Financial Fraud Mitigation With Blockchain Technology

OWASP Indonesia Meetup 2017

Dimaz Ankaa Wijaya
4 March 2017 | Mozilla Community Space | Jakarta, Indonesia
Dimaz Ankaa Wijaya, S.Kom., MNS, CSXF

• Education
  – 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)
  – Bitcoin Tingkat Lanjut (2016, Puspantara)

• Contact
  – https://kriptologi.com
  – dimaz@kriptologi.com
Today’s Menu

• Introduction to Bitcoin
• Financial Fraud
• Blockchain
• Summary
Bitcoin is not currency; it's the internet of money!

— Andreas Antonopoulos —
History of Bitcoin

Bitcoin was created by a group of developers lead by the famed pseudonym “Satoshi Nakamoto” who has never revealed his/her real identity. Satoshi could also represent the entire group.

The first Bitcoin transaction happens between Satoshi and Hal Finney. It works!

FATF issues warning about digital currencies.

Amagi makes its first gold sale for Bitcoin!

Bitcoin ruled as currency by Texas judge.

University of Nicosia in Cyprus accepts Bitcoin.

Microsoft accepts Bitcoin

2007

Jan 03

the first Block is mined! Bitcoins now exist!

May 22

SilkRoad opens for business

2009

2010

2011

2013

2014

Dec. 10

Sep. 11

Nov. 19

Bloomberg adds BTC to the ticker!

First Bitcoin ATM is unveiled.

Bitcoin hits $1,000 (after massive drop)

10,000 BTC was spent on one pizza in the first real-world Bitcoin transaction in Jacksonville, FL

Amagi makes its first gold sale for Bitcoin!

FBI shuts down SilkRoad.

Overstock.com now accepts Bitcoin

THE HONEYNET PROJECT
Centralized vs Decentralized

A centralised ledger tracks asset movements within the financial system between institutions.

A distributed ledger eliminates the need for central authorities to certify asset ownership. Instead it is held and verified by many institutions, to cut down on fraud and manipulation.

Source: FT research
How a Bitcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

**WALLETS AND ADDRESSES**

Bob and Alice both have Bitcoin "wallets" on their computers. A wallet is a file that provides access to multiple Bitcoin addresses.

Bob creates a new Bitcoin address for Alice to send her payment to.

Alice tells her Bitcoin client that she'd like to handle the entire amount to Bob's address.

**PUBLIC KEY CRYPTOGRAPHY 101**

When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that an address signed with the private key is valid.

Alice also holds the private key for each of her addresses. The Bitcoin client signs the transaction request with the private key of the address she's transferring bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

**CRYPTOGRAPHIC HASHES**

Cryptographic hash functions transform a collection of data into an unbreakable string, called a "hash value." Every tiny change in the original data drastically changes the resulting hash value. And it's essentially impossible to predict what a hash value will be before it is produced.

The root of evil? The hash value is much easier to generate than it is to predict. The Bitcoin network requires that the new hash value in a transaction be a particular value—specifically, it must start with a certain number of zero's.

**NONCES**

To create different hash values from the same data, Bitcoin uses "nonces." A nonce is a random number that is added to the hash prior to hashing. Changing the nonce results in a wildly different hash value.

Each block includes a "coinbase" transaction that pays out 100 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

**THE MINER'S TASK**

The miners have to solve a problem, and they do it one transaction block at a time. The problem is to find a nonce that, when added to all the transaction data, produces a hash value that starts with a certain number of zeros.

**TRANSACTION VERIFIED**

As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different nonce—and then redo all the work of all the following miners. Such a feat is nearly impossible.
Blockchain Overview

- Individual 'transaction' events
- Blockchain new blocks are added approximately every 10 mins.
- New block of transaction includes a security 'hash' of previous block.
- Multiple computer 'mining' servers check the validity of the blocks in the chain. The quickest to check the latest block gets payment.
- Successful transactions
  - Block validated as 'honest' part of the chain.
  - Rejected
THE HONEYNET PROJECT
Digital Signature

Sender

1. Key Generation:
   - Public
   - Private

2. Signing Algorithm

3. Signature

4. Verification Algorithm

5. Message:
   - Cryptocompare.com
   - sent by signer

Receiver
Bitcoin Transaction

- Receiver
- Sender

Transaction:
- Owner 1's Public Key
- Hash
- Owner 0's Signature
- Owner 1's Private Key

Transaction:
- Owner 2's Public Key
- Hash
- Owner 1's Signature
- Owner 2's Private Key

Transaction:
- Owner 3's Public Key
- Hash
- Owner 2's Signature
- Owner 3's Private Key
Mining
Proof of Work (PoW)

Miners calculate values that match the requirement to create new blocks.

PoW protects the blocks from tampering.
P2P Network

Each server has a complete copy of the blockchain.

They communicate through P2P protocol.
Financial Fraud

• ID Theft
• Cyber Security
• Credit Card Fraud
Financial Fraud (2)

- Falsifying data
  - Enron
  - WorldCom
- Fake document
Financial Scheme
Employing Blockchain in Finance Industry

- Transparent – visible ledger
- Trustless – no central authority needed
- Cryptography – digital signature
- Permanent – blockchain
Privacy Model

• Disconnecting Identities and Transactions

Traditional Privacy Model

Identities → Transactions → Trusted Third Party → Counterparty → Public

New Privacy Model

Identities → Transactions → Public
Blockchain-based Digital Certificate
Multisignature
Visible Transactions

Transaction 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18

INPUTS From
From (previous transactions Joe has received):
Joe

OUTPUTS To
Output #0 Alice’s Address 0.1005 BTC
Transaction Fees: 0.0005 BTC

Transaction 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

INPUTS From
7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18: 0
Alice

OUTPUTS To
Output #0 Bob’s Address 0.0150 BTC (spent)
Output #1 Alice’s Address (change) 0.0845 BTC (unspent)
Transaction Fees: 0.0005 BTC

Transaction 2bbac8bb3a57a2363407ac8c16a67015ed2e88a4388af58cf90299e0744d3de4

INPUTS From
0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2: 0
Bob

OUTPUTS To
Output #0 Gopesh’s Address 0.0100 BTC (unspent)
Output #1 Bob’s Address (change) 0.0845 BTC (unspent)
Transaction Fees: 0.0005 BTC
No Single Point of Failure

- Peer-to-Peer Network
- Multiple nodes
- Synchronization
Eliminating Middleman

- Reducing fees and risks
Customized Transactions

• Escrow transaction
• Hash-locked transaction
• Time-locked transaction
...And Many More!

- Ring Signature (Monero)
- Smart Contract (Ethereum)
Current Usage

• Loyalty Program
Recent Development

- R3CEV
- Hyperledger
- Blockchain of things
- Ms. Azure’s BaaS
Summary

• Blockchain supports transparency in financial industry by using public ledger.
• Blockchain protects the data from unauthorized modification.
• Blockchain supports authentication and non-repudiation in financial transaction by utilizing cryptographic functions.
• These characteristics minimize the risk in financial fraud.
Thank You