Blockchain Based Secured Multipurpose Identity (SMID) Management System for Smart Cities

by

Abrarul Hassan Rahat
17101313
Tassnim Jaman Joti
17101345
Tania Akter
17101037
Humayra Tasnin
17101071
Mamunur Rashid Rumon
17101156

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science And Engineering

Department of Computer Science and Engineering
Brac University
September 2021

Declaration

It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

Student's Full Name & Signature:

Abrarul Hassan

Abrarul Hassan Rahat
17101313

Tassnim Jaman

Tassnim Jaman Joti
17101345

Tania Akter

Tania Akter
17101037

Humayra Tasnin

Humayra Tasnin
17101071

Mamunur Rashid Rumon

Mamunur Rashid Rumon
17101156

Approval

The thesis/project titled "Blockchain Based Secured Multipurpose Identity (SMID) Management System for Smart City " submitted by

1. Abrarul Hassan Rahat (17101313)
2. Tassnim Jaman Joti (17101345)
3. Tania Akter (17101037)
4. Humayra Tasnin (17101071)
5. Mamunur Rashid Rumon (17101156)

Of Summer, 2021 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on September26, 2021.

Examining Committee:

Supervisor:

Iqbal

Md.Iqbal Hossain
Associate Professor
Department of Computer Science and Engineering
Brac University

Co-Supervisor:

Md. Arif Shakil
Lecturer
Department of Computer Science and Engineering
Brac University

Program Coordinator:

Md.Golam Rabiul Alam
Associate Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chairperson)

Ms.Sadia Hamid Kazi
Head of the Department
Department of Computer Science and Engineering
Brac University

Abstract

Blockchain, the decentralized architecture and distributed public ledger technology that enables Bitcoin, has recently drawn a strong interest from governments, financial institutions, and high-tech companies. In modern technological era, blockchain is intended to provide a secure, irreversible, and transparent information management platform for practically any application, and it also plays a vital role in establishing the future of cities. A major number of today's well-known crypto-stages are based on the Blockchain concept. In today's digital era, Identification of an individual is one of the most important concerns for businesses and many other public institutions. Digital identity has started playing a vital role in this sector as the data may be used to identify an individual and his fundamental qualities like name, address, health status, credit score and others. In this paper, we will look at how Blockchain can be used to secure digital identities. Digital identity is a trustworthy idea that describes how people can use or what type of attribute or parameter can be used to identify someone's identity, as well as the various privacy concepts or concerns that are related with someone's identity. The identity is used for different kind of application which is typically decentralized and any organization can take control over the identity data which reasons a large number of identity fraud as well. The idea is to build a model for single multipurpose identity, which will be secured using blockchain technology. Instead of several identification documents, users can use this single multipurpose identity to prove their identity in various sectors such as the government and other private sectors to access particular services. An automated and real time verification of identity through smart contracts can verify the identity data. The blockchain will provide a tamper-proof method of storing documents or data that can be audited by the government. User will have control over which of their credential the service provider can access. Our model will also ensure that the user can see how his identity data was accessed by multiple vendors as whenever someone tries to access someone's identity and the user will be able to see how his identity data was used by looking into it as an individual.

Keywords: Block Chain; Digital Identity; Information Security; Secured Identity; Smart Contract; Data Mining ; Multi Purpose

Acknowledgement

Firstly, all praise to the Great Allah for whom our thesis have been completed without any major interruption.

Secondly, to our supervisor Mr. Iqbal Hossain sir for his kind support and advice in our work. He helped us whenever we needed help.

Thirdly, to our co-supervisor Mr.Arif Shakil sir for his kind support and advice in our work. He also helped us whenever we needed help. And finally to our parents without their throughout support it may not be possible. With their kind support and prayer we are now on the verge of our graduation.

Table of Contents

List of Figures

List of Tables

Nomenclature

The next list describes several symbols & abbreviation that will be later used within the body of the document

AI	Artificial Intelligence
API	Application Programming Interface
ATM	Automated Teller Machine
DAO	Decentralized Autonomous Organization
dAPP	Decentralized Application
DCOS	Digital City Operation System
DDOs	Decentralized denial-of-Service
DI	Digital Identity
DID	Decentralized Identification
DMV	Driving License Provider
eID	E-residency Identity Document
EOA	Externally Owned Account
EVM	Ethereum Virtual Machine
GDRP	General Data Protection Regulation
HMAC	Hash-based Message Authentication Code
HTTP	Hyper Text Transfer Protocol
IAM	Identity and Access management
ICT	Information and communication technology
ID	Identity Document
IDPC	Governmental Identity Provider Commission
IoT	Internet of things
IOTA	Innovative type of distributed ledger technology for IoT

MAC	Media Access Control Address
NFC	Near Field Communication
NID	National Identity Document
$P2P$	Peer to Peer Network
PIN	Personal Identification Number
$PKCS11$	Public-Key Cryptography Standard (one of the)
PoW	Proof of Work
SID	Security Identifier
$SMID$	Secured Multipurpose Identity
SP	Service Provider
SSI	Self-Sovereign Identities
SSN	Social Security Number
T	Transformation Oracle
V	Verification Oracle

Chapter 1

Introduction

We began our research by emphasizing the significance of blockchain technology in the development of smart cities. A smart city is a platform composed mainly of information and communication technology (ICT) for the development, implementation, and promotion of sustainable practices to address the increasing challenges of urbanization. To build a more livable urban environment utilizing making optimal use of resources and reducing costs, smart cities are concentrating on the usage of modern innovations like IoT, Big Data, AI, Machine Learning, and other technologies. We analyzed how blockchain technology may benefit the development of urban areas and based on that we identified some key application fields such as governance, economy, smart home, education, digital identity, mobility etc. From these major application areas, we focused on single multipurpose digital identity and how blockchain may be carried out to construct a secured digital identity.

Blockchain is a set of protocols and encryption technologies that allow data to be safely stored on a distributed network. This acts as a ledger for the underlying growth of new virtual currencies. For internet's next generation, it is the leading force as well as a tool for fundamentally altering society and the economy, resulting in a more decentralized world. As the possibilities of such technology are extremely substantial, Blockchain has become a phrase that has captured the imagination and fascinates many. People from all around the world may now trust and transact with others in huge peer-to-peer networks without the need for centralized management which never happen before in the human history. The trust is established via protocols, cryptography, and computer code, not by centralized institutions. This dramatically improves our ability to collaborate and cooperate amongst organizations and individuals within peer-to-peer networks, potentially allowing us to establish global networks without the use of centralized formal institutions.

The Blockchain is a so-called emergent technology that is currently being evaluated at a breakneck pace. This is not only a technology, but also a culture and society dedicated to making the world more equal through decentralization. It is a movement that seeks to disrupt the disturbances in order to restructure the internet, so upending the existing centralized system. It is a new type of technology that combines cryptography with decentralized computing. Satoshi Nakamoto's ingenuity was in combining them in novel ways to establish a concept in which a network of computers collaborates to maintain a shared and secure database. String blocks make up this database. Hash is the name given to each piece of re-coded data that has been encrypted and given a unique identification. The Blockchain relies on a distributed consensus approach to verify database changes since to the lack of a centralized component. To create an entry into the Blockchain system, all computers must agree on the current state of the users, as no computer can make a modification without the permission of others. A block is added to the Blockchain as a permanent record after it is completed. Whenever a block is finished, a new one is created. The Blockchain contains an infinite number of such blocks, each of which is linked to the next by links in a chain in chronological order. The transactions on the Blockchain are changeable, which means they can't be removed. Each block has a hash value that is determined by the previous block. As a result, they are all linked together, which implies that if one is modified, all of the other blocks related to it will alternate in the future. This protects the data from tampering.

We're using Blockchain to secure digital identification in this case. Over a billion people throughout the world are unable to confirm their identity with any degree of assurance. Many of those persons never had a form of verified ID to begin with, and identity theft affects more than 15 million people in the United States in 2018. The solution enables establishing, tracking, and preserving digital identity more efficient, user-friendly, safe, and less vulnerable to fraud by leveraging the power of Blockchain. Emerging standards, such as verified and decentralized identifiers, are used to create digital identities. As a result, such digital certificates would be able to work globally, would be more trustworthy, and would protect personal information.

Digital identity is a collection of information that enables individuals to verify their personal information. This can be used as basic reassurance for any identification claim and may have a variety of applications in situations requiring identity confirmation, including health records, voting, taxation, or border crossing. The United Nations' Declaration on "The Rights of the Child" grants every living individual the fundamental human right of having an identity. It usually includes a person's name, date of birth, nationality, and state identification number. A person cannot vote, work, or own property without having their identification verified. Traditional identity management is centralized, which implies that the process of issuing and validating is carried out entirely by state-authorized agencies. This entails providing personal information to a third party, which can then be linked to other entities. The information might be used in other ways that the owner did not even think about.

People find it difficult to understand what happens to their personal data once it is transferred to a third party. This gives rise to another core issue associated with decentralization, which is the potential for identity theft, because personal data such as passport numbers, Revenue numbers, or credit card information are preserved in a centralized server, making it extremely easy for cyber-attacks, and this is where Blockchain comes in as a potential solution. All data, regardless of its purpose, is maintained and confirmed across several participating nodes in Blockchain. This eliminates two of the most common human-related cases of tampering: negligence and malevolent action. Various consensus techniques are in responsible of ensuring that numerous nodes sign off on a legitimate decision before it is made. By disseminating the information across a peer-to-peer network, it is possible to maintain consistent and up to date. Something that is a vital part of a much bigger issue of data integrity. This is crucial because tampering with public records can have a negative impact on citizens, businesses, and government services. By indexing the stored data with hashes, we can prevent such tampering effectively. Any piece of data that is modified and does not match the Blockchain will be rejected. Blockchain will enable security and data encryption, as well as ensuring network integrity and eliminating the requirement for trust within the network. Zero-knowledge proof can be another way of identification by which we can resolve the issue. The validity of the attester is verified rather than the validity of the information. By using zero-knowledge-proof, we can effectively proof the information without exposing it.

Zero-knowledge-proof ensures that entities can trust one another by permitting them to authenticate any set of data without unveiling it. All data can be additionally secured by cryptography solution achieved by combining public and private keys without automated and decentralized management.

The public decentralized identification is a token that identifies its target, validates the owner's authority over it, and enables the owner to establish trustworthy interactions. These does not depend on any centralized authorities or identity provides. Variable credentials enable the owner to securely and reliably express real-world credentials on the Blockchain. They put an end to the framework that links users, verifiers, and identity owners. Moreover, a decentralized key management system is another fundamental element that enables digital identity to function. The traditional distribution of key certificates is replaced by using the Blockchain. As a result, no central authorization is required. Decentralization in Blockchain effectively means that the identity is managed by its holder which is claimed and it removes 3rd parties from the process. As a result, it entirely belongs to its possessor and cannot be taken away or used without the user's consent. Real-world benefits include social analysis, strengthened border security, secure cashless payments, and more efficient taxation. It can also be deployed to secure fair and transparent elections, as we've just witnessed. Conventionally administered elections are susceptible to at least several major challenges, including the propagation of false news, campaign propaganda, data hacking, and voting software hacking. Hackers may also be lured to meddle with the technology used to announce election results. Using Blockchain an electronic voting system which will be tamper proof can solve the issue.

As we can see Blockchain can be radically set the framework from seamless and security usages of digital identity by human beings. It is more secure, transparent, and tamper proof than digital identity management solutions, and it reduces the risks of human error.

1.1 Research Problem

The importance and difficulty of internet security have been brought to people's notice in recent years [21]. Many times, sensitive personal information is often misused or leaked, financial assets have been compromised, and so on. These security incidents are directly or indirectly related that can cause internet users to suffer economic losses in some ways. As a result, how to manage an identity becomes a significant issue for both internet corporations and academic scholars [36]. In the analog world, identity is mostly based on identification cards that include adequate information such as name, date of birth, photo to authenticate a person, and written signatures. In the digital world, authentication largely based on a digital signature which consists of a public and private key pair. One of the most essential and hardest homeland security concerns is identity management. Identity management must balance complexity and scalability with privacy and security requirements, made specific obstacles and impeding usability.

Companies frequently collect sensitive data about their customers and store it alongside non-sensitive commercial data [27]. With the growth of user privacy-centric rules like ‘General Data Protection Regulation (GDPR) and a change in business attention, new business risks are created. These data become less effective in generating product enhancement and achieving meaningful consumer data when they are restricted to secure data vaults. Many companies would attempt costly and hazardous projects to strike the right balance between data security and business demands if they were threatened with severe fines or if they had superior IT skills. On the other hand, there are almost 10 billion internet-connected devices which can be increased to 22 billion by 2025 [27]. Sensors, monitors, and other IoT-connected devices must be identified, and access to sensitive and non-sensitive data must be handled securely. To solve this service gap, Prominent IT manufacturers have started to develop IoT management platform. Furthermore, having a proper method to identify ourselves and our belongings is essential for creating a healthy society and global market. Those identification data are stored in the central government servers and are issued by centralized entities [27]. For a variety of reasons, physical identification is not available to all humans. More than 1 billion people in the world have no way of proving their identity ownership. For that, there are a good number of people who cannot cast votes in elections, own property and create bank accounts, etc.

For both the governmental and private sectors, identity verification and identification have long been an essential component of service delivery [8]. As citizens continue to do more online, digital identification is an essential yet unfulfilled element of the digital era for their protection in both domestically and globally. There is no service for the citizen to proclaim their own identity without trusting the third parties with the online service they want to access. Blockchain identity management systems could be utilize to address today’s identification difficulties. Inaccessibility is one of the main reasons that a major portion of people do not have their identity status. For that, those people are facing problems to access the existing financial system. As our most sensitive identification data is stored in a centralized government that is maintained by legacy software, hackers can attack the centralized system that includes millions of identifiable information. Moreover, people juggle many identities related to their usernames on several websites. There is no identified method for transferring data from one platform to another. Furthermore, because of the weak link between digital and offline identities, creating new identities is quite simple. For example, due to lack of tight supervision and weakness in the system, a group of brokers and unethical Election Commission workers had been faking national ID cards for years. According to the investigation, each of those fake NID cards is sold at USD 0.1million to 0.15millions and those fake IDs were used frequently in bank loan works and mostly for selling someone else’s land. Around 1,057 people have received NID cards for the second time just changing information except for name and photo for their ill motives. Safety is a flexible type of security that demands less limitation. However, a safety issue can easily be turned into a security problem because of sensible attacks [8]. Identify theft caused by compromising the integrity of the authenticating agent in such a way that the X person can take the identity of Y person and harm that Y person. By blockchain-based digital identities, people can build and maintain identities that combine decentralized IDs, identity management, and embedded encryption.

1.2 Research Objective

Digital identity management is a process for recognizing, validating and authorizing people to gain access to sensitive information. Our research aim is to implement a digital identity solution based on blockchain that will allow identity owners to place their faith in relationship that they already have with trusted people. They main purpose of our research is described below-

- No multiple entities will be there for one person. Identity fraud is one of the world's fastest-growing crimes, and a primary facilitator is the internet [8]. The use of false identifiers, fraudulent identification documents, or a stolen identity is all part of identity fraud. Our system should able to verify the information of a person in some way that the data will not be repeated.

- Ensuring the authentication of the system. Authentication, defined as the process of identifying whether someone or anything is who or what they claim to be, is a critical component of any secure online system that handles sensitive data or transactions. The establishment of a secure network permits to exchange sensitive data providing trustworthy, confidentiality and integrity service on the exchanged data.

- Providing a framework which is scalable, globally usable. Centralized identity management system is controlled by third party for which it is very difficult to manage large number of citizens. So, the system is not scalable. Creating a framework which is able to increase or decrease the system's ability depends on the processing requirements is our main goal.

- Creating a system on data sharing. Blockchain is an irreversible digital ledger that can be configured to records almost any transaction in real time with complete transparency. The decentralized behavior of blockchain will give a chance to our system to access the shared data.

- Constructing a multi-purpose identity card that will include a driving license, bank accounts, passport and so on. Some application areas' identity numbers will be included on the card. Users can use a single card to identify themselves as well as run some applications.

- The system will have both privacy and security by design. Blockchain refers to a new technology capable of delivering a different perspective than digital currency one that has previously been known for features such as transparency and privacy. In identity management system, several levels of confidentiality and security can be defined using blockchain technology and also documentation of transparency and flexibility.

- In the system, Identity-based record sharing in the system should be accomplished using the concept of verifiable credentials.

- Ensuring how the data will securely store, update and retrieve trusted identity from blockchain.

- In our system, blocks will only store the consent proof of data sharing between the identity owners and revocation registry. Proof of work (PoW) is essential for security, fraud prevention, and trust building. Independent data processors cannot deceive about a transaction because of its security.

- Our propose system which is basically used for identity purpose can also be used as a multipurpose card. We can use this card as driving license, ATM card etc. It is very much hassle for a person to handle various kinds of cards for each work. One has to carry identity card, driving license, numerous bank cards and so on. We want to reduce this with the help of our proposed card. One can use this as a driving license. So they don't need to carry another extra driving license card. Some people have to carry many bank ATM cards for transaction in different banks which is also a problem to maintain. With the help of our proposed card one can use it for transaction in any bank. They don't need to carry separate ATM cards. One can also avail any type of social services digitally by using this card. So they don't have to face numerous problems and hassles to get any social services. With the help of our proposed card life would be so much easy for a person.

.

Chapter 2

Literature Review

In the last decade, the concept of smart cities has grown in popularity, allowing inhabitants to better satisfy their housing, transportation, energy, and other infrastructural needs, and becoming an important part of eliminating poverty and inequality, unemployment, and energy management. Efficient traffic condition, parking management, sustainable electricity, sophisticated office towers, and enhancements to public works are all features of successful smart city initiatives, but citizen engagement will move them forward. According to Gartner, public participation, service enhancement, and citizen experience will all be essential to smart city success [5].

Smart city projects are the latest impetus for the Gulf's economic diversification. The participation of the people who live and work there is crucial to the success or failure of these programs. Citizen involvement is critical because citizens may provide critical feedback for enhancing existing services and influencing the development of new ones. Citizens must be educated and informed about their city's smart transformation, and they must be encouraged to participate in pilot programs and other projects. And, to do so, digital identification is critical.

When smart cities can foster citizen involvement, they increase their prospects of success and sustainability. Digital identity is one method to get started. The capacity to prove an individual's identity via any government digital platform is crucial for fostering inclusively and giving individuals with access to government services. By 2050, up to 70% of the world's population is expected to live in smart cities, with strategic management of people's digital identities playing a key role.

This section provides all of the relevant literature to understand this thesis. These include Blockchain technology, an introduction to the identity management system, problems of current identity management systems, blockchain in identity management, digital identity.

2.1 Blockchain Technology

Blockchain refers to a network of immutable digital ledgers for information exchange that not only stores the history of financial transactions like it does in bitcoin but also can store anything of value [18]. A blockchain, in layman's terms, is a massive collection of relevant documentation that cannot be expunged, deleted, or edited. It is a distributed and decentralized network as there's no central computer or device on which the entire chain is saved. Instead, each block node involved in transactions keeps a copy of the transactions, and the previous blocks' data is continually preserved in new blocks. Every time a transaction takes place on the blockchain, a record of it is recorded to each participant's ledger.

Blockchain is a decentralized, immutable ledger that records digital asset ownership in the form of transactions and blocks. The basic structure of a block includes the block number, hash of the previous block, transaction contents, nonce, and timestamp. The nonce is a random variable in this case, whereas the timestamp is a continuous variable. Validators or miners (computational nodes) continuously hash static (block) and dynamic (timestamp and nonce) data in order to find a value that begins with a string of several consecutive preceding zeros. This process is commonly referred to as a cryptographic puzzle. The winner is the miner who first finds the true hash value and is allowed to add the block to the blockchain. The Proof-of-Work (PoW) consensus algorithm is the method for determining if a block is valid or not [7]. The primary functions of blockchain are described below:

In blockchain technology, every node in a blockchain network, including miners, has a Pool of Memory that contains all current transactions that are waiting to be added to the blockchain to produce a new block. All transactions are verified and summarized through a Merkel tree. If it is authentic, some transactions are included in the block which miners throughout the smart home network can then use for mining. To erase processed transactions from the Memory pool, miners construct a hash of the block by modifying the nonce and timestamp. The resulting hash is then compared to the target by the system. When a miner completes mining a block, it is successfully added to the chain. If the hash exceeds the target value, then the miner again starts constructing a hash of the block by modifying the nonce and the timestamp. If the hash value is less than the goal value, the PoW (Proof of Work) is certified as successful and the block is put to the blockchain. As a result, this notification is sent throughout the network, informing every linked node that finished transactions should be removed from the Memory pool. The Blockchain's chaining and decentralized process make tampering with previously accepted transactions impractical. A manipulating of a single block transaction results in an alternating Merkel root hash value for the transactions contained in the block, as well as a separate hash value for the manipulated block. As a result, the Blockchain network's ledger data is considered immutable.

2.1.1 Permissioned and Permission-less Blockchain

Permissioned Blockchain: Permissioned blockchains are closed networks in which previously selected parties connect and participate in consensus and data validation, sometimes as members of a consortium [24]. They are partially decentralized in the sense that, unlike permission less blockchains, they are dispersed among known participants rather than unknown individuals. Tokens and digital assets are possible, but they're not as common as they once were. The key points of permissioned blockchains are:

- Controlled transparency primarily based totally at the desires of collaborating organizations
- Development via way of means of personal entities
- Lack of obscurity

- Lack of a vital authority, however a personal institution authorizes decisions.

Permission-less Blockchain: Permission less blockchain, additionally called faithless or public blockchains, are open networks wherein all of us can take part with inside the consensus method utilized by blockchains to validate transactions and data. They are absolutely decentralized and disbursed amongst unknown parties. The key traits of permission much less blockchains are:

- Full lucidity of transactions
- supply development
- Obscurity, with a few exceptions
- Lack of a principal authority
- Heavy use of tokens and different virtual property as incentives to take part.

Permissionless Blockchain	**Permissioned Blockchain**
Open network	Closed network
Public and trustless	Private and permission sandbox
Full transparency	Controlled transparency
Mostly anonymous	Not anonymous
Privacy depends on technological limitations	Privacy depends on governance decision
No central authority	No single authority
Transaction does not depend on permission	Transaction only depends on permission
Slower and inaccessible	Faster and more scalable
Costly	Inexpensive

Table 2.1: Permission-less Blockchain vs Permissioned Blockchain

2.2 Introduction to Identity Management System

Identity management, often known as identity and access management (IAM), is the comprehensive discipline responsible for confirming an identity of a user and range of access to a system. Both authentication and accessibility restriction, which govern each user's level of access to a specific system, are both crucial in securing user data in that context. An identity management system prevents illegal access to systems and resources, helps to prevent enterprise or protected data ex-filtration, and provides alerts and alarms when unauthorized personnel or programs attempt to gain access, whether from within or beyond the enterprise perimeter.

An example of Identity management would be customers or employees having the access level, privileges, and limitations to access software and hardware within a company or enterprise. Another example would be the issuing and verification of birth certificates, national identification cards, passports, or driver's licenses in a government setting, allowing a user/citizen to not only establish his identity but also access government and non-government services

2.3 Problems of Current Identity Management Systems

Most digital transactions necessitate the disclosure of particular personal information before users can access services. For example, before using platforms like Amazon Pay, PayPal, or Google Wallet to conduct financial transactions, consumers must always enter their sign-up/login information. As a result, digital clones of the same individual emerge throughout these various channels. This also reveals a slew of security flaws. As the Equifax attack illustrated, gaining access to a large database reveals all of a user's personal information and emphasizes the current system's high susceptibility.[34]

Most existing systems rely heavily on obtaining personal information without the owner's knowledge, and third parties can gain access to this information without the subject's consent. Furthermore, information stored in these online databases may be shared with third parties without the authorization of the individual. Although this is sometimes done in the best interests of the subject or for their benefit, such as offering appropriate goods and services for them to try out, it makes no difference that the individual's consent was not requested and that control was left in the hands of the database's owners.

The vast majority of today's identification systems are ineffective and outdated. Identities must be portable and verifiable at all times, and digitalization can help with that [17]. However, being digital isn't enough. Identity must also be kept secret and safe.

Several industries are affected by the shortcomings of current identity management systems:

Government: Excess bureaucracy is a result of a lack of interconnectivity across departments and levels of government. As a result, process times and prices increase.

Healthcare: Healthcare information networks are a top priority for hackers. The networked structure of modern healthcare facilities—specifically, the integration of so much essential data gathered from a large portion of the population—makes it a visible target for hackers and cyber-criminals.

Education: Each year, it is believed that two hundred thousand fake academic certificates are marketed in the United States alone. Buying and selling fake academic degrees is also a widespread occurrence in Bangladesh. Due to the difficulties in confirming the authenticity of these credentials, unqualified people are hired, causing brand damage to institutions and hiring organizations.

Banking: Proper identification of the client to the bank and the bank to the consumer is crucial in providing financial services to consumers for financial institutions. Individual and business clients are increasingly accessing banking solutions via the internet distribution channel. Banks support this type of access since it is a low-cost, high-efficiency technique of offering financial services. The requirement for login information such as passwords reduces the security of banking for users.

Businesses in general: The existing requirement to maintain personal data of clients and workers is a source of liability for businesses. Due to GDPR violations, a personal data leak may result in massive fines.

2.4 Blockchain in Identity Management System

By allowing individuals to keep data on a blockchain rather than on hackable servers, blockchain technology offers a potential solution to the problem mentioned. Once information is recorded on a blockchain, it is encrypted and cannot be changed or removed, making large-scale data breaches extremely difficult, if not impossible. In the age of digitalization, where everything is either digital or has a digital representation, and everything is connected, blockchain is recognized as a significant invention. By giving everything a digital identity, spreading storage rather than centralizing it, and automating procedures, blockchain's unique technology can provide transparency and confidence to the digital ecosystem. In most circumstances, cryptography is used to manage identity. Cryptography as a tool, on the other hand, has both pros and limitations. Cryptography can be used to prove that a message came from a specific source (Message Authenticity). This attribute is demonstrated using digital signatures and certificates. It can be used to prove that one message is related to another or that one communication arrived before the other. To demonstrate this property, hashes and/or Merkle Trees can be employed. Cryptography can ensure that only the intended recipients can understand a communication (Confidentiality). This quality can be ensured by encryption and decryption. It can also confirm that a message has been received or retrieved in its original state (Integrity). To ensure this quality, message authentication codes (MAC or HMAC) might be utilized.

A number of features of Blockchain make it ideal for efficient and secure identity management, such as:

- Immutable and transparent feature of blockchain. For identity management, immutability and transparency are essential.

- Blockchain technology prevents vulnerabilities and denial of service attacks, making it more suitable for identity management systems.

- Blockchain allows for efficient implementation of public key cryptography and hazing. It can be used to verify identity-based papers are integral and authentic and can be expanded to include digital identities. It can be used to certify records from a third party. It also aids the exchange of records via smart contracts based on permissions.

- Since a central authority does not govern blockchain, it eliminates or minimizes monopolies in identity management. It also enables worldwide identification and record integration.

- Blockchain provides incentives in the form of cryptocurrency that can be used for specific reasons, for example, by offering participants incentives to share data.

- Asymmetric cryptographic (public-key cryptography) keys are used in Blockchain to identify asset owners. To ascribe digital identity to things, blockchain-based identity solutions employ the idea of asymmetric cryptography. Asymmetric encryption enables to encrypt and decode messages using two keys, so only private key of the key pair can decrypt a message encrypted with a public key, and vice versa. Public-key cryptography is used in Blockchain to verify transaction legitimacy and asset ownership.

2.4.1 Verifiable Credentials

Physical credentials such as an ID card, driver's license, health insurance card, or even an academic certificate have few digital counterparts. A digital credential, or digital asset, can be as reliable as a government-issued physical ID card. Verifiable credentials are digital identity owners' credentials that are machine-readable, private, and cryptographically secure. Self-sovereign identity is supported by verifiable credentials, which allow identity owners to store credentials in an identity account and use them to prove who they are. Verifiable credentials are normally confirmed by a third party, but they can also be self-attested. The concept of digital signatures is used for attestation. By signing identity owner's records with its private key, an attester (issuer) with a DID creates a verifiable credential, which is cryptographically verifiable by a verifier using the attester's public key. Verifiable Credentials are kept confidential. The ID holder has the option of choosing whatever aspects of their identity they want to reveal. They may, for example, display their birth year without revealing their birth date or month. The interaction between the ID Holder and the ID Verifiers is always in the hands of the ID Holder. They can revoke the relationship at any time because they know what data was given and when (there's an audit trail). Through the application of cryptography, they are tamper-proof. Verifiable Credentials can be checked at any time and from any location. Even if the issuer no longer exists, with the exception of circumstances where credentials were issued using Private DIDs and the issuers DID was not written to the ledger.

2.4.2 Decentralized Identifier

Decentralized Identifiers (DIDs) have been identified as the foundation of self-sovereign identity, and their significance cannot be emphasized. A DID is a pseudo-anonymous identifier for a person, company, object, or other entity. A private key is used to protect each DID. Only the owner of a private key may demonstrate that they own or have control over their identity. One individual can have many DIDs, limiting the extent to which they can be followed throughout their various activities. Each DID is frequently coupled with a set of attestations (verifiable credentials) supplied by other DIDs attesting to the DID's distinctive qualities (e.g., location, age, diplomas, payslips). Because these credentials are cryptographically signed by their issuers, DID owners can store them locally rather than depending on a single profile provider. Establishing decentralized identities necessitates the use of cryptography. Private keys are solely known by the owner in cryptography, whereas public keys are widely distributed. This combo accomplishes two goals. The first is authentication, in which the public key verifies that a holder of the paired private key sent the transmission. The second method is encryption, in which only the holder of the paired private key can decrypt communication encrypted with the public key. A Verifiable Credential is linked to an organization's Public DID when it is issued. The same Public DID is also maintained on the blockchain, which is a digital ledger that cannot be altered. Without having to contact the issuer, someone who wishes to verify the Credential's authenticity/validity can look up the DID on the blockchain to determine who issued it.

2.5 Digital Identity management

Today, there are a variety of instances in which an entity, such as a person or an organization, in possession of personal information want or wants to establish the information's authenticity to a third party. It is sometimes simpler to reach an agreement when there is some level of confidence between the prover and the verifier. In instances where strong authentication is required or when there is no confidence prior to authentication, reaching an agreement becomes exponentially more difficult, particularly when verification is undertaken over the Internet. This is an important requirement for the identity management system to establish trust in between the tester and the verifier when there are doubts about the validity of the statement.

A digital identity is a set of traits such as name, date of birth, and so on or information associated with an entity that is utilized by computer systems to represent an external agent. To be specific, this set of attributes is linked to a Subject, and Authorization or Authentication agent(s) use this information for their respective functions. In essence, a digital identity is nothing more than a claim that an authentication agent verifies.

When the user creates and registers a DID on a self-sovereign identity and data platform, a private and public keys is generated by the process. In the event that public keys associated with a DID are compromised they can be stored on-chain for security purpose. Attestation can be attached on chain to make sure scalability and compliance with privacy standards, but whole data itself should not be added.

2.6 Related Works

Digital representation of knowledge about a certain person or organization is known as a digital identity (DI). Such data consists of a set of assertions made by one subject regarding another subject. In this section, we tried to critically review the previous relevant researches regarding digital identity management systems based on blockchain technology.

In the paper [33], the authors concentrated on a critical element of digital city management which is the reliable identification of specific citizens. They stored and securely sent user attributes to other verification systems. They intended to establish a system which can help develop digital infrastructure for the management of intelligent cities. The establishment of smart cities may be a technique for optimizing asset usage in order to address the issues posed by rapid urbanization and urban population growth. Evolution Several studies have stated that there are more than currently, 50 percent of the world's population lives in cities, and this puts a lot of pressure on the infrastructure and services. Despite the enormous costs of developing, creating, operating, and maintaining them, smart cities offer an answer to better energy, water, and waste management. They claimed DCOS as Digital City Operation System which must be structured to securely identify smart city's constituent components, allowing for optimal utilization and efficient access. It's important to note that in order to use the smart city's services, citizens must engage with all of the smart city's component subsystems. Despite hardware or software, users need an interface for access to infrastructure-based services. For that, the authors wanted to design a framework where an identity can be viewed as a collection of personal characteristics that identify a participant and allow him or her to be associated with a group and conduct transactions with other members. They mentioned about three types of identities such as inherent attributes, accumulated attributes and assigned attributes which will allow entities to take advantage of community services by demonstrating that they have the requisite traits to participate in system transactions.

According to [23], Blockchain-based applications have a potential to boost public and private sector efficiency and service delivery. Based on their personal experience with a digital identification ecological perspective, in this paper, the writers emphasized the potential advantages of applying blockchain technology to address present and future identity verification difficulties and authentication in a Canadian environment. Identity verification and authentication were always a critical component in services both in the private and public sectors; nevertheless, changing citizens' needs in the digital age have shown that creative solutions are necessary to confirm that someone they claim is confident. Previously existing identity solutions do not suit this modern approach, instead depend on physical identification documents, processes, and procedures that necessitate costly and time-consuming counter visits. Today's identity- verification methods are fraud with the high cost such as variations of username and password are inconvenient and easily forgotten, driving licenses are less secure and very tough to verify. In this paper, the authors approached the benefits of blockchain and the digital ecosystem. They intended to explain that people must be able to demonstrate who they are with new digital standards and instruments that are trusted through the economy in a safe and privacy-enhancing way. Businesses, governments, and consumers all require assistance to battle escalating rates of cybercrime, minimize the risk and inconvenience of digital transactions, and boost citizen trust and safety. The author mainly tried to develop a better smart ecosystem with a new digital identity where people can access the facilities of the smart cities with their secured and privacy-enhanced identity.

The authors of the paper [30] looked into the use of Blockchain technology in identity systems. The authors proposed a Blockchain technology-based digital identity verification and recording and logging system. The authors of the document focused on laying the foundation for "decentralized digital identity" as a "autonomous digital identity" backed up by modern cryptography and digital certificates, while also describing problems and challenges in terms of safety and privacy, usability and globalized, which traditional identity management methods have to face. In addition, they reviewed existing literature's solutions and put forward a system that utilizes powerful features of Blockchain to create a truly private, secure digital identity solution that allows identity owners to have complete control over their portable identity and identity-based records without relying on centralized authorities.

This research [27] defines and investigates the issues with Identification Management Systems, and proposes a method for establishing self-sovereign identity using blockchain technology using cryptographic proofs. According to the authors, conflicting interests and responsibilities generated an incentive distortion between the Subject, Authentication agent, and Authorization agent. Type 1, type 2, and type 3 attacks are the result of these issues. Their solution started with atomically establishing the building blocks of an Identity Management system (claims, trust, and digital identities) and subsequently grew into a full-fledged self-sovereign identity management system based on polynomial-time algorithms (G, T, and V). For the Transformation oracle (T) and Verification oracle (V), the supporting cryptographic proofs for attaining security and privacy are represented as a security game (V). They also compared and contrasted their findings with other studies and explained why their solution is secure. They argue that Trust, as defined in their research article, is transitive as long as the claims shared are still true under a certain verification technique trusted by the Service provider. This trust could serve as a secure foundation for the proposed self-sovereign Identity management system.

This study [31] provides a comprehensive, criteria-driven study of the solutions and technologies for this rapidly evolving field, as well as a comparison of their capabilities to those of existing solutions. The authors presented a complete set of requirements that included ecosystem aspects, end-user functionality, mobility and cost factors, compliance/liability, EU regulation, standardization, and integration to highlight the benefits and downsides of alternative solutions. For evaluating blockchain-based IAM systems, the authors developed a comprehensive set of 75 evaluation criteria. They evaluated 43 products based on these parameters. They also discovered that the evaluated products had a wide range of maturity levels, with only a few of them being able to compete with established blockchain-free alternatives in terms of end-user convenience. The majority of solutions lack the obvious economic model that is required to run a multi-node network for extended periods of time. They also mentioned that they intend to expand the evaluation criteria to IDs for machines and things, i.e. IoT, as part of their future work.

In our model we proposed a card which can be used in many purpose. This type of card is still not been introduced in our country but in other countries like Estonia, Finland, Luxemburg already started to implement these type of cards in some extent to help the people. Estonia has each an eID for residents and an "e-residency" program. The eID is issued as a PKCS11 smart "ID-Card" with the capacity to sign and encrypt files and emails, carry out on-line login, make payments use telemedicine etc. The keypair saved at the smartcard is well suited to the X.509 standard; more recent playing cards upload a contactless interface (NFC). In addition to the "ID-Card", a separate "digi-ID" card is to be had for the ones Estonian residents who already own a valid "ID-Card" in any case. The important variations to the "ID-Card" is that the "digi-ID" lacks any printed embossed information, and for that reason can best be utilized in digital environments, whilst the "ID-Card" additionally serves as a visible identification document. The third eID in Estonia is the "Mobiil-ID" that is small SIM-sized card for cellular phones. "Mobiil-ID" serves as a person's identity and as a virtual signing solution, very much like the 2 different cards. Like the previously referred to cards it could be used to get admission to precise e-offerings along with e-taxing and digitally signal files, however with the delivered fee of now no longer requiring an external card reader for the duration of the process. To make use of the "Mobiil-ID", the consumer makes use of two PIN codes: the primary code is wanted for identity to the cardboard and the second code is wanted to unlock the signature functionality. "Smart-ID" is the corresponding cellular app a good way to get admission to the "Mobiil-ID" functionalities. The Finnish eID changed into delivered in 1999 and changed into a number of the first actual operational country wide eID scheme withinside the world; it's far noncompulsory and the costs are especially high. Currently, the Finnish eID system sees especially low use; it does now no longer employ or guide blockchain technologies. In 2015, independently from the overall national eID scheme, the Finnish Immigration Services and the Helsinki-primarily based totally startup agency MONI commenced a assignment in which the companions partner a virtual identification with the prepaid MasterCard debit cards which might be supplied to asylum seekers and refugees who're missing official/paper identity documents. The debit playing cards are related to corresponding specific virtual identities which are created for refugees on blockchain; this turns the debit playing cards right into a type of government- issued eIDs. Deployed on an Ethereum blockchain platform, the answer potentially allows lots of refugees to take part in regular tasks till they get hold of everyday ID documents. However, the software program with inside the trial additionally seems to document the monetary transactions made with the cardboard.

Chapter 3

Methodolgy

Our model's main goal is to make it possible for the system to carry out such a task. It means to assure the privacy and security of numerous forms of data transactions on a big scale to make it easier for people to use the system by establishing trustworthiness to construct such a structure.

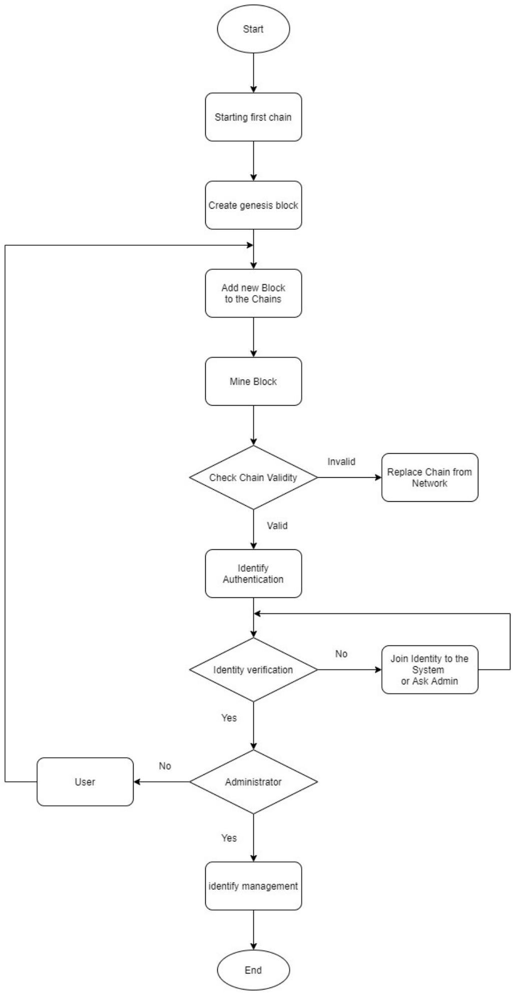
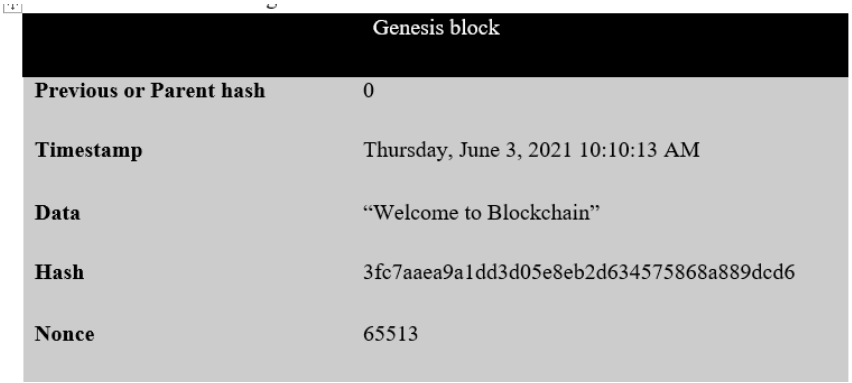


Figure 3.1: Workflow of Secured Multipurpose Identity Card

3.1 Genesis Block

A Genesis Block is the moniker given to a cryptocurrency's first block.A block-chain is made up of a sequence of blocks that are used to store data on transactions that take place on a block-chain network [14]. Each of the blocks contains a singular header and each such block is identified by its block header hash individually. These blocks get layered—one on top of the other, with the Genesis Block being the foundation—and they grow tall until the highest of the block-chain is reached and therefore the sequence is complete [9]. One of the features that makes a block-chain-based crypto-currency so secure is the layers and rich history of each sequence. Blocks are essentially digital containers in which data about network transactions is permanently maintained. A block contains a list of some or all of the most recent bitcoin transactions that haven't yet been recorded in any previous blocks. As a result, a block is similar to a page in a ledger or a record. When a block is 'completed,' it gives to the following block in the block-chain [15]. Because the genesis Block, also mentioned as Block 0, is that the very first block upon which additional blocks during a block-chain are added. it's effectively the ancestor that each other block can trace its lineage back to, since every block references the one preceding it. This began the tactic of validating bitcoin transactions and introducing new bitcoins into existence.



Genesis block	
Previous or Parent hash	0
Timestamp	Thursday, June 3, 2021 10:10:13 AM
Data	"Welcome to Blockchain"
Hash	3fc7aaea9a1dd3d05e8eb2d634575868a889dcd6
Nonce	65513

Figure 3.2: Genesis Block

3.2 Data Blocks

Aside from the genesis block, all of the blocks in our block-chain serve as primary data storage units. All proceedings are recorded in data blocks that are then added to the block-chain. Subsequently this linkage of blocks through chains are known as block-chain. The block-chain is a digital ledger. Our block-chain's complete structure is in the capacity of each block is connected to its foregoing hashes in a connected rundown. The blocks or nodes are the most important part of the block-chain for storing information [19]. These blocks contain all transactional and non-transactional data and are uploaded to the block-chain except for side chains or multiple threaded chains like IOTA the blocks in our architecture are added linearly across a chain to the previous hash like a linked list [20].

3.3 Previous Hash

All of the blocks in our block-chain are linked by the previous hash (SHA256) which ensures the integrity of the block-chain's one-way retrieval [19].The hash utilized in this system was a 64-bit SHA256 hash that is immutable, meaning it can never be overwritten [19]. All of the blocks in our system refer to the previous block and consequently to the genesis block. However, travelling through the blocks will never lead to the genesis block because the blocks are dynamically formed and change on a regular basis. As a result, Block-chain maintains its integrity and is unchangeable.

3.4 Current Hash

Every block in our block-chain contains a hash that serves as the block's unique identifier [20]. These hashes are immutable and serve as the foundation of the block-chain, as they both represent and connect our whole network. Each block references to the previous block's hash. The difficulty now is how these hashes are created so that they are both non-deterministic and unique. The timestamp, nonce, and flags are used to construct these hashes. Because all of these numbers are unique, we only construct one hash from the 264 numbers, with a chance of 1 in 3.71011 that the hashes will match [32].

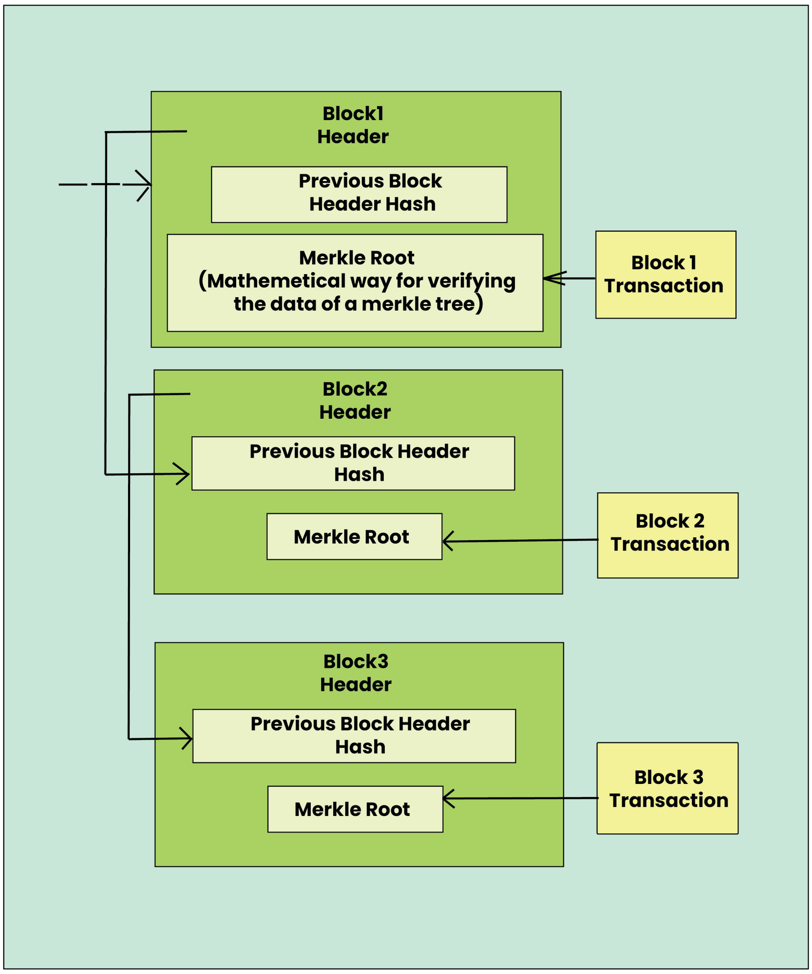
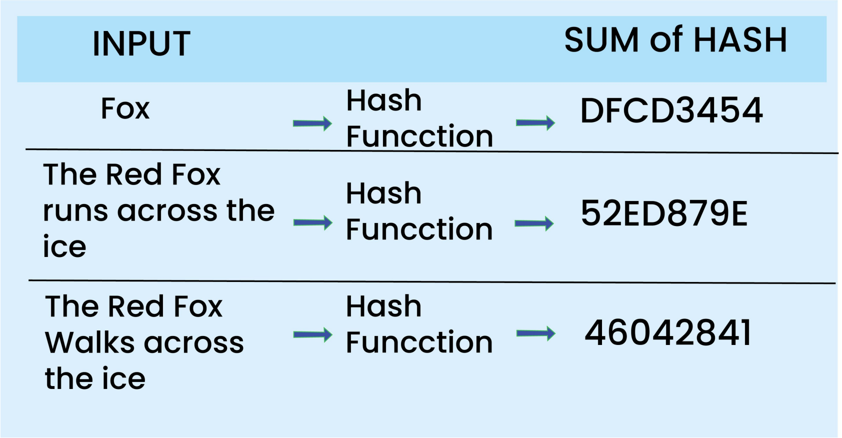


Figure 3.3: Connection of each block



INPUT				SUM of HASH
Fox	→	Hash Funcction	→	DFCD3454
The Red Fox runs across the ice	→	Hash Funcction	→	52ED879E
The Red Fox Walks across the ice	→	Hash Funcction	→	46042841

Figure 3.4: SHA256 Algorithm

3.5 Timestamp

The timestamp, often known as a timestamp, is a short piece of data recorded in each block as a unique serial number, whose main purpose is to determine the exact time the block was created which has been mined and validated by the block-chain network [26]. This timestamp is also used for generating a unique hash that makes the block-chain more transparent.

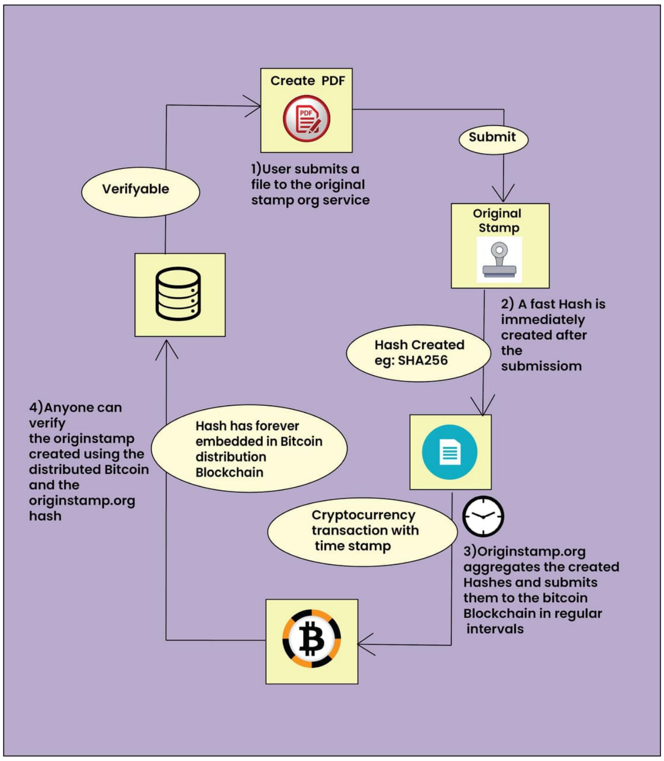

Create PDF
Submit
1)User submits a file to the original stamp org service
Verifyable
Original Stamp
2) A fast Hash is immediately created after the submissiom
Hash Created eg: SHA256
4)Anyone can verify the originstamp created using the distributed Bitcoin and the originstamp.org hash
Hash has forever embedded in Bitcoin distribution Blockchain
Cryptocurrency transaction with time stamp
3)Originstamp.org aggregates the created Hashes and submits them to the bitcoin Blockchain in regular intervals

Figure 3.5: Timestamp in blockchain

3.6 Nonce

In cryptographic communication, a nonce is a one-time-only random number. They are frequently composed of pseudo-random or random numbers. Many nonce include a timestamp to ensure they are delivered on time, though this requires company-wide clock synchronization. Including a client nonce in access authentication improves security in a number of ways. To ensure that a nonce is only used once, it should be time-variant (with a fine-grained timestamp in its value) or generated with enough random bits to ensure that a previously constructed value has a statistically negligible chance of being repeated [29].

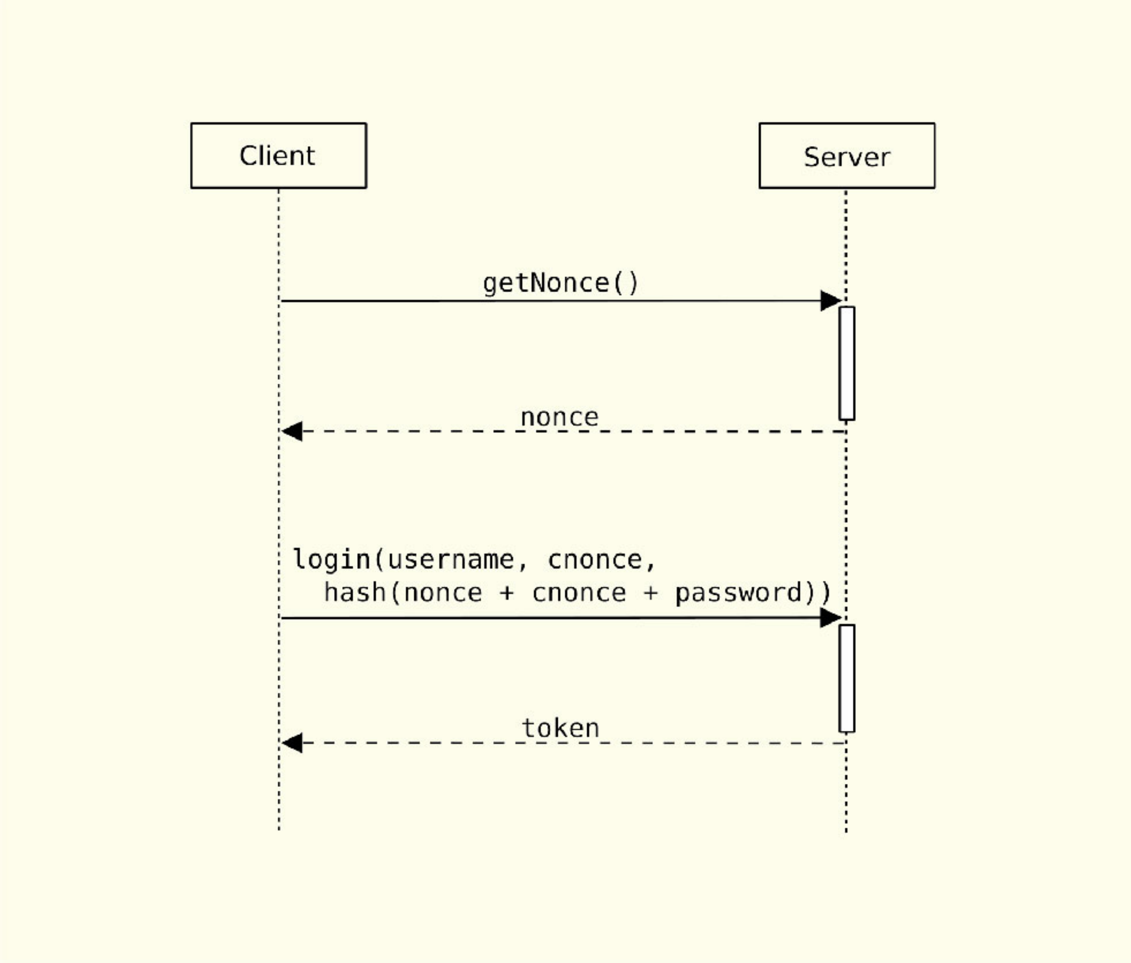


Figure 3.6: Working mechanism of nonce

3.7 Consensus

Consensus is first and foremost an agreement that can be used as a fault-tolerant technique for a digitalized system [16]. The inclusion of a third party that controlled time and money was one of the most critical concerns with traditional transactions [22]. Block-chain overcame this restriction, but it still required some kind of algorithm to monitor information activity or transactions. This introduced the concept of agreement. For our system, we created a consensus protocol and applied it to provide transparency and secure communication. The Proof-of-Work algorithm, which allows a digitalized and decentralized system to determine whether a transaction is genuine or not, is the most important aspect of consensus in our system.

3.8 Proof Of Work

Proof of work (PoW) is a decentralized agreement method that requires network members to invest energy tackling a self-assertive numerical riddle to keep the framework from being hacked [3]. Verification of work is utilized generally in cryptographic money mining, for approving exchanges and mining new tokens.In fact, it has complete control over all transactions within the framework and bears no third-party liability.

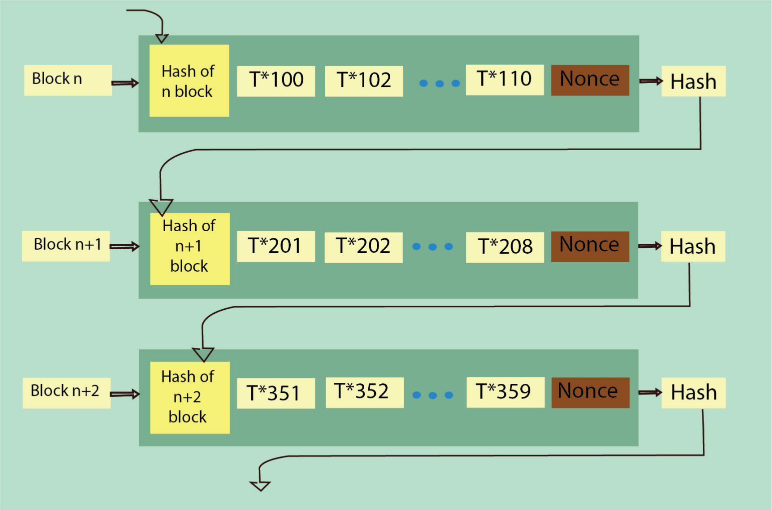


Figure 3.7: Proof of work algorithm

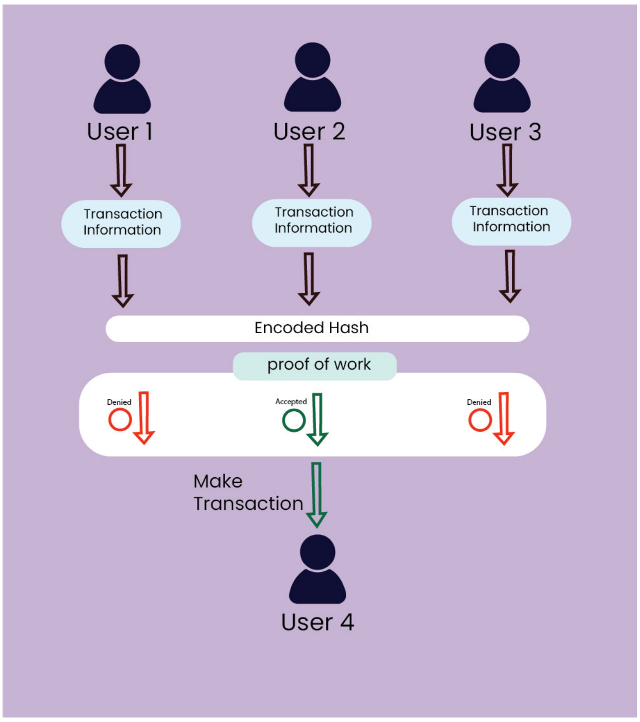


Figure 3.8: How Proof of work secures the system

In a traditional system, for example, if a person wants to transfer property, money, or information, he almost always has to go through a third party. In this situation, the term "transaction" refers to the act of giving something to someone for the purpose of receiving it. However, in this case, the block-chain notion is revolutionary. Proof-Of-Work validates the transaction by looking through all the blocks available in the blockchain and makes the calculation whether this is legitimate transaction or not. In our Blockchain, the Proof-Of Work works by all the blocks validating the transaction and whether the transaction actually exists or not [11].

3.9 Distributed Ledger

A distributed ledger is a data set which is shared, synchronized across different locales, establishments, or geographic areas by a gathering of individuals. It takes into account public "witnesses" to be available during exchanges. Each organization hub's part approaches the accounts shared across the organization and may hold a uniform duplicate of them. Several seconds or minutes, any changes or increments to the record are reflected and duplicated to all members. An appropriated record remains as opposed to an incorporated record, which is that the kind of record that the dominant part organizations use. A solitary mark of disappointment makes a concentrated record more defenseless against digital assaults and misrepresentation. Since past, records are at the guts of financial exchanges, fully intent on recording contracts, installments, purchase sell bargains, or moving resources or property. The excursion which started with recording on earth tablets or papyrus took a tremendous jump with the development of paper. Throughout the most recent couple of many years, PCs have given the technique for record-keeping and record support with extraordinary comfort and speed [13]. With the advancement of technology, knowledge held on computers is evolving into increasingly higher forms that are cryptographically safe, quick, and decentralized. Companies can cash in of this generation in lots of forms, a technique being via distributed ledgers. A distributed ledger is a decentralized ledger of any transactions or contracts this is maintained throughout a couple of locations and people, doing away with the want for a single authority to prevent manipulation. A vital authority isn't required to authorize or validate any transactions on this manner. While centralized ledgers are at risk of cyber-attacks, distributed ledgers are intrinsically extra hard to assault due to the fact an attack should target all the allotted copies on the equal time to be successful. Furthermore, these records are immune to malicious changes by one party. By being difficult to control and attack, distributed ledgers leave extensive transparency. Distributed ledgers also minimize operational inefficiencies, shorten the time it takes to complete a transaction, and are automated, allowing them to operate 24 hours a day, seven days a week, all of which lower total costs for the businesses who utilize them. Distributed ledgers also provide for a smooth flow of data, making it easier for accountants to follow an audit trail when conducting financial audits. This reduces the chances of a company's financial books being compromised by fraud. The reduction in paper usage is also good for the environment.

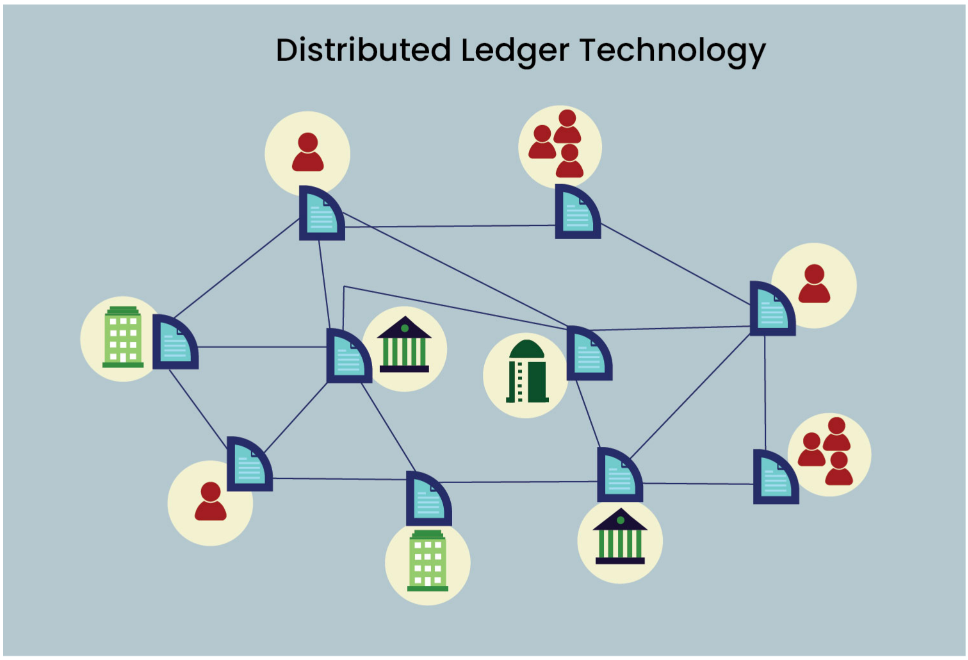


Figure 3.9: Distributed Ledger

3.10 Decentralized System

Decentralization alludes to the development of control and dynamic from an incorporated element (individual, association, or gathering) to a scattered organization with regards to obstruct chain [2]. The idea of decentralization isn't new. Three essential organization plans are frequently analyzed when fostering an innovation arrangement: concentrated, appropriated, and decentralized. While block-chain advancements frequently utilize decentralized organizations, a block- chain application itself can't be arranged just as being decentralized or not. Maybe, decentralization ought to be applied to all parts of a block chain application on a sliding scale. More noteworthy and more pleasant help is regularly refined by decentralizing the administration of and admittance to assets in an application. Decentralization has a few disadvantages, for example, lower exchange throughput, yet the advantages of improved security and administration levels exceed the downsides [4]. Each block-chain convention, decentralized Application (dApp), Decentralized Autonomous Organization (DAO), or other block chain related arrangement embraces fluctuating degrees of decentralization. The selection level is typically upheld the development of the appropriate response, the time-demonstrated unwavering quality of its motivator models and agreement systems, and in this way the capacity of the establishing group to find some kind of harmony. Numerous DAOs, for instance, have segments at different phases of decentralization: prophets (outsider administrations that furnish brilliant agreements with outer data) could be part of the way decentralized, agreements could be completely concentrated, and the administration interaction for changing boundaries could be local area driven and decentralized. Decentralized block-chain arrangements are being investigated and utilized by associations, everything being equal, sizes, and ventures for a bigger scope. Some remarkable models incorporate applications that give quick unfamiliar or crisis help to those that need it most, without the intercession of a bank, government or outsider substance. On the other hand, applications that let individuals to deal with their own computerized characters and information. Today, web-based media stages, organizations, and different gatherings sell this data for a benefit, with no worth to the person. It is simpler to make it populist for everybody on the off chance that it were decentralized.

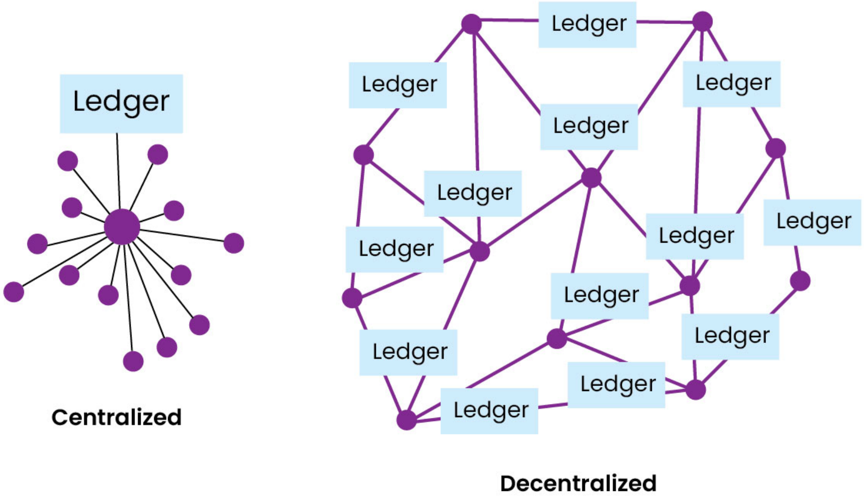


Figure 3.10: Decentralized System

3.11 Smart Contract

Smart contracts inherit the features of the underlying block-chains, together with an immutable information document and the potential to lessen single factors of failure. Smart contracts also can communicate with each other via calls. Smart contracts, in evaluation to standard paper contracts that depend upon middlemen and third-party intermediaries for execution, automate contractual operations, put off contacts among parties, and decrease management costs [10]. Smart contracts on public block-chains, also known as public smart contracts, have attracted a wide range of business applications due to their ease of deployment. While permissioned smart contracts or smart contracts on permissioned block-chains are increasingly commonly employed in collaborative business processes because they offer the ability to avoid unwanted changes, enhance efficiency, and save money. Despite the buzz surrounding block-chain and smart contracts, the technology remains in its early stages.

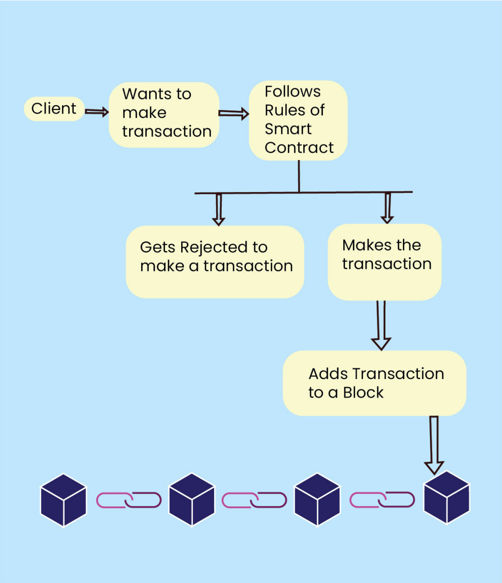

Client
Wants to make transaction
Follows Rules of Smart Contract
Gets Rejected to make a transaction
Makes the transaction
Adds Transaction to a Block

Figure 3.11: Flowchart of Smart Contract

3.11.1 Public Smart Contracts

Public smart contracts set no necessity for companions to take part, consequently all friends reserve the privilege to convey brilliant agreements. While making or conjuring keen agreements on a public block-chain, one is often obliged to pay a charge to forestall spamming. Restricted by it's usefulness, the prearranging language utilized in Bit coin is not really utilized in building complex legally binding terms. While the broadly useful Solidity language in Ethereum may be applied for lots extra extensive collection of utilizations. As in step with Etherscan a few of the one million Ethereum debts that out and out maintain 105.6 million Ethers, 1/2 of of them are contract accounts with a whole equilibrium of 12 million Ether [12]. Contenders, for example, Neo and EOS are additionally autonomous blockchains working with peer agreement and keen agreements. To give peruses an instinctive thought of how keen agreements work on open blockchains, we beneath clarify the component of

Ethereum contracts. For network agreement, Ethereum utilizes the proof of-work (PoW) mining measure. Ethereum brilliant agreements live in Ethereum Virtual Machines (EVMs), which segregates them from the blockchain organization to forestall the code running inside from meddling with different cycles. At the point when a savvy contract is dispatched, it gets an extraordinary location that is attached to an equilibrium, practically identical to a remotely controlled record (EOA) that a client claims. Exchanges can be sent from a brilliant agreement to an EOA or another agreement.

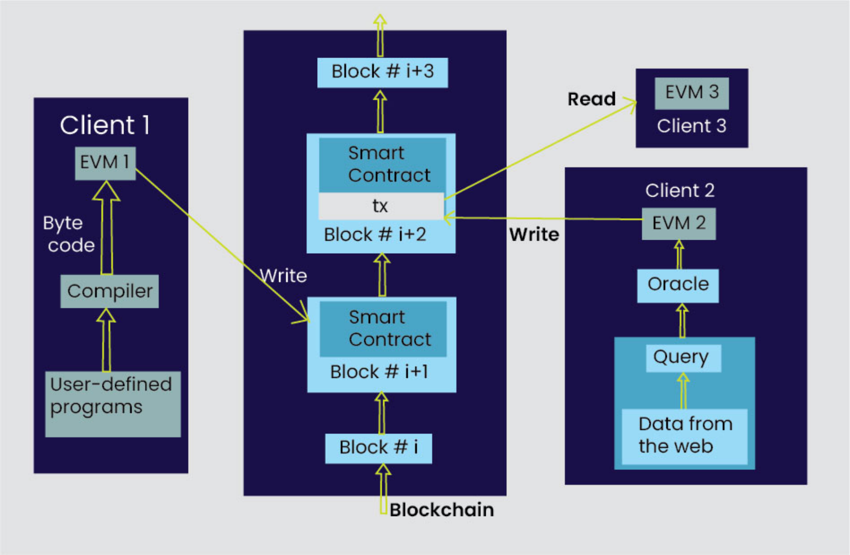


Figure 3.12: Mechanism of Ethereum Smart Contract

3.12 On Chain and Off Chain

On-chain: On-chain transactions are those that take place on a blockchain and are recorded in a distributed, public ledger [25]. On-chain transactions are those that have been verified or authenticated and result in a change to the blockchain network as a whole. On a blockchain, transactions must be authenticated by a number of the network's participants, known as miners. A transaction is only valid once all participants have verified it and reached an agreement on its validity. The transaction facts is sooner or later recorded at the block and dispatched to the network's users. Once a transaction gets sufficient confirmations from network individuals primarily based totally at the network's consensus mechanism, it will become nearly irreversible, relying at the network protocol. In maximum cases, it may best be undone if the bulk of the blockchain's hashing power concurs to undo the transaction.
Off-chain: Off-chain transaction takes the cost outside of the blockchain. It can be carried out the usage of more than one methods. There may be a transfer agreement among transacting events. Using a 3rd party together with a guarantor who ensures to honor the transaction. Present-day price processors together with PayPal work on those lines. A participant purchases coupons in change for the crypto-tokens and offers the code to every other party who can then redeem them. Redemption is feasible with inside the equal crypto-currency or in unique ones, relying at the coupon carrier provider. In the most effective way, events may even change their

personal keys regarding a hard and fast quantity of crypto coins. This way, the coins by no means go away the address/wallet, however the currency gets a brand new proprietor off-chain. To maintain blockchain transactions assure, verifiable, translucent, and fast, on-chain transactions have to take vicinity in actual time. In fact, however, that is not often the case. Before verifying a transaction, on-chain transactions can take a prolonged time to collect an enough variety of verification and authentications from network participants. Additionally, each time a block transaction is added to the blockchain, miners must validate the transactions by utilizing computers to solve complex math problems. If the volume of the transaction is large or the network is congested, it may take the miners longer to validate all of the transactions, especially if the number of miners is limited As a result, the other parties file a lawsuit. As we discussed above that there are several reasons why an on chain is a problem when architecting a blockchain. So, the solution is we can use off chain to architect a blockchain. One common use of off-chain storage may be to aid a cache of the maximum latest values of the state of on-chain facts or to preserve up direct for superior seek and analytics [37]. Off-chain facts storage structures may be without difficulty used as a backup to include the big quantity of artifact software facts. This is accomplished via way of means of the use of the point-in-time artifact facts that's saved off-chain. Another essential thing of the off-chain device is that it is able to without difficulty save any kind of actual touchy facts. As on-chain facts is non-negotiable in phrases of modification, this form of trouble does now no longer stand up with the off-chain facts control device. A few of the apparent benefits are:

- It's faster. The transactions are recorded instantly, while not having to look forward to the network confirmations.
- It's cheaper. Transactions performed off-chain are commonly free.
- It's greater private. These transfers aren't seen on the general public blockchain.

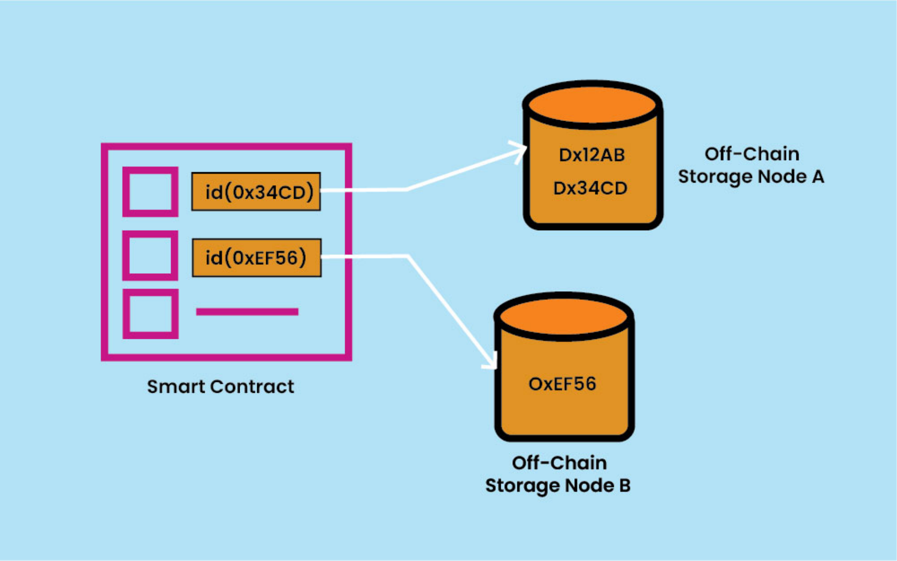


Figure 3.13: Content addressable storage

To keep data off-chain, we use hashed-based content addressable storage in our proposed model. It is too expensive, when a large amount of data associated with a smart contract is stored on-chain. Only the hash value is stored within the smart contract in the hashed based content addressable off chain storage. Users can use the smart contract to retrieve the hash value from on-chain storage, and they can use this hash value to retrieve the main data from off-chain storage. They can check the validity of the data they've retrieved by computing its hashed value and comparing it to the hashed value recorded in the smart contract. Because any change within the records may immediately modify its scope and invalidate its references or the hash value. This storage allows for the trustless outsourcing of records to an off chain storage system. This way, a utility's storage costs can be greatly lowered, and files that couldn't previously be saved on-chain can now be referenced without establishing trust.

3.13 Mining

Block chain is a sort of PC network. Mining is a strategy for checking new transactions. Different approval techniques are utilized by various Block-chain executions. Prior to adding new Block-chain exchanges to the Block, all excavators who are associated with mining are given a numerical riddle to address [13]. This is a difficult numerical issue dependent on the hash technique that must be settled by beast force. There are no alternate ways to taking care of this issue; you should check every conceivable answer for confirm in the event that it is right. Discovering the arrangement doesn't require insight; all things considered, it needs speed up. Proof of-Work is the name given to the numerical arrangement. The Proof-of-work is the excavator has invested the exertion and assets important to get the appropriate response [10]. Block-chain mining, as recently said, requires a lot of assets. The digger acquires a Mining compensation for contributing their time and assets in this.

3.13.1 Working mechanism of mining

Block-chain is a type of computer network. Mining is nearly impossible on a standard desktop computer, and it necessitates specialized gear with better computational speeds. Individual mining and mining pools are the two methods of mining.

3.13.2 Individual mining

Each miner will installation their hardware and check in for mining here. When new transactions occur, all miners in that Block-chain community are provided with a mathematical puzzle. The hardware of the miners starts off evolved to paintings on a solution. The first miner to find out the answer informs all different miners of its discovery. To keep away from wrong certification of the Block, the alternative miners then confirm it. Once the miner's solution is verified, the miner gets the reward, and the transactions are delivered to the Block-chain.

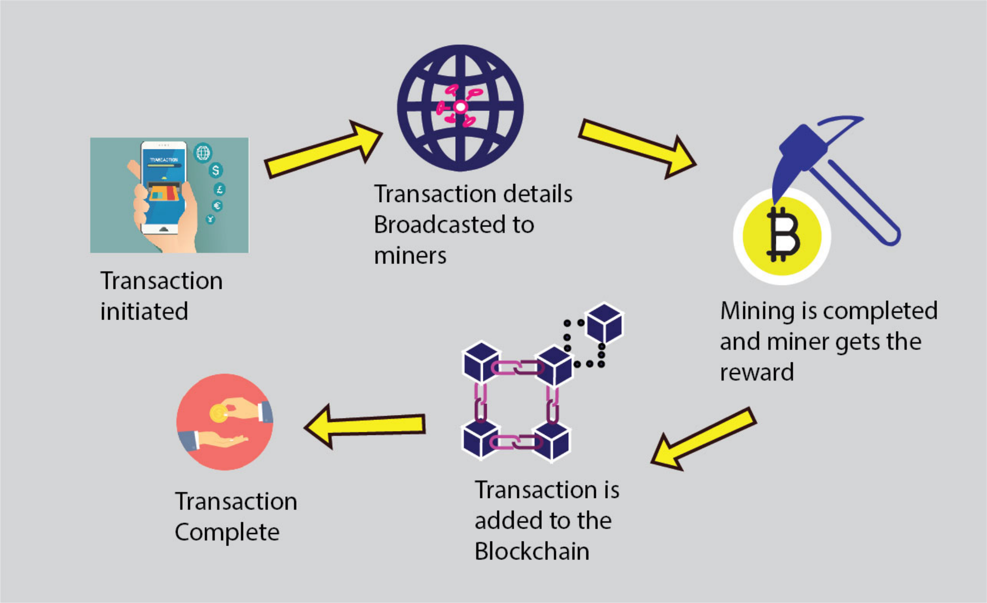

Transaction initiated
Transaction details Broadcasted to miners
Mining is completed and miner gets the reward
Transaction is added to the Blockchain
Transaction Complete

Figure 3.14: Individual Mining

3.13.3 Mining Pool

A mining pool is a joint organization of cryptocurrency miners who integrate their computational assets over a community to reinforce the opportunity of locating a block or in any other case efficiently mining for cryptocurrency. A sole miner may not every time has the assets to mine the Block-chain. In this case, a Mining Pool is formed by a assemble of miners [28].

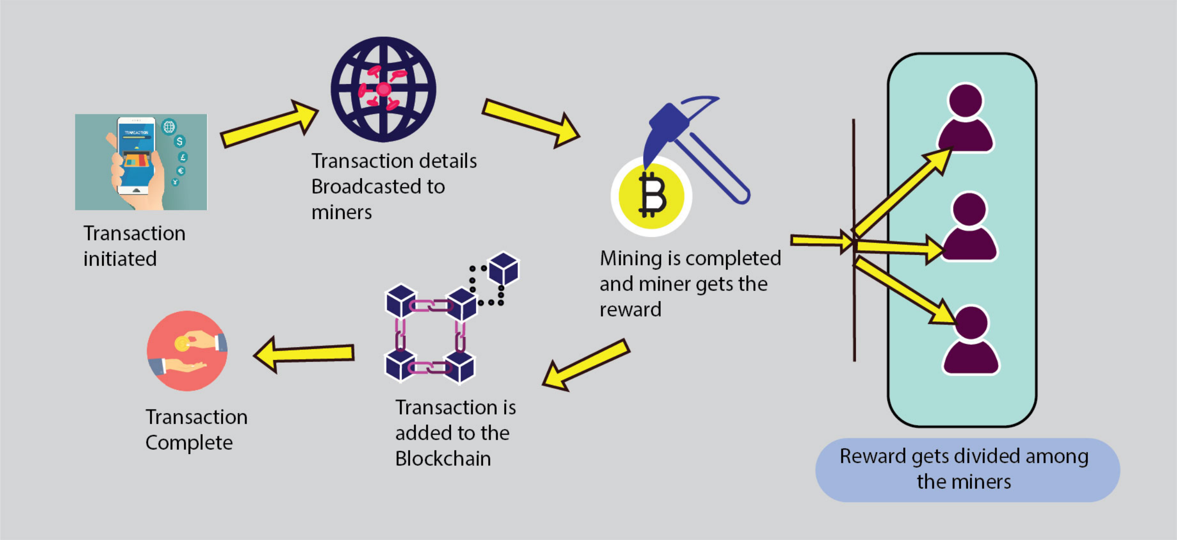

Transaction initiated
Transaction details Broadcasted to miners
Mining is completed and miner gets the reward
Transaction is added to the Blockchain
Transaction Complete
Reward gets divided among the miners

Figure 3.15: Mining Pool

These miners pool their resources in order to mine the Block-chain more quickly. The Mining Pool, like Individual Mining, receives the challenge and is rewarded for successfully solving it. This prize is shared among the miners based on how much they supplied in terms of resources.

3.14 Cryptography

Cryptography is a word that is gotten from the Greek letters ”Kryptos” signifies covered up or secret and ”graphein” signifies to comp top of stack [6]. The workmanship or study of mystery coding, especially figure frameworks and codes. An essential job is played by cryptography for guaranteeing secure correspondence between various substances [2]. The whole component in our block chain system is planned so nobody knows the genuine data of another without the key or the person's assent. For instance, if an individual need to share any sort of data on the square chain with someone else. This data will in like manner be sent through the sender's public key, guaranteeing that nobody will energetically attack it. We constructed the framework with the end goal that this public key is known by each and every individual who needs to execute data or follow that individual. The private key, then again, is a key that lone the client knows and can use for his own motivations in our framework. In the last stage, the client utilizes this private key to get to and modify his own data. This is cozy, and its exposure may represent a significant mischief to that individual, as anybody may follow the genuine key of his hash and unravel it by looking at the general population and private keys.

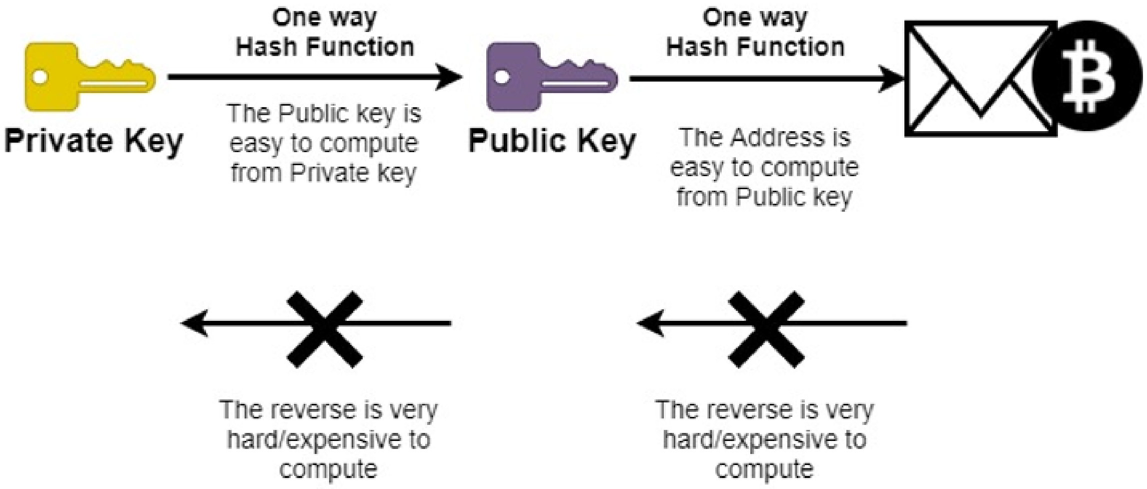

One way
Hash Function
The Public key is easy to compute from Private key
Private Key
Public Key
One way
Hash Function
The Address is easy to compute from Public key
The reverse is very hard/expensive to compute
The reverse is very hard/expensive to compute

Figure 3.16: Hash Cryptography

3.14.1 Public Key

A public key is used to publicly display an individual's information, so that everyone on the block-chain knows who that person is and what additional information he has. Furthermore, the public key is used on the block-chain to transact information between persons. This public key is used to send and receive information and data. The public key is hashed in our system using the person's Gmail account, his National Identification Number (e.g. NID, SSN, SID), his birth date, and a security number that we supply [5]. We used the SHA256 hash, which has proven to be unpredictable in the past. As a result, the hash can never be predicted

3.14.2 Private Key

Aside from the public key in our system, this key access all of a person's information. The private key is used to gain access to all of that person's information as well as to make changes and transactions in his account. Any user in our block-chain system must log in using his private key, and he can only transact and make changes to his account using this key [1].The disclosure of a person's private key poses a major threat to that person's data. Any individual can identify the real key that was used to hash the keys and gain access to that person's account by comparing both the public and private key. We used a Gmail account, the person's National Identification Number, his birth date, a security number, and a password provided by that individual to establish this private key, just as we did with the public key.

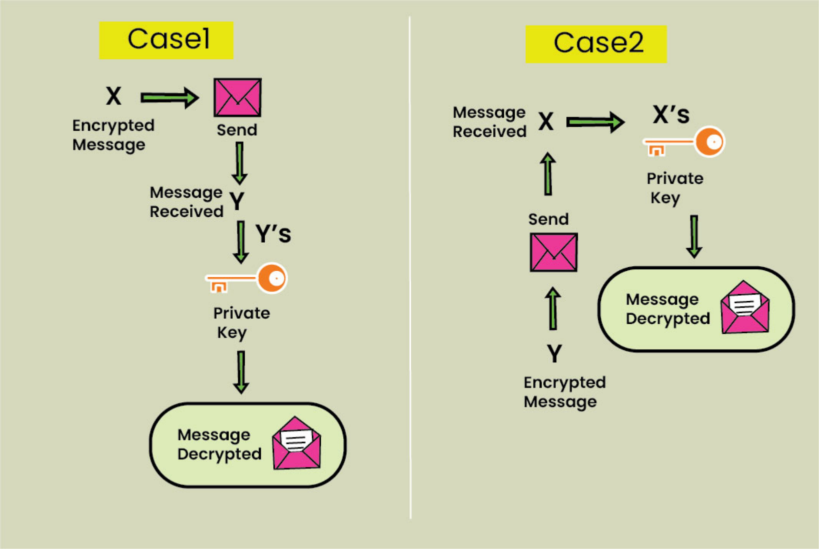


Figure 3.17: Public key and Private key encryption

3.15 Revocation

Revocation is a method of removing or editing a credential. The chance for provider to revoke a credential is vital for identification infrastructure and to makes sure that identities are unique. Attributes can alternate through the years e.g. residence deal, number of children, and some credentials also have an expiry date e.g. passport or driver's license [35]. The truth is however to ensure trustworthiness of the tool and dispose of the possibility to defraud the credentials need to be immutable. After issuing, no one (now not even the company) can alternate the records of the credential. Hence, at the same time as attributes alternate, a brand new credential is issued and the previous one is set to be invalid. Thus, at each proof the user's wants to prove that the credentials used within are nonetheless valid. The revocation registry permits to reveal this without contacting the issuing party [36]. A Revocation Registry has 4 requirements:

- Credentials must be revocable through their provider;
- Revocation must be to the point and fast;

- Testing of revocation must preserve privacy;
- Proving and verifying the proof must be possible without the provider's consent.

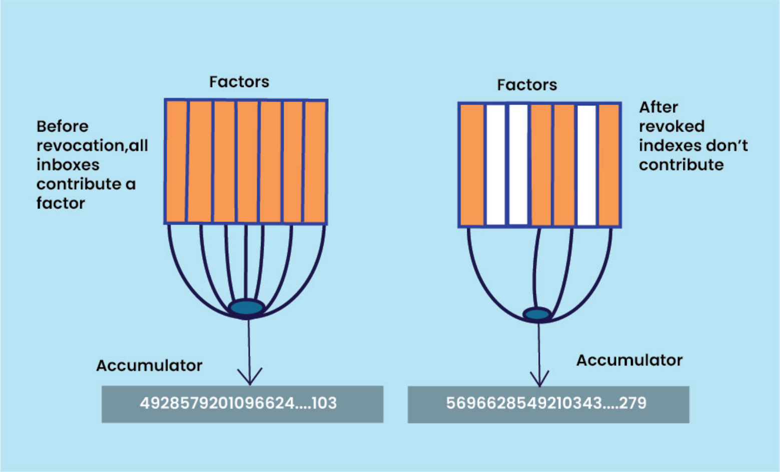

Factors
Before revocation,all inboxes contribute a factor
Accumulator
4928579201096624....103
Factors
After revoked indexes don't contribute
Accumulator
5696628549210343....279

Figure 3.18: Revocation of credentials

The goal is to reveal only the valid information with the help of accumulator. Only the registry of valid information is accounted while generating accumulator. Using this the Identity owner now can prove his or her credential as valid. This is the key concept of revocation registry.

Chapter 4

Blockchain Based Secured Multipurpose Identity Management Architecture

4.1 Proposed Architecture

In our proposed blockchain-based Secured Multipurpose Identity Management System, Government Identity Provider Commission (IDPC) is the main authority. IDPC permits specified authorities and other private organizations to join the network so that they can issue credentials to Citizens (Users) who want to use specific services supplied by the service providers (SP). Citizens (Users) cannot create, alter, or withdraw their identity proofing credentials in this system. Only IDPC and the relevant government trusted authorities can do so.

In this system, IDPC owns the smart contract, but government trusted authorities can integrate credentials into it. IDPC also controls which government trusted authorities have access to which User's credential, while the User can only control which service provider has access to their data. IDPC is responsible for registering and managing Users, it can register Users by reviewing their documents. To register for the network, User uses an IDPC provided registration interface, which can be accessed via a mobile application or a web browser. IDPC produces public-private key pairs through this registration interface. It then generates a blockchain account for the User, which is used to the deploy smart contract across the network, using this public key. Each User's unique identifier is the address of the smart contract which was deployed for them. User credentials can be integrated into smart contracts by IDPC and other government trusted authorities. They store the User's credentials off-chain in a hash based content-addressable storage system. Authority stores this hash value signed by its private key in a smart contract so that the service provider and trusted authority know who issued the credential during the credential authentication process.

In our architecture, a service provider (SP) is not the same as a trusted government authority. The service provider (SP) may be a traffic police who needs to know whether the driver is qualified to drive, and instead of showing the entire driving license, the driver could show a subset of the licensing credential or a modified license credential to verify that he is qualified to drive. IDPC, on the other hand, controls access to User's credentials by government trusted authorities. For example, other than NID information, the Passport provider has no access to any additional User credentials.

Users, on the other hand, can access smart contracts through their smart contract user account. In our proposed system, to prevent identity fraud or theft, Users have to sign in every time they want to access a smart contract. The sign-in mechanism can be biometric to add even more protection. Furthermore, biometric is used in our system to prevent an individual from having several identities.

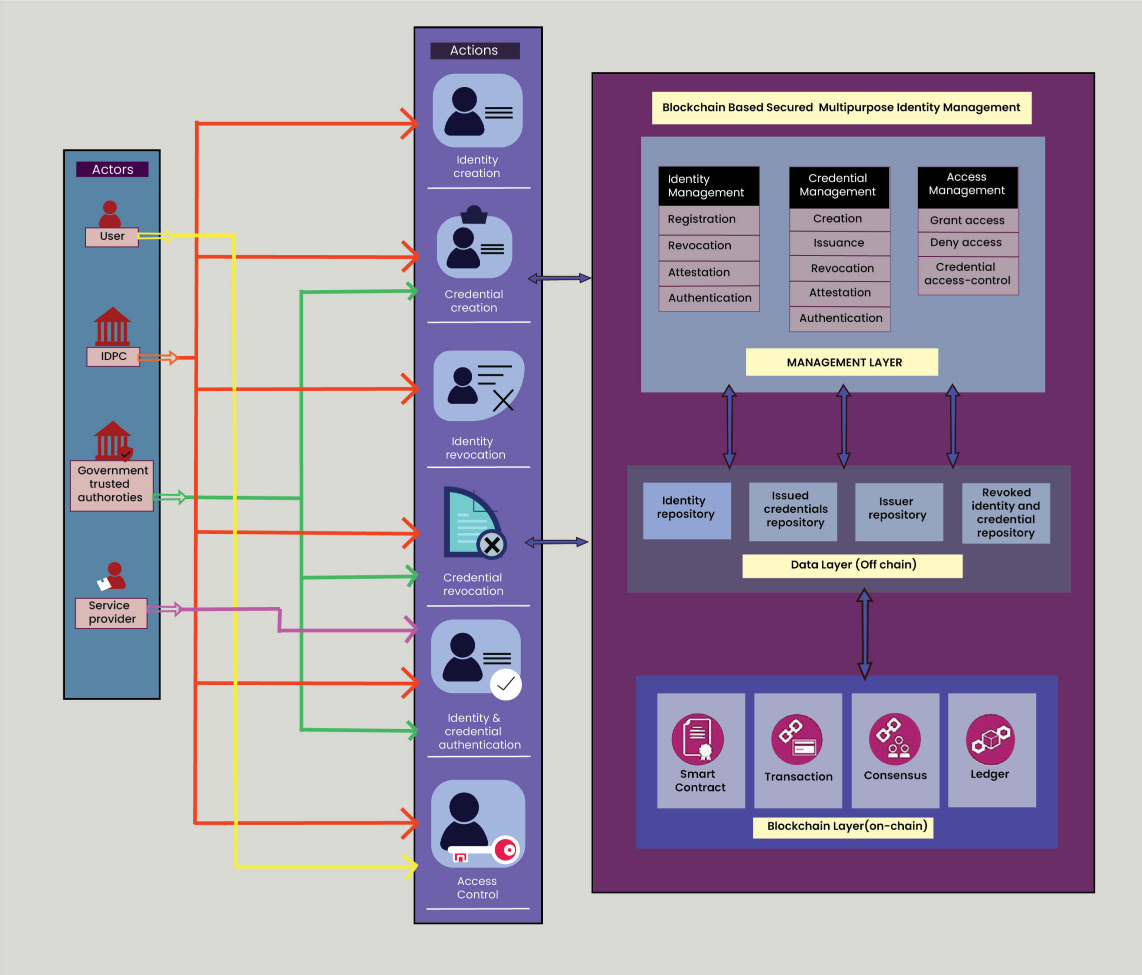


Figure 4.1: Architecture of blockchain based Secured Multipurpose Identity management system

4.2 Proposed Model

4.2.1 Secured Multipurpose Identity (SMID) Registration

In this phase, the Government Identity Provider Commission (IDPC) provides a unique identifier (SMID) to Users. Here, Users are citizens. IDPC provides all the necessary tools to join the blockchain network. It provides a registration interface that is accessible through a mobile app or web browser to create the public-private key pairs and the identifier as well. The User requests for SMID registration and submits the relevant documentation using this web browser or mobile application.

After verifying all the documents, using the registration interface IDPC generates the public-private key pairs. Using the public key IDPC creates a User blockchain account which is used to deploy the smart contract across the network. The address of the smart contract is the User's unique identifier. IDPC encrypts the private key using a credential and stores the association of the public key and the identifier into the blockchain ledger. It creates the credentials and stores the credentials off-chain in a hash based storage system. Credentials can be encrypted and kept in off-chain storage for additional security. The hash is then stored inside the blockchain ledger after signing it with IDPC's private key. And at the end of the registration phase, IDPC returns the signed hash value, identifier, public key, and the encrypted private key to the User. The hash value is then signed with the User's private key and stored in the User's device along with other received data. This hash value can be used to retrieve credentials from the content-addressable off-chain storage system.IDPC additionally takes the user's biometric information during this phase and stores the association of the identifier and biometric information on-chain. So that if the user later requests SMID, it can be easily identified that he has already been assigned a SMID

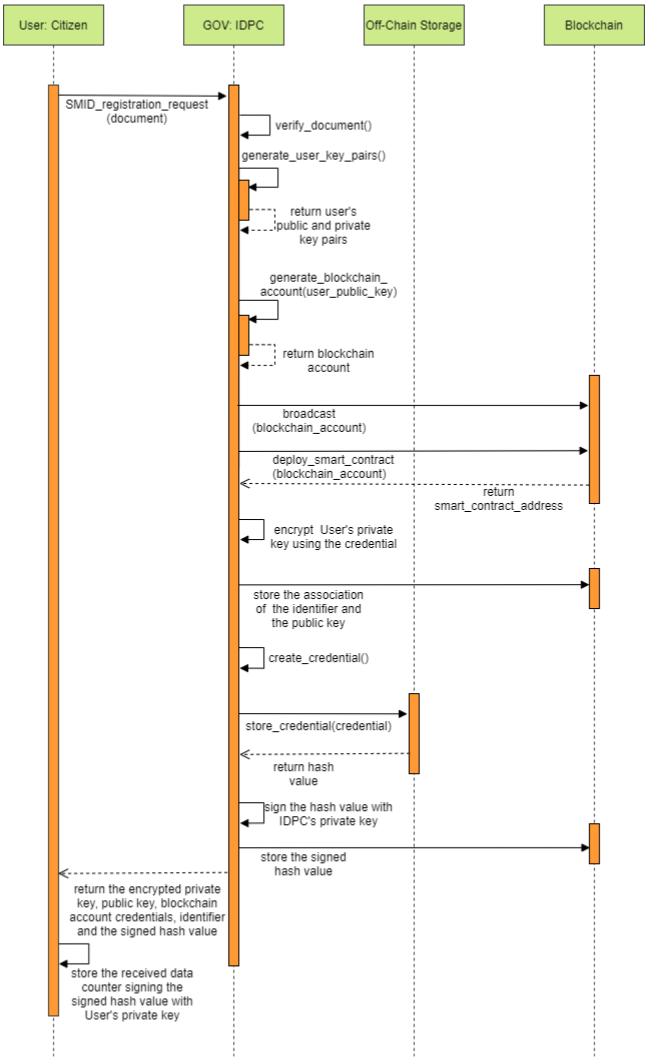

User: Citizen
GOV: IDPC
Off-Chain Storage
Blockchain
SMID_registration_request (document)
verify_document()
generate_user_key_pairs()
return user's public and private key pairs
generate_blockchain_ account(user_public_key)
return blockchain account
broadcast (blockchain_account)
deploy_smart_contract (blockchain_account)
return smart_contract_address
encrypt User's private key using the credential
store the association of the identifier and the public key
create_credential()
store_credential(credential)
return hash value
sign the hash value with IDPC's private key
store the signed hash value
return the encrypted private key, public key, blockchain account credentials, identifier and the signed hash value
store the received data counter signing the signed hash value with User's private key

Figure 4.2: SMID registration sequence diagram

Data = Sign (Hash (credentials), IDPCPRIVATEKEY)
UserDeviceData = Sign (Data, UserPRIVATEKEY)

IDPC additionally takes the user's biometric information during this phase and stores the association of the identifier and biometric information on-chain. So that if the same user later requests for SMID again, it can be easily identified that the person has already been assigned a SMID.

4.2.2 Credentials Registration By Government Trusted Authorities

Government trusted authorities can be Passport providers, Driving License providers (DMV), Insurance Company and so on. If a User has already received credentials from these trusted authorities before registering for SMID, IDPC will store all of the required credentials off-chain in a hash based system during the SMID registration phase. Otherwise, the User can later register their credentials in the following way. The User needs to authenticate himself to trusted authorities. The steps of the User Identity authentication process is given below:

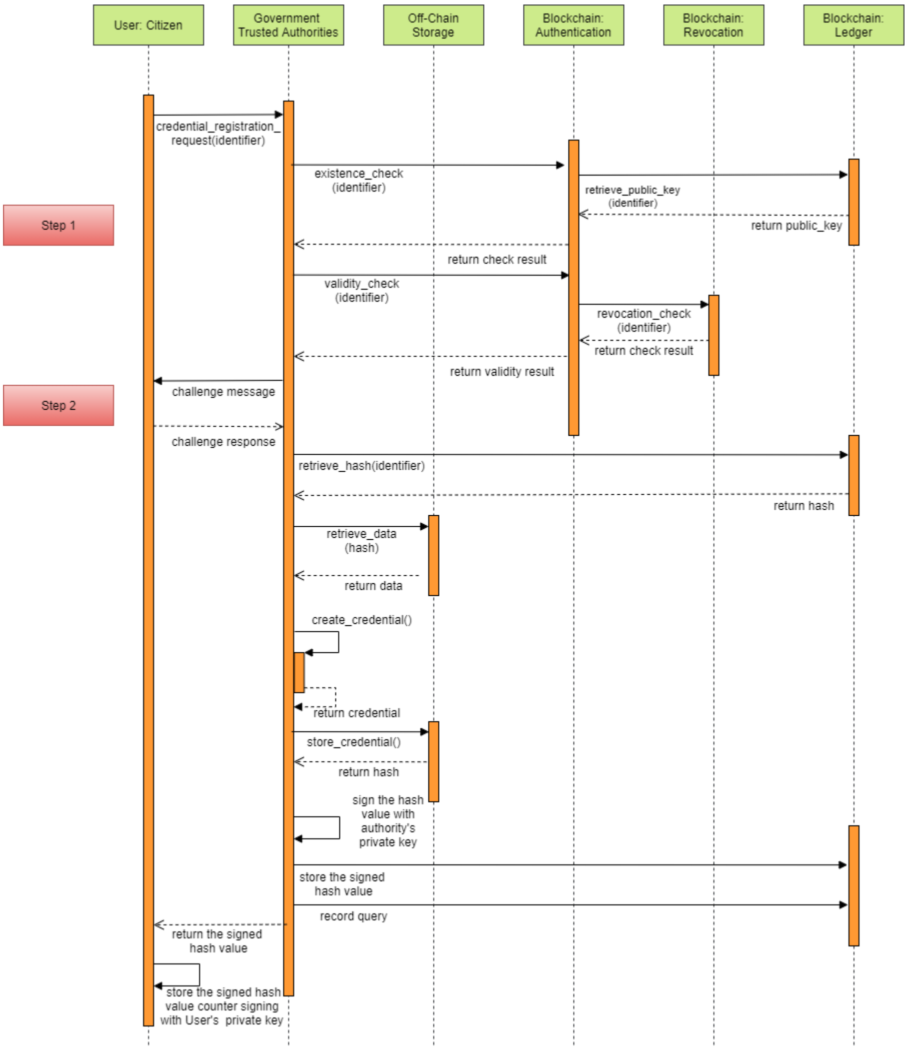

User: Citizen
Government Trusted Authorities
Off-Chain Storage
Blockchain: Authentication
Blockchain: Revocation
Blockchain: Ledger
Step 1
Step 2
credential_registration_request(identifier)
existence_check (identifier)
retrieve_public_key (identifier)
return public_key
return check result
validity_check (identifier)
revocation_check (identifier)
return check result
return validity result
challenge message
challenge response
retrieve_hash(identifier)
return hash
retrieve_data (hash)
return data
create_credential()
return credential
store_credential()
return hash
sign the hash value with authority's private key
store the signed hash value
record query
return the signed hash value
store the signed hash value counter signing with User's private key

Figure 4.3: Credential registration by Government Trusted Authority sequence diagram

Step 1: User submits a request for credentials to a trusted authority, along with its identifier. This identifier is used by the Authority to retrieve the public key from the blockchain ledger, and it ensures that the identifier is registered and verified by IDPC. As a result, the existence of the identification is validated. Following that, the identifier is checked for validity using the revocation function.
Step2: Next, the authority sends a random challenge to the User signing it with the User's public key. After receiving it, the User makes a digital signature using the random challenge and his private key and sends it back to the authority. The correct response guarantees that the public key and the identifier belong to the User.

In our proposed model, which user-credentials a trusted authority can access will be predefined. As a result, a trusted authority can only access specified credentials using an identifier. The hash value can be retrieved from the blockchain ledger using the identifier, and the data can be retrieved from off-chain storage using the hash value. In addition, a record of this query will be kept so that Users can see who has accessed their credentials.

Following that, the authority can generate a new credential and store it off-chain by its hash value. The authority then generates a digital signature using the hash value and private key, stores it in blockchain and returns it to the User. In IDPC's repository, all the trusted authorities' public keys associating with their identifiers will be maintained and can be updated by IDPC as well.

4.2.3 Service Provisioning

Service provisioning represents the phase where the User can access services provided by the Service Provider (SP) after the authentication of User's identity and credentials. In this phase there is two authentication process:

1. User Identity Authentication Process: The process is similar to the identity authentication process in the credentials registration phase. At first SP, checks the existence of the User's identifier and then validates whether it belongs to the User.
2. Credential Authentication Process: SP requests User's information after completing the identity authentication process. The User can provide the entire credential or a subset of it from their device. He can also provide modified credentials to SP to ensure minimal credential disclosure. SP uses the User's public key, which is stored in the blockchain, to verify that the supplied credential belongs to the User, and then it uses the Issuer's (Government Trusted Authority) public key, which is also stored in the blockchain, to verify that the credential was issued by a specific authority. SP then uses the revocation function to verify that the User's credentials are still valid. A record of which SP, User granted their credential will be maintained inside the blockchain.

After authenticating the User's identity and credentials SP provides the requested service to the User.

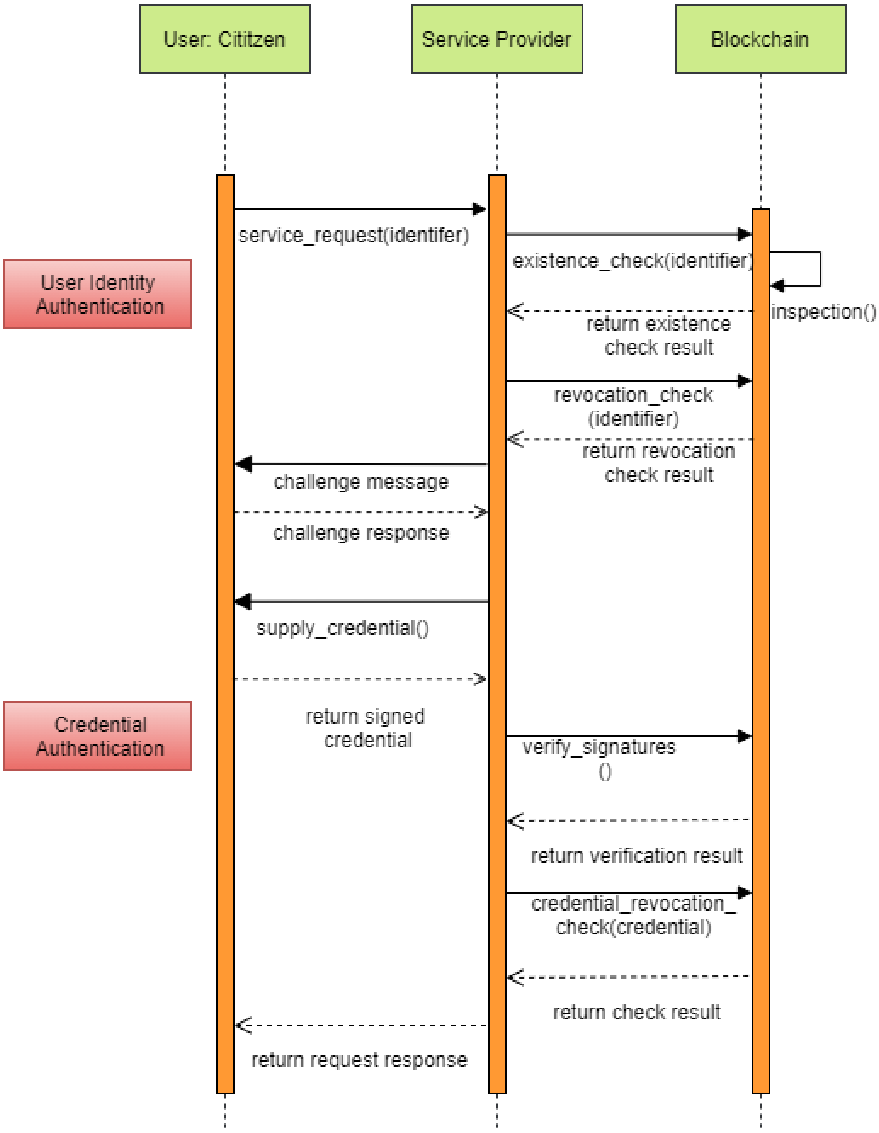

User: Cititzen
Service Provider
Blockchain
User Identity Authentication
Credential Authentication
service_request(identifer)
existence_check(identifier)
inspection()
return existence check result
revocation_check (identifier)
return revocation check result
challenge message
challenge response
supply_credential()
return signed credential
verify_signatures ()
return verification result
credential_revocation_check(credential)
return check result
return request response

Figure 4.4: Service provisioning sequence diagram

4.2.4 Identity and Credential Revocation

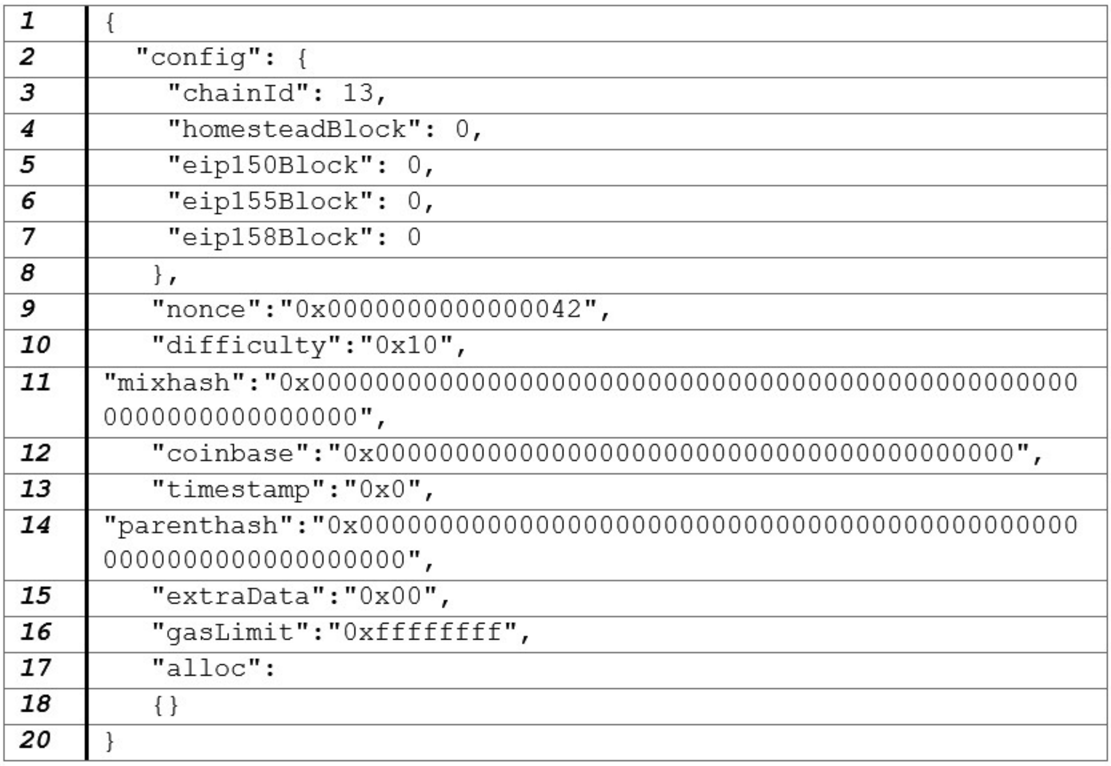
Identity revocation is used to invalidate a User identifier so that he can no longer access network resources using that identifier, whereas credential revocation is used to delete or update any credential. Issuers can update any User credential and store it inside the blockchain after invalidating the previous credential. There is a separate revocation repository in our proposed model that only contains revoked identities and credentials. The Issuer (Government Trusted Authority) and Service Provider (SP) can validate the validity of the User's identity and credential during any identity and credential authentication process by parsing the revocation repository.

Chapter 5

Implementation

For the implementation of our proposed model, we created test Blockchain using Ethereum Go in our machine. In methodology, we already explained the methods and many keywords that we will be using for implementation. For our test blockchain, we used Windows Operating System and installed Geth which allowed us to use create test blockchain using Ethereum Go client. We created Ethereum node in our machine in order to test and deploy our smart contact on our blockchain.

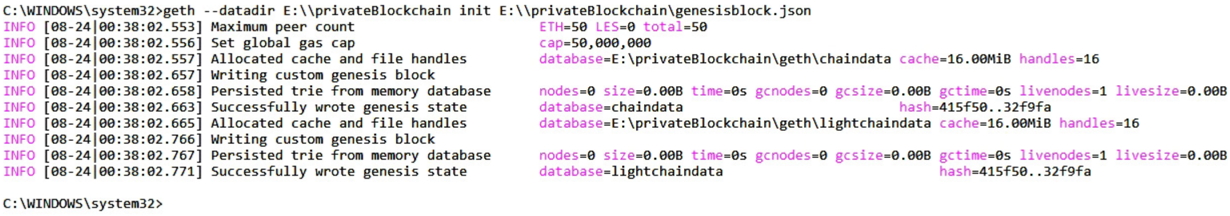
First, we had to create the directories where we will be storing files of our blockchain and genesis block. The Genesis block would become the first block of the chain and other blocks will build on it. Code that we used for the Genesisblock.json of our test Blockchain is given below.



```
{
  "config": {
    "chainId": 13,
    "homesteadBlock": 0,
    "eip150Block": 0,
    "eip155Block": 0,
    "eip158Block": 0
   },
   "nonce":"0x0000000000000042",
   "difficulty":"0x10",
"mixhash":"0x000000000000000000000000000000000000000000000000
0000000000000000",
   "coinbase":"0x0000000000000000000000000000000000000000",
   "timestamp":"0x0",
"parenthash":"0x000000000000000000000000000000000000000000000
0000000000000000000",
   "extraData":"0x00",
   "gasLimit":"0xffffffff",
   "alloc":
   {}
}
```

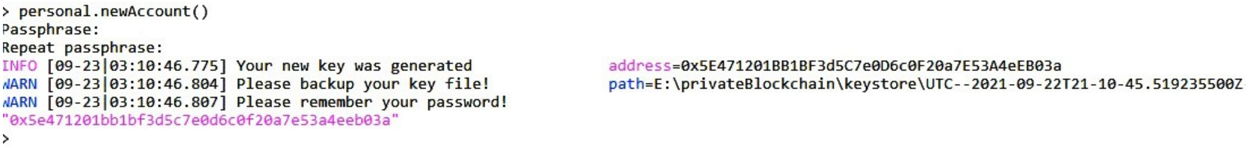
Figure 5.1: Code of Genesisblock.json

Here we set certain values in the genesis block to help us create the blockchain easily. The value of nonce and chainId are randomly generated. Being the first block the parenthash is set to all zeros as there is no block before it. As this is a test chain the value of difficulty is set to a lower value so that we can mine new blocks to the chain faster. Similarly, no value is added to the extraData block for this test blockchain. Next, we initialized our Genesisblock.json to create the blockchain. Once we successfully wrote the genesis state, we need to start creating Ethereum accounts. We use Ethereum accounts for transactions and generate test ethers in the accounts by mining. These Ethereum accounts with ethers are used to deploy the smart contract into our test blockchain.



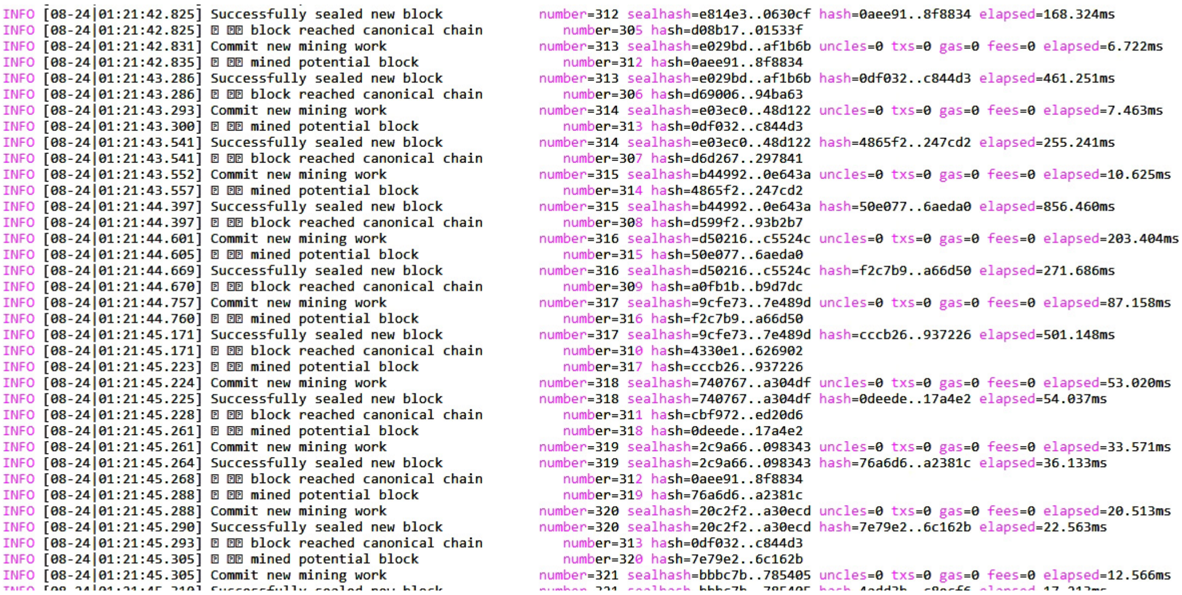
```
C:\WINDOWS\system32>geth --datadir E:\\privateBlockchain init E:\\privateBlockchain\genesisblock.json
INFO [08-24|00:38:02.553] Maximum peer count                       ETH=50 LES=0 total=50
INFO [08-24|00:38:02.556] Set global gas cap                       cap=50,000,000
INFO [08-24|00:38:02.557] Allocated cache and file handles         database=E:\privateBlockchain\geth\chaindata cache=16.00MiB handles=16
INFO [08-24|00:38:02.657] Writing custom genesis block
INFO [08-24|00:38:02.658] Persisted trie from memory database      nodes=0 size=0.00B time=0s gcnodes=0 gcsize=0.00B gctime=0s livenodes=1 livesize=0.00B
INFO [08-24|00:38:02.663] Successfully wrote genesis state         database=chaindata                      hash=415f50..32f9fa
INFO [08-24|00:38:02.665] Allocated cache and file handles         database=E:\privateBlockchain\geth\lightchaindata cache=16.00MiB handles=16
INFO [08-24|00:38:02.766] Writing custom genesis block
INFO [08-24|00:38:02.767] Persisted trie from memory database      nodes=0 size=0.00B time=0s gcnodes=0 gcsize=0.00B gctime=0s livenodes=1 livesize=0.00B
INFO [08-24|00:38:02.771] Successfully wrote genesis state         database=lightchaindata                      hash=415f50..32f9fa

C:\WINDOWS\system32>
```

Figure 5.2: Initializing genesisblock.json



```
> personal.newAccount()
Passphrase:
Repeat passphrase:
INFO [09-23|03:10:46.775] Your new key was generated               address=0x5E471201BB1BF3d5C7e0D6c0F20a7E53A4eEB03a
WARN [09-23|03:10:46.804] Please backup your key file!             path=E:\privateBlockchain\keystore\UTC--2021-09-22T21-10-45.519235500Z
WARN [09-23|03:10:46.807] Please remember your password!
"0x5e471201bb1bf3d5c7e0d6c0f20a7e53a4eeb03a"
>
```

Figure 5.3: Creating new Ethereum Account



```
INFO [08-24|01:21:42.825] Successfully sealed new block            number=312 sealhash=e814e3..0630cf hash=0aee91..8f8834 elapsed=168.324ms
INFO [08-24|01:21:42.825] □ □□ block reached canonical chain          number=305 hash=d08b17..01533f
INFO [08-24|01:21:42.831] Commit new mining work                   number=313 sealhash=e029bd..af1b6b uncles=0 txs=0 gas=0 fees=0 elapsed=6.722ms
INFO [08-24|01:21:42.835] □ □□ mined potential block                  number=312 hash=0aee91..8f8834
INFO [08-24|01:21:43.286] Successfully sealed new block            number=313 sealhash=e029bd..af1b6b hash=0df032..c844d3 elapsed=461.251ms
INFO [08-24|01:21:43.286] □ □□ block reached canonical chain          number=306 hash=d69006..94ba63
INFO [08-24|01:21:43.293] Commit new mining work                   number=314 sealhash=e03ec0..48d122 uncles=0 txs=0 gas=0 fees=0 elapsed=7.463ms
INFO [08-24|01:21:43.300] □ □□ mined potential block                  number=313 hash=0df032..c844d3
INFO [08-24|01:21:43.541] Successfully sealed new block            number=314 sealhash=e03ec0..48d122 hash=4865f2..247cd2 elapsed=255.241ms
INFO [08-24|01:21:43.541] □ □□ block reached canonical chain          number=307 hash=d6d267..297841
INFO [08-24|01:21:43.552] Commit new mining work                   number=315 sealhash=b44992..0e643a uncles=0 txs=0 gas=0 fees=0 elapsed=10.625ms
INFO [08-24|01:21:43.557] □ □□ mined potential block                  number=314 hash=4865f2..247cd2
INFO [08-24|01:21:44.397] Successfully sealed new block            number=315 sealhash=b44992..0e643a hash=50e077..6aeda0 elapsed=856.460ms
INFO [08-24|01:21:44.397] □ □□ block reached canonical chain          number=308 hash=d599f2..93b2b7
INFO [08-24|01:21:44.601] Commit new mining work                   number=316 sealhash=d50216..c5524c uncles=0 txs=0 gas=0 fees=0 elapsed=203.404ms
INFO [08-24|01:21:44.605] □ □□ mined potential block                  number=315 hash=50e077..6aeda0
INFO [08-24|01:21:44.669] Successfully sealed new block            number=316 sealhash=d50216..c5524c hash=f2c7b9..a66d50 elapsed=271.686ms
INFO [08-24|01:21:44.670] □ □□ block reached canonical chain          number=309 hash=a0fb1b..b9d7dc
INFO [08-24|01:21:44.757] Commit new mining work                   number=317 sealhash=9cfe73..7e489d uncles=0 txs=0 gas=0 fees=0 elapsed=87.158ms
INFO [08-24|01:21:44.760] □ □□ mined potential block                  number=316 hash=f2c7b9..a66d50
INFO [08-24|01:21:45.171] Successfully sealed new block            number=317 sealhash=9cfe73..7e489d hash=cccb26..937226 elapsed=501.148ms
INFO [08-24|01:21:45.171] □ □□ block reached canonical chain          number=310 hash=4330e1..626902
INFO [08-24|01:21:45.223] □ □□ mined potential block                  number=317 hash=cccb26..937226
INFO [08-24|01:21:45.224] Commit new mining work                   number=318 sealhash=740767..a304df uncles=0 txs=0 gas=0 fees=0 elapsed=53.020ms
INFO [08-24|01:21:45.225] Successfully sealed new block            number=318 sealhash=740767..a304df hash=0deede..17a4e2 elapsed=54.037ms
INFO [08-24|01:21:45.228] □ □□ block reached canonical chain          number=311 hash=cbf972..ed20d6
INFO [08-24|01:21:45.261] □ □□ mined potential block                  number=318 hash=0deede..17a4e2
INFO [08-24|01:21:45.261] Commit new mining work                   number=319 sealhash=2c9a66..098343 uncles=0 txs=0 gas=0 fees=0 elapsed=33.571ms
INFO [08-24|01:21:45.264] Successfully sealed new block            number=319 sealhash=2c9a66..098343 hash=76a6d6..a2381c elapsed=36.133ms
INFO [08-24|01:21:45.268] □ □□ block reached canonical chain          number=312 hash=0aee91..8f8834
INFO [08-24|01:21:45.288] □ □□ mined potential block                  number=319 hash=76a6d6..a2381c
INFO [08-24|01:21:45.288] Commit new mining work                   number=320 sealhash=20c2f2..a30ecd uncles=0 txs=0 gas=0 fees=0 elapsed=20.513ms
INFO [08-24|01:21:45.290] Successfully sealed new block            number=320 sealhash=20c2f2..a30ecd hash=7e79e2..6c162b elapsed=22.563ms
INFO [08-24|01:21:45.293] □ □□ block reached canonical chain          number=313 hash=0df032..c844d3
INFO [08-24|01:21:45.305] □ □□ mined potential block                  number=320 hash=7e79e2..6c162b
INFO [08-24|01:21:45.305] Commit new mining work                   number=321 sealhash=bbbc7b..785405 uncles=0 txs=0 gas=0 fees=0 elapsed=12.566ms
```

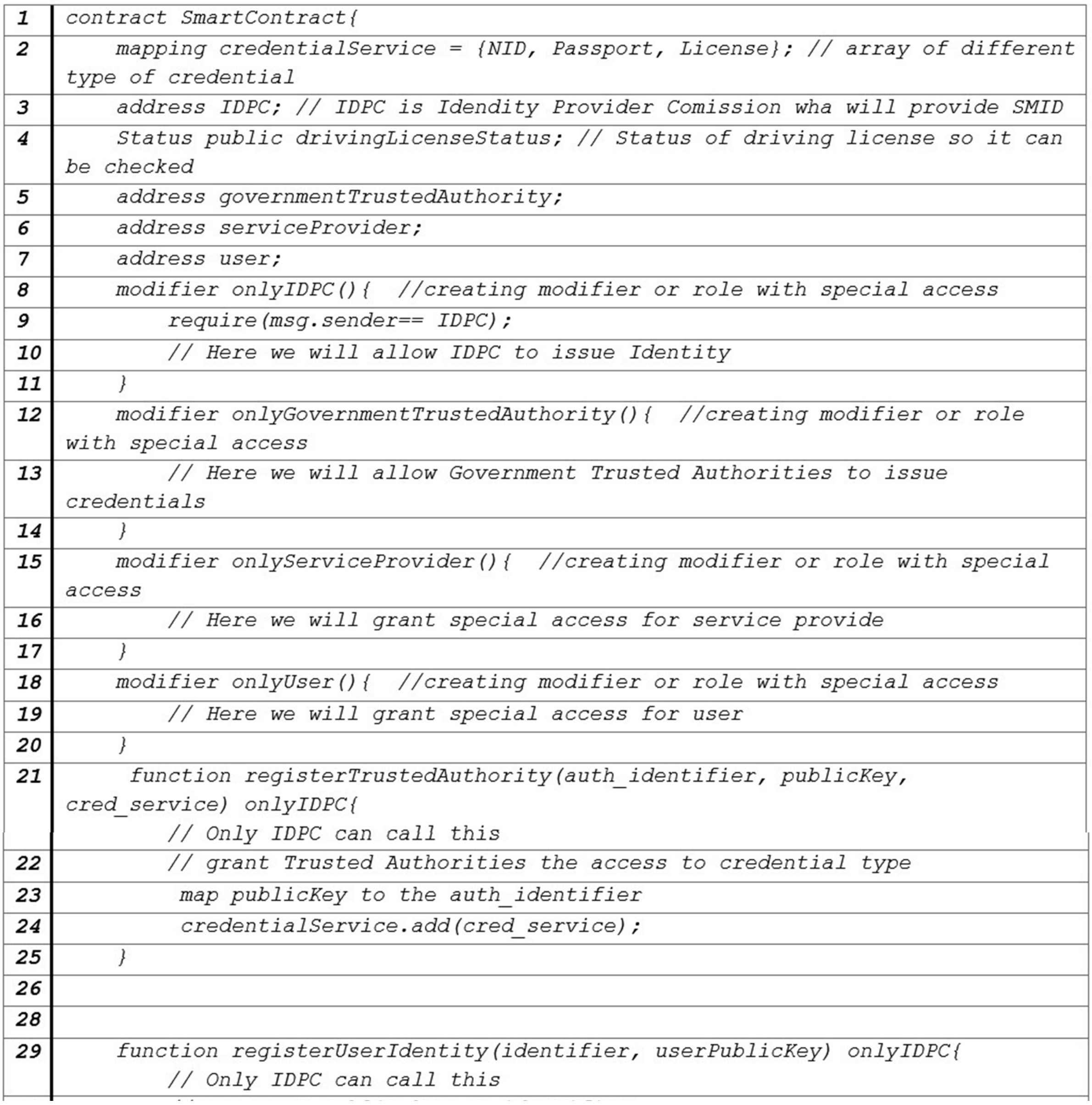
Figure 5.4: Mining process

We interacted and used geth though the command prompt of our Windows machine. For geth command we can either use the “geth –” to access the geth commands or enter into geth console to access them. We used the console and bellow we listed few console commands that we used throughout the process of creating our test blockchain.

Console Commands	**Explanation**
personal.newAccount()	Creates a new Ethereum account
eth.accounts	Show the list of Ethereum accounts created
eth.getBalance(“address“)	Shows the balance of the account address
personal.unlockAccount(“address”)	Unlock account for transfer of ether
miner.start()	Starts mining process
miner.stop()	Stops mining process

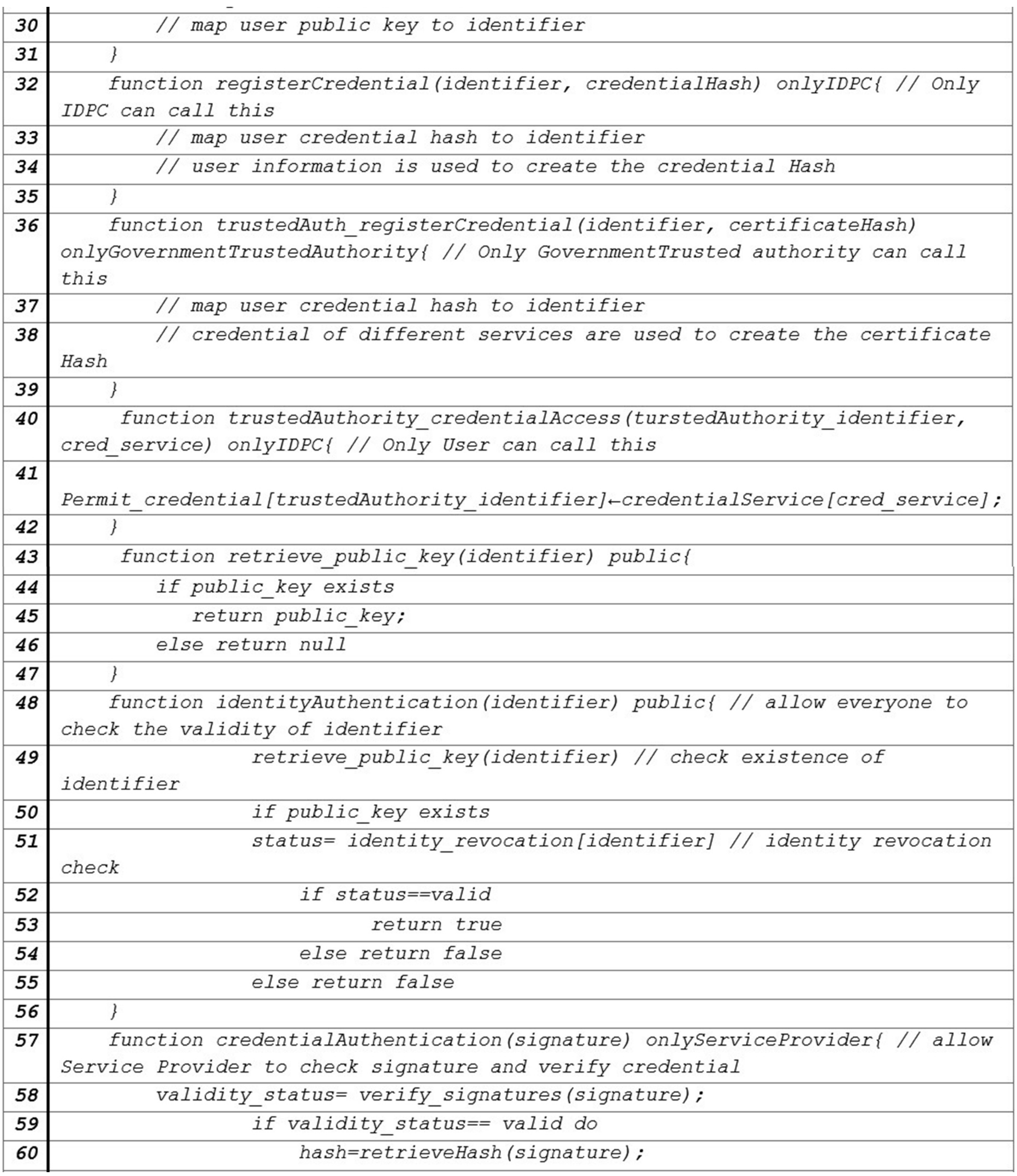
Table 5.1: Ethereum Blockchain Commands

We also created a demo Smart Contract to show some of the potential applications of our proposed method. We have used the language Solidity for our Ethereum based Smart Contract and compiled using the online Remix IDE. The pseudo code of our demo Smart Contract is shown below.



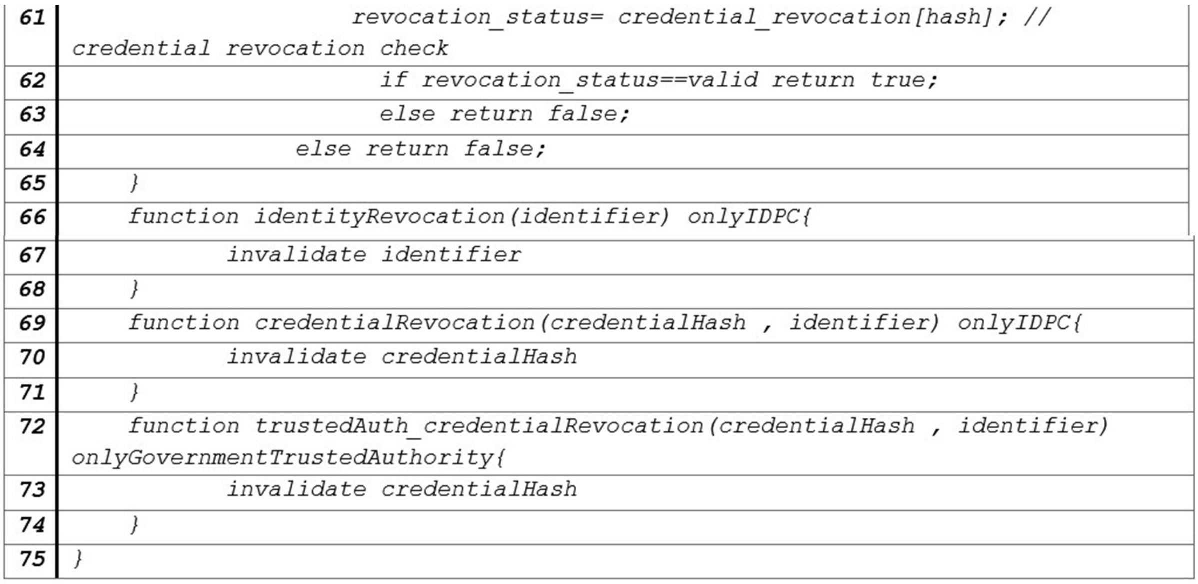
```
contract SmartContract{
    mapping credentialService = {NID, Passport, License}; // array of different type of credential
    address IDPC; // IDPC is Idendity Provider Comission wha will provide SMID
    Status public drivingLicenseStatus; // Status of driving license so it can be checked
    address governmentTrustedAuthority;
    address serviceProvider;
    address user;
    modifier onlyIDPC(){  //creating modifier or role with special access
        require(msg.sender== IDPC);
        // Here we will allow IDPC to issue Identity
    }
    modifier onlyGovernmentTrustedAuthority(){  //creating modifier or role with special access
        // Here we will allow Government Trusted Authorities to issue credentials
    }
    modifier onlyServiceProvider(){  //creating modifier or role with special access
        // Here we will grant special access for service provide
    }
    modifier onlyUser(){  //creating modifier or role with special access
        // Here we will grant special access for user
    }
     function registerTrustedAuthority(auth_identifier, publicKey, cred_service) onlyIDPC{
        // Only IDPC can call this
        // grant Trusted Authorities the access to credential type
         map publicKey to the auth_identifier
         credentialService.add(cred_service);
    }


    function registerUserIdentity(identifier, userPublicKey) onlyIDPC{
        // Only IDPC can call this
```

Figure 5.5: Pseudo Code of Smart Contact- part 1



```
        // map user public key to identifier
    }
    function registerCredential(identifier, credentialHash) onlyIDPC{ // Only IDPC can call this
        // map user credential hash to identifier
        // user information is used to create the credential Hash
    }
    function trustedAuth_registerCredential(identifier, certificateHash) onlyGovernmentTrustedAuthority{ // Only GovernmentTrusted authority can call this
        // map user credential hash to identifier
        // credential of different services are used to create the certificate Hash
    }
     function trustedAuthority_credentialAccess(turstedAuthority_identifier, cred_service) onlyIDPC{ // Only User can call this
Permit_credential[trustedAuthority_identifier]←credentialService[cred_service];
    }
     function retrieve_public_key(identifier) public{
        if public_key exists
           return public_key;
        else return null
    }
    function identityAuthentication(identifier) public{ // allow everyone to check the validity of identifier
                retrieve_public_key(identifier) // check existence of identifier
                if public_key exists
                status= identity_revocation[identifier] // identity revocation check
                    if status==valid
                          return true
                    else return false
                else return false
    }
    function credentialAuthentication(signature) onlyServiceProvider{ // allow Service Provider to check signature and verify credential
        validity_status= verify_signatures(signature);
                if validity_status== valid do
                    hash=retrieveHash(signature);
```

Figure 5.6: Pseudo Code of Smart Contact-part 2



```
                    revocation_status= credential_revocation[hash]; // credential revocation check
                        if revocation_status==valid return true;
                        else return false;
                else return false;
    }
    function identityRevocation(identifier) onlyIDPC{
        invalidate identifier
    }
    function credentialRevocation(credentialHash , identifier) onlyIDPC{
        invalidate credentialHash
    }
    function trustedAuth_credentialRevocation(credentialHash , identifier) onlyGovernmentTrustedAuthority{
        invalidate credentialHash
    }
}
```

Figure 5.7: Pseudo Code of Smart Contact-part 3

We introduced a smart contract template with 11 primary functions in our blockchain-based Secured Multipurpose Identity management system, as shown in the figure above. The following are the key features of these functions.

- registerTrustedAuthority: IDPC use this function to register government trusted authorities, store their public keys on the blockchain network and thus adds trusted authority provided credential service on the network. If any government authority or private organization wants to collaborate with IDPC or wants to add their services in our secured multipurpose identity system, using this function IDPC can register them and their credential service on the blockchain network.

- registerUserIdentity: IDPC use this function to register User and store their public keys on the blockchain network. The public key is stored with their corresponding smart contract address, which is their unique identifier. IDPC uses this function to register a citizen (User) on the blockchain network when he requests SMID registration.

- registerCredential: This function allows IDPC to register User's credential on the blockchain network by storing the returned hash value from the content addressable storage system. IDPC stores the hash value signing it with its private key. The signed hash value is stored associating with their corresponding identifier. This function registers User credentials after the registration of User identifier on the blockchain network.

- trustedAuth_registerCredential: Trusted authorities use this function to store the returned hash value from the content addressable storage system and register the User's certificate or credential on the blockchain network. The private key of the trusted authority is used to sign the credential or certificate. The signed hash value is stored associating with their corresponding identifier. This function only registers trusted authority given credentials on the blockchain, if the User's identity and credential authentication are both true.

- trustedAuthority_credentialAccess: IDPC uses this authorization function to determine which trusted authority has access to which user credential. IDPC uses this function to regulate authority access to User's credentials because not all trusted authorities require access to all of the user's certificates or credentials. For example, a passport provider does not require a user's driver's license to create a passport, which is why IDPC prevents passport providers from accessing any of the user's credentials other than NID information.

- retrieve_public_key: Using the user's, trusted authority's, or IDPC's unique identifier, anyone can retrieve the public key of the user, trusted authority, or IDPC. Retrieving the public key ensures that the identifier corresponds to the entity that has it.

- identityAuthentication: This function allows anyone to check the validity of an identifier by checking its existence calling the function retrieve_public_key and checking whether the identifier was revoked.

- credentialAuthentication: This function allows service provider to verify the validity of the signature provided by the user and do a revocation check to see if the credential has been revoked or not.

- identityRevocation: This function allows IDPC to invalidate the identifier of any particular user or trusted authority.

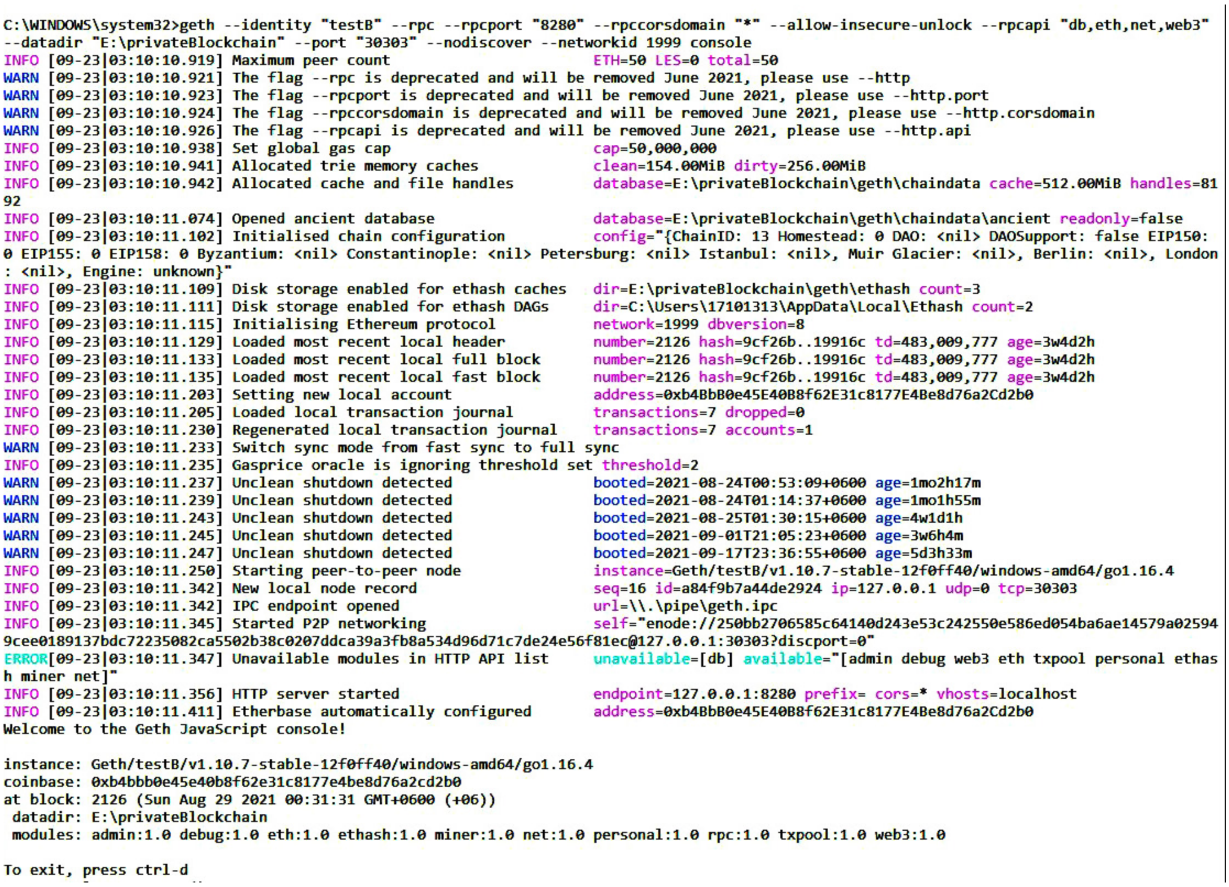
- credentialRevocation: Using the user's identifier and the credential hash value, IDPC can invalidate the credentials of a specific user.

- trustedAuth_credentialRevocation: Using the user's identifier and the credential hash value, a trusted authority can invalidate the credentials or certificate of a specific user. If a User's certificate or credential has expired or been updated, such as a driver's license, DMV can use this function to invalidate the previous license and register a new driving license on the blockchain network.

In order to connect our test blockchain to the smart contract in Remix IDE we need to use Web3 provider and local host address. In the geth console we need to give some command in order to setup the blockchain to allow remote access and dedicated port number for Web3 connection. For our test Blockchain we set

- name or identity as "testB"
- enabled "rpc" which will allow remote access to the blockchain
- port as "8280" which can be accessed by Web3
- networkid "1999"

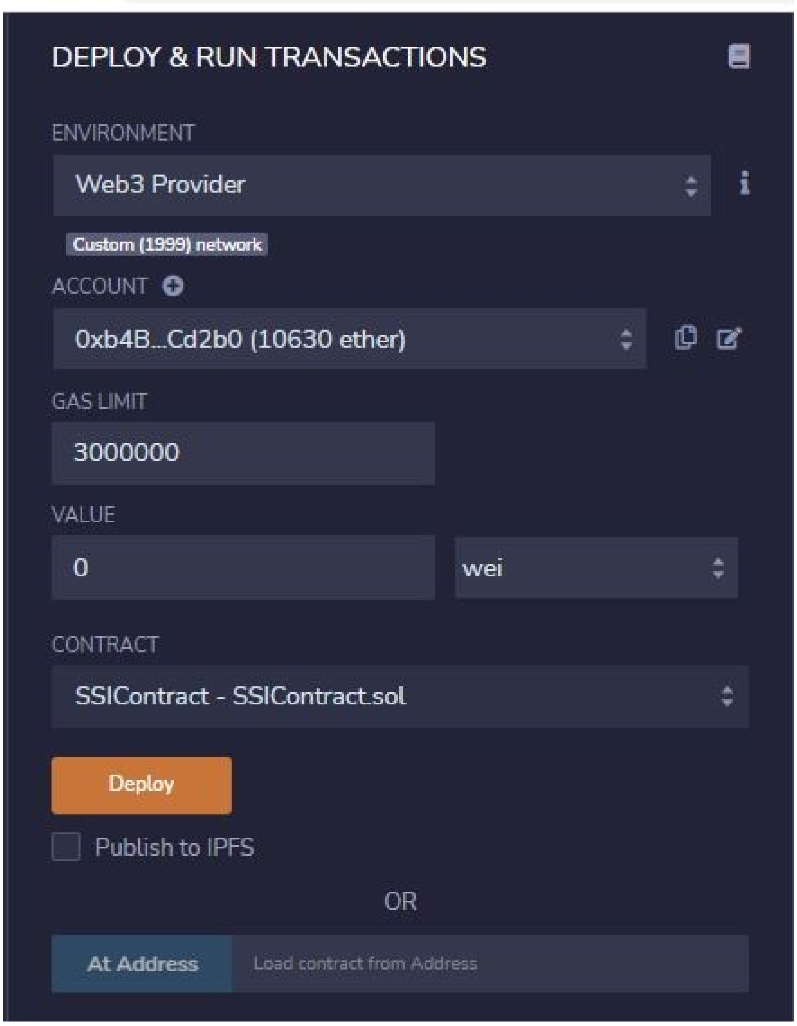
With Web3 address 127.0.0.1:8280 we could connect our demo Smart Contract with our test blockchain for deployment as shown in Figure 5.9



```
C:\WINDOWS\system32>geth --identity "testB" --rpc --rpcport "8280" --rpccorsdomain "*" --allow-insecure-unlock --rpcapi "db,eth,net,web3"
--datadir "E:\privateBlockchain" --port "30303" --nodiscover --networkid 1999 console
INFO [09-23|03:10:10.919] Maximum peer count                       ETH=50 LES=0 total=50
WARN [09-23|03:10:10.921] The flag --rpc is deprecated and will be removed June 2021, please use --http
WARN [09-23|03:10:10.923] The flag --rpcport is deprecated and will be removed June 2021, please use --http.port
WARN [09-23|03:10:10.924] The flag --rpccorsdomain is deprecated and will be removed June 2021, please use --http.corsdomain
WARN [09-23|03:10:10.926] The flag --rpcapi is deprecated and will be removed June 2021, please use --http.api
INFO [09-23|03:10:10.938] Set global gas cap                       cap=50,000,000
INFO [09-23|03:10:10.941] Allocated trie memory caches             clean=154.00MiB dirty=256.00MiB
INFO [09-23|03:10:10.942] Allocated cache and file handles         database=E:\privateBlockchain\geth\chaindata cache=512.00MiB handles=81
92
INFO [09-23|03:10:11.074] Opened ancient database                  database=E:\privateBlockchain\geth\chaindata\ancient readonly=false
INFO [09-23|03:10:11.102] Initialised chain configuration          config="{ChainID: 13 Homestead: 0 DAO: <nil> DAOSupport: false EIP150:
0 EIP155: 0 EIP158: 0 Byzantium: <nil> Constantinople: <nil> Petersburg: <nil> Istanbul: <nil>, Muir Glacier: <nil>, Berlin: <nil>, London
: <nil>, Engine: unknown}"
INFO [09-23|03:10:11.109] Disk storage enabled for ethash caches   dir=E:\privateBlockchain\geth\ethash count=3
INFO [09-23|03:10:11.111] Disk storage enabled for ethash DAGs     dir=C:\Users\17101313\AppData\Local\Ethash count=2
INFO [09-23|03:10:11.115] Initialising Ethereum protocol           network=1999 dbversion=8
INFO [09-23|03:10:11.129] Loaded most recent local header          number=2126 hash=9cf26b..19916c td=483,009,777 age=3w4d2h
INFO [09-23|03:10:11.133] Loaded most recent local full block      number=2126 hash=9cf26b..19916c td=483,009,777 age=3w4d2h
INFO [09-23|03:10:11.135] Loaded most recent local fast block      number=2126 hash=9cf26b..19916c td=483,009,777 age=3w4d2h
INFO [09-23|03:10:11.203] Setting new local account                address=0xb4BbB0e45E40B8f62E31c8177E4Be8d76a2Cd2b0
INFO [09-23|03:10:11.205] Loaded local transaction journal         transactions=7 dropped=0
INFO [09-23|03:10:11.230] Regenerated local transaction journal    transactions=7 accounts=1
WARN [09-23|03:10:11.233] Switch sync mode from fast sync to full sync
INFO [09-23|03:10:11.235] Gasprice oracle is ignoring threshold set threshold=2
WARN [09-23|03:10:11.237] Unclean shutdown detected                booted=2021-08-24T00:53:09+0600 age=1mo2h17m
WARN [09-23|03:10:11.239] Unclean shutdown detected                booted=2021-08-24T01:14:37+0600 age=1mo1h55m
WARN [09-23|03:10:11.243] Unclean shutdown detected                booted=2021-08-25T01:30:15+0600 age=4w1d1h
WARN [09-23|03:10:11.245] Unclean shutdown detected                booted=2021-09-01T21:05:23+0600 age=3w6h4m
WARN [09-23|03:10:11.247] Unclean shutdown detected                booted=2021-09-17T23:36:55+0600 age=5d3h33m
INFO [09-23|03:10:11.250] Starting peer-to-peer node               instance=Geth/testB/v1.10.7-stable-12f0ff40/windows-amd64/go1.16.4
INFO [09-23|03:10:11.342] New local node record                    seq=16 id=a84f9b7a44de2924 ip=127.0.0.1 udp=0 tcp=30303
INFO [09-23|03:10:11.342] IPC endpoint opened                      url=\\.\pipe\geth.ipc
INFO [09-23|03:10:11.345] Started P2P networking                   self="enode://250bb2706585c64140d243e53c242550e586ed054ba6ae14579a02594
9cee0189137bdc72235082ca5502b38c0207ddca39a3fb8a534d96d71c7de24e56f81ec@127.0.0.1:30303?discport=0"
ERROR[09-23|03:10:11.347] Unavailable modules in HTTP API list     unavailable=[db] available="[admin debug web3 eth txpool personal ethas
h miner net]"
INFO [09-23|03:10:11.356] HTTP server started                      endpoint=127.0.0.1:8280 prefix= cors=* vhosts=localhost
INFO [09-23|03:10:11.411] Etherbase automatically configured       address=0xb4BbB0e45E40B8f62E31c8177E4Be8d76a2Cd2b0
Welcome to the Geth JavaScript console!

instance: Geth/testB/v1.10.7-stable-12f0ff40/windows-amd64/go1.16.4
coinbase: 0xb4bbb0e45e40b8f62e31c8177e4be8d76a2cd2b0
at block: 2126 (Sun Aug 29 2021 00:31:31 GMT+0600 (+06))
 datadir: E:\privateBlockchain
 modules: admin:1.0 debug:1.0 eth:1.0 ethash:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txpool:1.0 web3:1.0

To exit, press ctrl-d
```

Figure 5.8: Screenshot of Setup of Blockchain for Web3

Our demo Smart Contract is short and only shows some of the basic functionality it can provide. Just like the Driving license information, many other services can be added to the same Identity. Our way of implementation can also be changed and improved which we will further discuss in future works.



DEPLOY & RUN TRANSACTIONS

ENVIRONMENT

Web3 Provider

Custom (1999) network

ACCOUNT

0xb4B...Cd2b0 (10630 ether)

GAS LIMIT

3000000

VALUE

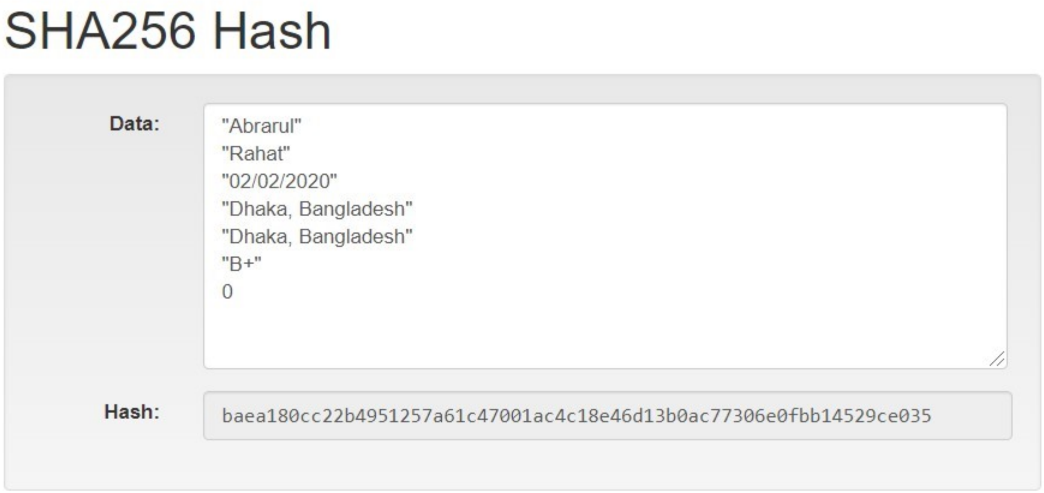
0 wei

CONTRACT

SSIContract - SSIContract.sol

Figure 5.9: Screenshot of Deployed Smart Contract in Remix IDE

Backend Workflow and Diagrams: In order to minimize the data stored each transaction in the block we hashed the data. The data generates a unique hash for a particular set of data. That hash is stored in the Block which takes less space for more efficient storage. We used SHA256 for our implementation.



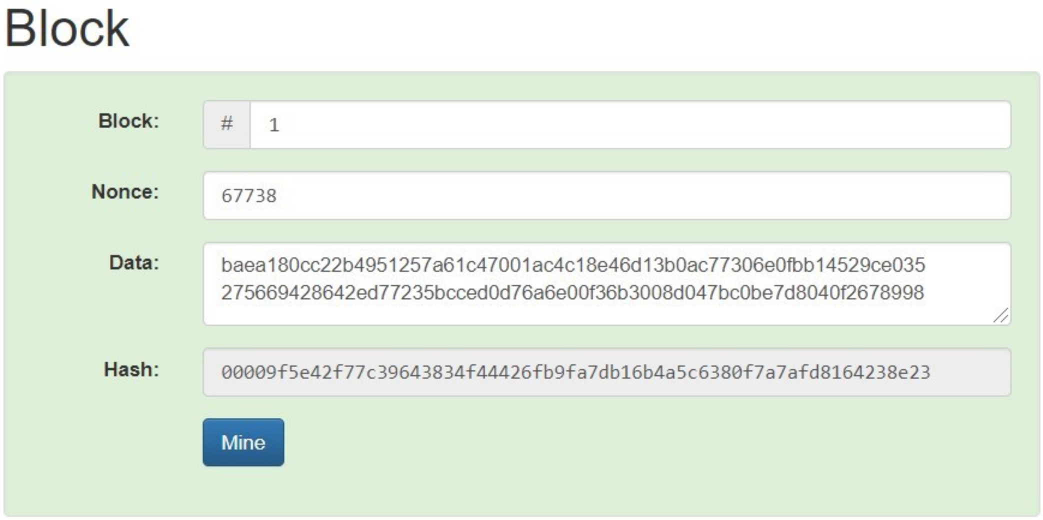
SHA256 Hash

Data:

```
"Abrarul"
"Rahat"
"02/02/2020"
"Dhaka, Bangladesh"
"Dhaka, Bangladesh"
"B+"
0
```

Hash: baea180cc22b4951257a61c47001ac4c18e46d13b0ac77306e0fbb14529ce035

Figure 5.10: Hash generated from data using SHA256



Block

Block: # 1

Nonce: 67738

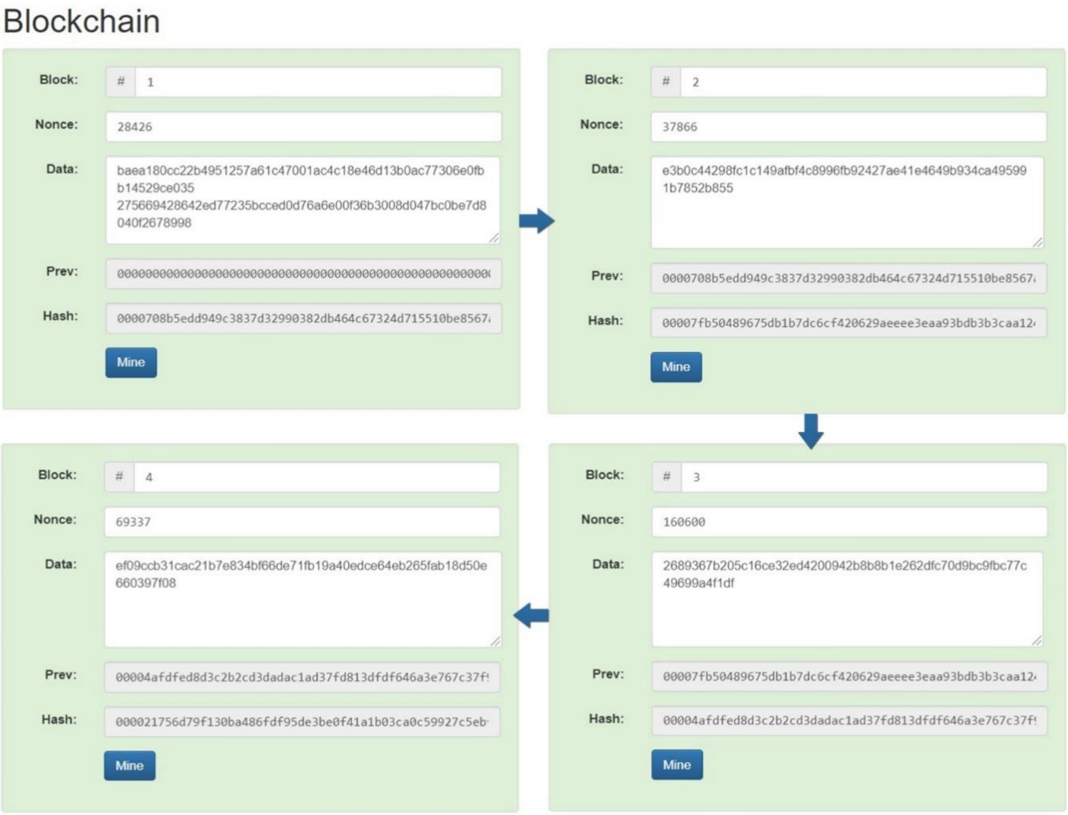
Data:

```
baea180cc22b4951257a61c47001ac4c18e46d13b0ac77306e0fbb14529ce035
275669428642ed77235bcced0d76a6e00f36b3008d047bc0be7d8040f2678998
```

Hash: 00009f5e42f77c39643834f44426fb9fa7db16b4a5c6380f7a7afd8164238e23

Figure 5.11: Block1 with data

Each Block can contain hash information of multiple data as we see in the figure 5.6. Once the hash is put in the block, the block gets mined by the miner to generate a Nonce and Hash for the block. This hash of block is then used by the next block to create the blockchain. As new block gets added to the end, the chain keeps getting longer. Changing any value in the block will reset the hash of the block and the block will need to be mined again to generate new hash. Altering any block at the middle of the blockchain will as a result invalidate all the blocks after it as the next block contains the old hash. Adding new hash to the block will reset its hash and will need to be mined again. As a result, all the blocks after the altered block needs to be altered and mined again making it a very difficult task.



Blockchain

Block: # 1

Nonce: 28426

Data: baea180cc22b4951257a61c47001ac4c18e46d13b0ac77306e0fb b14529ce035 275669428642ed77235bcced0d76a6e00f36b3008d047bc0be7d8 040f2678998

Prev: 00000000000000000000000000000000000000000000000000000

Hash: 0000708b5edd949c3837d32990382db464c67324d715510be8567

Block: # 2

Nonce: 37866

Data: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca49599 1b7852b855

Prev: 0000708b5edd949c3837d32990382db464c67324d715510be8567

Hash: 00007fb50489675db1b7dc6cf420629aeeee3eaa93bdb3b3caa12

Block: # 4

Nonce: 69337

Data: ef09ccb31cac21b7e834bf66de71fb19a40edce64eb265fab18d50e 660397f08

Prev: 00004afdfed8d3c2b2cd3dadac1ad37fd813dfdf646a3e767c37f

Hash: 000021756d79f130ba486fdf95de3be0f41a1b03ca0c59927c5eb

Block: # 3

Nonce: 160600

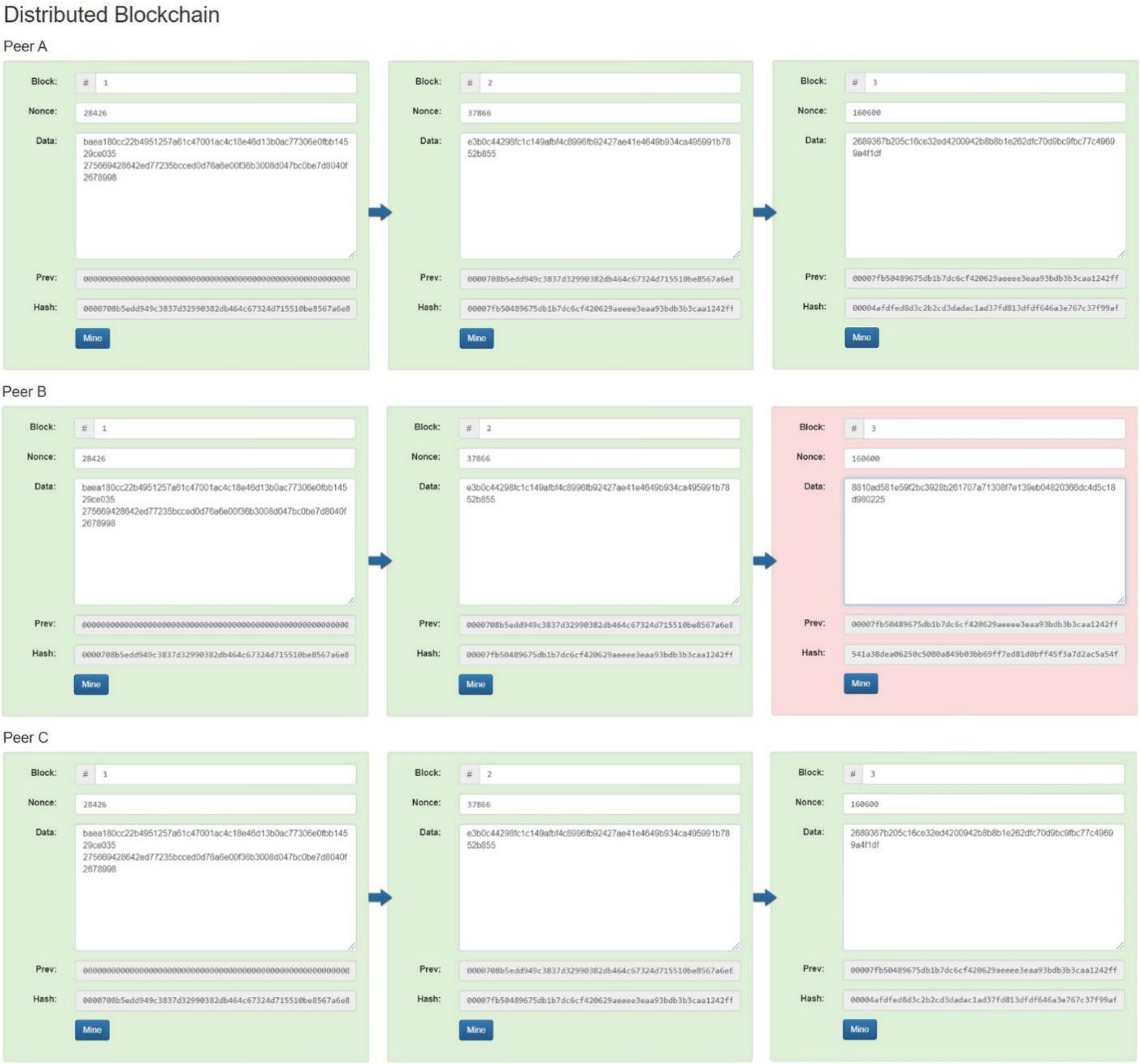
Data: 2689367b205c16ce32ed4200942b8b8b1e262dfc70d9bc9fbc77c 49699a4f1df

Prev: 00007fb50489675db1b7dc6cf420629aeeee3eaa93bdb3b3caa12

Hash: 00004afdfed8d3c2b2cd3dadac1ad37fd813dfdf646a3e767c37f

Figure 5.12: Blockchain with four blocks

As the blockchain will be a part of the distributed network where each peer will have a copy of the valid blockchain, any peer with altered block will be easily identified. Before any data is validated, the peers need to come to a consensus about the correct blockchain. As in the figure 5.8 we can see 3 peers, each with their own copy of the blockchain. Peer B has a faulty block in red which does not match with the blockchain of peer A or peer C. As both peer A and peer C has identical blockchain, we can come to a consensus that the blockchain they have is the correct one as majority of the peers' chain matched. In practice there will be more than thousands of peers and altering the blockchain of more than half of those peers would be close to impossible. Hence the consensus will always choose the right blockchain.



Distributed Blockchain

Peer A

Block: # 1
Nonce: 28426
Data: baea180cc22b4951257a61c47001ac4c18e46d13b0ac77306e0fbb145
29ce035
275669428642ed77235bcced0d76a6e00f36b3008d047bc0be7d8040f
2678998
Prev: 0000000000000000000000000000000000000000000000000000000000
Hash: 0000708b5edd949c3837d32990382db464c67324d715510be8567a6e8

Block: # 2
Nonce: 37866
Data: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b78
52b855
Prev: 0000708b5edd949c3837d32990382db464c67324d715510be8567a6e8
Hash: 00007fb50489675db1b7dc6cf420629aeeee3eaa93bdb3b3caa1242ff

Block: # 3
Nonce: 160600
Data: 2689367b205c16ce32ed4200942b8b8b1e262dfc70d9bc9fbc77c4969
9a4f1df
Prev: 00007fb50489675db1b7dc6cf420629aeeee3eaa93bdb3b3caa1242ff
Hash: 00004afdfed8d3c2b2cd3dadac1ad37fd813dfdf646a3e767c37f99af

Peer B

Block: # 1
Nonce: 28426
Data: baea180cc22b4951257a61c47001ac4c18e46d13b0ac77306e0fbb145
29ce035
275669428642ed77235bcced0d76a6e00f36b3008d047bc0be7d8040f
2678998
Prev: 0000000000000000000000000000000000000000000000000000000000
Hash: 0000708b5edd949c3837d32990382db464c67324d715510be8567a6e8

Block: # 2
Nonce: 37866
Data: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b78
52b855
Prev: 0000708b5edd949c3837d32990382db464c67324d715510be8567a6e8
Hash: 00007fb50489675db1b7dc6cf420629aeeee3eaa93bdb3b3caa1242ff

Block: # 3
Nonce: 160600
Data: 8810ad581e59f2bc3928b261707a71308f7e139eb04820366dc4d5c18
d980225
Prev: 00007fb50489675db1b7dc6cf420629aeeee3eaa93bdb3b3caa1242ff
Hash: 541a38dea06250c5080a849b03bb69ff7ed81d0bff45f3a7d2ac5a54f

Peer C

Block: # 1
Nonce: 28426
Data: baea180cc22b4951257a61c47001ac4c18e46d13b0ac77306e0fbb145
29ce035
275669428642ed77235bcced0d76a6e00f36b3008d047bc0be7d8040f
2678998
Prev: 0000000000000000000000000000000000000000000000000000000000
Hash: 0000708b5edd949c3837d32990382db464c67324d715510be8567a6e8

Block: # 2
Nonce: 37866
Data: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b78
52b855
Prev: 0000708b5edd949c3837d32990382db464c67324d715510be8567a6e8
Hash: 00007fb50489675db1b7dc6cf420629aeeee3eaa93bdb3b3caa1242ff

Block: # 3
Nonce: 160600
Data: 2689367b205c16ce32ed4200942b8b8b1e262dfc70d9bc9fbc77c4969
9a4f1df
Prev: 00007fb50489675db1b7dc6cf420629aeeee3eaa93bdb3b3caa1242ff
Hash: 00004afdfed8d3c2b2cd3dadac1ad37fd813dfdf646a3e767c37f99af

Figure 5.13: Distributed network of blockchain

Chapter 6

Result Analysis

The prototype of the Blockchain system accommodated four independent chains. Each has been initiated on a singular device using multiple socket addresses. Four PORT from the registered port range of 1024-49151 was used for choosing the desired ports. The four ports are 8280, 8281, 8282 and 8283. The IP address for local server is 127.0.0.1.

Chain Name	IP address	Port address
Chain1	127.0.0.1	8280
Chain2	127.0.0.1	8281
Chain3	127.0.0.1	8282
Chain4	127.0.0.1	8283

Table 6.1: Blockchain network chain address table.

Ethereum have become the primary blockchain to provide token advent service. It affords a tremendous stage of accept as true with because of its adulthood and sturdy role at the crypto-foreign money market. All tokens constructed on Ethereum use the ERC-20 standard. The documentation is properly written and organized, making the improvement procedure easier. A token on Ethereum can simplest be written in Solidity (its personal programming language), however with the HTTP API you may create dApps in any language.

Programming Language	Solidity(Ethereum's own language)
Token Standard	ERC-20
Virtual Machine	Native Virtual Machine
Wallet	A lot of options
Hardware wallet	Yes
Consensus	Proof of work
Primary sphere of use	Smart contracts
Number of transactions per seconds	15 transactions/second

Table 6.2: Ethereum Blockchain

The Blockchain system has multiple states. Each state can have different properties and different number of chains. In the system each chain was capable of identifying other operating chains in the network and communicate with the chains.

Thus, was able to collect information about the operational chains present in the Blockchain and compare the information of the blocks for verification.

The Blockchain system has multiple states. Each state can have different properties and different number of chains. In the system each chain was capable of identifying other operating chains in the network and communicate with the chains. Thus, was able to collect information about the operational chains present in the Blockchain and compare the information of the blocks for verification.

Index	Proof	Timestamp	Number of transactions
1	1	12:37:39.306775	0
2	342	12:37:44.511239	3
3	754	12:37:82.705479	7
4	2038	12:38:11.244657	9
5	5277	12:38:35.603245	12
6	4189	12:38:77.982216	11
7	10180	12:39:13.547898	14
8	34912	12:39:58.411266	13
9	108363	12:39:92.846244	15
10	147249	12:40:13.651794	14

Table 6.3: Transaction in a single chain of Blockchain

A model of different states of the Blockchain system needs better understanding for a clear visual of what is expected from each chain in the network and how the network should operate. The information of the model can create a visual representation of a optimal operation Information of nodes at different states of the system.

State	Time	Known chain in system
Initialization of system with chain 1	T0	Chain1 (127.0.0.1: 8280)
Initialization of chain 2	T1	Chain2 (127.0.0.1: 8281)
Initialization of chain 3	T2	Chain3 (127.0.0.1: 8282)
Initialization of chain 4	T3	Chain4 (127.0.0.1: 8283)

Table 6.4: State change table

Comparison Action	**SMID**	**Traditional Identity Card (NID)**
Data tampering or manipulation	False	True
Basic information	True	True
Correction on information Digitally	True	False
Adding new Information	True	False
Adding new government services	True	False
Binding bank account	True	False
Binding payment gateway	True	False
Cancellation of card or services digitally	True	False
Contains biometric information	True	True
Account verification	True	True
Can be lost or damaged	False	True
Temporary suspend account	True	True

Table 6.5: Comparison Table between SMID and NID

National identity cards which are being used in our country can be easily tampered or manipulated. Recently there have been many stories about the manipulation or tampering of the national identity card. Dr.Shahed who was the founder of regent hospital had been arrested because of fraud. He used to have five identity cards with different identities. He used those identity cards to fraud people. He also used those identity cards to escape from this country. Dr.Sabrina was another fraud who used to have three different identity cards to deceive people. She usurped more than 5core taka by using those fake identity cards. By these two stories it is clear that the national identity card which is being used in our country can easily be fabricated. The card which we proposed in our model is more secured and it cannot be easily manipulated or tampered. Whenever anyone tries to forge identity cards the chain will break and will be separated. So no one can forge it or manipulate any data. Basic information like name, address, date of birth and blood group will show in both traditional identity cards and our proposed digital identity card. If any information is wrong in a traditional identity card it is impossible to correct digitally. One has to go to the election commission office and has to face many hurdles to correct the information. In our proposed digital identity card it is very easy to correct any information digitally. This will reduce the vexation of the people. In traditional identity cards it is impossible to add any new information. Traditional identity cards only show the basic information of the citizen. If anyone wants to add any information they cannot do it because it is restricted to add any new information. In our proposed identity card any citizen can add new information without any restriction. They just have to request adding new information. One can also add new government services like driving license, vehicle registration etc. They can use this card as a driving license and vehicle registration card which is not possible in traditional national identity cards. Citizens cannot bind any bank account with the traditional identity card. They cannot use this card as a payment gateway. They cannot perform any type of transaction with the help of the identity card. But citizens can bind with any type of bank account and they can perform any type of transaction by using our proposed digital identity card. Both account verification and biometric information are available in both traditional national identity cards and our proposed digital identity card. Traditional national cards can be lost or damaged. After being lost and damaged it is very difficult to find it. As our proposed identity card is fully digital so it is very easy to find it after it is damaged or lost. Our proposed identity card is much more secured, dynamic and useful to use rather than the traditional identity card.

6.1 Cost Analysis

In our system we are using permissioned blockchain. Permissioned blockchains have numerous economic benefits, with a lot of them coming from the technical benefits they provide. Generally, they lessen expenses due to the fact they take away intermediaries, which turns into pointless in the blockchain protocol. It is confirmed that permissioned blockchain networks may want to lessen financial institution infrastructure charges among US$15 billion and $20 billion according to 12 months in 2022. In a blockchain community, there may be no want for complex audits for the reason that blockchain continues its personal permanent 'audits' and without delay publishes transactions via the blockchain. This glaringly reduces charges due to the fact financial institution outside audits, which might be of route mandatory, may be extraordinarily high priced Some slower, high priced charge networks with a quasi-monopolistic function also can be bypassed with the permissioned blockchains. This additionally reduces charges for banks. Maintenance charges for the networks also are decreased due to the fact, for lots aspects, the blockchain community can 'self-maintain' itself. Permissioned blockchains have remarkable technical and economic blessings with inside the context of the banking industry. They can lessen normal expenses in a totally green way.

Cryptocurrencies are sky rocketing both in price and its usability. In our implementation we used test Ethereum and ether as cryptocurrencies. Acquiring cryptocurrencies might sound very expensive at the current economy but in our proposed model we used permissioned blockchain which allows creation of a new cryptocurrency for its use. So, government can mint their own cryptocurrency for this permissioned blockchain and would not need to buy existing cryptocurrencies, which will drastically reduce the cost. Furthermore, the new currency and blockchain can be created in their preferred way to reduce the cost and the transaction time.

Another concern many might have is that blockchain storage is very expensive. In our architecture we stored the data in off chain connected to the content addressable storage and only the data hash is stored on chain. This reduced the data stored in the blockchain hence reducing the excessive storage cost.

Chapter 7

Conclusion and Future Work

We began our investigation to strengthen the security and privacy of Smart City using blockchain technology. Then, utilizing blockchain technology, we began our research on digital identification, which is an important component of Smart Cities. Blockchain is a massive database of public documents that cannot be altered, deleted, or destroyed. In our study, we suggested a workflow and technique for completing the task. In this research paper, we proposed a model and a possible implementation of the technology. We anticipate that, rather than the standard NID card, this will be the most secure method of digital identity following complete adoption as well as it can use as a multipurpose card. So citizens can avail any type of services by using this card. They do not have to carry a lot of separate cards instead by using this smart multipurpose card they would be much smarter than before. Life will be so much easy and hassle free because of this secured multipurpose identity card.

In our implementation and proposed model, we have used the Ethereum blockchain and poof of work mechanism as mean to propose our idea. But our proposed model can be easily implemented using other cryptocurrencies and blockchain methods. For example, better consensuses mechanism like proof of stake or proof of capacity can also be used. These consensuses mechanisms are fairly new to the industry as they are still being research and improved. Even Ethereum is shifting from their present proof of work model to proof of stake. So far, they are showing much more promising efficiency in energy consumption and low barriers to entry for miners. In the near future our model can be implemented much more efficiently by using newer consensuses mechanism.

Our architecture we suggested to sign-in every time the user access the wallet or smart contract for added security. Moreover, a biometric system is highly recommended for this sign in to make the security even more robust. Currently we are using fingerprint and face detection as most secured mean of biometric system. Further works can be done on this biometric system which will allow more convenient and secured sign in every time.

Smart contract is very important and crucial part of any decentralized application. Once deployed to the main blockchain, it cannot be altered. As a result, a robust smart contract must be needed for our proposed model and architecture. We tried our best to show most of the functionality of the model through our demo Smart contract. It is strongly suggested to invest more time and effort to create a robust Smart contract. There are already smart contract experts doing this job who must be consulted bore deploying the smart contract.

Bibliography

[1] H. v. Halteren, "Linguistic profiling for authorship recognition and verification," 2004.

[2] E. K. Lua, J. Crowcroft, M. Pias, R. Sharma, and S. Lim, "A survey and comparison of peer-to-peer overlay network schemes," *IEEE Communications Surveys & Tutorials*, vol. 7, no. 2, pp. 72–93, 2005.

[3] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," *IEEE Internet computing*, vol. 10, no. 1, pp. 82–89, 2006.

[4] P. Fraigniaud, C. Gavoille, and C. Paul, "Eclecticism shrinks even small worlds," *Distributed Computing*, vol. 18, no. 4, pp. 279–291, 2006.

[5] J. Han, M. Kamber, and D. Mining, "Concepts and techniques," *Morgan Kaufmann*, vol. 340, pp. 94 104–3205, 2006.

[6] S. J. Lincke and A. Holland, "Network security: Focus on security, skills, and stability," in *2007 37th Annual Frontiers In Education Conference-Global Engineering: Knowledge Without Borders, Opportunities Without Passports*, IEEE, 2007, F1D–10.

[7] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21 260, 2008.

[8] J. Cherus, J. Githeko, J. Siror, and K. Njagi, "Identity fraud: A literature review and future research directions," 2014.

[9] G. Foroglou and A.-L. Tsilidou, "Further applications of the blockchain," in *12th student conference on managerial science and technology*, 2015, pp. 1–8.

[10] I. Bentov, A. Gabizon, and A. Mizrahi, "Cryptocurrencies without proof of work," in *International conference on financial cryptography and data security*, Springer, 2016, pp. 142–157.

[11] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, 2016, pp. 3–16.

[12] S. Huckle, R. Bhattacharya, M. White, and N. Beloff, "Internet of things, blockchain and shared economy applications," *Procedia computer science*, vol. 98, pp. 461–466, 2016.

[13] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," in *International Conference on Financial Cryptography and Data Security*, Springer, 2016, pp. 515–532.

[14] S. Singh and N. Singh, “Blockchain: Future of financial and cyber security,” in *2016 2nd international conference on contemporary computing and informatics (IC3I)*, IEEE, 2016, pp. 463–467.

[15] A. B. Ayed, “A conceptual secure blockchain-based electronic voting system,” *International Journal of Network Security & Its Applications*, vol. 9, no. 3, pp. 01–09, 2017.

[16] A. Baliga, “Understanding blockchain consensus models,” *Persistent*, vol. 4, pp. 1–14, 2017.

[17] J. B. Bernabé, J. L. H. Ramos, and A. F. Gómez-Skarmeta, “Holistic privacy-preserving identity management system for the internet of things.,” *Mob. Inf. Syst.*, vol. 2017, pp. 6 384 186–1, 2017.

[18] I. Klaus, “Don tapscott and alex tapscott: Blockchain revolution,” *New Global Studies*, vol. 11, no. 1, pp. 47–53, 2017.

[19] B. Koteska, E. Karafiloski, and A. Mishev, “Blockchain implementation quality challenges: A literature,” in *SQAMIA 2017: 6th Workshop of Software Quality, Analysis, Monitoring, Improvement, and Applications*, 2017, pp. 11–13.

[20] J. Lindman, V. K. Tuunainen, and M. Rossi, “Opportunities and risks of blockchain technologies–a research agenda,” 2017.

[21] Y. Liu, Z. Zhao, G. Guo, X. Wang, Z. Tan, and S. Wang, “An identity management system based on blockchain,” in *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, IEEE, 2017, pp. 44–4409.

[22] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, “A review on consensus algorithm of blockchain,” in *2017 IEEE international conference on systems, man, and cybernetics (SMC)*, IEEE, 2017, pp. 2567–2572.

[23] G. Wolfond, “A blockchain ecosystem for digital identity: Improving service delivery in canada’s public and private sectors,” *Technology Innovation Management Review*, vol. 7, no. 10, 2017.

[24] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, *et al.*, “Hyperledger fabric: A distributed operating system for permissioned blockchains,” in *Proceedings of the thirteenth EuroSys conference*, 2018, pp. 1–15.

[25] T. Hepp, M. Sharinghousen, P. Ehret, A. Schoenhals, and B. Gipp, “On-chain vs. off-chain storage for supply-and blockchain integration,” *it-Information Technology*, vol. 60, no. 5-6, pp. 283–291, 2018.

[26] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, “Distributed blockchain-based data protection framework for modern power systems against cyber attacks,” *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3162–3173, 2018.

[27] K. Nyante, “Secure identity management on the blockchain,” M.S. thesis, University of Twente, 2018.

[28] R. Qin, Y. Yuan, and F.-Y. Wang, “Research on the selection strategies of blockchain mining pools,” *IEEE Transactions on Computational Social Systems*, vol. 5, no. 3, pp. 748–757, 2018.

[29] D. Anton and M. McFall, *Uniqueness and auditing of a data resource through an immutable record of transactions in a hash history*, US Patent 10,356,094, Jul. 2019.

[30] M. Aydar, S. Ayvaz, and S. C. Cetin, “Towards a blockchain based digital identity verification, record attestation and record sharing system,” *arXiv preprint arXiv:1906.09791*, 2019.

[31] M. Kuperberg, “Blockchain-based identity management: A survey from the enterprise and ecosystem perspective,” *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1008–1027, 2019.

[32] Y. Takefuji and H. Szu, “Blockchain is vulnerable against classic database approach,” *MOJ App Bio Biomech*, vol. 2, no. 5, pp. 102–103, 2019.

[33] K. O. Asamoah, H. Xia, S. Amofa, O. I. Amankona, K. Luo, Q. Xia, J. Gao, X. Du, and M. Guizani, “Zero-chain: A blockchain-based identity for digital city operating system,” *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10 336–10 346, 2020.

[34] J. Fruhlinger, “Equifax data breach faq: What happened, who was affected, what was the impact?” *CSO, February*, vol. 12, 2020.

[35] Y. C. E. Adja, B. Hammi, A. Serhrouchni, and S. Zeadally, “A blockchain-based certificate revocation management and status verification system,” *Computers & Security*, vol. 104, p. 102 209, 2021.

[36] M. Bouras, Q. Lu, S. Dhelim, and H. Ning, *A lightweight blockchain-based iot identity management approach. future internet 2021, 13, 24*, 2021.

[37] S.-T. Chao, Y. Zhao, and J. Zhao, “Reviewing blockchain scalability challenge with a discussion of off-chain approaches,”