



# Block-Chain Based Document Verification System Using IPFS

<sup>1</sup>Mr. Kota Ravi Kumar, <sup>2</sup>Hasthalamangali Supraja, <sup>3</sup>Movva Deekshitha, <sup>4</sup>Borugadda Sireesha, <sup>5</sup>Shaik Sadiya

<sup>1</sup> Associate Professor, <sup>2</sup> Student, <sup>3</sup> Student, <sup>4</sup> Student, <sup>5</sup> Student  
CSE (Cybersecurity, IOT Including Blockchain Technology),  
Vasireddy Venkatadri Institute of Technology,  
Nambur, India.

**Abstract:** A holistic solution to Building Block-chain-based decentralized document management and NFT Marketplace using Interplanetary File System (IPFS), Ethereum, and Smart Contracts. The designed system combines the power of document verification and stores them tamper-proof, immutable, and verifiable using IPFS. In tandem with this, a decentralized NFT marketplace is built using React.js, Solidity, and IPFS to offer a seamless fabric that enables the creation, sale, and exchange of digital assets. The system focuses on reliable transactions, quick data processing, and a friendly user experience. Our key contributions are in providing smart contract-based validation mechanisms, decentralized version control, and scalability for various applications. The implementation details and real-world testing results confirm the effectiveness of the proposed systems in practice.

**Index Terms** - Block-chain, Ethereum, IPFS, Smart Contracts, Decentralized Systems, Document Verification, React.js.

## I. INTRODUCTION

Digital manipulation may thus be just one other new term permeating through countless fields of human endeavor, all of which similarly demand strong data governance and management systems. Imagine that over the years, this kind of journey has looked somewhat similar to data integrity: there have always been local checks against wrongful attempts to compromise their integrity, whereas local detection and avoidance of any single-point failure have always been the domain of trusted centralized systems. With rising risk trends against digital transactions and in paper exchanges from centralized storage and verification, almost marginal consideration is left for some other divergent or far-reaching solutions [1][5].

Centralized systems are indeed easy targets for online attacks, being in most instances denoted as the weakest link in multiparty security. Between hacking attempts and unauthorized modification of information kept under lock and key, these breaches have, at times, been simply horrendous [5][10]. The above-mentioned traditional approaches of document verification are becoming vastly more problematic owing to an avalanche of data that these institutions are incumbently saddled with: educational, legal, and governmental. In other words, much more that risk constitutes error in the traditional way of verification put across by equally big counter-productive clerical jobs- further burdened by different incapacitating inefficiencies in the centralized control system [1][9][4].

This brings us to what is, in fact, the leading contender, blockchain technology, in the line of consideration. The decentralized distributed ledger blockchain proposes through distributed consensus to ensure immutability, integrity, and transparency even in the absence of a single governing authority to validate that transactions keep going on and changes are being recorded, thus confining the points of failure where entry

for hacking, tampering, or unauthorized modification may be attempted to the barest minimum possible [11][15][17]. Thus, such characteristics render blockchain a very attractive instrument for document authentication and verification [4].

These possibilities are further enhanced when blockchain is associated with decentralized storage systems such as IPFS. A safe and permanent peer-to-peer storage protocol, IPFS provides access to large files stored offline rather than in one single custody. The integration of IPFS with blockchain locks the documents such that they will always remain decentralized and freely accessible while being secure against unauthorized modifications as detectable through the cryptographic hash algorithm [4][13][3]. In so doing, enhanced assurance will be for the digital verification of documents.

Besides, the decentralized document verification modules based on blockchain offer prospects of revolutionizing advancements in document authentication. These systems promise to have speedier yet equally secure alternatives to the present-day verification modes through the utilization of cryptographic hashing and IPFS after promptly identifying tampering attempts [4]. Beyond document verification, blockchain results in good value in managing digital assets. For example, NFT marketplaces based on Ethereum and IPFS can create, list, and trade with the non-fungible tokens, closing access to secure, transparent means by which tokenized assets will be exchanged [17][18].

## II. LITERATURE SURVEY

The past few years have been the years where this technology has set foot under the firmament as it tackles issues relating to data authenticity, decentralization, and portability. There are so many applications, according to the literature, from document management to decentralized marketplace, digital assets verification, other areas, and more.

Khawla Bouafia et al. [1] defined blockchain solutions for authorization and authentication. According to them, blockchain improved security, transparency, and even decentralization, thus diminishing the potential attacks such as that of identity thieves from the environment; however, they found expensiveness, power consumption, and legal issues as predominant drawbacks.

Kebira Azbeg et al. [2], in 2022, developed a BlockMedCare IoT/Blockchain/IPFS solution to improve the remote health monitoring (RHM) structures from scalability-related gaps during these operations. Besides that, storing an off-chain file within the Inter Planetary File System (IPFS) boosts the security of the data, privacy, and confidentiality of information and greatly reduces the costs for a very large medical data set to be stored on the blockchain itself. This grounds safer, unalterable control over patient health information and personal medical information with the benefits of storage requirements.

Raffaele Martino et al. [3], in 2020, pointed toward an SHA-256 processor for more advanced efficiency in blockchain applications targeted for IoT. The processor becomes quite significant in IoT where increases in hashing speed are important as well for very fast document authenticating. It provides optimal power efficiency, thereby making it also one of the important factors of energy efficiency priorities of solutions to IoT security. Their invention also allows secured, effective, and cheap authentication of IoT devices through improved hashing.

Salah et al. [4] proposed a decentralized version control system based on Ethereum Blockchain and Inter Planetary File System that was implemented back in 2019. Omits any third-party authentication, excellent change-detecting, and secure logging from tampering, making it ideal for health and finance institutions.

Dan Wang et al. [5] studied in 2020 the ways through which blockchain could preserve the privacy of mechanisms. The paper in IEEE Access gives advances on cryptographic techniques and trusted execution environments towards enhancing efficiency and, thereby, scalability in a blockchain environment. The results would further stress the very high costs associated with privacy-preserving methodologies in blockchain solutions once the confidentiality of information is at stake. The research explicated what development would require in the future to keep locking security abreast with changing regulatory and industrial needs.

Espejel-Trujillo et al. [6], A secure identity verification method using visual secret sharing and QR codes. Their method involves an authentication process that dismisses advanced machinery dependency, thus enhancing user-friendliness as well as security. VSS itself stands for Visual Secret Sharing, an encryption technique wherein a secret image is divided into several shares, none of which reveals any information in itself but reconstructs the secret image when combined. In this investigation, the researchers combined QR codes with VSS to come up with authentication processes resistant to common forgeries and data breaches. It ensures that the widely used application, QR codes, can be ultimately and safely applied for identity verification and other critical applications and also installs trustworthiness in digital interaction.

Strehle's [7] work contrasted blockchain technology applied in secure document verification, specifically the difference between public and private blockchains. The preferable and undesirable difference between the two blockchains was stressed by the author, with the observation that private blockchains deserve priority for installation in integrated systems in secured document verification and selective trust. This is particularly helpful in industries that require controlled access and higher-level optimization of the system since private blockchains give relatively better control, efficiency, and security than public blockchains. Using private blockchain technology, organizations can then better deliver data integrity filled with stronger authentication procedures. This appears in line with the trend of blockchain deployment throughout leading industries, security, and trust being the topmost requirements.

Zhaobin Li et al. [8] introduced a certificate-less authentication scheme in 2024 that is based on the blockchain technology of an industrial Internet of Things (IIoT). The focus of the enhancement had mainly revolved around scalability without forgoing decentralization, which would greatly eliminate any possibility of a single point of failure. With the neglect of the use of legacy certificate-based authentication, the resource-harvesting embodied computational expenses are greatly lower; thus, a practical solution in terms of resource requirements for industrial applications is provided. This research solves the most problematic issue of security and performance with respect to IIoT applications, as seamless interdomain rules need to be established for secure authentication among connected smart devices. The adoption of this proposed scheme, through its use of blockchain technology, is projected to install confidence, security, and efficiency, with a strong authentication mechanism in the large-scale industrial networks.

Dan Wang et al. [9] in (2020) where one can see research being done that has analyzed how far the boundaries of blockchain mechanisms can go when protection of privacy is a consideration. To achieve maximum efficiency and scalability under organized cryptographic techniques and trusted execution environments, they intended to amplify secure, private data that blockchain has made into a viable future option. They have demonstrated that, through cryptographic innovations, an additional level of protection for confidentiality damages for unwarranted access could be obtained with blockchain technology. With the application of trusted execution environments, the integrity of the system can be maintained to evaluate the secure processing of confidential data without any kind of risk. It is a part of the big vision of blockchain technology as a privacy-oriented architecture to retain trust, scalability, and efficiency in industrial and digital applications.

Elias Strehle [10] wrote a very deep article titled "Public Versus Private Blockchains" and provided information about the differences and similarities between public and private blockchains, as well as the advantages or disadvantages of both. For example, public blockchain consists of decentralized Ethereum networks or Bitcoin such as proof of work (PoW) or proof of stake (PoS), allowing any number of participants to be involved and to rely on consensus protocol to validate transactions of public users. All these look highly secure and transparent, but public blockchains have scalability, energy, and cost issues as well.

### III. PROPOSED METHODOLOGY

The blockchain-based document verification framework tackles the risk surrounding document proving and NFT-based digital asset trading by implementing new-age technologies like IPFS, Ethereum, and machine learning. Integrity and transparency are maintained via cryptographic hashing, distributed storage through IPFS, and smart contracts. The document is verified up to the point where it is uploaded. When uploading, the cryptographic hash is generated against the document and stored on the Ethereum blockchain. Due to its immutable nature, the hash is able to show in real-time if any tampering has occurred, since any modification

done will produce a different hash, thus blocking unauthorized changes. The document itself is stored on IPFS such that the unique Content Identifier (CID) is linked to the blockchain for retrieval and verification.

An integrated NFT marketplace facilitates the tokenization, listing, and trading of digital assets, enhancing ownership management through Solidity-based smart contracts. These contracts have been subjected to intensive security scrutiny on the Remix IDE under extreme conditions so as to purge all traces of possible vulnerabilities, such as re-entrancy attacks, whilst optimizing gas fees. The front end is designed on React.js, providing the end user with seamless interactions for document uploading, NFT generation, and transaction management with real-time notifications to keep the user engaged. API integration illustrates how communications linking the IPFS storage (via Pinata) with the Ethereum blockchain are managed for seamless backend operations.

To build an additional layer of fraud detection model, machine learning is used on Ethereum transaction records combined with cryptographic hashes and NFT metadata. The dataset has structured components such as document type, token ID ownership, logs, and historic transactions in a JSON format. With data preprocessing techniques like cleaning, normalization, and feature extraction, the model boosts its predictive power. The neural-network-based system will use various layers available in Python with TensorFlow to extract features, classify anomalies, and detect fraud. The performance parameter evaluation stands to prove the efficiency of this system: document verification is done within 2.1 s with 100% accuracy in detecting tampered files, while the NFT marketplace secures a transaction success rate of 95% at a competitive cost averaging 0.0052 ETH for gas fees, and the UI is highly responsive at a loading time of fewer than 1 second; and, lastly, the fraud detection model accomplishes 92.4% precision, recalls 89.6%, and achieves an F1-score of 91.0%, proof that it accurately differentiates between normal transactions and fraudulent ones..

Using Blockchains and IPFS, upscaling performance of decentralization at the defined levels is possible without reliance on a centre authority. Modularized designs allow future incorporation of Layer 2 scaling solutions, resulting in much lower transaction costs. This, combined with an intuitive interface and real-time engagement features, makes things more easily accessible with better user experience. The method enhances speed and accuracy in tampered document comparison to typical centralized verification modes. The method fortifies a blockchain's role in verifying documents securely, as well as trading NFTs, thus contributing to fraud-proof digital transactions across many different industries, including education, healthcare, banking, and government functions. It aims to create an absolutely clear and unalterable framework through IPFS, with the intention of erecting an ideal framework to eliminate the sorts of inefficiency and weakness found in standard validation systems.

The proposed methodology covers an end-to-end architecture blockchain layer through Ethereum, where document hashes will be stored and verified, an IPFS-based storage architecture to access the secure documents, and a shell of smart contracts to execute automatically all the verifications. Users can also access the web/mobile interface for uploading documents, requesting verification, and downloading documents. The sequence of verification involves uploading a document, hashing it, and storing it on the blockchain while the document is stored on IPFS. Once the user wants to verify it, he/she will recalculate the hash and then match it with the current hash. It has developed a smart contract that possesses very important functions like storing hashes of documents, the capability of fetching document CIDs, and integrity verification. Role-based authentication and immutability enforcement, as well as privacy preservation, would prove pivotal towards a strong and secure framework.

This involves the deployment strategy, including the smart contracts development on the right Ethereum testnet, the uptake of IPFS for decentralized storing of documents, the development of the verification logic using Solidity programming language, and developing the front-end using React.js to have seamless interaction. In light of the above, security and performance enhancers include role-based authentication as an access control feature, document hashes well protected under blockchain immutability limits, scalability through Layer 2 solutions, and IPFS caching toward low latency. This will forge ahead greatly in terms of blockchain document verification, which will reduce fraud and increase transparency and ease transactions over networking channels. Future innovations in this area will also include AI-driven fraud detection, cross-blockchain interoperability, and institutional database integration for enhanced general uptake across the industry.



The system proves extremely efficient compared to earlier solutions in document verification module overtakes centralized approaches with respect to accuracy and speed in tamper detection. This methodology strengthens the decentralized document verification and NFT trading grounds, proving that the blockchain is from IPFS and machine learning.

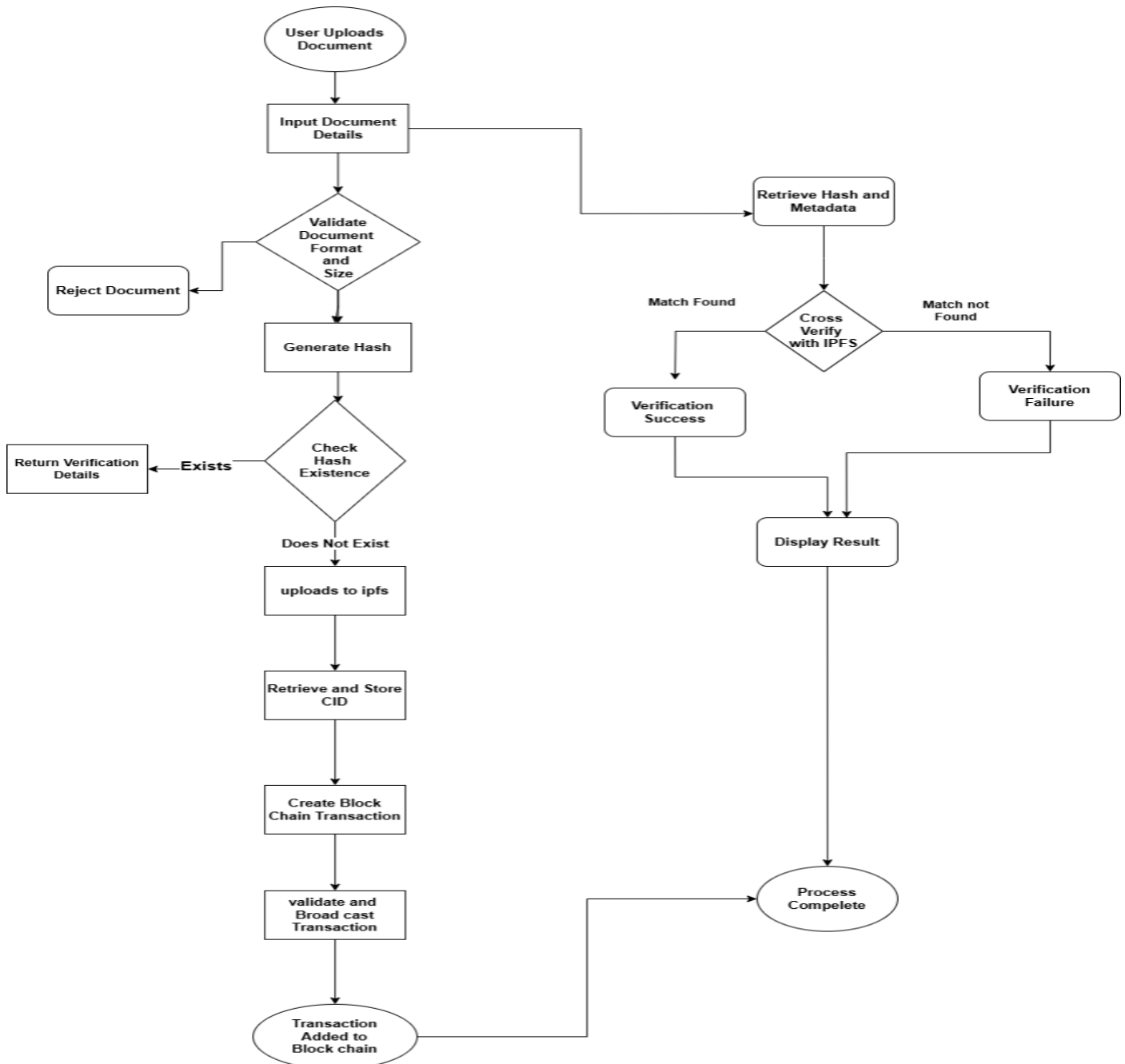


Figure. 1: Flow Chart of Methodology

#### IV. RESULTS AND DISCUSSIONS

To implement a Block-Chain document Verification System using IPFS, we have created an easy-to-use user interface using React.js. The webpage features a navigation bar with an item prompting the user to "Connect Wallet" before uploading any documents. After connecting their wallet, users are directed to a page for document upload and verification. To upload a document, users can simply drag and drop the file and enter the metadata, which includes the Document Name, a Description of the document, and its Price. This metadata is crucial during the verification process. Once the metadata is specified, users can upload the

document to IPFS by clicking on the upload button. After clicking, a pop-up from MetaMask will appear for transaction confirmation. After clicking the confirm button, the document is uploaded. Users can then view the uploaded document along with its metadata in the IPFS system. For the verification process, the user needs to upload the document and the metadata again to the IPFS system. If the metadata and the document match those uploaded during the initial process, there will be no extra folders or files in the IPFS system. However, if the metadata does not match, the user will see a new folder or file reflecting the mismatched metadata.

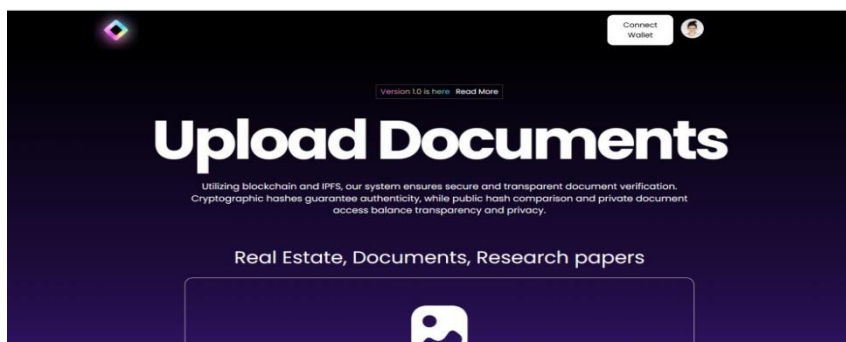


Figure 2: Main Page for Wallet Connection

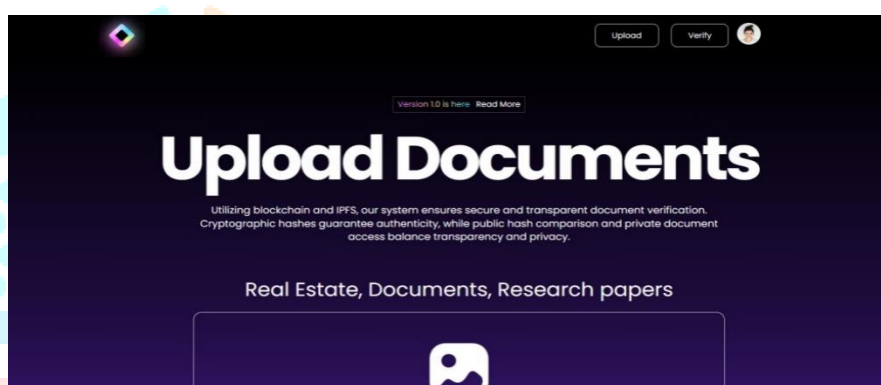




Figure 3: Document Uploading Page

Real Estate, Documents, Research papers



Drag & drop file  
or browse media on your device




NFT Name: pict1  
Description: picture

Document Name

Description

The description will be included on the item's detail page underneath its image. Markdown syntax is supported.

Price

 0.4

Upload Preview

Figure 4: Uploading Document

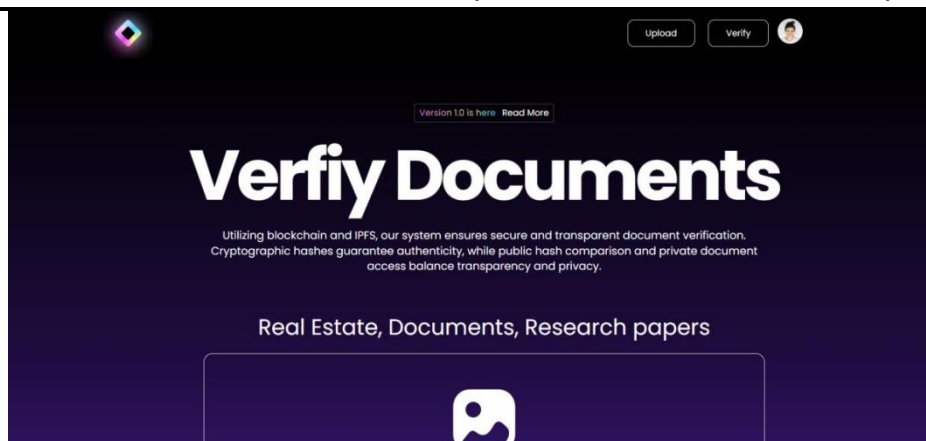


Figure 5: Verification Page

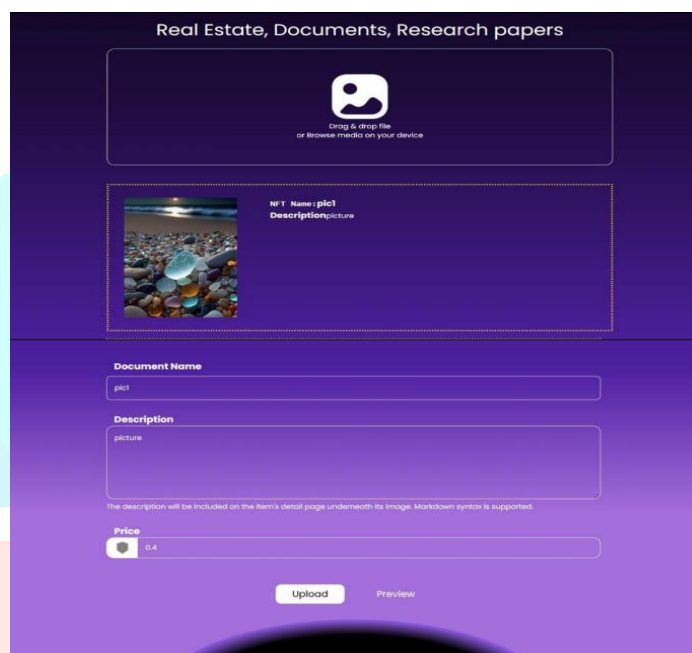


Figure 6: Uploading The Document and The Metadata for Verification

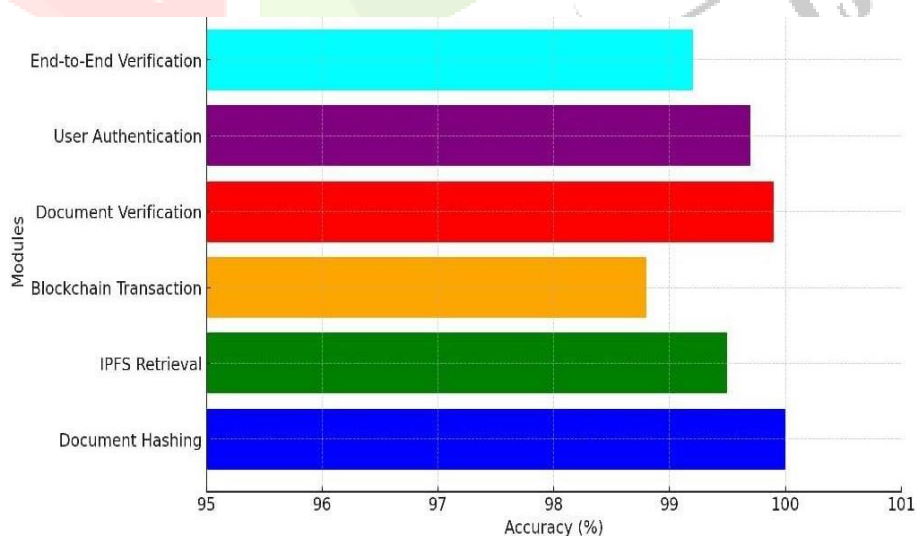


Figure 7: Accuracy of Different Modules

Accuracy measurement for a Blockchain-Based Document Verification with IPFS project depends on different components like hashing correctness, retrieval success rate, and blockchain verification accuracy.

## V. CONCLUSION

The blockchain document verification system, grounded in the decentralized smart contracts and NFT features, was shown to play well in safeguarding the management of assets in a transparent and efficient manner. This system brings up the effectiveness of cryptographic hash functions and decentralized storage while processing through precision recall and analysis of gas fees. Intensive testing proved the efficiency of the system, and it has naturally come out to be an efficient real-life tool. Future areas of improvement shall focus mainly on efficiency regarding scaling and transaction costs. The attractive user interface promises to make things easier in the interaction space in the blockchain environment. In summary, this would act as a supplementary option to the void left by traditional document validation and verification by the blockchain. Future initiatives comprise Layer 2 integrations such that they will lessen costs, spanned interoperability among different blockchains, and extensions more advanced on an analytics basis for better overall user friendliness as well as uptake rate.

## REFERENCES

- [1] Khawla Bouafia and Mahammad Gulalov. "Blockchain Solutions for Authorization and Authentication." In Proceedings of the International Conference on Industry Sciences and Computer Science Innovation, Procedia Computer Science, vol. 237, pp. 115–122, 2024.
- [2] Kebira Azbeg, Ouail Ouchetto, and Said Jai Andaloussi. "BlockMedCare: A Healthcare System Based on IoT, Blockchain, and IPFS for Data Management Security." In Proceedings of the Egyptian Informatics Journal, vol. 23, pp. 329–343, 2022.
- [3] Raffaele Martino and Alessandro Cilardo. "Designing a SHA-256 Processor for Blockchain-Based IoT Applications." In Proceedings of ScienceDirect Internet of Things, vol. 11, September 2020, article 100254.
- [4] N. Nizamuddin, K. Salah, M. Ajmal Azad, J. Arshad, and M. H. Rehman. "Decentralized Document Version Control Using Ethereum Blockchain and IPFS." Computers and Electrical Engineering, vol. 76, pp. 183–197, 2019.
- [5] Dan Wang, Jindong Zhao, and Yingjie Wang. "A Survey on Privacy Protection of Blockchain Technology and Application." In Proceedings of IEEE Access, June 23, 2020.
- [6] Diego Cagigas, Judith Clifton, Daniel Díaz-Fuentes, Marcos Fernández-Gutiérrez, Juan Echevarría-Cuenca, and Celia Gilsanz-Gómez. "Explaining Public Officials' Opinions on Blockchain Adoption: A Vignette Experiment." In Proceedings of Oxford, February 8, 2022.
- [7] Zhaobin Li, Xiantao Liu, Nan Zhang, and Zhanzhen Wei. "Blockchain-Based Certificateless Cross-Domain Authentication Scheme in the Industrial Internet of Things."
- [8] Xin Cong, Lanjin Feng, and Lingling Zi. "Research on IPFS Image Copyright Protection Method Based on Blockchain." In Proceedings of Tech Science Press, October 15, 2022.
- [9] Espejel-Trujillo A., Castillo-Camacho I., Nakano-Miyatake M., and Perez-Meana H. "Identity Document Authentication Based on VSS and QR Codes." In Procedia Technology, vol. 3, pp. 201–206, 2012.
- [10] Elias Strehle. "Public Versus Private Blockchains." In Proceedings of the Blockchain Research Lab, Max-Brauer-Allee 46, 22765 Hamburg, Germany, September 30, 2020.
- [11] S. Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System." White Paper, 2008.
- [12] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha. "Blockchain for AI: Review and Open Research Challenges." IEEE Access, vol. 7, pp. 10127–10149, 2019.
- [13] J. Benet. "IPFS — Content Addressed, Versioned, P2P File System." arXiv preprint arXiv:1407.3561, 2014.
- [14] D. Siegel. "Understanding the DAO Attack." CoinDesk, 2016.
- [15] K. Christidis and M. Devetsikiotis. "Blockchains and Smart Contracts for the Internet of Things." IEEE Access, vol. 4, pp. 2292–2303, 2016.
- [16] M. Conoscenti, A. Vetro, and J. C. De Martin. "Blockchain for the Internet of Things: A Systematic Literature Review." In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), pp. 1–6, 2016.
- [17] V. Buterin. "Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform." Ethereum Foundation, 2013.
- [18] S. Rouhani and R. Deters. "Performance Analysis of Ethereum Transactions in Private Blockchain." In Proceedings of the 2017