PaperChain

Dissertation submitted to

Shri Ramdeobaba College of Engineering & Management, Nagpur

in partial fulfillment of requirement for the award of degree of

Bachelor of Technology (B.Tech)

In

COMPUTER SCIENCE AND ENGINEERING

By

Anushka Zade(02)

Nisha Jain(08)

Palak Agrawal(09)

Akshat Deshmukh(24)

Of

VI Semester

Guide

Prof. Nisha Dable

CoGuide

Prof. Ashwini Gedekar

Department of Computer Science and Engineering

Shri Ramdeobaba College of Engineering & Management, Nagpur 440 013

(An Autonomous Institute affiliated to Rashtrasant Tukdoji Maharaj Nagpur University Nagpur)

April 2024

PaperChain

Dissertation submitted to

Shri Ramdeobaba College of Engineering & Management, Nagpur

in partial fulfillment of requirement for the award of degree of

Bachelor of Technology (B.Tech)

In

COMPUTER SCIENCE AND ENGINEERING

By

Anushka Zade(02)

Nisha Jain(08)

Palak Agrawal(09)

Akshat Deshmukh(24)

Of

VI Semester

Guide

Prof. Nisha Dable

CoGuide

Prof. Ashwini Gedekar

Department of Computer Science and Engineering

Shri Ramdeobaba College of Engineering & Management, Nagpur 440 013

(An Autonomous Institute affiliated to Rashtrasant Tukdoji Maharaj Nagpur University Nagpur)

April 2024

SHRI RAMDEOBABA COLLEGE OF ENGINEERING MANAGEMENT, NAGPUR

(An Autonomous Institute affiliated to Rashtrasant Tukdoji Maharaj Nagpur University Nagpur)

Department of Computer Science and Engineering

CERTIFICATE

This is to certify that the Thesis on **"PaperChain"** is a Bonafide work of Anushka Zade, Nisha Jain, Palak Agrawal and Akshat Deshmukh, submitted to the Rashtrasant Tukdoji Maharaj Nagpur University, Nagpur in partial fulfillment of the award of a Degree of Bachelor of Technology (B.Tech), in Computer Science and Engineering. It has been carried out at the Department of Computer Science and Engineering, Shri Ramdeobaba College of Engineering and Management, Nagpur during the academic year 2023-2024.

Date:

Place: Nagpur

Prof. Nisha Dable Project Guide Department of Computer Science and Engineering	Dr. R. Hablani Head of Department Department of Computer Science and Engineering

Dr. R. S. Pande
Principal

DECLARATION

We hereby declare that the thesis titled "**PaperChain**" submitted herein, has been carried out in the Department of Computer Science and Engineering of Shri Ramdeobaba College of Engineering and Management, Nagpur. The work is original and has not been submitted earlier as a whole or part for the award of any degree/diploma at this or any other institution / University.

Date:

Place: Nagpur

Name, roll no and sign of all students

Anushka Zade(02) _____

Nisha Jain(08) _____

Palak Agrawal(09) _____

Akshat Deshmukh(24) _____

APPROVAL SHEET

This report entitled **"PaperChain"** by **Anushka Zade, Nisha Jain, Palak Agrawal and Akshat Deshmukh** is approved for the degree of Bachelor of Technology (B.Tech).

Prof. Nisha Dable Project Guide	External Examiner

Dr. R. Hablani
Head of Department, CSE

Date:

Place: Nagpur

ACKNOWLEDGEMENTS

Any project small or big is not possible without the guidance and help of various people in various fields who have always given their valuable advice and support. We sincerely appreciate the inspiration, guidance, dedication and positivity shown by all those people who in some or the other way have contributed in making this project a success.

We are grateful to our Project Guide Prof. Nisha Dable ma'am who was always there to solve every small doubt about the project. She not only provided us the right path towards approaching our goal, but was also there to provide moral support and valuable inputs. We are indebted to our Seniors and Head of Department, Dr. R. Hablani sir, who gave us a positive response and provided us various approaches through which the project could be implemented and developed further.

We are thankful to all our panelists and supervisors who were present during the project presentation and submission for their valuable comments and advice which also helped us in improving our presentation and communication skills.

By-

Anushka Zade(02)

Nisha Jain(08)

Palak Agrawal(09)

Akshat Deshmukh(24)

ABSTRACT

Effective and secure management of land records is crucial for ensuring property ownership integrity. Outdated systems, which are often inefficient and vulnerable to fraud, require new and creative solutions. This is where PaperChain comes in - a trailblazing blockchain platform that is set to transform land record management. By utilizing the powerful infrastructure of Filecoin's virtual machine and Interplanetary Consensus (IPC) platforms, PaperChain creates a decentralized and tamper-proof environment.

PaperChain offers distinct interfaces for users, enabling seamless document upload and verification processes. Transactions are conducted using the **PaperChain cryptocurrency (PRC)**, with authentication ensured through **Metamask** integration. Furthermore, smart contracts play a pivotal role in automating processes and ensuring adherence to predefined rules and agreements.

Advanced document validation mechanisms, coupled with cryptographic techniques, safeguard against tampering and duplication attempts, bolstering the platform's security. The integration of **Filecoin's** infrastructure ensures reliable decentralized storage, further enhancing the platform's resilience.

PaperChain represents a paradigm shift in land record management, promising streamlined processes, heightened security, and increased trust in land administration systems. Its utilization of Filecoin, **smart contracts**, and advanced cryptographic techniques positions it as a frontrunner in the quest for efficient and secure land record management solutions.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 Background

The management of property ownership and acquisition has historically relied on manual, paper-based record-keeping systems and centralized databases maintained by various government agencies and institutions. This fragmented approach often leads to inefficiency, inconsistency, and vulnerability in property transactions, undermining the integrity and reliability of land records. Moreover, the reliance on centralized systems exposes land administration systems to risks such as data breaches, corruption, and manipulation. These challenges highlights the need for a more robust and resilient approach to property ownership and acquisition management.

1.2 Motivation

The limitations of traditional land administration systems underscore the importance of exploring innovative solutions to enhance the efficiency, transparency, and security of property transactions. The blockchain technology presents a promising opportunity to address these challenges by providing a decentralized, transparent, and immutable platform for recording and verifying property transactions. By leveraging blockchain's distributed ledger technology, cryptographic techniques, and smart contracts, it becomes possible to create a unified source of truth for land records, streamline verification processes, and mitigate the risk of fraud and disputes. The motivation behind this project is to harness the potential of blockchain technology to revolutionize property ownership and acquisition management, ultimately improving the integrity, efficiency, and security of real estate transactions.

1.3 Objective

1. Develop PaperChain, a blockchain-based solution for managing land records:

- Design a scalable blockchain architecture using Filecoin's virtual machine and IPC platform.
- Implement smart contracts to handle land record transactions securely and efficiently.

2.Ensure integrity, transparency, and security of land records:

- Utilize decentralized storage and cryptographic verification to safeguard against tampering and ensure data integrity.
- Implement consensus mechanisms to validate transactions and maintain network integrity.

3. Provide user-friendly interfaces for issuers and verifiers:

- Design separate interfaces tailored to the needs of issuers and verifiers for streamlined document upload and verification.
- Customize access controls to ensure data confidentiality and integrity based on user roles.

4. Integrate Metamask for secure transactions with PRC:

- Integrate Metamask to enable secure transactions using the PaperChain cryptocurrency (PRC).
- Develop seamless integration protocols for user convenience and security.

5. Implement document validation mechanisms:

- Develop algorithms for comprehensive document validation to prevent tampering and duplication.
- Utilize digital signatures and timestamping for establishing document authenticity and traceability.

CHAPTER 2
LITERATURE REVIEW

In the past few years, there has been significant progress made in the area of blockchain. The use of blockchain technology has the potential to revolutionize the educational system by providing individuals with innovative and cost-effective ways to learn, as well as by altering the way teachers and students work together. Additionally, blockchain technology can be utilized for the issuing of unchangeable digital certificates, and it can enhance the present limitations of the existing certificate verification systems by making them quicker, more reliable, and independent of the central authority. The application of blockchain in the context of education has generated significant scientific interest in this field. Nonetheless, research endeavors on the adoption of blockchain in the verification of academic credentials are still in the development phase. In order to shed more light on the field, in this paper we focus on extensively reviewing the body of knowledge on blockchain-based systems for academic certificate verification. Hence, the purpose of this survey is to compile all relevant research into a systematic literature review, highlighting the key contributions from various researchers throughout the years with a focus on the past, present, and future. Based on the findings of this review, we provide some recommendations for future research directions and practical applications that can assist researchers, policymakers, and practitioners in the field.

CHAPTER 3
SYSTEM ARCHITECTURE

3.1 FileCoin VM:

3.1.1 Filecoin Virtual Machine (FVM) Launch: In March 2023, the FVM launch kicked off step 3 in the Filecoin Masterplan and enabled the support of smart contracts and user programmability on the Filecoin network. As of December 2023, 200+ projects are building on FVM with about 635,000 wallets created and 2,400+ unique contracts deployed, further solidifying Filecoin's position as the Layer-1 blockchain uniquely poised to power an open data economy.

3.1.2 Storage Growth: Another major goal of the Filecoin network is to onboard and safeguard humanity's data. In contribution to that goal, since January 2023, total client data onboarded has quadrupled and grown 19x in the last 18 months totaling 2 million terabytes of client data stored on the Filecoin network.

3.1.3 Filecoin Retrievals and Data Availability: As a stride to improve retrievability of Filecoin data, projects such as Boost, Lassie and Station were introduced in 2023 with a shared goal to simplify the retrieval process. Via better tooling and visibility into Filecoin data retrievals, the community can now monitor retrieval success rates and speed. Since its inception, Boost has emerged as the dominant storage node for Filecoin storage providers (SPs), marking a significant milestone in the evolution of Filecoin's storage infrastructure.

3.2 IPC:

InterPlanetary Consensus (IPC) is a protocol used in blockchain networks that allows participants to agree on the distributed ledger's state. It helps coordinate transactions and record them in a secure, decentralized manner without the need for a central authority.

3.2.1 How IPC Works:

IPC allows transactions and smart contracts to be executed across different blockchains securely and decentralized.

At its core, IPC leverages validator nodes that participate across multiple blockchains to relay transactions and data between chains. These validator nodes stake tokens and validate transactions on each blockchain they are part of.

When a transaction needs to occur between two different blockchains, it is submitted to the IPC protocol. The protocol routes the transaction to validator nodes staked on both chains. The validators verify the transaction is valid on both chains and if so, commit the transaction.

This allows assets, data, and smart contracts to execute seamlessly across blockchain platforms. Developers can leverage multiple blockchains while users only need to interact with one application layer.

3.2.2 Advantages of IPC:

Scalability: IPC enables much greater scalability than previous models. Through innovations like sharding, parallel processing, and hierarchical consensus structures, IPC blockchains can achieve thousands of transactions per second, making them viable for large-scale adoption.

Interoperability: IPC enables interoperability between different blockchains through standardized communication protocols. This allows assets, data, and transactions to flow seamlessly between IPC-based blockchains.

Increased Security: Attacks like 51% of attacks become orders of magnitude harder under IPC consensus rules. The multi-layer structure also provides security through redundancy. These security advantages will be essential as blockchain networks begin handling valuable transactions on a global scale during the next crypto boom.

3.3 Smart Contracts:

A smart contract is a digital agreement signed and stored on a blockchain network that executes automatically when the contract's terms and conditions (T&C) are met; the T&C is written in blockchain-specific programming languages like Solidity.

3.3.1 Functioning of Smart Contracts:

Agreement: The parties wanting to conduct business or exchange products or services must concur on the arrangement's terms and conditions. Furthermore, they must determine how a smart contract will operate, including the criteria that must be fulfilled for the agreement to be fulfilled.

Contract creation: Participants in a transaction may create a smart contract in many ways, including building it themselves or collaborating with a smart contract provider. The provisions of the contract are coded in a programming language. During this stage, verifying the contract's security thoroughly is critical.

Deployment: When the contract has been finalized, it must be published on the blockchain. The smart contract is uploaded to the blockchain in the same way as regular crypto transactions, with the code inserted into the data field of the exchange. Once the transaction has been verified, it's deemed active on the blockchain and cannot be reversed or amended.

Monitoring conditions: A smart contract runs by tracking the blockchain or a different reliable source for predetermined conditions or prompts. These triggers can be just about anything that can be digitally verified, like a date attained, a payment made, etc.

Execution: When the trigger parameters are met, the smart contract is activated as per the "if/when…then…" statement. This may implement only one or multiple actions, like passing funds to a vendor or registering the buyer's possession of an asset.

Recording: Contract execution results are promptly published on the blockchain.The blockchain system verifies the actions taken, logs their completion as an exchange, and stores the concluded agreement on the blockchain. This document is available at all times.

3.4 MetaMask:

MetaMask is a software cryptocurrency wallet used to interact with the Ethereum blockchain. It allows users to access their Ethereum wallet through a browser extension or mobile app, which can then be used to interact with decentralized applications.

Websites or other decentralized applications are able to connect, authenticate and/or integrate other smart contract functionality with a user's MetaMask wallet (and any other similar blockchain wallet browser extensions) via java script code that allows the website to send action prompts, signature requests, or transaction requests to the user through MetaMask as an intermediary.

CHAPTER 4
WORKFLOW

4.1 TechStack:

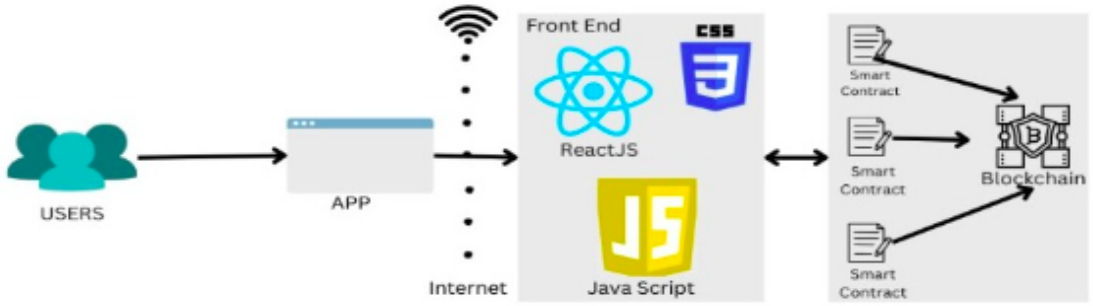

Figure 4.1- Tech Stack

Blockchain Platform: Filecoin chosen for document verification and file storage.

Front-end Development: React.js used for user interface development.

Smart Contracts: Remix IDE to determine the deployed smart contract transaction and execution costs required for our system to operate.

Integration: The ABI interface is processed by the Web3 provider instance for contract deployment.

4.2 Implementation Architecture:

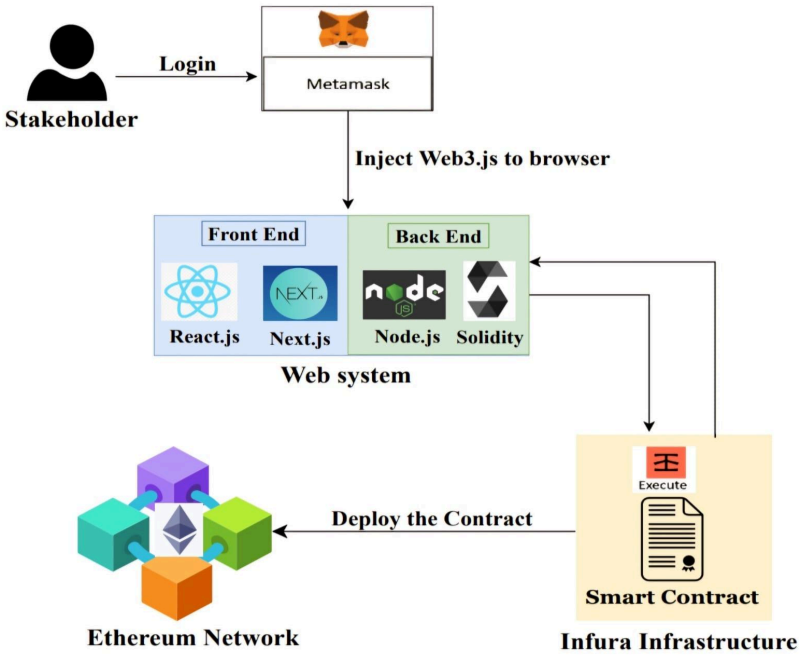

Figure 4.2.1- Implementation Architecture

The user first login as an issuer and connects its MetaMask wallet to PaperChain network which contains tFIL.

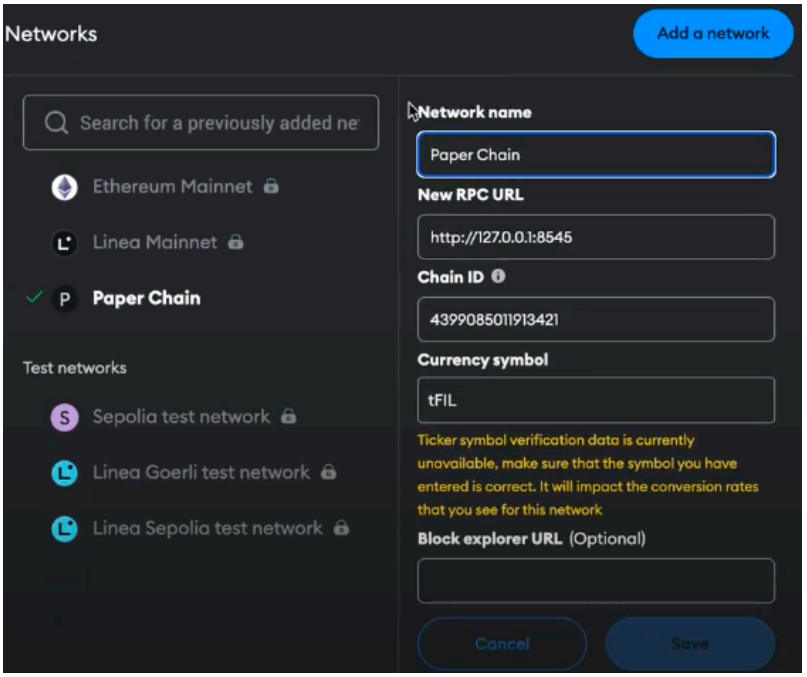

Figure 4.2.2- Add PaperChain as network

The Chain Id is obtained by deploying the IPC subnet on the host's machine.

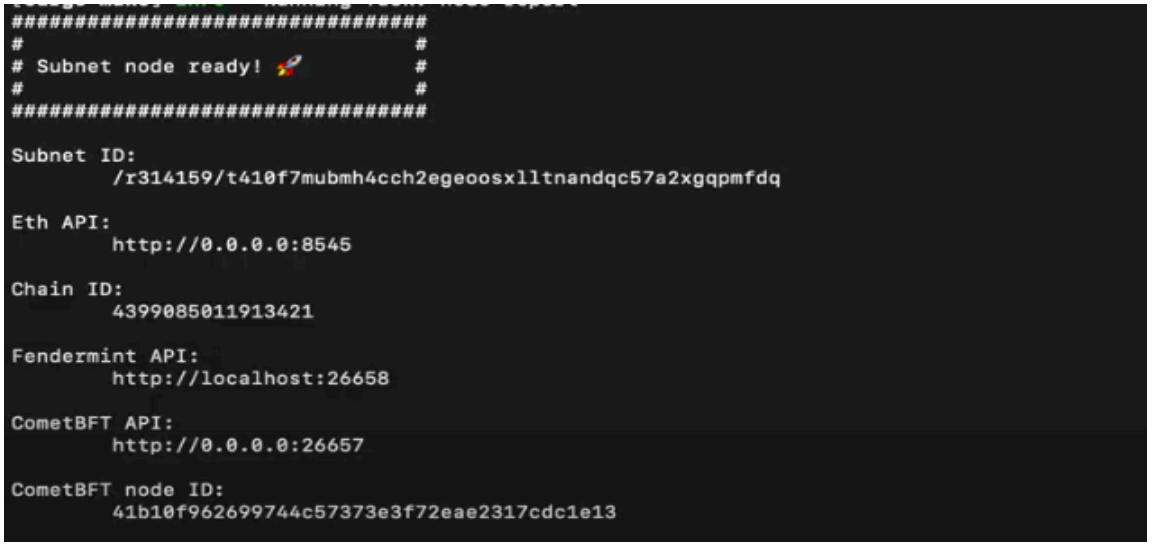

Figure 4.2.3- Subnet node

The frontend created using ReactJs and on backend the smart contract is written in Solidity is compiled and deployed on Remix IDE by intejecting MetaMask as Provider.

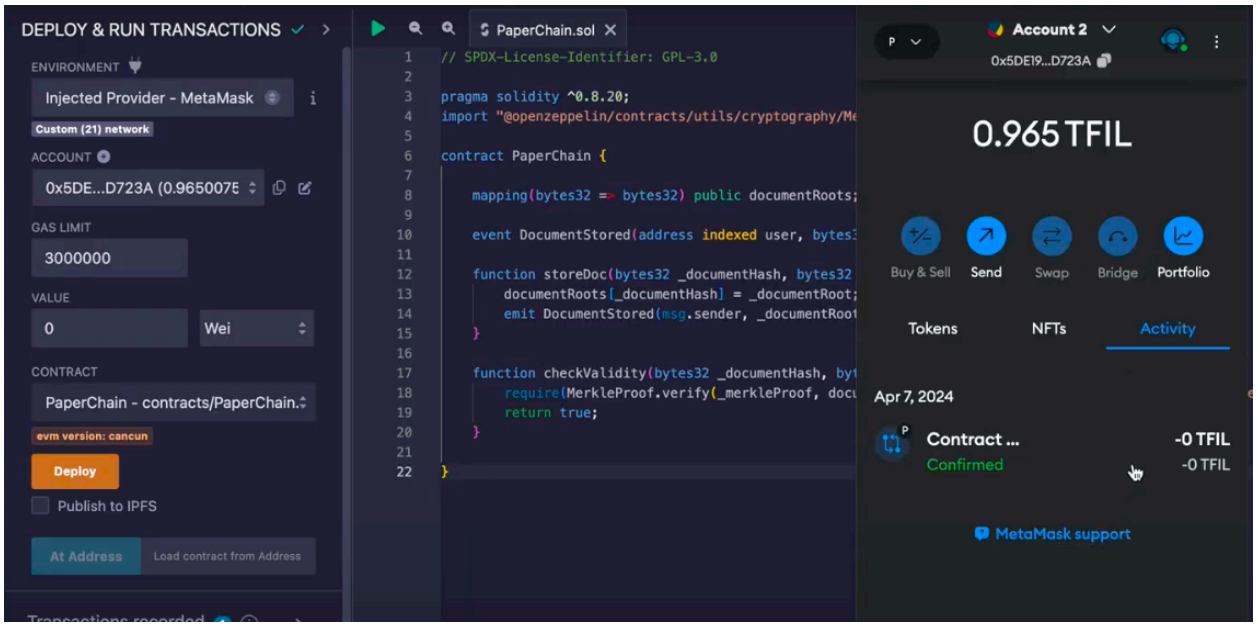

Figure 4.2.4- Deployment of contract on Remix IDE

Figure 4.2.5- Integration using PaperChainAddress

This contract is integrated to the IPC subnet by updating the PaperChainAddress i.e. the transaction id of the deployed contract in the contract folder.

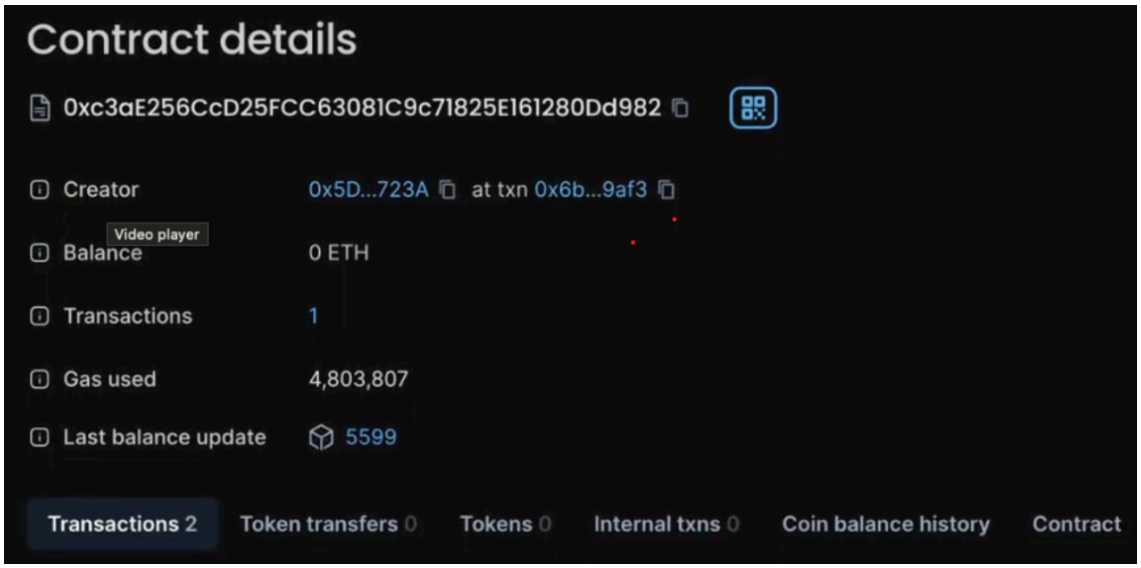

Figure 4.2.6- Exploration of created blocks

These transactions can be traced by using chain explorer for the deployed smart contract.

4.3 Mechanism:

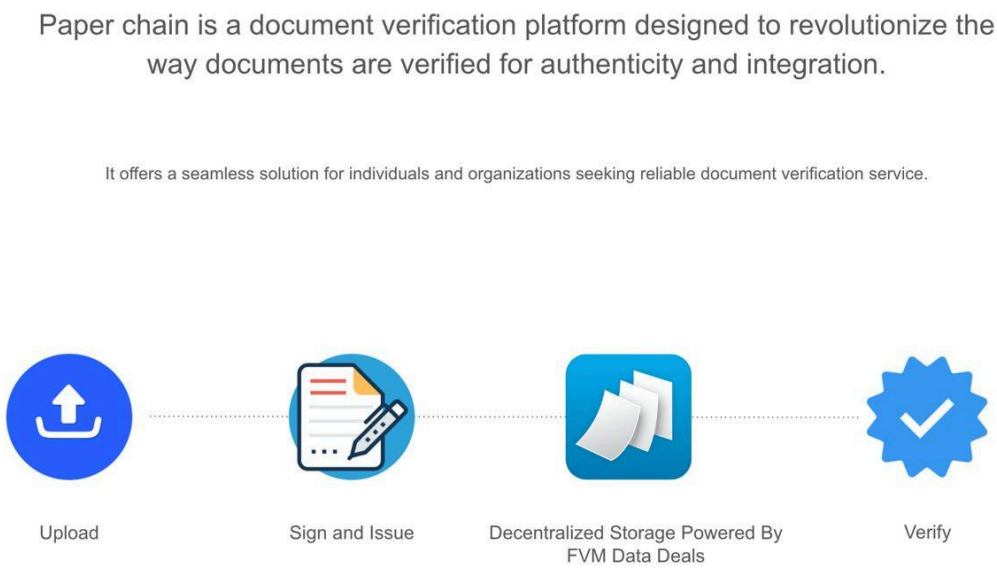

Figure 4.3- Steps for verification

The document verification and authentication is completed by PaperChain in following steps:

1. The issuer will first register and then proceed for login for their respective roles like issuer and verifier.
2. Then the document will be uploaded by the issuer in the system and will be digitally signed using the written algorithm. This helps in increasing the efficiency and eliminating errors and frauds in the system.
3. To verify the authenticity of a document the verifier will upload a document and if this is digitally signed it will map the hash value and will give a successful command prompt if it is mapped correctly.
4. The transaction will be reflected in the digital wallet and the car file will be generated.

Hence, completing the verification process.

4.3.1 User Interface:

A) Issuer Login:

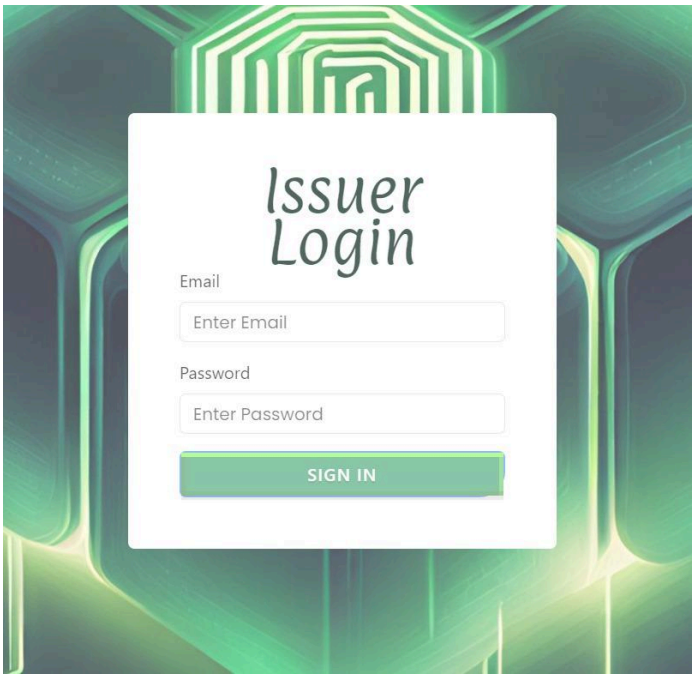

Figure 4.3.1A- Issuer Login

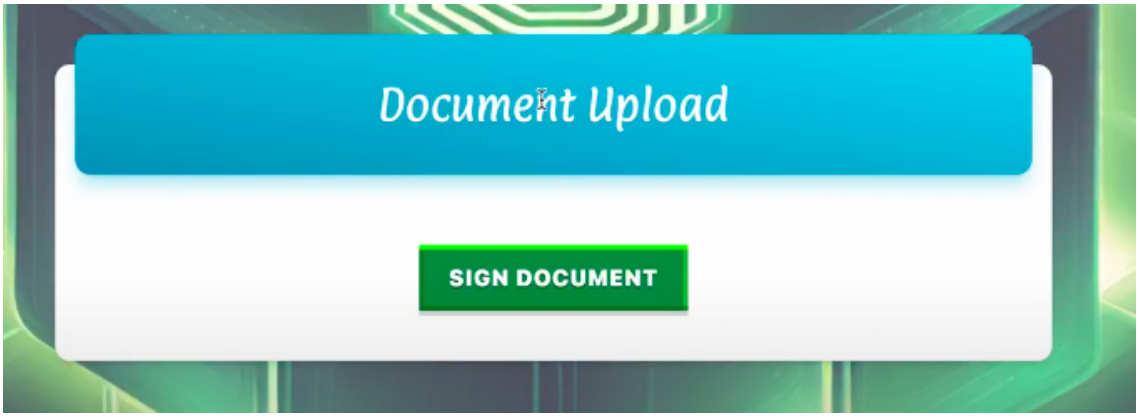

Figure 4.3.2A- Upload Document & Sign

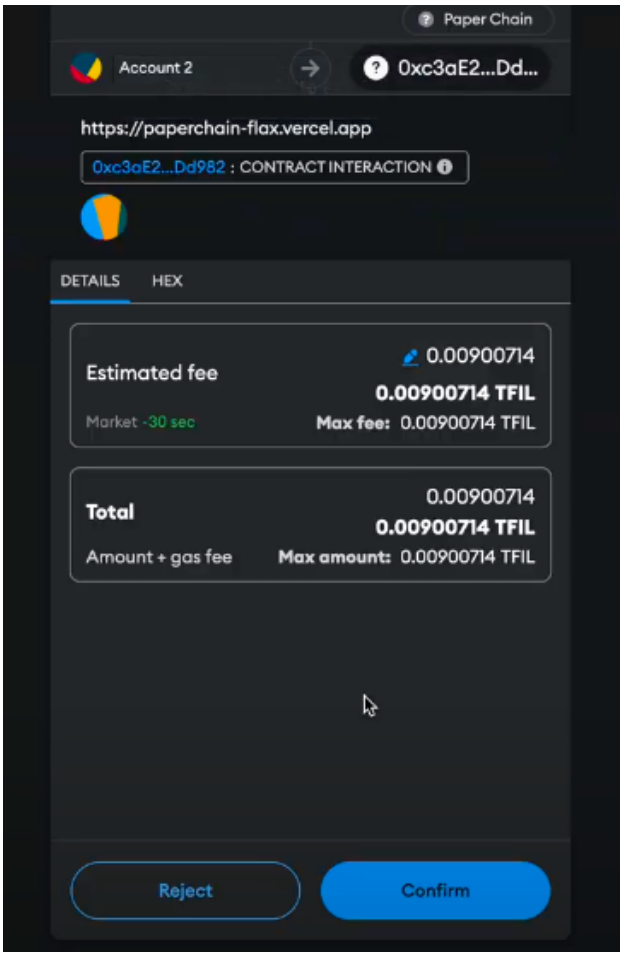

Figure 4.3.3A- MetaMask Transaction

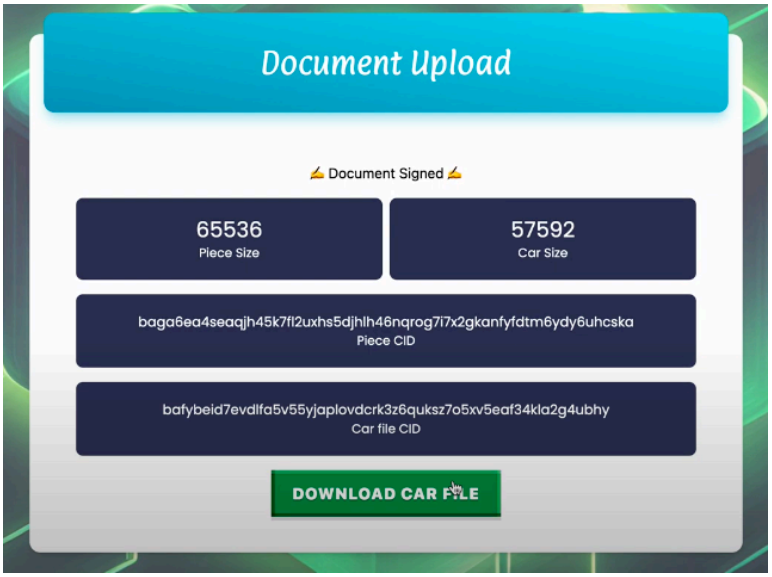

Figure 4.3.4A- Successful document updoaded

B) Verifier Login:

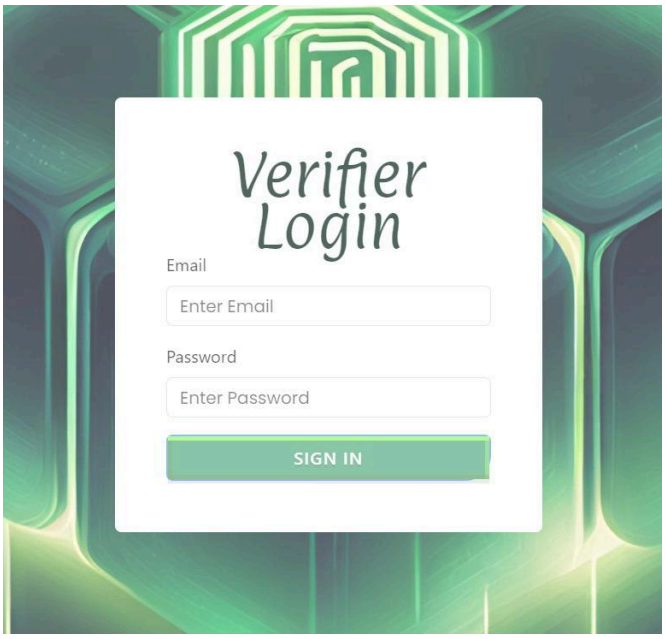

Figure 4.3.1B- Verifier Login

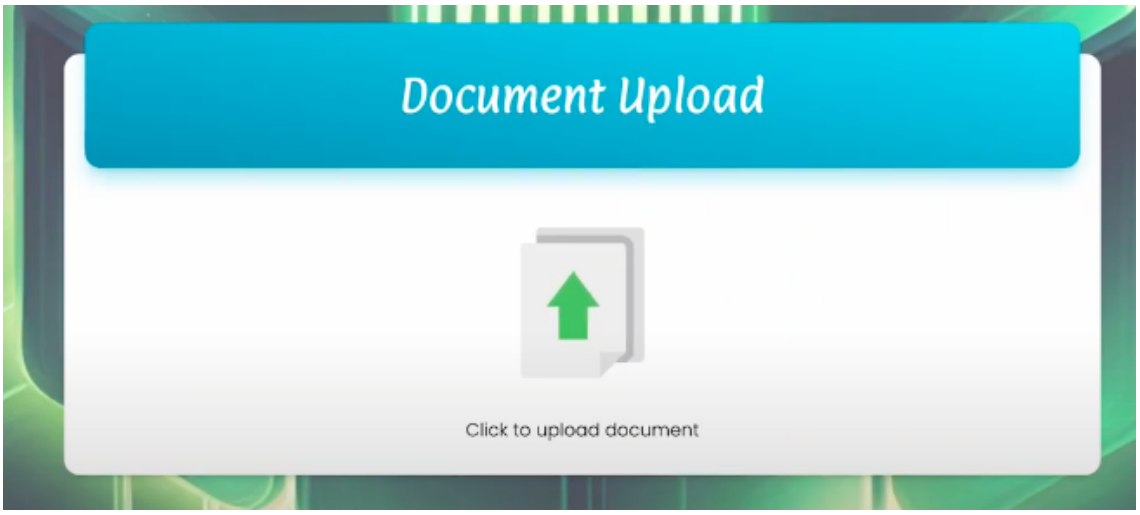

Figure 4.3.2B- Upload Document

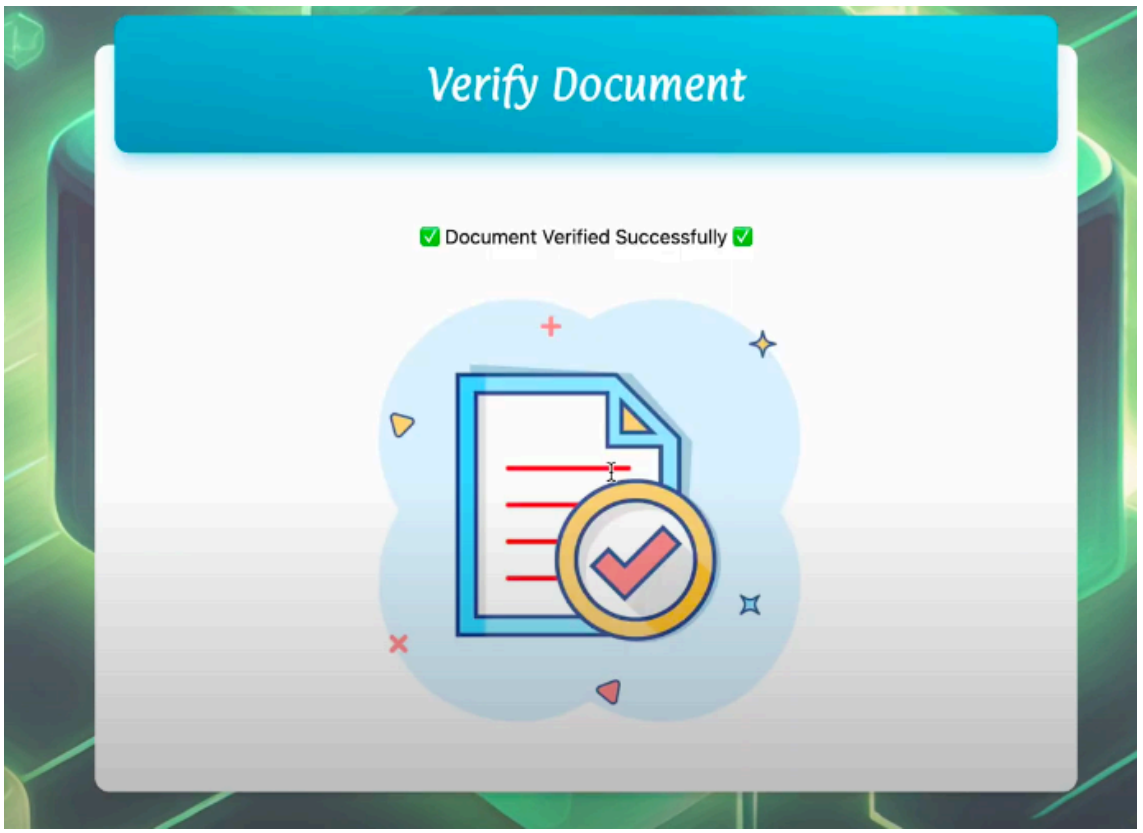

Figure 4.3.3B- Verified document uploaded

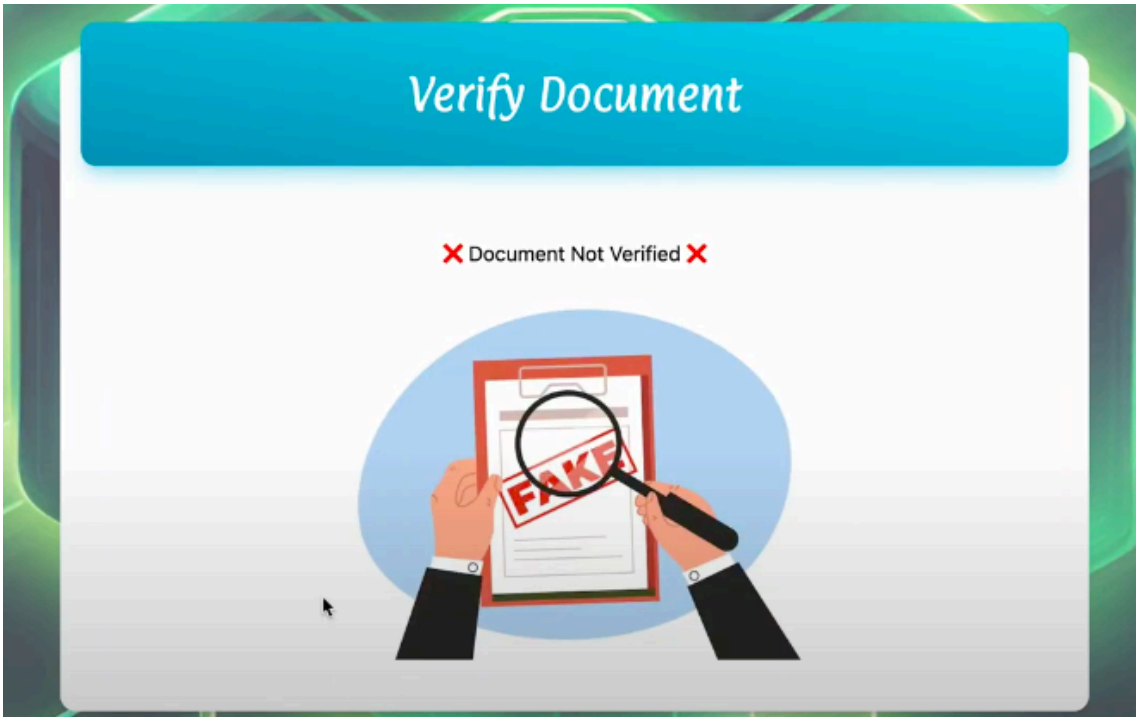

Figure 4.3.4B- Fake document uploaded

4.4 : Verification Procedure:

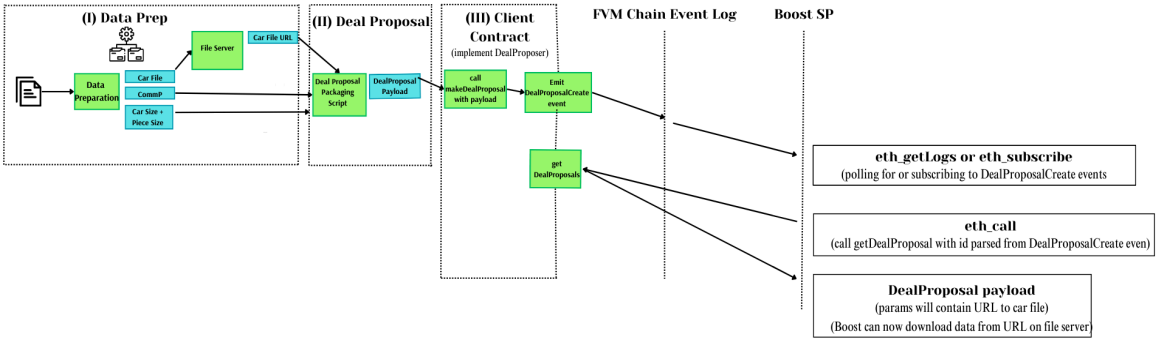

Figure 4.4- Verification Process

This diagram illustrates the overall flow and components involved in a data handling and distribution process, likely within a distributed system or service.

Data Preparation (I), where data is collected from a source and stored in a car file (compressed format) on a file server.

Deal Proposal stage (II), a Deal Proposal Payload is packaged, containing information about the car file.

Deal Proposal Contract component (III) then implements the DealProposal process. It takes the DealProposal Payload as input, creates a DealProposalCreate event, and emits this event.

EVM Chain Event Log (IV) logs and tracks the DealProposalCreate event.

The Boost SP component can then get or subscribe to the DealProposalCreate events. It can call getDealProposal with the parsed event details to retrieve the DealProposal payload. This payload contains the URL to the car file on the file server, allowing the Boost SP to download the data from that URL.

In summary, the flow involves data preparation, packaging a deal proposal with file metadata, creating and logging an event with the proposal details, and finally enabling a subscriber (Boost SP) to access and download the actual data file using the information from the logged event.

CHAPTER 5
CONCLUSION

5.1 Application:

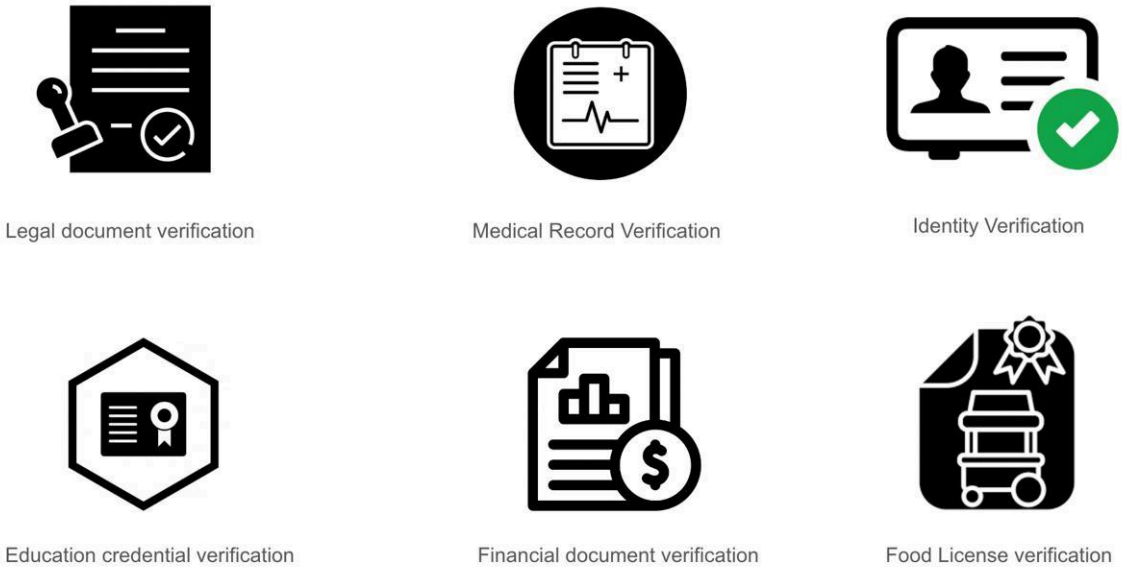

Figure 5.1 - Applications of PaperChain

PaperChain offers an extensive solution to document verification and authentication that spans across a number of domains, which include legal documents, medical records, identity verification, college degrees as well as financial among others. PaperChain then simplifies the process by providing secure platforms for issuers and verifiers in various stages. By incorporating these technologies PaperChain enhances assurance, productivity as well as privacy during various document authentication processes undertaken by different sectors for detection of forgery and errors.

5.2 Conclusion:

In our proposed solution, PaperChain is a strong answer for the validation and verification of documents that range from legal papers to medical records, identity cards to financial reports. To keep sensitive data like land records PaperChain uses blockchain technology and smart contracts to maintain its integrity, transparency, and security.

The decentralized storage and cryptographic proof protect against tampering and fraud while maintaining data integrity. Document uploads are made easy by user-friendly portals designed specifically for issuers and verifiers that pay special attention to confidentiality and integrity. When used with Metamask, they secure transactions with the PaperChain cryptocurrency – making it both convenient and safe for end users. Additionally, digital signatures as well as timestamping are among the advanced document validation mechanisms that enhance authenticity as well as traceability of documents within the ecosystem of PaperChain.

As a result, PaperChain can be seen as an advanced solution for effective, safe, credible document verification in various fields.

5.3 Future Scope:

In the future, PaperChain has a great deal of room to grow and innovate in the field of document authentication and verification. Here are a few potential areas of use:

1. Extension into New businesses: PaperChain can extend its services to accommodate a wider range of businesses, including healthcare, education, and finance, despite its initial focus being on land records. As part of this growth, the platform would be tailored to meet the particular verification needs of every industry.

2. Enhanced Security Measures: To keep up with new threats, security measures must constantly change. This could involve multi-factor authentication, advanced encryption techniques, and biometric verification methods to strengthen the platform's defenses against unauthorized access and data breaches.

3. Interoperability with Other Platforms: To enable smooth data interchange and interoperability, promote compatibility with other blockchain platforms and systems. This would facilitate PaperChain's integration with current systems utilized by businesses, governments, and other entities, leading to a wider adoption rate.

4. Research and Development: Make continuous investments in this area to raise the functionality, scalability, and performance of the platform. This entails investigating novel consensus techniques, maximizing the performance of smart contracts, and improving user experience via creative UI/UX design.

By following these development paths, PaperChain will be able to maintain its position as the industry leader in document authentication and verification, spurring innovation and adding value for all parties involved.

References:

[1] https://filecoin.io/blog/#posts

[2] https://docs.ipc.space/quickstarts/deploy-a-subnet

[3] https://docs.ipc.space/user-guides/performing-transactions-in-a-subnet

[4]https://medium.com/@DSPA-Asia/to-infinity-and-beyond-interplanetary-consensus-readies-for-blastoff-in-the-next-crypto-boom-6f53baf5d7d9#:~:text=Introduction,need%20for%20a%20central%20authority

[5]https://www.researchgate.net/publication/368729051_BLRS_An_Automated_Land_Records_Management_System_Using_Blockchain_Technology