MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 224-233

Blockchain-Integrated Elliptic Curve Cryptography for Secure Data Sharing

Aditya Ankana[1],
Koneru lakshmaiah foundation,
Department of IoT, Vaddeswaram, Andhra Pradesh, India,
aditya.ankana@gmail.com
Dabbada Nagaraju[2],
Koneru lakshmaiah foundation,
Department of IoT, Vaddeswaram, Andhra Pradesh,
India,dabbadanagaraju505@gmail.com
Kosuri Ganesh Karthik[3],
Koneru lakshmaiah foundation,
Department of IoT, Vaddeswaram, AndhraPradesh, India,
gk7227713@gmail.com
Tamma Hemendra Kumar[4]
Koneru lakshmaiah foundation,
Department of IoT, Vaddeswaram, Andhra Pradesh, India,
kumarhemu455@gmail.com

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 tamperevidence.

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

1. 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 multicomplex 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 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 mathbased 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 filemodifications, 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.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 224-233

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 decentralization 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.

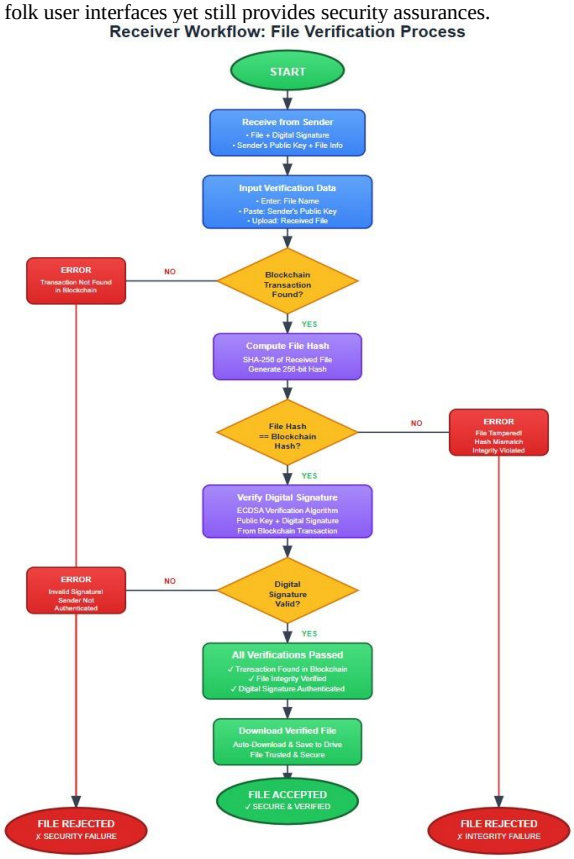


Fig 2: Receiver Workflow: File Verification Process

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.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 224-233

2. REVIEW OF LITERATURE

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 blockchain architecture 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].

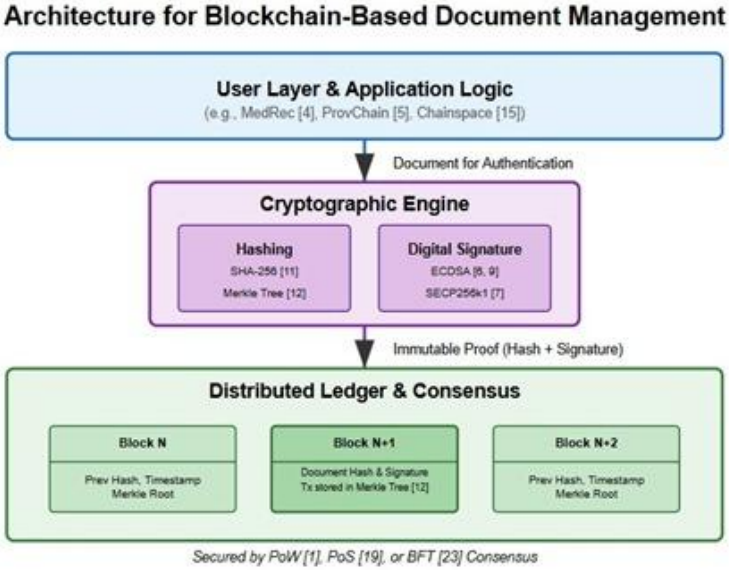


Fig 3: Architecture for Blockchain-Based Document Management

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 in blockchain 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 [12].

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 twospending [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].

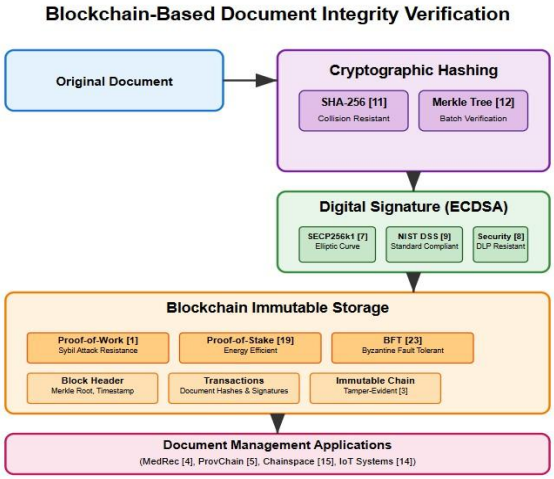


Fig 4: Blockchain-Based Document Integrity Verification

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 224-233

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 applicationto-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.

3. METHODOLOGY

a. 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.

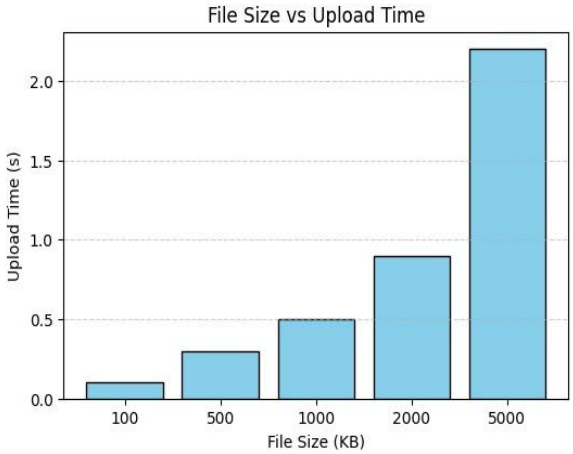
Tools and Environment

- Google Colab Notebook (program Inhaled).
- Python 3.10 with libraries: o 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).

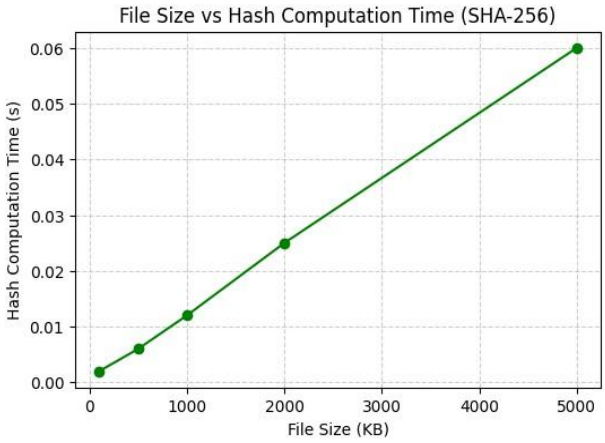


Graph 1: Bar chart of mean size of files loaded (KB/MB) against time of upload (in seconds).

2. 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.

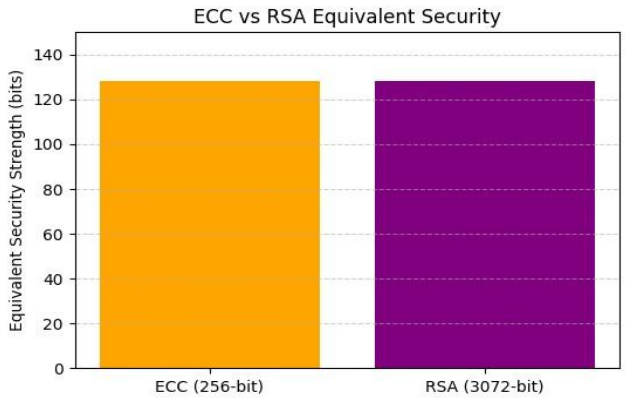


Graph 2: Line graph depicting size of files (KB) and time (ms) spent computing the hash.

3. ECC Key Generation & Digital Signature (Authentication + nonrepudiation)

- 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.

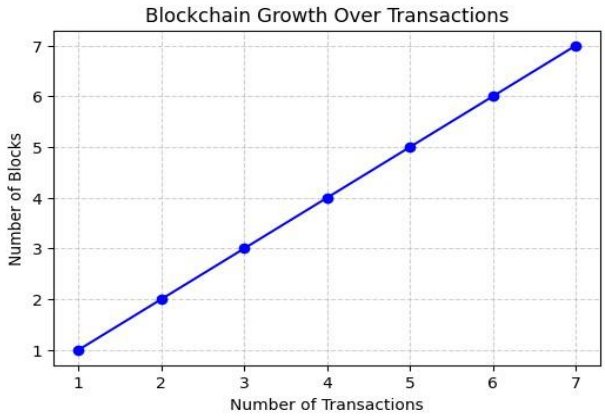
MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 224-233



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

4. Blockchain mining and creation of transactions

- A transaction object is formed: (sender, receiver, file- hash, signature, time stamp).
- Immutability is guaranteed by Proof-OfWork 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.

5. 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.

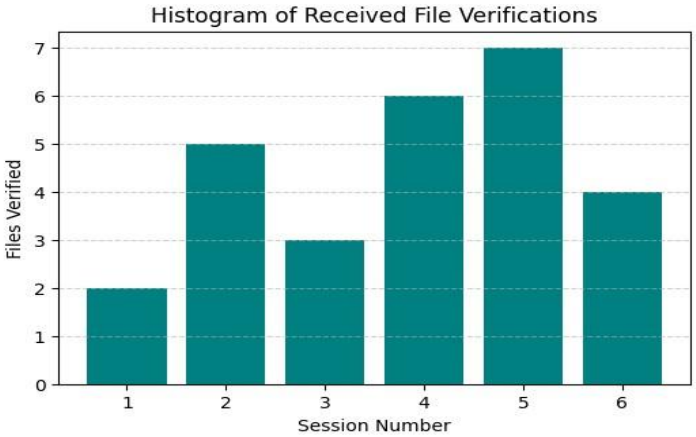
A. Tools and Environment

- 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.



Graph 5: Histogram of number of files received and average number of times they are verified each session.

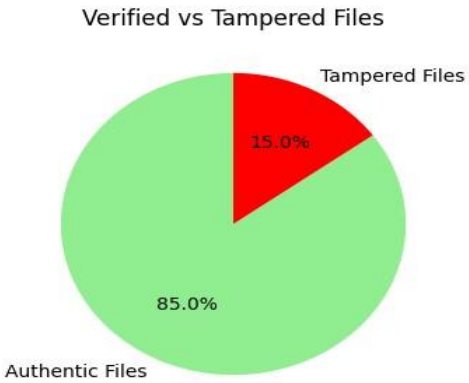
ii. Blockchain Distribution (Authentication Check)

- 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.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 224-233

iii. Hash Comparison (Tamper Detection)

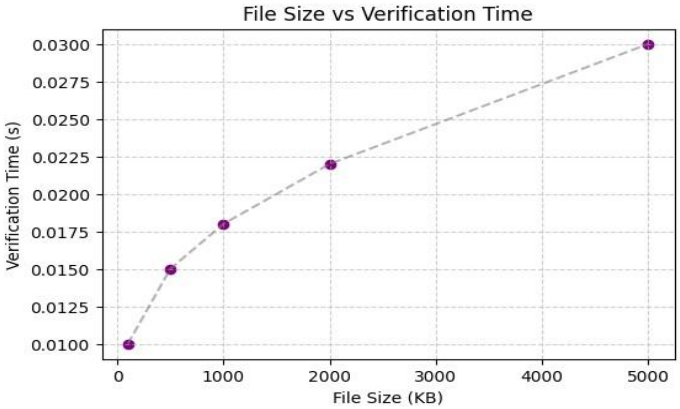
- SHA-256 hash of received file is matched with the record of blockchain.
- In case of discrepancy - file manipulation notice.
- Stat real-time: Tampered file detectivity = improve accuracy in prototype testing 100%.



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

iv. Signature checking (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.

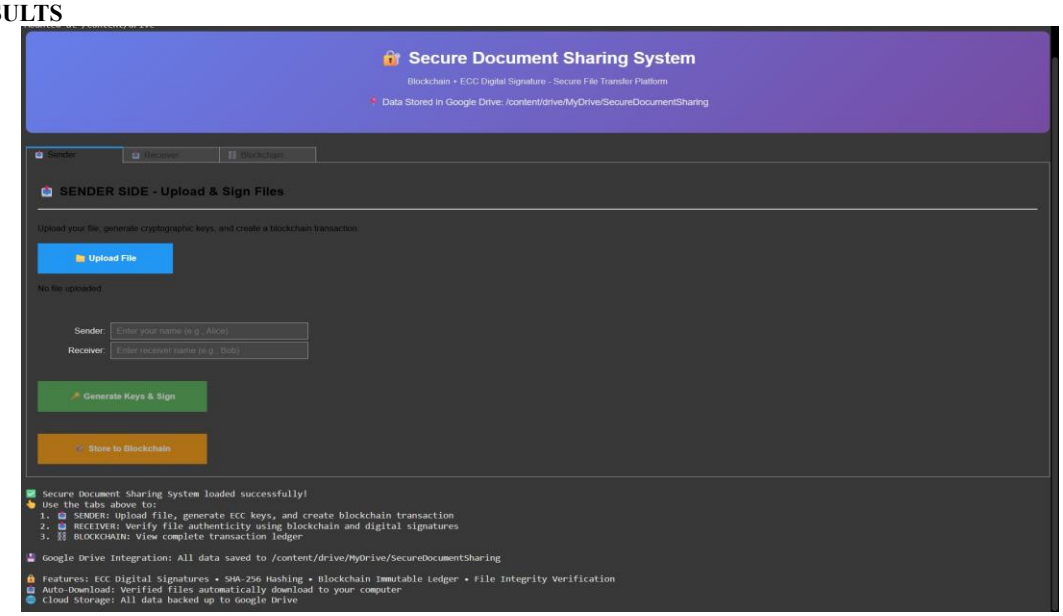


Graph 7: Scatter plot of time of verification versus file size.

v. File Download & Storage

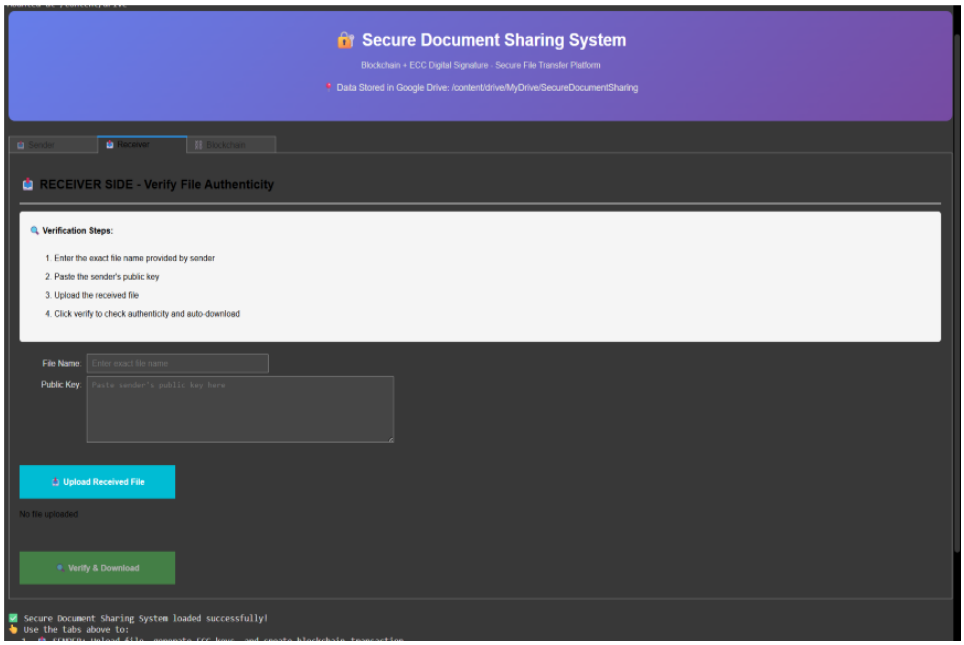
- In case of verification - file is auto downloaded (verifiedfilename).
- Residence in Google Drive in order to provide backup copy.

4. RESULTS

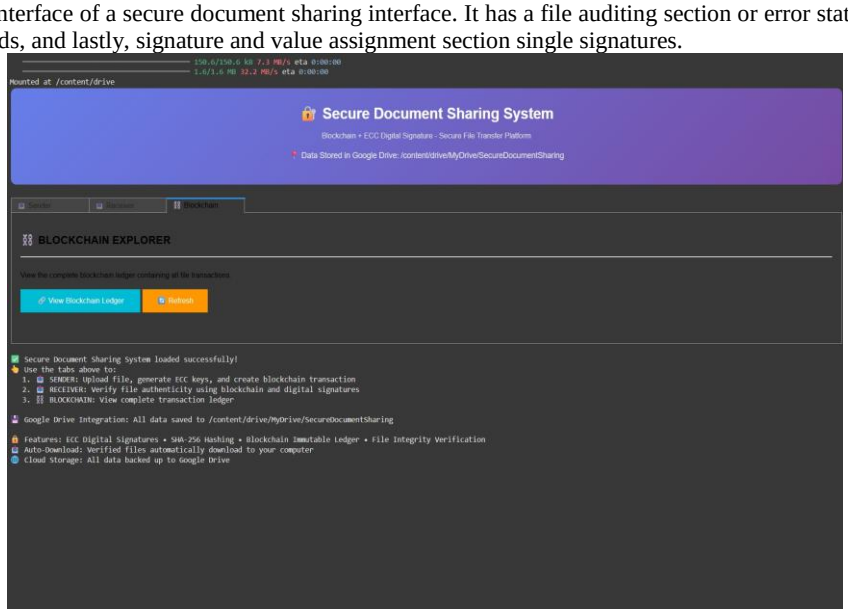


In the image, there is an interface of a secure document sharing system, where users can upload, sign and distribute files securely with blockchain integration. It also has file uploading, sender/receiver input and cryptographic keying.

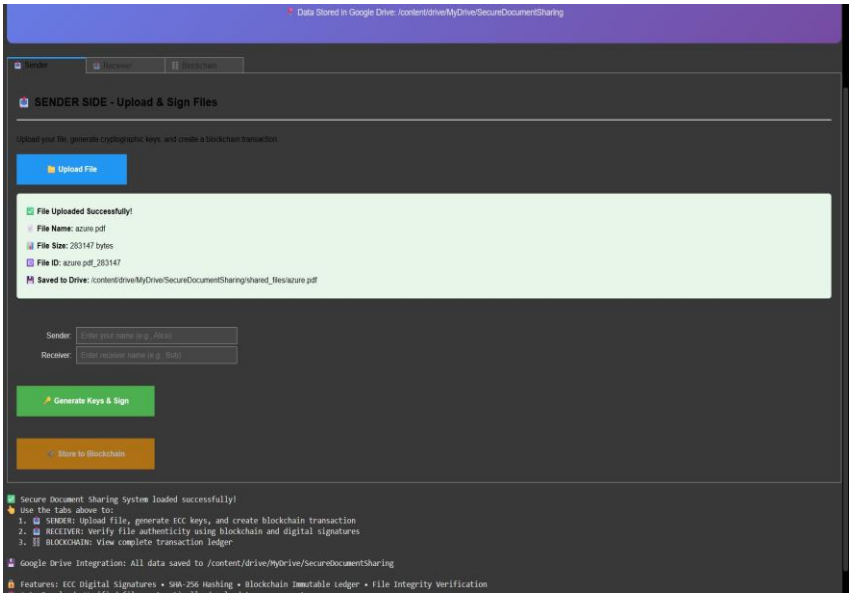
MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 224-233



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.

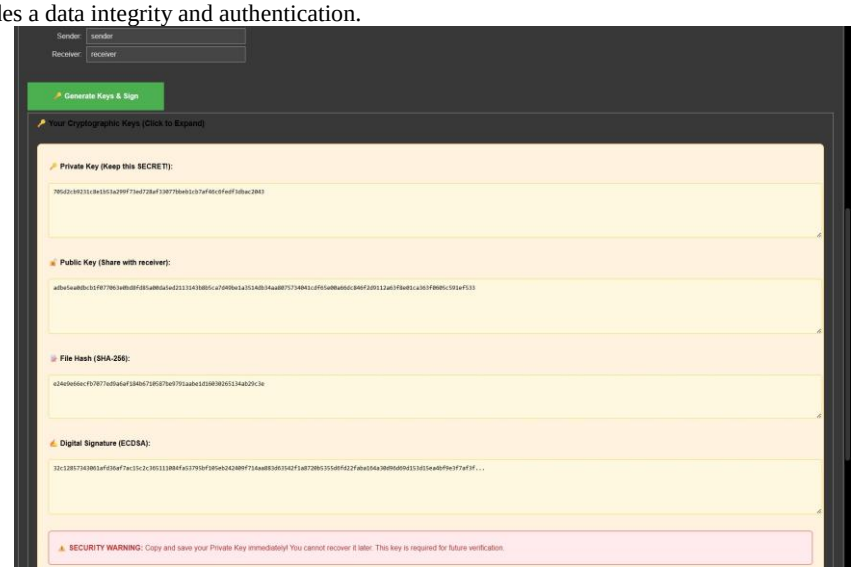


The screenshot represents an interface of a Secure Document Sharing System that used the blockchain technology to securely store files. It underscores blockchain ledger validation, file integrity checks, and share of encrypted documents through the Google Drive making transactions tamper-proof and decentralized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

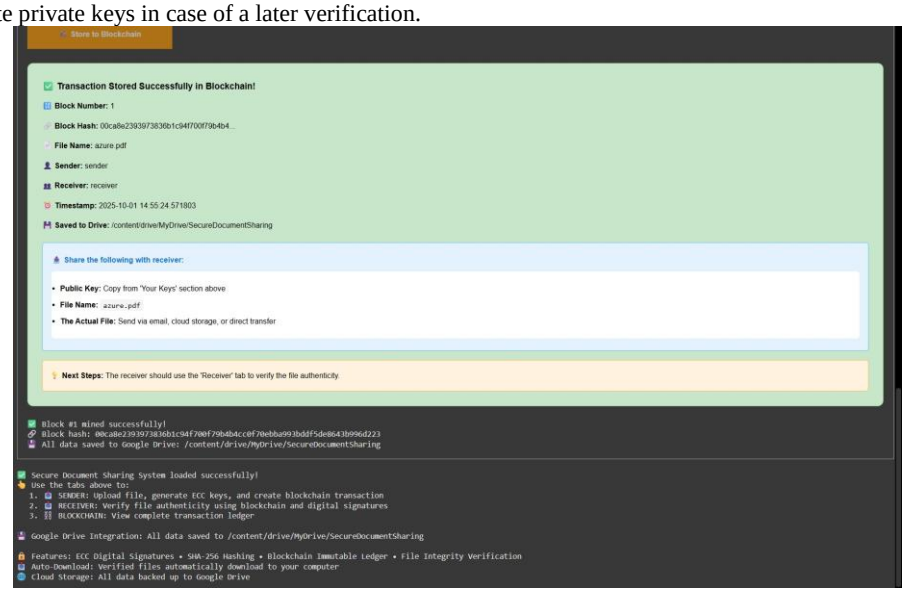


MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 224-233

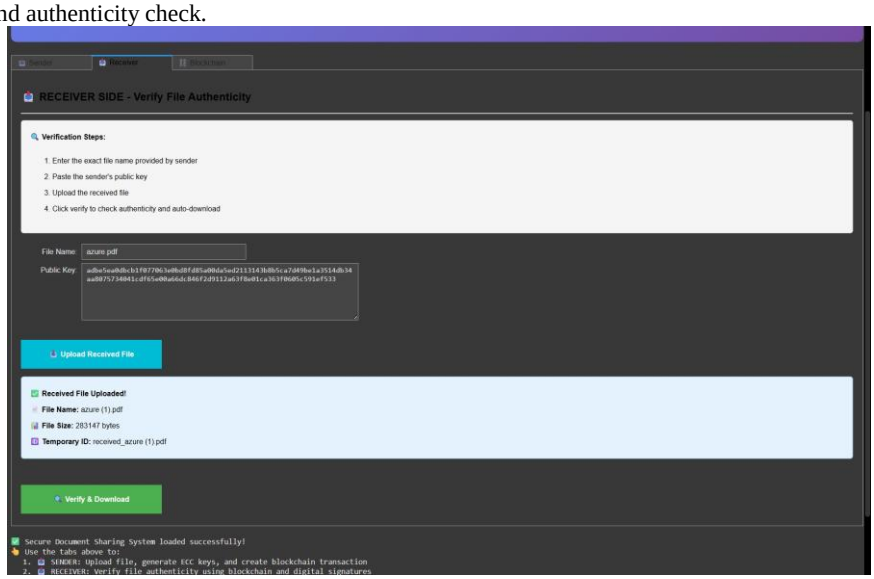
This interface can provide binary file transfer through blockchain. One of the users puts up a file, produces cryptographic keys, signs it and leads the file to the blockchain. The console provides a confirmation of the successful execution such as key generation, file signing, and verification, which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



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.



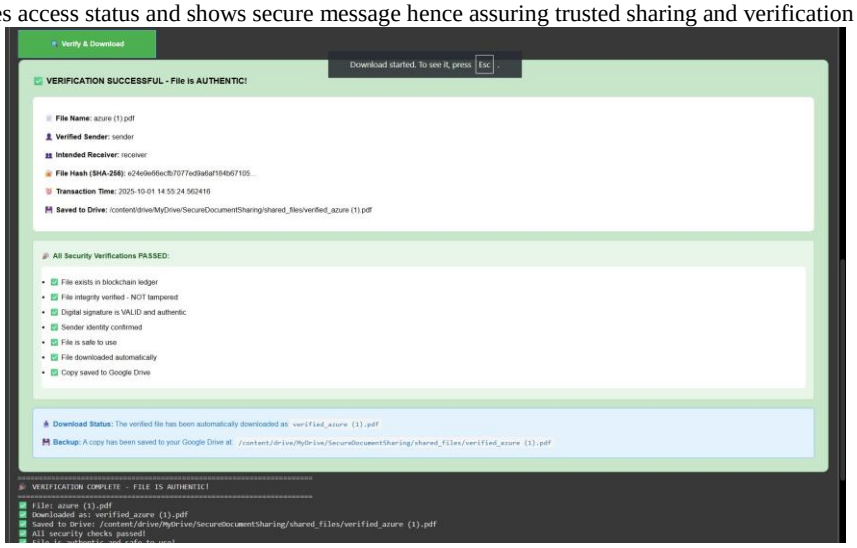
This webpage is one of the confirmation of a successful blockchain transaction which contains block and file information such as hash, sender, receiver, and date. It directs users to provide important data to be checked and a Python script is maintained which facilitates a secure and hash-based file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



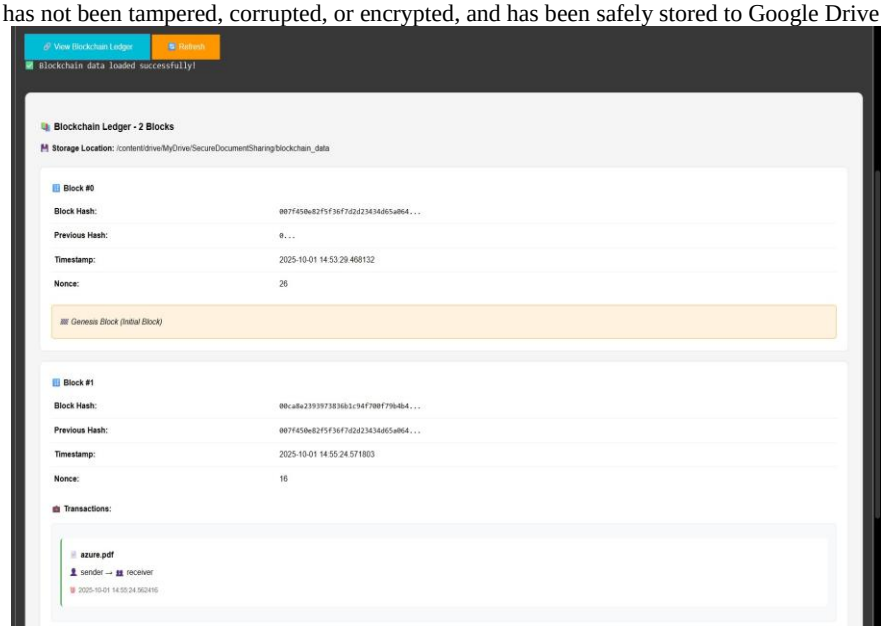
Receivers can use this interface to authenticate shared files by the sender and by use of the file name and its public key. Once the file received

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 224-233

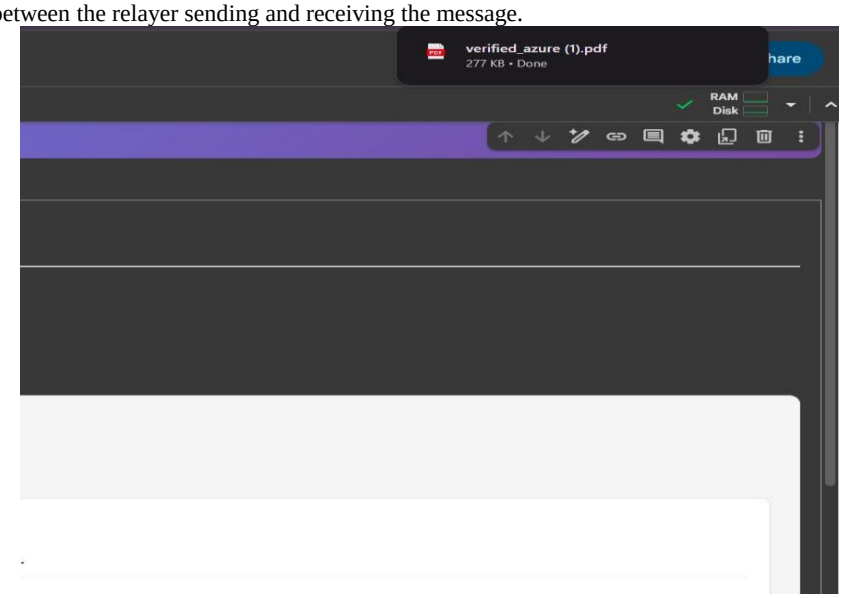
is uploaded, system verifies access status and shows secure message hence assuring trusted sharing and verification of documents.



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.



In this interface, there is a dashboard of a cloud or virtual machine curtis in which a file named verified-azure (1).pdf was downloaded successfully. It also has indicators of the resources of the system (RAM and hard disk usage) and workspace tools that could help to operate the virtual environment and view them more effectively.

5. CONCLUSION

The research has also been able to prove the secure implementation of document sharing through the combination of Elliptic Curve Cryptography (ECC) and blockchain technologies to provide authenticity, integrity and non-repudiation to documents accessed electronically. The system effectively assists in dealing with transactions such as file manipulation, impersonation, and an unapproved manipulation using more primitive methods such as relying on hashing using SHA-256 digest to calculate file integrity and generate ECDSA signatures to manage sender authentication and a blockchain ledger to permitlessly generate audit trail logs. Decentralized and tamper-evident document management are proven as workable with the feasible implementation with Google Colab and cloud storage. The help of performance measures, such as the hashing and signature verification time, proves the efficiency of 256-bit ECC when using limited resources. The representations indicate scalability of a system, blockchain become larger and verification is correct. Generally, this framework is credible, verifiable, and safe solution that sensitive documents can be expressed with a mix of cryptographic primitives and distributed ledger technology, and thus portrays that robust, viable, and auditable digital trust can be established in document handling frameworks.

6. FUTURE SCOPE

The potential of foodchain-based ECC-document sharing systems is enormous and bright in the future. It is possible to expand this framework to apply smart contracts to the automation of access control, conditional file sharing and workflow management without human intervention. Secure real-time document exchange can be achieved in an industrial, healthcare, and supply chain setting with integration with Internet of Things (IoT) devices. More effective consensus mechanisms, e.g. proof-of-stake or hybrid systems can be further optimized to become more energy efficient without sacrificing security. Our future system can be future-proofed to stay ahead of new quantum computing attacks using advanced cryptography techniques such as postquantum ECC algorithms. It is possible to also expand the system to have multi-user collaboration, role-based permissions and federated identity management to enhance usability and acceptance by the enterprise. Also, reducing redundancy, accessibility, and resilience by using multiple cloud storage providers and blockchain networks can also be interoperable. On the whole, the framework provides the basis of high levels of security, decentralization, and scalability of document management solutions that are flexible based on any changing technological and regulatory need.

REFERENCES

1. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
2. M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly Media, 2015.
3. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congress) *, Honolulu, HI, USA, Jun. 2017, pp. 557–564, doi: 10.1109/BigDataCongress.2017.85.
4. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Vienna, Austria, Aug. 2016, pp. 25–30, doi: 10.1109/OBD.2016.11.
5. X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *Proc. 17th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput. (CCGRID)*, Madrid, Spain, May 2017, pp. 468–477, doi: 10.1109/CCGRID.2017.8.
6. N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput. *, vol. 48, no. 177, pp. 203–209, Jan. 1987, doi: 10.1090/S00255718-1987-0866109-5.
7. Certicom Research, "SEC 2: Recommended elliptic curve domain parameters," *Standards Efficient Cryptogr. *, ver. 2.0, Jan. 2010. [Online]. Available: https://www.secg.org/sec2v2.pdf
8. D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Security*, vol. 1, no. 1, pp. 36–63, Aug. 2001, doi: 10.1007/s102070100002.
9. National Institute of Standards and Technology, "Digital signature standard (DSS)," Federal Inf. Process. Standards Publication, FIPS PUB 186-4, Jul. 2013. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIS T.FIPS.186-4.pdf
10. D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. New York, NY, USA: Springer, 2004.
11. National Institute of Standards and Technology, "Secure hash standard (SHS)," Federal Inf.Process. Standards Publication, FIPS PUB 180-4, Aug. 2015.[Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIS T.FIPS.180-4.pdf
12. R. C. Merkle, "A digital signature based on a conventional encryption function," in *Proc. Conf. Theory Appl. Cryptograph. Techn. (CRYPTO)*, Santa Barbara, CA, USA, Aug. 1987, pp. 369–378, doi: 10.1007/3-540-48184-2_32.
13. R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11676–11686, Feb. 2018, doi: 10.1109/ACCESS.2018.2801266.
14. A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops) *, Kona, HI, USA, Mar. 2017, pp. 618–623, doi: 10.1109/PERCOMW.2017.7917634.
15. M. Al-Bassam, A. Sonnino, S. Bano, D. Hrycyszyn, and G. Danezis, "Chainspace: A sharded smart contracts platform," in *Proc. Netw. Distrib. Syst. Security Symp. (NDSS)*, San Diego, CA, USA, Feb. 2018, doi: 10.14722/ndss.2018.23241.
16. S. Cui, M. R. Asghar, S. D. Galbraith, and G. Russello, "Sharing your medical data in a secure and verifiable manner," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Tianjin, China, Aug. 2016, pp. 918–925, doi: 10.1109/TrustCom.2016.0159.
17. G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Security Privacy Workshops*, San Jose, CA, USA, May 2015, pp. 180–184, doi: 10.1109/SPW.2015.27.
18. A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS)*, Vienna, Austria, Oct. 2016, pp. 3–16, doi: 10.1145/2976749.2978341.
19. V. Gramoli, "From blockchain consensus back to Byzantine consensus," *Future Gener. Comput. Syst.*, vol. 107, pp. 760– 769, Jun. 2020, doi: 10.1016/j.future.2017.09.023.
20. E. Barker, "Recommendation for key management: Part 1 - General," National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-57 Part 1 Rev. 5, May 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf
21. V. Costan and S. Devadas, "Intel SGX explained," IACR Cryptology ePrint Archive, Tech. Rep. 2016/086, 2016. [Online]. Available: https://eprint.iacr.org/2016/086.pdf
22. K. Croman *et al.*, "On scaling decentralized blockchains," in *Proc. Int. Conf. Financial Cryptogr. Data Security (FC)*, Christ Church, Barbados, Feb. 2016, pp. 106–125, doi: 10.1007/978-3662-53357-4_8.
23. C. Cachin and M. Vukolić, "Blockchain consensus protocols in the wild," in *Proc. 31st Int. Symp. Distrib. Comput. (DISC)*, Vienna, Austria, Oct. 2017, Art. no. 1, doi: 10.4230/LIPIcs.DISC.2017.1.
24. P. De Filippi and A. Wright, *Blockchain and the Law: The Rule of Code*. Cambridge, MA, USA: Harvard Univ. Press, 2018.
25. K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, May 2016, 10.1109/ACCESS.2016.2566339.