IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DECENTRALIZED DOCUMENT NOTARIZATION

Dr. Shobana M[1], Arun J[2], Suji S[3], Shanmugavel R M[4]

Department of Computer Science and Engineering -IOT, Saveetha Engineering College

Doi: https://doi.org/10.56975/ijcrt.v14i7.309008

Abstract **-** Conventional document notarization is based on centralized systems with added cost, delay and single points of failure. This paper introduces a decentralized notarization system that uses blockchain, IPFS, and new web technologies to offer verifications of digital documents that are not interchangeable, transparent and maintain privacy. The system creates a hash of the uploaded documents in the SHA-256 format, safely stores the file in IPFS and documents the hash with a time rating on an ethereum-based smart contract. Staking and reputation are used to encourage honest behavior among the notaries, and full-stack architecture can ensure that it is easy and scalable. Extensive testing of smart contracts, backend services, and frontend elements was very reliable and well functional. The real-world feasibility was tested by being deployed on the Sepolia testnet. The presented solution avoids the use of the centralized mediators and provides integrity, availability, and user-controlled certification of the digital records.

Keywords - Decentralized notarization, Blockchain, Smart contracts, IPFS, Document integrity, Ethereum, Distributed systems.

I. INTRODUCTION

Modern society is fast becoming digitized and this has altered the manner people, businesses and governments generate, share and keep information. Contracts, certificates, agreements and legal records which could only be completed and delivered in physical form are now largely produced and passed electronically. Although this transition has made the process more efficient and accessible, it has also created a major problem of building trust, authenticity, and integrity of digital documentation. Considering documents made of plastic, silk, or paper, where it is possible to stamp or seal them, and/or to add a signature, any digital file can be copied, edited, or counterfeited with little effort, sometimes leaving no evidence. Consequently, there has been a strong need to establish reliable procedures that ensure that the origin and integrity of digital documents are verified in legal, commerce, academic and administrative practice domains.

The historical legitimacy of traditional notarization has been used as a dependable means of document validation. The role of a notary public is to be a dispassionate observer that can identify people, note signatures and place an official seal on evidence that certifies the legitimacy of those signatures. Nevertheless, such model is centralized by its nature and has a geographic limitation. It needs physical presence or require attachment to particular authorized institutions, which result in delays, limitations (based on accessibility) and extra expenditures. Moreover, when it comes to centralized systems, there exists single points of failure: records can be lost, corrupted or distorted in case of compromising the authority that maintains records. When dealing with an international transaction, it might be even harder to check the authenticity of a notarial act due to the disparity in the legal systems and legal documents.

These limitations can also be overcome by the implementation of blockchain technology. A blockchain can be described as a distributed registry that is managed by a system of nodes which together substantiate and store transactions in an unamenable and unconscaled way. After data is stored in the blockchain it becomes computationally infeasible to change it, thus it forms a permanent and unreliable record. These features cause blockchain to be the best fit when it comes to reducing the need to be granted trust without resorting to centralized intermediaries, in application. Rather than having one authority, the participants use the cryptographic proves and consensus mechanisms to confirm the originality of the information that is recorded. This metaparadigm allows building decentralized trust infrastructures that have the potential to facilitate safe digital notarization [1].

The use of cryptographic hash is a major concept in blockchain based notarization. Instead of storing whole documents on-chain, which is not only inefficient, it is possible that sensitive information can be leaked, the system can create a unique hash value, which serves as a kind of digital fingerprint of the document. Any slight change in the file leads to a entirely different hash that makes it a good tool in checking integrity of the file. Since all that is written in the blockchain is a hash and a time stamp, the system creates evidence that at a certain time a certain version of a document has existed, and remains private. This methodology will guarantee privacy by default, so it will be in compliance with data protection laws, as the source material will not be leaked publicly [2].

Although it has its benefits, blockchain by itself is not the best storage of large files because of the cost and scalability issues. In response, blockchain is combined with decentralized storage computing, through the InterPlanetary File System (IPFS). The IPFS is a decentralized storage system relying on a peer-to-peer network and addressing files through content-based addressing, generating a Content Identifier (CID) based on a hash of the file. The mechanism of integrity verification of any file retrieved is in place. The system has a hybrid architecture, by saving documents on IPFS and pinning their hash on the blockchain to achieve a balance between cost efficiency, resilience, and immutability. Such integration marks a great step to decentralized management of digital records [3].

In addition to technical infrastructure, to build trust in the context of a decentralized notarization system, systems need to monitor accountability of the participants. Under the conventional systems, they tend to trust institutional powers of notaries.

In a decentralized scheme, economic incentives and clear governance systems can serve the same purpose. Notary registration and staking rules and penalties can be applied by using smart contracts that are self-executing programs on the blockchain. Securing notaries to post cryptocurrency would instill financial responsibility, and will reduce systems to discourage incompetence or bad faith. Trust is also enhanced by reputation trackings in that the user can review the reliability of the notaries depending on historical performance [4].

The usability of decentralized applications is also of crucial importance. To realize the usage of blockchain-based notarization in the real world, the system should offer a convenient user interface to hide the technicality. New web-based technologies allow to create the responsive interface showing the user how to upload documents, complete notarization requests, and verification. Brown-box interface Integration with browser-based wallets enables hiring of transactions using secure signature, whose private key is not revealed, and the back-end service manages communication among the user interface, storage network, and blockchain layer. The entire stack strategy makes sure that the advantages of decentralization can reach even non-technical applicants.

This paper gives a design and implementation of a document notarization system, which is decentralized, employs a blockchain and IPFS together with a web based application architecture. The suggested system includes the flaws of the conventional notarization by ensuring that there are no points of failure, less dependence on intermediaries and would impose worldwide, provable certification of document authenticity. The framework is based on the use of cryptographic methods, decentralized storage, and smart contracts to provide a secure and privacy-sensitive digital trust environment. The entire testing and deployment in a published test network is an experiment to prove the feasibility and durability of the method that shows that the system has the potential of transforming document verification practices in the more digitalized world [5].

The format of this book has been in the way that the literature review has been introduced in the II section. Part III addresses the methodology with the operationality of the same as well. Results and discussions are found in section IV. Lastly, the last section of V is the final findings and recommendations.

The format of this book has been in the way that the literature review has been introduced in the II section. Part III addresses the methodology with the operationality of the same as well. Results and discussions are found in section IV. Lastly, the last section of V is the final findings and recommendations.

II. LITERATURE SURVEY

The development of decentralized document notarization is the result of the combination of blockchain technology, systems of digital identities, and secure records. Conventional notarization is deeply rooted in centralized points of authority, paper-and-pencil documentation and jurisdiction-based verification procedures that tend to generate inefficiencies, facilitate cost rises, and interoperability. As a result of the emergence of distributed ledger technologies, scholars have investigated the potential role of decentralization in developing greater transparency, integrity, and long-term verifiability of legal and transactional records. The purpose of these systems is attribution (tamper resistance), cryptographic confirmation of authenticity and verification (independent verification) without trusting to a single trusted third-party. With the growing spread of digital transformation in legal, financial, and governmental fields, decentralized notarization systems are being considered an essential element of reliable digital ecosystems, particularly in cases where cross-border acknowledgment, automation, and auditability are the properties.

It has made recent efforts to augment the infrastructure on decentralized validation and distribution of trust. Distributed ledger solutions that are enterprise oriented illustrate how the verification of transactions can be achieved reliably by permissioned notary service without damaging confidentiality in regulated contexts [6]. Selecting and organization mechanisms of notary groups have been also investigated to enhance resilience and equity of distributed decision making [7]. Privacy-conscious improvements also deal with the disclosure of transaction metadata, with an improved proposal to have better notary mechanisms that trade-off between disclosure and privacy [8]. The value of scalable interoperability is emphasized through architectural breakthroughs that combine notary services and relay-chain/case-cross-chain constructions, which make sure that verifying the validity of data that has been notarized requires validating it in more than one blockchain network without compromising the security assurances [9]. These components together form the structural foundation that the decentralized notarization systems need to operate effectively in the heterogeneous digital environments.

In addition to infrastructure, studies have also been undertaken on the role of the decentralized model of reputation, consensus and evaluation in enhancing trust in the process of notarization. Mechanisms Dynamic reputation assessment have been presented to value nodes that are engaged in cross-chain ecosystems and assist, among other things, in deterring bad behavior without compromising decentralization [10]. Algorithms tailored to cross-chain notaries will be used to assure a balanced participation, fault tolerance, which is critical when notarization requires distributed committees and no longer

requires dedicated authorities [11]. Multi-indicator evaluation schemes also build on this concept by introducing a variety of performance and credibility measures into the process of making decisions involving notaries and enhancing reliability in service-related situations that are more complex [12]. To the extent that their application is provided to digital asset transfers, notary groups establishment models demonstrate how systematic multilayer control systems may oversee authenticity and mitigate against duplicature spending or deceitful records changes across chains [13]. All these contributions support the notion that decentralized notarization should consist of cryptographic assurance and adaptive trust management.

Focus has also shifted to pragmatic models which relate notarization logic to smart contracts and electronic documentation systems. Models of blockchain-based secure digital record keeping show the ability of automated notarization processes to substitute manual certification without losing evidentiary value [14]. Mechanisms to monitor and control distributed notaries used in a consortium setting reveal that monitoring and regulation of distributed notaries can be achieved with respect to preserving the principle of decentralization, a key factor in adopting institutions [15]. Collaborative network models investigate the capacity of electronic notary services to cross organizational boundaries so as to share trust infrastructures amongst two or more stakeholders [16]. Research on cross-chain consensus in complex trust environments focus on adaptive design framework which can sustain reliability despite a variation in the governance and security assumptions of the participating networks [17]. These attempts connect theory-based protocol design to systems focused on applications and explicate how decentralized notarization might be applied in a context of the real-life legal, commercial, and inter-organizational relations.

Lastly, supporting and base-level technologies entail the cryptography and systems support, which underpins notarization services of advanced nature. As autonomous notarization systems that are developed alongside national eID systems point to the opportunities of an effective identity binding and legally significant digital signatures in the blockchain activity [18]. Secure execution environments and threshold cryptography Open, distributed notary services indicate how centralized certification can be unquestioning substituted by collective signing and verification [19]. Notarization services through service schemes tied to notary schemes and cryptographic locking schemes extend notarization services even to cross-chain service interaction, where proofs of existence and integrity are verifiable despite using cross-platform interactions [20]. What all of these core works demonstrates is that decentralized document notarization is not a single technology itself but rather a stacked ecosystem of identity, consensus, privacy, and interoperability to create an environment of trustful and scalable digital certification.

III. METHODOLOGY

This section entails the step-by-step design methodology that is to be used in designing and implementing the decentralized document notarization system. The solution is based on a combination of blockchain smart contracts, cryptography, distributed storage, and full-stack web development to establish a verifiable workflow and a secure notarization solution. Every phase of the methodology was to be buttered at the seams containing integrity, privacy, transparency, and usability whilst being smooth scaling and cost effective. Division of system architecture into logical layers such as frontend, backend, blockchain and decentralized storage was meant to offer modularity and easy maintenance. The process of development was based on the iterative model enabling the constant advancement of APIs, user interfaces, and smart contracts. Security, performance and reliability issues were factored in the whole process so that each phase of the document life cycle, such as the upload, verification etc would be done in a controlled and tamper resistant form.

A. Document Upload and Cryptographic Hash Generation.

In the process, the initial action in the methodology is the safe onboarding of a document into the system. Users post online digital files in a web-based interface created in React. First validation is done by the frontend to make sure that supported formats like PDF, DOCX or TXT get accepted. After the file has been received, it is sent to the backend server using HTTPS in order to avoid interception. The server calculates a cryptographic hash (SHA-256) of the contents of the document. This hash is like a digital fingerprint, it is impossible to have the same value in the file, changing one single bit would result in a totally different one. The primitiveness integrity reference stored in the database is the hash. Notably, hashing is done prior to any interaction within the blockchain environment, so that the sensitive file contents are never accessed out of the secure server environment.

B. Decentralized Storage in IPFS.

Once hashed, the original file is stored on InterPlanetary File System (IPFS), which is a decentralized peer-to-peer file network. The backend communicates with an IPFS node through the HTTP API in order to upload the file. Having been stored, IPFS returns a Content Identifier (CID), obtained out of the cryptographic hash of the file and provides content-addressable storage. This implies that as the file is altered, a different CID shall be formed and it will be easy to identify tampering. The system logically stores the CID in the relational database and associated with the already created hash (SHA-256). In order to be sure of long-term availability, the system adds connectivity to a pinning service which keeps consistent copies of the file throughout the IPFS network. The hybrid storage model lowers the cost of blockchain, and it maintains blockchain resilience or verifiability.

C. Notarization through Smart Contracts.

The Ethereum smart contracts based on Solidity are what control the process of notarization. A user provides a notarization request that has document hash and IPFS CID. This request is put in line with registered notaries in view. With a wallet called metamask, notaries access the system by Web3, locating the signature blockchain transactions safely. On the

confirmation of a request, the notarizeDocument function of the smart contract is called. The role ascertains that the required amount of cryptocurrency has been staked by the notary and only then the transaction can occur. Upon submission of validity the document hash, date and address of the notary are entered in the blockchain. A notification is emitted to indicate a successful notarization. This forms a secure and resilient record of presence and integrity that is placed upon a decentralized registry.

D. Backend Backend -Blockchain Integration.

The backend layer is a connection between the user interface and the blockchain network. The backend has been implemented with Spring boot and it uses Web3j to communicate with the deployed smart contracts. Additionally, when initiating a notarization, the backend builds a transaction request and signs it with the wallet of the user. Upon the payment in the Ethereum network, the backend keeps track of the transaction by waiting on receipts and subscribing to the events emitted by the contract. After confirmation, the transaction hash and the notarization status of the blockchain transaction are recorded in the database. Similar to consistency, this synchronization guarantees that off-chain records and on-chain data are consistent. Error management, retry and secure set up of blockchain credentials is also managed by the backend using environment variables.

E. Confirmation and Sanity Check.

Verification is to be made easy, transparent and any user can access it. To authenticate a document, a system re-computes its SHA-256 hash and compares it with the number obtained in the database. The system then transmits a query to the blockchain by the stored transaction hash or document hash to determine that there exists a notarization record that matches the query. When a match is located, the timestamp and address of a notary are retrieved and presented. This can demonstrate that the document was in that precise form at a point of time. When the re-computed hash is not equal to the one on-chain, the system will consider the document modified or unverified. The on-chain validation together with off-chain hash validation makes this very powerful with high integrity guarantees, but leaves the contents of the documents hidden.

F. Security, Testing, and Deployment Strategy.

Security was ensured in the development life cycle. Frontend/backend communications are encrypted with the help of HTTPS, and input checks are made to avoid injection and file-based attacks. The access control modifiers and reentrancy protection that were implemented to prevent common vulnerabilities in smart contracts made them reentry-safe. Unit contract tests were developed in Hardhat, Mocha, and Chai and backend services were developed in JUnit and Mockito. Jest and React Testing Library were used to validate Frontend components. Complete user workflow was simulated with integration and end-to-end testing that was used to assure reliability across the layers. The deployment was done in a step-by-step manner with the implemented contracts operating on the Sepolia testnet and the server being a Linux server with NGINX where it hosted the backend services and served the frontend assets as static files. This guaranteed scalability and production-readiness.

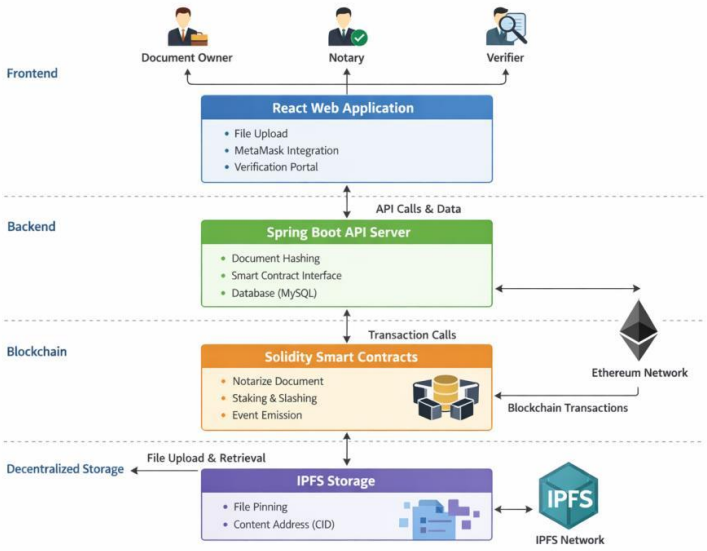

Fig. 1: System Architecture

IV. RESULT AND DISCUSSION

The adopted decentralized document notarization system was tested to figure out its level of effectiveness, reliability, and feasibility. The functional appropriateness, performance of the system, and reliability of the interaction with the blockchain and the efficiency of the overall process of work with users were tested. The evaluation aim was not merely to ensure that every part was functioning well singly, but also to observe that the system as an entirety offered customers a smooth, secure, and hack proof notarization experience. The findings indicate that the hybrid system, comprising of blockchain immutability, IPFS distributed storage, and a conventional backend, proves effective in resolving the drawbacks

of centralized notarization systems, and is still usable.

One of the largest concerns of the analysis was the accuracy of the cryptographic verification. Various documents of different sizes and formats were put in IPFS, hashed and stored on the blockchain and notarized. Integrity validation carried out many times revealed that the sha256 hash calculated and uploaded during upload was always the same as the calculated hash during verification. Any change of even a single word in a document would lead to a totally different hash making verification to fail as anticipated. This is testimony of the fact that this system is dependable in the detection of tampering and document integrity. Also, keeping the hash on-chain only meant that no sensitive data covering in a document was revealed, which proved the privacy-preserving design to be effective.

Normal operating conditions in the performance testing evaluated the responsiveness of the system. It took only a few seconds to perform the upload as well as the hashing operation on a normal document of less than 10 MB. With IPFS storage, the latency was slightly dependant on the network conditions, and retrieval was non-random and verifiable through CID matching. The confirmation time of a blockchain transaction depended on the testnet conditions with an average of 15 to 45 seconds. Even though this delay is a characteristic of blockchain consensus, it was possible to show users real-time transaction status updates on the frontend and thus minimized the level of uncertainty. Transaction confirmation via backup polling mechanism, followed by notification of event listeners, was the reason why the user interface updated as soon as the block had been confirmed.

Another area that was of analysis was smart contract reliability. The core contract functions, such as the notary registration, staking, notarization and retrieval of records were all put to test with the edge cases of insufficient stake, duplication submissions and unauthorised access as well. The contract rightly repudiated invalid functioning and imposed staking obligations ahead of permitting notarization. The measurements of gas usage demonstrated that tracking the usage of hashes and a timestamp were much cheaper to store than larger data structures. This proves the cost effectiveness of this design and supports the choice of off-chain storage to store documents.

There was a stable performance of the backend services during API integration testing. REST applications properly managed metadata storage of documents, status updates, and blockchain synchronization. The events presented in the blockchain were reflected in the database records, and it had been affirmed that the off-chain and on-chain states were matched correctly. Failure or dropped transaction management was properly implemented through error-handling routines that sent notification to users and permitted their retries. The modular structure made it easy to switch between configuration like changing blockchain networks or IPFS nodes too, which underscores the portability and scalability of the system.

Frontend was tested in terms of usability, and consistent interaction with blockchain events. The users could add wallets, scan documents, place notarization orders and check the outcomes by using a step-by-step interface. Status indicators like progress spinners and alerts and confirmation message enhanced transparency in case of blockchain processing delay. Transactional updates were critical to keep the interface updated so that when a transaction has been mined, it is reflected instantly in the interface without the necessity to refresh it manually. These characteristics greatly amplified user experience though the functionality of blockchain was asynchronous.

Table 1: Summary of functional testing.

Module	Test Scenarios	Passed	Failed	Success Rate
Document Upload & Hash	20	20	0	100%
IPFS Storage	15	15	0	100%
Smart Contract Actions	25	25	0	100%
Verification Process	18	18	0	100%

Table 2: Performance Metrics

Operation	Average Time	Notes
Document Upload & Hashing	2–4 sec	Depends on file size
IPFS Upload	3–6 sec	Network dependent
Blockchain Confirmation	15–45 sec	Sepolia testnet latency
Verification Check	< 5 sec	Includes blockchain query

Table 1 results shows that all major functional modules were functioning as planned. Testing showed no data corruption and integrity mismatches. Performance measurements Table 2 show that the majority of delays can be explained by blockchain confirmation time that is predicted to appear in decentralised systems. The processes that were carried out off-chain were prompt and quick. The coverage percentages are also high which indicates that the system was fully tested at several layers lowering chances of faults not being detected shown in Table 3.

Table 3: Overview of Test coverage.

Component	Framework Used	Coverage
Smart Contracts	Hardhat (Mocha/Chai)	95%
Spring Boot Backend	JUnit, Mockito	92%
React Frontend	Jest, React Testing Lib.	88%

```
    // Register as notary
    function registerAsNotary(string memory _name) public payable {
        require(msg.value == STAKE_AMOUNT, "Incorrect stake amount");
        require(!notaries[msg.sender].isActive, "Already registered as notary");
        require(!usedNames[_name], "Name already taken");
        notaries[msg.sender] = NotaryInfo({
            notaryAddress: msg.sender,
            name: _name,
            isActive: true,
            stakeAmount: msg.value,
            successfulNotarizations: 0,
            slashedCount: 0
        });
        usedNames[_name] = true;
        emit NotaryRegistered(msg.sender, _name);
        emit StakeDeposited(msg.sender, msg.value);
    }
    // Register document with IPFS CID
    function registerDocument(string memory _ipfsCid, string memory _documentName) public {
        require(bytes(_ipfsCid).length > 0, "Invalid IPFS CID");
        require(documents[_ipfsCid].owner == address(0), "Document already registered");

        documents[_ipfsCid] = Document({
            ipfsCid: _ipfsCid,
            owner: msg.sender,
            timestamp: block.timestamp,
            documentName: _documentName,
            isNotarized: false,
            notaries: new address[](0)
        });
```

Fig 2: Notarization of Smart Contracts.

```
public TransactionReceipt registerNotary(String notaryAddress, String name, BigInteger stakeAmount) throws Exception
    log.info("📄 Registering notary on blockchain: {} | Address: {} | Stake: {} wei",
            name, notaryAddress, stakeAmount);
    validateContractState();

    try {
        // Debug: Check what we're sending
        log.info("🔍 Contract call details:");
        log.info("   - Name: {}", name);
        log.info("   - Stake Amount: {} wei", stakeAmount);
        log.info("   - Required Stake: {} wei", getStakeAmount());
        log.info("   - Sender Address: {}", getCurrentAccountAddress());

        // Check if stake amount matches exactly
        BigInteger requiredStake = getStakeAmount();
        if (!stakeAmount.equals(requiredStake)) {
            log.error("❌ Stake amount mismatch: got {}, expected {}", stakeAmount, requiredStake);
            throw new RuntimeException("Stake amount must be exactly " + requiredStake + " wei");
        }

        // Try the contract call
        log.info("📞 Calling contract.registerAsNotary({}, {})", name, stakeAmount);
        TransactionReceipt receipt = contract.registerAsNotary(name, stakeAmount).send();

        log.info("✅ Notary registered. TX: {}", receipt.getTransactionHash());
        return receipt;
```

Fig 3: Backend Service Interaction with Blockchain.

```
export const connectWallet = async() => {
    if (window.ethereum) {
        try {
            await window.ethereum.request({ method: 'eth_requestAccounts' });
            return true;
        } catch (error) {
            console.error('User denied account access');
            return false;
        }
    } else {
        alert('Please install MetaMask!');
        return false;
    }
};

export const getCurrentAccount = async() => {
    const accounts = await web3.eth.getAccounts();
    return accounts[0];
};

export const calculateHash = async(file) => {
    return new Promise((resolve, reject) => {
        const reader = new FileReader();
        reader.onload = (e) => {
            const buffer = e.target.result;
            const hash = web3.utils.sha3(buffer);
            resolve(hash);
        };
```

Fig 4: Frontend Wallet and Connection and Transaction Flow.

Figure 2 gives an idea of the Solidity function that is used to verify the stake of a notary, hash the document and emit an event in case of successful notarization. Here is an example of this Figure 3 which is the Spring Boot service method available on Web3j that is used to invoke the smart contract and to track the status of the transaction. The Figure 4 shows the React element that communicates with MetaMask and establishes a signer and sends the transaction of the notarization process.

By and large, the analysis indicates that the system meets the design requirements of security, transparency, and decentralization. The combination of blockchain and IPFS ensures powerful assurances of permanent and accessibility whereas the web-based user interface remains accessible. Though blockchain latency is a limitation, the architecture manages to curb the issues of usability by using asynchronous updates and definite feedback mechanisms. The results obtained prove that the implementation of decentralized notarization platforms can be considered as viable alternatives to the traditional and centralized solutions.

V. CONCLUSION

This research paper outlined the design, implementation and evaluation of a decentralized document notarization system that uses blockchain, IPFS and full-stack web application as a substitute to the traditional non-tamper proof notarization. The system achieves integrity, transparency, and privacy by storing the cryptographic document hashes on a public blockchain and storing the actual files on a decentralized storage network, eliminating the need to otherwise use centralized authorities to do those functions. The use of smart contract based staking and reputation further enhances trust since it adds accountability to notaries. Detailed testing of smart contracts, back end, and front end elements proved that this system is reliable and functionally sound in a real-life testnet. In practice, the platform presents a globally verifiable and accessible mechanism of establishing document existence and integrity. Work in the future will be done on Layer-2 scalability, decentralized identity, privacy-enhancing zero-knowledge proofs, cross-chain interoperability and user-friendly mobile experiences.

REFERENCES

[1] L. Vlădilă, I. Genoiu, M.-L. Niță, and O. Mastacan, “Digital Versus Traditional Instruments in the Practice of Legal Professions: An Overview of the Lawyer and Public Notary Professions,” in Proc. 17th Int. Conf. Electronics, Computers and Artificial Intelligence (ECAI), Târgoviște, Romania, 2025, pp. 1–6, doi: 10.1109/ECAI65401.2025.11095496.

[2] A. Méndez, L. Cabanillas, and D. R. López, “Transparent Notary Service: A Transparency Framework for Secure and Verifiable Network Evidence,”in Proc. IEEE 11th Int. Conf. Network Softwarization (NetSoft), Budapest, Hungary, 2025, pp. 573–578, doi: 10.1109/NetSoft64993.2025.11080618.

[3] M. Mondal and A. Banerjee, “DyNoS: Dynamic Notary Subset Selection Framework for Validating Cross-Chain Transactions Using Stackelberg Game,” in Proc. IEEE 31st Int. Conf. Parallel and Distributed Systems (ICPADS), Hefei, China, 2025, pp. 1–8, doi:
10.1109/ICPADS67057.2025.11323128.

[4] H. Liang et al., “NCCP: A Notary Group-Based Cross-Chain Channel Protocol for Secure and Scalable Interoperable Payments,” in Proc. IEEE 31st Int. Conf. Parallel and Distributed Systems (ICPADS), Hefei, China, 2025, pp. 1–8, doi: 10.1109/ICPADS67057.2025.11322951.

[5] K. Zhang et al., “DPNM: A Differential Private Notary Mechanism for Privacy Preservation in Cross-Chain Transactions,” IEEE Trans. Inf. Forensics Security, vol. 20, pp. 2224–2236, 2025, doi: 10.1109/TIFS.2025.3527357.

[6] V. S. Venu et al., “Secure Enterprise Transaction with Corda Technology,” in Proc. World Skills Conf. Universal Data Analytics and Sciences (WorldSUAS), Indore, India, 2025, pp. 1–5, doi: 10.1109/WorldSUAS66815.2025.11198949.

[7] X. Huang and M. Tan, “Election Method of Notary Group Based on Block-out Memory,” in Proc. 2nd Int. Conf. Mechatronics, IoT and Industrial Informatics (ICMIII), Melbourne, Australia, 2024, pp. 131–135, doi: 10.1109/ICMIII62623.2024.00031.

[8] Z. S. Tan, C. H. Chen, X. B. Chen, and X. Yang, “ A Study on Privacy Protection of Cross-Chain Transactions Based on Improved Notary Mechanisms,” IEEE Access, vol. 12, pp. 95846–95856, 2024, doi: 10.1109/ACCESS.2024.3425475.

[9] S. Yang et al., “Cross-chain Architecture of Blockchain Integrating Notary Mechanism and Relay-chain Technology,” in Proc. 4th Int. Conf. Blockchain Technology and Information Security (ICBCTIS), Wuhan, China, 2024, pp. 36–42, doi: 10.1109/ICBCTIS64495.2024.00014.

[10] X. Hu et al.,“ A Blockchain Cross-Chain Transaction Method Based on Decentralized Dynamic Reputation Value Assessment,” IEEE Trans. Netw. Service Manag., vol. 21, no. 5, pp. 5597–5612, Oct. 2024, doi: 10.1109/TNSM.2024.3433414.

[11] L. Cao and H. Yang, “Two-Phase Election Algorithm for Cross-Chain Notaries,” in Proc. 3rd Int. Conf. Computer Science and Blockchain (CCSB), Shenzhen, China, 2023, pp. 53–58, doi: 10.1109/CCSB60789.2023.10398755.

[12] L. Chen et al.,“ A Multiple Indicator Credit Ranking Scheme Based on Notary Mechanism,” in Proc. IEEE DASC/PiCom/CBDCom/CyberSciTech, Abu Dhabi, UAE, 2023, pp. 492–498, doi: 10.1109/DASC/PiCom/CBDCom/Cy59711.2023.10361347.

[13] X. Niu et al., “NFT Cross-Chain Transfer Method Under the Notary Group Scheme,” in Proc. 26th
Int. Conf. Computer Supported Cooperative Work in Design (CSCWD), Rio de Janeiro, Brazil, 2023, pp. 996–1001, doi: 10.1109/CSCWD57460.2023.10152551.

[14] E. Nasr et al.,“ A Disruptive Blockchain Framework for Notary: Smart Contract and Digital Record Keeping,” in Proc. IEEE Int. Multidisciplinary Conf. Engineering Technology (IMCET), Beirut, Lebanon, 2023, pp. 253–258, doi: 10.1109/IMCET59736.2023.10368247.

[15] J. Wang et al., “Cross-chain Supervision Mechanism of Distributed Notaries for Consortium Blockchain,” in Proc. 6th Int. Conf. Artificial Intelligence and Big Data (ICAIBD), Chengdu, China, 2023, pp. 579–584, doi: 10.1109/ICAIBD57115.2023.10206042.

[16] J. Goulão and A. I. Oliveira, “Blockchain Technology for E-Notary in Collaborative Networks,” in Proc. 7th Int. Young Engineers Forum (YEF-ECE), Caparica/Lisbon, Portugal, 2023, pp. 89–94, doi: 10.1109/YEF-ECE58420.2023.10209295.

[17] C. Liu et al., “Research on Cross-Chain Consensus Models in Complex Trust Environments,” in Proc. Int. Conf. Networking and Network Applications (NaNA), Qingdao, China, 2023, pp. 350–358, doi: 10.1109/NaNA60121.2023.00065.

[18] S. Haga and K. Omote, “Blockchain-Based Autonomous Notarization System Using National eID Card,” IEEE Access, vol. 10, pp. 87477–87489, 2022, doi: 10.1109/ACCESS.2022.3199744.

[19] Z. Yin et al., “Bool Network: An Open, Distributed, Secure Cross-Chain Notary Platform,” IEEE Trans. Inf. Forensics Security, vol. 17, pp. 3465–3478, 2022, doi: 10.1109/TIFS.2022.3209546.

[20] Y. Sun, L. Yi, L. Duan, and W. Wang,“ A Decentralized Cross-Chain Service Protocol Based on Notary Schemes and Hash-Locking,” in Proc. IEEE Int. Conf. Services Computing (SCC), Barcelona, Spain, 2022, pp. 152–157, doi: 10.1109/SCC55611.2022.00033.