
Virtual Police Station

This project report is submitted to
Silicon Institute of Technology, Bhubaneswar
in partial fulfillment of the requirements for the award of the degree of
Bachelor of Technology
in
Computer Science and Engineering

Submitted by
Tirlochan Singh (1701209389)
Ashutosh Rath (1701209093)
Guru Sauri Vargav (1701209337)
Chiranjibi Rout (1701209375)

Under the Esteemed Supervision of
Dr. Kasturi Dhal



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SILICON INSTITUTE OF TECHNOLOGY
SILICON HILLS, BHUBANESWAR – 751024, ODISHA, INDIA
December, 2020

CERTIFICATE

This is to certify that the work contained in the project entitled “**Virtual Police Station**”, submitted by **Tirlochan Singh (Regd. No.: 1701209389)**, **Ashutosh Rath (Regd. No.: 1701209093)**, **Guru Sauri Vargav (Regd. No.: 1701209337)** and **Chiranjibi Rout (Regd. No.: 1701209375)** is a record of bonafide works carried out by them under my supervision and guidance. The contents embodied in the project is being submitted as a part of 7th semester project for the undergraduate curriculum and have not been submitted for the award of any other degree or diploma in this or any other university.

Date : 11/12/2020

Place: Bhubaneswar

Dr. Kasturi Dhal

Asst. Professor

Department of Computer Science & Engineering

External Examiner



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SILICON INSTITUTE OF TECHNOLOGY
BHUBANESWAR – 751024**

DECLARATION

We hereby certify that:-

- a. The work contained in the project is original and has been done by ourselves under the supervision of our supervisor.
- b. The work has not been submitted to any other Institute for any degree or diploma.
- c. We have conformed to the norms and guidelines given to us by the Project Review Committee of our department.
- d. Whenever we have used materials (data, theoretical analysis and text) from other sources, we have given due credit to them by citing them in the text of the project and giving their details in the references.

Date :11/12/2020

Place:Bhubaneswar

Tirlochan Singh (1701209389)

Ashutosh Rath (1701209093)

Guru Sauri Vargav (1701209337)

Chiranjibi Rout (1701209375)



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SILICON INSTITUTE OF TECHNOLOGY
BHUBANESWAR – 751024**

ACKNOWLEDGEMENTS

It is our pleasure to be indebted to various people, who directly or indirectly contributed in the development of this work and who influenced our thinking, behavior and acts during the course of study

We are thankful to **Dr. Kasturi Dhal** for her support, cooperation and motivation provided to us, and also for her constant inspiration, presence and blessings.

We also extend our sincere appreciation to **Dr. Bikram Keshari Mishra** and **Dr. Pradyumna Kumar Tripathy** who provided their valuable suggestions and precious time in accomplishing our project.

Lastly, we would like to thank the almighty and our parents for their moral support and our friends with whom we share day to-day experience and received lots of suggestion and motivation.

Tirlochan Singh

Ashutsoh Rath

Guru Sauri Vargav

Chiranjibi Rout



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SILICON INSTITUTE OF TECHNOLOGY
BHUBANESWAR – 751024**

ABSTRACT

The proposed solution focuses on making a web-app based portal to capture all the details of an incident, where the eyewitness/victim can avail the services of a police station without visiting the police station physically with utmost ease.

The web portal will be available in two interfaces:

1. Chat-bot Interface
2. Manual Interface (User interacts with system manually)

FIRs/Complaints can be lodged in 3 ways

1. Manually writing the FIR/Complaint in the interface provided
2. Uploading snapshot of pre-written report
3. Using the chat bot interface and giving required information

Once the user validates themselves, they can lodge, track any form of complaint or FIR that has been made by them. The Higher Authorities, similarly can update or track any cases under them, thereby giving both the authorities and user, complete transparency of the process. We also provide an innovative auto escalation and performance mechanism, so that cases can be solved with utmost care and minimal time, thereby freeing personnel for more important tasks

Keywords: *IPFS, Decentralised System, Blockchain, Web Application*

LIST OF ABBREVIATIONS

<u>Abbreviation</u>	<u>Description</u>
BTC	Bitcoin
CID	Content Identifier
DAO	Decentralized Autonomous Organization
DAPP	Decentralized Applications
DHT	Distributed Hash Table
DoS	Denial of Service
EEA	Enterprise Ethereum Alliance
ETH	Ethereum
EVM	Ethereum Virtual Machine
HTTP	Hyper Text Transfer Protocol
IPFS	InterPlanetary File System
IPLD	InterPlanetary Linked Data
OWASP	Open Web Application Security Project
SHA	Secure Hash Algorithms

LIST OF FIGURES

	Page No
Chapter 1.	
Figure 1.1. Traditional Client Server model	3
Figure 1.2. Centralized Network vs Decentralized Network	4
Figure 1.3. Transaction in Ethereum Network	5
Figure 1.4. SHA-256 Hash Value	6
Figure 1.5. SHA-256 Digest Example	7
Figure 1.6. Network Layer	9
Figure 1.7. HTTP Request - Response Protocol	10
Figure 1.8. Distributed Hash Table	11
Figure 1.9. Ethereum Smart Contract	14
Figure 1.10. User Flow Diagram	18
Figure 1.11. Police Flow Diagram	19
Chapter 2.	
Figure 2.1. Architecture of Blockchain	23

CONTENTS

<u>CONTENT DETAILS</u>	<u>PAGE NO.</u>
Title Page	i
Certificate	ii
Declaration	iii
Acknowledgement	iv
Abstract	v
List of Abbreviations	vi
List of Figures	vii
Contents	viii
Chapter 1.	<i>Introduction</i>
	1 – 19
1.1. Introduction	1
1.2. Background	2-16
1.2.1. Blockchain Technology	2
1.2.2. IPFS	9
1.2.3. IPFS and Blockchain	12
1.2.4. Ethereum	12
1.2.5. Ethereum Smart Contract	14
1.3. Problem Statement	16
1.4. Objective and Motivation	17
1.5. Proposed Method	17
Chapter 2.	<i>Literature Review</i>
	20 – 32
2.1. Literature Review	20
2.2. Security in Blockchain	21
2.3. Types of Blockchain	28-32
2.3.1. Public Blockchain	28
2.3.2. Private Blockchain	29
Chapter 3.	<i>Conclusion and Future Scope</i>
	33-34
3.1. Conclusion	33
3.2. Future Scope	33
3.3. Contribution	34
3.4. References	34

CHAPTER 1

INTRODUCTION

Imagine a ledger in a distributed network, which contains all the transactions, plus updates itself whenever there is a fresh transaction. The ledger is not in the aids of a centralized administration, and each individual in the distributed network carries a portrait of the ledger. However there is a challenge; once an article is recorded on the ledger, it cannot be destroyed. That signified the concise summary about blockchain technology. In the primary journal about the blockchain technology, the first application which was addressed was Bitcoin. At present this technology is maintained to preserve the bitcoin transactions, this digital record doesn't fall below one administration. Individual transactions are recorded on the bitcoin network, in this, every individual system is a node. These nodes act autonomously during executing the mathematical functions, computing the transactions. The aforementioned transaction will be communicated to other nodes in the decentralized fabric network by a multi-hop broadcast. The critical component is combining a transaction.

A valid transaction makes a block and various valid blocks connected collectively to develop a blockchain network. The blocks are verified and attached to a chain, once they have an adequate consensus. Fundamentally, when we want to attach a block in blockchain we should prove its genuineness. A block requires a minimum number of consensus whenever it is added in the network. The popular consensus mechanism used is Proof of Work, Proof of Stack and the Byzantine fault tolerance to authorize the block. When the freshly generated block is chained with the other block it counterfeits itself with the additional nodes present in the distributed network. Every time an individual demands to nullify a verified block from the blockchain, all the subsequent blocks need to be transformed in the network which is computationally impracticable. Momentarily, visualize the transparency it delivers when the blockchain is developed for sustaining the police statements including the First Investigation Reports (FIR). In this system, an individual zone is a node of the distributed fabric network having the copy of the blockchain. Whenever there is a new complaint which is recorded there will be an FIR connected with that complaint which is timestamped by the system. The respected

complaint can be provided with a cryptographically generated hash key so that the integrity of the block can be authenticated. To prove the genuineness of the block, we will be applying the consensus mechanism. The valid block will be announced to all the nodes present in the distributed network with the timestamp. The end-user needs to login from their mobile to file a complaint, to login an individual should have their unique Aadhaar number for verification. The app will require the location so that the complaint can efficiently be transferred to the nearby police station. The validation of the block is easy, we merely have to associate with the hash key. Once the block signifies a valid block it will be securely connected to the previous blocks which will make the invalidation computationally very complicated, challenging implying an oversimplification. The innumerable confirmations a block grows, the further decentralized the hash power.

1.2. BACKGROUND

1.2.1. Blockchain Technology

A blockchain is, in the simplest of terms, a time-stamped series of immutable records of data that is managed by a cluster of computers not owned by any single entity. Each of these blocks of data (i.e. block) is secured and bound to each other using cryptographic principles (i.e. chain). So, what is so special about it's capabilities?

The blockchain network has no central authority, it is the very definition of a democratized system. Since it is a shared and immutable ledger, the information in it is open for anyone and everyone to see. Hence, anything that is built on the blockchain is by its very nature transparent and everyone involved is accountable for their actions.

The blockchain is a simple yet ingenious way of passing information from A to B in a fully automated and safe manner. One party to a transaction initiates the process by creating a block. This block is verified by thousands, perhaps millions of computers distributed around the net. The verified block is added to a chain, which is stored across the net, creating not just a unique record, but a unique record with a unique history. Falsifying a single record would mean falsifying the entire chain in millions of instances. That is virtually impossible.

The three main properties of Blockchain Technology which have helped it gain widespread acclaim are as follows:

➤ **Decentralization**

Before Bitcoin and BitTorrent came along, we were more used to centralized services. The idea is very simple. You have a centralized entity that stored all the data and you'd have to interact solely with this entity to get whatever information you required.

Another example of a centralized system is the banks. They store all your money, and the only way that you can pay someone is by going through the bank.

The traditional client-server model is a perfect example of this:

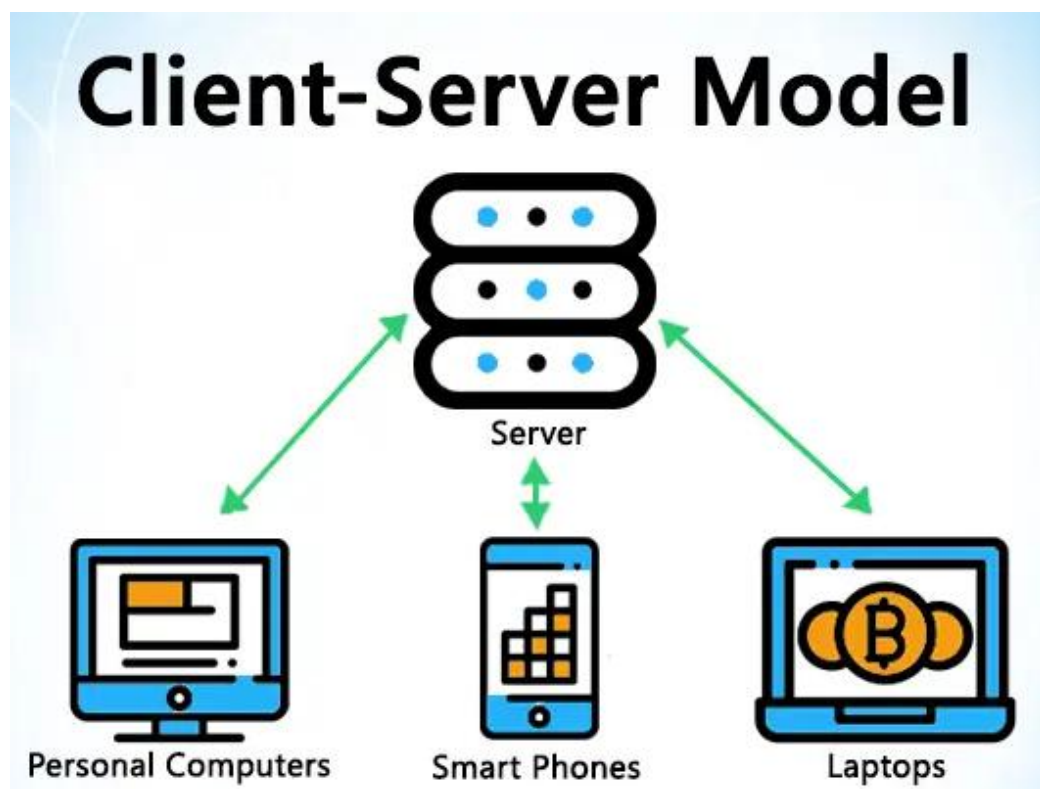


Figure 1.1. Traditional Client Server Model

When you Google search for something, you send a query to the server who then gets back at you with the relevant information. That is a simple client-server. Now, centralized systems have treated us well for many years, however, they have several vulnerabilities.

Firstly, because they are centralized, all the data is stored in one spot. This makes them easy target spots for potential hackers. If the centralized system were to go through a software upgrade, it would halt the entire system

What if the centralized entity somehow shuts down for whatever reason? That way nobody will be able to access the information that it possesses. Worst case scenario, what if this entity gets corrupted and malicious? If that happens then all the data that is inside the blockchain will be compromised.

So, what happens if we just take this centralized entity away?

In a decentralized system, the information is not stored by one single entity. In fact, everyone in the network owns the information. In a decentralized network, if you wanted to interact with your friend then you can do so directly without going through a third party. That was the main ideology behind Bitcoins. You and only you alone are in charge of your money. You can send your money to anyone you want without having to go through a bank.

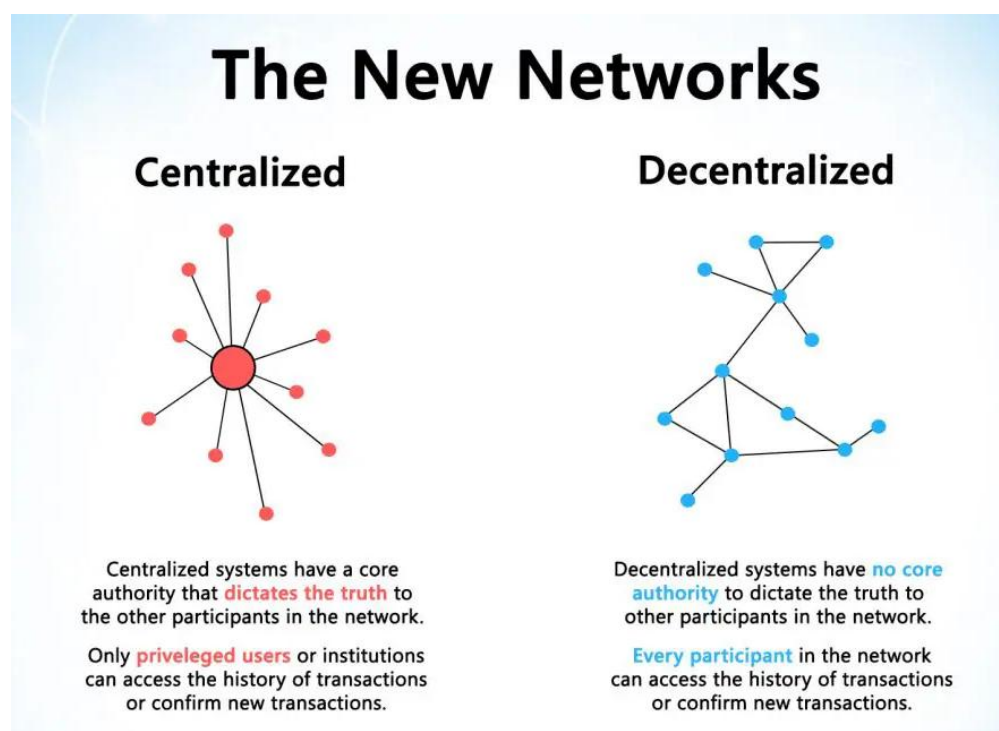


Figure 1.2. Centralized Network vs Decentralized Network

➤ Transparency

One of the most interesting and misunderstood concepts in blockchain is “transparency.” Some say blockchain gives privacy while some say that it is transparent. Why do you think that happens?

Well... a person’s identity is hidden via complex cryptography and represented only by their public address.

So, if you were to look up a person’s transaction history, you will not see “Bob sent 1 BTC” instead you will see “1MF1bhsFLkBzzz9vpFYEmvwT2TbyCt7NZJ sent 1 BTC”.

The below is the snapshot of a Ethereum transactions:








TxHash	Block	Age	From	To	Value	[TxFee]
0x2d055e4585ae2a...	5629306	16 secs ago	0x003e3655090890...	 0x2bdc9191de5c1b...	0,004741591554641 Ether	0.000294
0xb4d37c791ff4cde...	5629306	16 secs ago	0x6c3b4faf413e0e4...	 0xf14cb3acac7b230...	0,744767225 Ether	0.000294
0x9979410dcb5f4c...	5629306	16 secs ago	0x99bcd75abbac05...	 0x2d42ee86390c59...	0,016294 Ether	0.000294
0x189c4d4aae09be...	5629306	16 secs ago	0x175cd602b2a1e7...	 0xd39681bb0586fb...	0,01 Ether	0.000294
0xda0e9bbb11fb77...	5629306	16 secs ago	0x73a065367d111c...	  0x01995786f14357...	0 Ether	0.00150007
0x6be498fafad9acb...	5629306	16 secs ago	0xa3eb206871124a...	 0x8a91cac422e55e...	0,029594 Ether	0.000294

Figure 1.3. Transaction in Ethereum Network

So, while the person’s real identity is secure, you will still see all the transactions that were done by their public address. This level of transparency has never existed before within a financial system. It adds that extra, and much needed, level of accountability which is required by some of these biggest institutions.

From the point of view of cryptocurrency, if you know the public address of one of these big companies, you can simply pop it in an explorer and look at all the transactions that they have engaged in. This forces them to be honest, something that they have never had to deal with before.

However, that’s not the best use-case. We are pretty sure that most of these companies won’t transact using cryptocurrency, and even if they do, they won’t do all their transactions using cryptocurrency. However, what if the blockchain was integrated...say in their supply chain?

We can see why something like this can be very helpful for the finance industry right?

➤ Immutability

Immutability, in the context of the blockchain, means that once something has been entered into the blockchain, it cannot be tampered with.

How valuable this will be for a financial institutes?

Imagine how many embezzlement cases can be nipped in the bud if people know that they can't "work the books" and fiddle around with company accounts. The reason why the blockchain gets this property is that of the cryptographic hash function.

In simple terms, hashing means taking an input string of any length and giving out an output of a fixed length. In the context of cryptocurrencies like bitcoin, the transactions are taken as input and run through a hashing algorithm (Bitcoin uses SHA-256) which gives an output of a fixed length.

Let's see how the hashing process works. We are going to put in certain inputs. For example, we are going to use the SHA-256 (Secure Hashing Algorithm 256).

INPUT	HASH
Hi	3639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8
Welcome to blockgeeks. Glad to have you here.	53A53FC9E2A03F9B6E66D84BA701574CD9CF5F01FB498C41731881BCDC68A7C8

Figure 1.4. SHA-256 Hash Value

As we can see, in the case of SHA-256, no matter how big or small our input is, the output will always have a fixed 256-bits length. This becomes critical when we are dealing with a huge amount of data and transactions. So basically, instead of remembering the input data which could be huge, we can just remember the hash and keep track.

A cryptographic hash function is a special class of hash functions that has various properties making it ideal for cryptography. There are certain properties that a cryptographic hash function needs to have in order to be considered secure.

There is one property that occur in every hash algorithm is called the "Avalanche Effect."

What does that mean?

Even if you make a small change in your input, the changes that will be reflected in the hash will be huge. Let's test it out using SHA-256:

INPUT	HASH
This is a test	C7BE1ED902FB8DD4D48997C6452F5D7E509FBCDBE2808B16BCF4EDCE4C07D14E
this is a test	2E99758548972A8E8822AD47FA1017FF72F06F3FF6A016851F45C398732BC50C

Figure 1.5. SHA-256 Digest Example

Even though we just changed the case of the first alphabet of the input, look at how much that has affected the output hash. Now, let's go back to our previous point when we were looking at blockchain architecture. What we said was:

The blockchain is a linked list that contains data and a hash pointer that points to its previous block, hence creating the chain. What is a hash pointer? A hash pointer is similar to a pointer, but instead of just containing the address of the previous block it also contains the hash of the data inside the previous block.

This one small tweak is what makes blockchains so amazingly reliable and trailblazing.

Imagine this for a second, a hacker attacks block 3 and tries to change the data. Because of the properties of hash functions, a slight change in data will change the hash drastically. This means that any slight changes made in block 3, will change the hash which is stored in block 2, now that in turn will change the data and the hash of block 2 which will result in changes in block 1 and so on and so forth. This will completely change the chain, which is impossible. This is exactly how blockchains attain immutability.

The use of networks and nodes in cryptocurrencies.

The peer-to-peer network structure in cryptocurrency is structured according to the consensus mechanism that they are utilizing. For cryptocurrency like Bitcoin and Ethereum which uses a normal proof-of-work consensus mechanism (Ethereum will eventually move on to Proof of Stake), all the nodes have the same privilege. The idea is to create an egalitarian network. The nodes are not given any special privileges, however,

their functions and degree of participation may differ. There is no centralized server/entity, nor is there any hierarchy. It is a flat topology.

These decentralized cryptocurrencies are structured like that because of a simple reason, to stay true to their philosophy. The idea is to have a currency system, where everyone is treated as an equal and there is no governing body, which can determine the value of the currency based on a whim. This is true for both Bitcoin and Ethereum.

Now, if there is no central system, how would everyone in the system get to know that a certain transaction has happened? The network follows the gossip protocol. Think of how gossip spreads. Suppose Alice sent 3 ETH to Bob. The nodes nearest to her will get to know of this, and then they will tell the nodes closest to them, and then they will tell their neighbours, and this will keep on spreading out until everyone knows. Nodes are basically your nosy, annoying relatives.

So, what is a node in the context of Ethereum? A node is simply a computer that participates in the Ethereum network. This participation can be in three ways:

1. By keeping a shallow-copy of the blockchain aka a Light Client
2. By keeping a full copy of the blockchain aka a Full Node
3. By verifying the transactions aka Mining

However, the problem with this design is that it is not really that scalable. Which is why a lot of new generation cryptocurrencies adopt a leader-based consensus mechanism. In EOS, Cardano, Neo, etc. the nodes elect leader nodes or “supernodes” who are in charge of the consensus and overall network health. These cryptos are a lot faster but they are not the most decentralized of systems.

So, in a way, cryptos have to make the trade-off between speed and decentralization.

1.2.2. IPFS

At its core it is a versioned file system which can store files and track versions over time, very much like Git. It also defines how files move across a network, making it a distributed

file system, much like BitTorrent. In combining these two properties, IPFS enables a new permanent web and augments the way we use existing internet protocols like HTTP.

Simply put, the internet is a collection of protocols that describe how data moves around a network. Developers adopted these protocols over time and built their applications on top of this infrastructure. One of the protocols that serves as the backbone of the web is HTTP or HyperText Transfer Protocol. This was invented by Tim Berners-Lee in 1991.

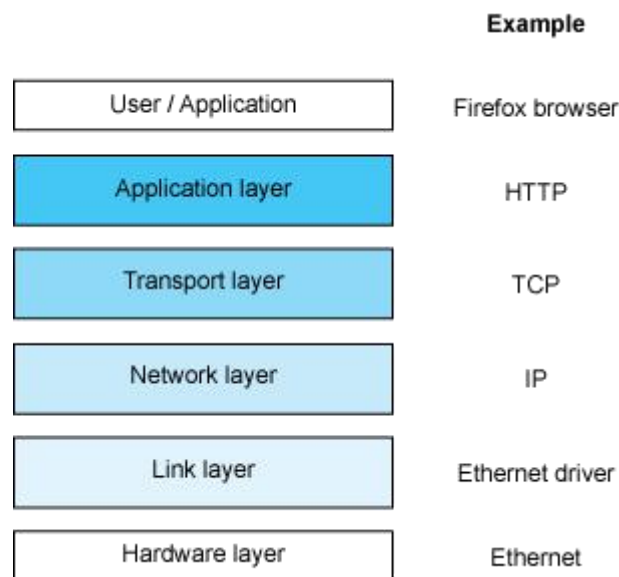


Figure 1.6. Network Layers

HTTP is a request-response protocol. A client, for example a web browser, sends a request to an external server. The server then returns a response message, for example, the Google homepage back to the client. This is a location-addressed protocol which means when I type google.com into my browser, it gets translated into an IP address of some Google server, then the request-response cycle is initiated with that server.

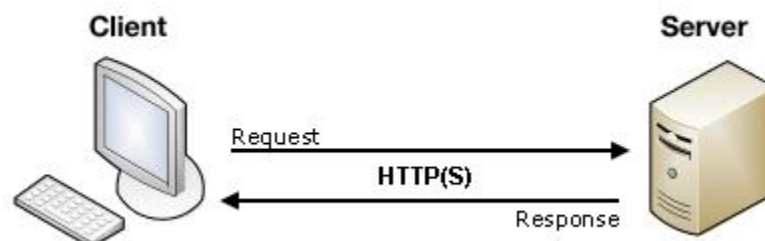


Figure 1.7. HTTP Request- Response Protocol

Problems with HTTP

Let's say you are sitting in a lecture hall, and the professor asks you to go to a specific website. Every student in the lecture makes a request to that website and are given a response. This means that the same exact data was sent individually to each student in the room. If there are 100 students, then that's 100 requests and 100 responses. This is obviously not the most efficient way to do things. Ideally, the students will be able to leverage their physical proximity to more efficiently retrieve the information they need.

HTTP also presents a big problem if there is some problem in the network's line of communication and the client is unable to connect with the server. This can happen if an ISP has an outage, a country is blocking some content, or if the content was simply deleted or moved. These types of broken links exist everywhere on the HTTP web.

The location-based addressing model of HTTP encourages centralization. It's convenient to trust a handful of applications with all our data but because of this much of the data on the web becomes siloed. This leaves those providers with enormous responsibility and power over our information.

How does IPFS work?

IPFS seeks to create a permanent and distributed web. It does this by using a content-addressed system instead of HTTP's location-based system.

An HTTP request would look like "http://10.20.30.40/folder/file.txt"

An IPFS request would look like "/ipfs/QmT5NvUtoM5n/folder/file.txt"

Instead of using a location address, IPFS uses a representation of the content itself to address the content. This is done using a cryptographic hash on a file and that is used as the address. The hash represents a root object and other objects can be found in its path. Instead of talking to a server, you gain access to this "starting point" of data. This way the

system leverages physical proximity. If someone very close to me has what I want, I'll get it directly from them instead of connecting to a central server. In the lecture example from earlier, the students in the classroom can pull the data from each other without all having to establish their own communication with the a server. With HTTP you are asking what is at a certain location whereas with IPFS you are asking where a certain file is. In order to accomplish this, IPFS synthesizes a few successful ideas from other peer-to-peer systems.

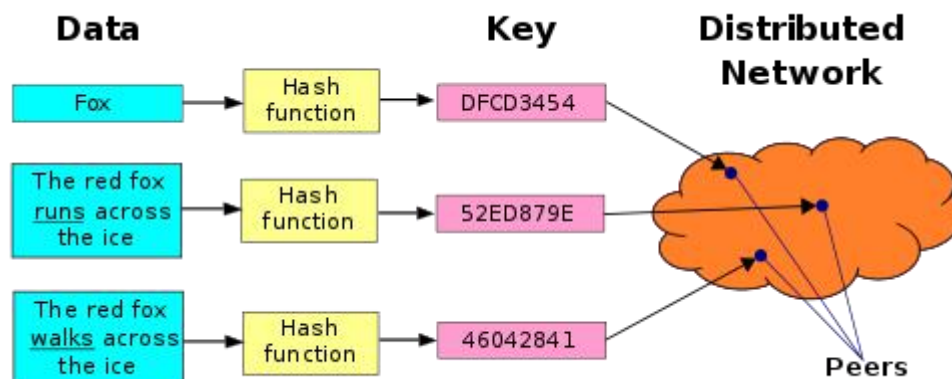


Figure 1.8. Distributed Hash Table

To store data, IPFS uses a Distributed Hash Table, or DHT. Once we have a hash, we ask the peer network who has the content located at that hash and we download the content directly from the node that has the data i want. Data is transferred between the nodes in the network using mechanisms similar to BitTorrent. A user looking for some content on the IPFS web finds neighbors who have access to that content. They then download small bits of the content from those neighbors. On top of the DHT and the BitTorrent protocols, IPFS uses a Merkle Tree. This is a data structure similar to the one Git uses as a version control system and the protocol used in the bitcoin blockchain. In Git, its used to track versions of source code, whereas in IPFS it's used to track content across the entire web.

1.2.3 IPFS And Blockchain

Because of the similarity in their structure, IPFS and blockchains can work well together. In fact, Juan Benet, the inventor of IPFS calls this a "great marriage." IPFS is one of a few projects that are part of a group called Protocol Labs, which was also founded by Benet.

Some projects from Protocol Labs closely related to IPFS are IPLD (Inter-Planetary Linked Data) and Filecoin. IPLD is a data model for distributed data structures like blockchains. This model allows for easy storage and access of blockchain data through IPFS. Users willing to store IPFS data will be rewarded with Filecoin. IPLD allows users to seamlessly interact with multiple blockchains and has been integrated with Ethereum and Bitcoin.

IPFS connects all these different blockchains in a way that's similar to how the web connects all these websites together. The same way that you can drop a link on one page that links to another page, you can drop a link in ethereum (for example) that links to zcash and IPFS can resolve all of that. — Juan Benet

IPFS and other projects from Protocol Labs are ambitious by nature. The idea of a permanent web that is resilient and efficient were no doubt also the goals of the original inventors of our internet protocols. However, over time as our usage of the web changed, weaknesses in these protocols became evident. Although it is in its early stages, IPFS shows promise in being a crucial piece of a new decentralized technology stack.

1.2.4. Ethereum

Beyond Bitcoin & first-generation decentralized applications blockchain was commonly associated with Bitcoin, blockchain technology has many other applications that go way beyond digital currencies. In fact, Bitcoin is only one of several hundred applications that use blockchain technology today.

Until relatively recently, building blockchain applications has required a complex background in coding, cryptography, mathematics as well as significant resources. But times have changed. Previously unimagined applications, from electronic voting & digitally recorded property assets to regulatory compliance & trading are now actively being developed and deployed faster than ever before. By providing developers with the tools to build decentralized applications, ethereum is making all of this possible.

Key Highlights

November 2013: Vitalik Buterin publishes the ethereum whitepaper.

January 2014: The development of the Ethereum platform was publicly announced. The original Ethereum development team consisted of Vitalik Buterin, Mihai Alisie, Anthony Di Iorio, and Charles Hoskinson.

At its simplest, ethereum is an open software platform based on blockchain technology that enables developers to build and deploy decentralized applications

Like Bitcoin, ethereum is a distributed public blockchain network. Although there are some significant technical differences between the two, the most important distinction to note is that Bitcoin and Ethereum differ substantially in purpose and capability. Bitcoin offers one particular application of blockchain technology, a peer to peer electronic cash system that enables online Bitcoin payments. While Bitcoin is used to track ownership of digital currency (bitcoins), ethereum focuses on running the programming code of any decentralized application.

In the Ethereum, instead of mining for bitcoin, miners work to earn Ether, a type of crypto token that fuels the network. Beyond a tradeable cryptocurrency, Ether is also used by application developers to pay for transaction fees and services on the ethereum network.

There is a second type of token that is used to pay miners fees for including transactions in their block, it is called gas, and every smart contract execution requires a certain amount of gas to be sent along with it to entice miners to put it in the blockchain.

“Bitcoin is first and foremost a currency; this is one particular application of a blockchain. However, it is far from the only application. To take a past example of a similar situation, e-mail is one particular use of the internet, and for sure helped popularise it, but there are many others.” – Gavin Wood, ethereum Co-Founder

1.2.5. Ethereum Smart Contract

Smart contract is just a phrase used to describe a computer code that can facilitate the exchange of money, content, property, shares, or anything of value. When running on the blockchain a smart contract becomes like a self-operating computer program that automatically executes when specific conditions are met. Because smart contracts run on

the blockchain, they run exactly as programmed without any possibility of censorship, downtime, fraud or third-party interference.

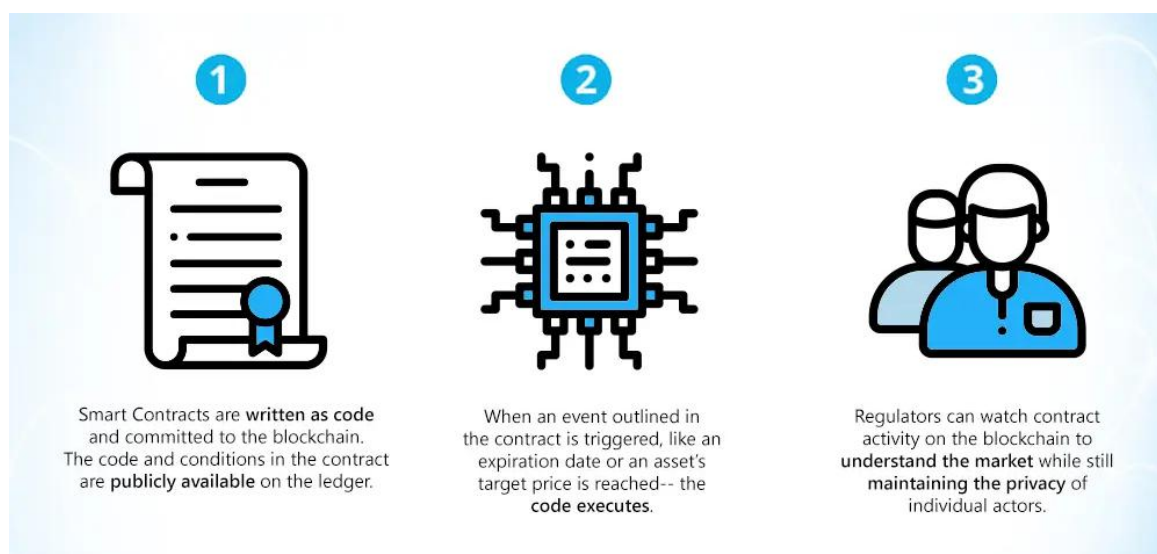


Figure 1.9. Ethereum Smart Contract

While all blockchains have the ability to process code, most are severely limited. ethereum is different. Rather than giving a set of limited operations, ethereum allows developers to create whatever operations they want. This means developers can build thousands of different applications that go way beyond anything we have seen before.

Before the creation of ethereum applications were designed to do a very limited set of operations. Bitcoin and other cryptocurrencies, for example, were developed exclusively to operate as peer-to-peer digital currencies.

Developers faced a problem. Ether expand the set of functions offered by Bitcoin and other types of applications, which is very complicated and time-consuming, or develop a new blockchain application and an entirely new platform as well. Recognizing this predicament, Ethereum's creator, Vitalik Buterin developed a new approach.

"I thought [those in the Bitcoin community] weren't approaching the problem in the right way. I thought they were going after individual applications; they were trying to kind of explicitly support each [use case] in a sort of Swiss Army knife protocol." – Vitalik Buterin, inventor of ethereum

Ethereum's core innovation, the Ethereum Virtual Machine (EVM) is a Turing complete software that runs on the ethereum network. It enables anyone to run any program, regardless of the programming language given enough time and memory. The ethereum Virtual Machine makes the process of creating blockchain applications much easier and efficient than ever before. Instead of having to build an entirely original blockchain for each new application, ethereum enables the development of potentially thousands of different applications all on one platform.

Ethereum enables developers to build and deploy decentralized applications. A decentralized application or DAPP serve some particular purpose to its users. Bitcoin, for example, is a DAPP that provides its users with a peer to peer electronic cash system that enables online Bitcoin payments. Because decentralized applications are made up of code that runs on a blockchain network, they are not controlled by any individual or central entity.

Any services that are centralized can be decentralized using ethereum. Think about all the intermediary services that exist across hundreds of different industries. From obvious services like loans provided by banks to intermediary services rarely thought about by most people like title registries, voting systems, regulatory compliance and much more.

Ethereum can also be used to build Decentralized Autonomous Organizations (DAO). A DAO is a fully autonomous, decentralized organization with no single leader. DAO's are run by programming code, on a collection of smart contracts written on ethereum. The code is designed to replace the rules and structure of a traditional organization, eliminating the need for people and centralized control. A DAO is owned by everyone who purchases tokens, but instead of each token equating to equity shares & ownership, tokens act as contributions that give people voting rights.

"A DAO consists of one or more contracts and could be funded by a group of like-minded individuals. A DAO operates completely transparently and completely independently of any human intervention, including its original creators. A DAO will stay on the network as long as it covers its survival costs and provides a useful service to its customer base".

1.3. PROBLEM STATEMENT

We have proposed this system keeping in mind the difficulties that people face during the registration of an FIR or a complaint at the police station. In the conventional system, the people have to physically visit the police station multiple times, which is very time-consuming. The same also consumes a whole lot of money and energy. The other disadvantages include the fear of getting abused or harmed by people against whom FIR is lodged. Filing FIR against a highly reputed person is sometimes a hard task. It is a common issue that people are often refused an FIR registration. The possible reasons could be that the police official genuinely does not believe the informant, or it could be that his refusal stems from the influence upon him of powerful vested personnel, who have managed to approach him before the informant. The Indian Legal System provides some options that one can exercise in such cases, but it is often seen that people do not have the required information, time, energy, and money to exercise the same. By allowing people to file their complaints directly, this system bypasses the police officers who are often reluctant to register the FIRs, mainly in kidnapping and ransom cases. This would also help eliminate corruption.

1.4. OBJECTIVE AND MOTIVATION

In recent years, blockchain technology has attracted increased interests worldwide in various domains such as finance, insurance, energy, logistics, and mobility. It has the potential to revolutionize the way applications will be built, operated, consumed, and marketed in the near future. In this context, consortium blockchains emerged as an interesting architecture concept that has some advantages of both the private and the public blockchains. These consortium blockchains can also be described as being semi-decentralized. They possess the security features that are inherent in public blockchains, whilst also allowing for a greater degree of control over the network. Proper maintenance of police station records is a prerequisite for the smooth functioning of a police station. However, nowadays, these records are highly vulnerable and are exposed to the risk of being breached or forged. Our proposed system would ensure transparency, security, and privacy of the records stored. The verification of the transaction information would

require some sort of consensus mechanism. Therefore, our objective is to design a platform through which user can easily and more efficiently file a FIR.

1.5. PROPOSED METHOD

The workflow to launch an FIR is as follows:

- The Complainer will have to login to the User Interface using there Aadhar number which will act as a protector so that we can verify them (The platform requires no need of any registration process for the user). Once the user is in the home page, he/she will have different option to launch an FIR

1. Manually writing the FIR
2. Interacting with the chat bot to launch the FIR
3. The user will have a option to provide evidence in image, audio or video format.

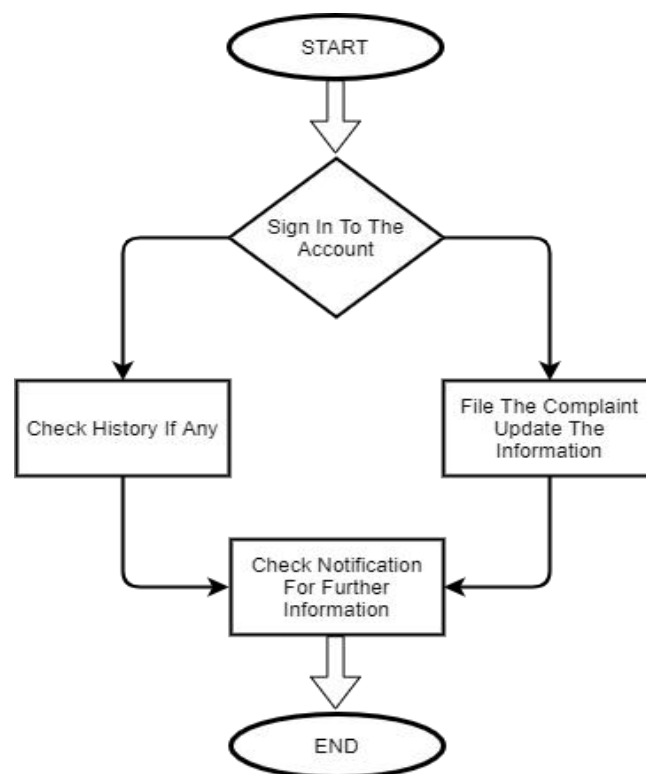


Figure 1.10. Flow Diagram (User)

- Once the FIR is launched successfully to the desired police station, the head of the police station will have the option either to investigate by his/her own or to assign a investigating officer to investigate. Investigating officer will investigate into the

matter with the CID value of the FIR, investigating officer will also provide regular update to the user with the CID value he/she is working with.

- Any changes in the FIR done by the investigating officer will act as a new transaction, and will be uploaded again in the IPFS as well as in the Ethereum network so that the user will get regular updates and can trace the investigation process.
- Once the case is resolved, reward mechanism will assign some sort of reward (which will help the department for the promotion of personals) to the investigating officer (The reward will be based on the type of case solved and the time taken to solve the case).
- The complete system is based on auto escalation facility in which, all the FIR's launched or assigned to the investigating officer will carry some priority which will be assigned on the basis of certain criteria such as cognizable case will be given more priority, non cognizable case will be given less priority. Based on the priority, if a case with higher priority is not getting updated or is not resolved within a certain duration of time then the case will be escalated to the higher authorities.
- The system resembles multi-level feedback queue upto some extent, where not only cognizable case but also non-cognizable case pending from a long time, will get more priority with time so that they can be resolved.
- If a investigating officer is not able to solve a case then he/she can forward the case to higher authority in that case the investigating officer need to change the public key associated with the FIR to the public key of the higher authority to whom the case is handovered, once higher authority accept the case he/she investigate into the matter. (Change of public key with the FIR is done so that user will get a clear idea about who is investigating into there matter)

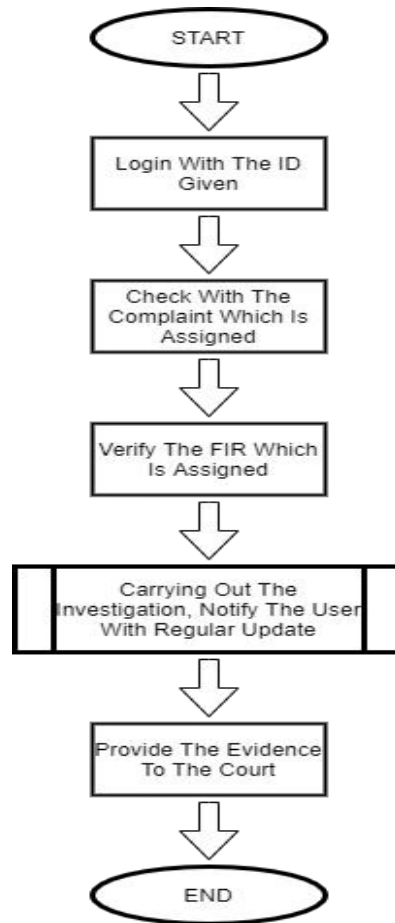


Figure 1.11. Flow Diagram(Police)

CHAPTER 2

LITERATURE REVIEW

The concept of Blockchain technology was first proposed by Satoshi Nakamoto, it is a cryptographically engineered software platform to store ledger using peer to peer network. It is a sequential chain of blocks where every block contains a cryptographically hash value of previous block, time-stamp and the block information. From the above method we can ensure the integrity and security of the block and we can identify the invalid block. The first application of this technology was Bitcoin, which allows cash transaction using internet, through peer to peer network without a central authority and in a trustless network. The author gave a resolution to the problem of double spending. The system uses the method of timestamp by hashing the block into continuous chain based of proof of work mechanism. The introduction of the DAPP and smart contract comes under picture after Ethereum and EVM. We have blocks in the Ethereum blockchain, these blocks are linked together and each blocks we have list of transaction similar to bitcoin. Inside these transaction we do have timestamp and other parameters which we can programme it. Ethereum blockchain gets stored in every miners computer which is called a node, it uses the proof of work algorithm to verify the network. The block contains the smart contract which has the code snippet that runs in each block, when the code computation is successfully executed in each miner's computer. It is sent to whole network so that the other miners can agree. The successful verification of the block will be added to the chain. Other than Ethereum and Bitcoin another example of decentralized system is IPFS. According to protocol lab they want to make the web completely distributed by running it top of the peer to peer networks, it will work similarly how bit-torrent works. In the current scenario when we want to download the content from the web, we have to provide the exact location which we call a URL. Present-day, the model which is followed to download the content is centralize i.e. it is govern by a particular organization – this is called location-based addressing, but if the server is down then we will not get the content. There is a chance that there must be someone who will have the copy of that content in their device which we were searching yet we won't be able to get that. To solve this issue IPFS works from location-based addressing to content-based addressing. All the files in the internet will have a unique figure print. When we want to

download the file we have to compare the hash value and the content will be available. In IPFS there are different types of file that we can store, an object is created in which files are stored, and these object can only store up to 256kb of data. So to store a file like a video n-1 number of objects are created and in n object all the n-1 objects are linked in a sequential manner. This can be used as a file system. The biggest disadvantage of this system is to keep the file available. So to avoid this we can incentivize people to keep the file available or we can proactively make the file distributed so that the file is available – this defines the system of Filecoin. Though DAPP demand was there in the market but still some organization are not able to migrate to public decentralized system due to data censorship, to solve this issue private blockchain was introduced. Hyperledger was the first platform which was allowing organizations to build decentralized applications in a private network so that there data can be secured from the outside world. Hyperledger is an open source platform, in 2015 people from different industry came together to make blockchain more accessible to the world. In this platform the member who are linked to the transaction will only be notified, this create privacy and confidentiality of the transaction. Hyperledger fabric came up with the concept of permissioned blockchain technology. Developers of Ethereum as well as Hyperledger platform are more focused towards decentralized crowd based platform that will identify the scams in internet and it will also provide notification to the other people about the scams in the internet, due to the growth of the cryptocurrency the scams have also increased like phishing website, fake projects and various scam scheme have grown these days. It works with the help of any browser. When a person will do any transaction through the internet there will be a flag which will appear in the browser which will say whether the website is safe or not if these notification does not appear then that person can provide them a report about the website and the developers will give them reward. The report will be verified by the developers of ethereum and hyperledger..

2.2. SECURITY IN BLOCKCHAIN

A blockchain has several built-in security features that make it attractive for purposes like land records, cryptocurrency transactions, etc. The security of personal data is a human right. A blockchain could be one of the methods of ensuring this.

Simply defined, a blockchain is, “A decentralised database containing sequential, cryptographically linked blocks of digitally signed asset transactions, governed by a consensus model.” Blockchain technology is a peer-to-peer networked database governed by a set of rules. A blockchain represents a shift away from traditional trust agents and a move towards transparency. As a technological building block, it permits applications from a broad band of industries to take advantage of sharing, tracking, and auditing digital assets.

Blockchain is a disruptive technology because of its ability to digitise, decentralise, secure and incentivise the validation of transactions. A wide swathe of industries is evaluating blockchain to determine what strategic differentiators could exist for their businesses if they leverage it.

This technology has the potential to improve security, processes and systems in the financial services domain, in government and every sphere where accurate, tamperproof record-keeping is essential.

The disrupted industries will include financial services, healthcare, aviation, global logistics and shipping, transportation, music, manufacturing, security, media, identity, automotive, land use and government.

Market research predicts that, by 2024, the global blockchain market is expected to be worth over US\$ 20 billion. The use and adoption of blockchain technology is expanding at a rapid pace, all over the world.

The Republic of Georgia has declared that it will use blockchain technology to validate property-related government transactions. Countries like Sweden, Honduras and others are also developing such similar blockchain based systems, for enabling secured e-governance.

Gartner projects that the business value added by blockchain will grow to US\$ 176 billion by 2025.

Recently, the Dubai government announced that it will put 100 per cent of its records pertaining to land registry on blockchain. DLD, in fact, claims to be the first such

government department anywhere in the world to adopt the blockchain for such high-level tasks.

The European Union's commercial research group, the European Innovation Council, has launched a programme to grant US\$ 3.04 billion (2.7 billion Euros) to 1000 projects that are developing systems and solutions using blockchain technology.

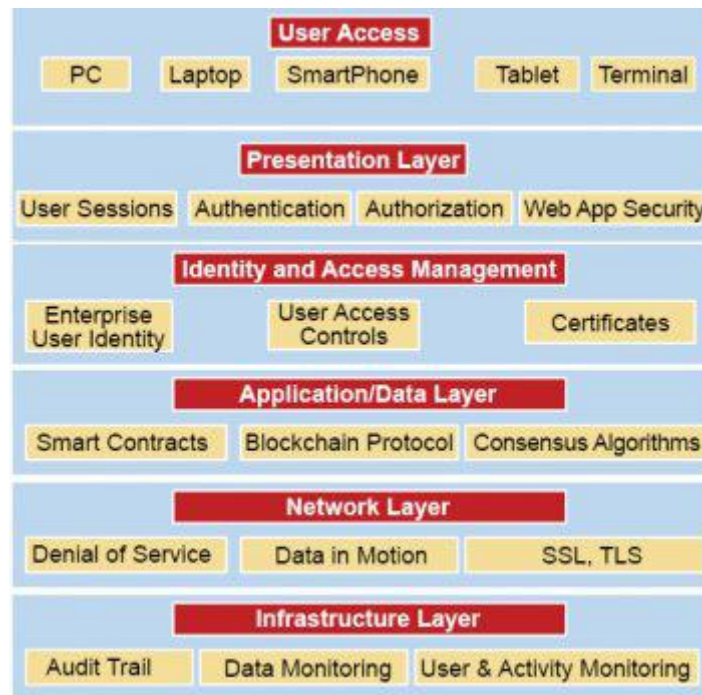


Figure 2.1. Architecture Of Blockchain

Every transaction that records and stores is not labelled as a blockchain. The following are the main characteristics of blockchain.

- **Digital:** All the information on blockchain is digitised, thus eliminating the need for manual documentation.
- **Distributed:** Blockchain distributes control among all peers in the transaction chain, creating a shared infrastructure within an enterprise system. Participants independently validate information without a centralised authority. There is no single point of failure because of how a distributed system operates. Even if one node fails, the remaining nodes continue to operate, ensuring no disruption.

- **Immutable:** All the transactions are immutable in a blockchain technology based system. Encryption is done for every transaction covering the time, date, the participants and the hash to the previous block.
- **Chronology:** Each block acts like a repository that stores information pertaining to a transaction and links to the previous block in the same transaction. These connected blocks form a chronological chain providing a trail of the underlying transaction.
- **Consensus based:** A transaction on blockchain is executed only if all the parties on the network unanimously approve it. Also, consensus based rules can be altered to suit various circumstances.
- **Digital signature:** Blockchain enables the exchange of transactional value using unique digital signatures that rely on public keys (decryption code known to everyone on the network). Private keys are codes known only to the owner to create proof of ownership. This is very critical in avoiding fraud in record management.
- **Consistent:** Blockchain data is complete, consistent, timely, accurate, and widely available.
- **Persistence:** Blockchain will not create/persist invalid transactions as determined by consensus. It is nearly impossible to delete or roll back transactions once they are included in the blockchain. Cryptographically, the blocks created are sealed in the chain. It is impossible to delete, edit or copy already created blocks and put them on the network. This leads to the creation of digital assets and ensures a high level of robustness and trust.
- **Anonymity:** Each user can interact with the blockchain with a generated address, which does not reveal the real identity of the user. Blockchain helps in recording transactions of any digital assets exchanged between two unknown parties. Security aspects supported by blockchain are critical in ensuring transparency, confidentiality and protection against fraud. The following are the high-level security features of the blockchain.

- **Ledger:** The ledger records every transaction in the blockchain. The ledger is a chain of blocks and information in the block is immutable. The distribution of the ledger is done to all the nodes.
- **Chain of blocks:** Blockchain is a chain of blocks. Each block has the hash value of the previous block and this forms a chain. Correction to data in a block (say, n) will change the hash value and will not validate with the hash stored in the next block ($n+1$). This will be a chain reaction and affect the overall chain. Therefore, this characteristic increases the protection of sensitive data or information.
- **Confidentiality:** Blockchain provides confidentiality by enabling users of a ledger to see authorised transactions only.
- **Transparency:** Blockchain allows the transactions and the ledger state to be maintained and be managed transparently by sharing the ledger to all nodes and using consensus algorithms to reach consensus among all nodes. Consensus algorithms also ensure the ordering and execution of the transactions.
- **Cryptology:** This enables secure transactions and makes blockchain immutable using hash based algorithms, which produce a fixed hash, based on the content of the block.
- **Smart contracts:** A smart contract is a computer code running on top of a blockchain containing a set of rules, on the basis of which the parties agree to interact with each other. If the pre-defined rules are fulfilled, then the agreement is automatically executed. No contract will execute without the network consensus.

Security reference architecture in the blockchain

Blockchain security ensures that the right people, internal or external, get access to the appropriate data and information at the right time and place, within the right channel. Security prevents and safeguards against malicious attacks; it protects enterprise data assets by securing and encrypting data while it is in motion or at rest. It also enables organizations to separate roles and responsibilities, protecting sensitive data without compromising privileged user access.

The security at various layers for an enterprise application is classified as:

1. User access layer security
2. Presentation layer security
3. Identity and access management layer security
4. Application/data layer security
5. Network layer security
6. Infrastructure layer security

Figure 2.1 gives a layered view of the security approach with blockchain.

User access layer: Various stakeholders, both internal and external, are part of this layer. They are the primary users of the systems. Stakeholders use channels to interact with the enterprise. They engage with various departments or business units of the enterprise over multiple channels, both physical and digital.

Presentation layer: The front-end application security should ensure the following. Authentication: Authentication is the assertion by a subscriber to prove his/her identity. The authenticators and factors are:

1. Something that one has to show (access card)
2. Something one knows (password) and
3. Something one is (biometric).

Authentication mechanisms should be commensurate with the strength of the identity model, the level of access and the sensitivity of the transaction. They must implement a

combination of multiple authenticators (aka multi-factor authentication).
Authorisation: Authorisation is a process to establish the right to perform transactions (actions), and claim access to assets and resources by a subscriber. In a blockchain application, the authorisation model should link the identity model and the authentication model. A good practice is to develop a multi-dimensional matrix of the account associated with identity, authentication and authorisation. This type of authorisation model will leave room to evolve into attribute based access control and role-based access control at the application level and, ultimately, at the organisational level, for enterprise blockchain applications. The authorisation model will typically address concepts such as separation of duties (SoD).

Web application security: Web application security should include protection against vulnerabilities identified in OWASP Top 20.

Identity and access management layer: A digital identity is a unique representation of a person or thing engaged in a digital transaction. Identity proofing, or enrolment, is the physical or digital process of verifying a subject's association with his/her real-world identity. An identity model and its associated identity proofing should provide reasonable assurance for the identity claimed by the subject. When the trust attributes of the blockchain application range from public to private, it is good practice to have multiple assurance levels for identity-proofing.

Application/data layer: The application security layer should ensure the following: Smart contracts and the blockchain processing platform are vetted to prevent things like calls to the unknown, valueless send, exception disorders, type casts, re-entrants, keeping secrets, immutable bugs, value (ether) lost in transfer and stack size limits. Blockchain protocols are vetted to prevent the blockchain from not converging as expected or into an unpredictable state, safeguarding the seed (genesis) block and ensuring timestamps are adequately protected.

Consensus algorithms that enable transparency by imposing a transaction order to be correct for a new block added to the blockchain. This ensures that all the nodes in the network are in agreement on the new transactions added to the block.

Network layer: Depending on the nature of the application and the type of the network (Internet-based, leased lines, virtual private network, etc), there should be appropriate controls extracted from the system. Controls related to boundary protection (data-in-motion) and DoS should be considered.

Infrastructure layer: Audit trail is for all the transactions that will be maintained by the blockchain. Transactions ordering and approval will be done by the consensus service on board. This ensures that the transactions are correct and transparent to other participants/nodes in the network.

Data protection: Data protection is the process of safeguarding important information or data from corruption, compromise or loss. As blockchain is immutable, data cannot be compromised and appropriate measures like redundancy can be taken to protect it from corruption and loss.

User and activity monitoring: All valid transactions performed by users can be tracked on blockchain. User onboarding and management will be done by membership service shipped along with the blockchain.

2.3. TYPES OF BLOCKCHAIN

Blockchains are classified as public, private or hybrid depending on the nature of the application. Public and private blockchains share many similarities as well as differences in their functionality.

2.3.1 Public Blockchain

A public blockchain does not have restrictions. Anyone with an internet connection can get access to the network and start validating blocks and sending transactions. Typically, such networks tend to offer some kind of incentive for users who validates the blocks.

Anyhow, this network tends to use Proof of Work or Proof of Stake consensus algorithms for validating the transactions.

It is a “Public” network in a true sense. In public blockchain architecture, you can download the protocol anytime, and you will not need any permission from anyone. The public blockchains portray the ideal model that makes the technology industry so lucrative.

Thus, it's completely decentralized, no single organization controls the ecosystem. Whereas a private blockchain can be changed and altered by the owning organization. A public blockchain surpassed the necessity of a third party. The system has a natural flow of its own – just like a flowing river. No one controls the flow path, yet everyone uses it. So, how can we define it easily? A self-governed, purely decentralized and autonomous digital public ledger. It's like that definition of democracy – of the people, by the people and for the people!

There are certain characteristics of public blockchain architecture.

1. Every node has access to read and write on the ledger
2. Anyone can download and add nodes to the system
3. The technology is fully decentralized in nature
4. It offers anonymity, which means no one can track your transactions back to you
5. It's a bit slower compared to the private blockchain

Public blockchains have a commonly shared consensus among the users of the network. If someone asks – why is the public network better? The first answer will be transparency.

The very reason the blockchains are considered the new monetizing system is it's transparent, and no has control over anything.

It was a big step up from central and federal banks who had been controlling the nature of how to transact. Also, you have to pay various charges whenever you want to send money to someone in the traditional method.

Moreover, all the histories of the transactions are kept hidden, away from the public eyes. Satoshi showed the world that our traditional system grew too old for the information age. When the common digital ledger is shared with the mass crowd, everyone can keep track of it. This results in more transparency and need of a third party validating the transactions.

2.3.2 Private Blockchain

A private blockchain is a type of blockchain network where only a single authority or organization has control over the network. It seems like it doesn't directly resonate with the main concept of blockchain now, does it? Well, even though private blockchain examples may seem like a centralized network, in reality, it can offer partial decentralization.

Also, in a network like this, you can't get an entry without any reason. In reality, this type of network is far suited as the internal technology for an enterprise. Why? Well, because as everything is dependent on technology nowadays, the previous ones simply can't keep up with the changing times. As a result, there are a lot of issues such as data theft, identity hack, and so on. Therefore, to safeguard a company's sensitive information, using private blockchains is the perfect option. So, without proper authentication, no one can enter this type of network. To make sure that any company can use blockchain, there are many blockchain companies that are working towards bringing a private version just for the sake of secrecy.

For example, Ethereum used to be a solely public platform. But now EEA is bringing Ethereum private blockchain with the same features and additional privacy for these high-end companies. There are some controversies regarding private blockchains. For example, many people think that using this tech doesn't mean you are using the core blockchain values. Well, that may be true, but the platform does come with all the features except it's only private. But for enterprise companies, a public blockchain isn't that suitable as there is much sensitive information that can get leaked. And so, private blockchains are extremely popular among high-end companies.

Best Features of Private Blockchain?

➤ Full Privacy

In reality, private blockchain platforms focus mainly on privacy instead of full disclosures. So, if you are interested in a technology where privacy is the greatest concern, then private blockchains are surely for you. On the other hand, an enterprise needs security and privacy because they always deal with cyber-attacks. Also, as they are dealing with sensitive information all the time, it makes it difficult to keep everything at bay. Thus, if a

company can use a private blockchain to tighten up its security facilities, then it'll be impossible for any hacker to hack into the system.

➤ **High Efficiency**

This type of blockchain platform offers the highest level of efficiency. In reality, private blockchain examples can show you that they work much better than traditional public blockchain platforms. But why? Well, it's because in private, only a handful of pre-authorized nodes gets an entry. So, there is no way the nodes can take up more resources than usual. But in a public blockchain, there are no limits to the number of nodes. As a result, the system slows down drastically when there are too many participants. But the private network is immune to that issue.

➤ **Scalability**

Actually, private platforms are more stable, and you will get the best performance out of it. The same goes for scalability. For a business to work efficiently, it should be scalable. So, with time it has to grow as well. But in a public blockchain, when the network starts to grow after a certain time, it starts to slow down as well. This is called a scalability issue. But private networks seem to be past this issue as it can grow but not slow down in any case. More so, this results in reduced fees, faster transactions, and so on.

➤ **Robust Architecture**

In reality, private networks have one of the robust network structures at the moment. They are made to be resilient to any issues. That's why they come with a good level of security protocols that helps to keep malicious activities at bay. In some of the platforms, you may even see firewall type feature that protects all the information within the ledger from outside and insider presence. I guess technically, an organization may alter transaction if they want to, but that is highly unlikely and will not go unnoticed.

Why Private Blockchain?

➤ Saves Resources

If you look at private blockchain examples, you will see that these platforms are saving a lot of resources. In reality, maintaining a private system is fairly simple and doesn't need that much attention. Thus, they take up only a handful of resources from public blockchain platforms. So, you get to save a lot of money and manpower that needs for these solutions. However, it doesn't mean that it will be entirely cheap or something. But comparing to other efficient technologies like this, it's the cheapest!

➤ Low Fee

In this network, you can transact with the minimum fees. Most of the time, you may not even need a fee, to begin with. In reality, this is completely a great reason to start with private blockchains. Also, these blockchains, in many cases, don't have a native token for the network. Thus, any kind of negative impact that the cryptocurrencies may bring won't be here.

➤ Regulations

Another good reason to use this network is the regulations. All the private blockchain examples in the real-world revolve around regulations. Actually, enterprise companies can't work without a regulatory system. And so, there should a proper way to perform certain tasks, and not following the rules will result in consequences. Thus, it assures more security for the participants.

➤ No Illegal Activity

The best part about private blockchain is that it doesn't have any possibility of allowing criminal activities. The issue is Bitcoin is a popular platform, but it's also responsible for any illegal activities. Thus, it has a bad reputation. But private blockchains are very selective. As a result, the only authorized person can enter the platform, which limits criminals.

CHAPTER 3

CONCLUSION

Blockchain has shown its potential for transforming traditional industries with its key characteristics — decentralisation, persistence, anonymity and auditability. Blockchain based enterprise applications increase the effectiveness of an enterprise, reduce cost of transactions and speed up interactions between the enterprises and its customers. Blockchain provides better security during transactions of any value. It is a unique and a universal technology that helps to streamline and automate nearly all customer services or legal contracts, while increasing the transparency and effectiveness of enterprises. However, a lot of exploration is needed today in domains applying blockchain technology across various business units — on how to minimise enterprise costs, improve security in an era of cyber uncertainty and enhance customer delivery. We are proposing this system to secure the FIR system. We are trying to make the system simple and efficient. The decentralized network which we are building does not rely on any trust. The registered user can file a complaint through any device which is connect with an internet. The blockchain will make the network more secure, immutable and decentralized, we can say that it will be a corruption free network.

3.2. FUTURE SCOPE

- Use of data analytics to visualize percentage of crime and number of FIR launched from a particular area/town so that more police personal can be assigned to the town for it's betterment.
- Use of text recognition to detect fraud FIR's (Incase more than 2-3 fraud FIR's are detected from a user's account, his/her account will be permanently banned).
- Routing of FIR's based on type of case and it's priority (Simultaneously more than one police station can get involved in a case based on it's priority)

- Making the platform more user friendly and convenient by developing android app, integrating the system with Google assistant or amazon Alexa.

3.3. CONTRIBUTION

The project consists of mainly two components. One the development of web interface integrated with the chatbot and the other, developing the file system using the IPFS so as to store the FIRs securely using the CIDs generated.

The backend of the web interface is developed by Tirlochan using NodeJs and the frontend part has been integrated by Guru. The development of Chatbot using dialogflow has been done by Ashutosh Rath which is further integrated to the web interface by Tirlochan so as to provide the user a friendly real interface for filing the FIR. The second component of storing the FIRs using IPFS system and generating the CID of each FIR in a secure and distributed environment is a collaborative effort of Guru and Chiranjibi. The documentation work of the project has been carried out by Chiranjibi which forms a base for the project.

3.4. REFERENCES

- [1] <https://www.researchgate.net/>
- [2] <https://ethereum.org/en/developers/docs/>
- [3] <https://docs.ipfs.io/>.
- [4] <https://medium.com/coinmonks/a-hands-on-introduction-to-ipfs-ee65b594937>
- [5] <https://medium.com/mycrypto/the-ethereum-virtual-machine-how-does-it-work-9abac2b7c9e>



Department of Computer Science and Engineering
Silicon Institute of Technology,
Silicon Hills, Bhubaneswar –751024,
Odisha, India