**DIGITAL FORENSIC SYSTEMS**

**INTRODUCTION**

The blockchain technology can offer forensic applications with substantial benefits for the whole procedure of digital forensics investigation procedures, including the data collection, preserving, evidence validating, data analysis, and the presentation of the finding. Specifically, the blockchain can improve the transparency in each individual stage, e.g., it can assistant examiner to accurately identify the data sources in the early investigation stage, reduce the data storage, and improve transactional analysis efficiency, and subsequently can reduce the costs of the investigation. One of the most important problems in digital forensics is the management of evidence. Digital proof plays a very important role in crime investigation because it is employed to link persons with criminal activities. It is of extreme importance to guarantee integrity, authenticity, and audit of digital evidence as it moves along different levels of hierarchy i.e, from first responder to higher authorities responsible for handling cybercrime investigation. Digital proof comes with its own distinctive challenges associated with chain of custody. Blockchain technology’s capability to sectionalize comprehensive read of transactions back to origination provides monumental promise for the rhetorical community. Basically, it is a distributed information that maintains an incessantly growing tamper proof arrangement blocks that hold batches of individual transactions. It implements a decentralized fully replicated append-only ledger in a peer-to-peer network, originally deployed for the Bitcoin cryptocurrency. All participating nodes maintain a full local copy of the blockchain. The blockchain consists of a sequence of blocks containing the transactions of the ledger. Transactions within blocks are sorted chronologically and every block contains a cryptographic hash of the previous block within the chain.

**PROBLEM STATEMENT**

The increase in cybercrime, the unawareness of cybercrime among the general public, the insufficiency of expertise in the police service to conduct investigations, gather evidence, incriminate suspects, tampering the evidences and are problems when not addressed can pose some risk to victims and the country at large. To overcome these issues we are using Block-chain technology for Digital Forensics System to provide transparent mechanism for all the internal process of Digital Forensics investigation.

**FABRIC COMPONENTS**

**Ledger:** Blockchain forensics takes data from the blockchain to interpret the flow of digital assets.

Here our ledger (database) consists of Set of insight Crime-Scene Evidences.

**Peers:** Organisations in persons.

Here our peers are

1. Collection of datasets
2. Investigation and Reporting
3. Verification

**Channels:** A channel is a private communication pathway between two or more members of a Hyperledger Fabric network on Amazon Managed Blockchain.

**Certificate Authority:** A URL is generated according to the data uploaded to it. The generated URL is extracted and used for hashing in the blockchain. The extracted URL is considered as string and it is passed through hash algorithm for hashing. The timestamp also hashed along with URL for more integrity. The hashed value is stored in the block itself.

**SYSTEM ARCHITECTURE**

**INVESTIGATION AGENCY PROSECUTION AGENCY**

P-3

P-1

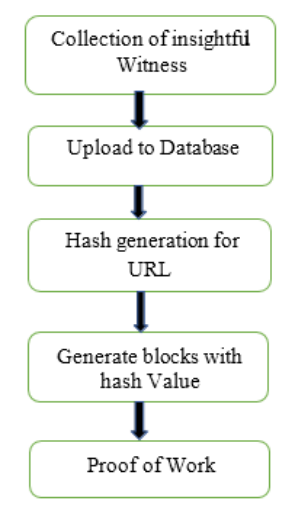
**I**

**P**

P-4

P-2

**HIGHLEVEL FLOW**

****

**SMART CONTRACT.**

SSSSSSMAJXSNX

Forensic contract

Store (Crime Scene,

Report, Evidence)

Save (Crime Scene) in database

Hash=generate hash (Crime Scene)

Save (hash) in ledger

**PROSECUTION**

**AGENCY**

**(ORG-2)**

Forensic contract

get (Crime Scene,

Evidence, report);

{

get (Crime Scene);

CrimeScene.verifier=Consumer

put (Crime Scene);

return Crime Scene;

}

**INVESTIGATION**

**AGENCY**

**(ORG-1)**

Application

Producer=Org1;

Consumer=Org2;

Verify (Crime Scene, Evidence, Report);

Application

Producer=Org2;

Consumer=Org1;

Verify (Crime Scene,

Evidence, Report);

**PSEUDO CODE**

1. Initialize the blockchain
2. Define the structure of the blocks to include:
   1. Timestamp
   2. Hash of the previous block
   3. Hash of the current block
   4. Data related to the digital forensic investigation
3. Create a genesis block with a predefined hash value
4. Start the investigation process by adding data to the blockchain
5. Create a new block for each piece of evidence discovered during the investigation
6. Add the timestamp, the hash of the previous block, and the data to the current block
7. Hash the current block
8. Validate the hash of the current block and the hash of the previous block to ensure the integrity of the blockchain
9. Repeat steps 5 to 8 until all the evidence has been added to the blockchain
10. Use cryptographic tools to analyze the blockchain and extract valuable information
11. Interpret the results of the investigation based on the extracted information