Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Preventing Digital Arrests with Blockchain Technology: A Delegate-Driven Approach

Anjana Rani[1], Monika Saxena[2]

[1]Research Scholar, Department of Computer Science, Banasthali Vidyapith, Banasthali, Newai, Rajasthan, India, anjanarani2814@gmail.com
[2]Professor, Department of Computer Science, Banasthali Vidyapith, Banasthali, Newai, Rajasthan, India, smonika@banasthali.in

A blockchain-based solution to address the challenges such as digital arrest, censorship, and tampering is presented in this study. Fundamental blockchain principles influenced this approach top ensure the integrity of the transactions and to detect fraud, utilizing robust tools for identifying censorship as well as tampering. A key feature of this paper is the process of block generation involving generation. Legal block is assigned by using these delegates in a sequential manner, just by copying the steps of the consensus process to ensure consistency and accuracy. To evaluate the proposed solution, derived a synthetic dataset from the actual data of transaction with some anomalies is used. To detect and ensure the overall validity of the blockchain, the blockchain integrity tests are deployed in this paper. The findings demonstrate that the proposed model successfully mitigates the impact of digital arrest while preserving the reliability as well as security of the system. This research also highlights the potential of blockchain technology to enhance transaction security and integrity, offering a practical method for detecting and countering the manipulations digitally.

CCS CONCEPTS • Network security • Cryptography

Keywords: Blockchain, Digital arrest, Synthetic Dataset, Delegate-Driven approach, Integrity.

1. Introduction

In the digital age, the term “digital arrest” refers to the hidden or altered online information and transactions that threaten the validity as well as reliability of the digital world, especially in blockchain networks. Blockchain is the type of technology which is very well known for its decentralization and immutability, so it is becoming even more obvious that the information integrity threats have the power to inhibit or modify the transactions.

For example, the fundamental principles of the Interplanetary File systems which is known as a decentralized storage solution is frequently utilized in thew applications of blockchain, which can be easily compromised by the content-censorship attacks as shown by the Sridhar et al. (2023) [1]. Furthermore, new regulations are placed over blockchain apps following new fines against certain platforms like Tornado, which results in the purposeful exclusion of one

or more transactions from one or more blocks to demonstrate compliance with the law; the soundness of this action raises questions about the capture of the resistant nature of the blockchain systems with regards to the impartiality and inclusivity [2].

1.1 Problem Statement

Despite the inherent advantages associated with blockchain technology, several challenges persist regarding the safeguarding of transaction integrity and the detection of manipulative activities in digital environment:

- Censorship Vulnerabilities: recent research indicates that a significant proportion of blockchain participants, including miners and validators, have engaged in the censorship of transactions to comply with legal obligations. This practice poses a risk to the neutrality of the network [2].
- Risks of Data Tampering: while blockchains Are designed to be immutable, certain attack techniques, specifically those exploiting the Distributed hash Table (DHT) utilized by IPFS, can result in covert alterations of stored data [1].
- Limitations of Consensus Mechanisms: the delayed integration of censored transactions in PoS systems indicates that conventional consensus protocols, including PoW and PoS, may not possess robust mechanisms to effectively prevent or address instances of censorship and data tampering [2].
- Insufficient Corrective Measures: the existing blockchain architecture remain vulnerable to persistent threats, as they often lack effective strategies for detecting and rectifying anomalies [3].

The above issues stronger protections against digital arrest, which are very much essential for maintaining the security, neutrality, and also reliability of blockchain networks.

1.2 Objectives\

This paper suggests a delegate-driven blockchain architecture to lessen the threats related to digital arrest. With this method, a rotating assembly delegate is given the task to create blocks. The following are some of the predicted advantages of the method used in this paper:

Increased Censorship Resistance: the possibility of coordinated attempts to suppress information (SSRN) is reduced when block creation is divided among several delegates [4].

Enhancement of Tampering Detection: the delegate framework's strict validation rules enable the system to detect as well as fix the tampered transactions early [5].

Enhanced Consensus Integrity: the delegate-driven paradigm seeks to overcome the drawbacks of conventional consensus processes by implementing protections against censorship and manipulation [3]

The study's goal is to aid in the creation of more robust blockchain syatems that can handle the difficulties presented by the digital arrest. This will be accomplished by evaluating the suggested framework on a synthetic dataset that mimics abnormalities found in the real world.

2 RELATED WORK

Because of the decentralized as well as unchangeable ledger systems, blockchain technology has become a powerful force in offering platforms which are censorship resistant. Tithonus is a good example, as it successfully hides the client requests in regular Bitcoin Transactions [5]. This is accomplished by using a peer-to-peer network and bitcoin blockchain to enable safe interactions. Additionally, by including censored letters into transactions, public blockchains like Ethereum have shown that they can counteract information censorship while guaranteeing that these records are immutable and publicly available [6].

Even with technological improvements, current blockchain systems still have trouble detecting and stopping censorship and manipulation. According to new research that looks at the problem of blockchain transaction censorship, fine-grained censorship may result in worse security for centralized transaction propagation services and block validators. Denial of Service (DoS) attacks may result from this vulnerability [3]. Furthermore, due to their basic design, some blockchain protocols could unintentionally permit transaction delays, endangering the system's security and fairness [2].

3 METHODOLOGY

3.1 Blockchain System Design

3.1.1 Delegate-Driven Block Creation Process.

The blockchain system's delegate-driven block building procedure guarantees fair participation and effective processing. According to this technique, a certain set of delegates is in charge of adding and validating blocks in a sequential manner. The delegate for each block is chosen using a round-robin scheduling method, as shown in Figure 1 below:

```
'delegate': self.delegates[(len(self.chain) % len(self.delegates))],
```

Figure 1: Delegate-Driven Block Creation

3.1.2 Utilization of Hash Functions

The process of adding pending transactions to the blockchain is done methodically. These transactions are first recorded in a temporary pool. The inclusion of pending transactions in the newly created block ensures their security. Each block is constructed with specific components to uphold the integrity of the blockchain:

- The hash of the preceding block: this element preserves chronological order and facilitates the connection between blocks.
- Transaction information: this encompasses data related to the sender, recipient, monetary value, and other indicators of potential censorship or tampering.
- Delegate Details: this specifies the delegate responsible for creating the block.

The integrity of each block is ensured through the application of a SHA-256 hash function, which safeguards against unauthorized alterations by converting the contents of the block into a unique hash value [8] [9] and this hash function is shown below in Figure 2:

```
block = chain[block_index]
if block['previous_hash'] != self.hash(previous_block):
    return False
```

Figure 2: Hash Function

3.2 Digital Arrest Mechanism

3.2.1 Detection of Censorship or Tampering in Transactions

The blockchain system incorporates mechanisms to detect potential digital alterations, such as tampering or censorship. The process of block validation relies on a structured analysis of transaction attributes to identify those transactions that are flagged as having been censored or altered as shown in Figure 3.

```
tampered_transactions = []
for block in self.chain:
    for transaction in block['transactions']:
        if transaction['is_censored'] or transaction['tampered']:
            tampered_transactions.append(transaction)
```

Figure 3: Detection of Tampered/Censored Data

In the event that such transactions are detected, a notification is issued, and these irregularities are documented for subsequent intervention [10].

3.2.2 Techniques to Fix Chain Problems and Separate Affected Transactions

Blockchain technology makes it easier to isolate transactions that are prohibited or changed from the chain, preventing unwanted changes. The maintenance of the blockchain's general validity is guaranteed by the remedial procedure depicted in Figure 4. The impacted transactions are removed during the chain's revalidation process, which preserves integrity.

```
for block in self.chain:
    valid_transactions = []
    for transaction in block['transactions']:
        if transaction['is_censored'] or transaction['tampered']:
            print("Tampered transaction removed:", transaction)
        else:
            valid_transactions.append(transaction)
    block['transactions'] = valid_transactions
```

Figure 4: Correction Process

Subsequent to the correction process, the blockchain is subjected to further testing to verify its reliability [10] [11].

3.3 Integration With Synthetic Dataset

In order to assess the system's performance, a synthetic dataset was created to mimic actual transaction data. The following components are included in this dataset:

- Unique IDs of the transactions
- Timestamps that fall within a reasonable timeframe

- Wallet addresses for both senders and recipients
- Transaction amounts
- Status flags indicating whether the transaction was successful, pending, or failed.
- Flags for censorship and tampering

3.3.1 Insertion of Abnormalities for Testing Purpose

Certain anomalies were purposefully added to the dataset in order to evaluate the system's capacity to identify and handle digital arrests. For example:

- The label "is_censored = True" was assigned to a designated subset of transactions.
- In addition, the flag indicating altered transactions was set to True for a different group of transactions.

A synthetic dataset comprising 1,000 transactions was subsequently saved in CSV format and integrated into the blockchain for testing purposes. Each transaction was methodically added to the blockchain, resulting in the consecutive production of blocks, in order to guarantee the inclusion of the anomalies [7] [11]. The following Python code was used to create the dataset:

data = generate_blockchain_data()

4 IMPLEMENTATION

The class architecture used in the proposed blockchain system was created in Python and includes all the capabilities required to enable a delegate-driven blockchain approach that aims to stop digital arrests. The following lists the main elements along with explanations of each:

4.1 Blockchain Class

Block Generation: The create_block function is used to incorporate new blocks into the blockchain. A timestamp, a set of transactions, the hash value of the previous block, and the delegate in charge of creating it are among the elements that make up each block. To replicate elements of a delegation-based consensus process, delegates are assigned in a round-robin fashion.

Transaction Incorporation: By taking the sender and recipient addresses, the transaction amount, the censorship status, and any flags suggesting tampering, the add_transaction method makes it easier to add transactions. Before being included into a block, transactions are first put into a pending pool.

Integrity Verification: To protect the integrity of the blockchain, the is_chain_valid function uses hash functions to determine the relationship between blocks and to identify any discrepancies that could result from illegal changes.

4.2 Identification And Management of Digital Arrest

The blockchain is thoroughly examined by the check_digital_arrest function to find any transactions that would point to censorship or manipulation.

Concurrently, the handle_digital_arrest function eliminates any invalid transactions while guaranteeing that valid ones maintain their integrity. This procedural change guarantees the blockchain's continued dependability.

4.3 Visualization

The blockchain is thoroughly examined by the check_digital_arrest function to find any transactions that would point to censorship or manipulation.

Concurrently, the handle_digital_arrest function eliminates any invalid transactions while guaranteeing that valid ones maintain their integrity. This procedural change guarantees the blockchain's continued dependability.

4.4 Security Protocols

Blockchain data is securely saved via data encryption, which is supported by the cryptography library. To do this, the system uses an existing cryptographic key or produces a new one as needed.

4.5 Dataset Generation

To test the system's performance, a synthetic dataset that properly represents genuine blockchain transactions was created. This approach was implemented using Python code to build a dataset with various components:

• Randomized wallet addresses represent a varied spectrum of users.

• Transaction metadata includes timestamps, sender and recipient addresses, quantities, transaction status (successful, pending, or failed), and evidence of censorship or manipulation.

4.5.1 Dataset Structure

The dataset comprises key columns, each serving a specific purpose:

- transaction_id: this column contains a unique identifier assigned to each transaction.
- timestamp: this indicates the time at which the transaction was created.
- from_address: this column represents the wallet address from which the transaction originates.
- to_address: this column represents the wallet address to which the transaction is directed.
- amount: this defines the monetary value of the transaction.
- status: this indicates the outcome of the transaction, categorizing it as successful, pending, or unsuccessful.
- is_censored: this Boolean flag indicates whether the transcation has been subjected to censorship.
- tampered: this Boolean flag signifies whether there has been any undetected tampering with the transaction.

Below is an example of the code utilized for the dataset generation;

5 EXPERIMENTAL EVALUATION

5.1 Setup

The experimental review aimed to determine the effectiveness of the proposed delegate-driven blockchain system in preventing digital arrests, such as censorship or manipulation. The experimental setup was implemented in a Python-based development environment.

- Hardware: includes a 512GB SSD, 16GB RAM, and an Intel Core i7 processor.
- Software: Python 3.13 with cryptography, Matplotlib, NetworkX, and Pandas packages.

The synthetic dataset, consisting of 1,000 records meant to simulate genuine blockchain transactions, included a variety of data points such as transaction IDs, timestamps, sender and recipient wallet addresses, transaction amounts, and flags indicating instances of censorship and manipulation. The synthetic dataset, which is detailed in the file name synthetic_blockchain_data.csv, has 50 distinct wallets. Anomalies, such as filtered and edited transactions, were put into the dataset for testing. This simulated dataset was linked into the blockchain application, and a delegate-driven mechanism was used to create blocks whenever a transaction was uploaded to the blockchain. To ensure the blockchain's integrity, transactions that were recognized as censored or changed were subjected to a number of detection and repair procedures.

5.2 Performance Metrics

5.2.1 Outcomes of the chain integrity validation

A hashing-based approach was used to check the blockchain's integrity and verify that the blocks were properly linked. To provide a safe chain structure, each block contains the hash of its predecessor. The results of the validation testing showed the following:

- The original chain was confirmed to be legitimate, as there were no interruptions in the hash linkages between the blocks.
- Alerts were generated, and transactions suspected have been filtered or altered and separated for corrective action.

5.2.2 Identification and rectification of tampered data

The identification of signs indicating censorship or tampering in blockchain transactions has enabled the successful detection of compromised digital records. The following anomalies were identified:

- Transactions exhibiting censorship are marked by is_censored = True
- Transactions that have undergone tampering are denoted as Tampered = True.

The transactions flagged in this manner were subsequently removed from the blockchain using the rectification mechanism, thereby ensuring the operational integrity of the system.

Following the resolution of all identified issues, a post-correction validation was conducted to confirm the ongoing validity of the blockchain.

5.3 Results

5.3.1 Comparison of Blockchain Performance

The performance of the blockchain exhibited improvements in both efficiency and fairness due to the implementation of a delegate-driven method for block creation.

- DELEGATE-DRIVEN MECHANISM: the allocation of blocks to delegates in a round-robin manner significantly mitigated risk associated with centralization. This approach ensured a fair distribution of responsibilities in the block creation process.
- WITHOUT DELEGATE-DRIVEN MECHANISM: the analysis indicated a tendency towards potential centralization and inefficiencies, as some nodes maintained disproportionate control over the block creation process.

5.3.2 VISUALIZATION OF BLOCKCHAIN STRUCTURE AND TRANSACTION FLOW

The structure of the blockchain and specific transaction details were illustrated through the use of directed graphs. This framework highlighted the following elements:

- The interrelationships between components, timestamps associated with transactions, indices of blocks, and the delegates assigned to each block.
- The transaction details within each block were categorized according to flagged and regular status.

Furthermore, the transaction logs and accompanying graphs provided evidence of the effective implementation of the blockchain systems, as well as its robustness in detecting and rectifying discrepancies.

6 CONCLUSION

This study describes a delegate-driven blockchain architecture that addresses the major concerns related with digital arrest, such as transaction manipulation and censorship. The proposed architecture includes a delegate-based block production technique, a strong system for detecting censorship and manipulation, and a rectification mechanism designed to restore the blockchain's integrity. A synthetic dataset was used to conduct performance assessments, which allowed for a full examination of the system's functions. This dataset was created intended to simulate real-world transaction settings while also introducing numerous abnormalities.

The results show that the suggested technique is successful at preventing digital arrests while retaining the dependability and integrity of blockchain transactions. Furthermore, testing with the synthetic dataset confirmed the system's capacity to detect abnormalities, isolate corrupted transactions, and repair the blockchain to maintain its integrity.

To improve the efficiency and integrity of the block formation process, future research will look into the use of artificial intelligence-driven delegate selection techniques. Furthermore,

efforts will be made to improve the model's resilience for practical applications and broaden its applicability to bigger datasets. These developments are intended to strengthen the system's defences against digital arrest and to increase public trust in blockchain technology.

References

1)Sridhar, S., Ascigil, O., Keizer, N., Genon, F., Pierre, S., Psaras, Y., ... & Król, M. (2023). Content censorship in the interplanetary file system. arXiv preprint arXiv:2307.12212.

2)Wahrstätter, A., Ernstberger, J., Yaish, A., Zhou, L., Qin, K., Tsuchiya, T., ... & Gervais, A. (2024, May). Blockchain censorship. In Proceedings of the ACM on Web Conference 2024 (pp. 1632-1643).

3)Wang, Z., Xiong, X., & Knottenbelt, W. J. (2023, July). Blockchain transaction censorship:(in) secure and (in) efficient?. In The International Conference on Mathematical Research for Blockchain Economy (pp. 78-94). Cham: Springer Nature Switzerland.

4)Khazzaka, M. (2024). Bitcoin: Censorship Resistance Against Hash Dominance. Available at SSRN 4803116.

5)Recabarren, R., & Carbunar, B. (2018). Tithonus: A bitcoin based censorship resilient system. arXiv preprint arXiv:1810.00279.

6)Rocco, G. (2019). Public Blockchains as a Means to Resist Information Censorship.

7)Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International journal of web and grid services, 14(4), 352-375.\

8)Mühlberger, R., Bachhofner, S., Castelló Ferrer, E., Di Ciccio, C., Weber, I., Wöhrer, M., & Zdun, U. (2020). Foundational oracle patterns: Connecting blockchain to the off-chain world. In Business Process Management: Blockchain and Robotic Process Automation Forum: BPM 2020 Blockchain and RPA Forum, Seville, Spain, September 13–18, 2020, Proceedings 18 (pp. 35-51). Springer International Publishing.

9)Rehman, M., Javaid, N., Awais, M., Imran, M., & Naseer, N. (2019, December). Cloud based secure service providing for IoTs using blockchain. In 2019 IEEE Global Communications Conference (GLOBECOM) (pp. 1-7). IEEE.

10)Hassan, M. U., Rehmani, M. H., & Chen, J. (2022). Anomaly detection in blockchain networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 25(1), 289-318.

11)Daghmehchi Firoozjaei, M., Ghorbani, A., Kim, H., & Song, J. (2020). Hy-Bridge: A hybrid blockchain for privacy-preserving and trustful energy transactions in Internet-of-Things platforms. Sensors, 20(3), 928.