Synopsis
on
A Secure Forensic Evidence Sharing Platform Using Blockchain Technology

Submitted in the partial fulfillment of the
Degree of Bachelor of Technology
(Computer Science and Engineering)

Submitted by
Avdhesh Chaudhary (02315002719)
Amar Sinha (04415002719)
Chirag Aggarwal (04615002719)

Under the supervision of
Mr. Vikrant Shokeen
(Assistant Professor CSE)

Department of Computer Science and Engineering
Maharaja Surajmal Institute of Technology
Janakpuri, New Delhi.

2019-23

INDEX

	Pg.No.
1. Abstract	1
2. Introduction	2
3. Literature review	3
4. Objectives	4
5. Research Methodology	5
6. Gantt chart	6
7. References	8

Abstract

With the increasing amount of digital evidence being used in legal proceedings, there is a growing need for a secure platform that can facilitate the sharing of evidence between parties involved in a case.

Traditional methods of sharing evidence, such as email or physical copies, are vulnerable to hacking, tampering, and loss. This often results in the evidence getting thrown out of court leading to denial of justice and loss of time in the court of law.

To address these concerns, blockchain technology offers a promising solution. By leveraging the decentralized and immutable nature of blockchain, a secure evidence sharing platform can ensure that evidence is tamper-proof, traceable, and only accessible to authorized parties. This abstract explores the need for such a platform, and the potential benefits of using blockchain technology to secure the sharing of evidence.

Introduction

With the increasing reliance on digital evidence in legal proceedings, there is a growing need for a secure and reliable platform that can facilitate the sharing of evidence between parties involved in a case. The traditional methods of sharing evidence, such as email or physical copies, are vulnerable to hacking, tampering, and loss. This poses a significant challenge to the integrity of the legal system, as the trustworthiness of the evidence is paramount in ensuring a fair and just outcome.

To address these concerns, blockchain technology offers a promising solution. The decentralized and immutable nature of blockchain makes it an ideal platform for secure evidence sharing. By leveraging blockchain, a secure platform can be developed that ensures the integrity of the evidence, while also providing traceability and transparency in the sharing process. This will help to establish trust between the parties involved in a case, and enhance the reliability of the legal system as a whole.

The objective of this project is to develop a secure evidence sharing platform based on blockchain technology. The platform will provide a secure and reliable way to share digital evidence in a way that is tamper-proof, traceable, and only accessible to authorized parties. The platform will leverage the benefits of blockchain to ensure the integrity of the evidence, while also providing a user-friendly interface for seamless sharing and collaboration. Overall, this project aims to enhance the reliability and trustworthiness of the legal system by providing a secure evidence sharing platform based on blockchain technology.

Literature Survey

Several studies have investigated the potential of blockchain technology for secure and reliable data sharing, including the sharing of evidence in legal proceedings.

A study by Vigna and Casey (2015) explored the use of blockchain technology for secure document verification and timestamping. The study demonstrated that blockchain can provide a tamper-proof and reliable way to verify the authenticity of documents and data.

Another study by Kshetri (2018) reviewed the potential of blockchain technology for securing digital identities and data sharing in various domains, including law enforcement and legal proceedings. The study highlighted the benefits of blockchain, including enhanced security, privacy, and transparency.

More recently, a study by Kwak and Lee (2020) proposed a blockchain-based evidence management system for criminal investigations. The system leveraged the immutability and transparency of blockchain to ensure the integrity of the evidence and provide a reliable chain of custody.

Overall, these studies demonstrate the potential of blockchain technology for secure evidence sharing in legal proceedings. However, more research is needed to develop practical and user-friendly solutions that can be widely adopted by legal professionals and stakeholders. This project aims to build upon the existing literature by developing a secure evidence sharing platform that leverages the benefits of blockchain technology while also addressing the practical needs of legal professionals.

Objectives

The objective of the project is to develop a secure evidence sharing platform based on blockchain technology that can facilitate reliable and tamper-proof sharing of digital evidence between parties involved in legal proceedings. The specific objectives of the project include:

1. Develop a blockchain-based platform for secure and reliable evidence sharing: The platform will be built on blockchain technology to ensure the immutability, traceability, and transparency of the evidence sharing process.

2. Implement user authentication and authorization mechanisms: The platform will include user authentication and authorization mechanisms to ensure that only authorized parties can access and share evidence.

3. Design an intuitive user interface: The platform will have a user-friendly interface that enables legal professionals to easily upload, share, and collaborate on digital evidence.

4. Ensure compliance with legal and regulatory requirements: The platform will comply with relevant legal and regulatory requirements to ensure the admissibility of the evidence in court.

5. Test and evaluate the platform: The platform will be tested and evaluated to ensure that it meets the needs of legal professionals and stakeholders.

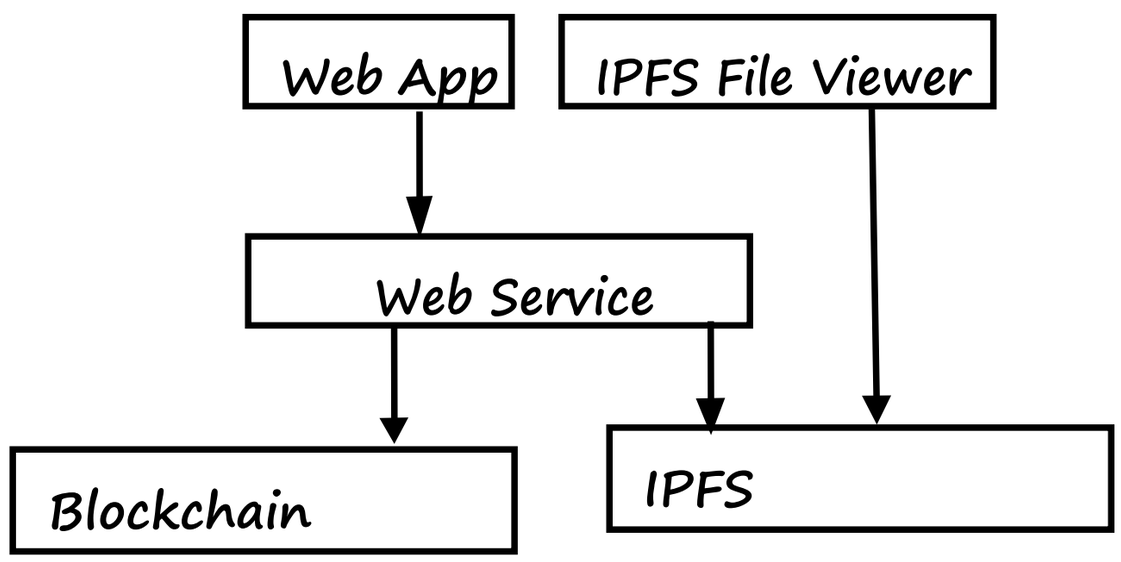
Methodology

Normally with a web application, you access a web application with your web browser. All the code for this application lives on a central web server, and interacts to a back-end (written in any programming language), which further interacts to a database. The blockchain application that we'll build works differently. Our implementation of storing file hash (SHA-256) in the private blockchain will be built upon ETH protocol keeping the file in a distributed file system – IPFS.

A quick explanation on how it has been structured.
At the top, there is a browser with two components.

- The first one – Web App – allows us to send a request to the hosted Web Service in a simple and clear way. This request received by the web service is processed and, as a result, data is pushed further to the blockchain and IPFS network. It handles two types of requests – the first which writes and the second which only reads and doesn't make any changes.

- The second component in a browser area is the IPFS File Viewer whichhelps to explore files stored in a distributed file system. It comes with our IPFS node configuration, and it can display a file or even play a movie if its extension is recognized by the system. IPFS File Viewer searches for file without any intermediaries, providing that it is fulfilled by user. He or she has to know the file's path or hash (these two terms can be used interchangeably) generated by the system, in order to view the file. The hash from IPFS is completely different from the one generated by the file content, therefore we store both in the smart contract.



Our blockchain application with NodeJS, React, Ganache, Truffle, Web3.js, and Solidity smartcontracts approach can be divided into following steps:

Front-End preparation:

The front-end required for this project would help the user to interact with the application. For the front-end, ReactJs, bootstrap and other libraries would be used.

Blockchain and Back-End Preparation:

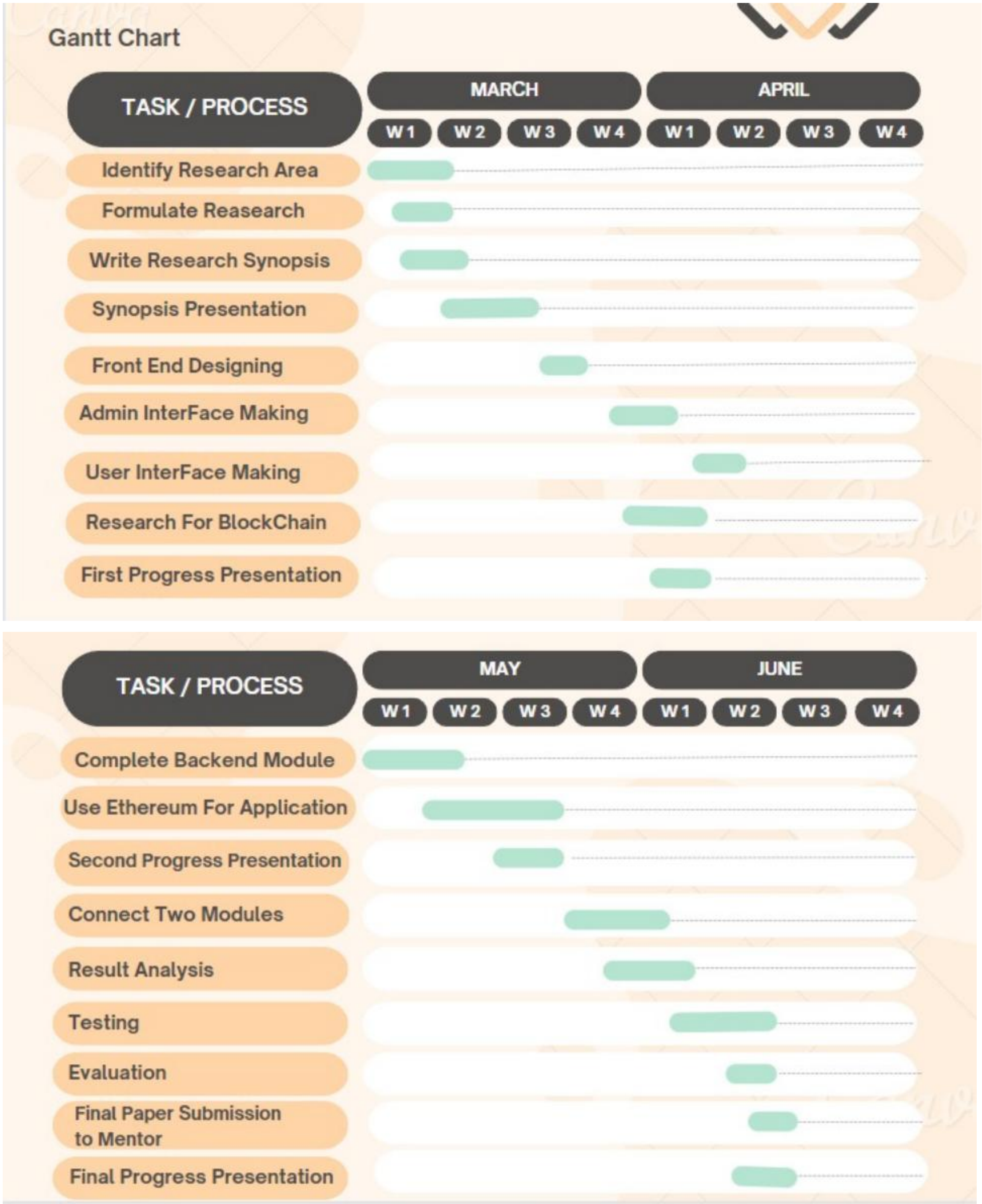
1. Smart contracts the building blocks we use to create blockchain applications. They are programs that we can write with source code and deploy to the blockchain. They are written in the Solidity programming language. Smart contracts are immutable, which means that once they've been created, they cannot change! Once a smart contract is deployed to a blockchain, its code cannot be updated like a normal application. That's because it represents a digital contract or agreement.

2. Ganache Personal Blockchain is a personal blockchain, which is a local development blockchain that can be used to mimic the behavior of a public blockchain.

3. NodeJS - Now that you have a private blockchain running, you need to configure your environment for developing smart contracts. The first dependency you'll need is NodePackage Manager, or NPM, which comes with Node.js.

4. Truffle Framework provides a suite of tools for developing Ethereum smart contacts with the Solidity programming language.

Gantt Chart


Gantt Chart
TASK / PROCESS
MARCH
APRIL
W1
W2
W3
W4
W1
W2
W3
W4
Identify Research Area
Formulate Reasearch
Write Research Synopsis
Synopsis Presentation
Front End Designing
Admin InterFace Making
User InterFace Making
Research For BlockChain
First Progress Presentation
TASK / PROCESS
MAY
JUNE
W1
W2
W3
W4
W1
W2
W3
W4
Complete Backend Module
Use Ethereum For Application
Second Progress Presentation
Connect Two Modules
Result Analysis
Testing
Evaluation
Final Paper Submission to Mentor
Final Progress Presentation

References

1. Prof. Renuka BS, Kusuma S, Blockchain based digital investigation framework, International Research Journal of Engineering and Technology (IRJET), June 2021.

2. Dr. Reshma Basu, Deeksha G, M Preethi, Triveni S, Blockchain Technology for securing forensic evidence, International Journal of Creative Research Thoughts,June 2022

3. Abdullah Al Omar, Shahriar Rahman, Report on the criminal record management system.conference paper 2018 December, research gate.

4. Dr.S. Harihara Gopalan and S. Akila Suba . Forensicchain: Blockchain-based digital forensics chain of custody. Digital Investigation, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277- 3878, Volume-8, Issue-2S11, September2019.

5. Muqaddas Naz , Fahad A. Al-zahrani, Rabiya Khalid, Nadeem Javaid 1, Ali Mustafa Qamar,Muhammad Khalil Afzal and Muhammad Shafiq. A Secure Data Sharing Platform UsingBlockchain and Interplanetary File System, Sustainability, December 2019

6. Steichen, M.; Fiz Pontiveros, B.; Norvill, R.; Shbair, W. Blockchain-Based, Decentralized Access Control for IPFS. In Proceedings of the 2018 IEEE International Conference on Blockchain (Blockchain-2018), Halifax, NS, Canada, 30 July 2018–3 August 2018; pp. 1499–1506

7. Liu, “How the blockchain could transform the process of documenting electronic chain ofcustody.”