ICEAIST-25
M.A.M. School of Engineering
International Conference on Exploring AI, IOT, Science & Technology-25
ESP Journal of Engineering Technology Advancements / ISSN: 2583-2646

Original article

Blockchain-Based Online C rime Complaints System

Prof.U.Ranjani [1],Kabilan Inambu [2], Mugesh R [3],Panneerselvam K [4],Vaseeharan V [5,]

[1] *Professor,Department Of Computer Science & Engineering,M.A.M School Of Engineering,Tamilnadu,India,*

[2,3,4,5] *Ug Scholar,M.A.M School Of Engineering, Tiruchirappalli,Tamilnadu,India*

Abstract: *Many professions, including law enforcement, are looking into blockchain technology because there is a growing demand for public services to have digital infrastructure that is safe, clear, and can't be changed. Internet crime reporting systems that have been around for a while include issues such data tampering, lack of openness, limited traceability, and public distrust. This paper suggests a blockchain-based online crime reporting system that employs decentralized ledger technology to ensure sure the procedure is secure, immutable, and easy to follow. The system uses smart contracts to automatically organize complaints and change their status. It also protects users' information by encrypting it and limiting who can see it. A layered architecture that employs IPFS to store files, smart contracts to automate workflows, and identity verification makes sure that crime complaints are safely recorded and processed in a fashion that is easy to see. The suggested model provides people more power, makes the police more responsible, and gives digital policing a structure that can evolve. This page discusses about the idea behind the system, how it will be put into action, how it will be used in the real world, and any problems that might come up with it. It finishes with a vision for how things can get better in the future, including introducing AI and working together across borders.*

Keywords: *Blockchain, reporting crimes, decentralized systems, law enforcement, smart contracts, public safety, transparency, data integrity, digital justice, handling complaints, cybersecurity, IPFS, an unchangeable ledger, online crime complaints, digital policing, e-governance, privacy protection, records that can't be changed, citizen empowerment, and legal technology*

I. INTRODUCTION

Reporting crimes is an important aspect of any justice system because it allows the police act fast and keep people safe. In the last several years, governments around the world have been adopting internet platforms to make it easier and faster to report crimes. But this vital process's digital transformation hasn't come without its own issues. Most of the time, traditional internet methods for filing criminal complaints employ centralized databases that are managed by some government agencies. These technologies might be useful, but they come with a lot of hazards, like data manipulation, unauthorized access, selective editing, server outages, insider threats, and delays imposed by red tape. The organizations that are designed to protect the peace may modify complaint records on intentionally or by accident. This can make people less likely to want to get involved, make the system less obvious, and make people lose faith in it.

Also, persons who are victims of sensitive crimes like sexual harassment, cyberstalking, financial fraud, domestic abuse, or human rights violations often don't want to file complaints because they are frightened of getting injured, don't want to be embarrassed, or don't trust the police. People in many poor countries may assume that their complaints won't be taken seriously or, worse, that they will be modified or wiped totally because corruption is rampant or the law isn't always followed. Not only does this make it difficult to seek justice, but it also allows criminals get away with their crimes, which affects social order and people's trust in the police.

Blockchain technology offers a fresh and powerful way to fix problems that have been there for a long time. Blockchain was first intended to be the basic technology behind cryptocurrencies like Bitcoin. Since then, it has expanded into a bigger framework that people are looking into using in a lot of different domains, such banking, supply chain management, voting, healthcare, and more recently, delivering public services. A blockchain is a decentralized and distributed ledger that maintains track of transactions, or in this example, complaint entries, in a succession of blocks that are cryptographically linked to each other. The contents of the transaction, a timestamp, and a cryptographic hash of the block before it are included in each block. Once something is uploaded to a blockchain, it is very hard to edit or remove it. This is because you would have to change every block that comes after it and get most nodes in the network to agree.

Blockchain could be a good way to keep internet crime reports safe because it can't be changed, is open, and is spread around. When complaints are saved on a blockchain network, it is practically impossible for anyone, whether police officers, IT administrators, or hackers, to change the data. There is a time stamp on each entry, and all the nodes in the network can check it. This makes sure that everything is clear and accountable. There are also no single points of failure on the blockchain, which makes the network stronger.

Smart contracts are programs that run on their own and are stored on the blockchain. You can use them to automate critical aspects of the complaint process. For instance, if someone complains, a smart contract may immediately send it to the proper police department, let the right individuals know, and maintain track of the complaint's status while the inquiry is going on. These automated processes make things operate more smoothly by cutting down on the need for individuals to get involved, lowering the likelihood of delays or bias, and making things function more smoothly.

You can secure users' privacy with data encryption and permissioned access control systems, especially when the information is sensitive. Each user may be given a private key so they can check on the status of their complaint and see their records. Only authorized officials or legal organizations can see or amend complaint data through a controlled interface. The InterPlanetary File System (IPFS) can also be used to organize and store multimedia evidence including images, videos, and documents. IPFS is a way to store files that isn't centralized and just keeps the hash of the file on-chain. This protects the data while still letting it flourish. It is better than putting these enormous files directly on the blockchain, which can be slow.

This kind of system can also help people file complaints without using their true names, which is good for whistleblowers and other persons who are at risk. It can also enable journalists, researchers, government agencies, and NGOs real-time dashboards and analytics to see how crime is happening, how resources are being used, and how many cases are still active. This can help people make better choices based on facts and come up with better ways to stop crime.

In short, an online crime complaints system based on blockchain is a citizen-centered, clear, and immutable option to old centralized platforms that have flaws built in. It protects information, promotes public trust, speeds up the handling of cases, and makes institutions more responsible. Adding blockchain to crime reporting systems is a brave but crucial step forward as governments around the world try to make their digital systems and governance better. This research paper talks a lot about the architecture, design approach, implementation tools, benefits, difficulties, and prospective future enhancements of this kind of system. With this research, we want to highlight how new technologies like blockchain can revolutionize the way digital justice is served in the 21st century.

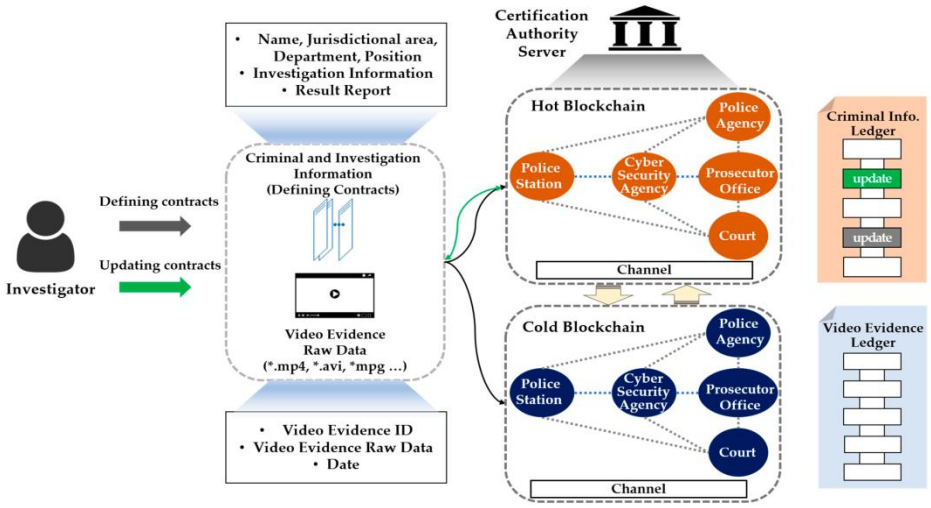

Figure 1.Blockchain-Based Online Crime Complaint Systems

II. BACKGROUND AND MOTIVATION

It is a basic right to be able to report a crime, and it is also an integral aspect of a functioning legal system. Sadly, in many parts of the world, it is still hard, ambiguous, and intimidating to file a complaint. Digital governance has come a long way, but most of the ways that victims can report crimes are still done by hand, on paper, or are only partially digital. Some places have web portals, but they are hard to use, don't work effectively with backend systems, and don't have obvious ways to follow up or be open about what they do. Because of this, the folks who these services are meant to benefit don't often use them.

One of the main difficulties with the present complaint systems is that people don't trust them. People who have been wounded often don't want to report crimes, especially those that entail violence against women, corruption, human trafficking, cybercrimes, and political abuse. A lot of people are scared that those in charge will ignore, mishandle, or actively suppress complaints. persons who complain may even be punished, harassed, or left out of social circles for seeking to hold strong persons or groups responsible in other situations. This worry is made worse by the fact that in centralized systems, one group, such a local police station, a regional headquarters, or a government agency, normally has control over the data. This makes it simple to update or erase the data without leaving any evidence.

Corruption makes the problem more worse. There are records of complaints being modified, deleted, or not written down at all in the first place. When people complain against powerful people, their problems often go away or are reported as "resolved" without a proper investigation. In rural or disadvantaged areas, not having access to technology or not having enough resources makes the problem worse, making it much difficult and less reliable to report crimes. From a systemic point of view, this leads to underreporting, a lack of accountability, a loss of public trust in law enforcement, and the continuance of injustice.

Because of these issues, it is vitally important to set up processes that can make sure that criminal complaint procedures are fair, open, and accountable. Blockchain technology is the answer that will revolutionize the world. At its core, blockchain is a distributed ledger system. This means that instead of just one central server, data is stored on numerous nodes. You can't change or delete a record once it's been written unless everyone on the network agrees. This immutability is true because of cryptographic hashing and a chain-based structure, where each block is connected to the one before it.

Using this technology for criminal complaints makes sure that once a complaint is made, it is placed on a ledger that is easy to read and can't be modified. No one can change or take it down without getting caught, not even the police. This affords us a level of accountability and data integrity that has never been seen before. Also, because blockchain is decentralized, a lot of different entities, like the police, the courts, human rights groups, and even regular people, can see complaint data based on their roles and permissions. This protects the system from going too far.

Another important factor is that the folks who are protesting can stay anonymous and safe. People can file complaints on a blockchain-based website without using their real name or using a fake name. Depending on the law, only certain people may know who they are, or their identity may stay a secret. This allows victims and whistleblowers the strength to speak up without fear, even when doing so could get them in trouble with the law or with society.

ou can also use blockchain to keep track of and see what's going on during the follow-up. Every action taken to handle a complaint—assigning it, looking into it, closing it—can be recorded on-chain as a new transaction, making a case history that can't be modified. This enables consumers see how their concerns are being addressed right away and gives higher-ups or oversight groups a method to make sure that due process is being followed.

Lastly, the main argument for making an online crime complaints system based on blockchain is because the current systems are inefficient, corrupt, and don't have enough confidence. It is possible to make a crime reporting system that is citizen-centered, strong, and trustworthy by using the major benefits of blockchain, such as its ability to be unchangeable, clear, decentralized, and secure. This kind of system would not only make the rule of law stronger, but it would also motivate individuals to get involved in their communities, reform institutions, and employ technology to make justice more fair.

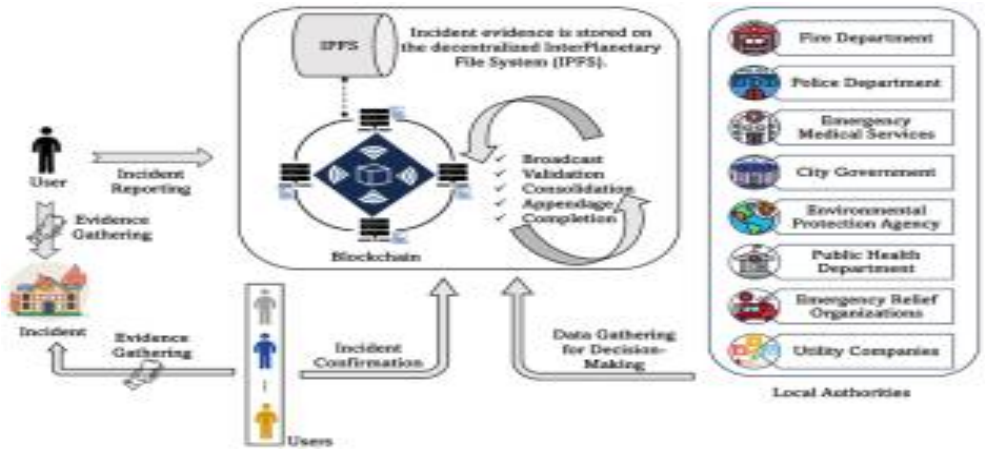

Figure 2. Context & Motivation

III. OVERVIEW OF BLOCKCHAIN TECHNOLOGY

In several fields, blockchain technology is transforming how data is stored, reviewed, and shared. It gives us new possibilities to make digital infrastructure that is safe and open. Blockchain is a decentralized ledger technology that allows computers to store data across a network of nodes. In a peer-to-peer (P2P) network, each node stores a copy of the complete ledger that is always up to date. This is not like most centralized databases, which are run by one person or group. This decentralized structure makes sure that there is no one point of failure, which makes the system more stable and trustworthy.

A block is the part of a blockchain ledger that holds each entry. These blocks are connected together by cryptographic hashes so that they form a continuous and immutable sequence. Each block has a list of transactions or data entries, a timestamp, and the cryptographic hash of the block that came before it. This hash not only makes sure that the data is valid, but it also makes it unique. When someone alters a block, the hash of that block changes, which makes all the blocks that come after it useless. This feature makes it almost impossible to update the blockchain and shows that it has been tampered with. In most cases, altering just one record would mean changing all of the blocks on most of the nodes in the network. This is not practical in practice or with the computational power available.

Blockchain systems use consensus methods to make sure that everything is the same and to stop fraudulent entries. These are rules that make sure that all the nodes in the network agree on how the blockchain should look. Proof of Work (PoW) and Proof of Stake (PoS) are two of the most common approaches to come to an agreement. In Proof of Work (PoW), nodes (miners) use a lot of processing power to solve complex math problems that generate new blocks and confirm transactions. On the other side, PoS picks validators based on how much cryptocurrency they have and are willing to "stake" as collateral. You can use any way depending on what the system needs, including security, energy efficiency, or transaction speed.

A lot of new blockchain apps use smart contracts. When specific conditions are met, smart contracts are programs that run on the blockchain and do certain things automatically. Smart contracts can take care of critical functions in an online criminal complaint system, such as validating that a complaint was filed, forwarding it to the relevant departments, updating its status, and letting people who need to know know. These automated systems make things work more smoothly by cutting down on the need for individuals to get involved, cutting down on bias or delays, and making things function more smoothly.

Another important feature about blockchain is that it is open. Anyone who utilizes a public blockchain may examine the history of transactions. This makes it easy to hold people accountable and check their work. In private or permissioned blockchains, access might be limited based on roles. This helps apps that need to be private, safe, and open at the same time, like crime reporting, find a way to do all three.

Blockchain is a perfect platform for systems that need to manage data in a secure, traceable, and tamper-proof fashion since it is decentralized, immutable, consensus-based, automated through smart contracts, and open. These features can make sure that complaints are collected, saved, and processed in a fashion that can't be changed, can be traced via an audit trail, and is open to authorized users for the purpose of reporting crimes. Blockchain is the technology that makes up the backbone of a new criminal reporting system that is more reliable, faster, and focused on what citizens need.

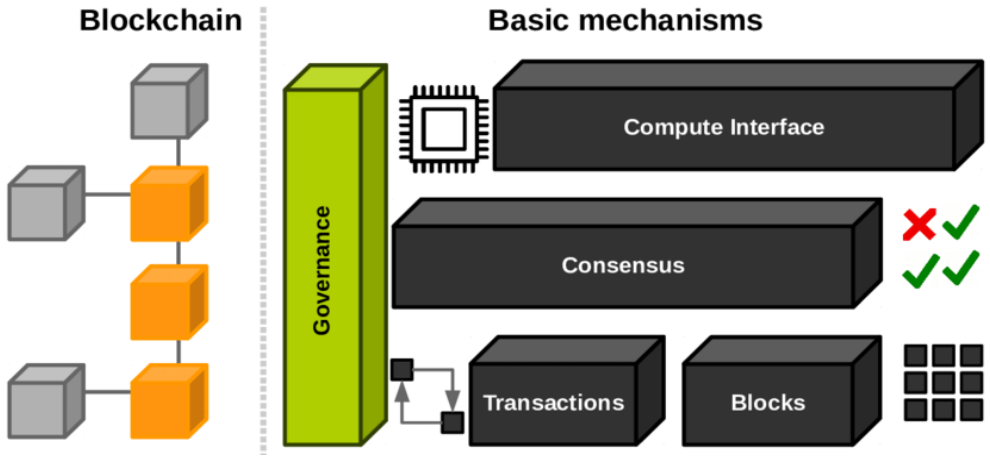

Figure 3..Four-Layered Framework

IV. SYSTEM ARCHITECTURE AND DESIGN

It is important to carefully plan the design of a solid blockchain-based online criminal complaint system so that it is safe, scalable, easy to use, and open. Most of the time, the system has a lot of layers that are all connected and each one has a separate job. There is the User Interface Layer, the Application Logic Layer, the Blockchain Layer, the Evidence Storage Layer, and the Law Enforcement Dashboard. They work together to create a safe, citizen-focused digital platform that can rapidly and reliably manage sensitive crime-related data.

A. User Interface Layer

The User Interface (UI) layer is what people can see and utilize on the system. This layer needs to be simple to use and accessible through public kiosks, smartphone apps, and online browsers. In India, people can sign up or log in with digital IDs like Aadhaar, fingerprints, or two-factor authentication. People who are frightened of retaliation or disgrace should be able to report crimes in both identifiable and anonymous methods.

The UI should make it easy for users to file a complaint. People who have been hurt can give details about the crime, upload evidence including photos, videos, and documents, choose the sort of crime, and say where it happened. The complaint is sent to the application logic layer for processing, and a time stamp is made automatically. The interface should support a lot of languages and have features like voice-to-text for individuals who are blind or don't know how to use computers so that everyone can use it.

B. Application Logic Layer

The brain of the system is the application logic layer. It checks to see if the input is genuine, organizes complaints, and chooses where to deliver them. This layer makes sure that all the required fields are filled out, that the attachments are the proper size and type, and that there are no duplicate reports in the system. It also features AI modules that help categorize complaints into groups depending on how serious they are, how urgent they are, and the keywords they use.

Once the complaint has been checked out and found to be valid, it is forwarded to the smart contract engine. There, pre-written code looks at the crime and transmits it right away to the right jurisdiction or law enforcement organization. In particularly serious cases, including threats to life or terrorism, a high-priority flag can be raised and things could get worse right away.

C. Blockchain Layer

The blockchain layer is the most important part of the system. It retains a record of every complaint that can't be changed. Once the complaint has been checked out and put into a category, a cryptographic hash of the data is created and stored on the blockchain. This hash is like a digital fingerprint that makes sure that no one can edit or delete the complaint's contents without being noticed.

There is a date, a complaint hash, and links to the block before it in each block. This makes a chain that can't be broken. All of the nodes in the blockchain network, such as police agencies, legal institutions, and oversight bodies, have copies of the ledger that are all the same. This decentralization keeps the data safe even if one node gets hacked. Hyperledger Fabric and Quorum are two examples of public permissioned blockchains that are suitable for these kinds of apps because they let users in but are still open.

D. Evidence Storage Layer (IPFS Integration)

The InterPlanetary File System (IPFS) is used by the system to store large files like movies, pictures, and documents because on-chain data storage has some constraints. When a user submits proof, the file is first saved on the IPFS network. Then, a unique hash of the file is made. The blockchain then keeps this hash and the complaint's metadata in a safe place. This method maintains files safe and real because any alteration to the original file would change the hash.

You can also encrypt files with this layer, which means that only persons who are allowed to can see and access sensitive information. Smart contracts can set up a role-based access control mechanism that allows you regulate who can use decryption keys.

E. Law Enforcement Dashboard

Police officers, detectives, and other government workers who are allowed to do so can use a particular dashboard to deal with, keep an eye on, and respond to complaints. This interface offers real-time updates on new cases, reports that have been marked, and investigations that have been assigned. Officers can write notes, modify statuses (like "Under Review," "In Investigation," or "Closed"), upload files, and give other officers tasks. It is impossible to modify any of these activities because they are all time-stamped and documented on the blockchain.

The dashboard also has a lot of analytics capabilities, such as heatmaps that show where crimes happen most often, counts of open cases, and measures of how quickly people respond. Audit logs reveal exactly who viewed or altered any part of a complaint, which makes sure that everyone is responsible and honest.

F. Security and Access Control Mechanisms

There is security embedded into all layers. To keep user data safe while it is kept and transferred, we use standard encryption methods like AES-256 and RSA. Role-based access controls make sure that users can only see information that is

relevant to their professions. For example, a public prosecutor might be able to examine evidence files and the progress of an investigation, but a community officer might only be able to see statistics that have been made anonymous.

Smart contracts also automatically set rules on who can see what. If someone tries to break the rules of security, alarms go out and the action may be marked as suspect for further investigation.

V. COMPLAINT FILING PROCESS

The way to file a complaint in a blockchain-based crime complaint system should be safe, simple, and easy to understand. It overcomes the shortcomings with current systems by using blockchain's ability to keep records that can't be modified, smart contract automation, and digital identity verification. This process gives citizens the power to safely report crimes, makes sure that complaints are handled correctly, and keeps a record of what the authorities do that can't be modified.

The first step in the process is to check the user's identity and confirm that they are who they say they are. This is very crucial to keep spammers and other unscrupulous people from taking advantage of the system. Users can log in with biometric verification, secure login credentials, or digital identities that the government gives them, like Aadhaar in India. But the system also lets people report crimes anonymously or under a fake name if they feel threatened or don't want to be known, particularly in cases of domestic abuse, sexual assault, or political corruption. National laws and standards around privacy make these methods possible.

Users are guided through a structured complaint form after their identity has been verified. This form lets them say what happened, where it happened, when it happened, and who was involved. They can even show proof to back up their allegation. You can use pictures, videos, papers, and audio recordings as proof. These files are safely uploaded and stored in a distributed storage system like IPFS. The blockchain just retains a hashed reference of each file so that it can't be modified and so that the blockchain doesn't get too massive.

After that, the user has to choose a type of offense from a list that includes theft, harassment, cybercrime, violence, fraud, or those who are missing. The input data starts the smart contracts, which automatically sorts the complaint and gives it an initial status, such as "Pending Review." These smart contracts follow rules that have been set up in the system, and they can move the case up to "High Priority" if it involves serious crimes or threats to life.

After that, the person who complained gets a special tracking ID. With this ID, the user may check how their complaint is progressing in real time, so they don't have to go to the police station over and over again to get updates. The system automatically sends alerts to the proper police departments or personnel, making sure that the issue is handled straight away. Assigned officers get alerts and can respond from their own secure dashboard.

Every change or action that happens during the complaint is logged on the blockchain as a new transaction. For example, the assignment of an officer, the review of evidence, updates on the status of an investigation, and court hearing dates are all documented with a time stamp that can't be modified. This makes it easy to maintain track of everything that happens with a complaint, preventing records from being changed or destroyed, and makes sure that no part of the complaint process can be hidden or faked.

Victims can also check their case history at any moment by logging in with their tracking ID or login information. This makes everything apparent. Dashboards can show researchers and the public statistics about complaints without giving away who made them. These numbers can show crime trends by area, type, and response time while keeping users' identities secure.

In the end, the act of making a complaint is a simple, secure, and open way to get people to trust crime reporting again. It connects people to the legal system through automation and the security of blockchain, which makes the procedure both fast and responsible.

VI. SECURITY AND PRIVACY CONSIDERATIONS

Any system that handles sensitive crime-related information must follow tight rules for privacy and security. A crime complaint platform based on blockchain needs to be properly thought out to protect the identities of victims, make sure that data is transferred safely, and limit access to sensitive case data to only those who need it. Blockchain includes built-in features like decentralization, encryption, and transparency that help meet these needs.

One of the key ways the system keeps itself safe is by using Public-Key Infrastructure (PKI) for end-to-end encryption. When a complaint is sent, it is encrypted using the public key of the authority in control, which might be the police department. Only persons with the right private key can read and see the information. This keeps the information private and protected from others who shouldn't be able to see it, even on the network.

Zero-knowledge proofs (ZKPs) are another way to improve privacy. ZKPs let a user prove that a complaint or data entry exists without giving away any real information. This is very useful when people need to show that they filed a legal complaint without giving up any confidential information about the case, like in whistleblower instances.

Permissions based on position control who can see and use information. For instance, police officers, prosecutors, and court staff can only see and work with information that is important to their job. This stops people from viewing too much and helps stop misuse or overreach.

Blockchain maintains data sovereignty and makes it more resilient because it is decentralized. It's impossible to lose, modify, or remove data without permission because complaints are spread out across many nodes. Also, Distributed Denial of Service (DDoS) attacks, which are common in traditional web-based systems, are considerably less likely to happen because there isn't a central server.

The blockchain-based complaint system is incredibly safe and keeps your privacy protected since it uses cryptographic protocols, access control mechanisms, and a decentralized design. This keeps trust, privacy, and following the regulations for protecting data all in check.

VII. BENEFITS OF THE PROPOSED SYSTEM

There are several benefits to using a blockchain-based criminal complaint platform for technology, society, and institutions. The key good things are:

Records that can't be edited or deleted: The blockchain keeps each complaint forever and can't be changed or removed without permission. This makes it almost impossible to edit data, which inhibits anybody from corrupting, manipulating, or removing complaints without permission.

All actions, like filing a complaint, getting updates on an investigation, and assigning police, are recorded with a time stamp and can be seen by the public (where appropriate). This makes people and outside observers trust each other more. It's easy to examine what has transpired in a case since blockchain is open.

- **Citizen Empowerment:** People who have been hurt can safely report crimes and, if they want to, do so without providing their name. This is especially helpful for those who live in remote, rural, or disadvantaged places where it's hard to travel to a police station or where people assume the police are not nice.
- **Better accountability for police enforcement:** Once a complaint is entered into the blockchain, police enforcement can't ignore or deny it. It is simpler to hold persons or departments accountable for delays or carelessness when all activities that follow are recorded.
- **Tracking Cases and Monitoring in Real Time**: Complainants get a unique tracking ID and can observe how their case is moving online in real time. Also, police departments can keep an eye on how well their team is doing and how quickly they are making progress on investigations. This helps things run more smoothly.
- **Data-Driven Policy and Crime Analytics:** Public dashboards that exhibit anonymous complaint data help governments and analysts discover crime trends, hot spots in certain places, and patterns that repeat over and over again. This helps you make decisions based on facts and use your resources better.
- **Uptime and Resilience:** The system is particularly fault-tolerant because it is not centralized. There is no one point of failure, therefore it can handle DDoS attacks and crashes in the infrastructure.
- **Collaboration Across Borders:** Blockchain can readily link states or even countries because it has no borders. This is highly vital for fighting crimes that happen across borders, such as drug trafficking, money laundering, cyber fraud, and human trafficking.

Smart contracts take care of things like forwarding complaints to the relevant department, updating the status, and sending alerts. This helps people make fewer mistakes and the administration run more smoothly.

- **Scalability and Interoperability:** The system can be developed to incorporate other municipal services, including traffic violations or civil matters, and it can operate with existing e-Governance frameworks and digital ID systems.

VIII. USE CASE SCENARIOS

The planned blockchain-based crime complaints system is more than simply a new piece of technology; it's also a really useful tool that can be used in a lot of other parts of society. By fixing faults with traditional reporting techniques, the system can offer individuals more power, make institutions stronger, and improve how police respond to crimes in a range of settings.

Victims of domestic violence often have mental, emotional, and social problems that make it hard for them to call the police. People can safely register complaints from home or a shelter using this technology. This is preferable than coming to

a police station, where they can feel guilty or terrified. Their complaints are registered even before they feel safe enough to come forward in person because they are time-stamped, unchangeable, and kept safe.

People in rural and underserved areas usually don't register concerns since there aren't many police officers there or they don't come around very often. People who live in rural areas can report crimes through a decentralized complaint system that can be accessed by community kiosks or mobile devices. Higher-ups and district-level administrators can see these entries right away, so local officials can't ignore or block them.

Anti-Corruption and Whistleblowing: People who work for the government or a corporation are often scared to report fraud or other wrongdoings because they think they will be in trouble. They can use blockchain to send encrypted and anonymous complaints. The website keeps track of when and how the report was made, so anti-corruption groups can see how the complaints are going without revealing the whistleblower's name.

Cybercrime and Digital Harassment: Phishing, financial fraud, cyberbullying, and online harassment all use digital evidence including screenshots, emails, and chat logs. You can hash these and save them in IPFS. Then, you can post the cryptographic reference on the blockchain. This keeps the evidence safe and ensures sure it hasn't been modified, which is highly vital for it to be used in court.

Civil Society, NGOs, and Media ReportingOrganizations that work on women's rights, public safety, or media freedom can use anonymized data to look at crime trends, report faults with the system, or press for reform. Public dashboards can display how many complaints there are, what kinds they are, and how long it takes to deal with them. This makes the system of law enforcement more open.

These examples highlight how blockchain can be used to make crime reporting more accessible, safe, and accountable.

IX. TECHNICAL IMPLEMENTATION TOOLS

You require blockchain infrastructure, smart contract programming, secure storage solutions, and easy-to-use interfaces to build a crime complaints system that operates on a blockchain. You will need the following tools and technologies to build up this kind of system:

A. Blockchain Platforms

- Ethereum is an excellent platform for programs that are public and decentralized. Has a lot of developers and good smart contract functionality. Good when being honest is highly crucial.
- Hyperledger Fabric is best for business-level apps that need permission, such those used by the government. provides you more control over who may access it and has a modular structure.
- Polygon is a Layer 2 scaling solution for Ethereum that speeds up and lowers the cost of transactions. This is useful for large deployments.

B. Creating Smart Contracts

- The main language for writing smart contracts that operate with Ethereum is Solidity. You can review complaints, get updates on cases, and issue notifications with it.
- It's easy to write, compile, test, and deploy smart contracts with Remix IDE and Truffle Suite.

C. Front-End Technologies

- Two popular JavaScript frameworks for building dynamic user interfaces for reporting complaints, keeping track of cases, and dashboards are React and Angular.
- Web3.js and Ethers.js are libraries that link the front end to the blockchain network.

D. Ways to keep files safe

- IPFS (InterPlanetary File System) is a technique to store large data like films, photos, and documents that doesn't rely on a central server. The blockchain merely keeps the file hash to make sure that references can't be modified.
- Filecoin is an incentive layer on top of IPFS that is based on blockchain technology. It lets you safely rent decentralized storage space.

E. Oracles and how they work in the real world

- Chainlink helps smart contracts get information from outside sources, such time, place, and legal records. This makes them more aware of their environment and more automatic.

F. How to Stay Safe

- End-to-End Encryption: Use RSA to safely share keys and AES (Advanced Encryption Standard) to protect data that isn't being used.
- Zero-Knowledge Proofs (ZKP): You can use these to check things without giving up any private information.

G. Checking identity and authentication

- You can gain safe and personalized access with biometric authentication by using your face or fingerprint.
- Two-Factor Authentication (2FA) is a means to keep anyone from gaining into your account without your consent. It uses a password and a one-time password (OTP) delivered by email or text message.
- Use Aadhaar Integration (for India) or other national ID APIs to find out who the user is.

H.APIs and Working Together

- RESTful APIs that let you talk to police databases, judicial systems, or national cybercrime portals that are up to date.
- Support for Android and iOS mobile platforms so that more people can utilize it.

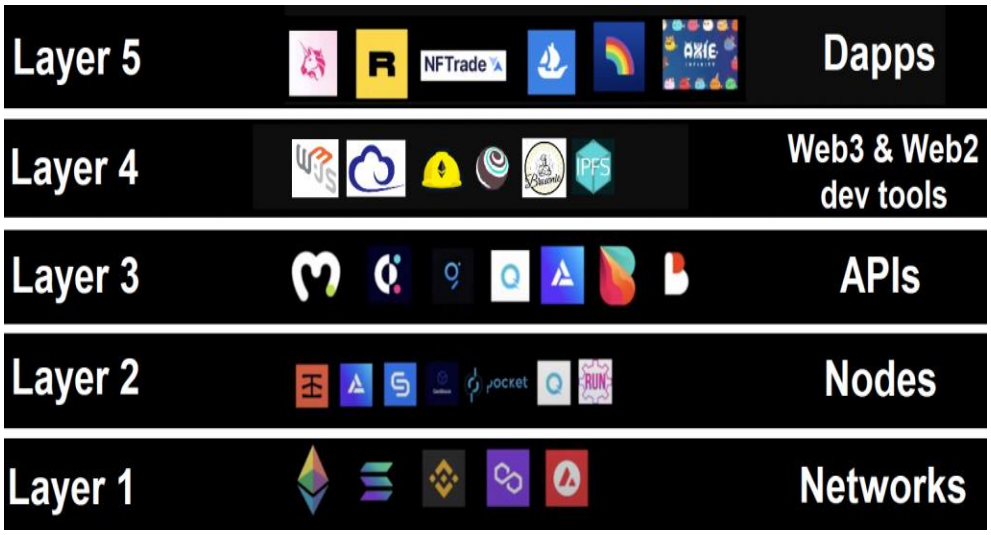

Figure 4.Application & Front-End Layer

X. CHALLENGES AND LIMITATIONS

A blockchain-based online crime complaints system could transform the way we deal with crime, but there are a lot of big challenges and limitations that need to be fixed first. Scalability is one of the most crucial things to consider about. Ethereum and other public blockchain networks are safe and decentralized, but they typically have problems with too many people using them, slow transaction processing times, and expensive gas prices. When the system has to deal with a lot of complaints, file uploads, and real-time changes from multiple areas at once, these challenges can make it run more slowly. Layer 2 solutions like Polygon and other permissioned blockchains like Hyperledger Fabric might help, but they still need to be carefully planned to make sure they can handle a lot of traffic.

Privacy is also a hard issue to deal with. The blockchain's immutability feature makes sure that once a complaint is registered, it can't be modified. But this can be a problem if the complaint is fake, fraudulent, or needs to be taken down for legal reasons. It may be against the law and against the rules to not be allowed to delete or update this kind of data. There are other standards for protecting data at the national and international levels. For example, the General Data Protection Regulation (GDPR) in Europe and the Data Protection Bill in India. These restrictions may limit how people can keep, distribute, and access personal data. Following these rules when using a decentralized and distributed system is still a huge technical and legal issue.

Another issue is that not everyone can use it, especially in regions with poor internet connections or among people who aren't extremely tech-savvy. People that have to deal with cryptographic keys, wallets, or verification methods might not feel safe utilizing blockchain-based apps. Starting out can also be very expensive. Building infrastructure, making cybersecurity better, developing blockchain technology, training police personnel, and linking to current government databases can all be quite expensive. This could make it hard for some places to afford widespread use.

It can also be problematic to work with older systems, such as police records management systems, court file databases, or forensic evidence repositories. This is because it often needs middleware layers and APIs that are made just for it. Lastly, public institutions that are used to doing things the old-fashioned manner may not want to switch to new ones. People might not like it because they are afraid of losing control, being held accountable, or not being able to see what is going on. But these difficulties can still be fixed. These issues can be addressed with on purpose through staggered rollouts, educating stakeholders, public awareness campaigns, and robust policy frameworks. This will let blockchain fulfill its full potential as a revolutionary way to report crimes.

XI. FUTURE ENHANCEMENTS

As the blockchain-based online crime complaints system gets better, there are many things that can be done to make it more useful, easier to use, and available to more people around the world. One such alternative is to use artificial intelligence (AI) to make decisions and analyze data automatically. AI systems can assist police uncover patterns that show complaints are bogus or spam, which makes their jobs easier. These algorithms can also look at old data to determine places where crime happens a lot, find organized crime, and even anticipate where crime will get worse, which helps police stay ahead of the game.

Being able to quickly connect to national identity databases (like Aadhaar in India or Social Security in the U.S.) and systems for managing court proceedings would be another huge step ahead. This kind of connection can make it possible to digitize everything from filing a complaint to going to court. This cuts down on paperwork, speeds up justice, and makes it easier to keep track of cases. Blockchain interoperability protocols like Polkadot or Cosmos could make it possible for different government platforms, like those in law enforcement, the courts, and forensics, to share verified data safely within a unified framework.

Also, machine learning might be used to sort complaints by how serious they are, how urgent they are, or how long the user has been using the service. This would assist the police make better use of their resources. It would be easier for everyone, even those who can't read or write well or have a disability, to utilize the platform if it supported several languages, mobile apps, and voice-based complaint filing.

In the end, the platform might grow to let agencies like INTERPOL operate together across borders. This would allow countries to safely and without a central authority communicate complaint data, digital evidence, and criminal records. By making blockchain a shared, unchangeable evidence storage, verifiable, real-time cooperation will help fight hacking, trafficking, and terrorism across borders more effectively.

XII. CONCLUSION

Using blockchain technology to make crime reporting systems better is a big step forward in the struggle for government that is open, responsible, and focused on what people need. Victims have had a tougher time getting justice and are less inclined to come forward since traditional procedures of filing crime complaints are often delayed, lack transparency, and are prone to corruption. These issues are particularly greater in rural, poor, or bureaucratically packed places where it can be scary, take a long time, and even be dangerous to file a complaint. A blockchain-based online crime complaints system fixes these difficulties that have been around for a long time by giving users control over their data and making sure it stays safe and immutable.

The key qualities of blockchain—being unchangeable, open, and decentralized—are quite comparable to what a good crime reporting system needs. Once a complaint is submitted, the blockchain ledger preserves a permanent record of it, making it almost hard to modify. This makes it harder for records to be modified or rejected because police, judges, and victims all have access to the same verified set of facts. Smart contracts automate the processes of sorting cases, sending out notifications, and providing evidence. This makes things run even more smoothly.

The system also makes things easier to get to and provides people more authority than ever before. People may report crimes from anywhere, see how their complaints are being handled in real time, and get updates without ever having to go to a police station. This is especially life-changing for those who have been victims of sensitive crimes like domestic abuse, workplace harassment, or cyberbullying, when privacy and anonymity are highly crucial. Public dashboards that show anonymized data and crime stats make things even more open and help with making policy choices and selecting how to spend money.

That so, there are a number of issues that need to be worked out before full-scale adoption can happen. It is vital to properly deal with legal, technological, and institutional issues such making ensuring that data protection laws are followed, dealing with scalability, retaining compatibility with previous systems, and getting past political opposition. But there are ways to fix these difficulties. Using pilot projects, training stakeholders, and making minor improvements to technology, governments can gently shift from their current systems to blockchain-enabled platforms.

In the future, the system might be a lot more helpful if it could work with AI, national ID systems, and international court networks. Future advancements, such as case prioritization based on machine learning, user interfaces that function in several languages and voices, and blockchain interoperability protocols, will make the system smarter, more inclusive, and more connected to the world.

Lastly, a blockchain-based online crime complaints system is not merely a new technology; it is something that society needs. This strategy gives us a completely different way to look about how people trust the justice system at a time

when they want more from institutions in terms of openness, responsibility, and responsiveness. Blockchain technology may assist update how crime is reported and make sure that justice is not just done, but also seen to be done. It does this by providing victims more power, making law enforcement more effective, and protecting the integrity of complaints.

XIII.REFERENCES

[1]. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.
[2]. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *IEEE International Congress on Big Data*.
[3]. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access*, 4, 2292–2303.
[4]. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation Review*, 2(6–10), 71.
[5]. Wood, G. (2014). *Ethereum: A Secure Decentralized Generalized Transaction Ledger*. Ethereum Project Yellow Paper.
[6]. Hyperledger Fabric Documentation. https://hyperledger-fabric.readthedocs.io
[7]. Buterin, V. (2014). *A Next-Generation Smart Contract and Decentralized Application Platform*. Ethereum White Paper.
[8]. Polkadot White Paper. (2020). https://polkadot.network/Polkadot-lightpaper.pdf
[9]. Cosmos Network. (2021). https://cosmos.network
[10]. Dinh, T. T. A., et al. (2018). Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering*.
[11]. Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. *IEEE Security and Privacy Workshops*.
[12]. Zeng, Y., et al. (2019). Research on blockchain technology applied in online petitions. *International Journal of Web Information Systems*, 15(2).
[13]. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems*, 107, 841–853.
[14]. Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. Penguin.
[15]. Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation*, 6(1), 45–62.
[16]. Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media.
[17]. Treiblmaier, H. (2018). The impact of blockchain on e-government: A research agenda. *Government Information Quarterly*, 35(4), 703–710.
[18]. Turkanović, M., et al. (2018). EDI-Auth: Decentralized, blockchain-based authentication system for the Internet of Things. *Future Generation Computer Systems*, 76, 475–491.
[19]. Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied Sciences*, 9(9), 1788.
[20]. Berners-Lee, T. (2020). *Solid: A Vision for Re-decentralizing the Web*. https://solidproject.org/
[21]. InterPlanetary File System (IPFS). https://ipfs.io
[22]. Filecoin Documentation. https://docs.filecoin.io/
[23]. Chainlink Documentation. https://docs.chain.link/
[24]. Bhattacharya, S. (2021). Cybercrime in India and digital evidence on blockchain. *International Journal of Cyber Forensics and Advanced Threat Investigations*.
[25]. Misra, S., & Saha, S. (2021). Blockchain technology for cybersecurity and data privacy. *Wiley Online Library*.
[26]. Tan, W. L., & Low, P. L. (2020). Applying blockchain for crime and fraud reporting in Malaysia. *International Journal of Computer Applications*, 176(31), 28–34.
[27]. Jain, A., & Goel, S. (2020). E-governance using blockchain technology. *International Journal of Computer Sciences and Engineering*, 8(10).
[28]. Rathi, A., & Sharma, N. (2022). Blockchain for governance and transparency in India. *Journal of Digital Government*.
[29]. Kshetri, N. (2017). Can blockchain strengthen the internet of things? *IT Professional*, 19(4), 68–72.
[30]. Singh, A., & Chaurasia, B. K. (2021). Blockchain-based crime reporting system: A decentralized approach. *International Journal of Engineering and Advanced Technology (IJEAT)*, 11(2), 81–87.
[31]. Kumar, P., & Yadav, P. (2021). Digital trust in law enforcement: Blockchain-based approach. *Journal of Digital Crime and Policing*, 2(1).
[32]. O'Leary, D. E. (2019). Models of auditing in blockchain environments. *Journal of Emerging Technologies in Accounting*, 16(1), 29–41.
[33]. Jain, R., & Sharma, R. (2022). Role of blockchain in smart governance: An Indian perspective. *Asian Journal of Research in Social Sciences and Humanities*, 12(2).
[34]. Chaudhary, M., & Sharma, S. (2023). Blockchain-based identity verification for crime investigation. *Journal of Information Security Research*, 14(1).
[35]. United Nations Office on Drugs and Crime (UNODC). (2023). *Blockchain and Law Enforcement Toolkit*. https://www.unodc.org
[36]. Bhattacharya, M., & Thapa, J. (2020). Blockchain: A game-changer for anti-corruption mechanisms. *Transparency International Research Papers*.
[37]. Ministry of Electronics and IT (MeitY), India. (2021). *Blockchain Strategy for India*. https://meity.gov.in

[38]. Chatterjee, R., & Patel, R. (2021). Blockchain in Indian police and justice system: Possibilities and challenges. *Indian Journal of Public Administration*, 67(3), 520–534.
[39]. Sharma, R., & Sharma, P. (2022). Blockchain forensics: Legal, ethical and practical challenges. *Cyber Law Journal*, 8(1), 34–47.
[40]. Interpol Innovation Centre. (2023). *Blockchain for Law Enforcement Operations: A Strategic Brief*. https://www.interpol.int