UNIVERSITÀ
DI PARMA

Wallet multi-sig e attacco informatico a Bitfinex (2016)

Corso di Sicurezza Informatica (a.a. 2024/25)

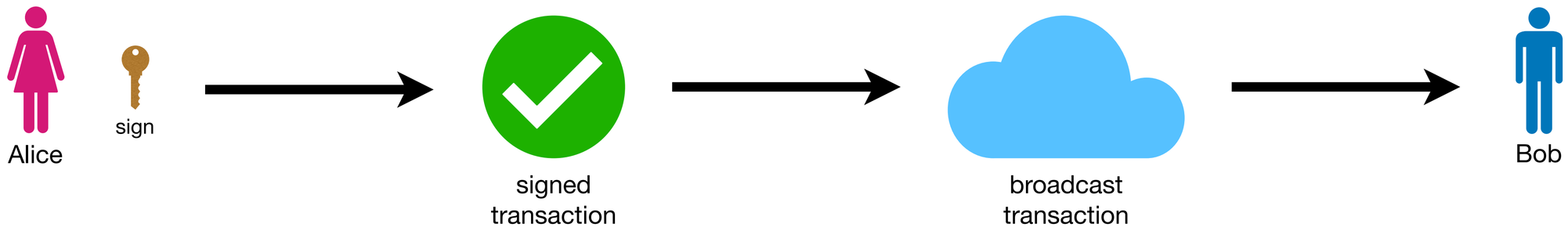
Merenda Saverio Mattia

Contenuto del seminario

- ***Capire*** il funzionamento dei wallet multi-sig nella blockchain
- ***Esplorare*** l'attacco informatico a Bitfinex (~120.000 bitcoin rubati)
- **Valutare** l'impatto e le implicazioni di questo evento

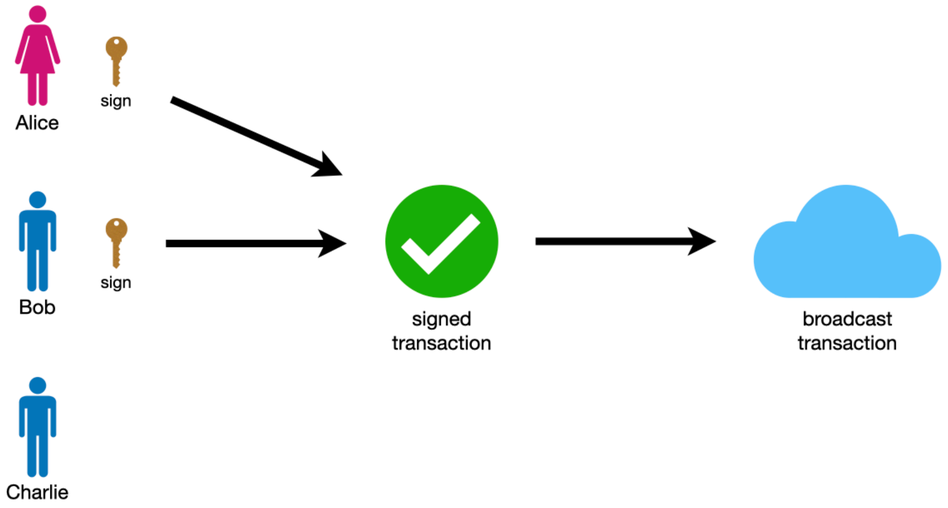
Funzionamento di una transazione standard

- Ogni utente possiede una **coppia di chiavi**:
  - **Pubblica:** identifica l'utente nella rete
  - **Privata:** firma le transazioni



Funzionamento dei wallet multi-sig

- ***Schema N-of-M:*** almeno N chiavi su M totali sono necessarie per firmare una transazione
- Benefici principali:
  - **Maggiore sicurezza** grazie alla distribuzione delle chiavi
  - **Riduzione dei rischi** legati alla compromissione di una singola chiave



Configurazione multisig di Bitfinex

- ***Schema 2-of-3*** con BitGo
  - ***Chiave 1:*** Bitfinex
  - ***Chiave 2:*** BitGo
  - ***Chiave 3:*** backup offline
- **Necessarie due firme** per ogni transazione: una di Bitfinex e una di BitGo
- Collaborazione con BitGo per sicurezza aggiuntiva tramite firme multiple

L’attacco del 2016

- **Compromessi i sistemi di Bitfinex:** accesso alla chiave privata della piattaforma
- **Transazioni fraudolente** inviate a BitGo: approvate automaticamente senza controlli adeguati
- **Mancanza di monitoraggio** per rilevare comportamenti sospetti, come il volume anomalo di transazioni
- **Risultato:** trasferimento di ~120.000 bitcoin agli indirizzi degli hacker

Impatto e implicazioni

- Gli hacker hanno sfruttato:
  - **Compromissione** della chiave privata di Bitfinex
  - **Approfondimenti insufficienti** nei controlli automatici di BitGo
- Indagini condotte da FBI:
  - **Analisi forense** su blockchain per tracciare i fondi rubati
  - **Recupero di dati digitali:** un file criptato nel cloud conteneva chiavi e indirizzi
- Risultato delle indagini:
  - **Arresto** dei responsabili (Lichtenstein e Morgan)
  - **Recupero** di oltre 94.000 bitcoin (3,6 miliardi di dollari nel 2022)

Q&A

Wallet multi-sig e attacco informatico a Bitfinex (2016)

Corso di Sicurezza Informatica (a.a. 2024/25)

Merenda Saverio Mattia

UNIVERSITÀ
DI PARMA

Bibliografia

1. *U.S. Department of Justice: justice.gov/usao-dc/2016-bitfinex-hack*
2. *Wikipedia: wikipedia.org/wiki/2016_Bitfinex_hack*
3. *Bitbo: calendar.bitbo.io/bitfinex-hack/*
4. *The Sun: thesun.co.uk/news/17594836/heather-morgan-husband-ilya-lichtenstein/*
5. *Associated Press: apnews.com/article/bb592f0f06cdd8c2854a1a2259660c70*
6. *The Cyber Express: thecyberexpress.com/hack-of-bitfinex-for-laundering/*