MEST Journal
DOI 10.12709/mest.13.13.01.06

FORENSIC ANALYSIS OF PRIVATE BLOCKCHAINS IN THE PUBLIC SECTOR: CHALLENGES, TECHNIQUES, AND FUTURE

Milan Feltovic
University of Žilina, Faculty of Security Engineering, Žilina, Slovakia
https://orcid.org/0009-0004-3057-2912

JEL Category: **C88**

Abstract

This article explores the forensic analysis of private blockchains in the public sector, focusing on identifying challenges, describing techniques, and predicting future trends. Unlike public blockchains, private blockchains provide a higher level of access control and data protection, making them attractive for various public applications such as digital land registries, citizen identity management systems, supply chain tracking, and healthcare record management. Forensic analysis of private blockchains is a specialized discipline that combines traditional digital forensic principles with a deep understanding of blockchain technology and cryptography. The main components of this discipline are the identification, collection, preservation, analysis, and presentation of evidence. The article also examines specific aspects such as the analysis of cryptographic evidence, the examination of block structures, and data integrity verification. The importance of forensic analysis of private blockchains grows with their increasing use in the public sector. This article highlights the need for specialized tools and methodologies development, continuous education of forensic experts, and international cooperation in standardization and knowledge exchange. Future trends include the integration of artificial intelligence, the improvement of methods for preserving evidence integrity, and addressing legal and ethical challenges associated with forensic analysis in an international context. The goal of this article is to provide a comprehensive overview of the forensic analysis of private blockchains and to emphasize its key role in ensuring the integrity, transparency, and trustworthiness of digital systems in the public sector.

Keywords: *Private blockchains, digital forensics, cryptography, smart contracts, data security, identity management, transaction analysis, artificial intelligence.*

1 INTRODUCTION

Blockchain technology has become a significant element of digital transformation adopted by organizations worldwide in recent years. Public blockchains, such as Bitcoin and Ethereum, are widely known for their openness and transparency

Address of the author:
Milan Feltovic
milan@feltovic.com

(Nakamoto, 2009). On the other hand, private blockchains are gaining increasing attention, particularly in the public sector, where their closed systems provide higher levels of access control and data protection (Anon, 2023).
Although private blockchains offer significant advantages in enhanced security and privacy protection, their complex structure and closed nature pose challenges for forensic analysis. With the growing deployment of private blockchains in the public sector, such as in healthcare records and identification systems, there is an increasing need for effective forensic methods to ensure their integrity and trustworthiness.

Forensic analysis of private blockchains is a specialized area of digital forensics that deals with investigating and analyzing data in these closed networks. It aims to ensure the integrity and trustworthiness of systems, identify potential security issues, and provide evidence for legal and administrative purposes. This article focuses on the challenges, techniques, and future of forensic analysis of private blockchains, providing an overview of how this field contributes to the security and efficiency of public systems (Bonet, 2023, Jun 23).

Existing research predominantly focuses on the technical aspects of blockchain technologies, but detailed forensic analysis of private blockchains, which would also encompass legal and ethical aspects, remains insufficiently explored. This research aims to fill this gap by providing a comprehensive perspective on the methods and tools necessary for legal evidence and compliance assurance.

2 METHODS

This study builds on my several years of experience as an expert in forensic operations, where I have developed a particular interest in blockchain technology and its applications in forensic analysis. To establish a theoretical foundation and overview of existing knowledge, I conducted a comprehensive literature review, analyzing academic articles, studies, and white papers available in digital libraries. In my research, I used keywords such as "forensic analysis," "private blockchain," "security strategies," and "public sector."

As part of my research, I also gathered practical insights, utilizing information from Chainalysis, a leader in blockchain analysis. This information provided valuable insights into current trends and tools used in the industry for monitoring and analyzing transactions on private blockchains. Additionally, I obtained technical details on the deployment of blockchain technologies such as Hyperledger Fabric and Ethereum through online documentation and resources available on GitHub.

Integrating theoretical knowledge from the literature review with practical information enabled a deeper understanding of the challenges and possibilities of forensic analysis of private blockchains. In the study, I critically evaluated sources, compared various opinions and techniques, and formulated conclusions based on a combination of personal experiences, and theoretical and practical knowledge.

Private blockchains are being utilized in various areas of the public sector, including:

- *Digital land registry*: For example, a project in Georgia uses blockchain to manage property rights and real estate records (Shang & Price, 2019).
- *Citizen identity management systems*: For instance, e-Estonia, where blockchain is used to manage identities and ensure the integrity of personal data (PWC, 2019).
- *Supply chain tracking*: For example, FDA projects in the USA use blockchain to track the movement of drugs and ensure their authenticity (Anon., 2020).
- *Healthcare record management*: For example, initiatives in Estonia use blockchain to manage and protect patient healthcare records (Einaste, 2018).

2.1 Definition of Forensic Analysis of Private Blockchains

Forensic analysis of private blockchains is a specialized area of digital forensics that involves the investigation and analysis of data in closed blockchain networks. The goal is to identify, collect, preserve, analyze, and present evidence that can be used for legal and administrative purposes (Xu, 2021). This discipline combines traditional digital forensic principles with a deep

understanding of blockchain technology, cryptography, and distributed systems.

2.1.1 Key Components of Forensic Analysis of Private Blockchains

Evidence identification: This process involves locating relevant data within the blockchain network, including transaction records, smart contracts, and metadata. It is crucial to accurately determine which data is relevant to the investigation (Zheng, 2020).

Evidence collection: Evidence collection requires specialized tools and techniques to extract data from blockchain nodes. It is essential to ensure the integrity and authenticity of the information obtained (NIST, 2023).

Evidence preservation: This includes creating forensic copies of blockchain data and securely storing them in a way that maintains their evidential value. It is important to keep the data unchanged and available for further analysis.

Evidence analysis: This step involves a detailed examination of the collected data using specialized tools and techniques. Analysis may include examining transactions, smart contracts, and network activity to identify suspicious or unusual behavior (Bonneau, J., et al., 2015).

Evidence presentation: Forensic analysis results must be presented clearly and understandably for legal and administrative purposes. This includes creating a report that clearly describes the findings and provides evidence to support conclusions.

2.1.2 Specific Aspects of Forensic Analysis of Private Blockchains

Cryptographic evidence analysis: This involves verifying digital signatures, checking the integrity of hashes, and analyzing cryptographic protocols used in the network (ENISA, 2023). These procedures ensure that the data has not been altered and is authentic.

Block structure examination: This requires a detailed understanding of block formats, their linkages, and the consensus mechanisms used in the blockchain network.

Data integrity verification: This involves checking the integrity of the blockchain chain and detecting any attempts to tamper with historical data. Ensuring data integrity is crucial for the trustworthiness of the entire system.

Access control analysis: In private blockchains, examining access control mechanisms and identity management is key. These mechanisms, which are not present in public blockchains, ensure that only authorized users have access to certain information (Günther, M., Liebkind, J., & Nyberg, T., 2020).

2.1.3 Difference from Forensic Analysis of Public Blockchains

Verification of access rights: Unlike public blockchains, where anonymity is the main challenge, forensic analysis of private blockchains focuses on verifying whether all actions in the network were performed by authorized users (Santos, C., Almeida, F., & Oliveira, L., 2021).

Identification of unauthorized changes: In private blockchains, it is important to detect any attempts to manipulate data or network configuration. These changes can have serious consequences for the security and trustworthiness of the system.

Audit log analysis: Detailed examination of logs and audit records, often more accessible in private networks, allows for identifying and tracking the actions of individual users and nodes in the network (Xu, 2021).

Analysis of specific consensus mechanisms: Private blockchains often use different consensus mechanisms than public networks. These mechanisms can be proprietary and require specialized knowledge and tools for their analysis (NIST, 2023).

2.1.4 Legal and Ethical Aspects

Compliance with data protection laws: Forensic analysis of private blockchains must consider data protection regulations, such as GDPR in the EU. It is essential to ensure that personal data is protected and processed following regulations (Zheng, 2020).

Confidentiality of sensitive business information: During forensic analysis, it is important to protect the confidentiality of business information to prevent its unauthorized disclosure or misuse (Risius, M. & Spohrer, K., 2017).

Respect for jurisdictional limitations: Especially in the case of international blockchain networks, it is necessary to comply with the legal regulations and restrictions of different jurisdictions. This may

involve cooperation with regulatory authorities and adherence to local laws.

2.2 Importance of Forensic Analysis of Private Blockchains

The forensic analysis of private blockchains is becoming increasingly important, especially with the growing adoption of blockchain technology in the public sector. This discipline plays a key role in ensuring the integrity, security, and trustworthiness of blockchain systems. Here are the main reasons why the forensic analysis of private blockchains is so crucial:

2.2.1 Key Factors Increasing the Importance of Forensic Analysis of Private Blockchains

Protection of critical infrastructure: Many government institutions implement blockchain technologies for managing critical data and processes, such as land registries, healthcare records, or identity management systems. Forensic analysis of private blockchains is crucial for identifying and investigating potential security incidents in these systems (Zyskind, G., Nathan, O., & Pentland, A., 2015).

Combating financial crime: Private blockchains are increasingly used in the financial sector. Forensic tools are essential for detecting fraud, money laundering, and other financial crimes in these systems. They help ensure that transactions are legitimate and that financial flows are transparent.

Ensuring the integrity of public records: Many countries implement blockchain technologies for managing public registries, such as land records or citizen registries. Forensic analysis is crucial for verifying the integrity of these records and investigating possible manipulations (ENISA, 2023). This helps maintain the credibility and accuracy of public information.

Supporting regulatory oversight: With the growing use of blockchain technologies, regulatory authorities need effective tools for monitoring and oversight. Forensic techniques enable regulators to monitor compliance with regulations, identify potential violations, and ensure that organizations adhere to applicable laws and standards (Santos, C., Almeida, F., & Oliveira, L., 2021).

2.2.2 Specific Benefits of Forensic Analysis of Private Blockchains

Increased transparency: Forensic tools enable detailed analysis of transactions and activities on the blockchain, contributing to higher transparency. This increases citizens' trust in public institutions and helps prevent corruption and fraud (Wuest & Gervais, 2018).

Improved auditability: Forensic analysis provides robust methods for auditing blockchain systems. This is key for ensuring accountability and integrity in public institutions. Regular audits can uncover inconsistencies and ensure that systems operate correctly (Günther, M., Liebkind, J., & Nyberg, T., 2020).

Faster detection and response to incidents: Forensic tools enable rapid identification of anomalies and potential security threats. This allows for quicker and more effective responses to incidents, minimizing damage and ensuring the rapid restoration of normal system operations (Bonneau, J., et al., 2015).

Supporting the legal system: Forensic analysis of private blockchains provides reliable evidence for legal proceedings. This is crucial for resolving disputes and enforcing laws in the digital environment. Evidence obtained from the blockchain can be used in court to support claims and charges.

2.2.3 Economic Aspects

Reducing financial losses: Effective forensic analysis can help quickly detect and stop fraudulent activities, leading to significant savings for the public sector. Rapid detection and remediation of issues minimize financial damages and increase confidence in blockchain technologies (Shang & Price, 2019).

Optimizing compliance costs: Forensic tools can automate many aspects of regulatory oversight, reducing compliance costs for public sector organizations. Automation reduces the need for manual checks and increases efficiency (NIST, 2023).

2.2.4 Future Trends Increasing Importance

Integration with artificial intelligence: Forensic tools are expected to increasingly use artificial intelligence for advanced data analysis. AI will enable more efficient detection of complex

patterns and anomalies, increasing the accuracy and speed of forensic analyses (Zheng, 2020).

International cooperation: With the increasing number of global blockchain projects, the need for cross-border forensic collaboration grows. This will require the development of new protocols and tools for international forensic analysis, improving the ability to address global issues (Zyskind, G., Nathan, O., & Pentland, A., 2015).

Response to new types of threats: As blockchain technologies evolve, new types of security threats will emerge. Forensic analysis will need to continuously innovate to address these threats and ensure the integrity of blockchain systems (Xu, 2021).

2.3 Techniques for Forensic Analysis of Private Blockchains

Forensic analysis of private blockchains employs various specialized techniques to analyze and investigate activities in closed blockchain networks. These techniques are continuously evolving with advancements in blockchain technologies. Here are the main categories of techniques with detailed descriptions:

2.3.1 Transaction Analysis

Tracking asset movement: This technique uses graph algorithms to map the flow of assets between addresses in the blockchain network. It helps identify transfer patterns that may indicate suspicious activities (Zheng, 2020).

Pattern analysis: This technique applies statistical methods to identify unusual frequencies or volumes of transactions. Machine learning is also used to detect anomalies in transaction data. Metadata analysis of transactions provides additional information about the nature of transfers.

Clustering analysis: This technique group addresses based on their transactions, helping identify potentially linked entities. Heuristic algorithms are used to uncover hidden relationships between participants in the blockchain network.

2.3.2 Smart Contract Analysis

Static code analysis: Examines the source code of smart contracts to identify potential vulnerabilities. Automated tools detect known patterns of risky code and analyze the contract logic to identify unexpected behaviors.

Dynamic analysis: This technique simulates the execution of smart contracts in a controlled environment, monitoring contract behavior under different input conditions and identifying potentially exploitable states or unexpected interactions (Zyskind, G., Nathan, O., & Pentland, A., 2015).

Symbolic execution: Uses formal methods to model mathematically all possible execution paths of a contract. Identifies conditions under which undesirable behavior may occur.

2.3.3 Network Architecture Analysis

Topological analysis: Maps the structure of the blockchain network, identifying key nodes and their interconnections. Analyzes the distribution of computational power in the network, helping understand how the network is organized and where potential weaknesses lie.

Consensus mechanism analysis: Examines the implementation and behavior of consensus algorithms. Identifies potential weaknesses in the consensus process, which is crucial for ensuring the integrity and trustworthiness of the blockchain network (NIST, 2023).

Network communication analysis: Monitors and analyzes communication patterns between nodes. Identifies anomalies in network traffic that may indicate an attack or other security issues.

2.3.4 Access Control and Identity Analysis

Audit of access rights: Examines the identity management and access control system in the blockchain network. Verifies whether all actions were performed by authorized users, ensuring no unauthorized accesses occurred.

Change analysis in rights: Tracks the history of changes in access rights and identifies potentially unauthorized or suspicious changes. This technique helps identify attempts to misuse access rights (Santos, C., Almeida, F., & Oliveira, L., 2021).

Behavioral analysis: Monitors and analyzes user behavior patterns in the network. Identifies

deviations from normal behavior that may indicate account compromise or other security threats.

2.3.5 Cryptographic Analysis

Signature verification: Verifies the integrity of digital signatures used in transactions and smart contracts. Identifies potentially forged or compromised signatures, which is crucial for ensuring the trustworthiness of data (Bonneau, J., et al., 2015).

Hash function analysis: Verifies the correctness of hash function implementation and usage. It looks for potential collisions or weaknesses in hash algorithms that could be exploited for data manipulation.

Cryptographic protocol analysis: Examines the implementation and usage of cryptographic protocols in the network. Identifies potential vulnerabilities in cryptographic schemes that could be used for attacks (Risius, M. & Spohrer, K., 2017).

2.3.6 Off-Chain Data Analysis

Correlation of on-chain and off-chain data: Connects blockchain transactions and events with external data. It uses external information sources to contextualize blockchain activities, helping better understand the broader context.

Metadata analysis: Examines additional information associated with blockchain transactions. Extracts and analyzes data stored in OP_RETURN fields or similar structures, providing supplementary information about transactions and their participants (NIST, 2023).

2.3.7 Temporal Analysis

Event timeline: Reconstructs the chronological sequence of events in the blockchain network. It identifies causal relationships between various activities, helping understand how individual events developed over time (ENISA, 2023).

Temporal pattern analysis: Examines the distribution of activities over time to identify unusual patterns. It uses anomaly detection techniques to identify non-standard temporal sequences that may indicate suspicious activities.

These techniques are often combined and applied iteratively during a forensic investigation. Their effective use requires a deep understanding of blockchain technology, cryptography, network protocols, and forensic principles. With the evolution of blockchain technologies, forensic techniques are expected to develop further to meet new challenges and threats.

2.4 Challenges of Forensic Analysis of Private Blockchains

Forensic analysis of private blockchains faces numerous technical, legal, and ethical challenges. These challenges can complicate investigating and analyzing data in closed blockchain networks. Here are the main challenges this field encounters:

2.4.1 Technical Challenges

Restricted access to network nodes: In private blockchains, it is not possible to freely access all nodes in the network. This limited access can hinder data collection and comprehensive network analysis, as not all nodes may be available for inspection and monitoring (Risius, M. & Spohrer, K., 2017).

Variety of implementations: Private blockchains can be implemented in various ways, meaning there is no single approach to accessing and analyzing them. Each implementation may require specific tools and techniques, increasing the complexity of forensic analysis.

Complexity of smart contracts: Smart contracts can be very complex and contain intricate logic and interactions. Analyzing these contracts requires advanced tools and expertise to identify potential vulnerabilities and inconsistencies (Zyskind, G., Nathan, O., & Pentland, A., 2015).

Proprietary consensus mechanisms: Private blockchains often use proprietary consensus mechanisms that are not commonly known and documented. Analyzing these mechanisms can be challenging and requires specialized knowledge and tools (Günther, M., Liebkind, J., & Nyberg, T., 2020).

2.4.2 Legal and Ethical Challenges

Uncertainties regarding jurisdiction: In the case of international private blockchains, it may be unclear which legal regulations and jurisdictions are relevant. This can complicate investigations, especially if network participants are from different countries with different laws and regulations (ENISA, 2023).

Data protection and privacy laws: Forensic analysis must be conducted in compliance with data protection regulations, such as GDPR in the EU. It must be ensured that sensitive personal data is protected and processed responsibly to avoid privacy violations (Zheng, 2020).

Ethical considerations: There are moral questions regarding the scope and methods of conducting forensic analysis in closed systems. It is important to balance the need for investigation and the protection of individual rights. Forensic analysts must work with a high degree of integrity and responsibility (Bonneau, J., et al., 2015).

Preserving the integrity of evidence: During forensic analysis, it is crucial to ensure that evidence remains unchanged and reliable. This includes creating forensic copies of data and securely storing them. It is also necessary to ensure the confidentiality of sensitive information to prevent unauthorized disclosure (Santos, C., Almeida, F., & Oliveira, L., 2021).

These technical, legal, and ethical challenges represent significant obstacles that need to be overcome for forensic analysis of private blockchains to be effective and reliable. Advanced tools, expert education, and international cooperation are key to addressing these challenges and ensuring the security and integrity of blockchain systems.

2.5 Technical Details of Forensic Analysis of Private Blockchains

These technical details provide an overview of specific methods and tools used in the forensic analysis of private blockchains. It is important to note that actual forensic analysis often requires a combination of various advanced techniques as well as a deep understanding of specific blockchain platforms and the context of the investigation.

2.5.1 Data Extraction from Blockchain Nodes

The data extraction from blockchain nodes is a crucial step in forensic analysis. Figure 1 shows an example of a Python script for extracting data from a Hyperledger Fabric node (Hyperledger, 2024).

```
from hfc.fabric import Client
# Initialize the client
client = Client(net_profile="connection-
profile.json")
# Connect to the network
client.new_channel('mychannel')
# Extract data from a specific block
block_number = 1000
block = client.query_block(block_number,
'mychannel')
# Analyze transactions in the block
for tx in block.get('data').get('data'):
    transaction =
tx.get('payload').get('data').get('actio
ns')[0].get('payload').get('action')
    print(f"Transaction: {transaction}")
```

Fig. 1 Extracting data from the Hyperledger Fabric node
Source: GitHub (2024)

This code (GitHub, 2024) serves to interact with the blockchain network on the Hyperledger Fabric platform using the hfc.fabric library. The code demonstrates how one can connect to the network, query blocks in the blockchain, and analyze transactions within them.

2.5.2 Transaction Analysis

After data extraction, the next step is transaction analysis. Figure 2 shows an example of a function for detecting unusual patterns in transactions.

```
import pandas as pd
from scipy import stats
def detect_anomalies(transactions):
    df = pd.DataFrame(transactions)
    df['z_score'] = stats.zscore(df['value'])
    anomalies = df[abs(df['z_score']) > 3]
    return anomalies
# Using the function
transactions = [{'value': 10}, {'value': 100},
{'value': -5}]
anomalies = detect_anomalies(transactions)
print(f"Detected anomalies: {anomalies}")
```

Fig.2 Transaction Analysis
Source: GitHub (2024)

This code (GitHub, 2024) serves to detect anomalous transactions in the dataset using a statistical method known as Z-score. It uses the pandas' library (Pandas, 2024) for data manipulation and SciPy for computing statistics. The code focuses on identifying transactions with extreme values compared to the rest of the dataset.

2.5.3 Smart Contract Analysis

Smart contract analysis is critical for uncovering potential vulnerabilities. Figure 3 shows an example of using the Mythril tool (Mythril, 2019) to analyze a Solidity smart contract:

```
from mythril.mythril import Mythril
from mythril.exceptions import
CriticalError
def analyze_contract(contract_file):
    myth = Mythril()
    try:

myth.load_from_solidity(contract_file)
        issues =
myth.fire_lasers(modules=["ether_thief",
"arbitrary_write"])
        for issue in issues:
            print(f"Issue:
{issue.description}")
    except CriticalError as ce:
        print(f"Critical error
encountered: {ce}")
# Using the function
analyze_contract("MyContract.sol")
```

Fig.3 Smart Contract Analysis
Source: Mythril (2019)

This code (GitHub, 2024) is a tool for static analysis of smart contracts written in Solidity, intended for the Ethereum blockchain. It uses the Mythril library, known for its capabilities to identify security vulnerabilities and issues in smart contracts.

2.5.4 Event Timeline Reconstruction

Event timeline reconstruction is important for understanding the sequence of activities. Figure 4 shows an example of a function to create a timeline.

This code (GitHub, 2024) is a tool for visualizing the timeline of events. It uses the pandas' library for data manipulation and Matplotlib (Hunter, J. D., 2007) for plotting the graph. It allows converting a list of events into a timeline with labels, where each event is displayed on the graph according to its timestamp.

```
        import pandas as pd
    import matplotlib.pyplot as plt
     def create_timeline(events):
       df = pd.DataFrame(events,
    columns=['timestamp', 'event'])
           df['timestamp'] =
    pd.to_datetime(df['timestamp'])
    df = df.sort_values('timestamp')
fig, ax = plt.subplots(figsize=(12, 6))
ax.plot(df['timestamp'], range(len(df)),
                'o-')
 for i, txt in enumerate(df['event']):
           ax.annotate(txt,
     (df['timestamp'].iloc[i], i),
  xytext=(10, 0), textcoords='offset
              points')
    plt.title('Timeline of Events')
          plt.xlabel('Time')
     plt.ylabel('Event Sequence')
          plt.tight_layout()
              plt.show()
        # Using the function
              events = [
   ('2023-01-01 10:00:00', 'Contract
            Deployment'),
    ('2023-01-02 15:30:00', 'Unusual
             Transaction'),
('2023-01-03 09:45:00', 'Access Pattern
              Change')
                ]
        create_timeline(events)
```

Fig.4 Timeline Reconstruction
Source: (GitHub, 2024)

2.5.5 Network Communication Analysis

Analyzing network communication between blockchain network nodes can reveal potential security issues. Figure 5 is an example of using the Scapy library (Scapy, 2024) to analyze network traffic:

```
from scapy.all import *
def analyze_network_traffic(pcap_file):
    packets = rdpcap(pcap_file)
    for packet in packets:
        if TCP in packet and
packet[TCP].dport == 7051:  # The Port
used by Hyperledger Fabric
            print(f"Blockchain
communication detected:
{packet.summary()}")
            if Raw in packet:
                payload =
packet[Raw].load
                # Analýza payload-u
# Using the function
analyze_network_traffic("blockchain_traf
fic.pcap")
```

Fig.5 Network Analysis
Source: (GitHub, 2024)

This code (GitHub, 2024) is a tool for analyzing network traffic, specifically focused on the captured communication of the Hyperledger Fabric blockchain, using the Scapy library. Scapy is a powerful Python library for packet manipulation, capturing, and analyzing network traffic.

2.6 Future of Forensic Analysis of Private Blockchains

The forensic analysis of private blockchains will continuously evolve and adapt to new challenges and technological advancements. It is full of challenges but also opportunities for improvement and innovation. Investments in new technology development, education of experts, and international cooperation will be crucial for ensuring the integrity and trustworthiness of blockchain systems in the public sector. Several key areas will significantly impact this discipline:

- *Development of standards*: International organizations, such as ISO (International Organization for Standardization) and NIST (National Institute of Standards and Technology), are working on creating standards and guidelines for blockchain technologies, including forensic analysis. ISO/TC 307 deals with the standardization of blockchain technologies, and NIST is developing guidelines for blockchain cybersecurity (NIST, 2023). These initiatives will help create unified procedures and improve the efficiency of forensic analyses.
- *Potential regulatory changes*: In the coming years, new regulations specific to blockchain technologies are expected to be adopted. In the European Union, legislation is being planned that will require forensically auditable records for blockchains used in the public sector. Similar legislation is being considered in the United States to increase transparency and accountability (Zheng, 2020). These regulatory changes will improve forensic investigation capabilities and increase confidence in blockchain technologies.
- *Integration with artificial intelligence*: Forensic tools are expected to increasingly utilize artificial intelligence (AI) for advanced data analysis. AI can help more quickly and accurately identify anomalies and suspicious patterns in blockchain data. This integration will enable more efficient and automated forensic analyses, increasing their accuracy and reliability (Risius, M. & Spohrer, K., 2017).
- *International cooperation*: With the growing number of international blockchain projects, the need for cross-border forensic cooperation increases. Organizations like Interpol and Europol emphasize international cooperation in the field of blockchain forensic analysis. This cooperation will include the development of new protocols and tools for sharing information and coordinating investigations between different countries (Günther, M., Liebkind, J., & Nyberg, T., 2020). International cooperation is essential for effectively addressing global blockchain-related issues.
- *Response to new types of threats*: As blockchain technologies evolve, new types of security threats will emerge. Forensic analysis must continuously innovate to address these new threats. Research and development of new techniques and tools will be crucial for ensuring that forensic analyses can identify and address new security challenges (Xu, 2021).

2.7 Artifacts and Their Analysis

Forensic analysis of private blockchains involves examining various types of data referred to as artifacts. These artifacts provide key information for the investigation and can include transaction data, smart contract data, logs and audit records, blockchain structure data, and configuration data. Each type of artifact is important for understanding and analyzing the blockchain network.

2.7.1 Transaction Data

Timestamps: These marks indicate the exact time and date of each transaction in the blockchain. They help reconstruct the chronology of events and identify transaction patterns (Bonneau, J., et al., 2015).

Participant identifiers: Public keys or other identifiers allow the identification of individual transaction participants. These identifiers are important for tracking the origin and destination of assets.

Transaction metadata: Includes the type of operation (such as asset transfer, smart contract signing), the amount of assets transferred, and additional information that can provide context for each transaction.

2.7.2 Smart Contract Data

Bytecode: The compiled code of the contract deployed on the blockchain. This code determines how the contract behaves and what operations it can perform (Santos, C., Almeida, F., & Oliveira, L., 2021).

Application Binary Interface (ABI): The definition of the contract's functions and parameters, allowing interaction with the smart contract. ABI is essential for understanding how the smart contract can be called and what data it expects.

Contract state: Current values of the variables in the contract. These data reflect the current state of the smart contract and can provide information about its historical and current operations (Zyskind, G., Nathan, O., & Pentland, A., 2015).

2.7.3 Logs and Audit Records

System logs: Records of operations at the blockchain platform level, which may include node activities, transactions, and consensus events (Zheng, 2020).

Application logs: Records generated by specific applications running on the blockchain. These logs can provide detailed information about the activities of individual applications and smart contracts (Risius, M. & Spohrer, K., 2017).

Audit records: Detailed information about user accesses and actions. These records are crucial for tracking who performed which operations and when.

2.7.4 Blockchain Structure Data

Block headers: Information about each block, including the hash of the previous block. Block headers provide data about the chain of blocks and allow the verification of blockchain integrity (Bonneau, J., et al., 2015).

Merkle tree: A structure used for efficient transaction verification. The Merkle tree allows quick and reliable verification that a transaction is part of a specific block without searching the entire block.

2.7.5 Configuration Data

Network settings: Information about the topology and rules of the network, such as consensus rules, the number of nodes, and their roles in the network. These data are crucial for understanding the functioning and behavior of the blockchain network (Santos, C., Almeida, F., & Oliveira, L., 2021).

Consensus rules: Details on how consensus is reached in the network. These rules determine how nodes cooperate to verify and add new blocks to the blockchain.

Why are these artifacts significant?

Timestamps and participant identifiers: Help forensic experts track when and who performed specific transactions, which is essential for reconstructing events and identifying suspicious activities.

Smart contract data: Provide a detailed view of the logic and execution of smart contracts, which is necessary for analyzing their security and correctness.

Logs and audit records: These are crucial for tracking operations and activities in the network, enabling the identification of unauthorized access and potential security incidents.

Blockchain structure data: It allows verification of the integrity and continuity of the blockchain, which is important for the trustworthiness and security of the entire network.

Configuration data: It provides context for the functioning of the network and allows the understanding of how the network is organized and how it reaches consensus (Zheng, 2020).

2.8 Analysis Tools

Several specialized tools have been developed specifically for the forensic analysis of private blockchains. These tools help ensure that data and operations in the blockchain network can be thoroughly analyzed to identify potential security issues, fraud, and other anomalies. The following tools are crucial for the effective management and analysis of private blockchain networks, as they help ensure their security, performance, and regulatory compliance:

- *Hyperledger Caliper* is a tool for benchmarking and performance analysis of private blockchains. It allows testing different blockchain implementations and measuring their performance using various indicators such as latency, throughput, and transactions per second (TPS). This tool helps developers and administrators understand the performance characteristics of their blockchain networks and identify areas where optimization is needed (NIST, 2023).
- *Accenture Blockchain Forensic Suite* is a comprehensive tool designed for forensic analysis of blockchain platforms such as

Hyperledger Fabric and R3 Corda. It includes tools for collecting, analyzing, and visualizing blockchain data, enabling the identification and tracking of transactions, verification of smart contract integrity, and analysis of network activity. This tool provides forensic analysts with robust means for investigating suspicious activities and ensuring regulatory compliance (Risius, M. & Spohrer, K., 2017).

- *Quorum Explorer* is a specialized tool designed for network analysis based on Quorum, an enterprise version of Ethereum. This tool allows monitoring and analysis of transactions, smart contracts, and network activity in the Quorum blockchain network. It provides visualizations and detailed overviews of the state of the network and its participants, helping organizations maintain oversight of their blockchain network, identify anomalies, and ensure optimal operation (Santos, C., Almeida, F., & Oliveira, L., 2021).

2.9 Case Studies

Given the sensitive nature of forensic investigations, many case details remain confidential. The following case studies are based on publicly available information and anonymized examples that illustrate the use of forensic analysis of private blockchains in the public sector.

2.9.1 Case No. 1: Uncovering fraud in the public procurement system (anonymized European country, 2022)

A government agency implemented a private blockchain system to manage public procurement to increase transparency and efficiency. Anomalies in contract awards were recorded, suggesting possible manipulation of the supplier selection process. Forensic experts reviewed the transaction history in the blockchain, focusing on patterns in contract awards. A detailed analysis of the smart contract code controlling the procurement process was conducted. They created a chronological reconstruction of key events in the system. The result was the discovery of unauthorized changes in the smart contract code that allowed the manipulation of selection criteria. A series of suspicious transactions linked to a specific administrator account were identified. The investigation led to the uncovering of a corruption scheme, legal consequences for those involved, and significant changes in the public procurement system.

2.9.2 Case No. 2: Protecting the integrity of the digital real estate registry (anonymized Asian country, 2023)

A government body implemented a private blockchain to manage the real estate registry to increase security and efficiency. Cases of unauthorized changes to property rights were reported. Experts examined the access records and permissions in the system. They analyzed in detail the metadata associated with transactions related to changes in property rights. They verified the integrity of digital signatures and hashes linked to the relevant transactions. The result was the identification of a series of unauthorized accesses to the system through compromised employee accounts and the detection of sophisticated malware that allowed the circumvention of security controls.

2.9.3 Case No. 3: Analyzing anomalies in the healthcare records system (anonymized North American country, 2024).

A regional healthcare system implemented a private blockchain to manage patient health records. Unusual patterns in access to health records were recorded, indicating a potential leak of sensitive data. Experts analyzed the access patterns to the records, identifying anomalies in the timing and frequency of access. They thoroughly examined the audit logs of the blockchain system and conducted a forensic analysis of network communication between the blockchain nodes. The result was the discovery of unauthorized access to the records through a poorly configured API.

These case studies illustrate the diversity and complexity of challenges faced by forensic analysis of private blockchains in the public sector. They also emphasize the importance of advanced forensic techniques and tools to preserve the integrity and security of these systems.

3 RESULTS

This study has yielded important findings regarding the forensic analysis of private blockchains in the public sector, reflecting the current state and identifying the main challenges and risks. Through the literature and sources

review, I discovered that the forensic challenges of private blockchains often relate to limited data access, high levels of encryption, and the lack of standardized tools for effective analysis. These factors make the acquisition and verification of forensic evidence complicated and require special techniques and approaches.

In addition to technical challenges, I identified security risks that include vulnerabilities in the implementation of smart contracts and potential data leakage through network interfaces. These security weaknesses demand increased attention and the development of new forensic methods to address them adequately.

From a legal and ethical perspective, the study highlighted significant dilemmas related to personal data protection and compliance with jurisdictional constraints. These findings underscore the need for a better regulatory framework and international agreements to help address issues associated with the use of forensic techniques in private blockchains.

Overall, my findings emphasize the complexity of forensic analysis of private blockchains and highlight the need for continuous research and development in this area to effectively face the challenges that these technologies bring.

4 CONCLUSIONS

Forensic analysis of private blockchains is an integral part of ensuring the integrity and trustworthiness of blockchain systems in the public sector. As this technology is increasingly adopted by various government and public institutions, the need for advanced forensic techniques and tools that enable effective investigation and analysis also grows. It is important to invest in the development and improvement of tools specifically designed for the analysis of private blockchains to address the specific challenges associated with closed systems, such as identifying unauthorized access and tracking transactions.

In this study, I emphasized the importance of continuous education and training for forensic experts who must keep pace with rapidly evolving technologies. These experts need not only technical skills but also an understanding of the legal and ethical aspects of forensic analysis. International collaboration in developing standards and sharing knowledge is crucial, as blockchain technology is a global phenomenon.

Regulatory authorities and international organizations should work together to create unified rules and procedures for blockchain forensic analysis. It is essential to find a balance between effective investigation and privacy protection to ensure that forensic analysis respects individual rights and complies with legal regulations concerning data protection.

Future research should focus on developing advanced techniques for analyzing complex smart contracts, which are becoming increasingly sophisticated and require new methods for identifying vulnerabilities and verifying their correct execution. This research should also improve methods for preserving the integrity of evidence in distributed systems, including the creation of forensic copies and the secure storage of data. Finally, research should address the legal and ethical challenges associated with forensic analysis in an international context to ensure that such analysis complies with global legal regulations and ethical standards.

In conclusion, forensic analysis of private blockchains is a critical tool for maintaining the security and trustworthiness of digital systems in the public sector. Investments in tool development, expert education, and international collaboration are key to the future success and effectiveness of forensic analysis in this dynamically evolving field.

WORKS CITED

Anon. (2023, Jun 28). *Introducing Splice, a New Hyperledger Lab for Canton Network interoperability.* Retrieved from Hyperledger Foundation: https://www.lfdecentralizedtrust.org/blog/introducing-splice-a-new-hyperledger-lab-that-supports-canton-network-interoperability

Anon. (2020). Retrieved from FDA DSCSA Blockchain Interoperability: https://www.fda.gov/media/169883/download

Bonet, J. (2023, Jun 23, June). *Consolidated Annual Activity Report 2022.* EUROPOL. Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated%20Annual%20Activity%20Report%202022.PDF

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. *2015 IEEE Symposium on Security and Privacy*, 104-121.

Einaste, T. (2018, Feb 26). *Blockchain and healthcare: the Estonian experience.* Retrieved from e-estonia.com: https://e-estonia.com/blockchain-healthcare-estonian-experience/

ENISA. (2023, Oct 19). *ENISA Threat Landscape 2023.* (I. Lella, E. Tsekmezoglou, M. Theocharidou, E. Magonara, A. Malatras, R. S. Naydenov, & C. Ciobanu, Eds.) doi:10.2824/782573

GitHub. (2024). *Fabric-sdk-py.* Retrieved from GitHub: https://github.com/hyperledger/fabric-sdk-py

Günther, M., Liebkind, J., & Nyberg, T. (2020). Digital Forensics in Blockchain Environments: Distinctive Features and Forensic Process. *Forensic Science International: Digital Investigation. 2020, 33*, 200-219.

Hunter, J. D. (2007). Retrieved from Matplotlib: A 2D Graphics Environment. Computing in Science & Engineering, vol. 9, no. 3, 2007: https://matplotlib.org/

Hyperledger. (2024). Retrieved from Hyperledger Fabric: https://www.hyperledger.org/

Mythril. (2019). *Mythril*. Retrieved from Github.com: https://mythril-classic.readthedocs.io/en/develop/about.html

Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved from https://bitcoin.org/bitcoin.pdf

NIST. (2023). Guidelines for Blockchain Cybersecurity. *NIST Special Publication 800-204*.

Pandas. (2024). *Pandas*. Retrieved from The Pandas Development Team: https://pandas.pydata.org/

PWC. (2019). Retrieved from Estonia – the Digital Republic Secured by Blockchain: https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf

Risius, M., & Spohrer, K. (2017). A Blockchain Research Framework: What We (don't) Know, Where We Go from Here, and How We Will Get There. *Business & Information Systems Engineering. 2017, 59(6)*, 385-409.

Santos, C., Almeida, F., & Oliveira, L. (2021). Blockchain: A Literature Review on Forensic Methods and Challenges. *IEEE Access. 2021, 9*, 312-330.

Scapy. (2024). *Scapy*. Retrieved from Scapy: https://scapy.net/

Shang, Q., & Price, A. (2019). A Blockchain-Based Land Titling Project in the Republic of Georgia. *Innovations: Technology, Governance, Globalization, 12*(3-4), 72-78.

Wuest, K., & Gervais, A. (2018). Do you need a Blockchain? *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)* (pp. 45-54). Zug, Switzerland: IEEE. doi:10.1109/CVCBT.2018.00011

Xu, J. (2021). Forensic Analysis of Private Blockchain Networks. *Journal of Digital Forensics, Security and Law. 2021, 16(2)*, 45-62.

Zheng, Z. e. (2020). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *International Congress on Big Data*, 557-564.

Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *IEEE Security and Privacy Workshops*, 180-184.

Received for publication: 01.07.2024
Revision received: 08.07.2024
Accepted for publication: 08.01.2025.

How to cite this article?

Style – **APA** *Sixth Edition:*

Feltovic, M. (2025, 01 15). Forensic Analysis of Private Blockchains in the Public Sector: Challenges, Techniques, and Future. (Z. Cekerevac, Ed.) *MEST Journal, 13*(1), 62-75. doi:10.12709/mest.13.13.01.06

Style – **Chicago** *Sixteenth Edition:*

Feltovic, Milan. "Forensic Analysis of Private Blockchains in the Public Sector: Challenges, Techniques, and Future." Edited by Zoran Cekerevac. MEST Journal (MESTE) 13, no. 1 (01 2025): 62-75.

Style – **GOST** *Name Sort:*

Feltovic Milan Forensic Analysis of Private Blockchains in the Public Sector: Challenges, Techniques, and Future [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE, 01 15, 2025. - 1 : Vol. 13. - pp. 62-75.

Style – **Harvard** *Anglia:*

Feltovic, M., 2025. Forensic Analysis of Private Blockchains in the Public Sector: Challenges, Techniques, and Future. *MEST Journal,* 15 01, 13(1), pp. 62-75.

Style – **ISO 690** *Numerical Reference:*

Forensic Analysis of Private Blockchains in the Public Sector: Challenges, Techniques, and Future. **Feltovic, Milan.** [ed.] Zoran Cekerevac. 1, Belgrade – Toronto : MESTE, 01 15, 2025, MEST Journal, Vol. 13, pp. 62-75.