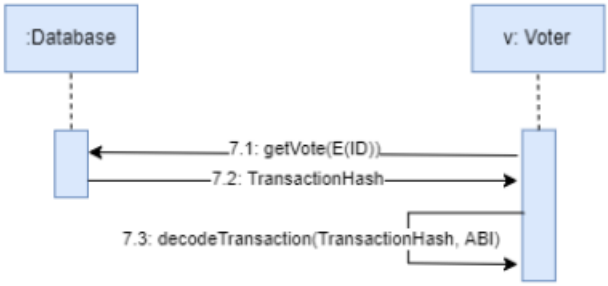

Figure 3.7: Querying the vote.

3.1.6.7 Election results

The election manager can end the voting phase. Voters can see the results of the election as shown in Figure 3.8.

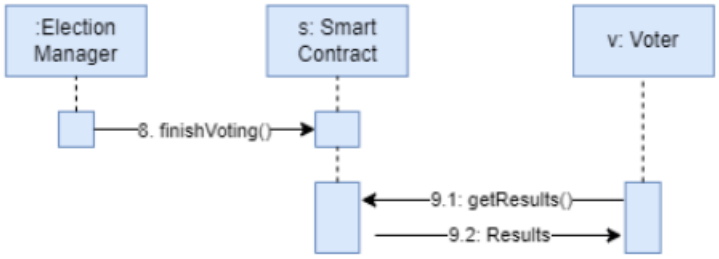

Figure 3.8: Reaching to election results.

3.2 Credential Verification

This component enables the secure validation of government-issued or institution-issued certificates, such as diplomas, criminal records, driver's licenses or health documents. This module is named as Credential Verification to include all kinds of verifiable attributes.

In traditional credential verification systems, such as Turkey's e-Government portal, individuals retrieve official documents (diplomas, criminal record certificates etc.) from institutions (universities, ministries etc.) and share them with third-party institutions in PDF format. These institutions verify the authenticity of the document using a verification code embedded in the PDF via the government's verification service. However, while this process ensures authenticity, it fails to maintain confidentiality: the PDF may be distributed beyond its intended scope, exposing sensitive personal data.

To address this privacy concern while preserving document authenticity, we propose an enhanced credential verification architecture leveraging blockchain, asymmetric encryption, and digital signatures. The system ensures that only authorized institutions can both verify the authenticity and access the content of official documents.

In the proposed system, institutions create signed credentials for confidential documents for users using elliptic curve digital signature algorithm (ECDSA). The credentials include structured data such as name, type, issuer, issue date, and expiration. These credentials are not stored directly on-chain but can be submitted and verified by any third party in the e-government system.

3.2.1 Document registration

The credential issuer (e.g., the government authority) performs the following steps:

- Hash Generation: The document content is processed through SHA-256 which is a a secure hashing algorithm to generate a unique document fingerprint.

- Digital Signature: The hash is digitally signed using the issuer's private key, ensuring non-repudiation and authenticity.
- Blockchain Recording: The signed hash, along with minimal metadata (document type, issuance date, and anonymized identifier), is recorded on the blockchain. This immutable record serves as the source of truth for all future verifications.

Importantly, the document itself is not stored on the blockchain, preserving confidentiality.

3.2.2 Document encryption and delivery

The document holder prepares the document for delivery with following stages:

- Encryption: Prior to transmission, the document is encrypted using the recipient institution's public key. This ensures that only the intended institution can decrypt and view the document content.
- Verification Token Preparation: The holder retrieves the blockchain record (signed hash and issuer signature) and includes this as a verification token.
- Transmission: Both the encrypted document and the verification token are transmitted to the recipient institution through the e-government portal.

3.2.3 Verification and access

Upon receiving the document, the institution (verifier) follows these steps:

- Blockchain Verification: Extracts the verification token (hash and issuer's signature). Computes the hash of the decrypted document and compares it with the blockchain-stored hash. Validates the issuer's signature using the issuer's public key to confirm document authenticity and integrity.
- Decryption and Access: Utilizes its private key to decrypt the document, gaining access to the full content.

With the help of proposed system, authenticity is verified independently via blockchain. Confidentiality is preserved through asymmetric encryption. Only the designated verifier can view the document.

The proposed blockchain-based credential verification system ensures a balance between trustworthy verification and privacy-preserving data sharing. By integrating blockchain-backed authenticity proofs with robust encryption-based access control, the system mitigates key vulnerabilities inherent in traditional credential-sharing processes. This architecture is particularly well-suited to digital governance ecosystems where both transparency and confidentiality are paramount.

4. CONCLUSION

In this study, an e-government system based on blockchain with E-Voting and Credential Verification components is proposed. The decentralized nature of blockchain technology eliminates the single point of failure in such systems that contain confidential personal information.

Digital signature mechanism and storing credentials on the blockchain allows credential verifications. Developed e-voting module provides a solution for problems in centralized e-voting systems with the help of blockchain technology.

In this study, a web application which interacts with Ethereum Sepolia network is developed by using React.js in client side. Google Firestore service is used as a database of the application. Queries are directly performed by a client application.

Ethereum is used to build Blockchain application. Solidity programming language is used to develop Ethereum smart contract and it is deployed to Rinkeby Test Network. Once the smart contract is deployed, the ABI (Application Binary Interface) of the contract, which defines the methods and structures used to interact with the binary contract, is stored in database. So that, ABI of the contract enables the users to communicate through Blockchain network.

To deploy smart contract to blockchain network, a server developed with Node.js is used. To use the application, a browser extension named Metamask is required which connects users to blockchain network by providing them Ethereum wallets.

With the help of this application, users can vote by sending transactions to Ethereum network.

The application is developed and tested to use in Chrome web browser with a Metamask extension. Other web browsers with Metamask extension probably support the application, but it is not tested. Metamask provides an account management system which creates Ethereum wallets to connect users to Ethereum networks [21]. With

the help of Metamask, it is possible to connect several Ethereum networks including Rinkeby test network. In this application, users are connected to Rinkeby test network. To establish this connection, whenever a user (election manager or voter) visits the web application, he/she needs to connect Metamask account, as can be seen in Figure 4.1.

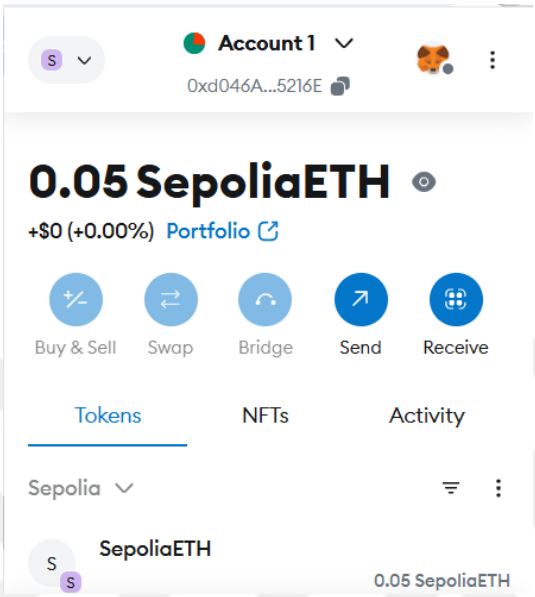

Figure 4.1: Metamask

After connection to Ethereum network is established, election manager can registers to system and add candidates. Then, starts the election. Figure 4.2 shows the election management page.

Figure 4.2: Election management page

In the voting phase, voters can login to system with ID-password combination. Figure 4.3 shows the login page.

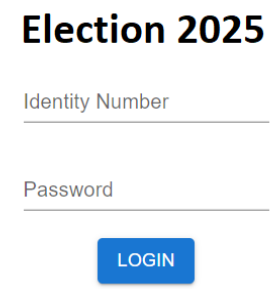

Figure 4.3: Login page

After a voter is authenticated, he/she will be redirected to voting page. In this page, voter can select a candidate and vote for the selected candidate. Voter can query the vote to be ensured the vote is sent to selected candidate. Voting page can be seen in 4.4.

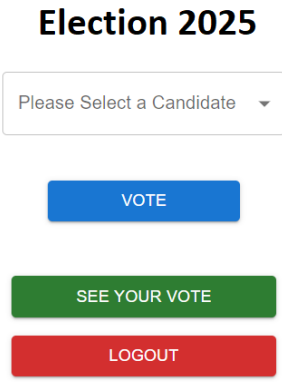

Figure 4.4: Voting page

As a future work, an identity management module can be integrated to the blockchain network. This module will enable users to create, manage, and authenticate their digital identities in a secure and decentralized manner. By leveraging blockchain's immutability and transparency, the identity management system can ensure data integrity, prevent identity fraud, and facilitate seamless access to other government services.

REFERENCES

[1] **Song, H.**, **Wei, Y.**, **Qu, Z. and Wang, W.** (2024). Unveiling Decentralization: A Comprehensive Review of Technologies, Comparison, Challenges in Bitcoin, Ethereum, and Solana Blockchain, https://arxiv.org/abs/2404.04841, 2404.04841.

[2] **Eenmaa, H. and Schmidt-Kessen, M.** (2018). Creating markets in no-trust environments: The law and economics of smart contracts, *Computer Law Security Review*, *35*, 69–88.

[3] **Rouhani, S. and Deters, R.** (2019). Security, Performance, and Applications of Smart Contracts: A Systematic Survey, *IEEE Access*, *7*, 50759–50779.

[4] **Mansour, M.**, **Salama, M.**, **Helmi, H. and Mursi, M.** (2023). A Survey on Blockchain in E-Government Services: Status and Challenges, *12*, 324–335.

[5] **Chouhan, S. and Sharma, G.** (2024). Online voting system model for secure voting using blockchain and Blake2B, *AIP Conference Proceedings*, *3217*(1), 020028, https://doi.org/10.1063/5.0234306, https://pubs.aip.org/aip/acp/article-pdf/doi/10.1063/5.0234306/20314214/020028_1_5.0234306.pdf.

[6] **Hajian Berenjestanaki, M.**, **Barzegar, H.R.**, **El Ioini, N. and Pahl, C.** (2024). Blockchain-Based E-Voting Systems: A Technology Review, *Electronics*, *13*(1), https://www.mdpi.com/2079-9292/13/1/17.

[7] **Kumar, R.**, **Badwal, L.**, **Avasthi, S. and Prakash, A.** (2023). A Secure Decentralized E-Voting with Blockchain Smart Contracts, 419–424.

[8] **Malkawi, M.**, **Bani Yassein, M. and Bataineh, A.** (2021). Blockchain based voting system for Jordan parliament elections, *International Journal of Electrical and Computer Engineering*, *11*, 4325–4335.

[9] **C M, R.**, **Hiremani, N.**, **Birje, M. and K R, N.** (2024). A novel smart contract based blockchain with sidechain for electronic voting, *International Journal of Electrical and Computer Engineering (IJECE)*, *14*, 617.

[10] **Vinayachandra and Karani, K.P.** (2025). Blockchain Based Cryptographic Algorithm for Data Protection in Electronic Voting System, *EAI Endorsed Transactions on Internet of Things*, *11*.

[11] **Mustafa, G.**, **Rafiq, W.**, **Jhamat, N.**, **Arshad, Z. and Rana, F.** (2024). Blockchain-based governance models in e-government: a comprehensive framework for legal, technical, ethical and security considerations, *International Journal of Law and Management*, *67*.

[12] **Woloshyn, R.** `https://www.cbc.ca/news/politics/canada-election-expensive-cost-1.6164267`, date retrieved: 29.05.2025.

[13] **Ohize, H.**, **Onumanyi, A.**, **Umar, B.**, **Lukman, A.**, **Isah, R.**, **Dogo, E.**, **Nuhu, B.**, **Olaniyi, O.**, **Ambafi, J.**, **Sheidu, V. and Ibrahim, M.** (2024). Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges, *Cluster Computing*, *28*.

[14] *Frequently asked questions*, `https://www.turkiye.gov.tr/bilgilendirme?konu=sikcaSorulanlar`, date retrieved: 29.05.2025.

[15] **Proctor, K.** (2024). Decentralization, Immutability, and Integrity: The Role of Blockchain Technology in Enhancing Cybersecurity.

[16] **Hofmann, F.**, **Wurster, S.**, **Ron, E. and Böhmecke-Schwafert, M.** (2017). The immutability concept of blockchains and benefits of early standardization, 1–8.

[17] **Jangid, H. and Meel, P.** (2023). Blockchain Protocols: Transforming the Web We Know, 545–557.

[18] **Kodwani, G.**, **Arora, S. and Atrey, P.K.** (2021). On Security of Key Derivation Functions in Password-based Cryptography, 109–114.

[19] **Kerckhoffs, A.** (1883). La cryptographie militaire, *Journal des Sciences Militaires*, 161–191.

[20] **Patel, A.**, **Sai, S.**, **Daiya, A.**, **Akolekar, H. and Chamola, V.** (2025). Blockchain enabled traceability in the jewel supply chain, *Scientific Reports*, *15*.

[21] (2022). *Metamask documentation*, `https://docs.metamask.io/guide/`.

CURRICULUM VITAE

Name SURNAME: Mustafa TOSUN

EDUCATION:

- **M.Sc.:** 2025, Istanbul Technical University, Faculty of Computer and Informatics Engineering, Department of Computer Engineering
- **B.Sc.:** 2022, Istanbul Technical University, Faculty of Computer and Informatics Engineering, Department of Computer Engineering

PROFESSIONAL EXPERIENCE AND REWARDS:

- Mar 2025 - Present, Research Assistant at ITU Cybersecurity Engineering Dept., SPF Lab, Istanbul
- Aug 2022 - Mar 2025, Software Engineer at Baykar Technologies, Istanbul

PUBLICATIONS, PRESENTATIONS AND PATENTS ON THE THESIS:

- **Tosun, Mustafa**, Bahtiyar, Şerif (2025). Reputation Based Decision Making Consensus Mechanism for Drone Swarms with Ethereum Blockchain, *The 6th Joint International Conference on AI, Big Data and Blockchain*, August, 2025, Istanbul, Türkiye.
- **Tosun, Mustafa**, Bahtiyar, Şerif (2025). Blockchain Based Transparent and Trustworthy E-Voting System, *Eighth International Balkan Conference on Communications and Networking*, June, 2025, Piraeus, Greece.
- **Tosun, Mustafa**, Bahtiyar, Şerif (2025). Reputation Based Decision Making Consensus Mechanism for UAV Swarms with Ethereum Blockchain, *4th International Graduate Research Symposium*, May, 2025, Istanbul, Türkiye.