A Blockchain-Based Framework for Secure and Decentralized Document Integrity Using Filecoin and Smart Contract

Abhijeet R. Raipurkar
School of Computer Science & Engineering, Shri Ramdeobaba College of Engineering & Management, Ramdeobaba University, Nagpur
raipurkarar@rknec.edu

Anushka Zade
School of Computer Science & Engineering, Shri Ramdeobaba College of Engineering & Management, Ramdeobaba University, Nagpur
zadeaj_1@rknec.edu

Palak Agrawal
School of Computer Science & Engineering, Shri Ramdeobaba College of Engineering & Management, Ramdeobaba University, Nagpur
agrawalps_6@rknec.edu

Praful R. Pardhi
School of Computer Science & Engineering, Shri Ramdeobaba College of Engineering & Management, Ramdeobaba University, Nagpur
pardhipr@rknec.edu

Nisha Jain
School of Computer Science & Engineering, Shri Ramdeobaba College of Engineering & Management, Ramdeobaba University, Nagpur
jainn@rknec.edu

Akshat Deshmukh
School of Computer Science & Engineering, Shri Ramdeobaba College of Engineering & Management, Ramdeobaba University, Nagpur
deshmukhar@rknec.edu

Abstract — **This paper introduces PaperChain, a blockchain-based platform that addresses the inefficiencies, security vulnerabilities, and outdated processes inherent in traditional document management systems. Traditional systems struggle with issues like fraud, data breaches, and manual errors. PaperChain tackles these challenges with a decentralized approach using Filecoin's infrastructure and the Interplanetary Consensus (IPC) system. The platform provides a tamper-proof record-keeping environment, leveraging smart contracts for automation and PaperChain cryptocurrency (PRC) for transactions. The integration of MetaMask further simplifies authentication, while Filecoin's decentralized storage ensures advanced cryptographic validation mechanisms to protect against document tampering and duplication. PaperChain sets a new standard for secure and transparent document management in the digital age.**

Keywords— Filecoin Virtual Machine(FVM), Interplanetary Consensus(IPC), Decentralized Document Management, Blockchain, document integrity.

I. Introduction

The secure and efficient management of records is critical across various sectors, including finance, healthcare and legal documentation in today's digital era [1]. They have traditionally been in the form of manual systems, paper documents and managing organization or government databases. While record management has used them for years they are increasingly unable to meet all demands of a fast digitizing world. Such traditional systems are often inefficient, inconsistent and also vulnerable which can cause delays, mistakes and even fraudulent activities that could lead to loss of vital records' integrity and reliability [2].

The main challenges which affect the old ways are that they depend on databases which have centralization, they are costly places. Data breaches, corruption, unauthorized manipulation, and equally grave security threats are possible in centralized systems. In such systems all documents are kept in either one single area or a few sites and therefore they become too tempting for hackers or people within the organization itself who may wish to tamper with them. Moreover due to various manual record keeping processes involving paper, it opens up avenues for human mistakes, record duplications and loss or destruction of important papers. This illustrates just how traditional techniques cannot necessarily serve the fast-changing requirements of today's increasingly integrated world [3]. However, while many blockchain-based systems provide improvements, they also come with limitations. Existing solutions often lack scalability, suffer from high operational costs, and provide limited user interfaces for document verification. There is still a need for more comprehensive frameworks that offer better performance in terms of document retrieval speed, user accessibility, and scalability.

Fresh technologies for better, safer, and effective dealings with record-keeping have been investigated in pursuit of finding more reliable record-keeping systems. In this direction, blockchain technology has been found to be very promising in providing solutions to these problems. On the whole, blockchain functions by offering a decentralized, open, and unchangeable platform for transaction recording and validation, thus becoming useful for secure record-keeping. In contrast to traditional centralized systems, where all data are stored in one place, blockchain uses distributed ledgers that are spread through a network of computers which minimizes the chances of tampering or illegal alterations [4]. Additionally, each transaction or entry added onto the blockchain is secured cryptographically and subsequently linked to the prior one, resulting in an indelible chain of blocks that are exceptionally hard if not impossible to modify without being detected [5].

In real-world applications, blockchain has already demonstrated its efficacy in improving record management. For example, medical record systems like MedRec and government record systems have leveraged blockchain to enhance data integrity, transparency, and security. These use cases highlight blockchain's potential to reduce fraud and improve efficiency in document management systems.

Blockchain technology does not protect records alone; it is accompanied by several other advantages. It facilitates process automation through smart contracts. Smart contracts can be described as self-executing contracts whereby the performance takes place with each agreement's conditions clearly stated in lines of code. Under such agreements defaults are not entertained hence avoiding any need for middlemen who may involve themselves in between acts unless otherwise stated by parties involved in a contract. Therefore, it eliminates complexities involved during adulatory checks thus reducing administrative costs and minimizing risks of mistakes or controversies [6].

There is no doubt that using blockchain to manage records is an attractive proposition. The concept is aimed at creating a platform that not only secures records but also enhances the transparency and efficiency of the entire record management process. A decentralized, tamper-proof environment for managing and verifying records is provided by PaperChain, which is based on the blockchain. In addition to ensuring security and integrity of data, PaperChain offers user-friendly interfaces for easy uploading and verification of documents through Filecoin's Virtual Machine as well as Interplanetary Consensus platforms.

A. Motivations and Objectives

This study's goal is for PaperChain to investigate how it can revolutionize record management and verification by addressing the weaknesses inherent in old-fashioned methods. PaperChain aims to offer one integrated and secure solution for contemporary document control through the use of decentralized storage space, cryptographic tools, as well as smart contracts. In doing so, this investigation will show how blockchain technology can change recordkeeping practices transforming them into reliable, safer digital futures.

II. Related Work

The recent growth in blockchain technology has fostered the development of various systems providing secure and decentralized document management.

Zyskind, Nathan and Petland [7] presented a decentralized computation platform, Enigma, which guarantees privacy. This research finding adds to the current study by bringing out the need for decentralization and privacy in systems that are implemented using blockchains.

In the year 2020, the work by Jin, Su ,Yao and Wang [8] has presented a blockchain-based IPFS electronic medical record storage and access scheme. The study is of great essence in understanding the application of blockchain to ensure secure storage, mainly because it deals with a key document integrity framework.

Rahman et al [9] contributed a secure Internet of Health Things framework with improved provenance, courtesy of blockchain-managed federated learning. The study proposed the application of such a blockchain to guarantee greater provenance and robustness, which are required towards the integrity of documents.

Xu, Chen, Blasch [10] unveiled a decentralized access control strategy based on blockchain capabilities that provides situational awareness in space. This paper outlines the mechanism of access control in a decentralized framework that has proven an influential factor in maintaining secure and authorized document management.

Nikita, Antorweep and Chunming [11] introduced a blockchain-oriented trading mechanism that employs both fungible and non-fungible tokens for community-focused energy services. All these factors make such a system easily reproducible in a document management system.

Gauhar et al. [12] presented a blockchain-centric xDBAuth framework targeting cross domain authentication and authorization for the Internet of Things. This research finding contributes to the understanding of blockchain-based authentication mechanisms which can be integrated into the document integrity framework.

Yuan et al. introduced CSEdge, a collaborative edge storage system that works in a blockchain environment for multi-access edge computing. This paper provides insights into the use of blockchain for collaborative storage in relation to the decentralized document management framework [13].

Duan et al. [14] discussed hands-on examination of changing data in distributed storage systems. This study sought to design auditing mechanisms that may check on the integrity of dynamically changing data stored at decentralized storage systems. This result has an importance for understanding challenges and opportunities of auditing document integrity in decentralized storage networks.

The research findings collectively contribute to the understanding of different aspects of blockchain technology, including privacy, secure storage, provenance, access control, transactions, authentication, and collaborative storage. However, there are still areas of uncertainty that require attention in upcoming studies.

Filecoin integration and intelligent contracts for decentralized document integrity remains underexplored. While existing research provides insights into blockchain technology, there is a need to focus specifically on how Filecoin and smart contracts can be combined for secure and automated document management. Future studies should aim to develop and evaluate a framework that leverages Filecoin for storage and smart contracts for managing documents in real-world scenarios. Although current findings are valuable, further research is essential to address these gaps and create a robust solution for decentralized document integrity.

III. Methodology

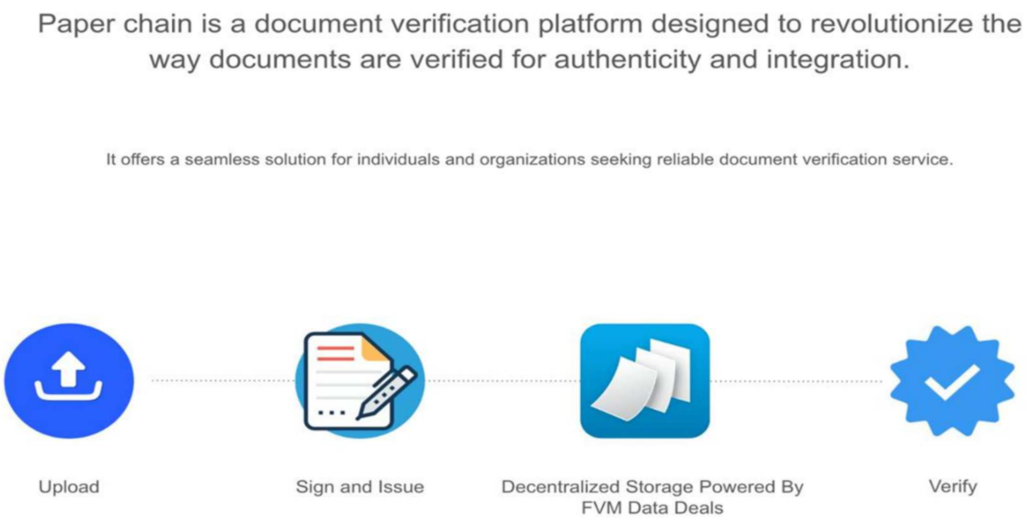
The research introduces PaperChain, a blockchain-based framework that integrates Filecoin and smart contracts for secure and decentralized document management. The framework utilizes the Filecoin Virtual Machine (FVM) and InterPlanetary Consensus (IPC) for storage and consensus, providing a robust system for managing documents.

A. Filecoin VM

The Filecoin Virtual Machine (FVM) launched in March 2023, enabling smart contracts on the network. As of December 2023, over 200 projects operate on FVM, supporting an open data economy with over 1.65 million wallets and more than 2,400 smart contracts deployed [15] [16]. Filecoin's storage network has significantly grown, storing approximately 2 million terabytes of client data [16].

Retrieval tools like Boost and Lassie improved data accessibility [17].

B. IPC



Paper chain is a document verification platform designed to revolutionize the way documents are verified for authenticity and integration.

It offers a seamless solution for individuals and organizations seeking reliable document verification service.

Fig. 1 Overview of PaperChain

The **InterPlanetary Consensus (IPC)** offers a reliable and distributed structure to process transactions across different blockchains. Validator nodes are vital components of this framework as they confirm the validity of transactions between chains, ensuring that assets, data, and contracts can be executed smoothly across networks. These validator nodes are strategically staked on multiple blockchains to relay information and approve transactions between them [18] [19]. Once the validators confirm that a transaction is legitimate on both chains, it gets committed, safeguarding the integrity of the exchange [18] [20]. Moreover, IPC enhances scalability by employing techniques like sharding, parallel processing, and hierarchical consensus structures [18]. This ensures that the system can efficiently handle large volumes of transactions. Additionally, IPC promotes interoperability between different blockchains through standardized communication protocols[19], making cross-chain interactions easier. The system also strengthens security by making attacks, such as 51% attacks, significantly more difficult, providing a higher level of protection for decentralized networks [19].

C. Smart Contracts

A smart contract is a computerized agreement with digital signatures and preserved in a blockchain system, performing automatically when conditions are met [21] [22].

Participants create smart contracts by encoding clauses in a programming language like Solidity and deploying them to a blockchain [21] [22].

Smart contracts monitor blockchain or other sources for predetermined conditions and execute actions based on these triggers [22].

The blockchain records contract execution and its outcomes, ensuring transparency and immutability [22]

D. Metamask

MetaMask is an online crypto wallet software designed to engage with Ethereum blockchains. Users can access their Ethereum wallets via browser extensions or mobile applications, making decentralized transactions easy [23]. MetaMask connects users to decentralized websites and applications through JavaScript code, enabling them to perform smart contract activities through action prompts, signature requests, or transaction requests [23].

E. Mechanism

As shown in Fig.1 The issuer first registers and logs into the system. Afterward, the issuer uploads the document, which is digitally signed using a cryptographic algorithm to prevent tampering. The verifier can then upload the document for authentication. The system verifies the document's integrity by matching its hash value with the stored data. Upon successful verification, the transaction is completed, and the corresponding file is reflected in the digital wallet. This streamlined process ensures both issuers and verifiers can interact with the system seamlessly, reducing fraud risks and improving efficiency.

F. Verification Process

Fig.2 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.

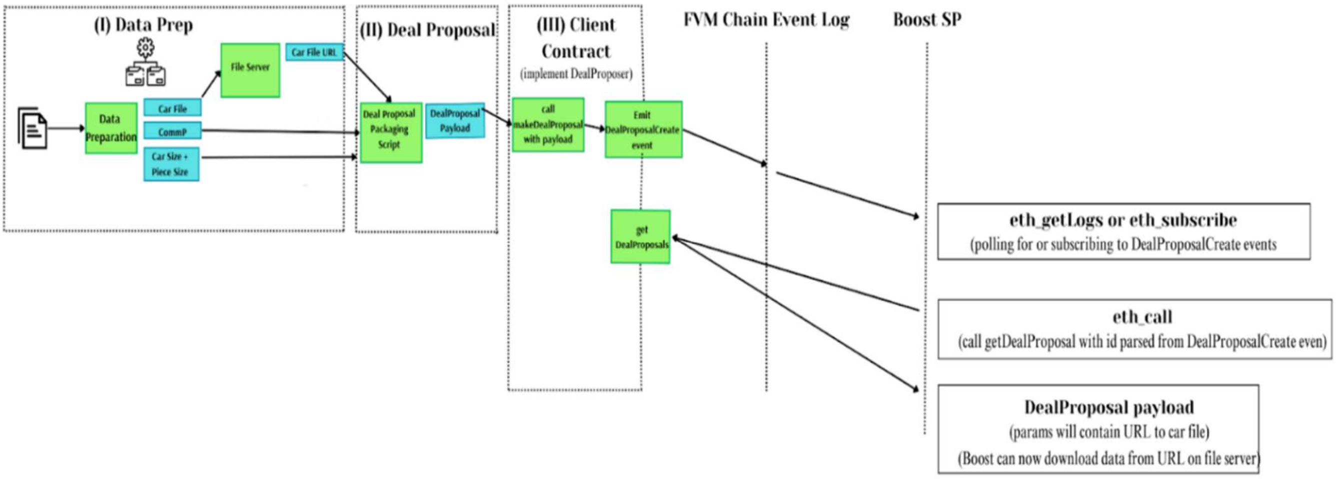

(I) Data Prep
Data Preparation
Car File
CommP
Car Size + Piece Size
File Server
Car File URL
(II) Deal Proposal
Deal Proposal Packaging Script
DealProposal Payload
(III) Client Contract
(implement DealProposer)
call makeDealProposal with payload
Emit DealProposalCreate event
get DealProposals
FVM Chain Event Log
Boost SP
eth_getLogs or eth_subscribe
(polling for or subscribing to DealProposalCreate events
eth_call
(call getDealProposal with id parsed from DealProposalCreate even)
DealProposal payload
(params will contain URL to car file)
(Boost can now download data from URL on file server)

Fig. 2 Verification Process

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

IV. Implementation

Fig. 3 depicts a decentralized application (DApp) architecture using Ethereum blockchain and MetaMask wallet. It involves a front-end, back-end, and smart contract deployed on the Ethereum network.

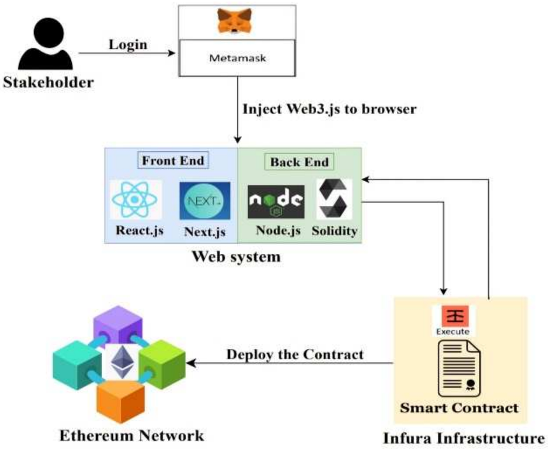
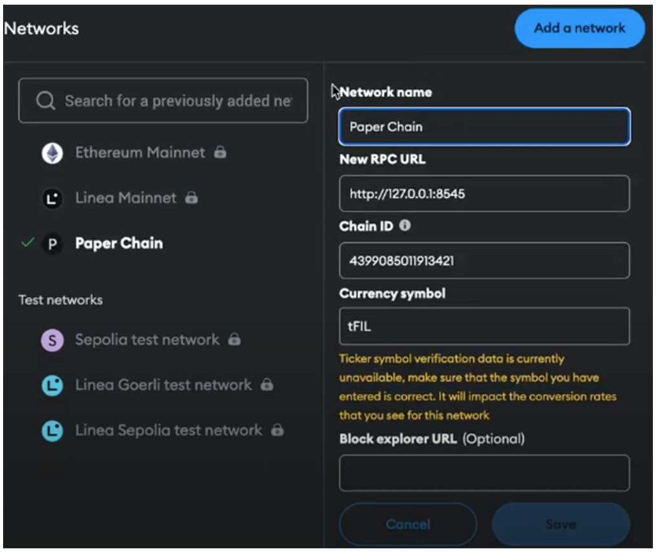


Fig. 5 Implementation Architecture

The user first login as an issuer and connects its MetaMask wallet to PaperChain network which contains tFIL that is shown in Fig.4.



Network name
Paper Chain

New RPC URL
http://127.0.0.1:8545

Chain ID
4399085011913421

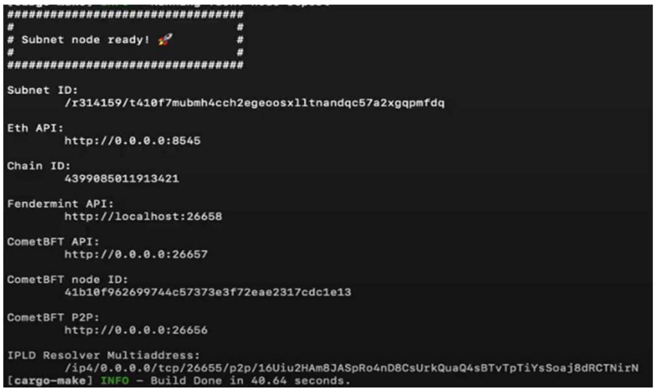
Currency symbol
tFIL

Ticker symbol verification data is currently unavailable, make sure that the symbol you have entered is correct. It will impact the conversion rates that you see for this network

Block explorer URL (Optional)

Fig. 3 Add PaperChain as network

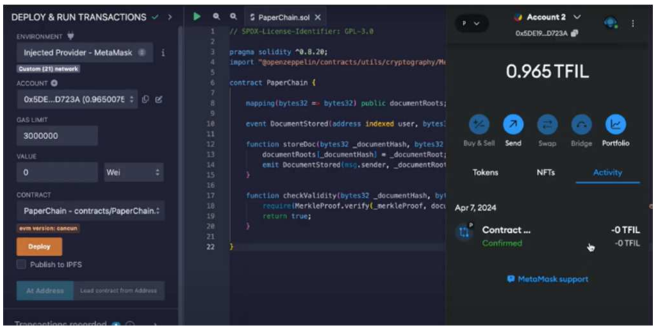
The Chain Id is obtained by deploying the IPC subnet on the host's machine this is shown in Fig.5.



```
###################################
#                                 #
# Subnet node ready! 🚀           #
#                                 #
###################################

Subnet ID:
        /r314159/t410f7mubmh4cch2egeoosxlltnandqc57a2xgqpmfdq

Eth API:
        http://0.0.0.0:8545

Chain ID:
        4399085011913421

Fendermint API:
        http://localhost:26658

CometBFT API:
        http://0.0.0.0:26657

CometBFT node ID:
        41b10f962699744c57373e3f72eae2317cdc1e13

CometBFT P2P:
        http://0.0.0.0:26656

IPLD Resolver Multiaddress:
        /ip4/0.0.0.0/tcp/26655/p2p/16Uiu2HAm8JASpRo4nD8CsUrkQuaQ4sBTvTpTiYsSoaj8dRCTNirN
[cargo-make] INFO - Build Done in 40.64 seconds.
```

Fig. 4 Subnet Node

The graphical user interface was constructed using ReactJs while the Solidity based smart contract was compiled and deployed on Remix IDE with MetaMask injected as Provider. It is shown by Fig.6.



DEPLOY & RUN TRANSACTIONS

ENVIRONMENT: Injected Provider - MetaMask
Custom (21) network

ACCOUNT: 0x5DE...D723A (0.965007E

GAS LIMIT: 3000000

VALUE: 0 Wei

CONTRACT: PaperChain - contracts/PaperChain.

evm version: cancun

Deploy

□ Publish to IPFS

At Address | Load contract from Address

PaperChain.sol

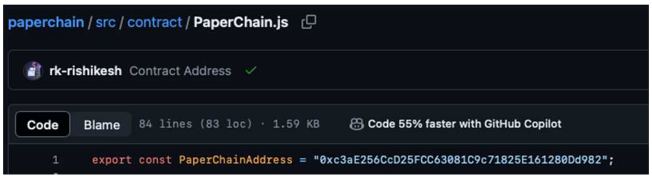
```
// SPDX-License-Identifier: GPL-3.0

pragma solidity ^0.8.20;
import "@openzeppelin/contracts/utils/cryptography/M

contract PaperChain {

    mapping(bytes32 => bytes32) public documentRoots;

    event DocumentStored(address indexed user, bytes

    function storeDoc(bytes32 _documentHash, bytes32
        documentRoots[_documentHash] = _documentRoot;
        emit DocumentStored(msg.sender, _documentRoot
    }

    function checkValidity(bytes32 _documentHash, byt
        require(MerkleProof.verify(_merkleProof, docu
        return true;
    }

}
```

Account 2
0x5DE19...D723A

0.965 TFIL

Apr 7, 2024
Contract ... Confirmed -0 TFIL -0 TFIL

Fig. 6 Deployment of contract on Remix IDE



paperchain / src / contract / PaperChain.js

rk-rishikesh Contract Address ✓

Code | Blame 84 lines (83 loc) · 1.59 KB

```
export const PaperChainAddress = "0xc3aE256CcD25FCC63081C9c71825E161280Dd982";
```

Fig. 7 Integration using PaperChainAddress

Fig.7 shows that 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. These transactions can be traced by using chain explorer for the deployed smart contract.

V. Results and Discussion

We present a detailed analysis of our framework, which integrates Filecoin with InterPlanetary Consensus (IPC) and compares it with Ethereum and other decentralized solutions. The evaluation focuses on several key metrics, including interoperability, scalability, data retrieval efficiency, security, storage cost efficiency, and transaction speed. The findings are supported by statistical data, tables, and graphs to illustrate the comparative advantages of Filecoin.

TABLE I. compares our Filecoin + IPC framework with other decentralized solutions across various metrics, highlighting the key advantages of our approach.

TABLE I. COMPARISON OF OUR FRAMEWORK WITH OTHER SOLUTIONS

Observation point	**Our Framework (Filecoin + IPC)**	**Other Decentralized Solutions**
Interoperability	Seamless multi blockchain interoperability via IPC	Limited, often requiring complex bridging mechanisms
Scalability	High scalability with sharding and parallel processing in FVM	Scalability may be limited, leading to higher latency and costs
Data Retrieval Efficiency	Optimized with tools like Boost and Lassie for fast access	Often slower, especially with large datasets or high demand
Security	Multi-layered consensus with enhanced protection	Typically relies on single-layer consensus, vulnerable to specific attacks
Storage and Cost Efficiency	Cost-effective storage with distributed redundancy	Can be more expensive, with less efficient redundancy management

TABLE II. ETHEREUM VS FILECOIN PERFORMANCE METRICS

Metric	**Ethereum**	**Filecoin**
Transactions Per Second	12-15 TPS	30-70 TPS
Average Transaction Latency	10-15 seconds	2-5 seconds
Data Retrieval Speed	10-20 seconds	2-5 seconds using Boost and Lassie
Cost per GB (Storage)	$0.10-$0.15	$0.01-$0.05
Smart Contracts Deployed	~2,000	~2,400
Total Wallets	~1.5 million	~1.65 million

TABLE II. above compares the various performance metrics of Ethereum and Filecoin over the past year.

Filecoin consistently achieves higher TPS with more transaction efficiency. Ethereum's TPS has remained relatively stagnant, reflecting its scalability limitations under heavy usage. This can be shown in the Fig.9.

Filecoin's optimized retrieval mechanism reduces latency and improves user experience during peak loads, outperforming Ethereum's basic retrieval methods.

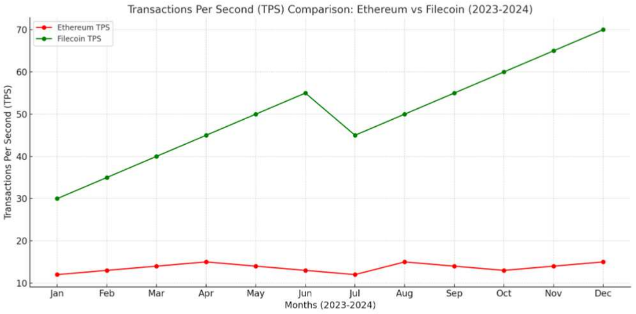


Fig. 8. Transactions Per Second (TPS) Comparison: Ethereum vs Filecoin (2023-2024)

Filecoin's ability to maintain a higher average and peak TPS showcases its technical advantages in a decentralized network environment.

VI. Conclusion And Future Scope

In our proposed solution, PaperChain stands out as a robust framework for the validation and verification of documents, encompassing a wide range of applications from legal papers to medical records, identity cards to financial reports. Leveraging blockchain technology and smart contracts, PaperChain ensures that sensitive data, such as land records, is maintained with the highest levels of integrity, transparency, and security.

The decentralized storage system, complemented by cryptographic proofs, safeguards against tampering and fraud while preserving data integrity. Document uploads are facilitated through user-friendly portals specifically designed for issuers and verifiers, focusing on confidentiality and integrity. When integrated with **MetaMask**, transactions are secured using the **PaperChain** cryptocurrency, enhancing convenience and safety for end users. Additionally, advanced document validation mechanisms like digital signatures and timestamping bolster the authenticity and traceability of documents within the PaperChain ecosystem.

Looking ahead, PaperChain has significant potential for growth and innovation in document authentication and verification. To scale effectively and accommodate increased user demand and data volume, the platform will implement various strategies. These include optimizing the underlying infrastructure to support higher transaction throughput and exploring new business opportunities that leverage blockchain for diverse sectors. Enhanced security measures will be developed to protect against emerging threats, and interoperability with other platforms will be prioritized to create a seamless user experience across different systems.

By pursuing these development paths, PaperChain aims to maintain its leadership position in the document authentication and verification industry, fostering innovation and delivering added value for all stakeholders involved. This forward-thinking approach ensures that PaperChain is not only a solution for today but also a scalable platform for the future.

VII. References

[1] O. Aramide, R. Ajibola, O. S. Olatunji and A. Oduroye, "Improving Records Management And Security For Successful Business Performance: The Role Of New Media," p. 3734, 01 2020.

[2] Z. Yusof, "Issues and Challenges in Records Management," 2008.

[3] M. Noman, C. M. F. Benjamin, C. K. H. Patrick and L. Cheuk-Kwong, "Centralized and Distributed Anonymization for High-Dimensional Healthcare Data," vol. 4, no. 4, pp. 1-33, 2010.

[4] Z. Zheng, S. Xie, H.-N. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017.

[5] F. Hofmann, S. Wurster, E. Ron and M. Böhmecke-Schwafert, "The immutability concept of blockchains and benefits of early standardization," pp. 1-8, 2017.

[6] H. Taherdoost, "Smart Contracts in Blockchain Technology: A Critical Review," *Information,* vol. 14, p. 117, 2023.

[7] Zyskind G, Nathan O and Petland A, "Enigma: decentralizedcomputation platform with guaranteed privacy," arXiv, 2015.

[8] J. Sun, X. Yao, S. Wang and Y. Wu, "Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records in IPFS," *IEEE Access,* vol. 8, pp. 59389-59401, 2020.

[9] M. A. Rahman, M. S. Hossain, M. S. Islam, N. A. Alrajeh and G. Muhammad, "Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach," *IEEE Access,* vol. 8, pp. 205071-205087, 2020.

[10] R. Xu, Y. Chen, E. Blasch and G. Chen, "Exploration of blockchain-enabled decentralized capability-based access control strategy for space situation awareness," *Optical Engineering,* vol. 58, pp. 041609--, 2019.

[11] K. Nikita, C. Antorweep and R. Chunming, "Blockchain Based Transaction System with Fungible and Non-Fungible Tokens for a Community-Based Energy Infrastructure," *Sensors,* vol. 21, no. 11, p. 3822, 2021.

[12] G. Ali, N. Ahmad, Y. Cao, S. Khan, H. Cruickshank, E. A. Qazi and A. Ali, "xDBAuth: Blockchain Based Cross Domain Authentication and Authorization Framework for Internet of Things," *IEEE Access,* vol. 8, pp. 58800-58816, 2020.

[13] L. Yuan, Q. He, F. Chen, J. Zhang, L. Qi, X. Xu, Y. Xiang and Y. Yang, "CSEdge: Enabling Collaborative Edge Storage for Multi-Access Edge Computing Based on Blockchain," *IEEE Transactions on Parallel and Distributed Systems,* vol. 33, no. 8, pp. 1873-1887, 2022.

[14] H. Duan, Y. Du, L. Zheng, C. Wang, M. H. Au and Q. Wang, "Towards Practical Auditing of Dynamic Data in Decentralized Storage," *IEEE Transactions on Dependable and Secure Computing,* vol. 20, no. 1, pp. 708-723, 2023.

[15] "Filecoin," [Online]. Available: https://fvm.filecoin.io/.

[16] "Roadmap | Filecoin Docs," [Online]. Available: https://docs.filecoin.io/smart-contracts/fundamentals/roadmap. [Accessed 1 September 2024].

[17] "Filecoin Virtual Machine," [Online]. Available: https://filecoin.io/blog/posts/filecoin-virtual-machine-fvm-builder-cohort-launches-to-mainnet/. [Accessed 01 September 2024].

[18] Z. Hussein, M. A. Salama and S. A. El-Rahman, "Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms," *Cybersecurity,* vol. 6, no. 1, pp. 2523-3246, 2023.

[19] "What are blockchain consensus rules," [Online]. Available: https://www.bitstamp.net/en-gb/learn/security/what-are-blockchain-consensus-rules/.

[20] A. Á. Iván, G. Vincent and S. Johannes, "Unsealing the secrets of blockchain consensus: A systematic comparison of the formal security of proof-of-work and proof-of-stake," in *SAC: Symposium on Applied Computing*, Avila, 2024.

[21] "Smart Contracts," [Online]. Available: https://woolypooly.com/en/blog/smart-contracts.

[22] A. G. Garnett, "How Smart Contract work," [Online]. Available: https://www.britannica.com/money/how-smart-contracts-work.

[23] W. Vermaak, "What is Metamask," 2021. [Online]. Available: https://coinmarketcap.com/academy/author/werner-vermaak.

[24] "What is metamask," [Online]. Available: https://www.bitstamp.net/en-gb/learn/web3/what-is-metamask/.