Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 19 No. 14 (2025) | OPEN ACCESS

https://doi.org/10.3991/ijim.v19i14.56869

SPECIAL FOCUS PAPER

ChequeGuard: A Mobile-Enabled Blockchain Framework to Mitigate Fake Cheque Scams

Asokan Vasudevan[1,2] (✉), Manonmani Thayanithi[3], Abinaya Pandiyarajan[3], N. Raja[4], Arya Kumar[5]

[1]Faculty of Business and Communications, INTI International University, Nilai, Malaysia

[2]Wekerle Business School, Budapest, Hungary

[3]Department of Computer Science and Engineering, Mepco Schlenk Engineering College, Sivakasi, Tamil Nadu, India

[4]Department of Visual Communication, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India

[5]Department of Commerce, KIIT University, Bhubaneswar, Odisha, India

asokan.vasudevan@newinti.edu.my

ABSTRACT

Fake cheque scams remain a pressing financial concern, leading to substantial monetary losses and legal challenges. The absence of real-time authentication mechanisms often results in delayed scam detection by financial institutions. This report presents a mobile-based blockchain system using wireless communication and distributed ledger technology to authenticate cheques in real-time and prevent fraud. Our system integrates Namecoin, SHA-256 hashing, and elliptic curve digital signature algorithm (ECDSA) into a secure mobile computing environment to enable accessibility and scalability. The system has two significant operational phases: cheque issue and authentication. When issued, banks retain cheque information on the blockchain using Lagrange polynomials, and aggregation is achieved rapidly. Authentication at the point of withdrawal confirms the cheque as valid by verifying blockchain-stored data, preventing reuse and forgery. This framework helps achieve financial inclusion through the enabling of ubiquitous mobile access to secure cheque authentication services, resulting in cost-effective, real-world applications. By virtue of applying mobile technology infrastructures and safe wireless networks, the solution not only enhances transaction safety but also adheres to the changing trends in adaptive digital finance and industrial applications. Mobile apps facilitate users to scan and verify and get instant fraud alerts, highly promoting accessibility, especially for rural dwellers.

KEYWORDS

blockchain, fake cheque prevention, wireless communication, mobile computing, financial inclusion, secure transactions, smart agent technologies, industrial applications, mobile security

1 INTRODUCTION

Apart from the explosive growth in mobile internet and smartphone use in India, mobile computing is at the heart of digital financial services to make payments, transfers, and fraud detection. While more people are moving online, cheques are a common mode of payment, exposing them to fraud. The most prevalent scam is

Vasudevan, A., Manonmani, T., Abinaya, P., Raja, N., Kumar, A. (2025). ChequeGuard: A Mobile-Enabled Blockchain Framework to Mitigate Fake Cheque Scams. *International Journal of Interactive Mobile Technologies (iJIM)*, 19(14), pp. 108–120. https://doi.org/10.3991/ijim.v19i14.56869

This article is a revised version of a paper presented at the Annual Conference on Innovating for Impact, held on February 19–20, 2025, at the Manipal Dubai Campus, Dubai, UAE. Article submitted 2025-04-26. Revision uploaded 2025-05-25. Final acceptance 2025-06-01.

writing spurious cheques with exaggerated amounts and then asking the victim to "refund" the "excess" money, causing enormous financial loss. Physical security features and magnetic ink character recognition (MICR) that are conventional cheque verification attributes are becoming less effective against high-tech forgery and advances in do-it-yourself cheque printing. This necessitates even more the imperative for a superior and safer solution. To meet this challenge, this research introduces ChequeGuard, a mobile-enabled, blockchain-based solution that facilitates secure, real-time cheque verification. With mobile phones and decentralised ledgers, the solution provides convenience, increases trust, and promotes financial inclusion in India's digitally evolving economy.

A typical cheque fraud case involves one selling something online being called by an impersonator who has pretended to be a real buyer. Upon agreeing on a price, the impersonator sends in a forged cheque as payment and rushes to collect the item. When the seller sees a provisional credit in the account, the seller is convinced that the transaction is genuine and goes ahead. But when the bank verifies the cheque and realises it is counterfeit, the amount credited is reversed. The goods are lost by the seller, and secondly, the bank can take the seller to court and the consequential legal implications that follow. It shows the necessity for real-time cheque validation systems to protect individuals against such fraudulent acts.

2 STATE-OF-THE-ART TECHNIQUES FOR FAKE CHEQUE DETECTION

In banking, cheque fraud is a critical issue that includes forgery, alteration, or endorsement of spurious cheques. Effective detection of such fraud is very important to prevent monetary losses and ensure the integrity of financial systems. With the progress of technology, different latest techniques have been implemented in order to improve detection of spurious cheques.

2.1 Optical character recognition (OCR)

Optical character recognition technology translates various forms of documents, i.e., scanned paper documents, PDFs, or photographs taken by a digital camera, into searchable and editable documents. OCR-based [1] cheque fraud check detection in financial documents employs deep learning methods to enhance the efficacy of identifying altered or forged text in cheques. An enhanced OCR-based system [2] for cheque fraud detection using convolutional neural networks (CNN) was developed and found robust against text alterations and forgeries in cheques. Multi-layer OCR [3] implements a multi-layered approach with additional verification layers. This technique has the capability of processing cheques in real-time, suitable for online banking applications. Processing the data with high power needs higher operational costs and is very sensitive to designs in cheques and printing quality. Advanced image processing algorithms are employed in [4] for OCR-based fake cheque detection. This technique is susceptible to sophisticated fraud techniques and requires frequent updates for better performance. The hybrid OCR and blockchain approach [5] ensures secure and tamper-proof cheque verification by providing an immutable audit trail for each cheque. This approach suffers from scalability issues for a huge volume of transactions.

2.2 Image processing techniques

Image processing techniques are used to analyse and extract features from cheque images, such as signatures, account numbers, and other relevant details. Robust feature extraction techniques with machine learning classifiers [1] effectively classify genuine and fake cheques with high detection accuracy. This method [6] employs advanced image processing algorithms to enhance the quality of the cheque image. Morphological operations are performed over the image to identify cheque alterations and forgeries. For optimal performance this technique requires high-quality images, and thus this approach is not suitable for real-time applications. In [7], hybrid image processing techniques to detect physical and digital alterations in the cheque. Need significant computing resources and expertise. Researchers [8] utilised deep learning models to extract complex patterns from cheque images. Though this technique exhibits high accuracy, the black-box nature of deep learning models makes their interpretation difficult. Feature extraction algorithms [9] utilise efficient algorithms to reduce the processing time. But this method needs ongoing monitoring and maintenance to ensure accuracy in real-time applications.

2.3 Machine learning algorithms

Machine learning models are trained on features extracted from cheques to classify them as genuine or fake. These models can learn complex patterns and improve detection accuracy over time. A comprehensive evaluation [10] of multiple machine learning algorithms was carried out with diverse cheque samples. This method demonstrates high accuracy and precision in detecting fraudulent cheques with a potential for overfitting if not properly managed. Ensemble learning-based methods [11] demonstrate improved detection rates compared to single classifiers and are effective in handling imbalanced datasets. The hybrid machine learning approach [12] combines multiple machine learning techniques to leverage their individual strengths. In this approach, extensive parameter tuning and cross-validation are required for efficient detection. Researchers [13] compare the deep learning and traditional machine learning models to demonstrate the superior performance of deep learning models in detecting complex fraud patterns. In this approach, data pre-processing and feature extraction can be time-consuming. However, implementation in real-world systems may face integration challenges.

2.4 Deep learning techniques

Deep learning models, particularly CNNs, have shown promising results in image classification tasks and are increasingly being applied to cheque fraud detection. Work done by [14] employs CNNs to detect forged signatures and altered text. This method is capable of identifying various types of cheque fraud and robust against variations in handwriting and cheque design. Deep CNN [10], [15] is utilised for automated feature extraction and classification to handle complex and subtle forgeries. Hybrid deep learning models [16] combine CNNs with recurrent neural networks (RNNs) for improved accuracy. This approach is capable of detecting both static and dynamic features in cheques. Lightweight deep learning models [17] are used for faster processing and are effective in detecting a wide range of cheque frauds in

real-time applications. These models suffer trade-offs between model complexity and processing speed.

2.5 Blockchain applications

Blockchain provides a decentralised and secure ledger, which can be used to verify the authenticity of cheques and prevent fraud. Several papers delve into specific blockchain use cases. Researchers in [18] propose a blockchain-based system to detect and prevent cheque fraud, enabling real-time authentication, scam identification, and cheque revocation while protecting customer privacy. A systematic mapping study [19] to categorise and analyse research on blockchain applications in central banking. Federated network [20] for edge surveillance cameras was introduced, which leverages blockchain technology to enforce privacy measures, manage blurring keys, and control video access. A cost-effective solution [21] was given for cross-blockchain interactions using a blockchain interoperability oracle with a threshold signature-based voting approach. Finally, a multi-signature scheme [22] was proposed for secure e-cheque issuance by joint account holders. Another group of papers focuses on the technical aspects of blockchain technology itself. Researchers [23] conduct a systematic review of decentralised consensus mechanisms, the core protocols that ensure agreement on the state of a blockchain network. Various blockchain consensus protocols [24] are analysed by evaluating their components, vulnerabilities, and performance metrics to provide insights for future protocol design. CoDAG blockchain protocol [25] utilises a directed acyclic graph (DAG) structure to improve transaction throughput, security, and efficiency. Researchers assess existing technologies and research directions related to blockchain regulation, covering areas like node tracking, consortium blockchain regulation and governance. Lastly, research initiatives are carried out to evaluate the performance of the Hyperledger Fabric blockchain framework, examining throughput, latency, and scalability metrics under varying network workloads. A system for depositing the cheques was proposed where cheques can be deposited electronically or physically via teller machines. They also proved space for professional miners to participate in the transactions. Authors take a different approach, investigating the operational pipeline and fraud kill chain of mobile gambling scams using qualitative and quantitative analysis of real-world data. This collection provides a broad overview of blockchain technology, from its applications in specific domains to the underlying technical aspects and considerations for secure implementation.

3 PROPOSED FAKE CHEQUE DETECTION APPROACH

ChequeGuard is a blockchain-based, mobile cheque fraud detection and prevention solution in real time. Being a mobile application, banks can now verify cheques in real time, saving the conventional 48-plus-hour float time. The system scans key cheque data—account number, cheque number, name of the drawer, and bank—and verifies them against an impenetrable, decentralised blockchain ledger. Using cryptographic primitives like digital signatures and hash functions, ChequeGuard ensures data integrity and tamper resistance. The approach combines the agility of mobile computing with the security of the blockchain to offer high-speed, scalable security for secure cheque authentication.

3.1 Fake cheques

A scammer can create a fake Cheque by the below two means:
Fake cheques

a) Obtaining genuine cheque details: Scammers get authentic cheque details such as the bank routing number, account number, and other details.
b) Producing the spurious cheque; Scammers utilize sophisticated graphic design software to replicate the appearance and feel of an actual cheque. They replicate the logo, watermark, fonts, and other security features of the bank so that the spurious cheque resembles a real one as closely as possible.
c) Printing the spurious cheque: Good printers and special paper are used to print the fake cheque. Spammers may even use magnetic ink to print the MICR line, the account and routing numbers of which shall be used to obtain the cheque cleared in the initial screenings.
d) Use and distribution: The fake cheque is deposited or negotiated in banks or shops. Remote deposit capture could also be used by fraudsters to deposit the cheque electronically, reducing the chances of detection even further.

Altered cheques

a) Theft of original cheques: Scammers steal blank or pre-written cheques from mailboxes, organizations, or individuals. These cheques are used as a point of departure for alteration.
b) Alteration of details: Fraudsters utilize chemical washing techniques or particular ink removers to erase the initial data on the cheque. This is referred to as cheque washing, eliminating the ink but not the paper.
c) Redrawing the cheque: After removing their own information, scammers redraw the cheque with fresh information, such as a new payee's name or changed amount. They employ special ink and pens to make it less traceable to do so.
d) Cashing or depositing the altered cheque: The forged cheque is then cashed or deposited into retailers or banks. The perpetrators can use forged IDs or have accomplices to avoid being caught along the way.

3.2 Blockchain structure

The system proposed here uses a blockchain infrastructure for securely storing customer information such as account numbers, account name holders, issuing banks and legitimate cheque numbers. In order to guarantee data authenticity and integrity, it utilises the elliptic curve digital signature algorithm (ECDSA) within a public-key infrastructure (PKI). Each bank has a distinct private-public key pair, with the private key creating a digital signature of a cryptographic hash of the contents of the block. Any change makes the signature invalid and tamper-resistant.

They are chained in chronological order, with each block including the hash of the previous one, creating an unalterable chain. Through the utilisation of secure hash functions like SHA-256, the system ensures that every block has a distinct, fixed-length fingerprint, making the system more secure and transparent in cheque validation.

3.3 CAI and CVI: The fingerprint of a cheque

Cheque authentication information (CAI) and Cheque validation information (CVI) are sophisticated data structures uniquely used for cheque verification.

Cheque authentication information. The cheques are digitally signed with the ECDSA, a cryptographic method for proof of authenticity using a pre-defined set of pre-generated public and private bank-generated keys. The digitally signed cheques are recorded on an immutable, tamper-evident blockchain ledger to record transactions chronologically and maintain transparency. Combining ECDSA with blockchain technology achieves cheque transaction security and validity as well as improved fraud protection.

Cheque validation information. This CVI is an electronic replica of your cheque, with all necessary information copied out of it. Using the same ECDSA and same private/public key pair on an ad hoc basis (as CAIs do), a crypto hash is created. The private key of the bank then "signs" said hash, creating an unbreakable seal for validating data authenticity and source. This CVI and ECDSA combination creates an additional security that verifies your cheque original and intact.

3.4 Proposed cheque guard system

The cheque validation process using blockchain technology leverages the decentralised, immutable, and transparent features of blockchain to enhance the security and efficiency of cheque transactions. Below is a detailed overview of a typical cheque authentication process.

Gathering information. The process starts by collecting the following details:

- Account number of the cheque holder
- Name of the account holder as it appears on the cheque
- Number of cheques contained within the chequebook
- Name of the issuing bank associated with the account

This information can be securely gathered via mobile banking applications integrated with the ChequeGuard system. Users can scan or input cheque data directly from their devices.

Key retrieval and signature generation. The system utilises the ECDSA to generate an exclusive digital signature for each cheque. It will obtain the account's cryptographic key pair, with the private key being used to sign the cheque data and the public key being used for verification purposes. It ensures the authenticity and integrity of each issued cheque.

Creating digital signature. With the modern age being a digital era, information integrity and authenticity are of utmost concern. Step in ECDSA, a cutting-edge approach that leverages the fascinating properties of elliptic curves to offer rugged security. ECDSA (see Algorithm 1) offers an impressive level of security with minimal key sizes, unlike other algorithms. This makes it ideal for situations where space cannot be afforded, for example, cryptocurrency transactions. Because of its minimal key size, ECDSA facilitates safe and effective digital currency transactions in the virtual world. The next time you hear ECDSA, do remember that it is more than a high-tech algorithm; it is the digital world's equivalent of an impenetrable stamp, safeguarding your data and confirming its authenticity in the ever-changing global virtual world.

Algorithm 1. Elliptic Curve Digital Signature Algorithm (Simplified)

Input:
- *M: Message to be signed*
- *(d,Qd): Private key pair, where d is the private key and Qd is the public key.*

Output:
- *(r,s): Signature of message M*

Steps:
1. *Hashing:*
   - *Compute the message digest e = H(M), where H is a cryptographic hash function.*
2. *Random number generation:*
   - *Generate a random integer k ∈ [1,n–1], where n is the order of the base point P of the chosen elliptic curve.*
3. *Signature generation:*
   - *Compute R = kP (point multi plication on the elliptic curve).*
   - *Compute s = (e+d·r)–1 (mod n) (modular inverse).*
4. *Signature:*
   - *The signature is the pair (r,s).*

Verification:
1. *Verify signature:*
   - *Given the message M, signature (r, s), and public key Qd:*
   - *Compute e = H(M).*
   - *check if 1 ≤ r ≤n–1.*
   - *Compute u = s–1 (mod n).*
   - *Compute v =(e+u·r) (mod n).*
   - *Verify if R = vP.*
2. *Validity:*
   - *If the verification step holds, the signature is valid. Otherwise, it is invalid.*

Cheque Authentication Information (CAI) generation process. The Cheque Authentication Information (CAI) generation process involves creating a secure, verifiable set of data for each cheque issued. This data is recorded on a blockchain to ensure its immutability and accessibility for authentication purposes. Below is a detailed breakdown of the CAI (Algorithm 2) generation process:

Algorithm 2. Cheque Authentication Information (CAI) Generation

Input:
- account_number: Account number associated with the Chequebook
- name: Name of the account holder
- num_cheques: Number of cheques in the chequebook
- issuing_bank _name: Name of the issuing bank
- (d,Qd): Private key pair of the issuing bank

Output: CAI: Cheque Authentication Information

Steps:
1. Data Concatenation:- Combine the input data into a single string:
   data = account number + name + cheque numbers + issuing bank name
2. Hashing:
   - Compute the hash of the data (e.g., SHA-256): hash = H(data)
3. Signature Generation (for each cheque):
   - For each cheque i (1 to num cheques):
   - Generate a unique random integer ki ∈ [1,n–1], where n is the order of the base point on the chosen elliptic curve.
   - Compute the signature for cheque i: Ri = ki · Qd si = (hash+d·Ri)–1 (mod n)
   - Combine Ri and si into a single signature: (Ri,si)
4. CAI Construction:
- Concatenate all cheque signatures into a single string separated by commas:
  CAI = (R1,s1),(R2,s2),...,(Rnum,cheques,snum cheques)
5. Return the generated CAI.

Algorithm 3. Cheque Validation Information (CVI) Generation

Input:
- cheque_data(account_number: Account number associated with theChequebook)
- name: Name of the account holder,
- num_cheques: Number of cheques in the chequebook,
- issuing_bank_name: Name of the issuing bank)
- (d,Qd): Private key pair of the issuing bank

Output: CVI: Cheque Validation Information

Steps:

1. Data Concatenation:
- Combine the cheque data into a single string: data = cheque data

2. Hashing:
- Compute the hash of the data using a cryptographic hash function (e.g., SHA-256):

hash = H(data)

3. Signature Generation:
- Generate a unique random integer $k \in [1,n-1]$, where n is the order of the base point on the chosen elliptic curve.
- Compute the signature for the cheque: $R=k\cdot Qd$ $s=(hash+d\cdot R)-1 \pmod n$

4. CVI Construction:
- Combine the signature components and cheque data into a single string: CVI = (R,s),data

5. Return
- Return the generated CVI.

Cheque validation information. Cheque validation information is an immutable data structure that ensures and authenticates the integrity of every cheque. CVI is placed in a blockchain for its immutability and verifiability. It starts by collecting basic cheque information like cheque number, amount, and payee. They are hashed to create a digital fingerprint that is unique. The bank applies its own private key to create a digital signature of hashed data for evidence of tampering. The generated CVI contains original cheque information, a hash, and a digital signature. Tampering with the cheque will be irreversible upon verification and thus be a form of easily detecting forgery, supplementing the transaction's security.

Verifying the signature. Cheque verification is initiated by a mobile app that securely connects with the blockchain network for real-time verification. The process starts by extracting the digital signature contained within the cheque and obtaining the issuing bank's public key. Employing elliptic curve cryptographic algorithms, the system checks the signature using the bank's public key. A successful match ensures that only the bank with the corresponding private key may have written the cheque. An optional blockchain verification is conducted to add further security. It consists of a search of the blockchain for a record that corresponds to the core data of the cheque (excluding the signature). Should a corresponding entry exist, it serves to add further guarantee of the authenticity of the cheque. The conclusive validation result is arrived at through the integration of the outcome of the digital signature check and, where relevant, the blockchain query. A valid signature, coupled with a verified record of the blockchain, authenticates the cheque.

ChequeGuard exploits this procedure to provide a safe, decentralised system to prevent fraud. With real-time authentication, scam detection, and cheque revocation as its features, it offers a sound solution to prevent fake cheque scams in the banking system.

Algorithm 4. Cheque Verification and Authentication

Input:
– cheque: Cheque object containing information (e.g., cheque number, amount, payee name, signature).

Output:
– valid: Boolean indicating whether the cheque is valid (true) or invalid (false).

Steps:
1. Signature Verification:
  – Extract the signature (R,s) from the cheque object- Retrieve the issuing bank's public key Q_d.
2. Hashing:
  – Compute the hash of the cheque data (excluding the signature) using a cryptographic hash function hash = H(cheque data)
3. Verification with Public Key:
  – Verify the signature using the bank's public key:
  if 1 ¡ = R ¡ = n–1 and R = vP, where:
  – n is the order of the base point on the chosen elliptic curve.
  – v = (hash+ u·R)–1 (mod n)
  – u = s–1 (mod n) then valid = true
  – else valid = false
4. Blockchain Search (Optional):
  – Optionally, search the blockchain for a record matching the cheque data (excluding the signature) if desired.
  – If the blockchain search is enabled:
  – Search the blockchain and store the search result (found).
5. Validity Determination:
  – Based on the signature verification and optional blockchain search:
  – If 'valid' is true (signature verified):
  – If 'found' is true (cheque data found in blockchain):
  – valid = true (confirmed valid cheque)
  – Else:- valid = false (potential issue, cheque not found on blockchain)
  – Else:- valid = false (invalid signature, potential fake cheque)
6. Return the value

As the threat posed by cheque scams continues to expand, adopting innovative solutions such as ChequeGuard becomes a necessity in building trust and reliability in cheque processing activities in general. Overall, ChequeGuard is a shining example of technological innovation in the battle against financial fraud, providing a strong and dependable instrument for cheque transaction protection. With this decentralised blockchain alternative, banking industry players can strengthen their defences against counterfeited cheque scams and protect the customers' trust in the cheque processing system.

3.5 Mobile integration and user interface

The ChequeGuard system is designed to be accessible through mobile banking applications or dedicated mobile apps. Key features include:

- Cheque scanning via camera
- QR-code-based verification
- Instant alerts on cheque validation status
- Secure login with biometric or 2FA

These features provide a seamless user experience while ensuring high levels of security and data integrity.

4 RESULTS AND DISCUSSION

4.1 Namecoin implementation

Cheque authentication information is stored in the system using Namecoin blockchain [18]. The Cheque authentication process implies exploring the blockchain for the block containing the relevant cheque authentication information.

Here's a breakdown of the implementation using Namecoin:

Data storage. The system stores CAI information on the Namecoin blockchain. This allows for a distributed and tamper-proof record of issued certificates.

Search method. The authentication process searches the blockchain for the block containing the CAI associated with the cheque being verified. This involves iterating through blocks, potentially starting from the last block, and working backwards.

Search cost. As blockchain length increases, search operations can become time-consuming. This challenge is acknowledged in existing research, which suggests that optimised search algorithms can significantly enhance performance in banking applications. Although the current prototype developed in Python may not offer peak efficiency, real-world deployments are expected to utilise high-performance infrastructure with targeted optimisations. To evaluate system efficiency, the average time for cheque authentication, including retrieval of CAI, was measured over 100 test cases. Various CAI positions within the blockchain were considered. The results showed consistent performance across scenarios, indicating the system's practicality for real-time cheque validation.

Best case (CAI at blockchain end). The best-case time of search is 0.30 seconds on average with a standard deviation of 0.15 seconds. This is because the search starts from the latest block and progresses backward, making it faster to find recently added information.

Middle of blockchain. 420.84 seconds on average with a standard deviation of 20.03 seconds. Searching through a significant portion of the blockchain takes more time.

Beginning of blockchain. 1469.68 seconds on average with a standard deviation of 80.40 seconds. This scenario requires searching the entire blockchain, leading to the longest average time.

CAI not found. 1476.21 seconds on average with a standard deviation of 75.50 seconds. Interestingly, the time to determine a missing CAI is very similar to searching the entire blockchain.

4.2 Hyperledger implementation

The system uses the Hyperledger blockchain to store CAI information. The Cheque authentication process involves searching the blockchain for the block containing the relevant CAI. Here's a breakdown of the implementation using Hyperledger:

Data storage. Similar to Namecoin, stores CAI information on the blockchain.

Search method. Leverages a state database (CouchDB) for optimized searching within the blockchain.

Search cost. The system demonstrates significantly faster search times compared to Namecoin, with all results obtained within milliseconds. The average authentication time ranges from 752.31 ms (when the CAI is not found) to 766.06 ms in the worst-case scenario, showing minimal variation across different conditions.

4.3 Our implementation

Search method. Both Ethereum and Namecoin require linear searches through blockchain records, which can be time-intensive for older entries. However, Ethereum supports smart contracts—programmable logic that may enable more efficient search mechanisms, offering a flexibility not available in Namecoin.

Performance. While performance is configuration-dependent, Ethereum generally offers faster transaction processing than Namecoin. This results in quicker addition of CAIs to the blockchain, thereby enhancing search efficiency and responsiveness.

Gas fees. Previous research [18] identified high gas fees during revalidation as a major limitation. In contrast, the proposed system incorporates optimisations that significantly reduce gas fees, thereby improving cost-efficiency and increasing practical viability.

Computation overhead. Block revalidation introduces notable computational overhead. The proposed approach eliminates the need for such revalidation, thereby improving system efficiency, reducing latency, and enhancing overall reliability.

5 CONCLUSION

ChequeGuard is a distributed blockchain solution designed to combat the new threat of forged cheque frauds. Using the transparency and irreversibility of blockchain, the system provides an authentic cheque verification, real-time scam detection, and cheque recall. All these together form a robust, fraud-free cheque processing framework. Deploying ChequeGuard in banking and financial institutions enhances security measures, protects customers from losing money, and establishes the integrity of cheques. Mobile app integration ensures convenience and accessibility, and smartphones become valuable tools for fraud discovery in urban as well as rural India. Additionally, ChequeGuard enhances system efficiency by eliminating gas fee problems and computation overhead. With more sophisticated methods of cheque fraud, adopting new technologies like ChequeGuard is essential in maintaining trust, enhancing the credibility of operations, and promoting secure financial transactions.

6 REFERENCES

[1] P. Agrawal, D. Chaudhary, V. Madaan, A. Zabrovskiy, and A. Tyagi, "Automated bank cheque verification using image processing and deep learning methods," *Multimedia Tools and Applications*, vol. 80, no. 3, pp. 5319–5350, 2021. https://doi.org/10.1007/s11042-020-09818-1

[2] S. G. Vidhya, C. Balarengadurai, and B. R. Prasad, "Enhancing cheque security: Forgery detection via signature recognition using optical character recognition and deep learning," in *Proceedings of the 2024 International Conference on Recent Advances in Science and Engineering Technology (ICRASET),* B G Nagara, Mandya, India, 2024, pp. 1–6. https://doi.org/10.1109/ICRASET63057.2024.10895001

[3] S. Srivastava, J. Priyadarshini, S. Gopal, S. Gupta, and H. S. Dayal, "Optical character recognition on bank cheques using 2D convolution neural network," in *Applications of Artificial Intelligence Techniques in Engineering*, in Advances in Intelligent Systems and Computing, H. Malik, S. Srivastava, Y. Sood, and A. Ahmad, Eds., Springer, Singapore vol. 697, 2019, pp. 589–596. https://doi.org/10.1007/978-981-13-1822-1_55

[4] D. Tuteja, R. Dhand, M. Reineu, J. Israni, D. Singh, and K. Dhal, "Automated signature verification in bank cheque processing using Siamese and convolutional neural networks," in *Proceedings of the 2024 First International Conference on Electronics, Communication and Signal Processing (ICECSP),* New Delhi, India, 2024, pp. 1–6. https://doi.org/10.1109/ICECSP61809.2024.10698370

[5] Y. Zhang, H. Liu, and X. Wang, "Application of artificial intelligence image recognition and blockchain technology in enhancing the security of cross-border financial transactions," *IIETA Transactions on Systems, Cybernetics and Security*, vol. 7, no. 4, pp. 221–228, 2022. https://doi.org/10.18280/tscs.070408

[6] S. P. Raghavendra, S. Ahamed, A. Danti, and D. Rohit, "Detection of fraudulent alteration of bank cheques using image processing techniques," in *Recent Trends in Image Processing and Pattern Recognition (RTIP2R 2020), Communications in Computer and Information Science*, K. C. Santosh and B. Gawali, Eds., Springer, Singapore, vol. 1380, 2021, pp. 469–477. https://doi.org/10.1007/978-981-16-0507-9_39

[7] S. S. Gonge, "Combination of neural network and advanced encryption and decryption technique is used for digital image watermarking," *Journal of Intelligent & Fuzzy Systems,* vol. 38, no. 5, pp. 6465–6474, 2020. https://doi.org/10.3233/JIFS-179727

[8] P. Senthil and S. Selvakumar, "A hybrid deep learning technique based integrated multimodel data fusion for forensic investigation," *Journal of Intelligent & Fuzzy Systems*, vol. 43, no. 5, pp. 6849–6862, 2022. https://doi:10.3233/JIFS-221307

[9] M. Ashwin Shenoy, S. Suvarna, and K. T. Rajgopal, "Online digital cheque signature verification using deep learning approach," in *Proceedings of the 2023 2nd International Conference on Edge Computing and Applications (ICECAA)*, Namakkal, India, 2023, pp. 866–871. https://doi.org/10.1109/ICECAA58104.2023.10212410

[10] R. Jayadevan, S. R. Kolhe, P. M. Patil, and U. Pal, "Automatic processing of handwritten bank cheque images: A survey," *International Journal on Document Analysis and Recognition (IJDAR)*, vol. 15, no. 4, pp. 267–296, 2012. https://doi.org/10.1007/s10032-011-0169-2

[11] A. A. Barbhuiya, A. K. Das, and S. Dey, "Predicting financial manipulation using an ensemble-based approach," *Vision The Journal of Business Perspective*, 2024. https://doi.org/10.1177/09722629241255833

[12] O. M. Aydın and R. Aktaş, "Detecting financial information manipulation by using supervised machine learning technics: SVM, PNN, KNN, DT," *Uluslararası İktisadi ve İdari İncelemeler Dergisi,* vol. 29, pp. 165–174, 2020. https://doi.org/10.18092/ulikidince.748742

[13] P. Uyyala and D. D. C. Yadav, "The advanced proprietary AI/ML solution as AntifraudTensorlink4cheque (AFTL4C) for Cheque fraud detection," *The International Journal of Analytical and Experimental Modal Analysis*, vol. 15, no. 4, pp. 1914–1921, 2023. https://doi.org/10.17613/v18z-ff84

[14] M. Ashwin Shenoy, S. Suvarna, and K. T. Rajgopal, "Online digital cheque signature verification using deep learning approach," in *Proceedings of the 2023 2nd International Conference on Edge Computing and Applications (ICECAA)*, Namakkal, India, 2023, pp. 866–871. https://doi.org/10.1109/ICECAA58104.2023.10212410

[15] S. G. Vidhya, C. Balarengadurai, and B. R. Prasad, "Enhancing cheque security: Forgery detection via signature recognition using optical character recognition and deep learning," in *Proceedings of the 2024 International Conference on Recent Advances in Science and Engineering Technology (ICRASET)*, B G Nagara, Mandya, India, 2024, pp. 1–6. https://doi.org/10.1109/ICRASET63057.2024.10895001

[16] M. Ashwin Shenoy, S. Suvarna, and K. T. Rajgopal, "Online digital cheque signature verification using deep learning approach," in *Proceedings of the 2023 2nd International Conference on Edge Computing and Applications (ICECAA)*, Namakkal, India, 2023, pp. 866–871. https://doi.org/10.1109/ICECAA58104.2023.10212410

[17] K. Ladrham and H. Gueddah, "Advanced OCR for digits: Exploring CNN for optimal performance," *Procedia Computer Science*, vol. 251, pp. 734–739, 2024. https://doi.org/10.1016/j.procs.2024.11.177

[18] B. Hammi, S. Zeadally, Y. C. E. Adja, M. D. Giudice, and J. Nebhen, "Blockchain-based solution for detecting and preventing fake check scams," *IEEE Transactions on Engineering Management*, vol. 69, no. 6, pp. 3710–3725, 2022. https://doi.org/10.1109/TEM.2021.3087112

[19] N. Dashkevich, S. Counsell, and G. Destefanis, "Blockchain application for central banks: A systematic mapping study," *IEEE Access*, vol. 8, pp. 139918–139952, 2020. https://doi.org/10.1109/ACCESS.2020.3012295

[20] A. Fitwi, Y. Chen, and S. Zhu, "A lightweight blockchain-based privacy protection for smart surveillance at the edge," in *2019 IEEE International Conference on Blockchain (Blockchain)*, Atlanta, GA, USA, 2019, pp. 552–555. https://doi.org/10.1109/Blockchain.2019.00080

[21] M. Sober, G. Scaffino, C. Spanring, and S. Schulte, "A voting-based blockchain interoperability oracle," in *2021 IEEE International Conference on Blockchain (Blockchain)*, Melbourne, Australia, 2021, pp. 160–169. https://doi.org/10.1109/Blockchain53845.2021.00030

[22] N. R. Sunitha, B. B. Amberker, and P. Koulgi, "Secure e-cheques for joint accounts with collective signing using forward-secure multi-signature scheme," in *Seventh IEEE/ACIS International Conference on Computer and Information Science (ICIS 2008)*, Portland, OR, USA, 2008, pp. 241–246. https://doi.org/10.1109/ICIS.2008.41

[23] W. Wang *et al.*, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019. https://doi.org/10.1c109/ACCESS.2019.2896108

[24] Y. Xiao, N. Zhang, W. Lou, and Y. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020. https://doi.org/10.1109/COMST.2020.2969706

[25] S. Yang, Z. Chen, L. Cui, M. Xu, Z. Ming, and K. Xu, "CoDAG: An efficient and compacted DAG-based blockchain protocol," in *2019 IEEE International Conference on Blockchain (Blockchain)*, Atlanta, GA, USA, 2019, pp. 314–318. https://doi.org/10.1109/Blockchain.2019.00049

7 AUTHORS

Asokan Vasudevan is a Professor at the Faculty of Business and Communications, INTI International University, Nilai, Negeri Sembilan, Malaysia. He also serves as a Research Fellow at Wekerle Business School, Budapest, Jázmin u. 10, 1083 Hungary (E-mail: asokan.vasudevan@newinti.edu.my).

Manonmani Thayanithi is a Senior Assistant Professor at the Department of Computer Science and Engineering, Mepco Schlenk Engineering College, Sivakasi, Tamil Nadu, India (E-mail: manonmani@mepcoeng.ac.in).

Abinaya Pandiyarajan is a Senior Assistant Professor at the Department of Computer Science and Engineering, Mepco Schlenk Engineering College, Sivakasi, Tamil Nadu, India (E-mail: abinayap@mepcoeng.ac.in).

Dr. N. Raja is an Assistant Professor at the Department of Visual Communication, Sathyabama Institute of science and Technology, Chennai, Tamil Nadu, India (E-mail: rajadigimedia2@gmail.com).

Dr. Arya Kumar is an Assistant Professor (II) at the Department of Commerce, KIIT University, Patia, Bhubaneswar – 751 024, Odisha, India (E-mail: arya.kumarfcm@kiit.ac.in).