ISSN: 2634 - 8853

Journal of Engineering and Applied Sciences Technology

Research Article

Open Access

Implementation of Elliptic Curve Digital Signatures in Blockchain for Management of Certificates in Higher Education

Faton Kabashi[1]*, Halili Snopçe[2], Artan Luma L[3], Azir Aliu[4] and Lamir Shkurti[5]

SEE University, Tetovo, North Macedonia, Kosovo

ABSTRACT

The implementation of Elliptic Curve Digital Signatures (ECDSA) in blockchain technology for certificate management in Higher Education is a promising solution that has the potential to revolutionize the way that certificates are managed and verified. The use of blockchain technology provides a decentralized and tamper-proof system that can be accessed by authorized parties from anywhere in the world. By utilizing blockchain technology, academic institutions can ensure the integrity and immutability of student certificates, minimizing the risk of fraud and forgery. The use of ECDS further strengthens the security of these certificates by offering a more efficient and secure method of digital signing. Additionally, blockchain technology can enable the creation of smart contracts that automate the process of issuing and verifying certificates, increasing efficiency and reducing administrative costs. Overall, the implementation of ECDS in blockchain technology has the potential to revolutionize the way academic institutions manage and verify student certificates, providing a reliable and trustworthy solution for the growing demand for digital credentials.

***Corresponding author**

Faton Kabashi, SEE University, Tetovo, North Macedonia, Kosovo.

Received: April 18, 2023; **Accepted:** April 24, 2023; **Published:** April 29, 2023

Keywords: ECDSA, Blockchain, Management of Certificates, Implementation, Higher Education

Introduction

The rapid advancements in digital technology have transformed various sectors across the globe, and higher education is no exception. With a growing need for secure and efficient methods of managing academic records, it is crucial for educational institutions to adapt to the changing landscape. One such innovation that has emerged as a promising solution is blockchain technology. Originally designed to underpin the digital currency Bitcoin, blockchain has expanded its applications beyond finance and is now revolutionizing certificate management in higher education [1].

Blockchain technology has the potential to revolutionize the way certificate management is done in higher education [2]. Traditionally, certificate management in higher education has been a cumbersome process, involving a lot of paperwork and manual processes. This can lead to errors, delays, and increased costs for both the educational institution and the student.

With blockchain technology, however, certificate management can be made more efficient, secure, and transparent. Blockchain technology can be used to create a tamper-proof digital ledger of all certificates issued by an educational institution [3]. Each certificate can be stored as a unique digital asset on the blockchain, with all relevant information about the certificate, such as the student's name, the course completed, and the grade achieved. This digital ledger can be accessed by authorized parties, such as employers or other educational institutions, to verify the authenticity of a certificate. This eliminates the need for the student to provide physical copies of their certificates, which can be lost or forged. It also provides a more efficient way for employers to verify the qualifications of potential employees, reducing the time and cost of the hiring process [4].

As we further explore the potential of blockchain technology in higher education, it is essential to understand its key features. A blockchain is a decentralized, distributed ledger that stores data in a series of interconnected blocks [5]. Each block contains a list of transactions, and once added to the chain, the data becomes virtually immutable [6]. This technology ensures data integrity and transparency, making it an ideal solution for certificate management in higher education [7].

Traditional certificate management systems often suffer from various issues, such as the risk of credential fraud, the time-consuming process of verifying academic records, and the challenge of maintaining and updating records securely. Blockchain technology offers a way to address these problems by digitizing certificates, streamlining the verification process, and ensuring the authenticity and immutability of records [8].

The implementation of blockchain in higher education has already seen success in various institutions worldwide. Notable examples include the University of Melbourne and the Massachusetts Institute of Technology, both of which have adopted blockchain-based systems for issuing digital diplomas. These systems allow graduates to access and share their credentials securely and quickly, while also enabling employers and other institutions to verify the authenticity of the documents with ease.

Despite the promising potential of blockchain technology in higher education, there are still challenges to overcome [9]. These include the need for interoperability between different blockchain platforms, addressing privacy concerns, and the cost of implementing and maintaining such systems [10]. Further research and collaboration between stakeholders, including educational institutions, technology providers, and regulatory bodies, are required to address these issues and facilitate the widespread adoption of blockchain technology for certificate management in higher education.

In conclusion, blockchain technology offers a promising solution to the challenges faced by traditional certificate management systems in higher education. By leveraging its unique features, such as decentralization, immutability, and transparency, educational institutions can enhance the security, efficiency, and accessibility of academic credentials. As more institutions adopt this technology, the future of certificate management in higher education is set to become more reliable, efficient, and secure.

Related Work

The use of mathematics in blockchain is a critical aspect of the technology's security and functionality. Several research studies have explored various mathematical concepts and techniques used in blockchain, including cryptography, hashing, and consensus mechanisms.

Cryptography is a fundamental concept in blockchain, which involves the use of mathematical algorithms to secure data. Research studies have focused on various cryptographic techniques, such as Elliptic Curve Cryptography (ECC) and Zero-Knowledge Proofs (ZKP) For example, a study by Bellés-Muñoz et al. explored the use of ECC in blockchain to improve its security and performance [11].

Hashing is another critical concept in blockchain, which is used to ensure the immutability of data on the blockchain. Several studies have explored the use of hashing algorithms, such as SHA-256 and Scrypt. For instance, a study by Navamani et al. examined the use of Scrypt in blockchain to improve its resistance to attacks [12]. Consensus mechanisms are also essential in blockchain, as they help to ensure that all participants on the network agree on the validity of transactions. Research studies have explored various consensus mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS). For example, a study by Zhang, R et al. compared the security and energy efficiency of PoW and PoS consensus mechanisms [13].

Other mathematical concepts such as game theory, probability theory, and graph theory are also used in blockchain. Game theory is used to model the behavior of participants in the blockchain network, while probability theory is used to calculate the likelihood of specific events. Graph theory is used to analyze the network structure of the blockchain and identify potential vulnerabilities.

S. Behnia, A. Akhavan, A. Akhshani, and A. Samsudin introduced an innovative image encryption method utilizing Jacobian elliptic map8. The original image data matrix is transformed into a one-dimensional matrix after interacting with the key, which consists of initial conditions and control parameters. The matrix elements are encrypted using a specific equation, and the matrix is then reformed to its initial dimensions [14].

Countless benefits derived from employing blockchain technology in education include the unchangeable nature and origin tracking of uploaded credentials, direct and safe communication among stakeholders, system-wide transparency and trust, as well as decentralized management through a distributed digital ledger [15].

The article suggests a mobile app for preserving and validating student certificates utilizing Hyperledger (a permissioned blockchain). To ensure privacy, records are kept encrypted. The authors evaluate their prototype against earlier works, focusing on on-chain storage capacity and scalability [16].

Alrikabi et al., introduced the educational process paradigm, highlighting numerous cloud-based inputs and outputs, and discussed how the digital cloud can be employed to address educational challenges across various organizations through distance learning [17]. The study examined the features of this environment and explored the potential of implementing them in universities and educational establishments.

This article introduces the development and execution of a blockchain-oriented domain authentication approach that maintains privacy for mobile, browser, and IoT devices. Furthermore, a comparison to alternative authentication techniques is provided. The primary benefits of this method are its ample storage and minimal bandwidth requirements for certificate authentication [18].

In conclusion, the use of mathematics in blockchain is essential to creating a secure and decentralized system that can be trusted by users. Researchers continue to explore various mathematical concepts and techniques to improve the performance, security, and functionality of blockchain technology.

Blockchain Technology

Blockchain technology is a decentralized, distributed ledger technology that allows for secure and transparent record-keeping [19]. Each block in the blockchain contains a record of transactions that have been verified by a network of computers, or nodes, on the network. Once a block is added to the blockchain, it cannot be altered or deleted, making it a tamper-proof and immutable record of all transactions [20].

In the context of certificate management in higher education, this means that certificates can be stored on a blockchain in a way that is secure and transparent. Each certificate would be stored as a unique digital asset on the blockchain, with all relevant information about the certificate, such as the student's name, the course completed, and the grade achieved. This information would be verified by the network of nodes on the blockchain, ensuring that the certificate is authentic and has not been tampered with.

Furthermore, because the blockchain is a decentralized ledger, there is no need for a central authority, such as a government or educational institution, to oversee the verification process. Instead, the network of nodes on the blockchain can verify the authenticity of a certificate in a decentralized and transparent way, reducing the risk of fraud and increasing trust in the certificate.

Overall, blockchain technology has the potential to transform certificate management in higher education by providing a more efficient, secure, and transparent way to store and verify certificates.

One of the key features of blockchain technology is its ability to provide a high level of security through the use of cryptographic algorithms [21]. Transactions on a blockchain are secured by digital signatures, which are created using public and private key pairs. Each participant in the network has their own unique key pair, and transactions can only be authorized by the owner of the private key [22].

In addition to security, blockchain technology also offers transparency and accountability. Because the ledger is distributed across a network of computers, every participant can view the entire history of transactions on the network. This creates a level of transparency that is not possible with traditional centralized systems [23].

Another important aspect of blockchain technology is its ability to automate processes through the use of smart contracts. Smart contracts are self-executing contracts that are programmed to automatically execute when certain conditions are met. They can be used to automate a wide range of business processes, such as supply chain management, insurance claims processing, and more [24].

Blockchain technology also has the potential to revolutionize industries such as finance, where it can provide faster, cheaper, and more secure transactions [25]. Cryptocurrencies like Bitcoin and Ethereum are built on blockchain technology, and have become popular for their ability to facilitate fast, low-cost transactions without the need for intermediaries [26].

There are many different types of blockchains, including public blockchains, private blockchains, and consortium blockchains [27]. Public blockchains are open to anyone, while private blockchains are restricted to a specific group of participants. Consortium blockchains are a hybrid of public and private blockchains, and are used by multiple organizations to create a shared database.

Preliminaries

This section provides a brief overview of three key concepts: elliptic curves and their properties, elliptic curve cryptography (ECC), and the elliptic curve digital signature algorithm (ECDSA).

Elliptic Curve (EC)

An elliptic curve is a type of mathematical curve defined by an equation of the form:

$y^2 = x^3 + ax + b$

where a and b are constants [28]. The curve has points with x and y coordinates that satisfy the equation, as well as a special point called the "point at infinity". The graph below shows an elliptic curve over the real numbers $\mathbb{R}$.

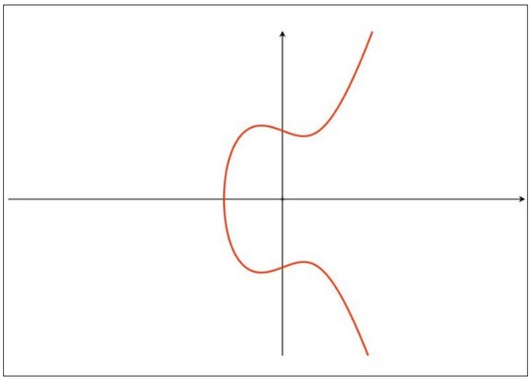

Figure 1: Graph of an Elliptic Curve

Elliptic curves have several interesting mathematical properties that make them useful in cryptography. One such property is their ability to form a group under a geometric operation called "point addition" [29]. Point addition involves drawing a line between two points on the curve and finding the third point where the line intersects the curve. The result is the reflection of this point about the x-axis.

Another important property of elliptic curves is their "discrete logarithm" problem. The discrete logarithm problem is the difficulty of computing the private key given the public key in a public-key cryptosystem. The security of elliptic curve cryptography depends on the difficulty of solving this problem [30].

Elliptic curves are used in various cryptographic applications, such as key exchange, digital signatures, and encryption [31]. The choice of elliptic curve is crucial for the security of the cryptographic system. The curve must have certain properties to be considered secure, such as a large prime order and resistance to attacks such as the "MOV attack" and the "Smart attack" [32]. Elliptic curves have become increasingly popular in cryptography due to their ability to provide the same level of security as other public-key cryptography algorithms such as RSA with shorter key lengths, which reduces the computational requirements and memory usage of cryptographic operations.

Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is a type of public key cryptography that is based on the mathematics of elliptic curves. It is a modern and efficient alternative to other public key cryptosystems, such as RSA and Diffie-Hellman, that provides the same level of security with much smaller key sizes [33].

In ECC, a user generates a public-private key pair using an elliptic curve and a point on that curve [34]. The public key is derived from the private key and can be shared with anyone. The private key, however, must be kept secret by the user. The security of the system is based on the difficulty of calculating the private key from the public key.

ECC is used in a variety of applications, including secure communication protocols, digital signatures, and encryption. It is particularly useful in environments with limited resources, such as mobile devices, as it requires fewer computational resources and smaller key sizes than other public key cryptosystems [35].

Elliptic Curve Digital Signature Algorithm (ECDSA)

The Elliptic Curve Digital Signature Algorithm (ECDSA) is a widely used public-key digital signature algorithm that is based on the mathematics of elliptic curves [36].

The algorithm consists of the following equations:

1. Key generation:

- The first step in using ECDSA is to generate a public-private key pair. This is done as follows:
- Choose an elliptic curve E over a finite field Fp, where p is a large prime number.
- Choose a base point G on the curve E, which has a large prime order n.
- Choose a random integer d, where $1 < d < n$, to be the private key.
- Calculate the public key $Q = d * G$, where $*$ denotes point multiplication on the elliptic curve.

2. Signing a message:
- Once the key pair has been generated, the user can sign a message using their private key as follows:
- Compute a hash of the message to be signed.
- Choose a random integer k, where $1 < k < n$.
- Compute the point R = $k * G$ on the curve.
- Calculate the integer $s = (h\,ash + d * x(R)) * k^{-1}\ mod\ n$, where $x(R)$ is the x-coordinate of R, and k^{-1} is the modular inverse of k modulo n.
- • The signature is the pair (R, S).

3. Verifying a signature:
- To verify a signature, the receiver of the message must have access to the sender's public key Q. The verification process is as follows:
- Compute the hash of the message.
- Calculate the integer $u_1 = h\,ash * \mathrm{s}^{-1}\ mod\ n$, and $u_2 = x(R) * s^{-1}\ mod\ \ n$.
- Compute the point $V = u_1 * G + u_2 * Q$ on the curve.
- The signature is valid if and only if $R = V$.

These equations may seem complex, but they form the backbone of the ECDSA algorithm and ensure that digital signatures are secure, efficient, and verifiable. ECDSA uses the properties of elliptic curves over finite fields to generate and verify digital signatures. The security of the algorithm depends on the choice of the elliptic curve and the parameters used in the algorithm. Therefore, it is essential to choose an appropriate curve and use secure implementations of the algorithm [37].

Implementation and Results

System Architecture

The architecture consists of the following components:

1. Educational Institution: This is the entity that issues the certificates. It interacts with the blockchain network to create a digital asset for each certificate issued.
2. Blockchain Network: This is the distributed ledger technology that stores all the digital assets as unique records on the blockchain. It provides a secure and tamper-proof way to store and verify the authenticity of certificates.
3. Certificate Verification Service: This is a web application that allows authorized parties, such as employers or other educational institutions, to verify the authenticity of a certificate. It interacts with the blockchain network to retrieve the relevant information about the certificate and displays it to the user.
4. Student Wallet: This is a digital wallet that stores all the certificates issued to a student. It provides a convenient way for the student to access and share their certificates with others.
5. Metadata Store: This is a database that stores all the metadata associated with each certificate, such as the student's name, the course completed, and the grade achieved. It is used by the educational institution to create the digital asset for each certificate and is also accessible by authorized parties through the Certificate Verification Service.

This architecture provides a secure, transparent, and efficient way to manage certificates in higher education using blockchain technology.

Implementation

Elliptic curve digital signatures (ECDSA) can be used in blockchain for the management of certificates in education. In fact, ECDSA is a commonly used algorithm for digital signatures in blockchain due to its efficiency and security. ECDSA is a type of public-key cryptography that involves the use of elliptic curves to generate a public key and a private key. The private key is used to sign the message, while the public key is used to verify the signature. ECDSA is a secure and efficient way to ensure that certificates in education are authenticated and tamper-proof.

In the context of certificate management in education, ECDSA can be used in the following way:

1. When a certificate is generated, the educational institution signs the certificate using its private key.
2. The digital signature, along with the certificate information, is added to the blockchain.
3. When a third party, such as an employer or another educational institution, requests verification of the certificate, they can retrieve the certificate information and digital signature from the blockchain.
4. The third party can use the educational institution's public key, which is also stored on the blockchain, to verify the digital signature and ensure the authenticity of the certificate.

Using ECDSA in blockchain for the management of certificates in education provides an extra layer of security, as it ensures that the certificate information is authentic and has not been tampered with. Additionally, the use of public-key cryptography ensures that only the educational institution with the corresponding private key can sign the certificate, preventing unauthorized parties from creating fake certificates.

Here's an example of how ECDSA can be implemented in blockchain for the management of certificates in education:

Assumptions:

- Each educational institution has a unique identifier (ID) that is stored on the blockchain.
- Each student has a unique ID that is also stored on the blockchain.
- Each certificate has a unique ID that is generated by the educational institution when a student graduates.

Implementation:

1. When a student graduates, the educational institution generates a unique certificate ID and adds it to the blockchain. The certificate ID is linked to the student's ID and the educational institution's ID.
2. The certificate information, such as the student's name, date of graduation, and the degree obtained, is added to the blockchain and linked to the certificate ID.
3. The educational institution signs the certificate using its private key, which is stored securely and cannot be accessed by anyone else. The signature is also added to the blockchain and linked to the certificate ID.
4. When an employer or another educational institution requests verification of a student's certificate, they can access the blockchain and retrieve the certificate information, including the certificate ID, the student's ID, and the educational institution's ID, as well as the digital signature.
5. The employer or educational institution can verify the authenticity of the certificate by using the educational institution's public key, which is also stored on the blockchain, to verify the digital signature.

Algorithm: ECDSA Implemented Using Python

```
import hashlib
import ecdsa

# Generate a new private key for the educational institution
private_key = ecdsa.SigningKey.generate()

# Convert the private key to a hex string and store it securely
private_key_hex = private_key.to_string().hex()

# Convert the hex string back to a private key object
private_key = ecdsa.SigningKey.from_string(bytes.
fromhex(private_key_hex), curve=ecdsa.SECP256k1)

# Generate a public key from the private key public_key = private_
key.get_verifying_key()

# Convert the public key to a hex string and store it on the
blockchain public_key_hex = public_key.to_string().hex()

# When a student graduates, generate a unique certificate ID
certificate_id = hashlib.sha256(b"certificate information").
hexdigest()

# Add the certificate ID, student ID, and educational institution
ID to the blockchain blockchain.add_certificate(certificate_id,
student_id, educational_institution_id)

# Generate a digital signature for the certificate using the
educational institution's private key signature = private_key.
sign(certificate_id.encode())

# Add the digital signature to the blockchain blockchain.add_
signature(certificate_id, signature)

# When a third party requests verification of a certificate, retrieve
the certificate information and digital signature from the blockchain
certificate_info = blockchain.get_certificate_info(certificate_id)
signature = blockchain.get_signature(certificate_id)

# Verify the digital signature using the educational institution's
public key public_key = ecdsa.VerifyingKey.from_string(bytes.
fromhex(public_key_hex), curve=ecdsa.SECP256k1)
is_valid = public_key.verify(signature, certificate_id.encode())

if is_valid: print ("Certificate is authentic.")
else: print ("Certificate is not authentic.")
```

This implementation uses the Python ECDSA library to generate and manage the private and public keys, as well as to generate and verify digital signatures using ECDSA. The hashlib library is used to generate a unique certificate ID using a hashing algorithm. The blockchain functions, such as add_certificate(), add_signature(), get_certificate_info(), and get_signature(), are used to store and retrieve the certificate information and digital signature from the blockchain.

Conclusion

The implementation of Elliptic Curve Digital Signatures (ECDS) in blockchain technology for managing certificates in higher education can bring significant benefits to the academic sector. By using blockchain technology, educational institutions can ensure the authenticity and immutability of student certificates, preventing fraud and forgery. ECDS can further enhance the security of these certificates, as they offer a more efficient and secure method of digital signing.

The use of ECDS in blockchain technology for certificate management provides a decentralized and tamper-proof system that can streamline the verification process. This can lead to improved efficiency and reduced administrative costs for educational institutions. Additionally, the use of blockchain technology can allow for the creation of smart contracts, which can automate the process of issuing and verifying certificates, further increasing efficiency.

In conclusion, the implementation of ECDS in blockchain technology for managing certificates in higher education can bring numerous benefits, including increased security, efficiency, and reduced administrative costs. Overall, the implementation of ECDSA in blockchain for certificate management in Higher Education is a promising solution that has the potential to revolutionize the way that certificates are managed and verified.

References

1. Gipp B, Meuschke N, Gernandt A (2015) Decentralized trusted timestamping using the crypto currency bitcoin. arXiv preprint arXiv:1502.04015.
2. Rahardja U, Hidayanto AN, Hariguna T, Aini Q (2019) Design framework on tertiary education system in Indonesia using blockchain technology. 2019 7th International Conference on Cyber and IT Service Management (CITSM) 7: 1-4.
3. Capece G, Levialdi Ghiron N, Pasquale F (2020) Blockchain technology: redefining trust for digital certificates. Sustainability 12: 8952.
4. Sarda P, Chowdhury MJM, Colman A, Kabir MA, Han J, et al. (2018) Blockchain for fraud prevention: a work-history fraud prevention system. 2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE) 1858-1863.
5. Young A, Verhulst S (2018) Creating immutable, stackable credentials through Blockchain at MIT. GOVLAB 1-10 https://blockchan.ge/blockchange-credentials.pdf.
6. Pelaitis D, Spathoulas G (2018) Developing a universal, decentralized and immutable erasmus credit transfer system on blockchain. 2018 Innovations in Intelligent Systems and Applications (INISTA) 1-6.
7. Palanivel K (2019) Blockchain architecture to higher education systems. Int J Latest Technol Eng Manag Appl Sci 8: 124-138.
8. Ahmad RW, Salah K, Jayaraman R, Yaqoob I, Ellahham S, et al. (2020) Blockchain and COVID-19 pandemic: Applications and challenges. IEEE Tech Rxiv 1-19.
9. Lopez B, García D, Alcaide A (2019) Blockchain Technology Facing Socioeconomic Challenges. Promise versus Probability. SocioEconomic Challenges 3: 13-24.
10. Moniruzzaman M, Khezr S, Yassine A, Benlamri R (2020) Blockchain for smart homes: Review of current trends and research challenges. Computers & Electrical Engineering 83: 106585.
11. Bellés-Muñoz M, Whitehat B, Baylina J, Daza V, Muñoz-Tapia JL, et al. (2021) Twisted edwards elliptic curves for zero-knowledge circuits. Mathematics 9: 3022.
12. Navamani TM (2021) A review on cryptocurrencies security. Journal of Applied Security Research 18: 1-21.
13. Zhang R, Chan WKV (2020) Evaluation of energy consumption in block-chains with proof of work and proof

of stake. Journal of Physics: Conference Series 1584: 012023.

14. Behnia S, Akhavan A, Akhshani A, Samsudin A (2013) Image Encryption based on the Jacobian Elliptic Maps, In The Journal of System and Software, Elsevier 86: 2429-2438.
15. Hewa T, Ylianttila M, Liyanage M (2020) Survey on blockchain based smart contracts: Applications, opportunities and challenges. Journal of Network and Computer Applications 177: 102857.
16. Arenas R, Fernandez P (2018) Credenceledger: a permissioned blockchain for verifiable academic credentials. 2018 IEEE international conference on engineering, technology and innovation (ICE/ITMC) 1-6.
17. Al-Malah DKAR, Aljazaery IA, Alrikabi HTS, Mutar HA (2020) Cloud Computing and its Impact on Online Education. Proceedings of the IOP Conference Series: Materials Science and Engineering, Baghdad, Iraq, 15–16 December 2020 1094: 012024.
18. Garba A, Chen Z, Guan Z, Srivastava G (2021) LightLedger: a novel blockchain-based domain certificate authentication and validation scheme. IEEE Trans Netw Sci Eng 8: 1698-1710.
19. Kutty RJ, Javed N (2021) Secure blockchain for admission processing in educational institutions. 2021 International Conference on Computer Communication and Informatics (ICCCI) 1-4.
20. Manu MR, Musthafa N, Balamurugan B, Chauhan R (2020) Blockchain components and concept. Blockchain technology and applications. 21-50.
21. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003081487-2/blockchain-components-concept-manu-namya-musthafa-balamurugan-rahul-chauhan
22. Cyran MA (2018) Blockchain as a foundation for sharing healthcare data. Blockchain in Healthcare Today 1: 1-6.
23. Aydar M, Cetin SC, Ayvaz S, Aygun B (2019) Private key encryption and recovery in blockchain. arXiv preprint arXiv:1907.04156.
24. Nawari NO, Ravindran S (2019) Blockchain technology and BIM process: review and potential applications. J Inf Technol Constr 24: 209-238.
25. Gatteschi V, Lamberti F, Demartini C, Pranteda C, Santamaría V, et al. (2018) Blockchain and smart contracts for insurance: Is the technology mature enough?. Future internet 10: 20.
26. Patrickson B (2021) What do blockchain technologies imply for digital creative industries?. Creativity and Innovation Management 30: 585-595.
27. Ahluwalia S, Mahto RV, Guerrero M (2020) Blockchain technology and startup financing: A transaction cost economics perspective. Technological Forecasting and Social Change 151: 119854.
28. Zheng Z, Xie S, Dai H, Chen X, Wang H, et al. (2017) An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress) 557-564.
29. Onuki H (2022) A primality proving using elliptic curves with complex multiplication by imaginary quadratic fields of class number three. arXiv preprint arXiv: 2211.15137.
30. Shores DM (2022) Cryptography Through the Lens of Group Theory. Electronic Theses and Dissertations 2507. 1-39
31. https://digitalcommons.georgiasouthern.edu/cgi/viewcontent.cgi?article=3731&context=etd.
32. Abdullah A, Mahalanobis A, Mallick VM (2020) A new method for solving the elliptic curve discrete logarithm problem. arXiv preprint arXiv:2005.05039.
33. Koppl M, Paulovic M, Orgon M, Pocarovsky S, Bohacik A, et al. (2021) Application of Cryptography Based on Elliptic Curves. 2021 2nd International Conference on Electronics, Communications and Information Technology (CECIT) 268-272.
34. Sedláček MV (2019) Examining and improving the security of elliptic curve cryptography https://is.muni.cz/th/vzvjz/sedlacek_rigo_thesis.pdf .
35. Ullah S, Zheng J, Din N, Hussain MT, Ullah F, et al. (2023) Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. Computer Science Review 47: 100530.
36. Soman P (2019) Lightweight Elliptical Curve Cryptography (ECC) for Data Integrity and User Authentication in Smart Transportation IoT System. Sustainable Communication Networks and Application: ICSCN 2019 39: 270.
37. Prakash YS, Narayan PH, Ramakrishna R, Sandeep GS, Ramesh VSS, et al. (2022) Digital Signatures and El Gamal Scheme Integration for Secure Data Transmission in Digital Transaction Survey. In 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) 892-898.
38. El Sobky W, Hamdy S, Mohamed MH (2021) Elliptic curve digital signature algorithm challenges and development stages. Int J Innov Technol Exploring Eng 10: 121-128.
39. Guruprakash J, Koppu S (2022) An Empirical Study to Demonstrate that EdDSA can be used as a Performance Improvement Alternative to ECDSA in Blockchain and IoT. Informatica 46: 277-290.