



Islamic University of Technology

Department of Computer Science and Engineering

Securing Digital Evidence with Blockchain

Istiaq Bin Salam Siaam 170042014

Nafis Mahmud 170042023

Abu Raihan Titas 170042026

Supervisors:

Md. Moniruzzaman (Asst. Prof)

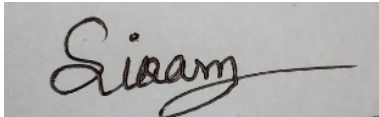
Faisal Hussain (Lecturer), Shakhawat Hossain (Asst. Prof)

A thesis submitted in partial fulfilment of the requirements of
the Islamic University of Technology for the degree of
Bachelor of Science in *Computer Science and Engineering*

May 19, 2022

Declaration of Candidate

This is to certify that the work presented in this thesis is the outcome of the analysis and experiments carried out by Istiaq Bin Salam Siaam, Nafis Mahmud, Md. Abu Raihan Titas under the supervision of MD. Moniruzzaman, Assistant Professor, Faisal Hussein, Lecturer, and Sakhawat Hossen, Assistant Professor, Department of Computer Science and Engineering (CSE), Islamic University of Technology (IUT), Dhaka, Bangladesh. It is also declared that neither of this thesis nor any part of this thesis has been submitted anywhere else for any degree or diploma. Information derived from the published and unpublished work of others has been acknowledged in the text and a list of references is given.

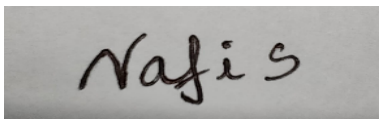


Istiaq Bin Salam Siaam

Student No.: 170042014,

Academic Year: 2020-21,

Date: 19 May, 2022.



Nafis Mahmud

Student No.: 170042023,

Academic Year: 2020-21,

Date: 19 May, 2022.



Md. Abu Raihan Titas

Student No.: 170042026,

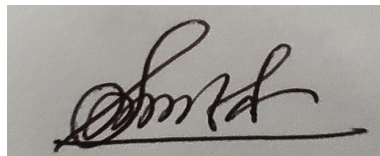
Academic Year: 2020-21,

Date: 19 May, 2022.

CERTIFICATE OF APPROVAL

The thesis titled **Securing Digital evidence with Blockchain** submitted by Istiaq Bin Salam Siaam , Nafis Mahmud, Md. Abu Raihan titas has been found as satisfactory and accepted.

Approved By:



MD. Moniruzzaman (Supervisor)

Assistant Professor

Computer Science & Engineering Department (CSE),
Islamic University of Technology (IUT), Gazipur.

Abstract

Blockchain, is a tamper-proof secure data storage technology that can be effectively used to solve a multitude of privacy, security and data integrity problems. In our particular attempt of research we've studied the phenomenon of using this technology to secure digital evidences that can be used in the court of law. Being government policy compliant and synced with data security goals, a successful implementation of this line of work can bring upon significant betterment to the judicial system of Bangladesh. In this particular line of work, we have studied, assessed and analysed the available and potential solutions for ensuring the security for digital evidence, which can be further developed and appropriated into technologically sound workarounds.

Acknowledgements

The work represented in this report is a collective effort of the team, supervisors and other peers in the relevant fields for the fruition of the endeavor taken and towards the betterment of the research work.

We would also like to thank our team members, our fellow undergrads and our family members for the continuous support and insights they provided. We would like to thank our supervisors, MD. Moniruzzaman sir, Faisal Hussain sir and MD Shakhawat Hossen sir for their gracious contribution and guideline throughout the process of this research work.

Lastly, Glory to Allah, the Almighty, the Merciful, without whose blessing no deed goes into fruitful conclusion. Ameen.

Contents

1	Introduction	1
1.1	Problem Statement	1
1.2	Motivation	2
1.3	Definitions and terminologies	2
1.3.1	Blockchain	2
1.3.2	Smart Contract	2
1.3.3	Tamper-Proof	3
1.3.4	Consensus Algorithm	3
1.3.5	Distributed Ledger	3
1.3.6	Digital Evidence	4
1.3.7	Digital Forensics	4
2	Literature Review	5
2.1	Block-DEF: A Secure Digital Evidence Framework using Blockchain	5
2.1.1	Problems and Limitations of the paper	5
2.1.2	Their Solution Approach	6
2.2	Two-Level Blockchain System for Digital Crime Evidence Management	6
2.2.1	Problems and Limitations of the paper	6
2.2.2	Their Solution Approach	6
2.3	Preventing Spoliation of Evidence with Blockchain: A Perspective from South Asia	6
2.4	Probe-IoT: A Public Digital Ledger Based Forensic Investigation Framework for IoT	8
2.4.1	Workflow	9
2.4.2	Investigation Stage	9
2.4.3	Conclusion	10
2.5	Blockchain Solutions for Forensic Evidence Preservation in IoT Environments	10
2.5.1	Conclusion	11
2.6	Categories of the available literature	11
2.6.1	Extracting and securing evidence with IoT devices	12
2.6.2	Digital Evidence Framework, protocols, chain of custody	14
2.6.3	Scalability and Architecture for storing large-size data	15
2.7	Other Related Works	15
2.8	Relevency of the works	15

3	Methodology	17
3.1	The Underlying Technology	17
3.2	The Architecture	17
3.3	Progressed Works	19
3.4	Existing Implementations	19
3.4.1	Used Tools and Frameworks	20
3.5	Our Implementation	21
4	Results and Case Study	22
4.1	Blockchain in justice system of bangladesh	22
4.1.1	High profile case of Evidence Spoilation	22
4.1.2	Challenges	22
4.2	Analysis of existing Solutions	23
4.3	Our Contribution	23
4.4	Compilation of the solution proposed	23
5	Discussion and Analysis	26
5.1	Analysis	26
5.2	Significance of the findings	26
5.3	Limitations	27
5.3.1	Shortcomings of the Available Literature	27
5.3.2	Shortcomings of the Available implementations	27
5.4	Suggestions	27
6	Conclusions and Future Work	28
6.1	Conclusions	28
6.2	Future Work	28

Chapter 1

Introduction

Blockchain is a peer-to-peer validation system to store information that is gaining popularity due to its promising ability of being secure and tamper-proof. Blockchain, as the name suggests, is architecturally a chain of blocks where each block has to reach some sort of agreement (the consensus algorithm) before a new block of information can be initiated or any kind of updates or changes in the existing blocks introduced. That makes tampering data or transaction info nearly impossible. The consensus protocols and algorithms are of numerous types, ex- proof of stake, proof of work and many more. These mechanisms makes adding new blocks into the system time-constrained and mathematically bounded enough to introduce any problematic tampering. And so, the gained advantage of using blockchains in appropriate real-world scenarios can be a very convenient and beneficial approach. Storing public domain data can be useful with the distributed ledger property.[1]

A distributed ledger is a database that is consensually shared and synchronized across multiple sites, institutions, or geographies, accessible by multiple people.[2] Underlying distributed ledgers is the same technology that is used by blockchain.

Digital Evidences are digital/computerized data such as cctv footage, internet usage info, files in local directories, and basically every other kind of data that can be used as evidence for judiciary cases in the court of law.

Setting the definitions, we'll move on to the depth of the situation.

1.1 Problem Statement

From a worldwide perspective, the necessity of critical data security is quite well-known. But we aspire to focus onto a more focused and localized aspect of data security, and that is, the preservation of digital evidence in Bangladesh.

As one of the most densely populated country in the world, Bangladesh produces a huge amount of data, Some of this can be crucial digital evidence. A lot of these type of data are stored in physical copies of minimized storage, like dvd archives or on sheets of paper, which are prone to data loss due to physical damage. [3] Other than that law enforcement agencies and department of justice preserve these in a centralized database system, These precious evidences are prone to external attacks and tampering. Attack on a centralized server may lead to massive leak to critical data or

severe data loss, all of these are a big systematic, judicial and financial liability, and also a threat to transparency of law and justice.

1.2 Motivation

Our incentive towards this particular field of research was to focus on the application-specific boundaries of the blockchain technology and utilizing the benefits into a real-world solution. For that matter, we have decided that the work should be something that fits the necessity of the local region we reside in, more specifically, the country of Bangladesh. Now, Bangladesh government have adopted a national blockchain strategy as a part of the broader 4th industrial revolution (4IR) movement. There are several useful and promising applications describe in the official government blockchain strategy document, and we chose to take '*Securing digital evidence*' under the judiciary applications subcategory.

Here's our argument behind the relevancy of choosing this particular topic:

- Digital evidences are one of the most 'prone to tamper' kind of data [4]
- Proper implementation of blockchain tech here can ensure justice a lot better
- If there is an attack on a centralized storage server, major data or investigation info leak, even massive data loss is a very probable threat.
- In the roadmap, it's one of the last implementation (around 2030s). Meaning probably no one in bangladesh has started it yet and we have a headstart.

1.3 Definitions and terminologies

Before moving on to further elaboration, here are some preliminary definitions necessary to understand the work.

1.3.1 Blockchain

Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. [5]

1.3.2 Smart Contract

A smart contract is a computer program or a transaction protocol which is intended to automatically execute, control or document legally relevant events and actions according to the terms of a contract or an agreement. Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met.

[6] They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss.

1.3.3 Tamper-Proof

A secure system where it is impossible to manipulate or tamper the stored data. Something that is achievable through the means of blockchain.

1.3.4 Consensus Algorithm

A consensus algorithm is a process in computer science used to achieve agreement on a single data value among distributed processes or systems. Consensus algorithms are designed to achieve reliability in a network involving multiple unreliable nodes. Solving that issue – known as the consensus problem – is important in distributed computing and multi-agent systems.

To accommodate this reality, consensus algorithms necessarily assume that some processes and systems will be unavailable and that some communications will be lost. As a result, consensus algorithms must be fault-tolerant. [7] They typically assume, for example, that only a portion of nodes will respond but require a response from that portion, such as 51 percent, at a minimum.

There are numerous variations of consensus algorithms, such as:

Proof of Work

Proof of work (PoW) is a form of cryptographic proof in which one party (the prover) proves to others (the verifiers) that a certain amount of a specific computational effort has been expended. Verifiers can subsequently confirm this expenditure with minimal effort on their part. A key feature of proof-of-work schemes is their asymmetry: the work – the computation – must be moderately hard (yet feasible) on the prover or requester side but easy to check for the verifier or service provider. This idea is also known as a CPU cost function, client puzzle, computational puzzle, or CPU pricing function. Another common feature are built-in incentive-structures that reward allocating computational capacity to the network with value in the form of money

Proof of Stake

Proof-of-stake reduces the amount of computational work needed to verify blocks and transactions that keep the blockchain, and thus a cryptocurrency, secure.

Proof-of-stake changes the way blocks are verified using the machines of coin owners. The owners offer their coins as collateral for the chance to validate blocks. Coin owners with staked coins become "validators."

1.3.5 Distributed Ledger

A distributed ledger is a database that is consensually shared and synchronized across multiple sites, institutions, or geographies, accessible by multiple people. It allows

transactions to have public "witnesses." The participant at each node of the network can access the recordings shared across that network and can own an identical copy of it. Any changes or additions made to the ledger are reflected and copied to all participants in a matter of seconds or minutes.

1.3.6 Digital Evidence

Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial.

1.3.7 Digital Forensics

Digital Forensics is defined as the process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law. [8]It is a science of finding evidence from digital media like a computer, mobile phone, server, or network. It provides the forensic team with the best techniques and tools to solve complicated digital-related cases.

Chapter 2

Literature Review

To begin with a disclaimer of sorts before delving into the studies, there were a number of criteria and obligations that needed to be fulfilled for solving the problem we mentioned beforehand.

The data size for such an endeavour is massive. We're talking about anywhere from terabytes to petabytes and even higher. And for blockchains, scalability is quite a big issue. Meaning we need a scheme where the actual evidence data is stored in a different storage and the metadata for those evidences are stored in the blockchain architecture. For such an architecture, at the initial stage we studied the architectures of different blockchain system, a comparative with directed acyclic graph [1] and a scalable blockchain protocol called bitcoin-NG.[9]

For that particular reason, we chose to study over blockchains that are lightweight, scalable and loosely coupled with a different storage system. First we came upon a paper on a topic called lightchain. It's a type of lightweight blockchain designed for industrial IoT devices. However, that particular type was not satisfactory for our ordeal and so we moved on to researches strictly based upon evidence collection. Here's the summary of the papers we could find on that regard.

2.1 Block-DEF: A Secure Digital Evidence Framework using Blockchain

Here, the proposed solution for addressing the digital-data-storage problem is centered around the concept of something called block-DEF. It's a loosely coupled blockchain architecture with three layers: service layer, blockchain layer and network layer. The original storage for evidences aren't within the bounds of blockchain but are maintained in a separate storage with a loosely coupled system. It is a lightweight blockchain combining a mixed block structure with an optimized name-based practical byzantine fault tolerance consensus mechanism.[10]

2.1.1 Problems and Limitations of the paper

The blockchain, even though scalable and lightweight, for the current infrastructure of bangladesh, it poses a problem because it's costly. A consortium blockchain of this

sort is not exactly designed bearing the case of cost-effectiveness in mind. The mixed structure of the blockchain leads to a major problem even though it significantly reduces the storage needed. That is, there is no full node in the network and node failure can break the blockchain which can ultimately diminish the very purpose it was built for.

2.1.2 Their Solution Approach

The Problems this paper immediately addresses is that it ensures the scalability and integrity validity of the blockchain storages which would otherwise be way too computationally expensive and exhausting to store such kind of data.

To solve the no full node problem, the paper proposes a solution in the form of two strategies. First being each block body distributed to multiple nodes in the network, and the second one being treating the storage module as a full node and storing complete blockchain in the module.

2.2 Two-Level Blockchain System for Digital Crime Evidence Management

The proposed approach in this paper is also of a multi-level blockchain but of a slightly different kind. Here, the two level of blockchains are hot and cold. In the hot blockchain, data subject to frequent change are stored; and unchanged or very rarely changeable datas are stored in the cold blockchain.[11]

2.2.1 Problems and Limitations of the paper

A major limitation is with the kind of data their proposed method stores. Their results said that the system is well suited for storing data that is basically large files and the system can perform searches upon them, but applying different kind of applications in general still seems to be a problem. Also, some performance enhancement is also required along with complexity reduction in the cold blockchain of their architecture.

2.2.2 Their Solution Approach

Their approach made storing video evidences, which is a major type of evidence file, effectively secure, scalable and adequately stored. Mixing their approach with other kind of methods may be an optimal way to ensure all sorts of evidence files.

2.3 Preventing Spoliation of Evidence with Blockchain: A Perspective from South Asia

South Asia faces a huge deal of evidence spoliation due to personal and political interest. There's also a fear of facing backlash for providing evidence. For this reason providing proper security to the evidence provider is essential. 'EvidenceChain' is a

conceptual model through which citizens can anonymously upload digital evidence having confidence that the evidence's integrity will be preserved in an unchangeable and indestructible manner. If coerced by the offenders or authorities, the person uploading the evidence might share it anonymously with investigative authorities or openly with the public. [3]

Any technical solution for preventing spoliation of evidence must meet the following conditions:

1. Usability
2. Privacy
3. Security

EVIDENCECHAIN maintains a public private hybrid blockchain model. The working model of EVIDENCECHAIN is given below:

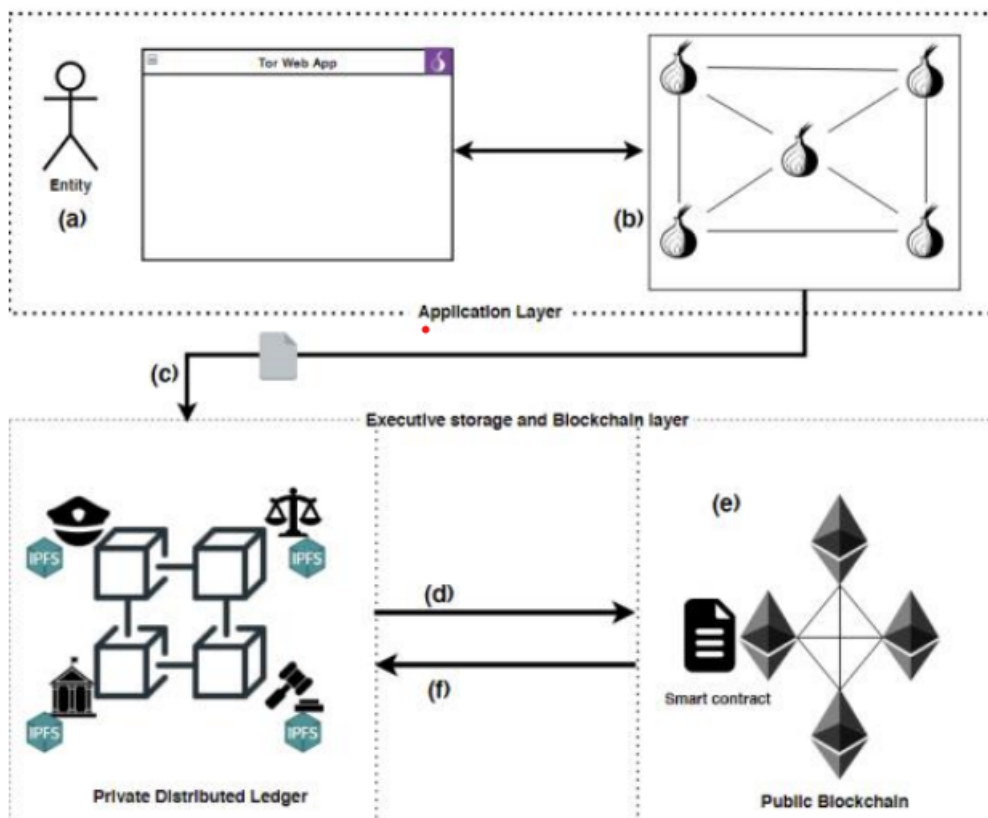


Figure 2.1: Flow of information through evidencechain

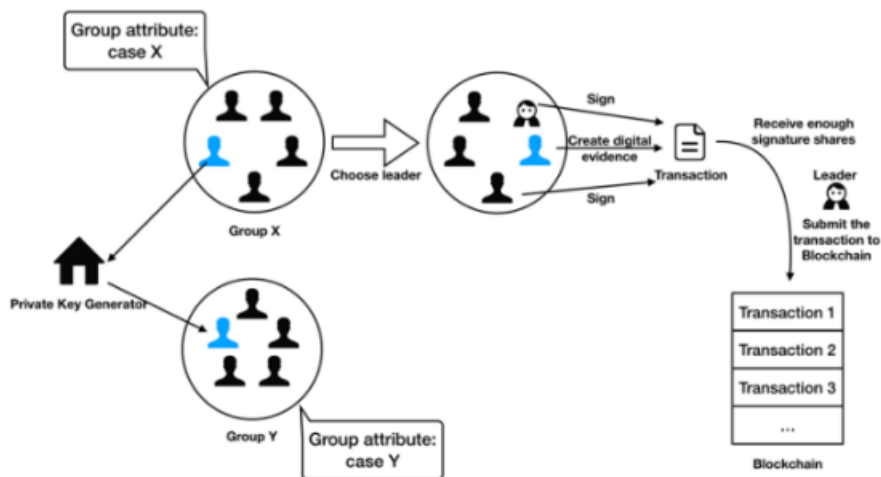


Figure 1. System model

Figure 2.2: Flow of information through evidencechain

2.4 Probe-IoT: A Public Digital Ledger Based Forensic Investigation Framework for IoT

Internet of Things (IoT) is deeply integrated in our life. A successful attack on a system based IoT can put the lives of its users in danger. Furthermore adversaries can jeopardize privacy, security and overall wellbeing of citizen. Probe-IoT is a forensic investigation platform for IoT-based systems that uses a decentralized, distributed, and public digital ledger to identify facts in IoT crime cases.

The ledger, dubbed blockchain, keeps track of a growing list of records. A transaction comprises information on the interactions that occur among the various entities of an IoT-based system, such as IoT devices, users, and cloud services, while a block contains a list of transactions. [2]

In an IoT-based system, interactions can be divided into the following three categories:

1. Things to users(T2U): a) A user (initiator) connects to an IoT device (target) remotely via a cloud service (intermediate) and gateway (intermediate), or vice versa; b) A user connects to an IoT device locally via a gateway, or vice versa.
2. Things to Cloud (T2C): An IoT device sends data to a cloud service via a gateway, or the other way around.
3. Things to Cloud (T2C): An IoT device sends data to a cloud service via a gateway, or the other way around.

2.4.1 Workflow

Transaction creation

The procedure of initiating a transaction for a T2U interaction is depicted in Figure 2. Transactions for T2C and T2T interactions are created using the same procedure. A transaction is started by the person who initiates the interaction. The parties to the transaction use their public keys issued by an Escrow provider to sign the transaction. The transaction is complete when the last party in the forwarding path of the interaction signs it. The transaction is sent to the blockchain network after it is done.

Insertion into blockchain ledgers

Stakeholders appoint miners to gather transactions on a regular basis. A miner collects transactions for a specific time period. The signatures associated to the transactions are validated by the miner. It then builds an interaction block with the transactions within. The miner then uploads the block to the network.

Escrow service

The public key of the Escrow service is used to encrypt the request and response data found in a transaction (Interactiondetails record in Figure 1.

2.4.2 Investigation Stage

An investigator is given the identities (IDs) of the entities involved in the event, as well as their public key validation data, during the course of the inquiry (Figure 3). The following is how an entity computes its public key validation data Pvd: i) chooses a nonce N; ii) signs the nonce and its ID as $SIGN(N \parallel ID)_s$ using its private key s ; iii) concatenates $SIGN(N \parallel ID)_s$ and N to generate $Pvd = N \parallel SIGN(N \parallel ID)_s$. The investigator gives the escrow service the IDs and obtains the entities' public keys. The investigator verifies the Pvd of each entity using the entity's public key. As a result, the investigator confirms that an entity's ID is not fabricated and that the Escrow's public key for that entity corresponds to the ID. The investigator then obtains the transactions including the public keys from the public ledger. The investigator gathers all transactions that occurred during the time frame of the occurrence. The transactions are subsequently delivered to the Escrow service by the investigator. Using the private key, the Escrow service decrypts the request and answer data in the transactions and transmits it back to the investigator through a secure channel. The investigator verifies the Pvd of each entity using the entity's public key. As a result, the investigator confirms that an entity's ID is not fabricated and that the Escrow's public key for that entity corresponds to the ID. The investigator then obtains the transactions including the public keys from the public ledger. The investigator gathers all transactions that occurred during the time frame of the occurrence. The transactions are subsequently delivered to the Escrow service by the investigator. Using the private key, the Escrow service decrypts the request and answer data in the transactions and transmits it back to the investigator through a secure channel.

Finally, the investigator reviews and analyzes the unencrypted communications in order to determine the facts in a criminal case or to settle a dispute.

2.4.3 Conclusion

In this paper, Probe-IoT, a public digital ledger-based forensic investigation platform for IoT-based systems is introduced. Probe-IoT records device-to-device, device-to-user, and device-to-cloud interactions in a public digital ledger akin to Bitcoin. The publicly available evidence is protected by Probe-IoT, which assures its secrecy, anonymity, and non-repudiation. During the investigation of a criminal occurrence, Probe-IoT additionally provides interfaces for evidence gathering and a system to validate the integrity of the evidence. We will continue to develop and test Probe-IoT in terms of connectivity, compute, energy, and storage cost for making and storing transactions in the future.

2.5 Blockchain Solutions for Forensic Evidence Preservation in IoT Environments

We propose our blockchain-based IoT forensic model in this paper (BLOF). There are three levels in IoT environments. The cloud, network, and device layers are the three of them. Our methodology takes advantage of blockchain's decentralized nature to ensure that logs generated in IoT contexts are saved on the network and can be verified by any of the network's participating nodes. [?]

When conducting a forensic examination, there are various artefacts to consider. Our methodology, on the other hand, is limited to system and event logs. The Cloud Service Providers (CSPs), Network Devices, and IoT Devices are the entities in our concept. The entities act as the network's blockchain nodes. A key generation mechanism is used to add new nodes to the network.

Before a transaction is written to the block, it is appended with a node's public key. A pair of keys is generated when a new node is created. The CSPs serve as the network's miners. CSPs are great candidates for mining because of their computing capability. A Blockchain Centre (BC), a Log Processing Centre (LPC), and a User Centre make up our concept (UC). Each of these components is discussed in length in the preceding subsections. we discuss each of these components into details.

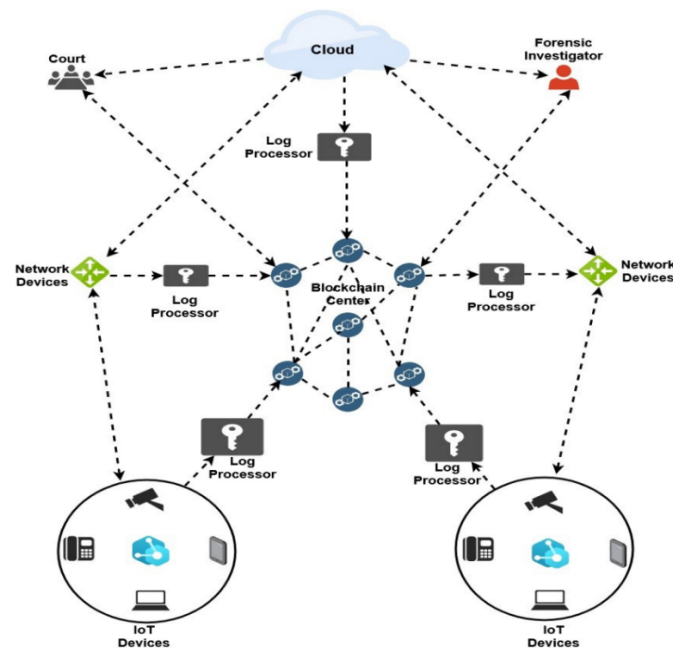


Figure 2.3: Proposed forensic Model

The proposed model is shown in Figure 1. The security of this technology, like any other computing technology, is an issue. With the amount of cyber-attacks on the rise, it's critical that such measures are taken. Crimes are investigated, and those who commit them are prosecuted. Because of the the cloud integration and the diverse nature of the IoT ecosystem On the network layer, forensic investigations in an IoT setting are extremely difficult. a difficult task Furthermore, it is incredibly difficult for stakeholders to choose the best course of action. They must rely on the legitimacy of the evidence they deal with in most circumstances. For these pieces of proof, service providers are needed.

2.5.1 Conclusion

The security of this technology, like any other computing technology, is an issue. With the amount of cyber-attacks on the rise, it's critical that such measures are taken. Crimes are investigated, and those who commit them are prosecuted. Because of the the cloud integration and the diverse nature of the IoT ecosystem On the network layer, forensic investigations in an IoT setting are extremely difficult. a difficult task Furthermore, it is incredibly difficult for stakeholders to choose the best course of action. They must rely on the legitimacy of the evidence they deal with in most circumstances. For these pieces of proof, service providers are needed.

2.6 Categories of the available literature

We have data about this particular field of academic literature for 2018-2020 and it is as follows:

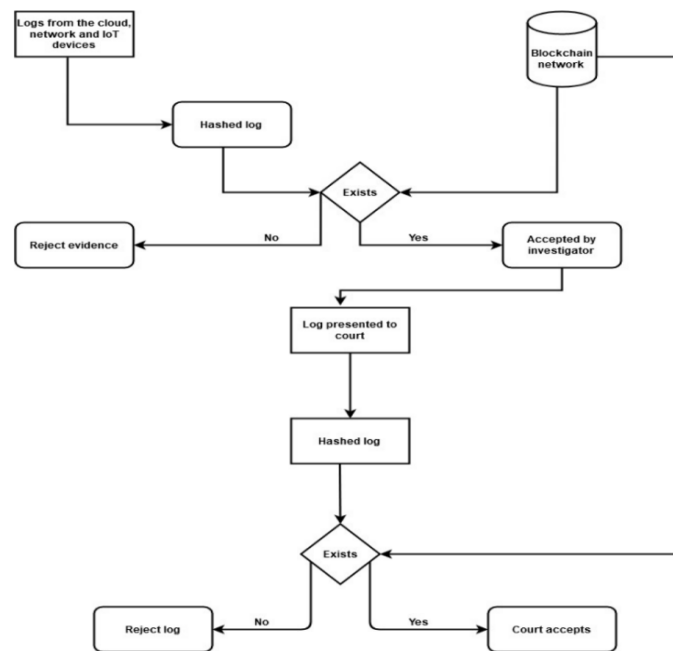


Figure 2.4: Verification Process

Publication type	Publication year		
	2018	2019	2020
Journal articles	2	10	
Serials		4	
Conference proceedings	4	7	1

The available literature can be categorized into the following three:-

1. Extracting and securing evidence with IoT devices
2. Digital Evidence Framework, protocols, chain of custody
3. Scalability and Architecture for storing large-size data

2.6.1 Extracting and securing evidence with IoT devices

Internet of things (IoT) devices, both household and industrial, have the capability to store data in multitude of forms . The academic literatures related to this sheds light on the mechanism and models on how to collect, extract, choose and store data from an IoT device to a blockchain-based system. For that regard they have articulated mechanisms, protocols and roadmaps. [12] [13] [14] [15] [16] [17] [18] [19] Some of the example mechanism diagrams are given.

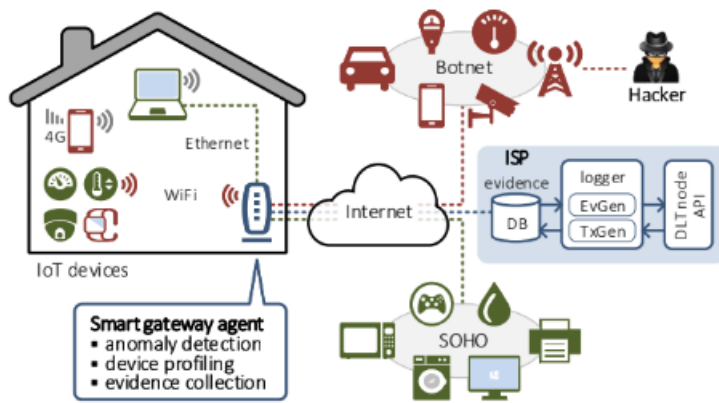


Fig. 1. An overview of Cyber-Trust’s forensic evidence collection process; it is assumed that the red-colored devices in the smart home have been attacked and this is detected by the SGA that collects the evidence.

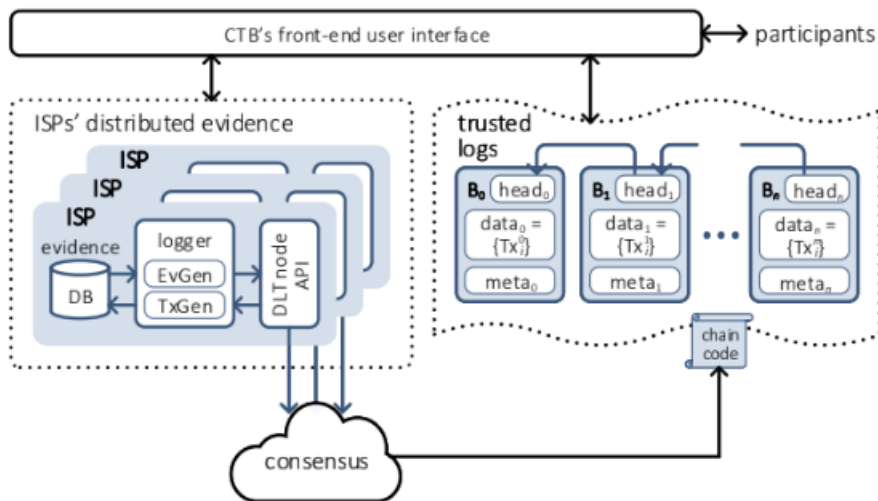
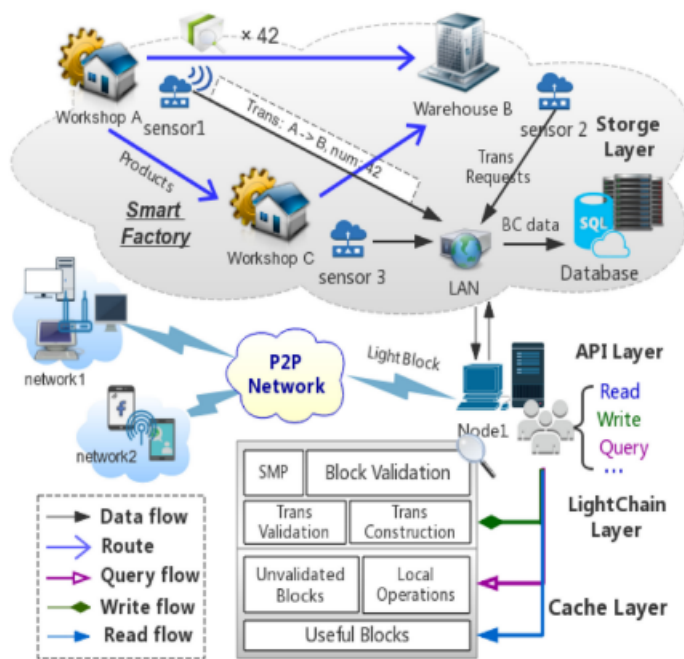


Fig. 2. High-level architecture of Cyber-Trust’s blockchain.



2.6.2 Digital Evidence Framework, protocols, chain of custody

Protocol and mechanism for chain of custody, from the reporting of the evidence to it's presenting at court, how the data will travel and by/to whom. Multi-Layered Framework for data protection are provided, with the aid of Access control and hyperledger proceedings. [8] [20] [19] [21] [22] [6]

Some diagrams may follow:

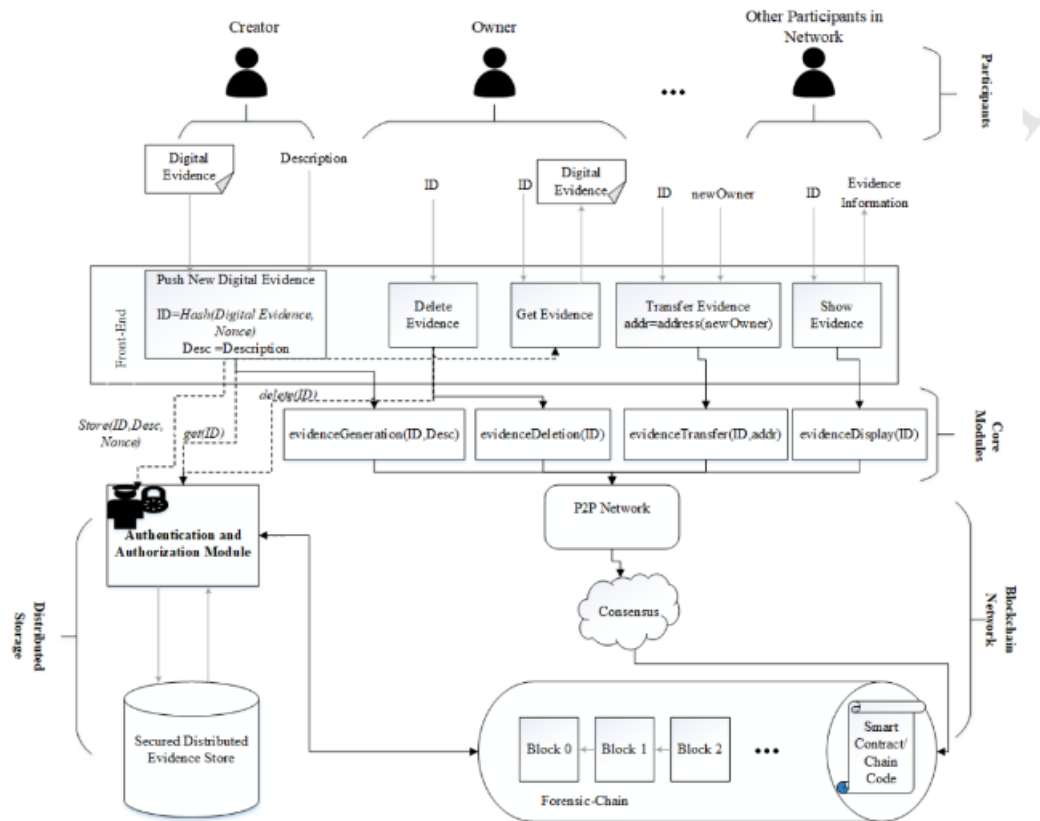


Figure 6: Operational Flow of Forensic-Chain

2.6.3 Scalability and Architecture for storing large-size data

Ideas and diagrams are discussed in the next chapter

2.7 Other Related Works

To fit with the criteria a handful of other academic works were explored. Among them two noteworthy ones are a lightweight blockchain system called **Lightchain for Industrial IoT devices** [23] which uses a consensus mechanism called green consensus to maintain the lightweight and computational low-cost. And to study the endeavor of securely storing and sharing large amount of data we explored a paper called **Blockchain for Secure and Efficient Data Sharing in Dehicular Edge Computing and Networks** . [24]

2.8 Relevancy of the works

To make the system work in the appropriate capacity as far as we know, the blockchain system requires three must-have properties:

- **Lightweightness and Scalability** : To store the massive amounts of data this is a must have. And for browsing through all these academic literature that was a first and foremost concern.
- **Security** : Security is an utmost concern of the system like an evidence collection framework. For any blockchain system, it is relevant to some degree.
- **Compliance** : The legal and statutory laws of the locality or culture has to be compliant and in sync with the digital evidence collection system. The relevant works mentioned and our endeavor complies with the vision of the Bangladesh govt as mentioned in the national blockchain strategy guideline document, subsection 4.9.

Chapter 3

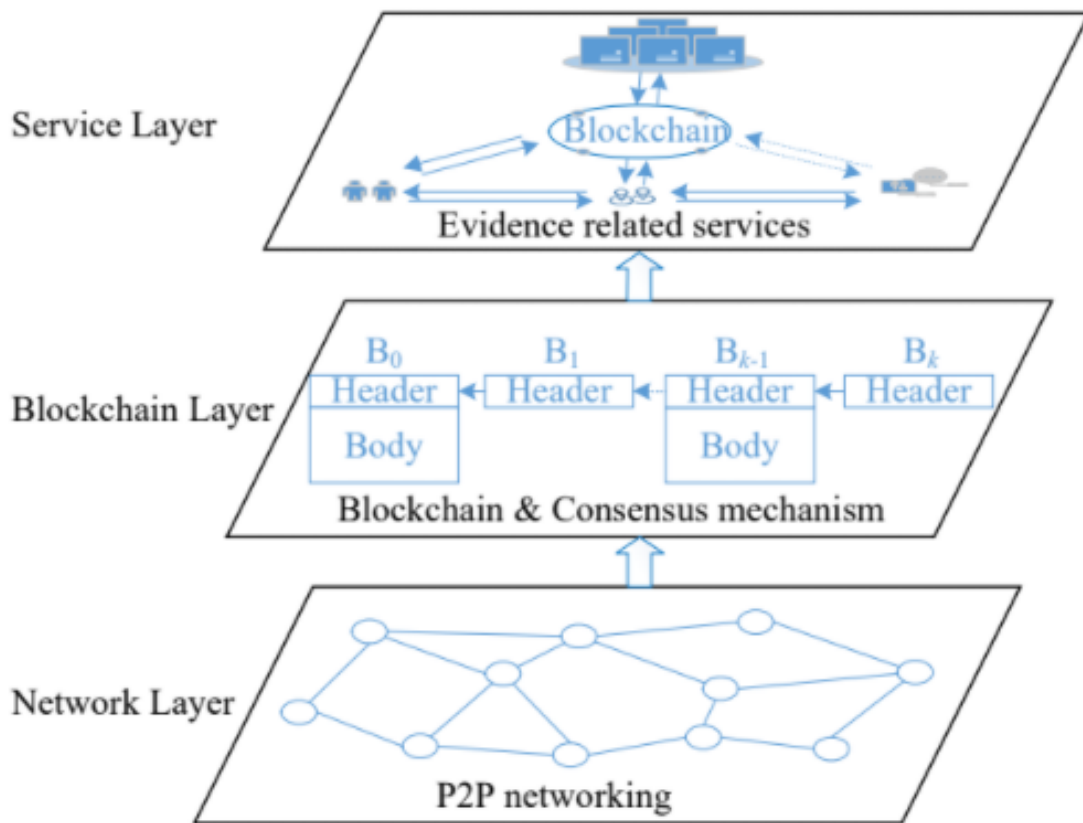
Methodology

3.1 The Underlying Technology

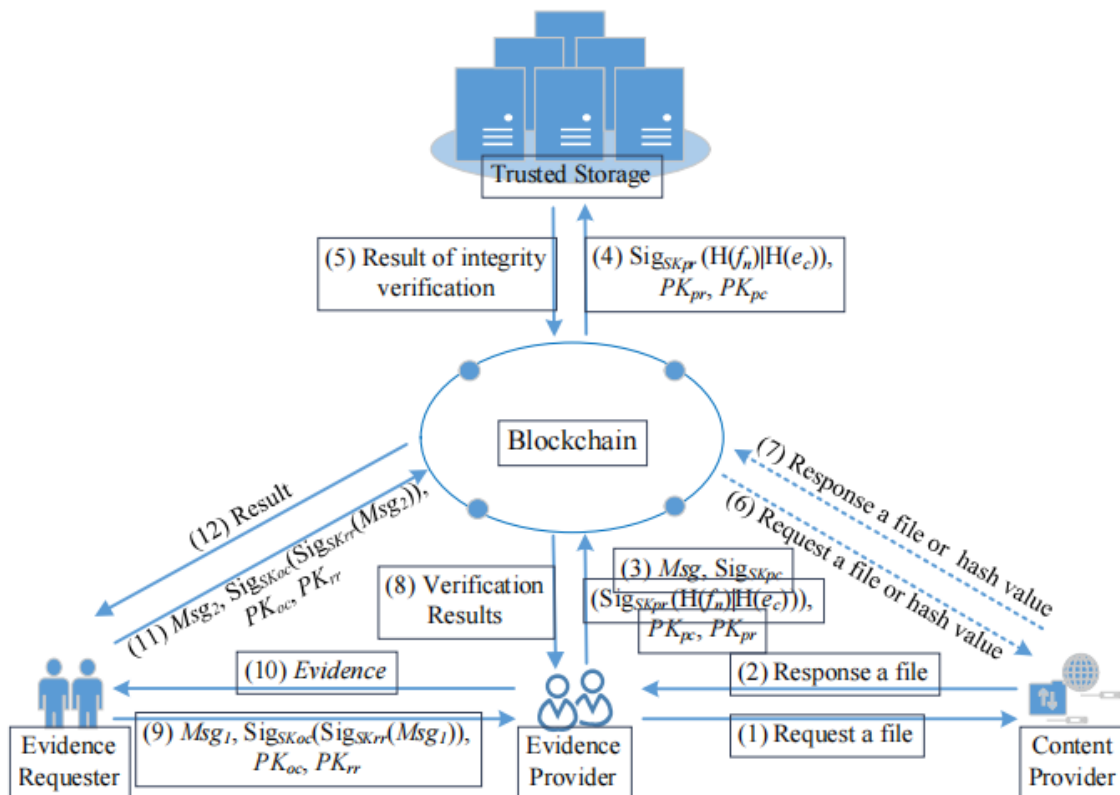
The core underlying mechanism is, needless to say, a modified or mixed framework consisting of blockchain architecture. Above on that, there are databases, storing mechanisms, effecting data sharing methods, quick and efficient searching, a vulnerability-free system, these are some of the concerns on the technology.

3.2 The Architecture

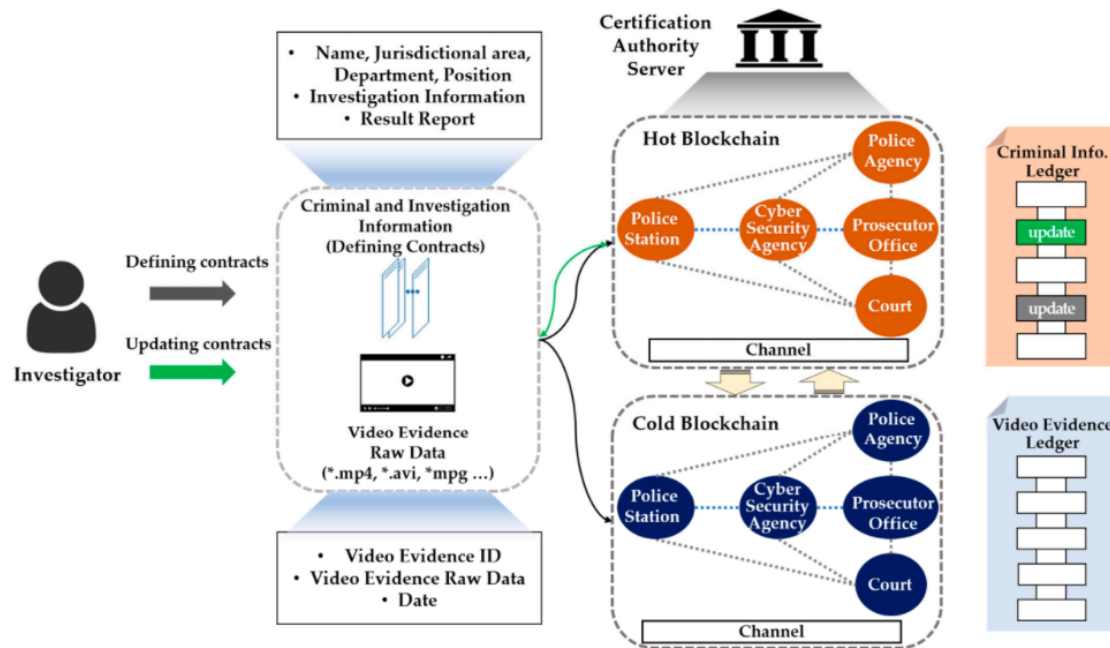
From the works we gathered, the architecture for coming up with a good evidence collection system, two overall methodology deemed an appropriate solution. First one being the three-layered block-DEF system.



Along with a well-devised evidence service model.



The second method encases the general methodology for the hot and cold blockchain architecture.



Our goal is to find a means to combining the various methods and to make them compliant to a suitable system for Bangladeshi judicial system.

3.3 Progressed Works

Up until now we have done the following:

- Study Existing Literature and models of solutions
- Study Existing Implementations
- Partial Implementation
- Conducting a case study
- Analyse the findings

3.4 Existing Implementations

There are a handful of existing implementations available online that we have studied and analysed for our own implementation. The existing ones usually are file systems stored in traditional blockchain architecture. We couldn't find source code or practical implementation for any of the academic literature that was provided.

3.4.1 Used Tools and Frameworks

Solidity

Solidity is an object-oriented, high-level language for implementing smart contracts. Smart contracts are programs which govern the behaviour of accounts within the Ethereum state.

Solidity is a curly-bracket language designed to target the Ethereum Virtual Machine (EVM). It is influenced by C++, Python and JavaScript. You can find more details about which languages Solidity has been inspired by in the language influences section. Solidity is statically typed, supports inheritance, libraries and complex user-defined types among other features.

With Solidity you can create contracts for uses such as voting, crowdfunding, blind auctions, and multi-signature wallets.

Truffle

A development environment, testing framework and asset pipeline for blockchains using the Ethereum Virtual Machine (EVM), aiming to make life as a developer easier. With Truffle, you get:

Built-in smart contract compilation, linking, deployment and binary management.

Automated contract testing for rapid development.

Scriptable, extensible deployment migrations framework.

Network management for deploying to any number of public private networks.

Package management with EthPM NPM, using the ERC190 standard.

Interactive console for direct contract communication.

Configurable build pipeline with support for tight integration.

External script runner that executes scripts within a Truffle environment

Web3.js

web3.js is a collection of libraries that allow you to interact with a local or remote ethereum node using HTTP, IPC or WebSocket.

IPFS

IPFS is a distributed system for storing and accessing files, websites, applications, and data.

Making it possible to download a file from many locations that aren't managed by one organization:

Supports a resilient internet. If someone attacks Wikipedia's web servers or an engineer at Wikipedia makes a big mistake that causes their servers to catch fire, you can still get the same webpages from somewhere else. Makes it harder to censor content. Because files on IPFS can come from many places, it's harder for anyone (whether they're states, corporations, or someone else) to block things. We hope IPFS can help provide ways to circumvent actions like these when they happen. Can speed up the web when you're far away or disconnected. If you can retrieve a file from someone nearby instead of hundreds or thousands of miles away, you can often get it

faster. This is especially valuable if your community is networked locally but doesn't have a good connection to the wider internet. (Well-funded organizations with technical expertise do this today by using multiple data centers or CDNs — content distribution networks)

Ganache

A part and a transaction testing tool of the truffle suite, Ganache is a personal blockchain for rapid Ethereum and Corda distributed application development. You can use Ganache across the entire development cycle; enabling you to develop, deploy, and test your dApps in a safe and deterministic environment.

Ganache comes in two flavors: a UI and CLI. Ganache UI is a desktop application supporting both Ethereum and Corda technology. The command-line tool, `ganache-cli` (formerly known as the TestRPC), is available for Ethereum development.

Metamask

MetaMask is the trailblazing tool enabling user interactions and experience on Web3. It is currently available as a browser extension and as a mobile app on both Android and iOS devices. It makes it easier to build a dapp - decentralized app and test its transactions and functionalities.

Programming Languages

For the front end of their application most existing solutions used javascript, python or Go language, or their frameworks.

3.5 Our Implementation

Since we couldn't find any of the source codes for the hybrid blockchain architecture, we had to rely on the pre-built frameworks and ethereum-based blockchain system to build our system. Due to time constraint we couldn't implement a meaningful implementation of a evidence storage system in a blockchain. The extent to which we could implement the system is uploading an image data to an IPFS system, which was subsequently supposed to pass through and be stored in a blockchain system.

Chapter 4

Results and Case Study

The results from the reviewed papers indicate that the scalability, security and data integrity are a possibility from the mentioned mechanisms. However, Since we proposed combining some methods or adapt them in some way to fit our own criterias from a Bangladesh perspective, the results may vary.

The system isn't built or tested by ourselves yet to carry out actual results. After the system is built, several standardization will be tested out to see how well the proposed system performs.

4.1 Blockchain in justice system of bangladesh

Bangladesh like many other developing country faces enormous challenge to ensure justice. Evidence temper is a everyday scenario here. Most of the evidence is recorded is a centralized. Hackers can easily manipulate the evidence and feed false data. Sometimes the evidence is kept in a physical file system.theft and tamperment is very easy with this kind of file system.Evidence providers get exposed and gets threatened by the powerful people. Blockchain which is a decentralized file system can solve these issues. Blockchain prevents unauthorized access to evidence .It preserves the identification of providers. Files are saved as chain of custody so all the evidence of a case are preserved together.

4.1.1 High profile case of Evidence Spoilation

In 2020, The Governor of the Bangladesh bank withheld the information about hack for 1 billion usd for over a month. This falls in the category of withholding information which is a very known form of evidence spoilation.

4.1.2 Challenges

Bangladesh lacks proper infrustructure. Bangladesh has one of the lowest bandwidth in the world .A vast part of rural people is out of the reach of internet.Digital illiteracy is also a major problem of this country.Root level implementation of blockchain can be challenging due to lack of internet access.

4.2 Analysis of existing Solutions

The solutions that are currently available have the following characteristics:

- Mostly theoretical
- Hybrid blockchain architecture
- Emphasises on what data to store more than how to store them
- Relatively new tech and scalability issue

4.3 Our Contribution

For all the existing works available, we've combined and analysed the trends and phenomena that are out there and made assumptions upon the effectiveness, feasibility and compliancy of the existing systems. The narrow-down of these findings may help individuals who study these works farther down the line for digital evidence protection and also scalable blockchain architecture.

4.4 Compilation of the solution proposed

: The collecting, preservation, and analysis of digital evidence has become an enormously crucial tool for solving cybercrime and preparing court cases because to advancements in the information technology landscape during the last two decades. As it is, digital evidence is crucial in cybercrime investigations. used to connect people to illegal activity As a result, ensuring the integrity, validity, and auditability of digital evidence is critical. as it goes through the chain of custody at several levels of hierarchy Cybercrime is being investigated. In terms of technology, today's technology is more sophisticated. in terms of portability and power. Billions of devices connected to the internet generate a massive amount of data that must be kept and accessible, providing significant issues in protecting the integrity and authenticity of digital evidence for its admission in a court of law. Because digital evidences are latent, volatile, and fragile, they can traverse jurisdictional borders rapidly and readily, and they are often time/machine dependent.

As a result, in a digital world, ensuring the validity and legality of methods and procedures used to obtain and transfer evidence is a significant difficulty. The capacity of blockchain technology to provide a full view of transactions (events/actions) back to their origins holds immense promise for the forensic community. In both intrusion detection and forensic evidence applications, blockchain solutions have recently been proposed, as blockchain can alleviate concerns of trust in both cases.

The smart home environment is a trend that is anticipated to become the standard in the near future, especially as our society gets more digitalized (for example, smart transportation). systems). As a result, the ability to recognize, gather, maintain, and share information is crucial. It will be analyzed evidential data from the heterogeneous HAS. Integrity, transparency, accountability, and secure data sharing are all values that

we hold dear. By analyzing compromised devices and gathering forensic evidence to determine the source of cyberattacks, the Cyber-Trust platform relies on advanced intrusion detection techniques to identify malicious activity and enhance the security of IoT environments. While the hashes and metadata of the evidence are stored on the blockchain, the evidential material is safely stored as raw data in an off-chain database. Built on top of HyperLedger Fabric, the CTB is a permissioned distributed ledger. The CoC method of recording and keeping a chronological history of digital evidences is dematerialized by the Cyberblockchain-based Trust's solution. Evidence chain is a public-private hybrid blockchain model.

Although the model's effectiveness in preventing evidence spoliation is theoretically and technically possible, it has yet to be shown in practice. The approach is based on usability, especially how straightforward the experience is. is a platform for the entire public to upload evidence anonymously. If people are unable to simply access the platform, it will fail. obstruct the system's greater adoption and effectiveness If the interne If the user interface is accessible over the internet, then it would be a compromise. Authorities and users' identities might both be monitored on the platform. Users should be targeted. As a result, a Tor web service-based interface is required. proposed by this paradigm, which, despite its robustness, retain anonymity, however non-technical users may find it difficult to utilize. found it challenging. any tainted official to tamper with the vetting process Furthermore, transparency, particularly the linkage of validated evidence with signatures and the immutable preservation of the integrity record on the blockchain, will transfer the fear of fraud. Using an EvidenceChain-like approach to transform the current centralized, tamper-prone, and attack-prone evidence management system into a distributed, immutable, and indestructible system will have two major impacts: First, by providing regular citizens and whistleblowers with a new paradigm, they will be able to use their authority to prevent evidence spoliation and human rights violations by disclosing evidence without fear of being exposed and retaliated against. Second, by converting the vetting process to a consensus-based method, any compromised actor inside the authorities will be prevented from manipulating the vetting process. Transparency, particularly tying validated evidence to signatures and immutably keeping the integrity record on public blockchain, is also important. The fear of retaliation will be transferred from regular citizens to authority. This is significant in the context of South Asia and other developing countries.

Fear of retaliation and the shift of power from authority to the public In the other direction, it may help to transform the post-colonial era. We believe that by adopting this approach, not only will we be able to reduce the amount of waste we produce, but we will also be able to spoliation of evidence, yet it has the capacity to maximize the possibilities for establishing societies that are transparent and just. The energy required for the execution of blockchain protocols based on proof of work (PoW), such as bitcoin , is a major factor to consider. At the time of writing, producing a single block on the bitcoin blockchain involves more than 260 hashing operations, resulting in significant energy consumption. Early calculations revealed that the protocol's energy requirements were comparable to those of a small country. This situation has prompted researchers to look into alternative blockchain protocols that would eliminate the need for proof of work by replacing it with a more energy-efficient

mechanism capable of providing identical assurances. It's worth noting that bitcoin's proof of work system supports a randomized "leader election" process in which one of the miners is chosen to issue the next block. Furthermore, assuming that all miners adhere to the protocol, this selection is made in a randomized manner proportional to each miner's computational power.

(Differentiations from the protocol may cause distortions.) "Selfish mining" tactics exemplify this proportionality. The concept of "proof of stake" is a natural alternative technique. (PoS). Rather than investing processing resources in the leader election process, miners instead execute a mechanism that selects a leader at random. chooses one of them equal to the stake each of them has, based on the current ledger on the blockchain. In effect, this creates a self-referential blockchain discipline: the blockchain is maintained by the stakeholders themselves, who are assigned labor (as well as rewards) based on the amount of stake they have as reflected in the ledger. Aside from that, the discipline should not impose any additional "artificial" computational requirements on the stakeholders. This sounds ideal in some ways, but implementing such a proof-of-stake protocol appears to present a number of definitional, technical, and analytic challenges.

Chapter 5

Discussion and Analysis

5.1 Analysis

Our core Findings are but not limited to:-

- Smart contract plays one of the most trivial roles in establishing the chain
- Choosing the right entries for the evidence database is important
- Hybrid blockchains are a necessity for scalability
- Monetary incentives are something to integrate to let the system into a better fruition
- Most of the current available literature does not have a practical, scalable solution yet.
- Infrastructure of BD is not yet ready to adopt this

5.2 Significance of the findings

It is necessary to focus on what is going to be the most efficient, long-term and cost-worthy outcome when it comes to storing massive amounts of data into a blockchain architecture. As we know, the transactions within a blockchain can get computationally expensive and it may wear out a system if the already established infrastructure is not sound enough. So, we have to think it from the bottom-up.

Secondly, the narrow-down of the findings may help future researchers to get an idea of what to focus on and what to avoid in terms of practicality, volatility and proper scalability and maintainability. So, the comparative, compilation and bringing down of the options at hand can be considered as a contribution.

Thirdly, The analysis shows that the identification of the stakeholders and participators in an evidence collection system is as significant as the mechanism that lets them have access to it. So conducting an analysis on each unique judiciary system before implementing is a must

5.3 Limitations

5.3.1 Shortcomings of the Available Literature

- No Practical Implementation publicly available
- No feasibility analysis
- Does not have much solution in terms of different type of data
- Does not shed much light on fail-safety of a system (such as node failure)

5.3.2 Shortcomings of the Available implementations

- Little to no work available on hybrid blockchain
- Issues on using different data types
- Frameworks and usage tools and subjects to constant changes
- Dependency issues among tools and frameworks makes it harder to work with

5.4 Suggestions

- Provide identity protection for evidence providers either by routing the transactions through onion/tor addresses, or by encrypting the identity of the provider.
- Establish a blockchain based system where transaction fees for uploading files are low or free.
- Combine the chain of custody (E.g. Forensic chain) with a hybrid architecture (E.g. hot-cold blockchain) to maximize security, scalability and computational benefits

Chapter 6

Conclusions and Future Work

6.1 Conclusions

The blockchain has the potential to bring a significant turnover to the technology world and it is a necessity that we apply its benefits to appropriate applications for the enhancement our community requires. And evidence collection is a very important one among them. And so, a scalable, secure and policy-adept blockchain based data collection system is a necessity for the betterment of the nation and the justice judiciary system.

6.2 Future Work

Here are the works we hope to cover in the future :

- Have a full-scale blockchain based evidence collection system.
- Ensure proper scalability of the system.
- Analyze and strengthen all the security aspects related to the system.
- Conduct a survey among authorizing law-enforcement and judiciary personnel for the possibility of putting it to official governmental usage.
- Combine different methods and mechanisms associated with the criteria of such a system to provide maximum efficiency
- Cover all the judiciary policies, making the system compliant with it
- Performance evaluation for different systems
- Data collection, survey and feasibility study for Bangladesh

References

- [1] F. M. Bencic and I. P. Zarko, "Distributed ledger technology: Blockchain compared to directed acyclic graph," in *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, Jul. 2018. [Online]. Available: <https://doi.org/10.1109/icdcs.2018.00171>
- [2] M. M. Hossain, R. Hasan, and S. Zawoad, "Probe-iot: A public digital ledger based forensic investigation framework for iot." in *INFOCOM workshops*, 2018, pp. 1–2.
- [3] A. Shahaab, C. Hewage, and I. Khan, "Preventing spoliation of evidence with blockchain: A perspective from south asia," in *2021 The 3rd International Conference on Blockchain Technology*, 2021, pp. 45–52.
- [4] Y. Aumann and Y. Lindell, "Security against covert adversaries: Efficient protocols for realistic adversaries," *Journal of Cryptology*, vol. 23, no. 2, pp. 281–343, 2010.
- [5] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, and P. Rimba, "A taxonomy of blockchain-based systems for architecture design," in *2017 IEEE international conference on software architecture (ICSA)*. IEEE, 2017, pp. 243–252.
- [6] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE symposium on security and privacy (SP)*. IEEE, 2016, pp. 839–858.
- [7] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," in *2014 USENIX Annual Technical Conference (Usenix ATC 14)*, 2014, pp. 305–319.
- [8] A. H. Lone and R. N. Mir, "Forensic-chain: Blockchain based digital forensics chain of custody with poc in hyperledger composer," *Digital investigation*, vol. 28, pp. 44–55, 2019.
- [9] I. Eyal, A. E. Gencer, E. G. Sirer, and R. V. Renesse, "Bitcoin-ng: A scalable blockchain protocol," in *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*. Santa Clara, CA: USENIX Association, Mar. 2016, pp. 45–59. [Online]. Available: <https://www.usenix.org/conference/nsdi16/technical-sessions/presentation/eyal>

- [10] Z. Tian, M. Li, M. Qiu, Y. Sun, and S. Su, "Block-DEF: A secure digital evidence framework using blockchain," *Information Sciences*, vol. 491, pp. 151–165, Jul. 2019. [Online]. Available: <https://doi.org/10.1016/j.ins.2019.04.011>
- [11] D. Kim, S.-Y. Ihm, and Y. Son, "Two-level blockchain system for digital crime evidence management," *Sensors*, vol. 21, no. 9, p. 3051, Apr. 2021. [Online]. Available: <https://doi.org/10.3390/s21093051>
- [12] F.-C. Cheng, "Automatic and secure wi-fi connection mechanisms for iot end-devices and gateways," in *International conference for emerging technologies in computing*. Springer, 2018, pp. 98–106.
- [13] C. Koliass, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.
- [14] A. MacDermott, T. Baker, and Q. Shi, "Iot forensics: Challenges for the iot era," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE, 2018, pp. 1–5.
- [15] T. D. Nguyen, S. Marchal, M. Miettinen, M. H. Dang, N. Asokan, and A.-R. Sadeghi, "Diot: A crowdsourced self-learning approach for detecting compromised iot devices," *arXiv preprint arXiv:1804.07474*, 2018.
- [16] H. Haddadi, V. Christophides, R. Teixeira, K. Cho, S. Suzuki, and A. Perrig, "Siotome: An edge-isp collaborative architecture for iot security," *Proc. IoTSec*, 2018.
- [17] P. Andriotis, G. Oikonomou, and T. Tryfonas, "Forensic analysis of wireless networking evidence of android smartphones," in *2012 IEEE International Workshop on Information Forensics and Security (WIFS)*. IEEE, 2012, pp. 109–114.
- [18] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," *Future generation computer systems*, vol. 82, pp. 395–411, 2018.
- [19] O. Yousuf and R. N. Mir, "A survey on the internet of things security: State-of-art, architecture, issues and countermeasures," *Information & Computer Security*, 2019.
- [20] S. Bonomi, M. Casini, and C. Ciccotelli, "B-coc: A blockchain-based chain of custody for evidences management in digital forensics," *arXiv preprint arXiv:1807.10359*, 2018.
- [21] A. Nieto, R. Roman, and J. Lopez, "Digital witness: Safeguarding digital evidence by using secure architectures in personal devices," *IEEE Network*, vol. 30, no. 6, pp. 34–41, 2016.
- [22] R. C. Merkle, "A digital signature based on a conventional encryption function," in *Conference on the theory and application of cryptographic techniques*. Springer, 1987, pp. 369–378.

- [23] Y. Liu, K. Wang, Y. Lin, and W. Xu, “ $\mathsf{LightChain}$: A lightweight blockchain system for industrial internet of things,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3571–3581, Jun. 2019. [Online]. Available: <https://doi.org/10.1109/tii.2019.2904049>
- [24] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, “Blockchain for secure and efficient data sharing in vehicular edge computing and networks,” *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019. [Online]. Available: <https://doi.org/10.1109/jiot.2018.2875542>