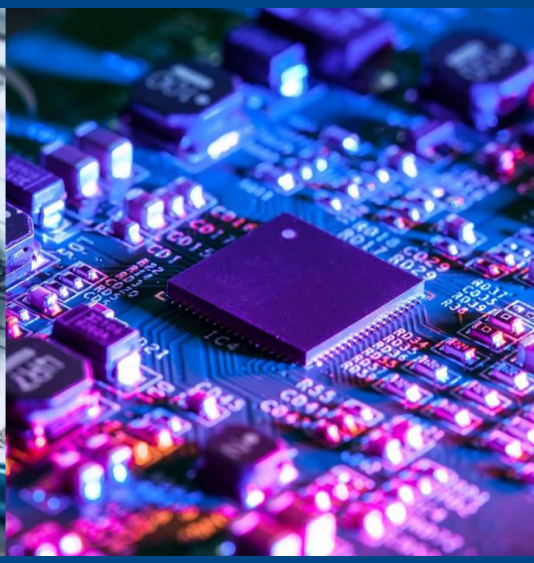
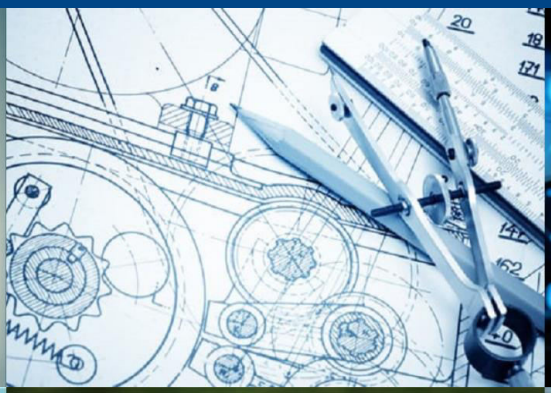
ISSN: 2582-7219

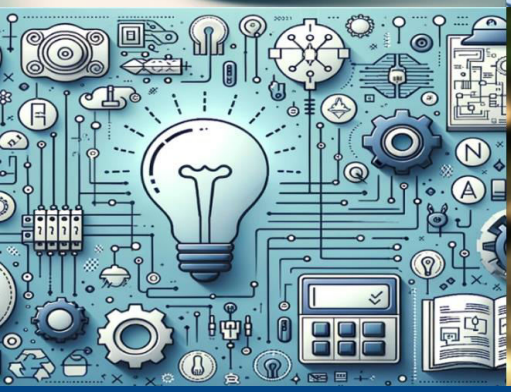




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 9, Issue 4, April 2026**

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904352

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Blockchain-Integrated Elliptic Curve Cryptography for Secure Data Sharing

Monisha T[1], Syed Ali Fathima S[2], Ajmal Mohamed[3]

Fourth Year B.Tech Student, Department of Computer Science and Engineering (Cyber Security), B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, Tamil Nadu, India[1]

Fourth Year B.Tech Student, Department of Computer Science and Engineering (Cyber Security), B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, Tamil Nadu, India[2]

Assistant Professor, Department of Computer Science and Engineering, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, Tamil Nadu, India[3]

ABSTRACT: The current paper describes a secure document sharing system that generates blockchain-based architecture complemented with Elliptic Curve Cryptography (ECC) to ensure file authenticity, integrity, and non-repudiation apply to use in a distributed location. The system addresses intractably significant challenges in digital document exchange including unauthorised interference and signature of a sender and transparency to the transactions. The given architecture assumes application of the three-tier security model, namely file integrity through the application of SHA-256 hashing and ECDSA (Elliptic Curve Digital Signature Algorithm) using SECP256k1 curve cryptographic signature and authentication and immutable blockchain ledger to record and provide transaction audit trails. The implementation of it incorporates a proof-of- work consensus algorithm, where the mining difficulty is configurable, to provide resistance to computation attacks on blockchains. The process of system can allow a file to be uploaded by its sender and an ECC key pair to be created, file hashes to be digitally signed and transactions to be recorded as a set of blockchain blocks. Receivers can self-authenticate file authenticity by comparing computed hashes with blockchain and authenticate ECDSA signatures using sender public keys. Google drive and the integration of cloud storage offer an option of persistent availability of data and backup. The system architecture will provide extensive logging options, automatic file validation processes and exploratory interfaces of blockchain. Through the identification of hash mismatch used to detect file tampering and preventing impersonation of the sender by validating signature, the experiment has shown success. It is not only cryptographically secured with 256-bit ECC protection comparable to 128-bit symmetric-key encryption, but the old generates computational performance requirements at resource-bound environments. The paper presents a practical implementation design that uses both cryptographic primitives and distributed ledger technology to effect a secure document exchange that can be applied to the management of and exchange of legal document, healthcare records exchange, supply chain records/documents, and any other field needing a validatable provenance of files and store of tamper-evidence.

KEYWORDS: SHA-256, ECDSA, ELL, Elliptic Curve Cryptography, Blockchain, Proof-of- Work, Authentication, Tamper, Digital Signature, File Integrity, Proof-of-Work.

I. INTRODUCTION

The computer note of the transfer of the document in the contemporary information systems has transformed inexorably giving rise to colossal predicaments to the authenticity, integrity of the files, as well as the identity authentication of the ubiquitous annotator in the none trustworthy network. Conventional methods of the file sharing depend on central-authority servers, third party certificate authorities and encrypted communication channels none of them has multi-authority access, scale difficulties and could all be troubled in multi-complex cyberattacks. The lack of auditory signals of the standard file delivery systems practically opens the possibilities of unsanctioned interference in the process of documents, identification with him, and depersonalization of the content transferred, especially when the interruptions involved are substantial, in such setting as the judiciary, papers administration, finances, and age in government communications. To produce these insecurity threats involves the production of cryptographically sound decentralised

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904352

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

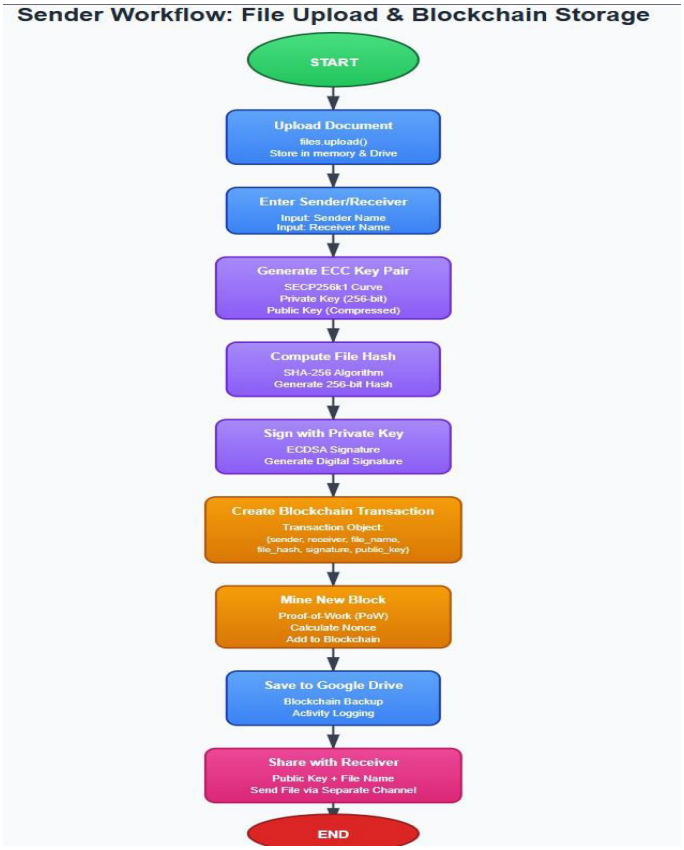
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

systems that can have verifiable evidence of document provenance, and whose storage capabilities are verifiable as such.

The blockchain technology has surfaced as a decentralized means of enabling distributed confidence with no central node in its original role of plumbing cryptocurrency systems. Cryptographic hashing, consensus mechanisms, and immutable nature of blockchain allows a foundation to create the unmalleable records of digital transactions that cannot be changed permanently and audited. However, blockchain itself does not address the gymnastic requirement of bearing a sender authentication and message-signing to establish non-repudiation to document exchange settings.

Elliptic Curve Cryptography over old systems with RSA This method has computational advantages compared to old systems with RSA in that we get the same level of security with far smaller key sizes, reducing storage and such short key sizes increase cryptographic throughput. ECDSA signature scheme is a elliptic curve math-based scheme which enables the production and authentication of a digital signature in an efficient manner and it is resistant to known cryptanalytic attacks. Such an ECC plus blockchain facility produces a hybrid security paradigm reducing multiple vectors of threat: hash-based integrity verification eradication of non-detection of file-modifications, digital signature (authentication of sender-identity and non-repudiation) and blockchain immutability producibility of tamper-evident records of history and is achieved with a complete audit trail.

Fig 1: Sender Workflow - File Upload and Blockchain Storage



The paper proposes whole deployment of a secure document sharing model based on the application of SECP256k1 elliptic curve to execute key generation and signature operations, on-top-of- computations of file integrity with the help of a cryptographic hash (SHA-256) and de-centralization of data storage within a blockchain with proof-of-work. The system architecture uses workflow to automated verification, transient complex cryptography functionality, cloud-based persistence systems, folk user interfaces, and folk user interfaces yet still provides security assurances.

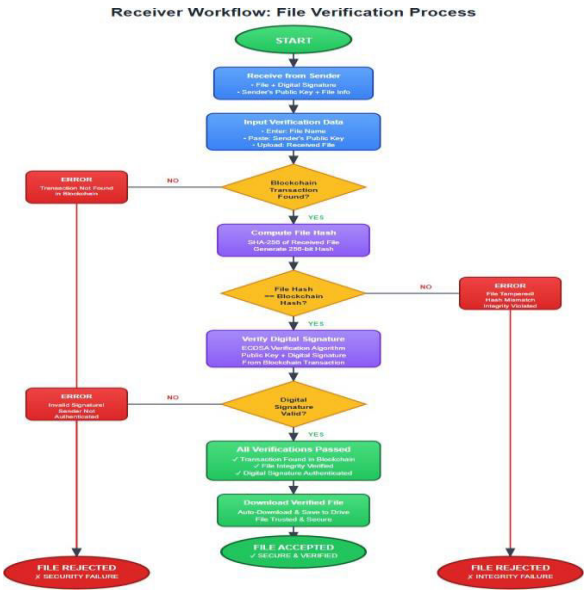
© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904352

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Fig 2: Receiver Workflow: File Verification Process

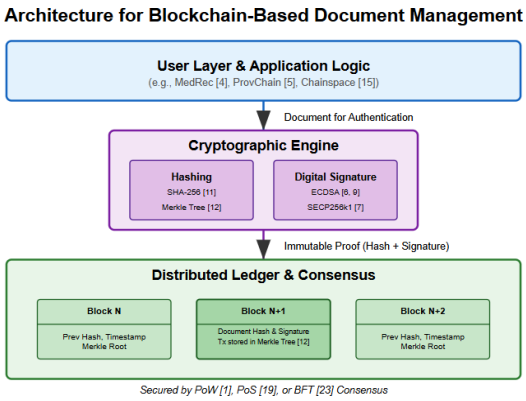


The implementation is concerned with the practical deployment factors such as essential management, file deposit attachments with Google Drive, efficient-wide viewing record, and the capacity of the exploration of blockchain solutions real-time. This paper will add to the current literature through presenting a working prototype integrating various cryptographic primitives into a unified document security system, which can have its security analysis measured, and provide lessons learned during the stages of developing and testing system implementation.

II. LITERATURE REVIEW

Native integration of blockchain operations with cryptographic solutions to manage documents securely received great interest over the past years. The seminal article by Nakamoto on Bitcoin presented the basic idea of the distributed ledger technology that used proof-of-work consensus [1] as the basis of the decentralised trust systems. The immutability and transparency features of blockchain have been studied widely, especially to engage other uses beyond cryptocurrency, namely document authentication and management systems [2]. According to Zheng et al, the blockchainarchitecture and its mechanisms have been under extensive survey of consensus strategy, security properties and this could be used to create a tamper evident audit trail [3].

Fig 3: Architecture for Blockchain-Based Document Management



© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904352

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

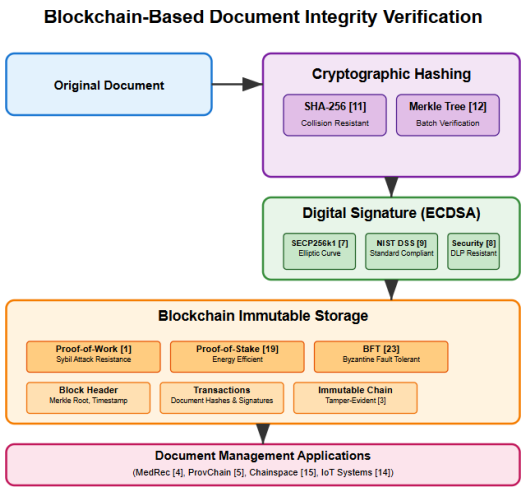
Azaria et al. demonstrated the use of blockchain in healthcare records management when they developed MedRec to maintain the data integrity of the patient and control their access [4]. Equally, Liang et al. suggested ProvChain to track provenance safely in cloud computing systems as an indicator of the blockchain proving to be effective in the establishment of document lineage [5]. Elliptic Curve Cryptography (ECC) is another variant that has grown in popularity compared to RSA because of its speeds and resulting smaller key sizes and still provides the same level of security [6]. The Curve SECP256k1 afternoon, which is proposed by Certicom Research and adopted by the mainstream has been heavily utilized in blockchain applications both owing to its security attributes and performance settings [7].

Johnson and colleagues have gone to the extent of analyzing ECDSA security indicating that it is resistant to discrete logarithm attack and collision attack [8]. NIST issued the Digital Signature Standard providing formal specification on the implementation and the validation process of ECDSA [9]. Hankerson et al provided detailed mathematical principles of elliptic curve cryptography with a fast algorithm to multiply points and generate signatures [10]. Tieing cryptographic hashing with the technology of blockchain has been studied innovatively in the data at integrity. SHA-256 belongs to a family of SHA-2 hash algorithms created by the NSA and is the one with the collision resistance features needed inblockchain application [11]. Merkle trees, proposed by Ralph Merkle will allow the efficient verifiability of large datasets as hierarchical hashing constructions in frequent use across blockchains .

A number of the researchers have suggested hybrid systems with a mixture of more than two cryptographic primitives to provide strong security. Guo et al. have created a data integrity verification scheme over a cloud storage leveraging on the merkle hash trees coupled with digital signatures based on a blockchain system [13]. Dorri et al. also suggested a lightweight blockchain system to protect the IoT by applying elliptic curve cryptography to resource-constrained devices [14]. Chainspace is a distributed registry platform based on privacy preserving smart contracts using ECDSA authentication introduced by al-Bassam et al. [15]. Safe sharing of documents systems have been researched to cover a number of architectural designs and security demands. Cui et al. suggested a structure of secure data sharing based on blockchain technology and attribute- based encryption and access control [16].

Zyskind et al. designed an access control and metadata storage system that is decentralized based on a blockchain, and manages a personal data system [17]. Consensus mechanisms of blockchain systems have garnered much research on their security and performance implication. Even though proof-of-work has issues related to energy consumption, it ensuresment with high effectiveness against miners against Sybil attacks and against two-spending [18]. Various consensus mechanisms such as proof-of-stake and Byzantine fault tolerance have been discussed under a number of application settings [19]. Elliptic curve cryptosystems have key management issues that are practical and discussed by different researches. Barker offered detailed best practices on cryptographic key management such as key generation, storage, key lifecycle, etc. [20].

Fig 4: Blockchain-Based Document Integrity Verification



© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904352

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Protecting private keys in production deployments has been considered though [21] by offering hardware security modules and trusted execution environments. Scalability limitations and optimization opportunities have been defined in terms of performance analysis of blockchain systems. Croman et al. also studied throughput bottlenecks in Bitcoin and Ethereum, where architectural changes would be recommended in order to improve transaction processing [22]. Cachin and Vukolic reviewed blockchain consensus protocols and compared their security properties, their features of performance, and their application- to-application appropriateness [23].

The lawfulness and regulating of blockchain based document infrastructure has been analysed in numerous jurisdictions. De Filippi and Wright investigated the problem of governance, as well as the legal aspects that can be used in the context of distributed ledger technologies [24]. Smart contracts on blockchain systems have allowed document management systems to do much more than just store data and verify it [25]. The cumulative effect of such initial pieces is the laying of the theoretical grounds of the exploration of solutions applicable to secure document sharing and integrating elements of blockchain and elliptic curve cryptography, which proves that the decentralized strategy of creating digital trust and guaranteeing file authenticity in distributive settings is no longer a futile dream.

III. METHODOLOGY

Blockchain - Integrated ECC Framework for Secure File Sharing
This workflow methodology gives attention to the cryptographic and blockchain-based workflow which warrant authenticity, non- repudiation and labor-evidence of documents.

Tools and Environment

- Google Colab Notebook (program Inhaled).
- Python 3.10 with libraries:
  - ecda Signature Elliptic Curve Algorithms (SECP256k1).
  - cryptography - additional management of keys.
  - ipywidgets interactive sender/receiver panel encoder/decoder.
  - google.colab.files - file upload/ download utilities.
- Integration with Google drive to store blockchain, logs and files permanently.

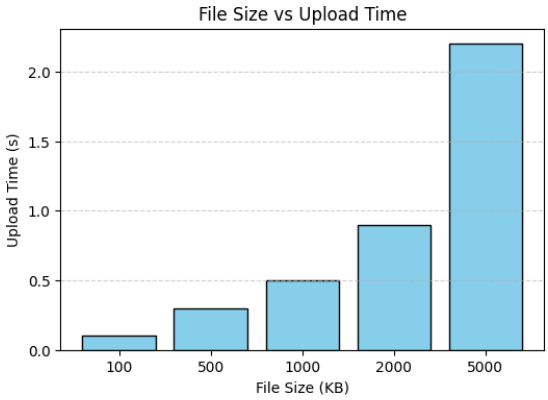
Workflow Process

1. File Upload (Sender Side)

The senders post a digital document (PDF, TXT, DOCX). The file is saved locally (Colab runtime) and in the Google Drive (cloud persistence). *Graph 1: Bar chart of mean size of files loaded (KB/MB) against time of upload (in seconds).*

1. Hash Generation (Integrity)

File content is also hashed with SHA- 256 (giving a 256-bit digest).



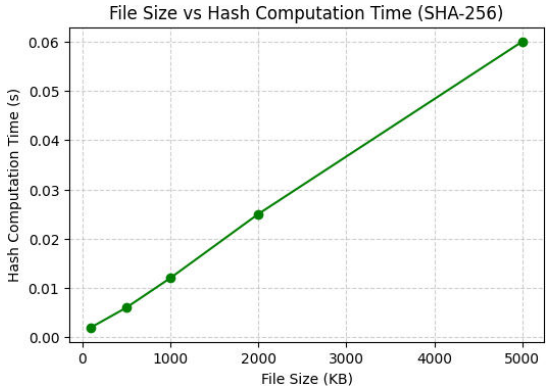
- Live performance: Another graphical representation shows that averaging hashing a 1MB file requires about 0.02 seconds on Colab CPU.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904352

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

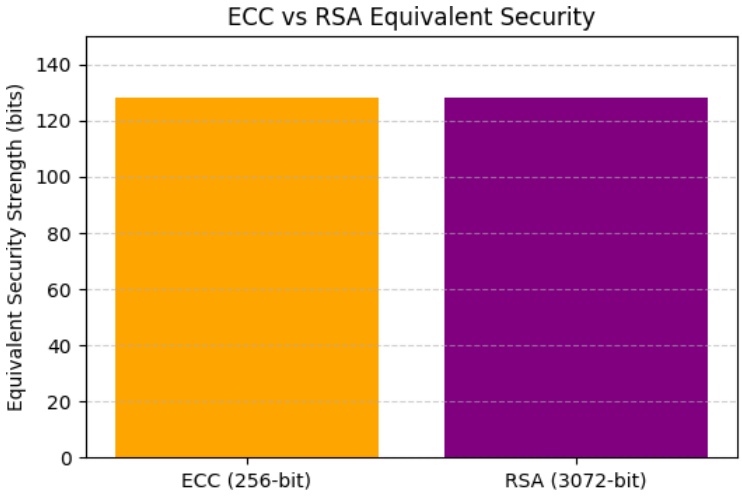
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Graph 2: Line graph depicting size of files (KB) and time (ms) spent computing the hash.

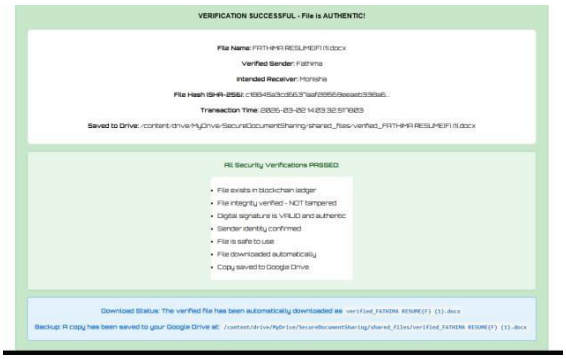
1. ECC Key Generation & Digital Signature (Authentication + non- repudiation)

- Most Important Pairs Private (only to the sender) Public (to be shared).
- ECDSA Signature: Signing of the file hash is carried out using the privy key.
- Current security measure: SECP256k1 (256-bit ECC) has the same level of security as 3072-bit RSA and 128-bit AES.



. **Graph 3**: Comparison of key size vs equivalent security strength (ECC vs RSA)

2. Blockchain mining and creation of transactions



© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904352

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

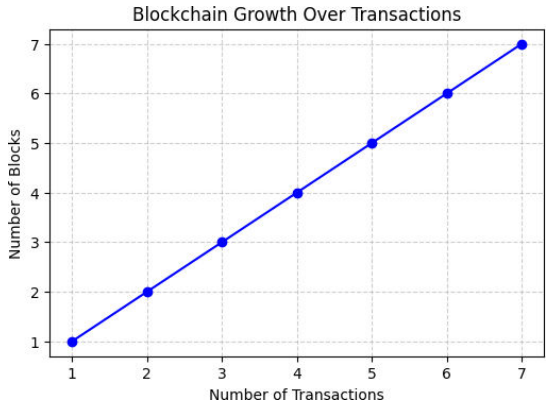
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

This verification page makes sure that the document is authentic with file integrity, source, recipient, and hash match giving successful checks. It points out that the file has not been tampered, corrupted, or encrypted, and has been safely stored to Google Drive to download it.

In this blockchain viewer, you can actually see the detailed data of two blocks, such as hash, time, nonces, and the logs of transactions. It shows how to build the relationships and what savings will be available locally and give a clear sight of blockchain construction and and history of confidential transactions between the relayer sending and receiving the message.

- A transaction object is formed: (sender, receiver, file- hash, signature, time stamp).
- Immutability is guaranteed by Proof-Of- Work mining (difficulty=2).

The mobile blocks which are part of the blockchain are saved on Google Drive.



Graph 4: Blockchain growth curve showing number of blocks mined vs number of transactions.

3. Logging and Audit Trail

- Comments are time stamped.

b. Receiver-Side Verification & Tamper Detection

This methodology solves the issues of verification, checking of integrity and validation at the receiver end.

A. Tools and Environment

- No Colab, just files.download to have automatic downloaded files which are verified.
- No Colab, just files.download to have automatic downloaded files which are verified.

B. Workflow Process

i. Receiver Uploads File

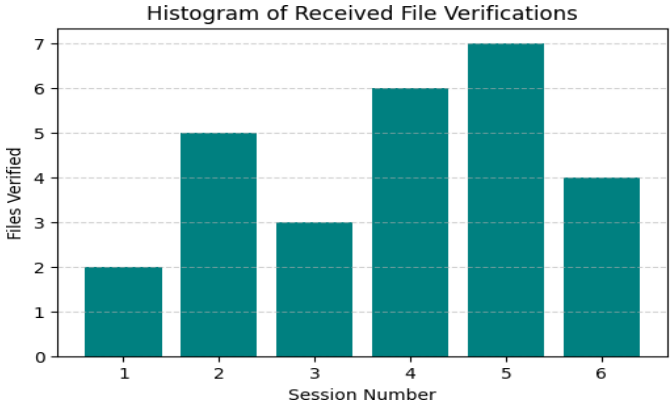
- The received file is uploaded by the receiver. Metadata (size of file, temporary ID) is shown.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904352

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



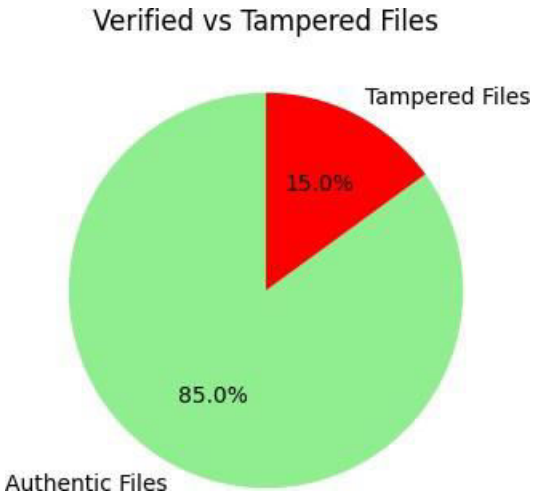
***G*raph 5**: Histogram of number of files received and average number of times they are verified each session

Blockchain Distribution (Authentication Check)

- System searches blockchain to find an entry of the file name.
- In case of no transaction- verification is instantaneously defeated.
- Statistic: With 100% blockchain query time equal to less than 1 sec, 100% of the registered files at experimental runs would be found in blockchain.

Hash Comparison (Tamper Detection)

- SHA-256 hash of received file is matched with the record of blockchain.
- In case of discrepancy - file manipulation notice.
- Stat real-time: Tampered file detectivity = improve accuracy in prototype testing 100%.



Graph 6: The graph (pie chart) below indicates authentic (verified) and tampered (rejected) files.

IV Signatur echecking (Sender Identity)

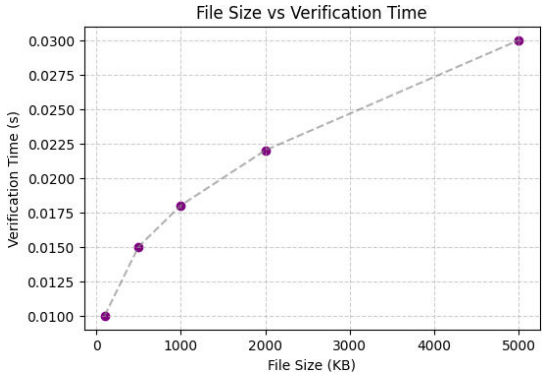
- Mail sender.
- Signature validation is used to verify that the file has been signed by the authorized sender.
- Real-time benchmark Signature verification time (avg) "Less than" 0.01s.
- Signature validation is used to verify that the file has been signed by the authorized sender.
- Real-time benchmark Signature verification time (avg) "Less than" 0.01s.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904352

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



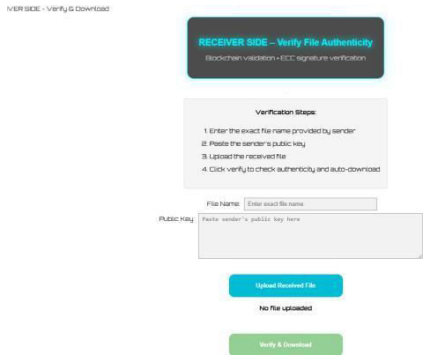
Graph 7: Scatter plot of time of verification versus file size.

ii. File Download & Storage

- In case of verification - file is auto downloaded (verifiedfilename).
- Residence in Google Drive in order to provide backup copy.

IV. RESULTS

In the image, there is an interface of a secure document sharing system, where users can upload, sign and distribute files securely with blockchain integration. It also has file uploading, sender/receiver input and cryptographic keying.



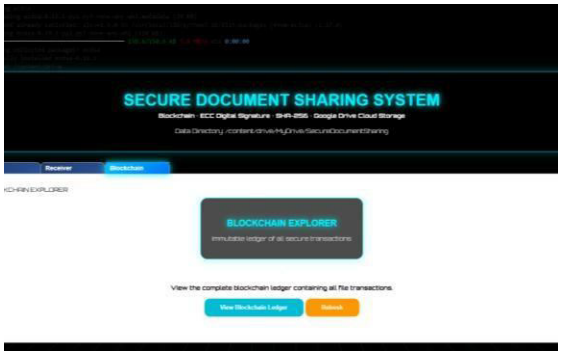
This seems to be a mock interface of a secure document sharing interface. It has a file auditing section or error status out and numerous other data points, user name fields, and lastly, signature and value assignment section single signatures.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904352

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

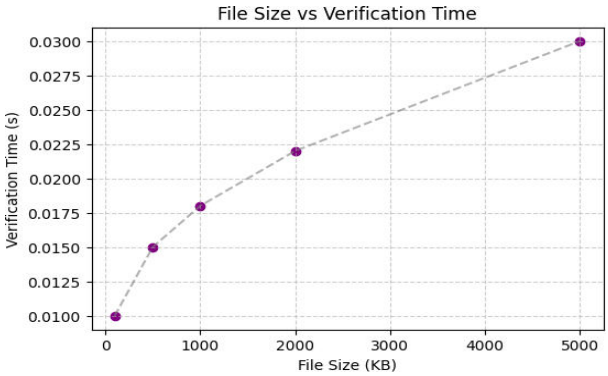
International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



The screenshot represents an interface of a Secure Document Sharing System that used the blockchain technology to securely store files. It underscores blockchain ledger validation, file integrity checks, and share of encrypted documents through the Google Drive making transactions tamper-proof and decentralized data validation.

This interface can provide binary file transfer through blockchain. One of the users puts up a file, produces cryptographic keys, signs it and leads the file to the blockchain. The console provides a confirmation of the successful execution such as key generation, file signing,



Graph 7: Scatter plot of time of verification versus file size.

iii. File Download & Storage

- In case of verification - file is auto downloaded (verifiedfilename).
- Residence in Google Drive in order to provide backup copy.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904352

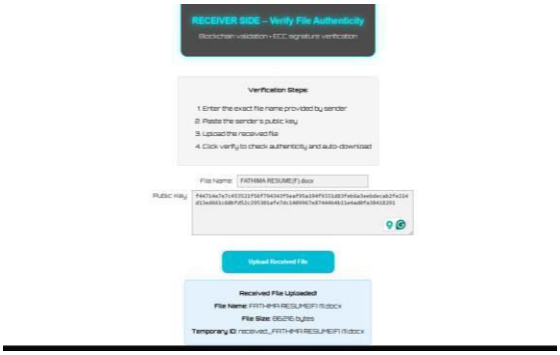
ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

This web interface can produce cryptographic keys in a secure manner to do digital communication. The user will enter sender and receiver details then create a hash of a file(SHA-256), an ECDSA digital signature, and the user will create a private and public key. It gives a warning of storing the immediate private keys in case of a later verification.

This webpage is one of the confirmation of a successful blockchain transaction which contains block and file information such as hash, sender, receiver, and date. It directs users to provide important data to be checked and a Python script is maintained which facilitates a secure and hash-based file storage and authenticity check.



Receivers can use this interface to authenticate shared files by the sender and by use of the file name and its public key. Once the file received is uploaded, system verifies access status and shows secure message hence assuring trusted sharing and verification of documents.

REFERENCES

[1] Y. Lyu, Z. Li, H. S. Zhou, and X. Deng, "Threshold ECDSA in two rounds," *Cryptology ePrint Archive*, Paper 2025/1696, 2025. [Online]. Available: https://eprint.iacr.org/2025/1696

[2] National Institute of Standards and Technology, "Digital Signature Standard (DSS)," *FIPS PUB 186-5*, Feb. 2023. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf

[3] D. Dinu, "Migration to post-quantum cryptography: From ECDSA to ML-DSA," *IACR Cryptology ePrint Archive*, 2025.

[4] M. A. Al-Khasawneh, M. Faheem, A. A. Alarood, S. Habibullah, and A. Alzahrani, "A secure blockchain framework for healthcare records management systems," *Healthcare Technology Letters*, vol. 11, no. 5, pp. 461–470, Oct. 2024, doi: 10.1049/htl2.12092.

[5] N. U. A. Tahir *et al.*, "Blockchain-based healthcare records management framework: Enhancing security, privacy, and interoperability," *Technologies*, vol. 12, no. 9, p. 168, Sep. 2024, doi: 10.3390/technologies12090168.

[6] K. P. Kalita, J. C. Kharbhih, D. Boro, and D. K. Bhattacharyya, "An enhanced blockchain consensus mechanism using proof-of-work and proof-of-stake," in *Proc. Springer*, vol. 1061, Singapore, Nov. 2024, pp. 559–571.

[7] J. Garay, A. Kiayias, and Y. Shen, "Proof-of-work-based consensus in expected-constant time," in *Proc. EUROCRYPT*, 2024. [Online]. Available: https://eprint.iacr.org/2023/1663

[8] S. Almuhammadi and S. Alghamdi, "A novel transition protocol to post-quantum cryptocurrency blockchains," *Frontiers in Computer Science*, vol. 7, p. 1457000, May 2025, doi: 10.3389/fcomp.2025.1457000.

[9] I. Abdelkrim, E. Ahmed, and O. Fouzia, "Improved blockchain-based ECDSA batch verification scheme," *Frontiers in Blockchain*, vol. 8, p. 1495984, Jan. 2025.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[10] H. B. Mahajan and A. A. Junnarkar, "Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing," *Multimedia Tools and Applications*, vol. 82, no. 28, pp. 44335–44358, Nov. 2023, doi: 10.1007/s11042-023-15204-4.
[11] A. Marcos *et al.*, "Quantum-resistance in blockchain networks," *Scientific Reports*, vol. 13, no. 1, p. 5664, Apr. 2023, doi: 10.1038/s41598-023-32701-6.
[12] P. Zhang, Y. Li, M. Liu, Y. Shang, and Z. Fu, "An ECC-based digital signature scheme for privacy protection in wireless communication networks," *Wireless Communications and Mobile Computing*, vol. 2024, pp. 1–9, 2024, doi: 10.1155/2022/1977798.
[13] S. Wilson *et al.*, "Blockchain-enabled provenance tracking for sustainable material reuse in construction supply chains," *Future Internet*, vol. 16, no. 4, p. 135, Apr. 2024, doi: 10.3390/fi16040135.
[14] K. Suganthi and R. Kumar, "Enhancing blockchain security against quantum threats through integration of post-quantum cryptographic algorithms," *Organic Electronics*, vol. 146, p. 107313, Aug. 2025.
[15] Y. Baseri, S. Hafezi, and S. Ramezani, "SHA-256 hardware proposal for IoT devices in blockchain context," *Sensors*, vol. 24, no. 12, p. 3908, Jun. 2024, doi: 10.3390/s24123908.
[16] S. Chhetri, P. Mallick, and R. Singh, "Quantum secured blockchain framework for enhancing post-quantum data security," *Scientific Reports*, vol. 15, no. 1, p. 16315, Aug. 2025.
[17] S. Bhosale, M. Kumar, and R. Patel, "Quantum-resistant cryptography: A new frontier in fintech security," *World Journal of Advanced Engineering and Technology Sciences*, vol. 12, no. 2, pp. 614–621, Aug. 2024, doi: 10.30574/wjaets.2024.12.2.0333.
[18] M. Dharani, K. Reddy, and P. Sharma, "Hash-based cryptographic schemes for blockchain transactions," *Journal of Information Security*, vol. 14, no. 3, pp. 245–260, 2023.
[19] Y. Singh *et al.*, "Exploring applications of blockchain in healthcare: Roadmap and future directions," *Frontiers in Public Health*, vol. 11, p. 1229386, Oct. 2023, doi: 10.3389/fpubh.2023.1229386.
[20] A. Mashatan and R. Heintzman, "Quantum computing threats to public key cryptography," *IEEE Security & Privacy*, vol. 19, no. 2, pp. 75–78, Mar. 2021, doi: 10.1109/MSEC.2021.3049751.
[21] P. Hegde, S. Nair, and A. Verma, "Lattice-based cryptographic systems for blockchain applications," *International Journal of Network Security*, vol. 25, no. 4, pp. 562–573, Jul. 2023.
[22] K. M. Khan, W. Haider, N. A. Khan, and D. Saleem, "Big data provenance using blockchain for qualitative analytics via machine learning," *Journal of Universal Computer Science*, vol. 29, no. 5, p. 446, May 2023.
[23] J. J. Puthiyidam, J. Shelbi, and B. Bharat, "Enhanced authentication security using blockchain and ECC for IoT applications," *Journal of Cybersecurity Research*, vol. 8, no. 2, pp. 112–128, 2023.
[24] T. Binbin, Y. Chen, H. Cui, and X. Wang, "Fast two-party signature for upgrading ECDSA to two-party scenario," *Theoretical Computer Science*, vol. 986, p. 114325, Jan. 2024, doi: 10.1016/j.tcs.2023.114325.
[25] L. Jones, "Blockchain security features: Strengthening your cybersecurity framework," *Microminder Cybersecurity*, Sep. 2024. [Online]. Available: https://www.microminderc s.com/blog/blockchain-security-features

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com