The Application of Blockchain of Custody in Criminal Investigation Process

Yueh-Tan Chiang a, Fu-Ching Tsai a

a Central Police University, Guishan, Taoyuan 333, Taiwan, R.O.C.

Abstract: The blockchain of custody framework can be used to facilitate the security and transparency of digital evidence in criminal investigation process. The corresponding actions with judicial process is simulated using private ethereum blockchain. Through implementation, we discussed the functionality and security issues of custody framework in blockchain. The experimental results indicate that the proposed framework can prevent digital evidence been tampered or contaminated and assure its legal defensibility with rigorous privilege management.

Keywords: Blockchain; Smart Contract; Digital Forensics; Chain of Custody

1. Introduction

![Figure 1. Digital evidence blockchain of custody flow chart](image)

2. Study Framework

![Figure 2. Study framework](image)

3. System Design

- The environment of system development: The study simulate an Ethereum private chain which composed with Node A and B with Geth.
- Smart contract design

![Table 1. Smart contract function design](image)

<table>
<thead>
<tr>
<th>Role</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>SetMember()</td>
<td>The account which can deploy the smart contract and is responsible for setting a list of members to distinguish between investigators or general users.</td>
</tr>
<tr>
<td>Creator</td>
<td>CreateEvidence()</td>
<td>The account that can create the digital evidence hash value and case description to the blockchain.</td>
</tr>
<tr>
<td>Owner</td>
<td>Transfer()</td>
<td>The account which holds the digital evidence and case custodian. The account can transfer the custodian and modify the case description.</td>
</tr>
<tr>
<td>General user</td>
<td>GetEvidence()</td>
<td>The account which can send a query to retrieve digital evidence hash value and other relevant case description.</td>
</tr>
</tbody>
</table>

4. Implementation

![Figure 3. Implementation process](image)

- Execute Blockchain
  Ethereum Ethereum private chain

- Deploy Smart Contract
  Deploy Smart Contract on private chain

- User Login
  Login Ethereum wallet

- Operate Function
  Test designed function

![Figure 4. Ethereum wallet operation interface](image)

5. Conclusion

- Functionality: The functionality of blockchain for not only maintaining the integrity of the digital evidence but also supporting effective proof of delivery.
- Security assessment: The rigorous principle of function design reflect the high standard requirement of security in law enforcement applications.

Acknowledgements

This research was partially supported by the Ministry of Science and Technology of the Republic of China under the Grants MOST 108-2410-H-015-001 -.