A Private Blockchain-Based System for Managing the Originality of Digital Evidence*

Hae-Yeong Cho[1], Seongho Lim[2], Nam In Park[2], Junseok Byun[2], and Sang-Min Choi[1*]

[1] Gyeongsang National University, Jinju-si, Republic of Korea
socilt54@gnu.ac.kr, jerassi@gnu.ac.kr
[2] National Forensic Service Digital division, Wonju-si, Republic of Korea
shlim2000@korea.kr, namin.park@gmail.com, jsbyun77@korea.kr

Abstract

The proliferation of digital evidence in legal processes necessitates robust mechanisms to guarantee its originality and integrity. However, the inherent malleability of digital data renders conventional centralized systems vulnerable to tampering, malicious insider threats, and data loss. This paper proposes a novel framework that conceptualizes each piece of evidence as a unique digital asset and represents it as a Non-Fungible Token (NFT) on a private blockchain. This approach establishes an immutable and transparent record for digital evidence management, ensuring originality from the point of collection. The transfer of NFTs between custodian wallets creates an unbreakable and auditable Chain of Custody. We implemented a prototype using GoQuorum, demonstrating the feasibility of this assetization model. This approach significantly enhances the trustworthiness of digital evidence by providing a cryptographically secure provenance trail.

1 Introduction

Current digital evidence management systems, predominantly centralized, exhibit fundamental limitations. They are susceptible to a Single Point of Failure (SPOF), making them vulnerable to external attacks, malicious insider threats, and data loss. Furthermore, verifying integrity and tracking the Chain of Custody often relies on manual, inefficient procedures that can impede judicial processes [1].

To overcome these challenges, recent research has explored blockchain for digital forensics. For instance, Lone and Mir proposed 'Forensic-chain' using Hyperledger Fabric to create immutable logs of forensic activities [1]. Similarly, Bacciu et al. demonstrated a smart contract-based framework for managing the Chain of Custody [2]. While these studies validate blockchain's potential, our work introduces a novel conceptual leap: the assetization of digital evidence. We leverage Non-Fungible Tokens (NFTs), a concept enabled by platforms like Ethereum [3], to treat each piece of evidence as a unique, non-interchangeable digital asset. This approach leverages the inherent immutability of blockchain technology to establish a transparent and cryptographically secure record of its provenance, from collection to courtroom presentation.

2 Proposed Architecture

Our system guarantees the originality, integrity, and Chain of Custody of digital evidence. This system adopts a private blockchain to address the confidentiality requirements of legal evidence.
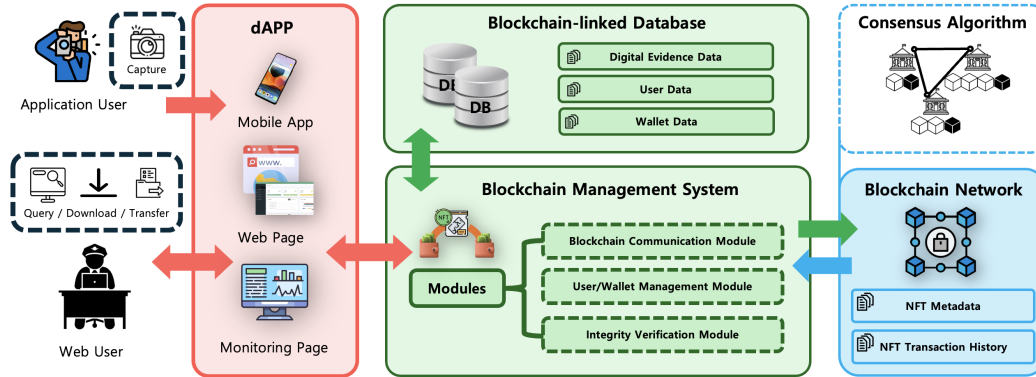

Figure 1:   The proposed system architecture.

We specifically selected GoQuorum, an enterprise version of Ethereum, for its mature ecosystem, permissioning capabilities, and efficient consensus mechanisms suitable for a consortium of judicial bodies. The system architecture, depicted in Figure 1, comprises a dApp, a management system, an off-chain database, and the private blockchain network.

The core mechanism is the management of evidence as NFTs. First, Evidence Registration (NFT Minting): Upon collection, the evidence's cryptographic hash and metadata are minted into a unique NFT. The integrity of the link between the on-chain NFT and the off-chain evidence file is guaranteed by embedding this hash into the NFT's metadata. Second, Chain of Custody (NFT Transfer): When evidence is transferred, the corresponding NFT is moved between custodian wallets (e.g., police to prosecution). This transaction is immutably recorded. Third, Integrity Verification: Any party can verify the evidence's integrity by comparing its current hash against the original hash stored within the NFT. To validate this architecture, we implemented a prototype using GoQuorum, Solidity (ERC-721), and a dApp, successfully demonstrating the core functionalities.

3   Conclusion

This paper introduced a novel framework for the assetization of digital evidence using a private blockchain and NFTs. By abstracting each piece of evidence as a unique digital asset, our system provides a robust solution to the critical challenges of ensuring originality, integrity, and a transparent Chain of Custody. The prototype implementation demonstrates that this NFT-centric approach is technically feasible and offers significant improvements over traditional systems.

Acknowledgement

References

[1] Abid H Lone and Roohie Naaz Mir. Forensic-chain: A blockchain-based digital forensics investigation framework. *Future Generation Computer Systems*, 95:321–339, 2019.

[2] Davide Bacciu, Andrea Cricenti, Alessandro De Franco, and Pietro Nannipieri. A smart contract-based framework for secure and transparent digital evidence management. *IEEE Transactions on Emerging Topics in Computing*, 9(3):1543–1555, 2021.

[3] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 2014.