Journal of Applied Engineering and Technological Science
Vol 6(2) 2025: 1215-1236

ADVANCEMENTS IN BLOCKCHAIN CRYPTOGRAPHY: SELF-SIGNED KEY APPLICATIONS FOR DIGITAL RECORD PROTECTION

Pawan Maheshwari[1*], Sunil Gupta[2]
School of Computer & System Sciences Jaipur National University, India[1]
HOD, School of Computer & System Sciences Jaipur National University, India[2]
pawan.sns@gmail.com[1], sunilg95@rediff.com[2]

Received: 18 October 2024, Revised: 01 April 2025, Accepted: 13 April 2025
**Corresponding Author*

ABSTRACT
The significant deployment of Electronic Health Records (EHRs) has introduced serious issues with data security and confidentiality. The proposed study addresses such issues by investigating innovation in blockchain cryptography, with a special focus on the application of self-signed keys for secure digital record management. The research combines the use of Elliptic Curve Cryptography (ECC) with a blockchain framework to suggest a decentralized and efficient solution for the management and authentication of digital records. The experimental evaluation of the proposed solution indicates the efficiency of the system with 1626.03 seconds of execution time, 0.0018 tps of throughput, and 3.1790 seconds of the average latency for 1000 transactions. Furthermore, the proposed solution reduces the encryption time to 3650 ms and the decryption time to 3968 ms as compared to the traditional implementation of the blockchain, with ensured data integrity. The outcome attests to the practicability of the employment of the application of the self-signed keys for the improvement of security, confidentiality, and integrity of data for healthcare systems. Furthermore, the proposed solution strengthens decentralized systems with the introduction of the optimized mechanism of cryptography that maintains efficiency with the guarantee of security, introducing a practical mechanism for the protection of confidential medical data for real-world systems.
Keywords: *Blockchain Technology, ECC, Security, Electronic Health Records (EHRs), Self-Signed Keys, Healthcare Data Protection.*

1. Introduction

Blockchain technology, originally designed for the 2008 distributed digital currency system, has revolutionized the establishment of trust for distributed systems (Sethaput & Innet, 2023). Blockchain, with the application of network-wide authentication and consensus of the participating parties, offers secure transactions among the participating parties with no intermediaries (Mohammed Ali & Mohammed Ali, 2023; Zheng et al., 2020), which is a revolution for the Internet and Internet of Things (IoT) transactions (Liang et al., 2020). Blockchain technology relies on the data structure of a blockchain for data authentication and data storage with the assistance of consensus algorithms for data generation and data update and encryption algorithms for the secure sending and receiving of information (D. Zhang et al., 2022).

With the arrival of Information and Communication Technology (ICT), healthcare organizations changed from paper-based institutions to Electronic Health Records (EHRs), which contain varied medical information, including personal and confidential nature (Rikiti et al., 2022), This accelerated the application of cloud networks for storing and making information available (Singh et al., 2022). However, traditional implementations of EHRs pose serious issues. These systems include centralized environments, point-to-point hospital communications, and single-point failure (Lucking et al., 2020). Furthermore, storing sensitive medical data within IoT-based health environments exposes the systems to greater attack surfaces for the purposes of security and makes them susceptible to tantamount attacks like Distributed Denial of Service (DDoS) and ransomware (Saleem & Abdulrahman, 2024; Lakhan et al., 2023). Therefore, cryptographic processes have been designed to prevent advanced security attacks (Muttaqin & Rahmadoni, 2020; Abead & Ali, 2024).

As a consequence of the transition from the traditional, paper-based method to the management of EHR, which enables patient information storage, access, and verification only

by accredited healthcare centers (Keshta & Odeh, 2021). The end of storage and inconsistencies would be through the implementation of an EHR management system, making the medical data more accessible and accurate. In recent years, research on the application of blockchain-based EHR systems for mitigating the disadvantages of traditional EHR systems and improving their performance has become prominent. Blockchain technology possesses attributes such as data confidentiality, distribution, and other aspects (Aoun et al., 2021). Specifically, some blockchains have introduced diversified frameworks such as Hyperledger and Ethereum (Ucbas et al., 2023). Both methods are similarly structured, with Hyperledger being the more power-saving and socially dependable option compared to other frameworks (Chukwu & Garg, 2020).

Traditional EHR systems are vulnerable, with health-related medical information being saved on individual medical servers, and the patient's information is not easily exchanged (Shah & Khan, 2020). When patients are transferred from one hospital to another, the hospitals have to carry out a smooth and direct data-sharing process, which is not straightforward and effective (Mensah, 2021). The systems are also centralized, creating single points of failure that affect the entire network (Pillai et al., 2022; Peng et al., 2021). Centralization of sensitive medical information also leads to security issues, making it susceptible to DDoS attacks and ransomware attacks (Yaacoub et al., 2020). Blockchain solves these issues by providing decentralization and information integrity by sharing records between distributed nodes and by creating a decentralized, public, append-only, immutable digital record secured through Public Key Encryption (Khan et al., 2024). It uses cryptographic hash functions like SHA-256 to offer data immutability and anonymity, (Naveen N & Thippeswamy, 2021) and consensus protocols and smart contracts for enhanced security and functionality (E. Zhang et al., 2021).

Blockchain technology in the healthcare industry enables the implementation of patient-controlled EHRs, which make individuals fully in charge of available information. This change diverts the prevailing practice from institution-focused to patient-need and patient preference based on the interoperability factor. Full EHR data storage on blockchain is not possible due to size and cost (Wenhua et al., 2023). Various blockchain models exist, and Hyperledger fabric is outstanding in performance, energy efficiency, and addressing bottleneck issues (Wang et al., 2020).

The integrity of digital records, particularly in the medical sector, is compromised by the implementation of centralized certificate authorities. Such traditional systems bring with them a sole point of failure, which maximizes data breaches and unauthorized access, posing risks to sensitive data. Ensuring the integrity and authenticity of digital documents without breaking patient confidentiality is critical because any loss would be of immense significance. In order to avert such risks, the demand for strong, decentralized cryptographic processes that provide security and facilitate the signing and authentication of transactions is growing increasingly.

Different studies have proposed blockchain-based frameworks for solving the assigned issues (Ajakwe et al., 2024). For example, the authors claim that the private blockchain approaches discussed by (Usman & Qamar, 2020) and (Ghazal et al., 2022) have been studied for better management of medical data. Other suggested solutions include the re-encryption oracles and Interplanetary File System (IPFS)-based Ethereum deployments for secure data exchange and storage proposed by (Madine et al., 2020). Nevertheless, computational efficiency, real-time data retrieval, and encryption overhead issues seem to interfere with these solutions, as argued by (Azbeg et al., 2022). Furthermore, centralized hospital store models such as those suggested by (Du et al., 2021; Khatoon, 2020) have numerous patient autonomy and security vulnerability issues. In addition, perspectives listed by (Na & Park, 2021; Tuan-Vinh Le & Tuan-Vinh Le, 2021; Zamani et al., 2020; Zhou et al., 2021) underline serious limitations for blockchain-based healthcare solutions that include high power needs for processing, more threats to interference by malicious attacks, and risk of privacy. The studies highlight that the architecture of blockchain itself, perhaps, can expose recent blocks to security threats and inefficiency in decentralized record management.

Based on these advancements, the present work adopts a new approach with the introduction of a self-signed key application (Chu et al., 2020). From the viewpoint of elliptic curve cryptography (ECC), the proposed approach increases both security and confidentiality while enhancing encryption and decryption speed. Alongside the enhancement to key access

control, computational efficiency, and decentralized record maintenance, the cryptographic approach proposed is scalable and efficient while improving the security and reliability of medical data storage in the decentralized framework.

Since the current blockchain-based healthcare systems suffer from various limitations. Centralized certificate authorities employed here have security risks, and there is a higher chance of unauthorized access and data tampering. Moreover, standard blockchain implementations are plagued with high computational overhead, poor access control, and privacy issues caused by poor encryption methods. These restrictions inhibit the use of blockchain technology in secure and scalable healthcare data management. Therefore, this work tries to solve these issues by introducing the following major contributions:

- Prevents the reliance on a central certificate authority using self-signed keys, offering better security and less dependency on other entities.
- Integrates self-signed keys within a blockchain framework, ensuring tamper-resistant digital records with improved verification mechanisms.
- Utilizes elliptic curve cryptography (ECC) with the secp256k1 curve, improving efficiency in securing and verifying digital records on the blockchain.
- Ensures confidentiality and integrity of patient data through robust cryptographic mechanisms, mitigating risks associated with unauthorized access.
- Provides an expandable, decentralized system for processing health records, giving safe, real-time access to data.

The subsequent sections are structured as follows: Section 2 presents a comprehensive literature review followed by the research objectives and dataset description in sections 3 and 4. The methodology is presented in section 5 which provides a comprehensive description of the step-by-step procedure of the proposed technique. Results and analysis of the performance of the proposed system are presented in section 6 followed by the discussion in section 7. Finally, the conclusion presents the findings and discusses future research avenues.

2. Literature Review

Blockchain technology for EHRs has come a long way in the past few years, to address primary issues of data security, integrity, and interoperability. In a study Usman & Qamar, (2020), introduced a Hyperledger-based EMRS framework for the improvement of data security, privacy, and accessibility. Though the research proved the feasibility of decentralized healthcare systems, it did not make use of advanced cryptographic techniques and high-performance real-time processing of transactions. Subsequently, Tith et al., (2020) proposed a blockchain consortium model for facilitating the access of EHR among institutions. This model allowed the healthcare provider to access and authenticate the record from anywhere within EHR systems irrespective of centralized administration, preventing the risk of single-point failures. Nevertheless, low scalability and greater latency with the model limited its use over vast healthcare networks, thereby necessitating the optimization of cryptographic processes.

To ensure even more security and confidentiality, the researchers utilized strong cryptographic algorithms and their corresponding blockchain platforms. To that effect, Chenthara et al., (2020) suggested using Hyperledger Fabric and the InterPlanetary File System (IPFS) to store EHRs securely. The framework enhanced data integrity, data confidentiality, and system scalability and therefore outperformed distributed healthcare systems. However, the system was constrained owing to the inefficiency of the encryption algorithm and hence prone to more execution time, resulting in low throughput. Similarly, B. Liu et al., (2020) introduced a control mechanism for digital certificates for the access management of the blockchain for the security of the data and improved communication. This framework is quite powerful but lacks large-scale application in real-life healthcare environments.

Later, G. Liu et al., (2024) introduced a low-computation and communication overhead consortium blockchain-based EHR-sharing system. The system augmented data confidentiality and security by restricting the intrusion of third parties and thereby reducing computational complexity. The system did not focus on low-latency processing and was therefore less suitable for applications requiring real-time responses in healthcare. Also, Kumari et al., (2023) presented a decentralized multi-authority PKI model to share EHRs efficiently. The model used

the binary tree structure and IPFS to ensure data integrity and fault tolerance. While their system improved security, in practice, it wasn't deployed within high-traffic healthcare networks, thereby hindering scalability.

Recently, research concentrated on incorporating Self-Sovereign Identity (SSI) and Verifiable Credentials (VCs) in the interest of better, patient-centric data privacy. Martínez et al., (2025) proposed an open-source management system for health data using SSI, Decentralized Identifiers (DIDs), and VCs. The essence of the system was that patients would have full control of their health data, with some arrangements for emergency access. On the downside, the proposed system needs rigorous testing to ascertain its applicability to large-scale healthcare settings: In throughput and latency performance, the system was not very competitive. Similarly, Shi et al., (2022) offered a blockchain-based authentication scheme for smart contracts and zero-knowledge proof (ZKP). Although their scheme, by enhancing security, has reduced registration time by up to 20% in other respects, it was not performant enough for high-computation settings and hence less practicable for complex healthcare workflows.

To address the cross-chain interoperability challenge, Ramesh et al., (2025) developed Polkadot-based Cross-chain for EHR-preserving Blockchain (PCEB) and Relay-as-a-Service-based Cross-chain (RaSCEB). The systems allow for seamless EHR exchange throughout healthcare networks, with no loss of data sovereignty. Transaction latency and throughput, however, were not explored well, and optimization for performance was proposed. Likewise, (Zou & Zeng, (2023) proposed expander signatures for effective generation and verification of signatures on low-resources devices for IoT healthcare systems. Despite being efficient, the work did not involve large-scale testing on busy blockchain networks, thus its real-world applicability was limited.

A notable development in cross-institutional EHR management was presented by (Ma et al., 2022), who designed a federated personal health data management framework (PHDMF) using blockchain and distributed ledger technology (DLT). Their model eliminated third-party endorsement, allowing secure cross-institutional data sharing. However, the low transaction throughput presented a scalability challenge, necessitating algorithmic enhancements for future data expansion. From a cryptographic perspective, Turan et al., (2024)introduced SemiDec-PKI, a blockchain-based public key infrastructure (PKI) architecture. Their model reduced reliance on central authorities, improving fault tolerance. Nevertheless, the framework required enhanced cryptographic optimization for higher efficiency. Similarly, Garba et al., (2023)proposed LightCert4IoTs, a lightweight certificate system for IoT devices. Although the framework minimized CPU and memory usage, it lacked large-scale testing in multi-IoT environments, limiting its real-world feasibility.

These studies reveal several persistent research gaps in current blockchain-based EHR systems, highlighting the need for optimized cryptographic mechanisms and more decentralized verification models, making blockchain solutions more efficient and practical for large-scale healthcare environments.

Table 1 - Summarized literature review

Author(s)	Objective of Study	Proposed Approach	Outcome	Research Gap
Usman & Qamar, (2020)	To enhance **privacy, security, and accessibility** of EMRS.	Blockchain-based **EMRS using Hyperledger**.	Improved **data privacy and accessibility** but lacked **real-time processing** efficiency.	Lacks **advanced cryptographic algorithms** and **scalability** in large healthcare networks.
Tith et al., (2020)	To enable **cross-institutional EHR access** without central authority.	**Consortium blockchain** model using Hyperledger Fabric.	Improved **cross-institutional record verification** but suffered from **higher latency**.	**Limited scalability** and no support for **real-time, large-scale operations**.
Chenthara et al., (2020)	To improve **data security, integrity, and privacy** in healthcare.	**Hyperledger Fabric + IPFS** for distributed EHR storage.	Improved **scalability, privacy, and integrity**.	Lacks **efficient encryption algorithms**, leading to **higher execution time** and reduced throughput.

B. Liu et al., (2020)	To enhance **blockchain data access control** and security.	**Digital certificate-based access mechanism**.	Improved **communication efficiency** and **data protection**.	Lacks **practical implementation** in large-scale healthcare networks.
Shi et al., (2022)	To develop a **decentralized authentication model**.	**Smart contracts + ZKP-based authentication**.	Improved **registration speed by 20%** and enhanced security.	**Poor performance in high-computation environments**, limiting its scalability.
Zou & Zeng, (2023)	To introduce **expander signatures** for efficient authentication.	**Expander signature scheme** for signature verification.	Faster **signature verification** on low-resource devices.	Lacks **large-scale testing** in high-traffic networks.
Martínez et al., (2025)	To develop a **patient-centric health data management framework**.	**SSI, DIDs, and VCs** for decentralized patient data management.	Improved **data sovereignty** and emergency access protocols.	Lacks **large-scale testing** and optimization for **throughput and latency**.
Ma et al., (2022)	To create a **federated PHD framework** for cross-institutional data sharing.	**Blockchain + Distributed Ledger Technology (DLT)**.	Enabled **cross-institutional data sharing** without third-party endorsement.	**Low transaction throughput**, limiting its scalability for real-time healthcare applications.
G. Liu et al., (2024)	To develop a **secure EHR sharing scheme**.	**Consortium blockchain** for privacy-focused EHR sharing.	Reduced **communication overhead** and improved data security.	Lacks **low-latency processing**, making it less practical for real-time applications.
Kumari et al., (2023)	To develop a **multi-authority-driven PKI** for EHR sharing.	**Binary tree structure + IPFS** for decentralized EHR management.	Enhanced **data integrity** and reduced **single-point failure** risks.	Lacks **validation in high-volume healthcare networks**, limiting its real-world scalability.
Ramesh et al., (2025)	To develop **cross-chain EHR-sharing frameworks**.	**Polkadot-based PCEB + RaSCEB** with relay-as-a-service.	Enabled **seamless EHR sharing** across multiple blockchains.	**Latency and throughput** optimization are not fully analyzed.
Turan et al., (2024)	To enhance **public key infrastructure (PKI)** with blockchain.	**SemiDec-PKI** framework.	Improved **fault tolerance** and reduced reliance on central authorities.	Lacks **cryptographic optimization** for better efficiency.
Garba et al., (2023)	To improve **IoT security with lightweight certificates**.	**LightCert4IoTs** for IoT devices.	Reduced **CPU and memory usage** in IoT environments.	Lacks **large-scale validation** in complex multi-IoT environments.

The existing literature highlights several gaps in blockchain-based EHR frameworks that hinder their large-scale applicability. Latency and throughput limitations remain a significant challenge, preventing real-time transaction processing and reducing system efficiency. Current frameworks often face performance bottlenecks due to slow encryption and verification mechanisms. Also, cross-chain interoperability is largely absent in existing models, restricting seamless data exchange between healthcare institutions. Moreover, the majority of systems are third-party certificate authority-based, which provides centralized points of failure and potential security threats. The absence of decentralized authentication mechanisms also restricts the trust and reliability of the systems.

3. Research objectives

- To create a framework for secure, decentralized EHR management based on the usage of self-signed keys.
- To make the encryption and decryption processes more efficient by adding ECC, reducing the execution time, and enhancing throughput.

- To improve data integrity and confidentiality by ending the reliance on centralized certificate authorities and making digital documents tamper-resistant and verifiable.
- To evaluate the performance and security of the proposed framework by measuring latency, throughput, and cryptographic efficiency under real-world healthcare environments.

4. Dataset description

One of the primary challenges for researchers in the healthcare sector is the scarcity of available public datasets. Because healthcare data is usually sensitive, it is not widely available to the public. However, there is a finite quantity of anonymized datasets that may be accessed on the internet. The proposed research requires data records including patient identifiers, such as name, birth date, and other contact data. This makes anonymized datasets inappropriate for the requirements.

To address the above problems, the proposed study utilized the MIMIC-III dataset (https://www.kaggle.com/datasets/asjad99/mimiciii). The dataset is publicly available and includes medical information from more than 40,000 individuals who were hospitalized in critical care units at Beth Israel Deaconess Medical Center between 2001 and 2012. The data has been anonymized to protect patient privacy. However, for the present experiment, this study employed just 1,000 records because of limitations in scalability and data management. This data collection approach supports the integration of blockchain cryptography, particularly self-signed keys making this an essential aspect of current research.

5. Methodology

This section presents the methodology for self-signed key applications for digital record protection using blockchain technology. The process begins with the initialization of the blockchain network, involving the setup of five nodes and the definition of the consensus mechanism (Proof of Work) to ensure reliable data validation. As illustrated in Figure 1, the proposed framework specifies the digital record format, for example, fields timestamp, data, and signature. The cryptography module creates a self-signed key pair with ECC and the secp256k1 curve, which provides stronger security with smaller key sizes, enabling faster encryption and decryption.

For verification, the system employs a test healthcare dataset of 1000 digital records with attributes like patient IDs, timestamps, medical history, and access logs, simulating actual healthcare interactions. The user authenticates a digital record, which is signed with the private key. The signed record is then hashed and posted to the blockchain network for verification. Once verified successfully, the record is stored in the immutable ledger forever, providing data integrity and traceability. Lastly, the system provides real-time access to records and verification by authorized users.

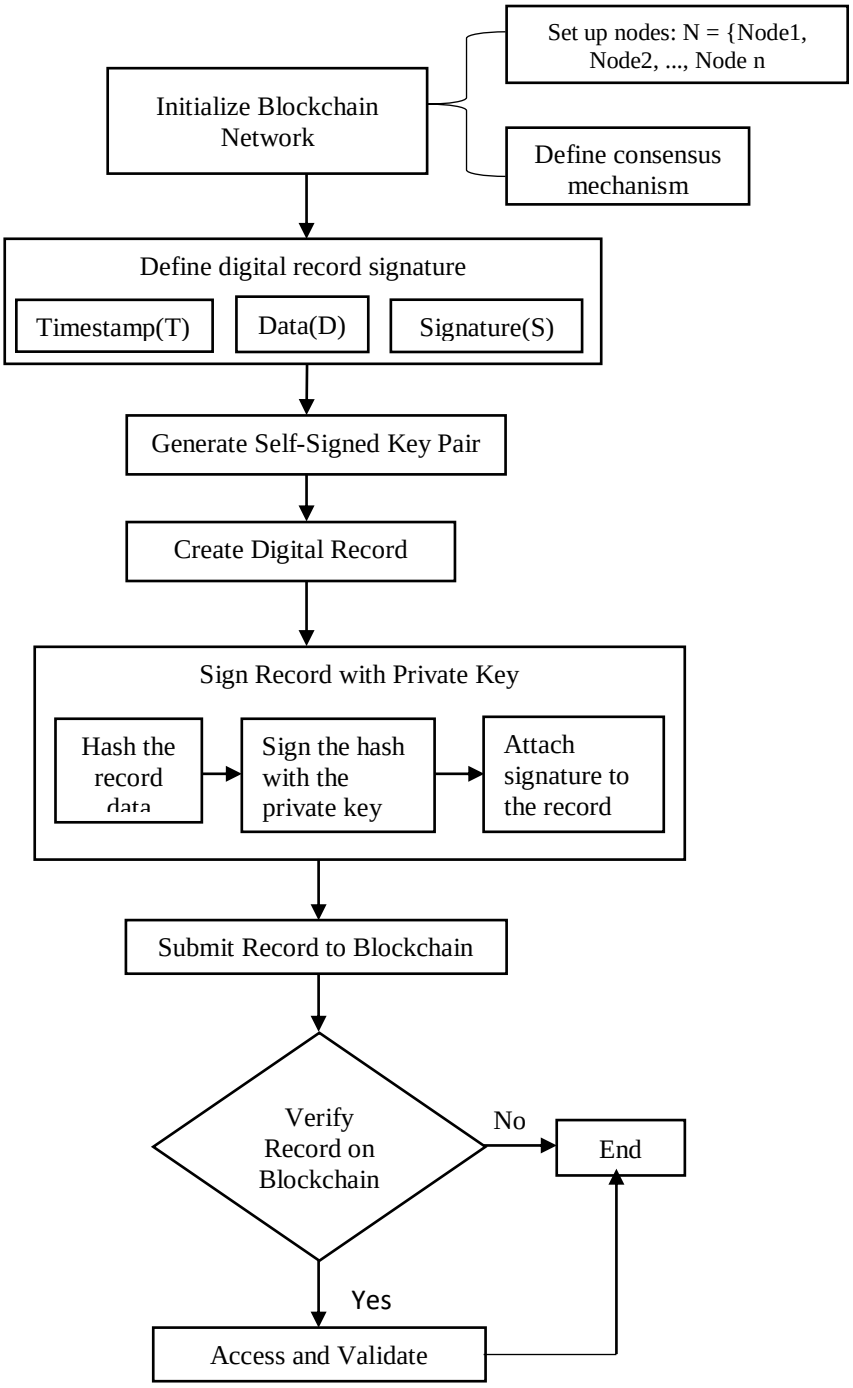

Fig. 1. Proposed framework.

The sequence diagram given in Figure 2 shows the interaction among the User, Blockchain Network, Digital Record, and Cryptography Module. The full workflow, from initializing the blockchain to the creation of self-signed key pairs, record generation, signing, and verification is depicted. The diagram also indicates the return of verified records, facilitating smooth and tamper-proof data handling. Moreover, the image perfectly depicts the sequential communication process between the modules concerning how the cryptography module produces and returns the signed record. It also illustrates the verification procedure carried out by the blockchain network before providing access to validated records. Such a comprehensive flow indicates the efficiency and security of the self-signed key mechanism in providing secure and tamper-proof digital record protection.

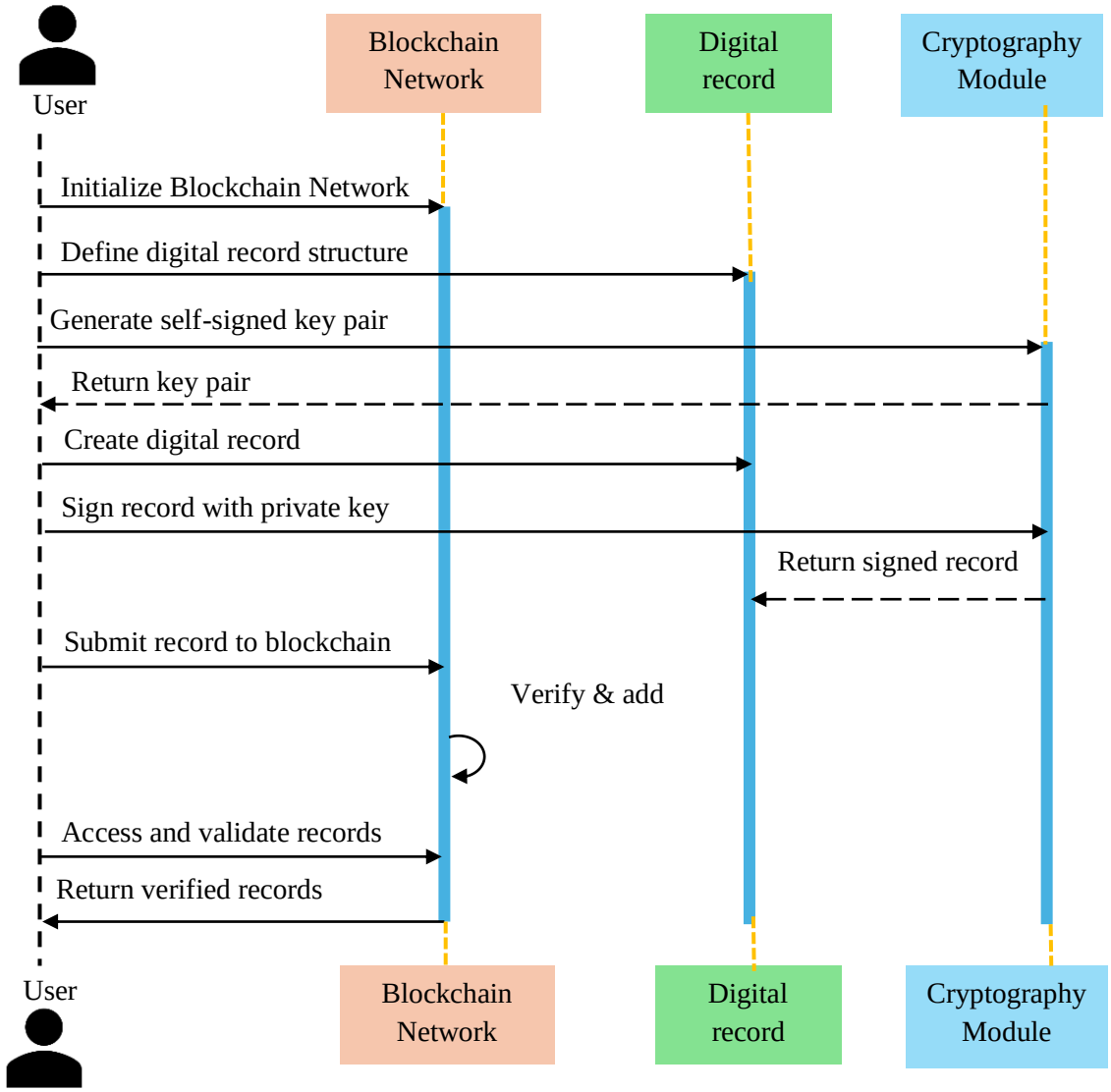

Fig. 2. Proposed Sequence Diagram.

This method is employed for its scalability, security, and efficiency. ECC was particularly chosen for its high-speed processing and lower key size over RSA, as it is most suitable for real-time blockchain applications. The use of self-signed keys eliminates the requirement for third-party certificate authorities, minimizing external dependencies while providing increased privacy. The framework is benchmarked with emulated blockchain interactions, and 1000 transactions are processed to measure throughput, encryption/decryption time, and latency. Performance metrics like execution time and transaction validation rate are measured to determine the efficiency of the system. The implementation is done by utilizing Python for cryptography and Hyperledger Fabric for blockchain networking.

5.1. Initializing Blockchain Network

Installation of the nodes, which are the foundation of a blockchain, is the initial process of creating a blockchain network. Every node must be set to make it able to connect to the network through the distribution of distinct codes and defining the mode of communication to enable nodes to communicate with each other. Afterward, there must be some mechanism of consensus to provide stability and uniformity to the blockchain. Principal mechanisms are Proof of Work (PoW) and Proof of Stake (PoS). In PoW, the nodes compute a difficult mathematical problem to verify the transactions and construct new blocks, which is expressed as $H(M) \leq T$ where H represents the hash function, M is the data for the block, and T represents the target difficulty. Validators are allocated in the PoS system to build additional blocks based on the number of

coins they have and are prepared to "stake" as collateral. This process reduces the amount of work required.

The fundamental blockchain architecture is then established by beginning with the development of the blockchain ledger. The ledger is a decentralized database that holds all transactions in linked blocks that create a chain. Each block has a header and a body. The header holds the metadata for the block, the hash of the previous block Hprev, a timestamp T, and a nonce N. The body holds the actual transactions. The hash of every block Hblock = H(Hprev||T||N||data) secures the blockchain by preventing any modification since modifying any of the block's sections would result in a different hash, and it would destroy the chain. Nodes create network protocols to manage communication, distribute transactions, and come to an agreement and ensure a secure and stable blockchain network.

5.2. Define Digital Record Structure

A few important steps are followed to specify the digital record format of a blockchain-based digital record safeguard system with self-signed keys. The digital record should contain important fields like a timestamp, data, and a signature.

- **Determine Fields for Digital Record:** The digital record structure must be meticulously designed to include essential fields that capture all necessary information for validation and verification processes. Key fields include:

Timestamp (T): This specifies the real-time at which the electronic record is created or modified. It is necessary to ensure the chronological order and the temporal consistency of the record.

Data (D): It includes actual data or payload that is supposed to be stored and protected. Data can simply mean anything that can be used as a digital resource, for example, text, images, or binary files.

Signature (S): It contains the digital signature that is made by the private key of the data owner. This signature assures the non-reprehensibility and authenticity of the data.

- **Include Timestamp, Data, and Signature Fields:** The structure of a digital record is defined so that the necessary fields for validation can be properly added. The structure can be represented in either a tuple or a data object containing the fields stated above.

$$R=\{T, D, S\} \quad (1)$$

Here, T represents the field for timestamping, in normal time format; D represents the data field, which holds the actual message to be signed; and S is the signature field, which holds the cryptographic signature over the data.

To further secure and ensure integrity within the digital record, each field is separately encoded and formatted. The timestamp (T) can be derived using standard libraries with accurate and self-consistent time records. The data (D) are usually encoded correctly. The signature (S) is produced by hashing T and D merged and encrypting that hash with the private key (kpriv) of the record's originator as follows:

$$H = \text{Hash}(T \| D) \quad (2)$$

$$S = Sign_{k_{priv}}(H) \quad (3)$$

Here H denotes the cryptographic hash of the timestamp concatenated with the data, and $Sign_{k_{priv}}$ is the signing operation with the owner's private key. Any changes in T or D would result in a different hash value, rendering the signature invalid; thus, this cryptographic mechanism serves as a strong verifier of its integrity and authenticity.

5.3. Generating Self-Signed Key Pair

Generating a self-signed key pair using ECC is a very important step as it enables secure digital signing of records in a blockchain system. ECC was chosen for its extreme security level and very small key sizes which is what makes it feasible for blockchain applications.

- **Use Elliptic Curve Cryptography:** Employ the ECC curve, which is widely used in blockchain systems like Bitcoin. The equation defines this elliptic curve:

$$y^2=x^3+ax+b \quad (4)$$

The parameters are a=0 and b=7, simplifying the equation to:

$$y^2=x^3+7 \quad (5)$$

The field Fp is a prime field where $p = 2^{256} - 2^{32} - 977$.

- **Generate Private Key:** The private key kpriv is a randomly generated integer in the range [1,n−1], where n is the order of the base point G on the elliptic curve. This base point G is a predefined point on the curve that all calculations are based on. The order n is a large prime number defining the number of points on the curve.

$$Kpriv \in [1, n-1] \quad (6)$$

- **Derive Public Key from Private Key:** The public key Kpub is derived by performing scalar multiplication of the private key Kpriv with the base point G:

$$K_{pub} = K_{priv} \cdot G \quad (7)$$

This operation involves adding point G to itself K_{priv} times on the elliptic curve. Scalar multiplication on an elliptic curve is computationally efficient but ensures that deriving $K_{priv}$from $K_{pub}$is infeasible due to the Elliptic Curve Discrete Logarithm Problem (ECDLP).

5.4. Create Digital Record

Populate the necessary fields with relevant data and include a timestamp to create a digital record.

- **Populate Record Fields with Relevant Data:** Define the record R with the required fields: timestamp (T), data (D), and signature (S). The data field D contains the actual information, while the signature S could be added later.
- **Add Timestamp:** Include the current timestamp in the record to ensure temporal integrity:

$$R = \{T, D, S\} \quad (1)$$

By following these steps, each digital record is uniquely identifiable, tamper-proof, and verifiable within the blockchain network.

5.5. Sign Record with Private Key

In order to confirm the integrity and authenticity of a digital record, it is signed with the private key. This involves several cryptographic steps:

- **Hash the Record Data:** Compute the cryptographic hash of the record data (D) and the timestamp (T). The hash function H ensures a fixed-size output that uniquely represents the input data.

$$H = Hash(T \parallel D) \quad (2)$$

Here, T‖D denotes the concatenation of the timestamp and the data.

- **Sign the Hash with the Private Key:** Use the private key (K_{priv}) to sign the computed hash. This signature operation generates a unique signature (S) using the elliptic curve digital signature algorithm (ECDSA):

$$S = Sign_{k_{priv}}(H) \quad (3)$$

This ensures that the signature can only be verified with the corresponding public key.

- **Attach Signature to the Record:** Incorporate the generated signature (S) into the digital record structure, ensuring the record is complete and ready for verification:

$$R = \{T, D, S\} \quad (1)$$

5.6. Submit Record to Blockchain

It is then submitted to the blockchain through a series of steps:

- **Package Signed Record into a Transaction:** The signed record R={T, D, S} is formulated into a transaction T_x. This transaction includes metadata and is prepared for submission to the blockchain network.

$$T_x = Transaction(R) \quad (8)$$

- **Broadcast Transaction to Network:** The transaction $T_x$is broadcast to all nodes within the blockchain network. This ensures that all participants receive the transaction for validation and inclusion.

$$Broadcast(T_x) \quad (9)$$

- **Miners/Validators Add Transaction to a Block:** Miners or validators verify the transaction's validity. They check the integrity of the data, the correctness of the signature using the public key, and the consistency with blockchain rules. Once validated, the transaction is included in a new block B, which is then added to the blockchain. Add to $Block(T_x) \rightarrow B$

The block B is appended to the existing blockchain BC:

$$BC = BC \cup \{B\} \quad (10)$$

5.7. Verify Record on Blockchain

A series of verification steps are conducted:

- **Check Record Signature Using Public Key:** The signature S of the record R={T, D, S} is validated using the corresponding public key Kpub. This involves recalculating the hash H of the timestamp T and data D and verifying that the signature matches:

$$H = Hash(T \parallel D) \quad (2)$$

$$Verify_{K_{pub}}(S, H) \quad (11)$$

- **Validate Record Data Integrity:** Ensure the data D and timestamp T have not been altered by recalculating the hash and comparing it to the original hash stored in the blockchain. This ensures the record remains tamper-proof.

$$H' = Hash(T \parallel D) \quad (12)$$

$$check\ H' = H \quad (13)$$

- **Confirm Record Inclusion in Blockchain:** Verify that the record R is included in block B within the blockchain BC. This can be done by querying the blockchain and ensuring the transaction containing R is part of the blockchain's immutable ledger:

$$R \in B\ and\ B \in BC \quad (14)$$

5.8. Access and Validate Records:

Accessing and validating records on the blockchain involves several technical steps to ensure the integrity and authenticity of the retrieved data.

- **Query Blockchain for Specific Records:** Retrieve the desired records R from the blockchain BC by querying with specific criteria such as timestamps, data fields, or transaction IDs. The query returns the relevant block B containing the records.

$$R \in Query(BC, criteria) \quad (15)$$

- **Verify Signatures and Data Integrity:** For each retrieved record, R={T, D, S} recompute the hash H from the timestamp T and data D. Verify the signature S using the public key Kpub to ensure the data has not been altered.

$$H' = Hash(T || D) \quad (12)$$

- **Use Public Key to Validate Record Authenticity:** Confirm the authenticity of the record by validating that the signature S was produced by the equivalent private key. This ensures that the record R is genuine and unaltered.

$$Authenticity \leftarrow Verify_{K_{pub}}(S, H') \quad (16)$$

By following these steps, the retrieved records from the blockchain are verified for integrity and authenticity, ensuring that they have not been tampered with and are genuine representations of the original data.

Algorithm: Blockchain-Based Self-Signed Keys for Digital Records

START

Step 1. Initialize Blockchain Network

- **Set up nodes**:
  N= {Node1, Node2,…Noden}
  ∀ Nodei ∈ N, configure (Nodei)
- **Define consensus mechanism:**
  Consensus Mechanism ← PoW
- **Implement basic blockchain structure**:
  Blockchain_Ledger ← {Genesis_Block}

Protocols = {P1, P2,…,Pm}

Step 2. Define Digital Record Structure

- **Determine fields for digital records:**
  F = {timestamp(T), data(D), signature(S)}
- **Include timestamp, data, and signature fields:**
  R= {T, D, S}

Step 3. Generate Self-Signed Key Pair

- **Use elliptic curve cryptography:**
  ECC ← secp256k1
- **Generate private key:**
  kpriv ∈ [1, n−1]
- **Derive public key from private key:**
  Kpub = kpriv· G

Step 4. Create Digital Record

- **Populate record fields with relevant data:**
  D ← Actual Data
- **Add timestamp:**
  T←Current
  R= {T, D}

Step 5. Sign Record with Private Key

- **Hash the record data:**
  H = Hash(T‖D)
- **Sign the hash with the private key:**
  $S = Sign_{kpriv}(H)$
- **Attach signature to the record:**
  R = {T, D, S}

Step 6. Submit Record to Blockchain

- **Package signed record into a transaction:**
  Tx = Transaction(R)
- **Broadcast transaction to network:**
  ∀ Nodei ∈ N, send(Tx,Nodei)
- **Miners/validators add transactions to a block:**
  B ← New Block containing Tx
  Blockchain_Ledger←Blockchain_Ledger ∪ {B}

Step 7. Verify Record on Blockchain

- **Check the record signature using the public key:**
  Valid = Verify Kpub (S, H)
- **Validate record data integrity:**
  H′ = Hash(T ‖ D)
  Integrity_Check = (H′==H)
- **Confirm record inclusion in the blockchain:**
  Inclusion_Check = (R ∈ B and B ∈ Blockchain_Ledger)

Step 8. Access and Validate Records

- **Query blockchain for specific records:**
  R← Query(Blockchain_Ledger, Criteria)
- **Verify signatures and data integrity:**
  H′= Hash(T‖D)
  Valid = VerifyKpub (S, H′)
- **Use public key to validate record authenticity:**
  Authenticity = Verify Kpub(S,H′)

END

6. Results and Analysis

Blockchain cryptography has undergone significant advancements, particularly in the area of digital record protection. One of the key innovations is the Self-Signed Key Approach which enhances security, data integrity, and authenticity for sensitive digital records. The use of ECC, in conjunction with blockchain-based ledgers, ensures secure, decentralized storage and verification of records. Below is an explanation of the results obtained from implementing the self-signed key application in a blockchain network.

Performance analysis of this cryptographic system reveals key metrics such as execution time, average latency, and throughput. For 100 transactions, the execution time is 107.01 seconds (s), with low latency at 1.0455s and throughput at 0.0078 tps, indicating efficient processing for smaller transaction volumes. However, as the transaction count rises to 1000, the

execution time increases to 1626.03s, with latency extending to 3.1790s, and throughput declining to 0.0018 tps, reflecting the increased computational overhead required for larger transaction loads and blockchain verification processes as shown in Table 2. Despite the linear increase in execution time and a gradual rise in latency, the system maintains reasonable performance even as the transaction volume scales.

Table 2 - Performance analysis of the proposed method

No. of Transactions	Execution Time (s)	Average Latency (s)	Average Throughput (tps)
100	107.01	1.0455	0.0078
200	289.45	1.3260	0.00576
300	457.95	1.6065	0.00444
400	634.39	1.8275	0.00348
500	841.46	2.1080	0.00300
600	1047.31	2.3715	0.00264
700	1162.11	2.5670	0.00252
800	1277.18	2.7880	0.00228
900	1482.67	2.9920	0.00204
1000	1626.03	3.1790	0.00180

While the proposed self-signed key approach shows a reduction in throughput and higher latency for larger data loads, these trade-offs are expected in systems that prioritize security and data integrity. Application of ECC with the decentralized and consensus-driven architecture of blockchain guarantees that even with a slight degradation in performance, the cryptographic solution would remain secure and scalable and thus an ideal system to secure digital documents in scenarios where security is necessary coupled with transaction processing.

With larger file sizes, centralized storage systems become bottlenecked because they use a single point of validation, hence less productive in dealing with large data sets. In contrast, blockchain systems spread the verification process across multiple nodes, reducing time consumption and improving overall performance for larger files. The graph given in Figure 3 compares time consumption for centralized and proposed blockchain-based storage as file size increases, demonstrating blockchain's efficiency for larger datasets. Centralized storage shows a sharp rise in time, from 1.2s at 5 MB to 4.5s at 25 MB, indicating inefficiencies with larger files due to bottlenecks in centralized verification. In contrast, the proposed blockchain storage increases more gradually, from 0.8s at 5 MB to 3s at 25 MB.

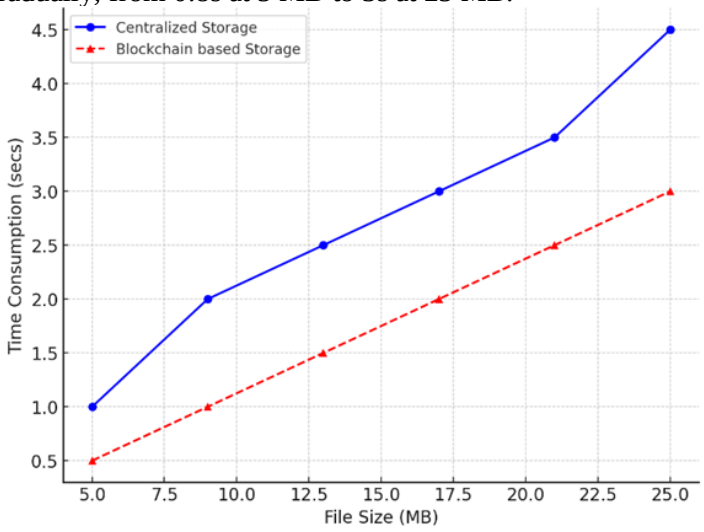

Fig. 3. Time Consumption

This reflects blockchain's distributed nature, which reduces bottlenecks and enhances performance for large files. Numerically, blockchain storage is 33% faster than centralized storage for a 25 MB file, making it more scalable and efficient for handling large datasets securely.

The communication cost over multiple rounds of a process, with the cost increasing gradually as the number of rounds progresses. In Figure 4 the y-axis shows communication cost on a logarithmic scale, while the x-axis represents the number of rounds. The steady upward trend

indicates that the communication cost increases slightly but consistently with each round, reflecting the cumulative overhead as the process advances.

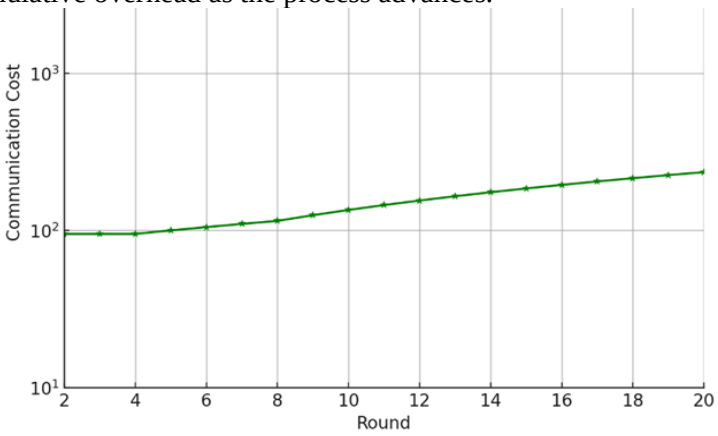

Fig. 4. Communication cost

The key generation process involves creating a private key and deriving the public key using ECC. Figure 5 shows that as the number of features in a digital record increases, the key generation time using ECC gradually increases. This indicates that the algorithm scales efficiently, with only a slight impact on key generation time as data complexity grows.

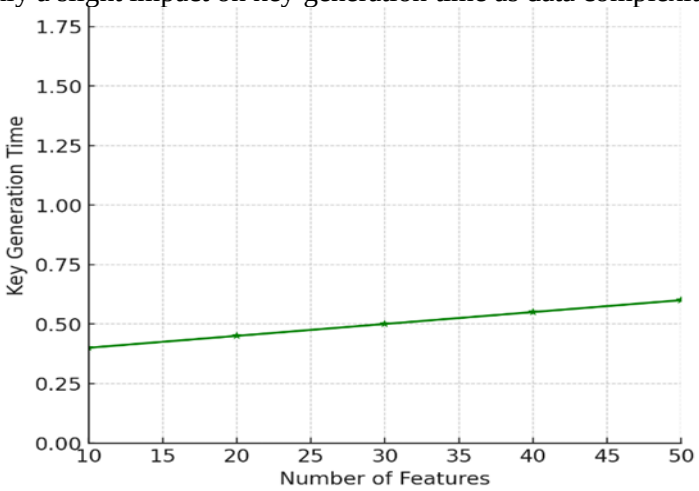

Fig. 5. Key Generation Time

Figure 6 depicts the download and upload times for various file sizes using the proposed method. As file size increases, both download and upload times also increase, with download times consistently lower than upload times across all file sizes.

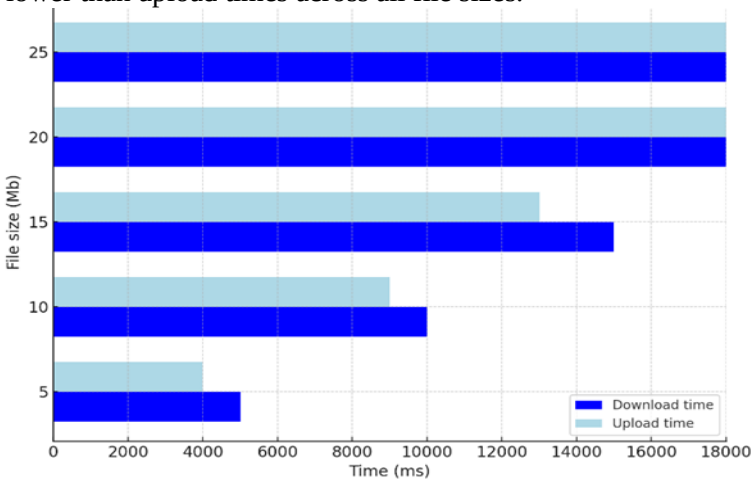

Fig. 6. Upload And Download Time Of The Proposed Method

Considering the observed performance trends, a comprehensive comparative analysis of the methodologies and models proposed by various authors concerning the method utilized in this study is conducted. The comparison is based on various parameters, including security, efficiency, and scalability, providing insights into the strengths and potential enhancements of the proposed approach.

The comparison with existing studies revealed that though previous research maintains Privacy Preservation and Access Control effectively, they miss some key security features present solely in the suggested self-signed key infrastructure. For example, none of the previous research includes Secure Search, an exclusive feature in the proposed technique as can be seen from Table 3. This enables the efficient querying of encrypted data while preserving privacy, which makes the proposed technique better in terms of data retrieval effectiveness. Moreover, though Data Auditing is pursued in a limited number of studies (Usman & Qamar, 2020; Chenthara et al., 2020; Ghazal et al., 2022; Madine et al., 2020), most of them do not pursue it and hence fail to verify data integrity. However, the proposed system always includes Data Auditing to ensure secure tampering detection and authentic data verification.

Table 3 - Comparison With Other Existing Studies

Study	Privacy Preservation	Secure Search	Data Auditing	Flexibility	Blockchain & Access Control	Decentralized Access	Time-Controlled Revocation	Decentralized Certificate Authority
Usman & Qamar, (2020)	✓	X	X	✓	✓	✓	X	X
Tith et al., (2020)	✓	X	✓	X	✓	✓	X	X
Chenthara et al., (2020)	✓	X	✓	✓	✓	X	X	X
B. Liu et al., (2020)	✓	X	✓	X	✓	✓	X	X
Zou & Zeng, (2023)	✓	X	✓	✓	✓	✓	X	X
Ghazal et al., (2022)	✓	X	✓	✓	✓	✓	X	X
Madine et al., (2020)	✓	X	✓	✓	✓	✓	X	X
Azbeg et al., (2022)	✓	X	✓	✓	✓	✓	X	X
Du et al., (2021)	✓	X	✓	✓	✓	✓	X	X
Khatoon, (2020)	✓	X	✓	✓	✓	✓	X	X
Na & Park, (2021)	✓	X	✓	✓	✓	✓	X	X

Tuan-Vinh Le & Tuan-Vinh Le, (2021)	✓	X	✓	✓	✓	✓	X	X
Zamani et al., (2020)	✓	X	✓	✓	✓	✓	X	X
Zhou et al., (2021)	✓	X	✓	✓	✓	✓	X	X
Ajakwe et al., (2024)	✓	X	✓	✓	✓	✓	X	X
Proposed Approach	✓	✓	✓	✓	✓	✓	✓	✓

Also, Time-Controlled Revocation, being of prime importance in data confidentiality through automatic revocation of access privileges after a fixed time duration, is completely lacking in all existing work. This unique characteristic of the proposed system guarantees controlled and limited data disclosure and less chance of unauthorized long-term access. Further, despite most of the existing works (Azbeg et al., 2022; Du et al., 2021; Khatoon, 2020) utilize blockchain for distributed storage, and still use centralized certificate authorities for key management, which can be potentially of a security risk by nature. Yet, the proposed work introduces Self-Signed Keys to remove third-party certificate authorities. This not only provides security by minimizing the reliance on other parties but also defeats trust-based weaknesses, and thus the system becomes robust and standalone.

Additionally, the comparison of encryption time of different cryptographic schemes for different file sizes given in Table 4 indicates that the proposed ECC (secp256k1) method on blockchain platform is superior to other methods presented by (S. et al., 2024) like Modified Policy Attribute-Based Encryption (MKP-ABE), Key Policy (KP)-ABE, Rivest Shamir Adelman (RSA), and Advanced Encryption Standard (AES). For a 5 MB file, the proposed ECC is 327 ms, much faster than AES and RSA taking 1538 ms and 1242 ms, respectively. By taking the file size to 25 MB, the proposed ECC is most effective at 3650 ms, while AES and RSA take 5701 ms and 5364 ms, respectively as depicted in Figure 7.

Table 4 - Comparison with existing approaches based on encryption time

File size (MB)	AES (ms)	KP-ABE (ms)	RSA (ms)	MKP-ABE (ms)	Proposed ECC secp256k1 (ms)
5.0	1538	701	1242	362	327
10.0	2448	1552	2112	1202	900
15.0	3634	2428	3228	2053	1325
20.0	4248	3004	3871	2473	2054
25.0	5701	4569	5364	4008	3650

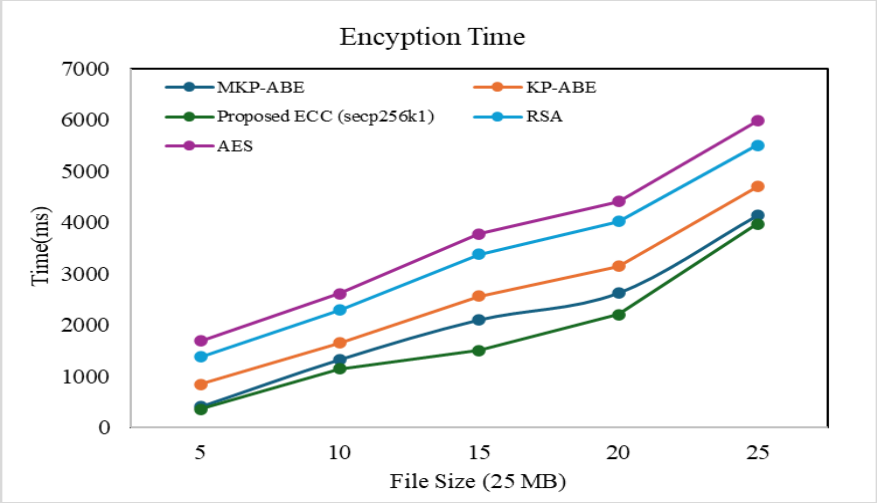

Fig. 7. Encryption time of various approaches

This shows that the suggested ECC executes faster encryption time for any file size compared to conventional methods and is an ideal selection for efficient and secure encryption.

Additionally, the comparison of decryption time across different cryptographic algorithms with varying file sizes, as presented in Table 5, serves to highlight even more the performance efficiency of the proposed ECC. For example, in decrypting a 5 MB file, ECC's decryption takes just 356 ms, faring much better than MKP-ABE (403 ms), KP-ABE (843 ms), RSA (1378 ms), and AES (1689 ms) presented by S. et al., (2024). Even when the file size is doubled to 25 MB, ECC's performance is continuous, taking just 3968 ms to decrypt, compared to AES and RSA at 5976 ms and 5501 ms, as illustrated in Figure 8.

Table 5 - Comparison with existing approaches based on decryption time

File size (MB)	Proposed ECC secp256k1 (ms)	MKP-ABE (ms)	KP-ABE (ms)	RSA (ms)	AES (ms)
5	356	403	843	1378	1689
10	1147	1325	1644	2286	2612
15	1507	2101	2558	3382	3776
20	2203	2624	3146	4015	4411
25	3968	4138	4701	5501	5976

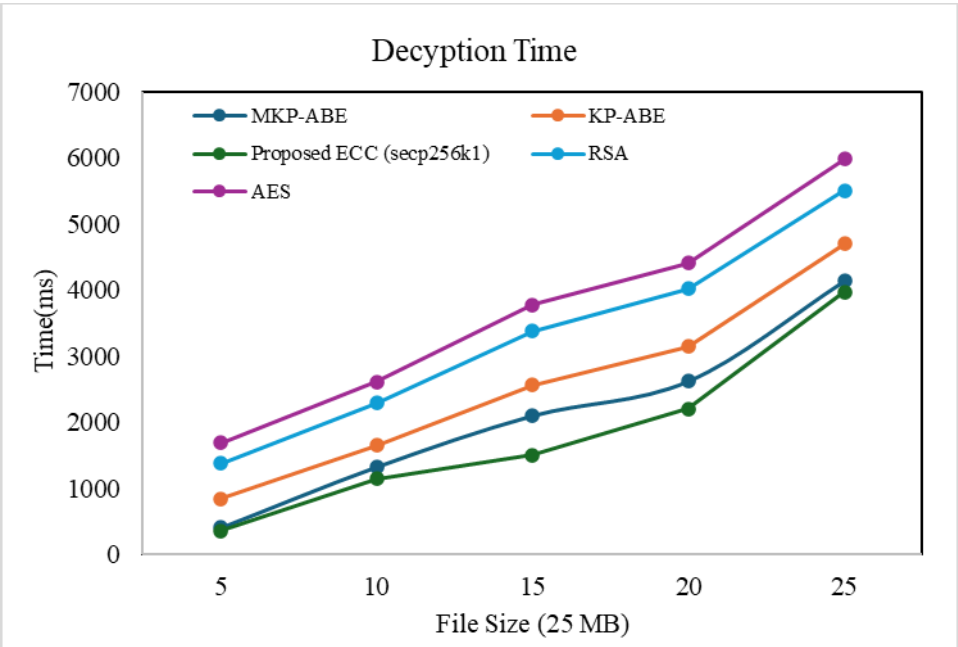

Fig. 8. Decryption time of various approaches

This implies that ECC always produces the highest decryption speeds and is a more suitable option for fast and secure data retrieval than conventional encryption schemes such as RSA and AES.

7. Discussion

The results of this study affirm that the self-signed key blockchain model is an effective, scalable, and secure way of securing digital documents. With the use of Elliptic Curve Cryptography (ECC) and the decentralized nature of the blockchain, the system can steer clear of the vulnerabilities of single points of failure and loss of data due to central storage. The performance analysis indicates that the system achieves higher encryption and decryption speeds than the conventional method. For example, ECC provides 3650 ms encryption time for a file of 25 MB, which is far better than RSA (5364 ms) and AES (5701 ms), demonstrating its efficiency. In addition, the model provides stable throughput and controllable latency and can achieve an average throughput of 0.0018 tps and a latency of 3.1790s on 1000 transactions, which demonstrates its reliability and scalability in processing large amounts of data. Moreover, the decentralized access and revocation model by time also greatly improves data privacy and access control, and it is best suited for sensitive industries like healthcare, finance, and supply chain management.

In comparison to the existing literature, the proposed model is clearly defined in terms of its performance and security advantages. In comparison to Chenthara et al., (2020)non-decentralized approach, the proposed model has Decentralized Access, Secure Search, and Time-Controlled Revocation and thus is more flexible and secure. Besides, unlike the third-party authority-based key management of Tith et al., (2020) and (B. Liu et al., 2020), the self-signed key process employed here does away with the need to depend on external authorities and thus guarantees maximum data confidentiality and independence. The utilization of ECC also has the advantage of reducing the encryption and decryption time compared to the RSA and AES algorithms employed in the present study. Overall, the research can prove that the proposed blockchain-based cryptographic system is not only secure and efficient but also scalable and thus particularly relevant to large-scale, real-time electronic record management systems.

8. Conclusion & Future Scope

The findings of this research confirm that the blockchain system with a self-signed key is an efficient, scalable, and secure option for digital document security. With the use of Elliptic Curve Cryptography and a decentralized blockchain process, the proposed system effectively mitigates the disadvantage of centralized storage, i.e., single points of failure and data leakage. Performance comparison illustrates that the proposed system provides faster encryption and decryption rates in comparison to conventional systems. ECC offers an encryption time of 3650 ms for a 25 MB file, which is quite low compared to RSA and AES, illustrating its efficiency. Besides this, the proposed technique exhibits low latency and constant throughput with 0.0018 tps average throughput and 3.1790s average latency for 1000 transactions, illustrating its stability and scalability with large data sizes. Additionally, the decentralized access mechanism and time-managed revocation processes greatly increase data access control and data confidentiality, and hence it is highly beneficial for sensitive applications such as healthcare, finance, and supply chain management.

The application of this work is not limited to integrity preservation of digital records. The framework provides a basis for designing complex systems for data-sharing and authentication involving the blockchain with added performance and confidentiality. The framework is efficient, and scalable, and is therefore a viable option for organizations that have to manage sensitive levels of information, which enhances trust and openness. There are opportunities for further research, particularly in using AI and machine learning for predictive analysis, as further development in real-time authentication and anomaly detection in blockchains is possible. Further development to the framework of integration with cross-chain interoperability and data-

sharing by multiple participants could further amplify applications in many fields, such as finance, medicine, and IoT systems.

References

Abead, S. A., & Ali, N. H. M. (2024). Lightweight Block and Stream Cipher Algorithm: A Review. *Journal of Applied Engineering and Technological Science (JAETS)*, *5*(2), 860–874. https://doi.org/10.37385/jaets.v5i2.3966

Ajakwe, S. O., Saviour, I. I., Ihekoronye, V. U., Nwankwo, O. U., Dini, M. A., Uchechi, I. U., Kim, D.-S., & Lee, J. M. (2024). Medical IoT Record Security and Blockchain: Systematic Review of Milieu, Milestones, and Momentum. *Big Data and Cognitive Computing*, *8*(9), 121. https://doi.org/10.3390/bdcc8090121

Aoun, A., Ilinca, A., Ghandour, M., & Ibrahim, H. (2021). A review of Industry 4.0 characteristics and challenges, with potential improvements using blockchain technology. *Computers & Industrial Engineering*, *162*, 107746. https://doi.org/10.1016/j.cie.2021.107746

Azbeg, K., Ouchetto, O., & Jai Andaloussi, S. (2022). BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. *Egyptian Informatics Journal*, *23*(2), 329–343. https://doi.org/10.1016/j.eij.2022.02.004

Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., & Chen, Z. (2020). Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. *PLOS ONE*, *15*(12), e0243043. https://doi.org/10.1371/journal.pone.0243043

Chu, Y., Kim, J. M., Lee, Y., Shim, S., & Huh, J. (2020). SS-DPKI: Self-Signed Certificate Based Decentralized Public Key Infrastructure for Secure Communication. *2020 IEEE International Conference on Consumer Electronics (ICCE)*, 1–6. https://doi.org/10.1109/ICCE46568.2020.9043086

Chukwu, E., & Garg, L. (2020). A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations. *IEEE Access*, *8*, 21196–21214. https://doi.org/10.1109/ACCESS.2020.2969881

Du, M., Chen, Q., Chen, J., & Ma, X. (2021). An Optimized Consortium Blockchain for Medical Information Sharing. *IEEE Transactions on Engineering Management*, *68*(6), 1677–1689. https://doi.org/10.1109/TEM.2020.2966832

Garba, A., Khoury, D., Balian, P., Haddad, S., Sayah, J., Chen, Z., Guan, Z., Hamdan, H., Charafeddine, J., & Al-Mutib, K. (2023). LightCert4IoTs: Blockchain-Based Lightweight Certificates Authentication for IoT Applications. *IEEE Access*, *11*, 28370–28383. https://doi.org/10.1109/ACCESS.2023.3259068

Ghazal, T. M., Hasan, M. K., Abdullah, S. N. H. S., Bakar, K. A. A., & Al Hamadi, H. (2022). Private blockchain-based encryption framework using computational intelligence approach. *Egyptian Informatics Journal*, *23*(4), 69–75. https://doi.org/10.1016/j.eij.2022.06.007

Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, *22*(2), 177–183. https://doi.org/10.1016/j.eij.2020.07.003

Khan, I., Phuyal, S., Correia, R., & C. Ferreira, J. (2024). A Survey of Distributed Ledger Technologies in the Health Domain. *Journal of Information Assurance and Security*, *19*(6), 249–265. https://doi.org/10.2478/ias-2024-0017

Khatoon, A. (2020). A Blockchain-Based Smart Contract System for Healthcare Management. *Electronics*, *9*(1), 94. https://doi.org/10.3390/electronics9010094

Kumari, A., Bhaskar, S., Patil, S., & Parmar, K. (2023). Decentralized and Multi-Authority based Public Key Infrastructure for Sharing Electronic Health Records. *Procedia Computer Science*, *230*, 44–54. https://doi.org/10.1016/j.procs.2023.12.059

Lakhan, A., Thinnukool, O., Groenli, T. M., & Khuwuthyakorn, P. (2023). RBEF: Ransomware Efficient Public Blockchain Framework for Digital Healthcare Application. *Sensors*, *23*(11), 5256. https://doi.org/10.3390/s23115256

Liang, W., Huang, W., Long, J., Zhang, K., Li, K.-C., & Zhang, D. (2020). Deep Reinforcement Learning for Resource Protection and Real-Time Detection in IoT Environment. *IEEE Internet of Things Journal*, *7*(7), 6392–6401. https://doi.org/10.1109/JIOT.2020.2974281

Liu, B., Xiao, L., Long, J., Tang, M., & Hosam, O. (2020). Secure Digital Certificate-Based Data Access Control Scheme in Blockchain. *IEEE Access*, *8*, 91751–91760. https://doi.org/10.1109/ACCESS.2020.2993921

Liu, G., Xie, H., Wang, W., & Huang, H. (2024). A secure and efficient electronic medical record data sharing scheme based on blockchain and proxy re-encryption. *Journal of Cloud Computing*, *13*(1), 44. https://doi.org/10.1186/s13677-024-00608-w

Lucking, M., Manke, R., Schinle, M., Kohout, L., Nickel, S., & Stork, W. (2020). Decentralized patient-centric data management for sharing IoT data streams. *2020 International Conference on Omni-Layer Intelligent Systems (COINS)*, 1–6. https://doi.org/10.1109/COINS49042.2020.9191653

Ma, L., Liao, Y., Fan, H., Zheng, X., Zhao, J., Xiao, Z., Zheng, G., & Xiong, Y. (2022). PHDMF: A Flexible and Scalable Personal Health Data Management Framework Based on Blockchain Technology. *Frontiers in Genetics*, *13*. https://doi.org/10.3389/fgene.2022.877870

Madine, M. M., Battah, A. A., Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y., Pesic, S., & Ellahham, S. (2020). Blockchain for Giving Patients Control Over Their Medical Records. *IEEE Access*, *8*, 193102–193115. https://doi.org/10.1109/ACCESS.2020.3032553

Martínez, A. L., Naghmouchi, M., Laurent, M., Garcia-Alfaro, J., Pérez, M. G., Martínez, A. R., & Nespoli, P. (2025). *Empower Healthcare through a Self-Sovereign Identity Infrastructure for Secure Electronic Health Data Access*. http://arxiv.org/abs/2501.12229

Mensah, B. A. (2021). *Implementing Blockchain Technology to Develop a National Electronic Data Exchange System for Medical Records*.

Mohammed Ali, N. A., & Mohammed Ali, F. A. (2023). Optimizing Cloud-Fog-Edge Job Scheduling Using Catastrophic Genetic Algorithm and Block Chain-Based Trust: A Collaborative Approach. *Journal of Applied Engineering and Technological Science (JAETS)*, *5*(1), 569–580. https://doi.org/10.37385/jaets.v5i1.3125

Muttaqin, K., & Rahmadoni, J. (2020). Analysis And Design of File Security System AES (Advanced Encryption Standard) Cryptography Based. *Journal of Applied Engineering and Technological Science (JAETS)*, *1*(2), 113–123. https://doi.org/10.37385/jaets.v1i2.78

Na, D., & Park, S. (2021). Fusion Chain: A Decentralized Lightweight Blockchain for IoT Security and Privacy. *Electronics*, *10*(4), 391. https://doi.org/10.3390/electronics10040391

Naveen N, & Thippeswamy, K. (2021). A Framework for Secure eHealth Data Privacy Preserving on Blockchain with SHA-256 in Cloud Environment. In *Turkish Online Journal of Qualitative Inquiry (TOJQI)* (Vol. 12, Issue 8).

Peng, L., Feng, W., Yan, Z., Li, Y., Zhou, X., & Shimizu, S. (2021). Privacy preservation in permissionless blockchain: A survey. *Digital Communications and Networks*, *7*(3), 295–307. https://doi.org/10.1016/j.dcan.2020.05.008

Pillai, B., Biswas, K., Hou, Z., & Muthukkumarasamy, V. (2022). Cross-Blockchain Technology: Integration Framework and Security Assumptions. *IEEE Access*, *10*, 41239–41259. https://doi.org/10.1109/ACCESS.2022.3167172

Ramesh, D., Santosh, T., Trivedi, M. C., & Le, C. H. (2025). Ensuring Digital Sovereignty in Cross-chain EHR Sharing: A Relay-as-a-Service Approach for Secure Healthcare Interoperability. *Procedia Computer Science*, *254*, 48–57. https://doi.org/10.1016/j.procs.2025.02.063

Rikiti, M. Z. A., Kusmayanto, E., & Kurniawati, R. (2022). Design And Development of Help Patient Data Management Information System at Sinergi Atap Negeri Foundation Web-Based Using Codeigniter. *Journal of Applied Engineering and Technological Science (JAETS)*, *3*(2), 235–245. https://doi.org/10.37385/jaets.v3i2.792

S., V., M., P., S., N., & Martinson, E. O. (2024). An Efficient Secure Sharing of Electronic Health Records Using IoT-Based Hyperledger Blockchain. *International Journal of Intelligent Systems*, *2024*, 1–16. https://doi.org/10.1155/2024/6995202

Saleem, A. D., & Abdulrahman, A. A. (2024). Attacks Detection in Internet of Things Using Machine Learning Techniques: A Review. *Journal of Applied Engineering and Technological Science (JAETS)*, *6*(1), 684–703. https://doi.org/10.37385/jaets.v6i1.4878

Sethaput, V., & Innet, S. (2023). Blockchain application for central bank digital currencies (CBDC). *Cluster Computing*, *26*(4), 2183–2197. https://doi.org/10.1007/s10586-022-03962-z

Shah, S. M., & Khan, R. A. (2020). Secondary Use of Electronic Health Record: Opportunities and Challenges. *IEEE Access*, *8*, 136947–136965. https://doi.org/10.1109/ACCESS.2020.3011099

Shi, J., Zeng, X., & Han, R. (2022). A Blockchain-Based Decentralized Public Key Infrastructure for Information-Centric Networks. *Information*, *13*(5), 264. https://doi.org/10.3390/info13050264

Singh, S., Pankaj, B., Nagarajan, K., P. Singh, N., & Bala, V. (2022). Blockchain with cloud for handling healthcare data: A privacy-friendly platform. *Materials Today: Proceedings*, *62*, 5021–5026. https://doi.org/10.1016/j.matpr.2022.04.910

Tith, D., Lee, J.-S., Suzuki, H., Wijesundara, W. M. A. B., Taira, N., Obi, T., & Ohyama, N. (2020). Application of Blockchain to Maintaining Patient Records in Electronic Health Record for Enhanced Privacy, Scalability, and Availability. *Healthcare Informatics Research*, *26*(1), 3. https://doi.org/10.4258/hir.2020.26.1.3

Tuan-Vinh Le, T.-V. Le, & Tuan-Vinh Le, C.-L. H. (2021). A Systematic Literature Review of Blockchain Technology: Security Properties, Applications and Challenges. **網際網路技術學刊**, *22*(4), 789–801. https://doi.org/10.53106/160792642021072204007

Turan, E., Sen, S., & Ergun, T. (2024). A Semi-Decentralized PKI Based on Blockchain With a Stake-Based Reward-Punishment Mechanism. *IEEE Access*, *12*, 60705–60721. https://doi.org/10.1109/ACCESS.2024.3394657

Ucbas, Y., Eleyan, A., Hammoudeh, M., & Alohaly, M. (2023). Performance and Scalability Analysis of Ethereum and Hyperledger Fabric. *IEEE Access*, *11*, 67156–67167. https://doi.org/10.1109/ACCESS.2023.3291618

Usman, M., & Qamar, U. (2020). Secure Electronic Medical Records Storage and Sharing Using Blockchain Technology. *Procedia Computer Science*, *174*, 321–327. https://doi.org/10.1016/j.procs.2020.06.093

Wang, H., Wang, Y., Taleb, T., & Jiang, X. (2020). Editorial: Special issue on security and privacy in network computing. *World Wide Web*, *23*(2), 951–957. https://doi.org/10.1007/s11280-019-00704-x

Wenhua, Z., Qamar, F., Abdali, T.-A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends. *Electronics*, *12*(3), 546. https://doi.org/10.3390/electronics12030546

Yaacoub, J.-P. A., Noura, M., Noura, H. N., Salman, O., Yaacoub, E., Couturier, R., & Chehab, A. (2020). Securing internet of medical things systems: Limitations, issues and recommendations. *Future Generation Computer Systems*, *105*, 581–606. https://doi.org/10.1016/j.future.2019.12.028

Zamani, E., He, Y., & Phillips, M. (2020). On the Security Risks of the Blockchain. *Journal of Computer Information Systems*, *60*(6), 495–506. https://doi.org/10.1080/08874417.2018.1538709

Zhang, D., Wang, S., Zhang, Y., Zhang, Q., & Zhang, Y. (2022). A Secure and Privacy-Preserving Medical Data Sharing via Consortium Blockchain. *Security and Communication Networks*, *2022*, 1–15. https://doi.org/10.1155/2022/2759787

Zhang, E., Li, M., Yiu, S.-M., Du, J., Zhu, J.-Z., & Jin, G.-G. (2021). Fair hierarchical secret sharing scheme based on smart contract. *Information Sciences*, *546*, 166–176. https://doi.org/10.1016/j.ins.2020.07.032

Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, *105*, 475–491. https://doi.org/10.1016/j.future.2019.12.019

Zhou, J., Feng, Y., Wang, Z., & Guo, D. (2021). Using Secure Multi-Party Computation to Protect Privacy on a Permissioned Blockchain. *Sensors*, *21*(4), 1540. https://doi.org/10.3390/s21041540

Zou, X., & Zeng, P. (2023). A New Digital Signature Primitive and Its Application in Blockchain. *IEEE Access*, *11*, 54607–54615. https://doi.org/10.1109/ACCESS.2023.3280638