Securing Digital Evidence Information in Bitcoin

A CASE STUDY IN DIRECTORATE GENERAL OF TAXES

DIMAZ ANKAA WIJAYA – MONASH UNIVERSITY
DONY ARIADI SUWARSONO – DIREKTORAT JENDERAL PAJAK

MONASH University

CV – Dimaz Ankaa Wijaya

- Education
  - FMIPA UGM – Sarjana Komputer (2007)
  - Faculty of IT, Monash University – Master of Networks and Security (2016)
- Field of Expertise
  - Digital Forensic, Database, software engineering
  - Network security, software security, cryptocurrency
- Book
  - Mengenal Bitcoin dan Cryptocurrency (2016, Puspantara)
- Contact
  - http://kriptologi.com
  - dimaz@kriptologi.com

Content

- INTRODUCTION
- THE PROPOSED METHOD
- EVALUATION

Introduction

Bitcoin

- Cryptocurrency - Digital payment system
- Created by Satoshi Nakamoto in 2008
- No Trusted Party / central authority e.g. bank
- Relies on cryptographic methods
- Decentralized system – distributed ledger
- Visible transaction history
- Blockchain infrastructure
  - Infeasible to tamper the data

Tax Fraud Preliminary Investigation

- PMK-239/PMK.3/2014 and SE-23/PJ/2015/
- Digital Forensic Procedures for tax fraud preliminary investigation.
- “Borrowing” digital data from taxpayers.
- Official letter as proof of borrowing the data.

Problem

- Official letter is a “trusted system” which is prone to fraud.
- Not a tamper-proof system.

Contribution

- Storing the hash values of digital evidence in Bitcoin transaction.
- Timestamp.
- Tamper-proof.

Related Works

- Asset Management System by using Bitcoin.
- Permanently record data to Bitcoin's blockchain.
- Null Data Transaction
  - Metadata information embedded in Bitcoin transaction

The Proposed Method

Bitcoin Address Generation

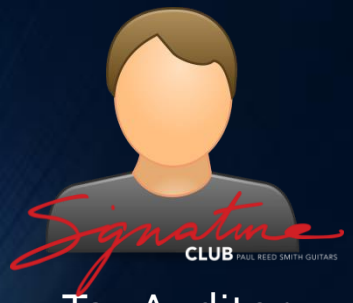
- Each party creates a new public key pair.
  - Tax Auditor address: PRV_ADDR
  - Taxpayer address: VRF_ADDR
- Tax Auditor as a Government official received the public key pair from a parent key pair owned by the Government by using hierarchical deterministic wallet scheme.
  - Government address: GOVT_ADDR

Verifying the Participants

- Digital certificate created by MIT Media Lab.
- Verifying the identity and the public key of each participant.

Data Insertion

- Utilizing 2-of-2 multisignature.
  - (PRV_ADDR, VRF_ADDR) -> TX(GOVT_ADDR, BTC|HASH)
- Inserting the hash value in the NULL DATA transaction.



Tax Auditor

Tax Payer

Bitcoin Transaction
Hash value

Government Address

Evaluation

Limitation and Assumption

- Could not stand against both parties cooperating to tamper the system.
- Assuming that the digital certificate authority always behaves honestly.
- Assuming that the Government (or anyone holding the GOVT_ADDR private key) always behaves honestly.

Security Evaluation

- The non-repudiation characteristic of the digital signatures in the Bitcoin transaction relies on the unforgeability of Elliptic Curve Cryptography.
- The data embedded in Bitcoin transaction proves that no information is tampered.

Performance and Transaction Fee

- Both transactions can be confirmed in the same block.
- A block in Bitcoin is created every 10 minutes (roughly).
- The protocol requires 2 transaction, each requires 10,000 satoshis. Thus it needs 20,000 satoshis.
- As per 31 May 2016, 20,000 satoshis were worth Rp 1,522.

Conclusion

- The protocol provides a failsafe of data tampering case.
- Future works: establishing a data holder for the Bitcoin address owner’s identity.

Thank you!