Feasibility of Multisig in CoinBlesk

Andreas Albrecht, Adrian Gasparini

Seminar: Internet Economics, University of Zurich
16.10.2014
Agenda

- Introduction to Bitcoin
- CoinBlesk
- Outlook: Multisig in CoinBlesk
- Summary and Discussion
Introduction to Bitcoin
What is Bitcoin?

- Bitcoin is a collection of concepts and technologies that form the basis of a digital money ecosystem.
- Units of currency called bitcoins are used to store and transmit value among participants in the bitcoin network.
- Bitcoin users communicate with each other using the bitcoin protocol primarily via the Internet.

source: Mastering Bitcoin, 2013, O'Reilly Media, Inc.
Bitcoin Overview

User A

private key

Transaction

User B

adapted from: https://bitcoin.org/en/how-it-works
### Transactions

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>1.50 BTC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Outputs</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob</td>
<td>1.00 BTC</td>
</tr>
<tr>
<td>Alice</td>
<td>0.50 BTC</td>
</tr>
</tbody>
</table>

Signed by Alice
Transaction Chains

Transaction 1

Inputs | Value   | Outputs | Value   
---|---------|---------|---------
Alice  | 1.50 BTC| #0: Bob | 1.00 BTC|
       |         | #1: Alice | 0.50 BTC|

Transaction 2

Inputs | Value   | Outputs | Value   
---|---------|---------|---------
Trx1 : 0 | 1.00 BTC| #0: Carol | 0.80 BTC|
       |         | #1: Bob  | 0.20 BTC|

Transaction 3

Inputs | Value   | Outputs | Value   
---|---------|---------|---------
Trx2 : 0 | 0.80 BTC| #0: Dave | 0.50 BTC|
       |         | #1: Carol | 0.30 BTC|
Miners produce the authoritative ledger of all transactions (the block chain).

⇒ Prevents double spending
What is CoinBlesk?

CoinBlesk is a **mobile online wallet** with the unique feature to exchange Bitcoins with **two-way NFC**.

This allows new use-cases such as:

- Offline mode: only one party needs to be connected to the Internet.
- Use case: roaming users with no Internet connection abroad.
- Use case: point-of-sale in areas with bad mobile Internet coverage.

source: https://bitcoin.csg.uzh.ch/
Architecture Overview

CoinBlesk Clients → CoinBlesk Server (Bitcoin Client) → Private keys of CoinBlesk users

TRX

BITSTAMP
CoinBlesk Demo
Load Bitcoins into CoinBlesk

0.50644831 BTC
232.94 CHF (1 BTC = 459.96 CHF)

Your last 3 transactions:
28-08-2014 16:58:05 From: simon, To: MensaBinz, Amount: 0.01075046 BTC (5.00 CHF)
28-08-2014 16:57:37 From: ExchangePoint, To: simon, Amount: 0.01073145 BTC (5.00 CHF)
28-08-2014 16:42:52 From: simon, To: MensaBinz, Amount: 0.01072808 BTC (5.00 CHF)

Pay In

Please submit your bitcoins to the following address. As soon as the incoming payment is verified we update your account balance. This takes approximately 1 hour.

Bitcoin Address:
mwvgmeBG6Pi87vhGnifHt3KVJwLy8GJ8MG

Process Transaction

Hold devices together to process transaction initiated by counterparty

OR

Create new Transaction

Copy To Clipboard
Send to Email
Show QR Code

source: https://bitcoin.csg.uzh.ch/usecases/
Merchant / Customer

Request

Exchange Rate: 1 BTC = 459.05 CHF
Balance: 0.50644831 BTC (232.48 CHF)
Currency: Enter amount in CHF

CHF 5.00
0.01089207 BTC

Establish NFC connection now (Hold devices together)

Send

Exchange Rate: 1 BTC = 459.05 CHF
Balance: 0.50644831 BTC (232.48 CHF)
Currency: Enter amount in CHF

CHF 1.50
0.00326762 BTC

Establish NFC connection now (Hold devices together)

source: https://bitcoin.csg.uzh.ch/usecases/
Multisig

Multisig in Bitcoin and CoinBlesk Integration
Motivation

How to keep Bitcoins safe and secure?
Multi-Signature Idea

- **Idea**: signature of multiple private keys is required to issue a transaction
- **M-of-N scheme**: out of N keys, M are required to spend coins

Multiple ways to implement it
- Outside of Bitcoin: e.g. with secret-sharing, threshold signatures
- In Bitcoin protocol: special “addresses” and scripts

e.g. 2-of-3 and given 3 keys, any 2 keys are sufficient and provide access to the coins
Multisig in Use

- Escrow services / contracts
  - e.g. 2-of-3
  - trusted 3rd party
  - solving dispute
    → Buyer protection

- Securing wallets
  - sophisticated “access” management
  - multiple keys (distributed)

Source: Multisig; Vitalik Buterin; The Future of Bitcoin, Cryptocorp; Securing wallets by integrating a third-party Oracle
Shamir’s Secret Sharing

- Split private key into $n$ pieces
- Require $k$ of pieces to reconstruct private key
- How?
  - Unique polynomial of degree $k-1$, requires $k$ points to be defined
  - Select $n$ arbitrary points on the curve

Advantages
- Simple
- No Bitcoin support required
- Protects key if pieces distributed (key loss, theft, …)

Drawbacks
- Key generation safe?
- Key is reconstructed → one time use
- Not bound to transaction

Source: Adi Shamir - How to share a secret
Threshold Signatures

- Split signing capability among \( n \) participants (key shares)
- require \( k \) shares for a signature
  - Joint signing protocol \( \rightarrow \) cryptography

Advantages
- No Bitcoin support required
- Protects key if pieces distributed (key loss, theft)
- Private key never reconstructed
- Bound to transaction

Drawbacks
- Generation of shares safe?
- Synchronous protocol (online)
- More complex

Source: Steven Goldfeder, Joseph Boneau, Edward W. Felten, Joshua A. Kroll, Arvind Narayanan - Securing Bitcoin wallets via threshold signatures
Multisig in Bitcoin

- Use blockchain and network to implement it
- New address (Pay-to-Script Hash, P2SH)
  - $n$ key pairs associated with an address
  - $k$ signatures required for spending coins
  - enforced by network

Advantages
- Included in Bitcoin
- Independent key pairs
- Bound to transaction and address
- Asynchronous protocol

Drawbacks
- Not anonymous (public chain)
- Bound to an address
- Increased transaction size / fees
- $M$ and $N$ limited due to size

**Multisig Address**

<table>
<thead>
<tr>
<th>Public Key</th>
<th>Private Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>0491bba251...</td>
<td>5JaTXbAUmf...</td>
</tr>
<tr>
<td>04865c4029...</td>
<td>5Jb7fCeh1W...</td>
</tr>
<tr>
<td>048d2455d2...</td>
<td>5JFjmGo5Fw...</td>
</tr>
</tbody>
</table>

1. **Generate 2-of-3 multisig address**

   - **TRX:** (some tid)
   - **In:** 3c9018e8d5...
   - **To:** (some address)
   - **Redeem Script:** 52410491bb...

2. **Receive some Bitcoins**

3. **Spend some Bitcoins**

   - **Address:** 3QJmV3qfvL... *(send BCT to this address)*
   - **Redeem Script:** 52410491bba251...4104865c4029...41048d2455d2...53ae

Based on example by: Gavin Andresen (https://gist.github.com/gavinandresen/3966071#file-twoofthree-sh)
Multisig in CoinBlesk: 2-of-2

Advantages
- Increased trust
- Compromised server or client gives no access to coins
- Legal situation? bank license?

Drawbacks
- Coins lost if one key destroyed
- Backup of user’s key required (user is responsible)
Multisig in CoinBlesk: 2-of-3

Advantages
- Compromised server or client gives no access to coins
- Legal situation? bank license?
- User does not need backup

Drawbacks
- Access to coins without user
- May require trusted 3rd party
- Or operator generates 2 keys
Summary and Discussion
Summary

- **Bitcoin Introduction**
  - Digital currency
  - Transactions
  - Blockchain and Mining

- **CoinBlesk**
  - Paying with Bitcoins → NFC payment system
  - Mobile clients and server

- **Multisig**
  - Multiple keys instead of one
  - New address type (P2SH)
  - New possibilities: escrow, securing access, contracts
  - Shamir, Threshold Signatures, Bitcoin Multisig
  - Scenarios for CoinBlesk
Bitcoins

Do you have any Bitcoin experiences?
Do you own Bitcoins?
Why / Why not?
Saftey of Bitcoins

How do (would) you store your wallet?

- Centralized service?
- On computer (online)
- Cold storage (offline, paper wallets, hardware)
Safety and Trust

Are you afraid of losing your coins?
Do you trust Bitcoin companies?
(e.g. Coinbase, BTC-e, Bitstamp, GreenAddress, …)
Did you know of the multisig concept?
Multisig in CoinBlesk

What would you prefer and why?

- Without multisig (keys on server)
- What if 2-of-2 implemented?
- What if 2-of-3 with trusted 3rd party?
What are the most important issues that need to be addressed for the success of Bitcoin?
Does multisig help? How?
References

Bitcoin

- Bitcoin Project - https://bitcoin.org/
- Bitcoin Wiki - https://en.bitcoin.it

CoinBlesk

- CoinBlesk - https://bitcoin.csg.uzh

Multisig

- Two of Three commands - Gavin Andresen https://gist.github.com/gavinandresen/3966071#file-twoofthree-sh
References

- Adi Shamir - How to share a secret - http://dl.acm.org/citation.cfm?id=359176
- Securing wallets by integrating a third-party Oracle - https://cryptocorp.co/technology.htm
References

Images

• Bitcoin - How it works - https://bitcoin.org/en/how-it-works
• MTGOX where is our money - Kiyoshi Ota / Bloomberg
• Bitcoin robber - http://www.bitcoinblog.me/the-wild-west-of-digital-currency/
• Stop malware - http://betanews.com/2013/06/18/microsofts-emet-4-adds-even-more-malware-blocking-power/
• Fighting business people - http://www.dealerelite.net/profiles/blogs/will-you-fight-to-win-a-customer