Driver's Reputation Management System Using Blockchain for Smart City

By
Md.Ammar Hossain Siam
18101418
Raufar Mostafa
20101312
Maliha Jahan Maisha
20101527
Shifath Jahan
20101521
Nafisa Muhammad
20101386

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
School of Data and Sciences
Brac University
May 2023

© 2023. BRAC University
All rights reserved.

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:

Siam Hossain

Md.Ammar Hossain Siam
18101418

Raufar Mostafa
20101312

Maisha

Maliha Jahan Maisha
20101527

Shifath Jahan Prity
20101521

Nafisa.

Nafisa Muhammad
20101386

Approval

The thesis titled "Driver's Reputation Management System Using Blockchain for Smart City" submitted by

1. Md.Ammar Hossain Siam (18101418)

2. Raufar Mostafa (20101312)

3. Maliha Jahan Maisha (20101527)

4. Shifath Jahan Prity (20101521)

5. Nafisa Muhammad (20101386)

of Summer, 2023 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on May 25,2023.

Examining Committee:

Iqbal

Supervisor:
(Member)

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

Program Coordinator:
(Member)

Dr. Golam Robiul Alam
Professor
Department of Computer Science and Engineering
Brac University

Departmental Head:
(Chair)

Dr. Sadia Hamid Kazi
Associate Professor
Department of Computer Science and Engineering
Brac University

Abstract

The driving system, in all its disorganized scale has long thrown a shadow of unpredictability and fluctuation making it concerning for public safety. A blockchain-based driver reputation management system for smart city is analyzed and explored in this research from the global perspective. Managing driver behavior and guaranteeing road safety have emerged as pressing issues in the wake of the meteoric rise of ”smart cities” throughout the world. The proposed system uses blockchain technology and IPFS (InterPlanetary File System) to assist with data management, reliability, and privacy concerns from perspective of emerging smart cities of Bangladesh. With the help of the reputation algorithm, the system ensures a reliable assessment of a driver's actions, enhancing the efficiency of subsequent decisions on sanctions and rewards, as well as driver management, in more general terms. This accuracy promotes accountability, encourages drivers to improve their behavior, and contributes to the overall goal of enhancing road safety in smart cities.

Index terms: *road accidents; driver reputation; blockchain; Hyperledger Fabric; Delegated Proof of Stake; IPFS; Smart contracts*

Acknowledgement

Firstly, all praise to Almighty Allah for whom our thesis have been completed without any major complications or interruption.

Secondly, to our supervisor Mr. Mohammad Iqbal Hossain sir for his kind support and advice in our work. He helped us through and through with our thesis at any given time.

And finally to our parents, as without their love and endless support this wouldn't have been possible.

Table of Contents

List of Figures

List of Acronyms

BRTA	Bangladesh Road Transport Authority
IPFS	Interplanetary File System
P2P	Peer to Peer
PoW	Proof of Work
PoS	Proof of Stake
DPoS	Delegated Proof of Stake
NID	National Identification
IoT	Internet of Things
ICT	Information and Communications Technology
CID	Content Identifier
IDP	Inverse Distribution Pooling
DAG	Directed Acyclic Graph
API	Application Programming Interface
PoR	Proof of Reputation
DApp	Decentralized Application
FIFO	First-in, first-out

Chapter 1

1 Introduction

Bangladesh's emergence was an exceptional wonder from multiple dimensions, but it has been significantly expanded in the economic and administrative sectors owing to modernized infrastructure and constructed roadways, the most tangible fate of the subcontinent's colonial past. However, in Bangladesh, road accident fatalities and injuries have been a hidden crisis. Accidents on the road are not only individual misfortunes; they also hamper growth in the economy and long-term sustainability. In addition to that, according to the latest statistics from the Bangladesh Road Transport Authority (BRTA), unlicensed drivers operate at least 10 lakh vehicles questioning transparency and loopholes for public safety in a democratic nation such as Bangladesh [1]. It clearly indicates that more than other reasons like proper roads or road safety awareness; the two most intertwined or primary causes of road accidents that impose a heavy impact on roads every day are a lack of certified drivers and dangerous driving by inexperienced drivers. Over-speeding and aggressive overtaking are responsible for around more than two-third of fatal road accidents being responsible for poor driving abilities and a concern for traffic laws.

1.1 Motivation

With the expansion of development on the international scene and the smart city digitization vision of Bangladesh, managing driver profile, including license validation and prior records, will undoubtedly fall under the spotlight. Driver profiling is essential in smart cities for tracking driving behaviors, addressing traffic violations, and dealing with potentially fatal circumstances.
According to a research undertaken in South Korea with the Korean Road Traffic Authority statistics and data, there is a decrease in road accidents after implementing licenses suspending practices by the authority due to past major traffic violations. Surprisingly, such drivers may also be reduced likely to get in road accidents in near future due to the fear of having their license suspension resulting in the accumulation of extra penalty points in their records.[2] In order to guarantee the transparency and valid records of a driver profile, it is important to implement an unbreakable system to maintain records at every stage of the process beginning with completing the qualifications for approving a license and continuing with behaviors

after getting a license.

1.2 Problem Statement

As we step forward in the time stream, along with Bangladesh's exponential expansion in today's globe, road safety has become a fundamental threat for public security and the economy worth 40 thousand crores taka in the prior three years including a decrease of 2-3 percent of its GDP annually by BRTA report[3]. Despite all the actions taken by the Bangladesh government, the alluring problem of road accidents and traffic rule violation is a constant on the roads of the country.

Published in the Bangladesh Road Safety Foundation's (RSF) annual report, at least 6,284 persons died and 7,468 were injured in road accidents between January and December 2021, up from 5,431 deaths and 7,379 injuries in road 3 accidents in 2020. Furthermore, the deaths and injuries resulted in a human resource loss to the tune of Tk.9,631 crore, according to the report [4].According to BRTA sources, in February 2022, The number of registered vehicles in Bangladesh was 5.12 million and there were around 4.74 million driving licenses, published in a report by Dhaka Tribune. Which also states that, the overall number of licenses is inaccurate as some drivers hold both licenses (heavy and light).With around three million license holders in the nation, an estimated two million vehicles are operated by unlicensed drivers [5].This gap clearly reflects and calls into question the safety of the general population on the roadways, both drivers and passengers. The great majority of these incidents are caused by driver malpractice, human negligence and behavior[6], as well as a lack of necessary authorization (i.e. licenses) and understanding about roads or vehicles. The mistakes are encouraged further by authorities or car owners due to a lack of appropriate data and a failure to recognize the skills and patterns of a driver's style used while driving.

In Bangladesh 81.40% drivers do not have any formal academic education or driving. Only 2% have formal driving training and proper knowledge about driving. Rest of the 16.70% drivers have some formal training along with some informal learning. Which means this 16.70% does not complete their proper training. [7] Coming to the reality of crossing the theoretical issue gaps, the present issues with the driver reputation management system are that drivers are labeled as 'safe/aggressive,' which is not the correct strategy to characterize a driver's conduct because a driver's behavior varies and depends on a variety of conditions [8]. For Example; According to Sacks and Nelson (1994), smoking is linked to a higher chance of being involved in a traffic accident. The connection between smoking and various forms of injuries and discovered that smokers were 50% more likely than nonsmokers to be involved in traffic accidents (Waller, 1986) [9].The current system fails to capture process accuracy and consistency, making it vulnerable to misuse by corrupted administrators who can issue licenses to ineligible drivers with no penalties or verification. Moreover, violators of regulatory standards are not held liable for their activities, and any offense is typically not traceable by the system instead, the owner is assigned for the fines which promotes both corruptions for the dishonest traffic police and authorities, as well as no impact over the driver or the violator. As a driver moves on from one duty to another, their behavior and past crime histories do not change therefore in the new field they again get into reckless driving, practicing speeding and breaking laws. There is no way of justifying their behavior and old practice and it can be risky for the new vehicle owner and their valuables. If a driver has a fake license he can immediately get onto another job by simply changing their identity. For preventing any intervention of any third party in the system of something as private and important as license issuing, there is an extreme necessity of a closed system which has impenetrable security.

This research focuses and explores how, by utilizing block chain in collaboration with a decentralized based hyper ledger fabric secured network, we can assure no data leakage and transparency of authentic driver record in order to create a driver reputation management system for smart cities.

1.3 Contributions and objectives of the research

To increase data clarity and eliminate authoritative or system influence by tracking a secure and methodical driver profile system utilizing BlockChain in a decentralized management hub would prevent irresponsible road accidents and contribute towards the development of smart city infrastructure.As our proposed driver reputation management system, which is essentially a driver profiling system, will store the driver's personal information as well as driving data collected through various means and monitoring, on a blockchain network (as manipulating data on a block chain is rather impossible once the data is stored), as well as performing a computer analysis based on the stored data as a measurement of how safe the roads are on the condition that the data is stored. Our suggested system would also store the car that the driver will be driving in order to monitor the driver's behavior and to make it easier to use.

- To introduce a decentralized and unbreakable system that includes drivers' unique license numbers, reference checking, traffic violation clearances and point reputations.
- To provide data security, confidentiality, validity, and transparency using distributed

ledger.

- To propose a reliable and unbiased reputation management system.
- To discover and explore Bangladesh's potential technological domains and growth in terms of Block-chain technology adaption and deployment, as well as accelerate the road-map for smart cities and digitization.

Chapter 2

2 Background Analysis

2.1 Blockchain Technology

Blockchain as a means of managing identities is a phenomenon that is currently being developed and popularized throughout the world. The introduction of Blockchain has transformed the IT sector and greatly improved security. Blockchain is a classification of distributed ledger that allows for the maintenance of an unalterable, impenetrable record of transaction data without the need for a reliable third party. As its name indicates, it is a chain of blocks containing transaction data, but the data it holds is digital. Every block contains the identity of participants along with their digital signature so transactions involving a singular person remain unique. The nature of blockchain allows it to be immutable and irreversible, thus making it a suitable network to keep track of any sort of transactions.[10]

2.1.1 Structure of Blockchain

The word "Blockchain" refers to a series of blocks and its technology is built to uphold the integrity of a chain by maintaining characteristics like continuity and reliability that are typical of the chains. Reliability is defined as the impossibility of replacing or removing a link from the chain. Continuity is defined as blocks that follow one another in a sequence determined during the establishment of a blockchain.[11] The blocks are secured by linking one block to the other by encrypting it, so data cannot be changed easily. In the structure of a blockchain network, a collection of nodes validate a transaction after which the record of the data is stored in the block. Each of the blockchain's elements are divided into components. A block contains a header and a body. The data is stored in the body of the block. The header of the block consists of the hash of the previous block, which is a function that can solve the encrypted problems required by a blockchain calculation,along with a timestamp, which is the time of the creation of the block, Nonce, which is the number validating when the work is completed and Merkle root,which is the root of all hashes in the blockchain. The calculation of the hash value is performed by transferring the previous block's header to the hash function[12].

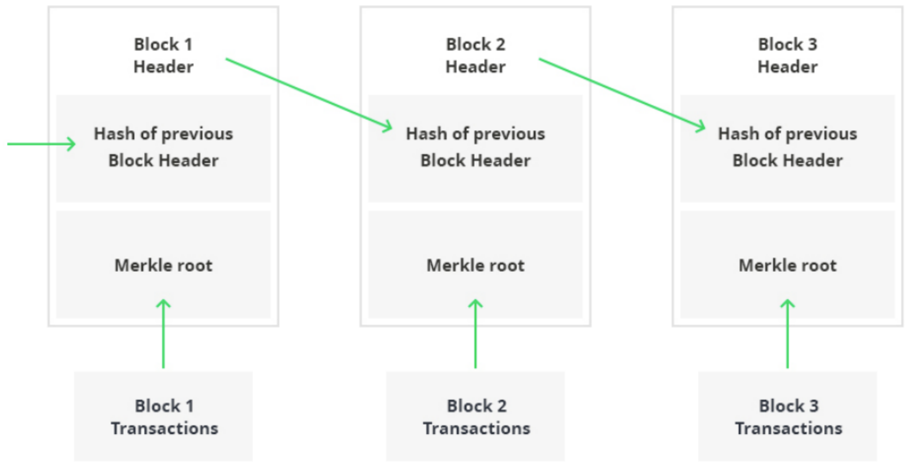


Figure 1: Structure of Blockchain

2.1.2 Types of Blockchain

There exists four types of blockchain:

i. **Public blockchain:** This blockchain allows anyone in the creation and validation of a block in the network. Anybody with an internet connection can register on a public blockchain platform to join the network as an authorized node and contribute to the blockchain. It is an open-source network that allows participation from anyone and treats every node equally. In this network, there isn't any restriction to access or permission and the interactions are open to the public. As a result, Bitcoin and Litecoin blockchains are the most widely used public blockchains. If users comply with security policies and procedures to the letter, public blockchains are generally secure. But only when participants don't actually follow the security guidelines is it dangerous.

ii. **Private blockchain:** This type of structure only allows certain authoritative figures to create and validate the blocks, thus making it more reserved. Participants in a private blockchain network must obtain permission from the main controlling body of the network in order to participate in it. To interact with the blockchain or take part in its operation, only selected actors within the private network are allowed. The private network can translate more quickly because there are a lot fewer people involved.The governing organization controls the level of security, authorizations, permissions, and accessibility. Therefore, private blockchains are used similarly to public blockchains but have a constrained and tiny network.

iii. **Consortium blockchain:** It is a semi-decentralized kind of blockchain in which a network of blockchains is controlled by multiple organizations. This is a blockchain network operated under a group of entities who all have the authority to control and participate in the chain, unlike a single governing one in the private network. But not everyone can take part in this network like the public. Higher levels of security are achieved by consortium blockchains since they are more decentralized than private blockchains. The typical users of consortium blockchains include financial institutions, governmental bodies, etc.

iv. **Hybrid blockchain:** It combines the features of public and private blockchains. The hybrid blockchain amalgamates components of both public and private blockchains for the purpose of resolving disputes in line with the circumstances. Transactions and information in a hybrid blockchain are encrypted for privacy, but may be validated in cases when it's required, such when a smart contract grants access to the data. Internal to the network, private information is stored but remains traceable. The private network of a hybrid blockchain is often utilized to validate a transaction. [13]

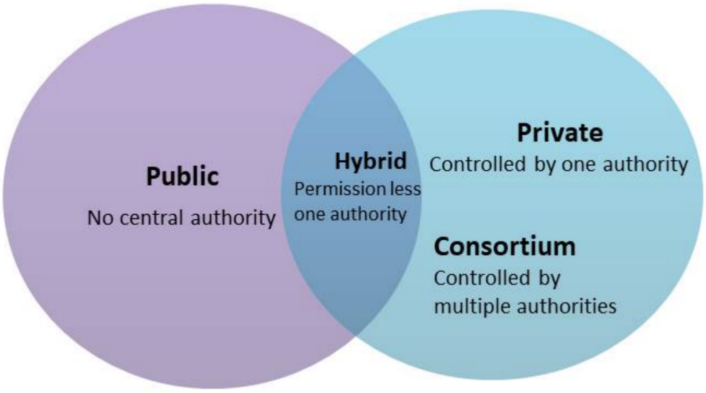


Figure 2: Types of Blockchain Architecture

2.1.3 Characteristics of Blockchain

Various characteristics of blockchain make it favorable for solving numerous issues. The characteristics of blockchain include:

1) **Decentralization:** Through the use of all participating nodes' resources and the elimination of many-to-one traffic flows, the lack of centralized control assures scalability and robustness, which in turn reduces latency and eliminates the single point of failure that the centralized model has.

2) **Immutability:** Once an information is entered and stored in a block,it is impossible to change. This prevents corruption of data and maintains data integrity.

3) **Security:** As there exists no lone instance of failure that will cease activity of the entire network, blockchain is more secure.

4) **Higher Capacity:** Blockchain allows thousands of computers to function together in contrast to a centralized system where only a few computers work together, thus providing increased capacity. [14]

5) **Traceability :**The block header's timestamp records the timing of the creation of a particular block thus origin of the blocks could be easily traced back. [15]

2.2 Introduction to Blockchain Architectures and its components

2.2.1 Hybrid architecture:

According to [16], blockchain structures can be classified into three types: distributed, where multiple servers are used to store the block chain in either public or private mode. The inclusion of data into the block chain is accomplished by these servers coming to an agreement, and the ledgers may even be freely or selectively distributed among one another. Implementing consensus can be done in a variety of ways, including through the usage of smart contracts and work proof. Private or hybrid blockchain architecture employs this kind of network. The hybrid blockchain could be run by a private group, but it would not be able to change transactions. Hybrid blockchains allow organizations to set up a private, permission-based system alongside a public, permission-less system, giving them greater control over who has access to what data in the blockchain and what content is made available to the public.

A hybrid blockchain lets people outside the closed network communicate to each other while keeping their privacy and anonymity. Because hybrid blockchain operates in a closed ecosystem, it cannot be subjected to a 51% attack from outsiders. Participants in the hybrid blockchain network can select the blockchain's users or decide which transactions should be made public and which should remain confidential. This ensures that an organization can successfully and profoundly manage its stakeholders. Transactions on a hybrid blockchain are faster and cheaper than on a public blockchain network, and it can accommodate more users. The low need for verification at nodes in the hybrid blockchain may be why transactions are so cheap. Sharma and Park [17] describe a hybrid blockchain architecture in which there are two separate block chains: one, called the "home network," which is centralized, and the other, called the "public network," which is decentralized. The contrast between centralized residential chains and ledgers and a decentralized public blockchain with a global ledger and public consensus based on work proof with the entire network demonstrates how smart cities could potentially be linked.

The information that is input into a blockchain can be saved in either a public or private ledger. The ledger has the capability of storing a single block as well as the entire block chain. On the other hand, IBM introduced a platform called Hyperledger in 2016 that has its own distinct approach to data recording. Thus, IBM simultaneously unveiled a new framework called Hyperledger and a blockchain development platform [18]. This requirement for a global blockchain platform was satisfied by the introduction of Ethereum, which was first announced in 2014 and then released and introduced in 2015.

2.2.2 Ethereum:

According to [19], Ethereum may be compared to a collection of nodes that each store the network's current state. Each node has access to and stores the global view or state because its data contains the entire transaction history of the others. Again, [19] says that the nodes that make up Ethereum are divided into two categories: contract accounts and nodes that are externally owned. A public-private key pair or smart contracts are used to implement this. Nodes, balance, storage roots, and code are all included in every node or block. Between two blocks, transactions are possible. Ethereum came up with smart contracts first. Every single transaction is completely viewable by anybody who has access to the internet, and this transparency extends to the entirety of the process.

2.2.3 Hyperledger Fabric:

Hyperledger Fabric, one of the most important blockchain research topics, is looked at with the help of performance diagnostics and optimization. [20].Gao et al. [18]: in order to provide a framework, he created a blockchain structure.Using Hyperledger, a distributed ledger was set up to connect all the people in a hybrid block chain and keep track of transactions. Each company uses a shared ledger to make sure that the transactions in the distributed block chain's supply chain are correct. Hyperledger is a platform that is open-source and can be used for the creation of distributed ledger systems. Its modular construction provides it with high levels of privacy, flexibility, reliability, and scalability, and this is made possible by its design.Depending on the situation, several access levels can be assigned to each member. All transactions are managed by Hyperledger Fabric, which utilizes chain code (smart contracts).

A Hyperledger Fabric network is made up of assets, peer nodes, a shared ledger, smart contracts, channels, organizations, Membership-Services Providers(MSPs), and ordering services [21].Research [22] compares and contrasts the capabilities of Ethereum with Hyperledger Fabric. Researchers came to the conclusion that Hyperledger Fabric did better than Ethereum in terms of latency and throughput while using less infrastructure resources. The data shows that Ethereum has a greater success rate for transactions, nevertheless. The article also looks into potential future research areas, which ought to cover more blockchain systems.

2.2.4 IPFS with blockchain:

The Interplanetary File System, or IPFS, said by Zheng et.al[23] is a file management system that lets users store files and keep track of how they change over time. A lot of progress has been made, and a lot of businesses have adopted IPFS since it was first introduced in 2016. Users may freely exchange data with one another using this technology. If you have a huge file that you need to upload and/or download over the Internet, IPFS is a great solution. In order to store information in a global and decentralized environment free of file size limits while maintaining transparency, researchers [24] have developed the IPFS using blockchain. In this case, the IPFS system takes the document's data and makes a unique hash of it. The hashes are then stored in a smart contract, which makes the system unchangeable. IPFS and blockchains are two technologies that could work well together because they are both built in similar ways. IPFS would connect all of these different blockchains in some manner analogous to the way the internet connects all of the websites currently online. In the same way that we can place a link on one page that takes us to another page, Ethereum can have a link placed within it that takes it to a different network, for instance.

2.2.5 Peer-to-peer(P2P) network:

Peers are several other computers that are interconnected via the internet.In a peer-to-peer network, two computers that are both connected to it can talk to each other without the help of any server computers [25]. Instead of having a central hub or middleman, peers or participants talk directly with each other. Each node has a copy of the information, and they may exchange it with one another without a third party's assistance [26]. P2P networks are available in two different varieties: A pure P2P network has nodes that are all the same, but a hybrid P2P network has a central hub. A blockchain network's decentralized design consists mostly of peers. All nodes act the same, store information the same way, and talk to the system in the same way. Since the chain is duplicated at each node in a peer-to-peer network, it is harder for bad people to attack.

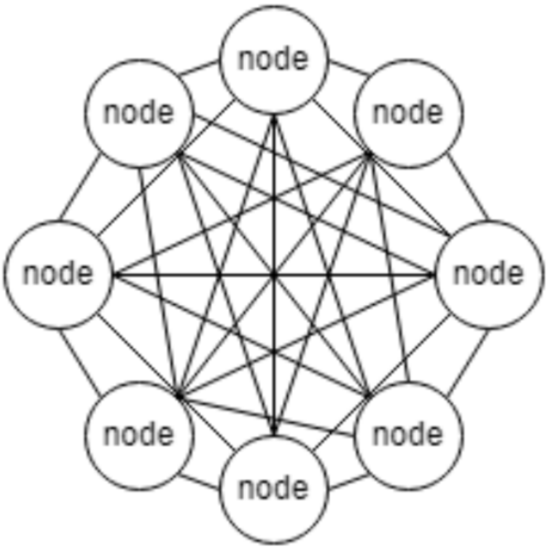


Figure 3: Peer-to-Peer Network

2.2.6 Smart Contract:

According to Catchlove (2017)[27], a smart contract can be defined simply as a set of rules and regulations including specific protocols encoded digitally that the involved parties should follow. Execution of a smart contract begins when predetermined conditions are met which results in meeting the expectations of having anticipated outcomes. These processes closely resemble conventional legal contracts, which document the mutual agreement of parties involved in the exchange or transfer of goods. Every step in the contract's execution is recorded as an immutable transaction on the Blockchain. Smart contracts ensure the implementation of proper access control and necessary contractual conditions. Developers, in particular, have the authority to grant access permissions for each function within the contract.

A smart contract is a great tool to use in any type of system. Some of the key features of smart contract are given below [27]:

1. **Digital Form:** By leveraging blockchain technology, smart contracts offer the ability for code to govern and execute various terms of the contract. This is made possible by registering the ownership of digital assets or digital representations of physical assets on the blockchain. The electronic format provides functionality that allows parties to initiate actions based on specific electronic triggers integrated into the blockchain. Since there is a high security system each transaction or interaction that takes place inside the smart contract uses a digital signature.

2. **Framework based on conditions:** In the realm of contract law, commitments are formed through the exchange of promises: if one party does something, the other party will reciprocate in a certain manner. Similarly, this conditional framework

forms the core of smart contracts and the underlying code that defines them. The incorporation of conditional statements is crucial in the coding of smart contracts.

3. **High Accuracy:** Boolean logic is used in smart contracts resulting in the production of either a true or false value through computation. This indicates that the computer coding of smart contracts does not allow for ambiguity which allows the contract to determine whether the incident actually took place or not more clearly. This is in contrast to traditional contracts where nuances and interpretations are often required. This reliance on strict syntax in smart contracts brings about a higher level of certainty, as the outcomes are precisely defined

4. **Performance based:** Performance is a notable concern in traditional contracts, as it is not always guaranteed. However, smart contracts address this issue by providing a higher level of performance assurance. Once the contract terms are programmed into code and deployed on a blockchain, the need to rely on the parties to fulfill the contract reduces.. Again, specific conditions and requirements for performance, such as asset transfers, can be directly encoded into smart contracts. Consequently, the potential for opportunistic breaches is significantly reduced or eliminated. Smart contracts prioritize performance and offer a greater likelihood of fulfilling contractual obligations compared to traditional contracts.

Zheng et al. (2020) suggests that a smart contract has four consecutive stages are discussed below [28]:

1. **Creation:** Lawyers or counselors assist the parties in preparing the initial contract. If the contracts are less formal or legally binding, the parties agree on the terms. Software programmers then convert the natural language agreement into a smart contract using computer languages like declarative languages and logic-based rule languages. This conversion process follows the principles of software development, including design, validation, and implementation.

2. **Deployment:** Once smart contracts are created, they are saved on the blockchain, and their immutability prevents modification. Even small changes require the creation of a new agreement. When smart contracts are deployed, all parties involved can access them on the blockchain. To ensure the security of the smart contract, the associated digital wallet is sealed using blockchain and digital assets technology.

3. **Execution:** After deployment, the smart contract's provisions are monitored. When the predefined conditions of the contract are met, the contractual procedures or functions are automatically executed. If a condition is true, the corresponding statement is executed, resulting in a transaction that is validated and executed by miners on the blockchain. It is important to understand that smart contracts are essentially programs consisting of declarative statements with logical connections.

4. **Completion:** Once the smart contracts are executed, the states of all parties involved are updated. The transactions that occur during the execution of smart contracts, as well as the updated states, are stored on the blockchain. At this stage, the parties complete the transfer of digital assets between each other. The digital assets of the involved parties are then unlocked, marking the completion of the entire life cycle of the smart contract.

2.2.7 Audit Trail and Blockchain:

A blockchain is a distributed ledger that contains every detail of every transaction that has ever taken place. Transaction authenticity and integrity are protected by cryptographic digital signatures. Because the blockchain is decentralized, anybody with the right equipment (nodes/miners) may process transactions and earn rewards. An independent audit is always necessary because of the possibility of manipulation at any stage of the transaction's lifetime.Exclusive access to the blockchain might be offered to auditors and investigators so that they may examine immutable, timestamped records of all transactions.
A process or system's audit trail is a chronicle of all activities that were taken and when they were taken including by whom. For reasons of auditing, compliance, or investigation, it leaves a clear and verifiable paper trail of activity that can be reviewed and analyzed [29]. There are several advantages to using blockchain technology in auditing. Due to the key feature as, transparency and immutability makes blockchain's audit trail reliable and impossible to modify. All transactions ever made are recorded in the blockchain and may be verified at any time. This openness boosts confidence, cuts down on middlemen, and enables audits in real time. As a result of its distributed structure, blockchain also removes the need for a trusted third party to verify transactions, making the audit trail more trustworthy. Thus, Blockchain-based audit trails are effective for building authenticity in legal systems because they are consensus-driven and tamper-proof records of systemic occurrences.

Digital signatures are a highly secure and trustworthy alternative to other audit trail methods like hash values and timestamps that are utilized for blockchain verification. As an element of public-key cryptography along with the blend of blockchain, digital signatures offer a reliable means of authentication and data integrity [30]. It can ensure that transactions have been authorized by the appropriate parties and through this data manipulation can be detected if it happens. Digital signature can be used for verification via audit trail in blockchain to certify that the data that has been recorded in the blockchain has not been tampered which certainly guarantees the integrity and validity of transactions. As stated by Stamp(2005), in cryptography, a digital signature is the process of attaching a distinct digital fingerprint to a message or document. It verifies the authenticity of the sender and the message's integrity throughout transmission and storage. Sender's private key is used as a means of digital signature while inputting the data and further this signature is then checked against the sender's public key to ensure its authenticity [31]. The blockchain system ensures that all transactions have been authorized by the proper parties and that data has not been tampered with by including digital signatures in the audit trail.

2.3 Hashing in Blockchain:

Hashing is a process through which input of any length is encrypted into a fixed lengthed output using mathematical functions. Hashes are used to establish relationships between blocks in a blockchain. Blockchain relies heavily on hash, a mathematical function, to ensure that all transactions and data kept on the distributed ledger remain secure and unchangeable. The hash is computed using a hashing method to establish a connection between two sets of data. The hash of the prior block is included in the data of each new block on the blockchain. Each node retains its own copy; therefore, anybody wishing to edit one block will be required to update the information throughout all nodes. Hash functions must guarantee that no two inputs result in the same hash value. This will result in maintaining the data integrity of the blocks in the blockchain. If there is even any slight change in the information that a block carries it would result in the hash to completely change and regenerate a new one. This allows the users to identify any new types of information when added to the blockchain promoting traceability. Hashes can also be used as an identifier of the blocks in a blockchain. Since a unique hash is generated every time a new block is added, any block can be traced using these unique hashes and the data preserved inside can be used further.

The most widely used hashing algorithms for file integrity checks are, CRC32, SHA-2, and MD5 a. Other popular hashing algorithms include xxhash, RipeMD, and Tiger.

MD5 is a hash capability that takes a series of information and converts it into a 128-bit unique finger impression. It is commonly utilized as a checksum to ensure the integrity of data. This hashing capability is being used for a long time now and one of its major drawbacks is that often collisions are created between the hashes that are generated here. Despite these vulnerabilities, it remains one of the most extensively used algorithms globally.

A cyclic redundancy check (CRC) is a type of error-detecting code that is commonly employed to identify unintentional alterations in data. When a data string is encoded using CRC32, the resulting hash output will always be the same. As a result, CRC32 is occasionally utilized as a hash algorithm for verifying file integrity. However, in modern times, the use of CRC32 has become less prevalent, primarily limited to applications such as Zip files and FTP servers.[32]

In order to hash Bitcoin transactions, the US National Security Agency created a hashing method known as Secure Hash Algorithm-256 (or SHA256). Ethereum, for its transactions, uses SHA-3, which is part of Guido Bertoni's family of cryptographic primitives called Keccak [14]. Elliptical curve hashing algorithms, which are used for the generation of public keys, have been established as a result of recent technical breakthroughs. The secp256k1 elliptic curve method is used to make public keys for the majority of popular blockchains, like Bitcoin and Ethereum [33]. Everyone on the blockchain network, or node, will have their own unique set of public and private keys.

Overall, blockchain technology's use of hashing guarantees data integrity, enables consensus processes, offers effective verification techniques, and improves privacy protection. It is a crucial cryptographic procedure that helps keep blockchain networks secure and dependable.

2.3.1 Private and public keys:

Asymmetric cryptography is utilized to implement public and private keys.It allows users to verify the legitimacy of a transaction using a digital signature. To begin, information is encoded and then decoded using a key in symmetric cryptography [34]. Unless the recipient has the decoding key, they won't be able to see the data. However, there is a security risk involved in transmitting the key across the network. Asymmetric cryptography [35] is a kind of cryptography in which the private key may be used to decode a public key, or vice versa. The user's private key is associated with a password they should keep secret, while the public key is associated with a username that will be known to many people. The system works as follows: if certain data or information has been hashed using the private key, the public key may decrypt it. A digital signature [36] is generated using this method,and it is used by other nodes to confirm that the sender and the author of the content are the same person. Since the public address is available to all nodes, the validity of any given transaction can be independently confirmed.However, this method may be used to transmit transactions to a single node or a group of nodes, ensuring that only those nodes can verify and decipher the information.

2.4 Consensus Protocols for Blockchain

A blockchain is made up of several blocks, each of which contains information on digital resources along with a header hash connecting it to the block prior to creating a chain-like network. The blocks are connected, and via a consensus process, new blocks may be inserted and withdrawn. The protocols, algorithms, or other computer systems known as consensus mechanisms are what make cryptocurrencies function. According to Rosenberg [37] The blockchain's transaction legitimacy and governance are determined by these systems of agreement. It is essential for the functioning of the blockchain platform. It concerns several aspects of the network applications, including transaction verification, energy consumption, network charges, efficiency, and others. The core blockchain's safety is maintained while transactions' veracity is verified without the involvement of any third party. Being a dynamic, self-regulating system, blockchain necessitates the adoption of a secure method to guarantee the veracity of the transactions. Individuals must come to an understanding on a consensus in order to do this. There have been several proposals for consensus systems, each with a unique set of underlying notions and uses. Proof-of-work (PoW) and proof-of-stake (PoS) are two of the most used consensus procedures when discussing blockchains.

2.4.1 Proof of work (PoW):

By requiring users of a network to expend effort solving an abstract cryptographic puzzle, PoW is a decentralized consensus technology that restrains somebody from modifying the system by enabling transactions to be conducted in a peer-to-peer contained environment without the need for a trustworthy third part said by Nakamoto [33].

To prevent spam emails, the concept was initially proposed in 1993. In 1997, it was given the official name "proof-of-work" by Adam Back. The technology sat mostly unused until Satoshi Nakamoto created Bitcoin in 2009 and began utilizing it to secure the blockchain.[38] In contrast, the proof-of-work approach relies on the fact that each node must solve a cryptographic puzzle before proceeding. As a reward for being the first to figure out the strategy, the miner award goes to that person. The term "hashrate" describes the entire aggregate computing power which is utilized to mine and execute transactions with PoW, which also pays those with speedier hardware. One's chances of producing the following block and earning the mining reward more commonly increase with increasing hashrate. The odds may be raised even more by miners joining forces to form known as "mining pools," which bundle their hashing power and share the rewards evenly among all of the miners participating in the pool.

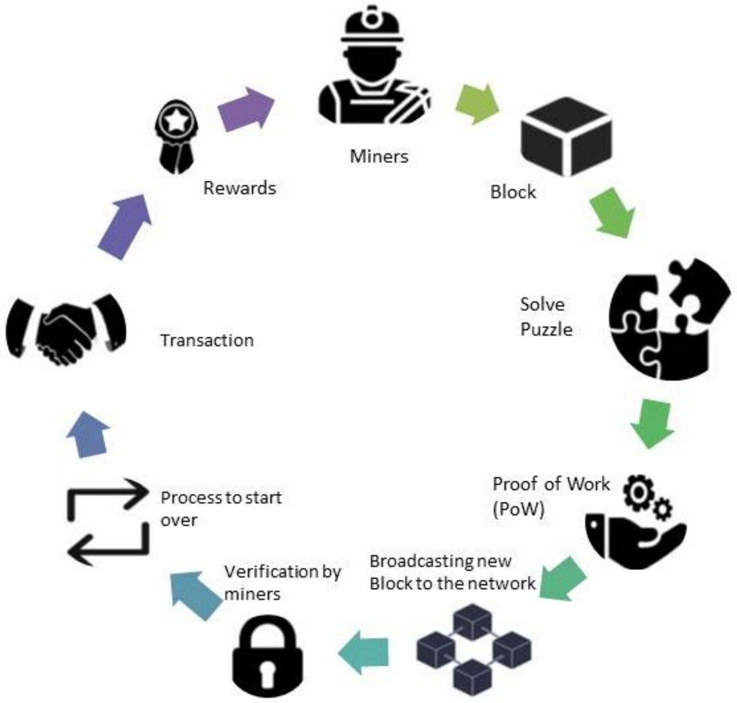


Figure 4: Proof-of-work working process

That increases risk and opposes further decentralization of the blockchain. In addition to that, the blockchain maybe effectively controlled and manipulated if a group of miners or an individual miner can accumulate [39].

2.4.2 Proof of stake (PoS):

In 2011,[36] a member on the Bitcointalk forum going by the moniker of QuantumMechanic developed a mechanism called ”proof-of-stake.” According to Kiayais, Russell alt.[40] Instead of ”miners,” ”validators” verify transactions in a proof-of-stake network, and ”block mining” is replaced by ”block minting” or ”block forging.” For a node to become a validator in a proof-of-stake network, rather than being selected at random as in proof-of-work,it must have staked a certain quantity of coins into the system. PeerCoin’s ”Coin Age” method provides a more detailed explanation of validator qualification; it allows holders of currencies older than 30 days to vie for the right to mine the next block, with the longest-held coins having the greatest chance of success said so by King and Nadal [41]. Furthermore Saleh[42] says the node receives transaction fees associated with the blocks they helped create as payment. Validators risk losing their stake if they participate in fraudulent transactions. This protects the good intentions of the validators, who stand to lose more money than they would earn in any other scenario.Finally, according to [43] Since anyone can't confirm transactions or mine for money with proof-of-stake, it uses a lot less energy. Since the cost of establishing a mining pool is reduced because mining gear is not required,more users are encouraged to establish a node, which increases the system"s stability and decentralization.

2.4.3 Delegated Proof of Stake (DPoS):

An alternative to the more popular PoS protocol is Delegated Proof of Stake (DPoS). According to [44] Developed from PoS, DPoS allows networks to select validators who verify blocks on their behalf. Delegates in DPoS are called "block producers" or witnesses. Following the election of all delegates, they must jointly examine each transaction and make a decision.Comparing PoW and PoS, DPoS offers numerous benefits. It has a number of advantages, including a low requirement for users to have powerful computers, which leads to good energy efficiency and speed. In DPoS technique, every individual of the network gets the opportunity to cast a vote, making it less centralized unlike PoW.Furthermore, said by Ouatttara, Ahmat, alt. [45], it solves the PoS's "rich grow wealthy conundrum" by making reputation, not money, the deciding factor in who gets chosen as a witness or block producer. While delegated proof of stake has made progress and is seen as more effective than other consensus methods, it may be insufficient for usage in smaller systems and may lead to centralized administration. According to Chaudhury [46] Delegated proof of stake, on the other hand, loses power when no one cares to cast a vote, as it's vulnerable to attacks that may be manipulated in various ways (such when the same witness repeatedly acts as the owner in proof of stake and when mining pools of proof of work are used). DPoS and PoS are quite similar, but the primary distinction between them is that DPoS takes a more democratic style and lets users who invest choose which representatives they wish to validate blocks. DPOS appears to be aviable consensus method addressing the blockchain's scalability issue as of right now, with an increasing number of applications and participants.

2.5 Proof of Reputation with Delegated Proof of Stake:

To validate transactions and generate blocks, DPoS uses a predetermined number of trustworthy validators, called delegates where token holders cast ballots to elect these representatives. According to Kleinrock et al. (2020), "Proof of Reputation" refers to a technique that takes into consideration the reputation or track record of participants to determine their weight or vote in a system in contrast [47]. Nakamoto

Fallback where Nakamoto consensus, and more precisely Proof of Work (PoW), is the most well-known consensus algorithm [33]. Along with the stake in the solution to a computational issue, the first node to complete the task is given the privilege of adding a new block to the blockchain. However, if it can be established as a backup in case the DPoS system is compromised or suffers technical difficulties. It improves the system's security, decentralization, dependability, and takes reputation into account in the consensus process by combining DPoS with PoR and having Nakamoto Fallback as a backup [47].

As stated by Hu et al. (2021), in a decentralized environment, the consensus algorithm is crucial to the blockchain's reliability. The Byzantine Generals Problem, one of the most fundamental obstacles in distributed algorithms, is intrinsically linked to the topic of consensus algorithms [48]. In the case that the EigenTrust algorithm is compromised or is unsuccessful then Proof of Reputation (PoR), can be employed as a backup [49]. By having peers give confirmation of their reputation, PoR seeks to ensure that reputation scores are reliable and accurate. This evidence may take the form of cryptographic signatures, verifiable transactions, or any other technique that proves the peer's reputation to be consistent and reliable.

Byzantine Faults:

'Byzantine faults' is a drawback which occurs when some of the nodes in a distributed system are broken or malicious and cause the system to behave erratically which makes to disrupt the system by deviating from the protocol, sending false information, or working in concert with other malicious nodes. Due to its similarities to the Byzantine Generals Problem, a famous distributed computing paradox, Byzantine faults have been given that name [48]. Consensus in a distributed system might be difficult to achieve due to the presence of Byzantine flaws [50]. Because they rely on trusted nodes, conventional consensus methods are susceptible to Byzantine failures. Malicious nodes make consensus harder to reach because they introduce inconsistencies into the network and cause nodes to disagree.

Eigentrust:

EigenTrust is a method based on trust that may be used in distributed systems to solve the Byzantine Generals Problem. Based on prior actions and interactions, each node in an EigenTrust network assigns a trust score to every other node in the network. In order to identify who may be trusted, nodes pool their trust data and share it with one another [51]. Integrating EigenTrust into a consensus process allows nodes to evaluate the trustworthiness of other nodes based on their reputation ratings (Gao et al., 2019) [52]. This aids in reducing the effect of Byzantine nodes that try to disrupt the consensus process by acting deliberately or supplying misleading information. The consensus process might give more credence to nodes with a history of truthfulness and dependability if they have better reputation ratings. As a result, the consensus conclusion is less likely to be swayed by Byzantine nodes, which may have lower reputation ratings. Mentioned by Gao et al. (2019), Reputation-based approaches increase the distributed system's resistance to Byzantine errors by making the consensus process more secure and trustworthy [52]. In spite of the presence of Byzantine faults, these fault-tolerant algorithms allow nodes to reach agreement, making the network more secure and resistant to attacks by malevolent actors or malfunctioning nodes.

Chapter 3

3 Literature Review

3.1 Current licensing system of Bangladesh: the procedure and flaws

In literature, there is a substantial amount of research related to the alleviation of fake licenses. As stated by Md. M. H. Ullah et. al[53] and investigated by G. Bitjoka et.al, fraudulent documents and licenses obtained by drivers which are conducted through the misuse of the system and its weakness can be reduced. As investigated by F. Leema[54], the current system for providing driver's licenses is heavily unreliable. In Bangladesh, the current steps are followed for one to obtain a license, according to BRTA. Firstly one must obtain the learner's license along with the driving license test date. On the day of the test, the candidate has to sit for a generic written test and then a viva, and finally a practical test. If they pass all three, a date for their license is given, otherwise they are required to apply for the test again. After the confirmation of them receiving a license,their biometrics are collected along with personal information such as NID, birth certificate or passport for a smart license card.[55] Now, in this system,there are plenty of ways to avoid giving the actual test, as there exists count less flaws. The major drawback in this system is that, bribery will secure anyone who offers the bribe a license, even though they might not be fit for one as all procedures are manually managed by authorities who are expected to be corrupt. Moreover, technology has advanced so much that producing counterfeit documents and licenses can be done effortlessly, and even more so by authorities thus leaving no room for detection.

3.2 Smart City and Blockchain: Bangladesh's perspective

3.2.1 Smart City

A smart city is one that makes use of technology and data to enhance sustainability, streamline urban services, and improve the quality of life for its residents. A savvy city commonly consolidates progressed computerized advances and creative answers for overseeing city resources and frameworks, like transportation frameworks, energy lattices, structures, and public spaces. These advances can assist with upgrading

asset utilization, diminish gridlock and contamination, work on open well-being, and improve admittance to data and administrations. In order to meet the requirements and interests of all residents, smart cities also involve citizen participation and collaboration with the private sector and other stakeholders. Some of the smart cities in the present world are Singapore, Barcelona, Amsterdam, Helsinki etc.
The intelligence of a city or how well-equipped a city is depends on a number of factors in its legislature, economy, social structure, and the core values that the city possess.

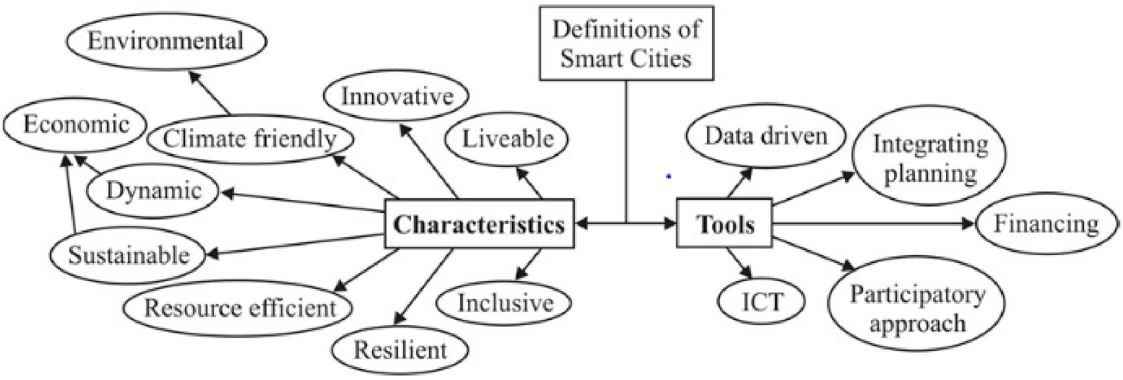


Figure 5: Characteristics and tools that are inclusive in a smart city

In the above figure[56], we can see that in order for a city to qualify as a smart city it has to have efficient resources which are also innovative, sustainable, dynamic, and resilient. A smart city also has technology based and efficient education, government, transactions which would make life easier in general. The approach towards life and the working mechanism of a smart city is data driven which includes a participatory approach, integrating planning, financing, and most importantly ICT.
Information and communication play a very important role in order to manage a smart city. Almost every interaction includes the usage of information and communication technology.
Information and communication are important in order to make efficient use of the infrastructure, economy, education, government, applying new amendments to society, and transportation. It also ensures sustainable development of society in cultural terms along with supporting evidence-based education, transaction of any sort, security, and transparency of data which is one of the biggest challenges in the 21st century.[56] Some of the elements of information and communication which would be essential in a smart city are:

1. **Internet of Things (IoT):** IoT sensors are usually used to collect data and automate complex systems like energy consumption, and traffic management in a smart

city. Thusly, savvy urban communities work on the proficiency of metropolitan administrations, decrease costs, and convey a better quality of living.[57]

2. **Big Data analytics:** Kaviraju, Kaviraju. (2022, June 7) has said that big Data frameworks bring effectiveness into an intricate information foundation. It can have an effect on transportation, public safety, city budgets, and other aspects of a city.[58]
3. **Smart Infrastructure:** Smart infrastructure defines the usage of technology in building the infrastructure as well as maintaining the infrastructure. A smart infrastructure is also data-driven and has the ability to use newfound data to use towards the development of the already existing infrastructures. A smart infrastructure is also an infrastructure that has the ability to automate its management system such as water management, fire management, quality management etc.
4. **4. Citizen Engagement:** Citizens can take more in-depth participation in a smart city with the help of ICT. Voting can be done by the citizens on any new proposed system through mobile applications again feedback can also be taken on any newly implemented system. As a result, citizens are more included in taking decisions that are major for the city.

Apart from the aforementioned technologies, Blockchain is also another important element of ICT. Implementation of blockchain in a smart city can ensure traceability, security, trust ,transparency of data across multiple platforms.
In conclusion, it can be said that a smart city is a city that is built around the motto of making the lives of the citizens easier and better which also ensures the participation from citizens.

3.2.2 Blockchain in Bangladesh

Bangladesh has been exploring the use of blockchain technology in various industries, including finance, supply chain, and land registry. Here are a few examples of recent work in blockchain in Bangladesh:

1) **Land registry:**Bangladesh's government is exploring the use of block chain to create a tamper-proof land registry system, which will make it easier to buy and sell land and reduce the likelihood of land disputes. [59]
2) **Financial Inclusion:** The Central Bank of Bangladesh has been experimenting with blockchain technology to increase financial inclusion in the country.[60] They are exploring the use of blockchain-based digital identities to enable un-banked individuals to access financial services.

2) **Supply Chain Management:**Some companies in Bangladesh are looking to implement blockchain technology to improve transparency and efficiency in their supplychains. For example, companies in the textile industry are exploring the use of blockchain to track the origin of materials and ensure that they are ethically sourced. [61] These are just a few examples of the ways in which blockchain technology is being explored in Bangladesh.The use cases of blockchain technology in Bangladesh and other developing countries will be different and it would be important to consider the specific needs and challenges of these countries when implementing the technology.

3.3 Driver's Reputation Management

Congestion and road accidents have been consequences of rapid urbanization in Bangladesh, where most road accidents are the result of unlicensed drivers or forged licenses.

As discussed by Afsari et al[7], road accident rates have increased due to driving habits of the drivers, who are not properly trained or lack proper licenses issued by the government. Moreover, police are the chief organization for the collection of data regarding any traffic misconduct, where the police are required to physically visit and check and then report back to the HQ. In this method, unless the traffic violation is severe, the drivers are not held back thus allowing them to break further traffic rules as there is no guarantee of the security of the data collected by the police, nor exists any digital record of it, due to it being a heavily manual procedure. In the case the drivers have authentic licenses, the possibility that they haven't been properly trained can not be excluded completely. Even with authentic licenses, drivers regularly cause numerous misconducts on the road such as accidents, speed driving and other traffic rules' violations.

Thus, a driver's reputation management system (i.e driver profiling) is of utmost importance to keep record of the driver's behavioral patterns while driving as a measurement to prevent road mishaps. Driver reputation management system is a proposed system where a driver's profile with all their law-breaking records on road will be stored and analyzed using in-vehicle devices as a means of monitoring. This will mainly record a driver's behavioral pattern as they drive, whether they are aggressive or safe to be on the road, based on their driving and law-abiding capabilities.Introducing such a system will make authorities and passengers aware of a person's driving pattern and will thus contribute to the improvement of road safety. Although existing works all involve identifying driver's behaviors, it seldom involves keeping a record of their driving pattern, thus failing to get an evaluation of the driver's overall reputation while on road. In instances where there is record-keeping done, it is done in such a way that tampering with the available data is unchallenged, which proves to be a great disadvantage for the authorities who are responsible for tracking such aggressive, law-violating drivers as well the ordinary public who are susceptible to falling victims in the hands of such drivers. Hence, we are proposing a blockchain based framework for keeping records of the drivers' profiles so data remains decentralized, secure and immutable.

This blockchain based framework will exist to ensure that the data regarding the drivers and their misconducts are not tampered with, thus creating a safe data transaction and will take Bangladesh one step further towards achieving the smart city goal.

3.4 Related Works

This section reviews the existing works related to driver's profiling systems, Blockchain based management systems and Blockchain based driver's profiling systems. Most of the methods of the driver's profiling consist of collection of data through in vehicle cameras i.e dash-cams, black boxes, sensors, smart phones, smart watches etc. Numerous works involving driver profiling systems have been conducted, most of which use a smartphone based sensor to recognize aggressive driving as a measurement for evaluating the score for the driver [62]. Driver identification based on driving information like speed, acceleration, steering wheel, etc. has lately become an innovative study subject since it can serve as the foundation for cutting-edge applications like car anti-theft and user-based insurance, among others.[12] .These mentioned ways of collecting data and analyzing them in order to create a profile for the drivers makes it effortless to identify the driving pattern of each individuals and can act as a way of preventing accidents ,car-theft and other mishaps both on road and off road.

In literature, there are a few notable works related to Blockchain based reputation management systems. Transparency, traceability, and security by design are characteristics of Distributed Ledger Technologies (DLTs), such as Blockchain. These features make using Blockchain to improve information security, privacy, and reliability acceptable in a wide range of settings. Works have been done where in a consortium blockchain, a category of permissioned blockchain, only a selected amount of certified (approved) nodes are given access for writing in the shared ledger, while everyone else can only use a blockchain query to access the ledger's data. The parking system benefits from this since only a small portion of users,parking lots, have parking offers and are required to register them on the shared ledger in order to act as blockchain validators, while the remaining users, drivers, have to search the blockchain to discover the parking offers.[63]. A. Pradana et.al [39] introduced a system where a driver's demerit points are to be added to a blockchain network due

to any traffic offense. They have implemented a Smart Contract Model where if the demerits crosses the 100 points threshold, the driver's license is suspended. Another work by N. Pramod et. al [64] proposes a Blockchain based driver's profiling system using a Public Key Infrastructure(PKI) based Certificate Authority (CA) to provide digital identification to drivers. In their system, they have introduced a service handling and an event handling blockchain. The service handling blockchain receives, verifies and authenticates a driver's personal information upon applying and the event handling blockchain handles the transactions of the driver's record keeping.
Md. M. H. Ullah et. al [53] proposed a Hyperledger Fabric based system, which provided them with distributed permission based block chain, to extract driver's information. In the system, to create a record against the faults of a driver, police have to file a complaint manually, which is easily averted if the police is corrupt.

Furthermore, numerous countries have implemented a driver's point system, where the drivers receive tickets or demerit points based on their behaviour on the road. Singapore has implemented a Driver's Improvement Point System(DIPS) where recognition of a dangerous driver and suspension of their licenses is done[21]. The demerit points in this system is assigned with fines for some traffic offenses including reckless driving, speeding and disobeying traffic lights. However, the system also rewards drivers for driving safely for a certain period of time. A lot of states in the United States of America also have a point system implemented. Various points are assigned to misconducts on the road such as speeding, reckless driving, hit and run, illegal turns etc and according to their point system, a 12 point reduction in a two years time period of two years will cause in suspension of license.[22] As such, many other countries have also implemented a point system of this sort which assigns demerit points to driving license holders.

The table below shows some comparisons between our research and existing works.

Paper	**Point System**	**Decentralized**	**Authenticity Detection**	**Storage Utilization**	**Deep Learning**	**Scope of License Renewal**
Our Research	Yes	Yes	Yes	Yes	Yes	Yes
[63]	No	Yes	Yes	No	No	No
[39]	Yes	Yes	Yes	No	No	No
[64]	No	Yes	Yes	No	No	No
[53]	Yes	Yes	Yes	Yes	No	No

Table 1: Comparison between other researchers' works and our research

In contrast to the systems proposed by other researchers and already existing driver's reputation systems, our proposed system will have a point system which will the driver's points according to their behaviour on the road, of which the data will be stored on the blockchain network alongside their records making the system tamper-proof. The data is thought to be collected via sensors, dash-cams, black-boxes, GPS already installed in the vehicles and also by complaints of the passengers, which will be used as evidences. Thus, authorities will be able to conduct a thorough investigation and update the point of the driver after each incident. When the driver's score reaches above a certain threshold, after which the driver will not be considered safe on the road and have his license seized.

Chapter 4

4 Methodology

4.1 System Overview

4.1.1 Use Case Diagram:

Description of the use-case diagram: The use-case has five actors. The system has four main actors: the driver, the owner of the vehicle, the passenger, and the police authority. The secondary player is BRTA, which is in charge of carrying out administrative tasks including validating licenses and managing the point system. One of the main characters, drivers, must register by providing their information if they haven't previously done so with BRTA. Once their registration has been verified, they may log in to the system, examine their own points, and, if their license is about to expire, submit an application for renewal. Using their NID, registered drivers may log in. If the vehicle is not already registered, the owner must register it by providing the required information. Owners of vehicles can check the driving history of the person who is connected to their car. Passengers can use the system to report any kind of misconduct or violations, and the complaints are subsequently investigated and documented. Police or Traffic Authorities can view complaints filed by passengers and verify them. They are also able to assign points to drivers, which are verified by BRTA and then are updated in the system. Police can also update the crime history of the driver in the system.

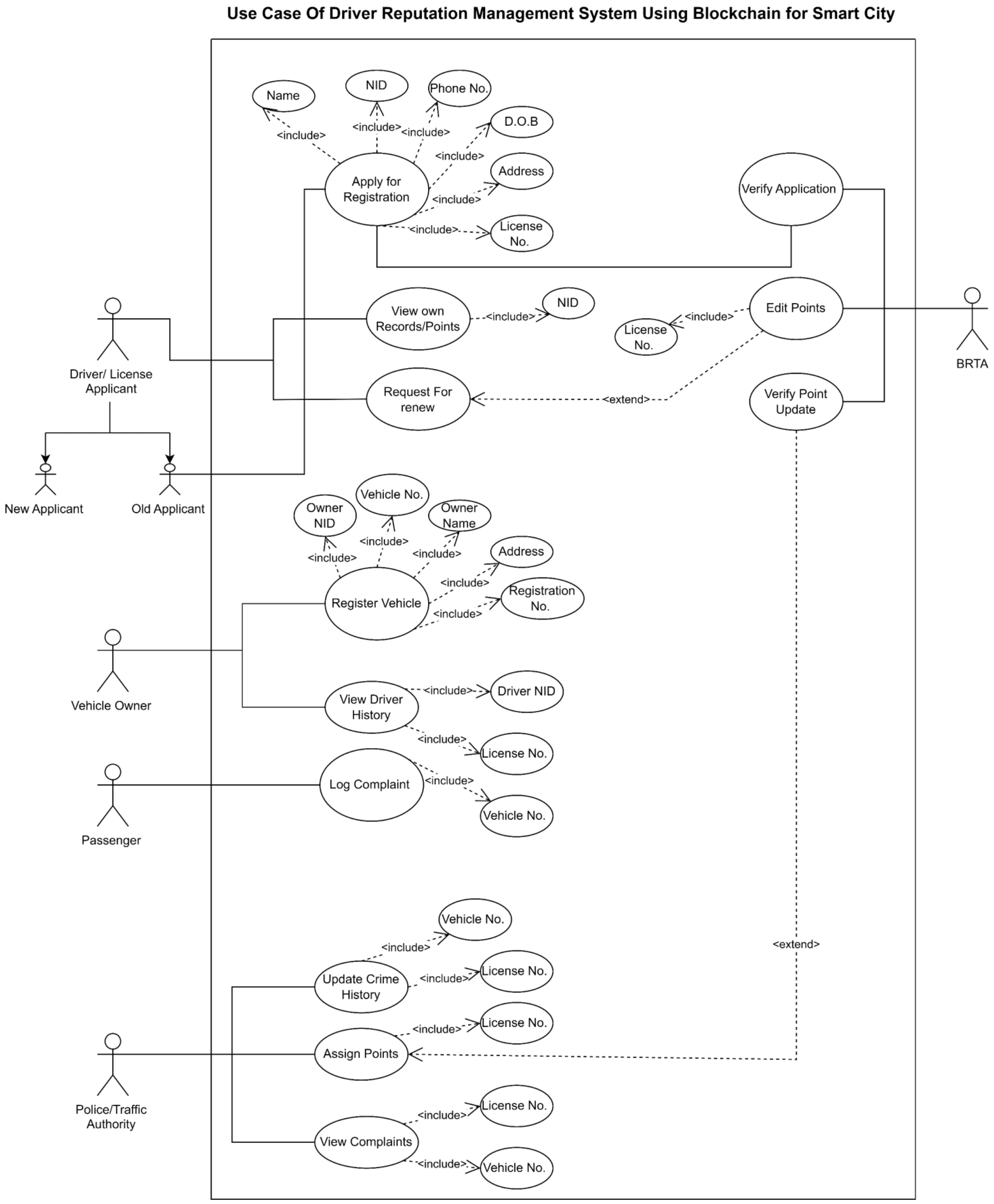


Figure 6: Use Case Diagram of the System

4.1.2 Activity Diagram:

Description of the activity diagram: Drivers gets access to the system and are prompted to provide their NID and Password. If they are a new applicant, they have to enter their information, which gets verified by BRTA and saved in the blockchain. After that, the driver is provided with a password which signifies that they are added to the system and thus they can log in to the system. A previously registered driver can log in to the system just by providing their necessary information. After logging in, the driver can view their own points and request for renewal of license if their license has expired. The request for renewal is sent to BRTA where BRTA verifies the request and renews the license and a confirmation of renewal is sent to the driver. This update is also stored in the blockchain. The process ends here.

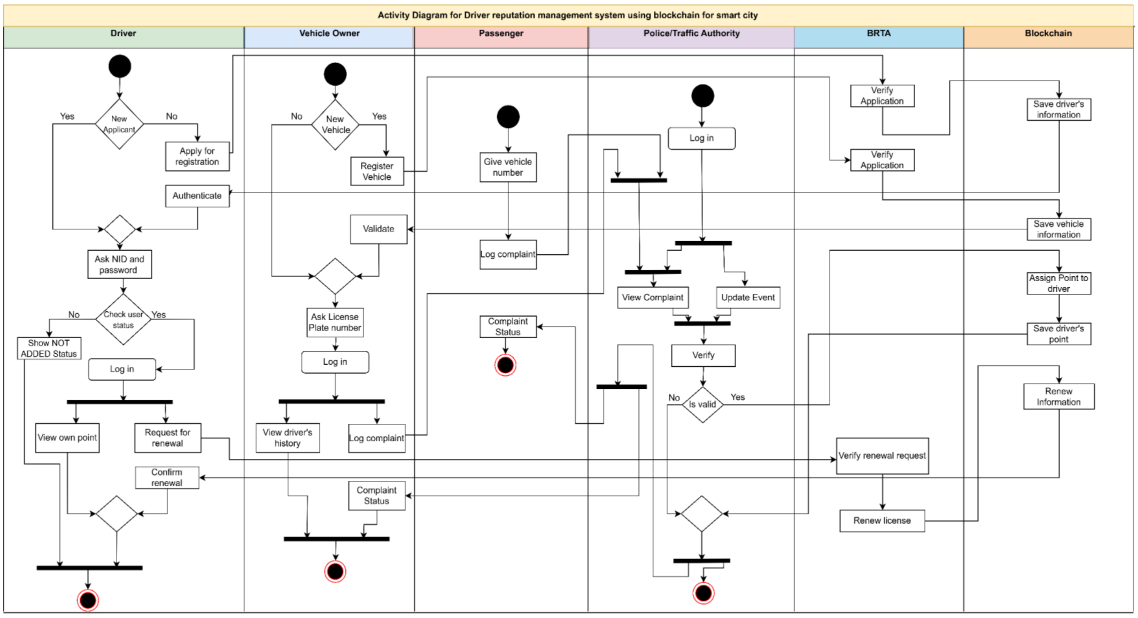


Figure 7: Activity Diagram of the System

A vehicle owner can log in to the system by providing their license plate number. If it is a new owner, or a different vehicle, the owner has to register their vehicle. This registration application is first verified by BRTA and the information is saved in the blockchain. After successful registration, the vehicle owner can log in to the system where they are able to view the history of the driver that is associated with their vehicle. They can also log complaints, which are then sent to the police or traffic authorities for further processing where later they can view their complaint status. This process ends here.

A passenger gets access to the system and can file complaints by providing the license plate number of the vehicle that is associated with the complaint. The complaint is later verified and a status report of the complaint can be viewed by the passenger. Police or Traffic authorities can log in to the system with their credentials and view complaints made by a passenger or vehicle owner. After that, they can verify the complaint made and update the event. If the complaint is valid, police or traffic authorities assign points to the driver of the vehicle. This information is updated and saved in the blockchain. If the complaint is invalid, no update of the crime is given and the process ends here.

4.2 Proposed Model

4.2.1 Customizing the system for Driving Reputation Management System Model:

The BRTA would originally construct the blocks upon the old driver or existing driver seeking to register after confirming the license numbers and other details along with timestamp and with clean records. In a similar manner, for new applicants, the blocks would be produced using their data from BRTA right from the start adding a positive reputation score for obtaining the license. The Genesis Block of our system is that initial block. The Genesis Block will be made for each driver based on their unique license number of the smart driving license by the BRTA. Then, if any accidents or occurrences take place, they will be included along with the event records with all the facts and the timestamp. After creating all of the information in the new block, the block would be closed and rendered immutable by creating a new hash. Subsequent blocks would be added using the old hash number. The following block will appoint the new hash to add points with the previous existing points for new events in a manner similar to that of earlier blocks updating the versions along with update of reputation score and CID of the evidence details of the cases or valid reports against an individual fetched from IPFS. This will connect each block to the prior hash and create a virtual chain that will assist individual drivers keep their reputations with accuracy and efficiently.

4.2.2 Basic Working Principle of the Model Diagram:

In our proposed system, individuals can preserve information about their driving records and vehicles on a blockchain and use tokens and permission-based architecture to control access to their driving records. By linking the driver's license to the vehicle, our solution makes it possible for the driver to access data about any accidents involving that particular vehicle. The following diagram shows our proposed paradigm in broad strokes.

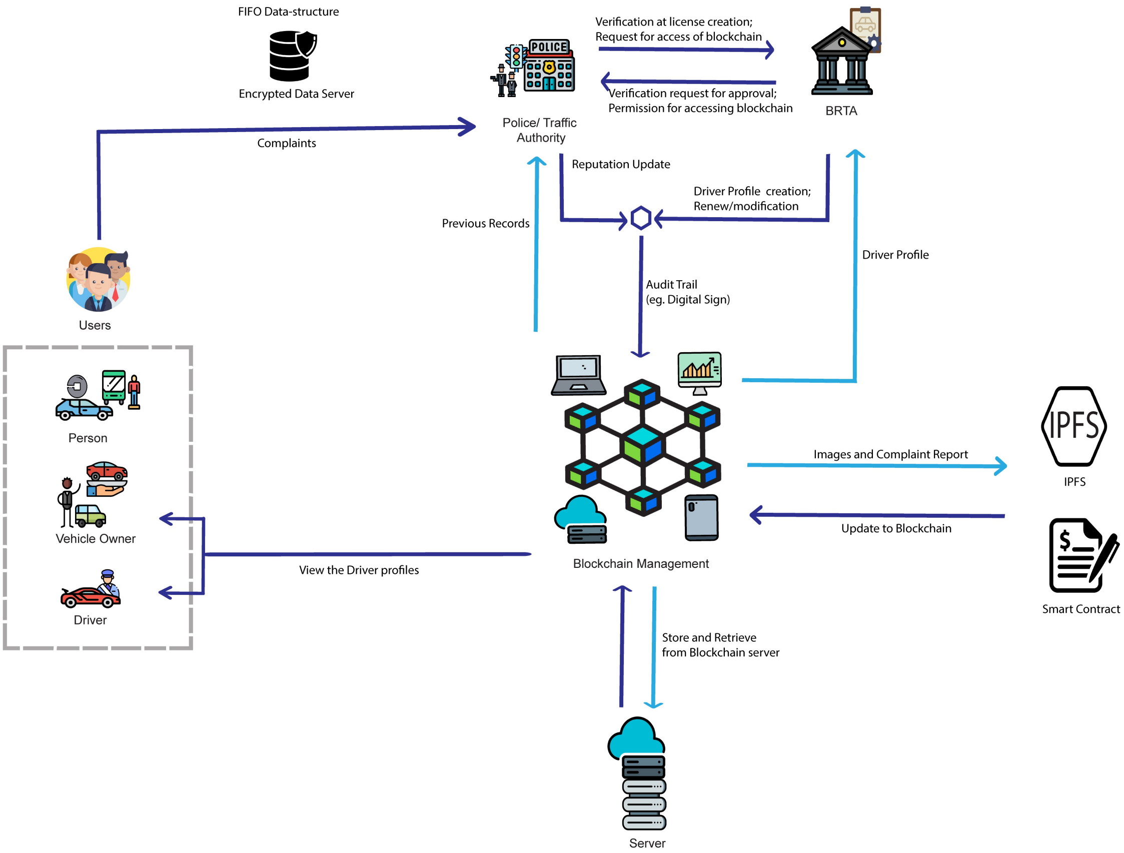

FIFO Data-structure
Encrypted Data Server
Complaints
Police/ Traffic Authority
Verification at license creation; Request for access of blockchain
Verification request for approval; Permission for accessing blockchain
BRTA
Reputation Update
Driver Profile creation; Renew/modification
Previous Records
Driver Profile
Audit Trail (eg. Digital Sign)
Users
Person
Vehicle Owner
Driver
View the Driver profiles
Blockchain Management
Images and Complaint Report
IPFS
Update to Blockchain
Smart Contract
Store and Retrieve from Blockchain server
Server

Figure 8: Working principle of Driver Reputation Management System using Blockchain

- **Schematic representation of the system's underlying workings:**

In our system, users can be divided into the following three groups: drivers, passengers, and owners. There are also representatives from BRTA and the police/traffic department.

The user interface allows users to report dangerous drivers to the appropriate authorities. This component of the system is crucial, since it determines the authenticity of the data and the drivers' standing in the community in response to user complaints. Users may view the current status of their complaints by entering their unique identification number. After receiving complaints from users, data would be encrypted on a back-end server before being sent to the police investigation management server, where it would be processed and used to conduct investigations. The server forwards the complaint to a law enforcement official who is responsible for examining the situation. Following the conclusion of the investigation, the officer will submit a report that will also be kept in the distributed ledger. The server will keep a first-in, first-out (FIFO) queue data structure encrypted filter system for any additional cases against a driver that have not been handled during an ongoing investigation. When an user has an issue with a driver, their complaint goes to the back of the queue. The traffic officer investigates the complaint at the front of the queue. When an investigation has been concluded, the complaint is removed from the front of the queue, and the reputation of the driver is updated accordingly. The vehicle owner has access to a driver's rating in the established blockchain-based driver reputation management system for smart cities. However, after the driver's reputation score has been changed on the blockchain ledger, then the driver is able to see it of his own reputation score. It's important that drivers know how they're doing so they may adjust their behavior and reputation accordingly.

Once a complaint has been entered into the system and placed in the queue, the police will investigate it. If the inquiry confirms the validity of the allegation, the relevant police authority will submit a request to the BRTA for permission to access the particular driver's block of chains to update the chain. Under correct protocol, the police authority changes the driver's reputation score after receiving a permit or public key to enter the system from the BRTA. This guarantees that the driver's record is updated only after appropriate process has been followed and an inquiry has been conducted. When issuing driver's licenses, the BRTA and the police authority are able to communicate with one another. The BRTA initiates the blockchain network with the creation of the genesis block when a driver receives a license with a certain amount of positive points. The BRTA is also able to make changes to or renew driver's licenses and other relevant documentation. Audit trails, such as digital signatures, will be used to confirm the accuracy of these revisions. This guarantees the safety and openness of any changes made to the driver's data.

The system will next sort the complaint's picture file and data file, and execute the appropriate reputation algorithm to determine the driver's reputation score, all of which will have occurred after the complaint has been entered into the blockchain management system. The reputation algorithm will utilize statistical equations to reliably and fairly determine the reputation score. The following procedure is for the system to utilize smart contracts to generate blocks that connect the ledgers on the blockchain. Smart contracts facilitate the automation and simplification of the blockchain network's event creation and verification processes.

The blocks are stored on the server after they have been generated by the system. After being generated, blocks in the blockchain cannot be changed or removed. By combining reputation algorithms, smart contracts, and blockchain technology, the proposed driver's reputation management system for smart cities can accurately and effectively determine a driver's reputation and reliably and securely impose any necessary penalties or fines.

- **Dataflow in Blockchain Management System via IPFS:**

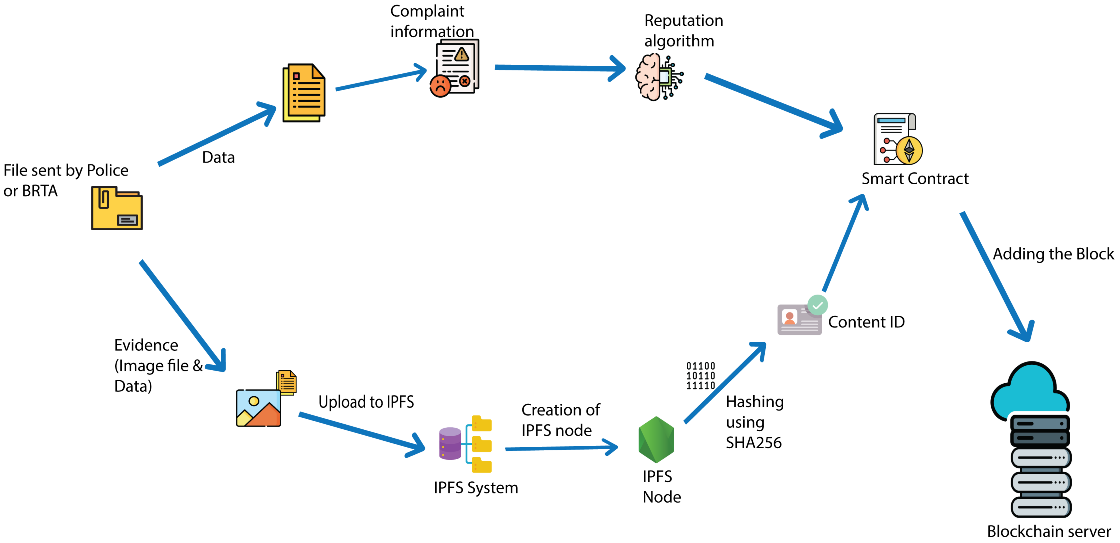


Figure 9: Dataflow in Blockchain management system via IPFS

When all of the details have been entered through the digital signature or audit trial, it will be split into two distinct groups depending on its format: images along with evidence details and algorithmic inputs. To upload the images and evidence details to IPFS, a node will be set up then cryptographic method sha256 will be used to produce a unique Content Identifier (CID), and finally the CID will be sent to the smart contract. On the other hand, the algorithm input will go through the complaint-based reputation model and executing the reputation algorithm for driver profiling the resultant score will be recorded in the smart contract. At last, the system will produce blocks utilizing smart contracts, which will link blockchain ledgers. The blocks will be permanently recorded on the server, making it possible to accurately determine a driver's reputation and effectively impose any fines or penalties that may be warranted. This procedure will assist in maintaining the system's driver reputation ledger up to date and secure, which will improve the system's ability to enforce traffic regulations and enhance road safety for everyone.

The blockchain network's storage capacity shortage has been an ongoing issue in this field because it is a distributed storage method. Faced with the current problems with the aid of the InterPlanetary File System (IPFS), it may effectively increase blockchain storage capacity while lowering computing costs for our system. Following authorization, these files may be converted back to their original, lossless state using the Inverse Distributed Pooling (IDP) technique [67]. Using IPFS, large files like image and documents of evidence a hash ID will be generated making it secure and tamper-proof along with reliability of no duplication and then it will be stored on the blockchain of the driver's reputation, making it less clogged and more secure.

- **Image and evidence storing in BlockChain with IPFS:**

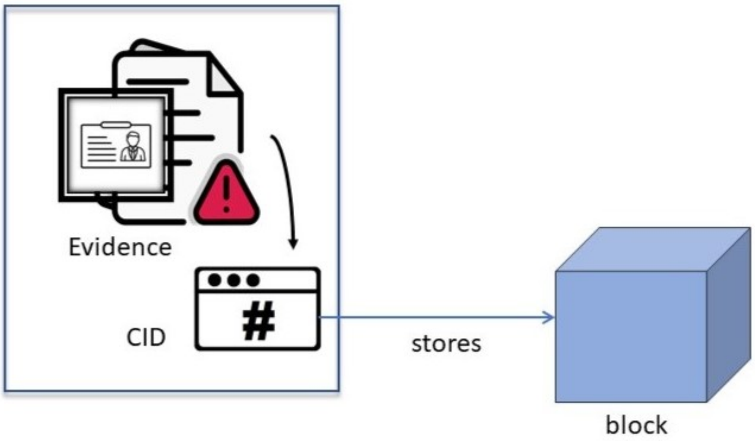


Figure 10: CID storing to Blockchain

To provide collective storage, block chain merges with IPFS. The hash code with an unique ID of the combined data divided in links is returned by IPFS and is kept in the block chain. This model of cooperation successfully addresses the block chain's storage capacity issue and maintains the consistency, veracity, and confidentiality of data [68]. In our system we will be using IPFS for making the system more content based addressing. A single object in IPFS can store up to 256 KB size limit [69]. This immutable distributed ledger IPFS can break up larger files than 256KB into numerous objects that are each 256 KB in size. The system then creates a vacant IPFS object that connects to all the other objects in the document [66]. But we will keep the size limit to 256 KB for the faster access of data.
When the data is sorted to enter the IPFS then firstly divided into chunks of small pieces for more efficient data accessible. Then after hashing a Merkle tree (or Merkle DAG) is generated taking all the chunks into a leaf-branch-root format. The root hash of the Merkle tree is calculated, and this represents the entire set of documentation and images associated with the event. In order to uniquely identify the incident data, the BRTA creates a CID by hashing the Merkle tree's root. The full IPFS dataset is referenced by this CID. Since IPFS utilizes content addressing, each particular chunk may be fetched by its associated CID.
Image files and associated information are stored in IPFS, which is used by our system. IPFS distributes file, application, and data storage and access. Decentralization, content addressing, and participation underpin this system. By spreading data out over several nodes, rather than keeping it all in one place, decentralization

makes it more resistant to intrusion. IPFS is one of a kind because it uses content addressing to determine which files to access instead of their physical locations. The content is identified by a cryptographic hash of the data. To elaborate, the IPFS API allows for simple storage of images as hashes once they have been transformed to ArrayBuffers. And, for bigger datasets Markle tree data structure will be used where the collection is divided into "leaves" and hashed in a Merkle tree. The root has will be formed following their parent hashes. Here, each chuck of hash comparison will help to verify the integrity of the image files for cases or accidents when stored.

The link of the object of blockchain would be stored in blocks of the users especially in case of driver's photo it will be stored in the genesis block of the driver's reputational blockchain so that we it is needed it can access the photo and documents faster upon calling the object from driver's blockchain.

4.2.3 Designing an Effective Reputation Model and Algorithm for Enhancing Driver Accountability

Trust and dependability are essential in the blockchain environment, and participant reputations play a big influence of developing it. Our concept requires a reputation model and algorithm for blockchain systems to evaluate and define drivers' trustworthiness, solidity, and performance. Drivers' reputation scores are used in this approach, allowing blockchain networks to make accurate assessments and connect with other networks. The accuracy and transparency of driver services may be strengthened with the addition of a blockchain-based driver reputation management system. Using the immutability of the blockchain, this system can collect and verify information about drivers such as their driving histories and scores etc. Smart cities can provide more reliable and secure transportation for their citizens by using this technology. The driver reputation management system's implementation of a reputation algorithm is a blockchain-based smart contract. When certain criteria are met, a smart contract will carry out the specified activities automatically. The smart contract evaluates and computes the driver's reputation score after each event or service, using the data recorded on the blockchain.

Initially, when the genesis block of the driver is added to the blockchain, the R_s value, which is the reputation score, is set to be at 50. Afterwards, for calculating the reputation score, the following algorithm will be used for our system:

$$R_s = \alpha . \sum_{e \in E} (w_e . v_e) + \beta . P_x + \delta$$

Here, α is the weighting factor for the number of events, which will be a fixed constant. β is a weighting factor for the already existing point of the driver, here β=1.

w_e is the weight of event e. In the case when an event 'e' on the road occurs, the amount of importance or weight is carried is represented by this. Next, v_e, , where v_e ¡ 0, is the value of event e where the value is fixed for all events that may take place on the road. For example, v_e=-5 for speeding, v_e=-10 for a minor accident and v_e=-30 for a major accident where many are injured.
P_x represents the existing point of the driver.

Finally, δ is the fixed value of the point to be added annually, according to the timestamp of the driver's registration in the system, to the already existing point of the all drivers in the system. This value is fixed for all drivers, and this constant ensures that the reputation score of the driver remains within a certain threshold after the driver has not encountered any misconducts on the road over a certain time period. This value will not be added every time the reputation score is calculated, however, it will serve as a reward point for all drivers.
However, determining the weight of the value of an event solely based on an event type will not give us the most reliable reputation score every time. Hence, we will calculate a "Trust factor", which will determine how much weight the value of an event must carry before calculating the reputation score.

Calculation of the Trust Factor, T_f:

The occurrence of an accident or any other on-road mishap can depend on several factors. First and foremost, the driver is undeniably at fault. However, this may not always completely be the case. By considering the driver to be completely at fault at all times, our introduced point system will cause the points of the driver to decrease at all times. Hence, the consideration of factors such as the time of experience the driver has driving, reputation of the environment where the mishap occurred and some variable external factors are crucial to consider. Thus, we are calculating a trust factor, where we take into consideration of the driver's experience in driving (in years), the reputation of the environment or area of the occurrence of the accident and external factors, such as the condition of the driver.
In order to ensure the credibility of the mishap caused by a driver, and whether the accident is completely independent of the conditions of the surrounding, the trust factor equation is

$$T_f = \mu.(\log E_t) + \sigma.R_e + \omega.E_x$$

In this equation, T_f represents the trust factor. Here, μ, σ and ω are fixed values where μ =0.2, σ=0.4 and ω=0.4, each representing the weights that the factors involved in determining the trust factor carry.

E_t represents the amount of years of experience a driver has on the roads. Here, the logarithm of the value is taken to shorten the value to an appropriate scale for calculation.

R_e is the reputation of an area, which is essentially a value between 0 to 1 where 0 represents an area least prone to accident and 1 being the most prone to accident. This value is prefixed and is thought to be collected based on the location obtained via GPS.

Finally, E_x, where $0 < E_x < 1$, represents external factors such as the state of the driver or if any hindrance was present to cause an unprecedented accident. This factor is to be determined using dash-cams and black boxes installed in the cars. The higher the value of, the more it is likely that external factors affected the accident.

After calculating the trust factor, we will calculate the weight of an event, represented by w_e in our Reputation Score equation which is given by

$$w_e = w_e - (w_e.T_f)$$

This value of w_e will be used in calculating the Reputation Score (R_s) of the driver of the first equation.

The total reputation score for a certain driver is calculated by giving weight to and evaluating these aspects based on established norms. By this method, we are able to obtain an effective reputation score of the driver as other factors which are not in control of the driver causing the accident such as the reputation of the environment is taken into account. Once the reputation score goes below a threshold value which determines if the driver is fit to be on the road, the driver will not be allowed on the road and their license will be seized.

In the case where the driver is renewing their license, the timestamp of their registration to the system will change as a new block will be created and their previous existing point will be their initial reputation score. Once the smart contract receives this information, it will adjust the driver's reputation score such that it more precisely represents the driver's actual performance. In addition, the automation provided by smart contracts ensures that the procedure is both precise and unbiased.

4.2.4 BlockChain Network System for Driver Reputation Management System

For our system, we have also used a hybrid architecture-based blockchain network. Here, the chains under BRTA, the Police Department, and the user (driver and owner) will be private to a certain group, while the passenger and user complaints will be public. The chain will have private information on it, like NID numbers, license numbers, etc., so a public blockchain won't be the best choice. In the area of getting complaints, there will be a public chain where anyone can file a complaint against the driver or vehicle in question. The police department and the BRTA will be in charge of the consortium network. Because of this, it will be a consortium network. So these two consortiums and public networks together will create our system, which will be a hybrid blockchain network merging with Delegated Proof-of-Stake (DPoS). In our system, DPoS consensus mechanism will be more beneficial as such the witnesses would be BRTA and police for the proper validation and verification of the events after proper investigation and then they can add points or participate in the renewal of the driving license. Both Hyperledger Fabric and Ethereum will be used in the construction of our system. We will utilize Ethereum in our public chain, which will handle the complaint-acceptance portion, as it can handle more events and is public, distributed, and decentralized. Hyperledger only organizations or individuals with an authorization certificate can view all network transactions. The reliability of the driver nodes is however guaranteed by the inclusion of this hybridization. The PoR system is used to regularly evaluate the driver nodes' reputation scores. The reputation model seeks to build a trustworthy and reliable network of driver nodes by combining PoR and Nakamoto consensus with a fallback mechanism, and including DPoS. This improves the system's reliability and effectiveness which helps keep the blockchain intact and guarantees precise reputation management for the driver profiling.

- **Dataflow of the data sharing inside the blockchain management:**

Data entered into the DApp by a user is separated into image data and user data. Images are uploaded to IPFS, where they are given an object and a hash. After that, IPFS will give the DApp a string that includes a hash of the information.To find the user's File Hash agreement's domain when they specify a path to share, the DApp looks up the path in the user's File List agreement. The contract is recovered using the address of the accumulating File Hash agreement, which is obtained by obtaining the encrypted string and the value of the IPFS hash using the recipient's private key.

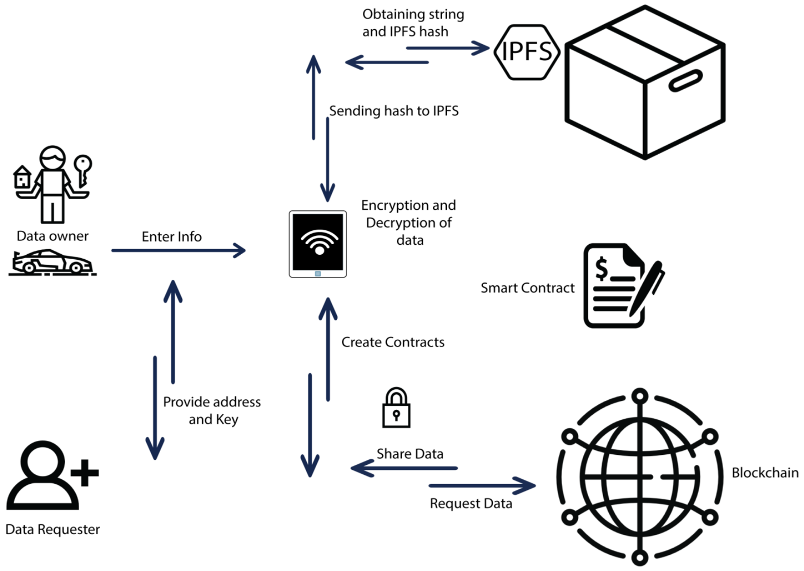


Figure 11: Process of Sharing Data

To facilitate data sharing between users, the decrypted string is decrypted with the data requester's public key. Using the public Data List document, a new File Hash contract is generated, and the encrypted IPFS data is then stored in the tender. The DApp then arranges the information, makes the request, and the blockchain transmits the contact validations list in an encrypted format. The encrypted data and IPFS hash are then combined and stored in the blockchain.

This method employs encryption to safeguard data during transmission on the blockchain, allowing for secure data sharing. IPFS and blockchain technology work together to keep data safe and make it simple for authorized users to access when needed.

- **Data storing process in the blockchain:**

Our data sharing technology encrypts and compresses acquired vehicle data before storing it in the recipient's agreement. The DApp then moves the photo and document URLs to the IPFS object. After passing the DApp's verification procedure, which is vetted by the BRTA and the police in real time, users can upload their information.

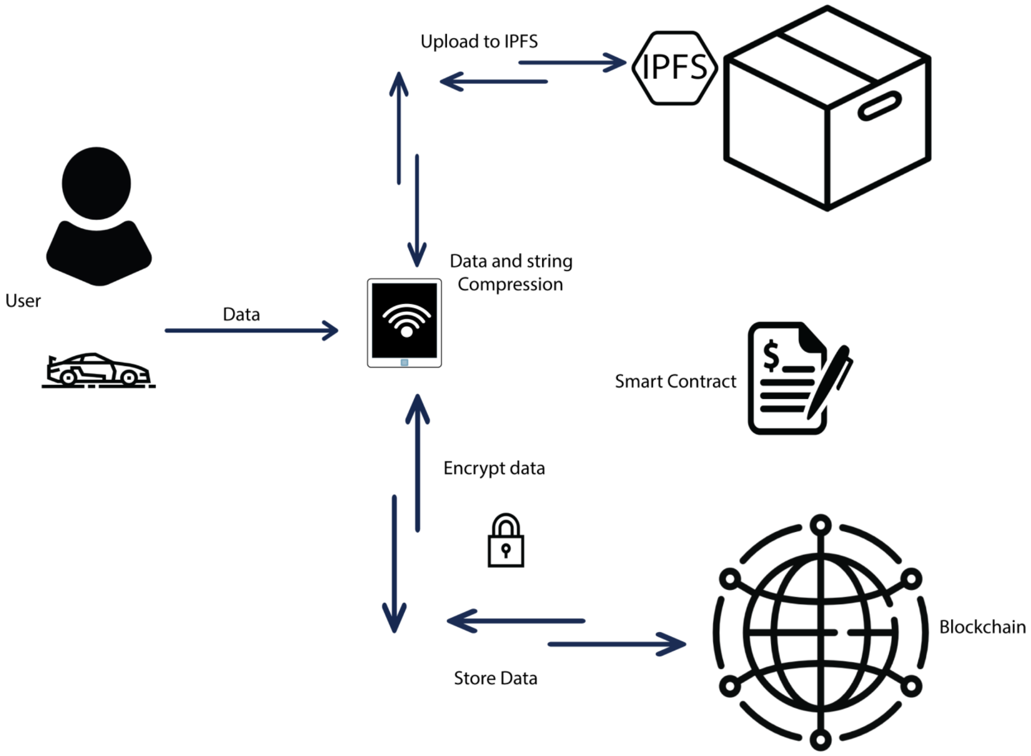


Figure 12: Process of Storing Data

Following a request from the blockchain, the DApp gets the encrypted data, does some initial decryption in solitude, and then retrieves the IPFS file. Next, a compressed string is generated from the imported vehicle data, and this string is then segmented and encrypted using the user's public key.

The encrypted data and IPFS hash values are both stored in File Hash contracts. File List contracts are built from User Data contracts. The File List contract does this by mapping and storing digital identity or certificate as proof of access. Using IPFS for efficient storage and retrieval, our solution combines data compression and encryption methods to store vehicle information safely in recipient agreements. Contracts are utilized to provide safe and responsible data sharing, while the DApp and blockchain are used to allow data exchange and access management.

Chapter 5

5 Implementation

The main ideology behind our system is transparency, integrity, and traceability, for which we have come up with an innovative idea to use smart contracts to set up a blockchain website where all the information will be handled with proof and transparency, which encompasses all the features. Our goal in the implementation was to showcase how our model could be potentially used in a smart city. To this end, we are interested in using blockchain technology and smart contracts to create a secure and immutable method for organizing data. Traceability will be a top priority in our system, allowing for the monitoring and verification of all events and actions. This will make it easier to spot errors and irregularities, increasing accountability and allowing for rapid measures to be taken when necessary.

5.1 Task Brief:

We attempted to build a system incorporating a user side and an authenticator side web based application that will be powered by Ethereum smart contracts that will connect to the blockchain directly. For this, we will connect to the Ethereum blockchain to add, remove, and fetch the information. The methods, software, and languages we have used are JavaScript, HTML, Solidity, Truffle Framework, Ganache, Ethereum Blockchain, MetaMask, and PHP. The uses of these vary from task to task. For example, we built the demo blockchain unit using JS, deployed our smart contract using Solidity and the Truffle framework, and connected it to a frontend using JS, HTML, and CSS.

5.2 Creating Blockchain genesis block:

The genesis block is the first block of a blockchain, and it acts as the beginning of the chain. For our test purpose, we have created a blockchain using JavaScript and wanted to portray how our blocks might look after the implementation of this chain. Firstly, we created a new directory in which we installed the necessary dependencies. After writing the codes needed, we were able to create the genesis block.

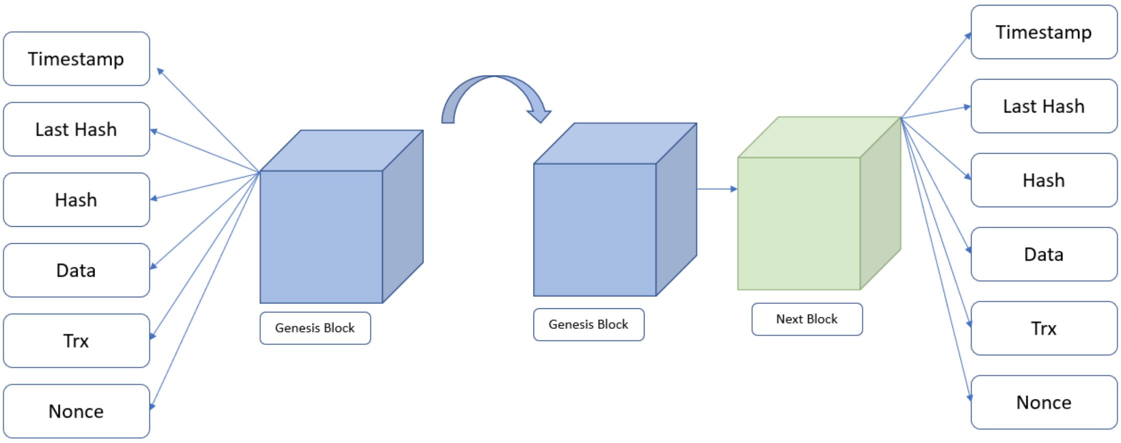
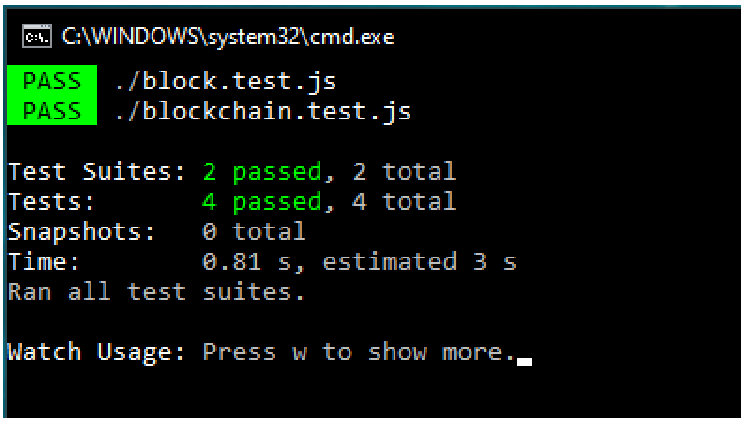


Figure 13: Creation of Genesis block and first mine block

Here we first created a genesis block, encompassing all the necessary information to create a blockchain. The time stamp is a constantly changing value, and the last hash points towards the last node of the chain. The information is hashed by the SHA256 hashing algorithm, and the nonce value is randomly generated for validation of the blocks. We ran some tests to make sure the blockchain is valid and has no errors.



```
 PASS  ./block.test.js
 PASS  ./blockchain.test.js

Test Suites: 2 passed, 2 total
Tests:       4 passed, 4 total
Snapshots:   0 total
Time:        0.81 s, estimated 3 s
Ran all test suites.

Watch Usage: Press w to show more.
```

Figure 14: Testing Blockchain

5.3 Installing necessary platforms

5.3.1 Ganache

We've chosen a local blockchain platform called Ganache for the deployment of blockchain, following the method we proposed. Ganache is an Ethereum-based Dapp development platform that facilitates the predetermined development, deployment, and testing of any decentralized application in a secure way. This imitates the characteristics of a personal blockchain network, which gives us access to some accounts where 100 ether have been assigned to each account for use in operations that require gas fees while launching smart contracts in a virtual environment, testing smart contracts, and giving us the information to connect to Ganache using some server information.

5.3.2 Connecting to MetaMask Ethereum Wallet

MetaMask is a virtual wallet for Ethereum-based cryptocurrencies. Through a web browser or the mobile app's built-in browser, users can access their Ethereum wallet, where they may store and manage account keys, broadcast transactions, send and receive Ethereum-based coins and tokens, and connect securely to decentralized apps. We used metamask to connect with the Ethereum blockchain and complete transfers and transactions.

5.3.3 Other Necessary Dependencies

For being able to use the devices and creating a proper virtual environment ecosystem, it was necessary that JavaScript be installed, including other related packets, as well as its PATH defined in the directory. Node.js was another important factor in the ecosystem as it had the packet manager along with other dependencies, which were very important for the process. It is also recommended that the framework that we have used, Truffle, a dependency of JavaScript. These installations can be a hassle and a time consuming factor, depending on the device.

5.3.4 Truffle Framework

The Truffle framework is a framework for testing and development environments which offers a collection of libraries and tools that simplify the process of developing, testing, and deploying smart contracts on the Ethereum blockchain. Through this tool one can build and manage Solidity (Ethereum's programming language) contracts, automate the testing with JavaScript or Solidity-based test scripts, along with managing the compilation and deployment. Moreover, Truffle is a flexible development environment that supports popular Ethereum client libraries like Ganache, and has a command-line interface (CLI) that simplifies development.

5.4 Project Setup

5.4.1 Creating a Smart Contract

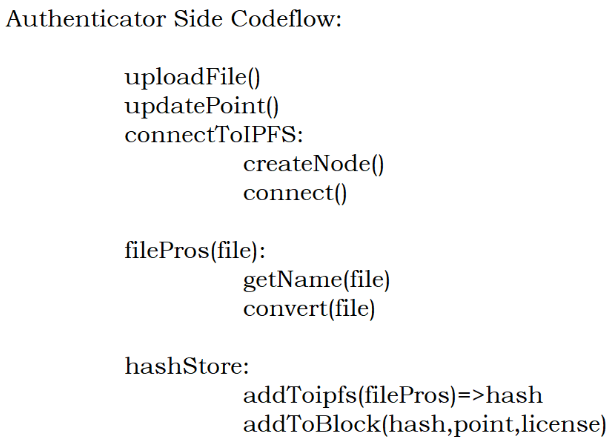
There are some programming languages to write smart contracts, such as Solidity, Vyper, Yul, Rust, etc., which are very special types of coding languages. For our system, we have used Solidity, which is very well known for being used in virtual environments, and better protective measures for mitigating costly mistakes, along with a better library and documentation. We should also note that while deploying a smart contract, it is stored in the blockchain, and as all actions that require some change in the chain require some amount of calculation to be performed, it costs some gas or transaction fee to be deployed.

5.4.2 Storing the file

According to our architecture, there are two types of data that are being updated on the blockchain. One is the evidence, which is stored as images and metadata (e.g., sensor readings, GPS location, etc.), and the other is the information about the driver's reputation score that is being updated after being calculated by our reputation calculation algorithm stated in the architecture. For updating the reputation score part, the information that is entered from the police or authenticator is run through our reputation management algorithm and sent to the smart contract, which will call the $addToBlockchain()$ function and store the information on the blockchain. The other part, storing through IPFS, has some other parts to be executed.

5.4.3 Storing in IPFS

In our proposed architecture, we suggested guaranteeing data transparency. In our case, the data consists of photographs related to evidence as well as other details relevant to the case (vehicle number, location, time, and so on). We chose IPFS as our storage system because it offers a distributed mechanism for storing and retrieving information. First of all, the authenticator will connect to the front end and upload the evidence, after which the application will connect to the IPFS node, following which it will upload the file to IPFS. Then the system will interact and extract the returned hashes (CID) from IPFS as we can see from the figures below are the CID and hashed decentralized information of the evidence file.



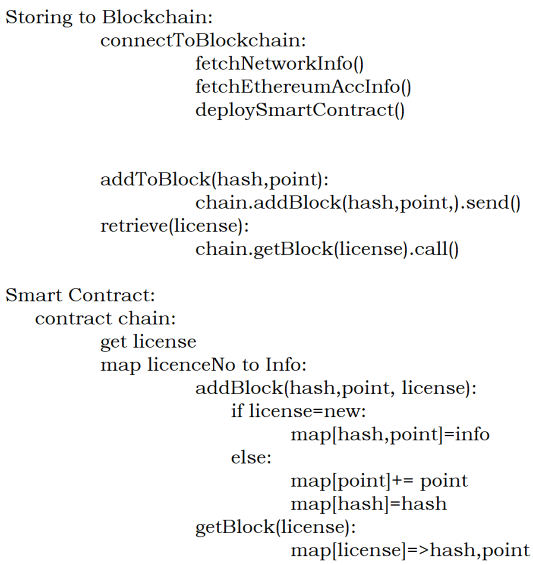
```
Authenticator Side Codeflow:

          uploadFile()
          updatePoint()
          connectToIPFS:
                    createNode()
                    connect()

          filePros(file):
                    getName(file)
                    convert(file)

          hashStore:
                    addToipfs(filePros)=>hash
                    addToBlock(hash,point,license)
```

Figure 15: IPFS Storage Pseudocode

From the pseudo code we can see our first step is to upload the files and connect to the IPFS node. After that the *filePros*() function takes the file and reads its name and converts the file for being uploaded in an optimized way. then the *hashStore*() function is called with the outcomes from *filePros*() function which calls *addToipfs*() and returns the hash that is generated by the IPFS system. Then the hash is stored by referring to the *addToBlock*() function which takes the hash, given point and license number.

5.4.4 Storing in Blockchain

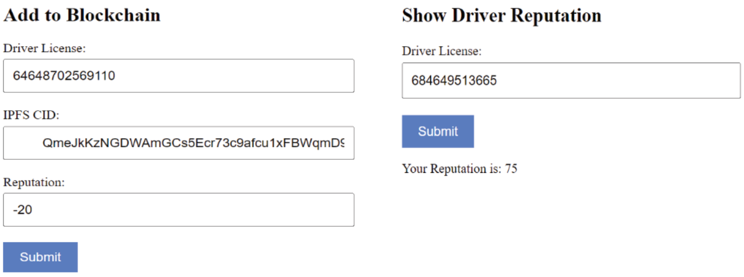
For storing data in the blockchain, the first task is being connected to the local blockchain environment that we have created by fetching the necessary information (host server, port address, etc.), then getting connected to the Ethereum wallet that we have proposed earlier (MetaMask), and then connecting and deploying our smart contracts, which will play their role as the mailman for the blockchain system, maintaining the flow of data to the blockchain. In our smart contract written by Solidity, we have used a special data structure called mapping, which maps one data type with another, almost like a dictionary in JavaScript. This attaches and associates the hash with the license number that is fetched at the beginning.



```
Storing to Blockchain:
            connectToBlockchain:
                        fetchNetworkInfo()
                        fetchEthereumAccInfo()
                        deploySmartContract()


            addToBlock(hash,point):
                        chain.addBlock(hash,point,).send()
            retrieve(license):
                        chain.getBlock(license).call()

Smart Contract:
    contract chain:
            get license
            map licenceNo to Info:
                        addBlock(hash,point, license):
                            if license=new:
                                    map[hash,point]=info
                            else:
                                    map[point]+= point
                                    map[hash]=hash
                        getBlock(license):
                                    map[license]=>hash,point
```

Figure 16: Smart Contract and Storing to Blockchain

Then the *addToBlock*() function is called, which connects with the smart contract, and as there is a *send*() after the function, it means new data will be stored in a block. Adding or making any change to the blockchain requires a transaction fee that has to be paid. It is paid by our Metamask wallet, and the Ethereum is fetched from Ganache, our virtual environment, which facilitates our payment of gas and performs the function. Then there is the function of retrieving the values from the blockchain, which is done by the *retrieve*() function. It is a *call*() function, therefore it does not require any gas, and it returns the value of the hash and the reputation score associated with the driver.



Add to Blockchain

Driver License: 64648702569110

IPFS CID: QmeJkKzNGDWAmGCs5Ecr73c9afcu1xFBWqmD

Reputation: -20

Show Driver Reputation

Driver License: 684649513665

Your Reputation is: 75

Figure 17: User Interface of the System

The user will have to log in to their account and provide their license number to see their reputation score, and the authority will log into their higher access account where they will input the driver's license number against which they want to file the complaint, and then they will upload the image, which will automatically generate an IPFS CID. After that, they have to input the crime they have been categorized as according to our algorithm and press submit. A request will be made from Metamask for digitally signing the transaction, which ensures an audit trail for the system. After signing the transaction with a metamask, the information is added to the blockchain.

Chapter 6

6 Analysis of our Proposed Model and Future Work

6.1 Blockchain in Driver Reputation Management

Blockchain technology is becoming increasingly important in various industries, including transportation, and it can play a critical role in a driver reputation management system for a smart city. Transparency is particularly important for a driver reputation management system, as the data used to calculate a driver's reputation must be accurate, reliable, and tamper-proof to be effective. The smart contract feature also enables automated and efficient processing of data, as well as making the system self-executing, which can be very helpful in case of immediate action, if required, such as revoking a license from a driver with low reputation. A significant problem with blockchain is its storage capacity and performance, which would be enhanced in our system by leveraging IPFS and storing the photos and documents in a separate object, improving performance without adding weight to the blockchain. Blockchain technology can play an important role in a driver reputation management system as it provides a secure, transparent, and tamper-proof way of storing and managing driver data. Additionally, its smart contract feature enables efficient processing of data, making the system self-executing, saving man-power and valuable time with no intermediary corruption.

6.2 Challenges of our system:

When developing and putting into practice a blockchain-based driver reputation management system for a smart city, there are several difficulties to take into account. One of the challenges is **scalability**. As more drivers sign up for the system, if the system is unable to handle huge amount of data, there will be more data to store and analyze on the blockchain. Another major problem is **interoperability** as blockchain networks are typically isolated from one another, and data stored on one blockchain cannot be easily shared with other systems. Making the system completely **free of third-party involvement** will enhance its reliability and integrity as currently, the system requires investigation by police and other authorities for the reputation score to be managed. Finally, getting drivers and the city to **adopt** and use the system is a challenge in itself. The system must be easy to use, user-friendly, and most crucially, provide drivers with real advantages like reduced insurance costs or incentives to drive responsibly.

6.3 Future Works

Using a blockchain system in order to manage a set of information in a decentralized form set in a smart city, would help every involved entity to get a good hold of the system and access information according to one's needs. The unique " Reward Point" system in our proposed model would help manage the misfortune of accidents and create an opportunity to create a transparent system that allows traceability and also promotes speed and high performance due to the adoption of the IPFS module. There are existing works on the management of licensing that promises to make the system more organized like ours but what makes our system stand out from those works is using a FIFO structure while storing the complaints that ensures that every complaint would be managed and solved properly. Again the involvement of IPFS to store the data such as pictures, videos, documents, etc. would increase the scalability of our system making it more organized.

Further Plausible advancements:

One of the major limitations of our system is the establishment of a "smart city" is still in the making, as a result, we are still unaware of the possible technological advancements. In the future, there are scopes of the inclusion of different types of sensors that would help us to measure the accuracy of the complaints filed and also make the process of filing the complaints smoother. Again implementing machine learning algorithms would automate the process of managing the driver's reputation management system and monitor the movements of vehicles and drivers in order to explain situations better. The process of data collection, and maintaining the accuracy of the data is also a mentionable field where improvements can be introduced. Blockchain technology itself is improving which would result in cost reduction, faster implementation, execution, and also create scope for inclusion of cybersecurity which would result in better prevention of data tampering, security, and authenticity of data. Apart from these, the "reward point system" can be further divided into a more filtrated state which would include the count of previous accidents and their level of severity.

Natural language processing can also be introduced in order to detect emotions from the written complaints which would provide the results of the level of truthness from the testimony of the spectators on the site of accidents.

We can incorporate incentivize drivers to behave in ways that benefit the broader goals of the smart city transportation system, such as reducing traffic congestion, improving air quality, and increasing safety. This can be achieved by providing rewards or recognition for drivers who consistently demonstrate positive behavior, such as following traffic rules, using eco-friendly vehicles, and avoiding peak traffic hours. Auditors, engagement with the citizens, and regular review of the system can help in eradicating any type of biases that may exist otherwise. This would tackle the regulatory and social challenges that may arise in our system in the future.

Hence, in the future, there will be considerable amount of scopes to add other features to the existing ones.

Chapter 7

7 Conclusion

Smart cities are cities with improved quality of life, which makes our proposed model of decentralized system of reputation management using blockchain technology have high potential for improving the lifestyle by minimizing illegal road activities and major incidents. The system keeps track of all the stages required in obtaining a license and after the license has been acquired, which is approved by authorities, so the authenticity of the licenses is ensured. Furthermore, the system also ensures transparency by making data easily accessible while maintaining the safety and integrity of it as blockchain technology is tamper-proof. Any sort of data duplication or override will have history checks and will require agreement from private networks to prevent third party involvement. As a result, our system is one unbreakable system for preserving records of the driver which includes their licenses, past records on the roads and the reputation point which will eventually determine the nature of the driving. Although the system is reliable, there exists a lot of challenges related to scalability, interoperability and adoption. With additional research, blockchain-based driver's reputation management systems will play a crucial role in building the transportation of smart cities, where the people can remain assured of their safety on roads leading to a safer urban life.

References

[1] Adhikary, T. S. (2022, February 16).Unfit vehicles: 5 lakh still on the road.The Daily Star.Retrieved September 18, 2022,from https://www.thedailystar.net /news/bangladesh/transport/news/unfit-vehicles-5-lakh-still-road2962921.

[2] Kim, K. S., Myeong, M. H., Kweon, Y. J. (2011). Differences in traffic violations and at-fault crashes between license suspension and revocation. Accident Analysis Prevention, 43(3), 755-761

[3] Prothom Alo (2018) Sharake Pachish Hajar Manusher Mertu, from https: //www. prothomalo.com/ bangladesh/article/1546891

[4] Road Accident: A Major Concern of Bangladesh — CGS. (n.d.). Retrieved September 18, 2022, from https://cgs-bd.com/article/9009/RoadAccident–A-Major-Concern-of-Bangladesh

[5] Mamun, S. (2022b, April 28). 2 million unlicensed drivers, half million unfit vehicles threatening road safety. Retrieved September 18, 2022, from https://www.dhakatribune.com/bangladesh/2022/04/27/2-million-unlicensed-drivers-half-million-unfit-vehicles-threatening-road-safety

[6] Treat, J. R., Tumbas, N. S., McDonald, S. T., Shinar, D., Hume, R. D., Mayer, R. E., ... Castellan, N. J. (1979). Tri-level study of the causes of traffic accidents: final report. Executive summary. Indiana University, Bloomington, Institute for Research in Public Safety.

[7] Afsari, F., Rahman, F. I. (2018, February). Analysis of accidents trend due to driving problems in Bangladesh. In 4 th International Conference on Civil Engineering for Sustainable Development (ICCESD 2018) (Vol. 4)

[8] Al-Hussein, W. A., Por, L. Y., Kiah, M. L. M., Zaidan, B. B. (2022). Driver behavior profiling and recognition using deep-learning methods: in ac15 cordance with traffic regulations and experts guidelines. International journal of environmental research and public health, 19(3), 1470.

[9] Sacks, J. J., Nelson, D. E. (1994). Smoking and injuries: An overview. Preventive Medicine, 23(4), 515– 520. https://doi.org/10.1006/pmed.1994.1070]; [Waller, J. A. (1986). On smoking and drinking and crashing. New York State Journal of Medicine, 86(9), 459–460.

[10] Ferdous, M. S., Sultana, J., Reza, M. S., Ahmed, S. (2020). National Blockchain Strategy: Bangladesh.

[11] Biktimirov, M. R.; Domashev, A. V.; Cherkashin, P. A.; Shcherbakov, A. Yu. (2017). Blockchain Technology: Universal Structure and Requirements.

Automatic Documentation and Mathematical Linguistics, 51(6), 235–238. doi:10.3103/S0005105517060036

[12] Liang, Y.-C. (2020). Dynamic Spectrum Management. Signals and Communication Technology, Chapter 5. doi:10.1007/978-981-15-0776-2

[13] Paul, P. (2021). Blockchain Technology and its Types—A Short Review. International Journal of Applied Science and Engineering, 9(2). https://doi.org/10.30954/2322-0465.2.2021.7

[14] Atlam, Hany Alenezi, Ahmed Alassafi, Madini Wills, Gary. (2018). Blockchain with Internet of Things: Benefits, Challenges and Future Directions. International Journal of Intelligent Systems and Applications. 10.10.5815/ijisa.2018.06.05.

[15] Su, Kehua; Li, Jie; Fu, Hongbo (2011). [IEEE 2011 International Conference on Electronics, Communications and Control (ICECC) - Ningbo, China (2011.09.9-2011.09.11)] 2011 International Conference on Electronics, Communications and Control (ICECC) - Smart city and the applications. , (), 1028–1031. doi:10.1109/ICECC.2011.6066743

[16] Franciscon, E. A., Nascimento, M. P., Granatyr, J., Weffort, M. R., Lessing, O. R., Scalabrin, E. E. (2019, May). A systematic literature review of blockchain architectures applied to public services 2019 IEEE 23rd International Conference on Computer Supported Cooperative Work in Design (CSCWD), pages 33–38. IEEE.

[17] Sharma, P. K., Park, J. H. (2018). Blockchain-based hybrid network architecture for the smart city. Future Generation Computer Systems, 86, 650–655.

[18] Gao Z. Gao, L. Xu, L. Chen, X. Zhao, Y. Lu, and W. Shi (2018). a unified, distributed, edger-based supply chain management system. Journal of Computer Science and Technology, 3237–248, 7–248

[19] Tikhomirov, S. (2017, October). Ethereum: the state of knowledge and research perspectives International Symposium on Security Foundations and Practice (pp. 206-221). Springer, Cham.

[20] Khan, D., Jung, L. T., Hashmani, M. A. (2021). Systematic literature review of challenges in blockchain scalability Applied Sciences, 11(20), 9372.

[21] Antwi, M., Adnane, A., Ahmad, F., Hussain, R., Ur Rehman, M. H.,Kerrache, C. A. (2021). The case of hyperledger fabric as a blockchain solution for healthcare applications Blockchain: Research and Applications, 2(1), 100012.

[22] Abdullah, A. M. (2017). Advanced encryption standard (AES) algorithm to encrypt and decrypt data Cryptography and Network Security, 16, 1–11.

[23] Zheng, Qiuhong; Li, Yi; Chen, Ping; Dong, Xinghua (2018). [IEEE 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI) - Santiago, Chile (2018.12.3-2018.12.6)] 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI) - An Innovative IPFS-Based Storage Model for Blockchain. , (), 704–708. doi:10.1109/WI.2018.000-8

[24] Vashistha, M., Barbhuiya, F. A. (2020, October). Document management system using blockchain and an interplanetary file system. Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure (pp. 212-213).

[25] Schollmeier, R. (2001, August). A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications In Proceedings of the First International Conference on Peer-to-Peer Computing (pp. 101–102), IEEE.

[26] Iansiti, M., Lakhani, K. R. (2017). Do not copy or post. HBR, R1701J, Jan-Feb.

[27] Catchlove, P. (2017). Smart Contracts: A New Era of Contract Use. Social Science Research Network. https://doi.org/10.2139/ssrn.3090226

[28] Zheng, Z., Xie, S., Dai, H., Chen, W., Chen, X., Weng, J., Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. Future Generation Computer Systems, 105, 475–491. https://doi.org/10.1016/j.future.2019.12.019

[29] Kalis, R., Belloum, A. (2018, December). Validating data integrity with blockchain. In 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom) (pp. 272-277). IEEE.

[30] Ryan, R., Donohue, M. (2017). Securities on Blockchain. The Business Lawyer, 73(1), 85–108. https://www.jstor.org/stable/26419192

[31] Stamp, M. (2005). Information Security: Principles and Practices. http://www.gbv.de/dms/hebis-darmstadt/toc/133619745.pdf

[32] Alexandr Kuznetsov, Inna Oleshko, Vladyslav Tymchenko, Konstantin Lisitsky, Mariia Rodinko, Andrii Kolhatin, "Performance Analysis of Cryptographic Hash Functions Suitable for Use in Blockchain", International Journal of Computer Network and Information Security(IJCNIS), Vol.13, No.2, pp.1-15, 2021. DOI: 10.5815/ijcnis.2021.02.01

[33] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260.

[34] Delfs, H., Knebl, H. (2015). Symmetric-key cryptography. In Introduction to Cryptography (pp. 11-48). Springer, Berlin, Heidelberg.

[35] Kube, N. (2018). Daniel Drescher: Blockchain basics: a non-technical introduction in 25 steps.

[36] Korpela, K., Hallikas, J., Dahlberg, T. (2017, January). Digital supply chain transformation toward blockchain integration. In proceedings of the 50 th Hawaii international conference on system sciences.

[37] Rosenberg, E. (2022, September 15). What is a consensus mechanism? Retrieved January 10, 2023, from https://www.thebalancemoney.com/whatis-a-consensus-mechanism-5211399

[38] Sheldon, R. (2021, August 9). A timeline and history of Blockchain technology. WhatIs.com. Retrieved January 10, 2023, from https://www.techtarget.com/whatis/feature/A-timeline-and-history-of-blockchain-technology

[39] Pradana, A., Goh, O. S., Yogan, J. K., Mohammed, A. A. (2018). Blockchain traffic offence demerit points smart contracts: Proof of work. International Journal of Advanced Computer Science and Applications, 9(11)

[40] Kiayias, A., Russell, A., David, B., Oliynykov, R. (2017, August). Ouroboros: A provably secure proof-of-stake blockchain protocol. In Annual international cryptology conference (pp. 357-388). Springer, Cham.

[41] King, S., Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper, August, 19(1).

[42] Saleh, F. (2021). Blockchain without waste: Proof-of-stake. The Review of financial studies, 34(3), 1156-1190.

[43] Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. IEEE Access, 7, 85727-85745

[44] Proof of stake vs. Delegated Proof of Stake. Gemini. (n.d.). Retrieved January 11, 2023, from https://www.gemini.com/cryptopedia/proofof-stake-delegated-pos-dpossection-delegated-proof-of-stake

[45] Ouattara, H. F., Ahmat, D., Ou´edraogo, F. T., Bissyand´e, T. F., Si´e, O. (2017, December). Blockchain consensus protocols. In International Conference on e-Infrastructure and e-Services for Developing Countries (pp. 304- 314). Springer, Cham.

[46] Chaudhury, A. (2021). RepuStake: A Delegated Proof of Stake Protocol that stores the past behavior of witnesses. Available at SSRN.

[47] Kleinrock,L., Ostrovsky, R.,& Zikas, V. (2020). Proof-of-Reputation Blockchain with Nakamoto Fallback. In Lecture Notes in Computer Science (pp. 16–38). Springer Science+Business Media. https://doi.org/10.1007/978-3-030-65277-7_2

[48] Hu, Q., Yan, B., Han, Y., & Yu, J. (2021). An Improved Delegated Proof of Stake Consensus Algorithm. Procedia Computer Science, 187, 341–346. https://doi.org/10.10.16/j.procs.2021.04.109

[49] Sun, Y., Yan, B., Yao, Y., & Yu, J. (2021). DT-DPoS: A Delegated Proof of Stake Consensus Algorithm with Dynamic Trust. Procedia Computer Science, 187, 371–376. https://doi.org/10.1016/j.procs.2021.04.113

[50] Abd-El-Malek, M., Ganger, G. R., Goodson, G. R., Reiter, M. K., Wylie, J. J. (2005). Fault-scalable Byzantine fault-tolerant services. ACM SIGOPS Operating Systems Review, 39(5), 59-74.

[51] Kamvar, S. D., Schlosser, M. T., Garcia-Molina, H. (2003, May). The eigentrust algorithm for reputation management in p2p networks. In Proceedings of the 12th international conference on World Wide Web (pp. 640-651).

[52] Gao, S., Yu, T., Zhu, J., Cai, W. (2019). T-PBFT: An EigenTrust-based practical Byzantine fault tolerance consensus algorithm. China Communications, 16(12), 111–123. https://doi.org/10.23919/jcc.2019.12.008

[53] Mazumder, M. M. H. U., Islam, T., Alam, M. R., Al Haque, M. E., Islam, M. S., Alam, M. M. (2021, January). A Novel Framework for Blockchain Based Driving License Management and Driver's Reputation System for Bangladesh. In 2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST) (pp. 263-268). IEEE.

[54] Leema, F. (2008). Efficacy of driver licensing in Bangladesh (Unpublished master's thesis).University of Calgary, Calgary, AB. doi:10.11575/PRISM/2011.

[55] BRTA Services. (n.d.). Retrieved January 14, 2023, from https://bsp.brta.gov.bd/services/driving-license?lan=en

[56] Eremia, M., Toma, L., & Sanduleac, M. (2017). The Smart City Concept in the 21st Century. Procedia Engineering, 181, 12–19. https://doi.org/10.1016/j.proeng.2017.02.

[57] Simmons, A. (2023, March 16). Smart City and Internet of Things (IoT) Technology. Dgtl Infra. https://dgtlinfra.com/smart-city-internet-of-things-iot/

[58] Kaviraju, & Kaviraju. (2022, June 7). Smart City – Big Data Analytics - KR Architecture World. KR Architecture World - Welcome to the blog world of Kaviraju. https://industry40.co.in/smart-city-big-data-analytics/

[59] Alam, Kazi Masudul Rahman, J.M. Tasnim, Anisha Akther, Aysha. (2020). A Blockchain-based Land Title Management System for Bangladesh. Journal of King Saud University - Computer and Information Sciences. 34. 10.1016/j.jksuci.2020.10.011.

[60] Nusrat, Syeda. (2021). Use of Blockchain Technology in Banking in Bangladesh; Usefulness, Hurdles and Recommendations.

[61] Hassan, Mohamad Ghozali Sharif, Kamal Imran Miraz, Mahadi. (2018). Supply Chain Management for Garments Industries Using Blockchain in Bangladesh. Journal of Business Management and Economic Research. 2. 13-20. 10.29226/TR1001.2018.54.

[62] Ferreira, J., Carvalho, E., Ferreira, B. V., de Souza, C., Suhara, Y., Pentland, A., Pessin, G. (2017). Driver behavior profiling: An investigation with different smartphone sensors and machine learning. PLoS one, 12(4), e0174959.

[63] Badr, M. M.,Al Amiri, W., Fouda, M. M., Mahmoud, M. M., Aljohani, A. J., Alasmary, W. (2020). Smart parking system with privacy preservation and reputation management using blockchain. IEEE Access, 8, 150823-150843.

[64] Pramod, N., Sankaran, S. (2019, December). Blockchain based framework for driver profiling in smart cities. In 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) (pp. 1-6). IEEE.

[65] Xua, G.Z. (2007) All you need to know about the driver's improvement point system (DIPS), Sgcarmart.com. Available at: https://www.sgcarmart.com/news/writeup.php?AID=22GASRC=sgcm

[66] U.S. Department of State. Available at: https://2009-2017.state.gov/ofm/dmv/c66584.htm

[67] Liu, F., Yang, C. Y., Yang, J., Kong, D. L., Zhou, A. M., Qi, J. Y.,Li, Z. B. (2022). A hybrid with distributed pooling blockchain protocol for image storage. Scientific reports, 12(1), 1-10.

[68] Koptyra, K., Ogiela, M. R. (2020). Imagechain—application of blockchain technology for images. Sensors, 21(1), 82.

[69] ShapeShift (2023) IPFs: A journey to complete decentralization, RSS. ShapeShift. Available at: https://shapeshift.com/library/ipfs-a-journey-tocomplete-decentralization (Accessed: January 13, 2023)