DFRWS EU 2020
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

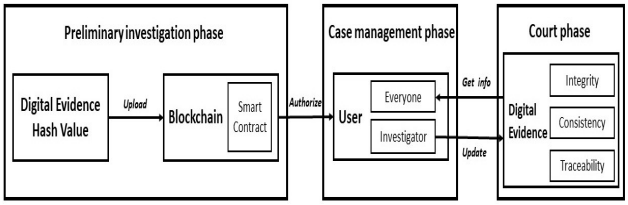

Figure 1. Digital evidence blockchain of custody flow chart

2. Study Framework

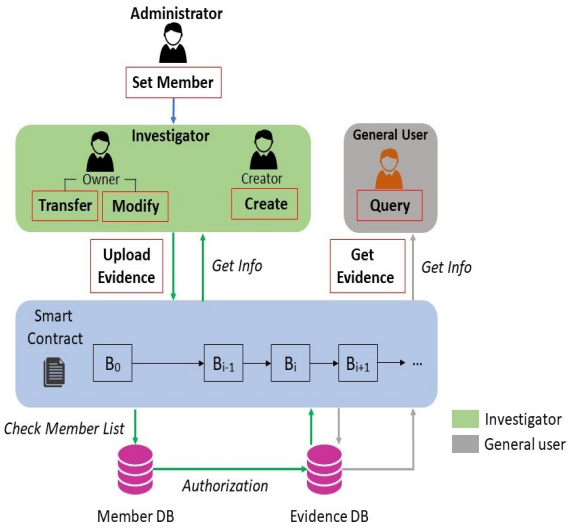

Figure 2. Study framework

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

Role	Funtion	Description
Administrator	SetMember()	The account which can deploy the smart contract and is responsible for setting a list of members to distinguish between investigators or general users.
Creator	CreateEvidence()	The account that can creat the digital evidence hash value and case description to the blockchain.
Owner	Transfer() ModifyEvidence()	The account which holds the digital evidence and case custodian. The account can transfer the custodian and modify the case description.
General user	GetEvidence()	The account which can sent a query to retrieve digital evidence hash value and other relevant case description.

4. Implementation

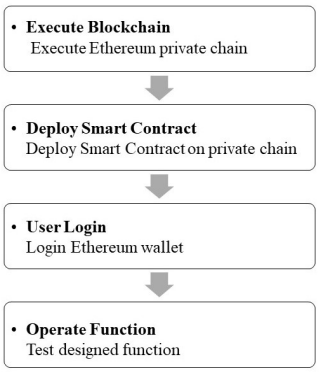

Figure 3. Implementation process

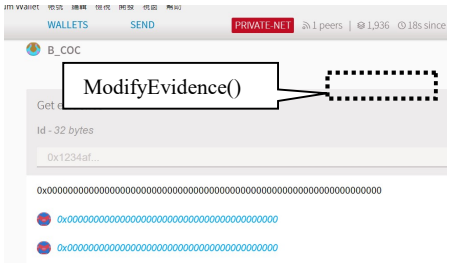

Figure 4. Ethereum wallet operation interface

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 funtion 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 -.