EECS 3482

Bitcoin Security and Attack on Mt. Gox

Adrian Apelo
Sani Patel

April 06, 2015

Background Information

- Bitcoin:
  - Decentralized digital currency, like virtual cash
  - No financial institutions mediating transaction (low transaction fee)
  - Transferred peer-to-peer
  - Issued in 2008, by Satoshi

HOW DO BITCOINS WORK?

'Miners' create Bitcoins by using computers to solve mathematical functions. The same process also verifies previous transactions

Bitcoin exchanges will trade between conventional currencies and Bitcoin, offering a way into the market for non-miners, as well as a way to cash out

Users download a Bitcoin 'wallet' that works a little like an email address, providing a way to store and receive currency. Bitcoins can be transferred from one wallet to another using a web browser or a phone app

Businesses create a wallet in the same way as an individual user, typically using a website button to enable a Bitcoin payment. For in-the-flesh enterprises, QR codes can be used to let customers pay quickly and easily

Attack on MT.GOX

- Mt. Gox – Bitcoin exchange based in Japan
  - By 2013, it was responsible for 70% of all Bitcoin transactions

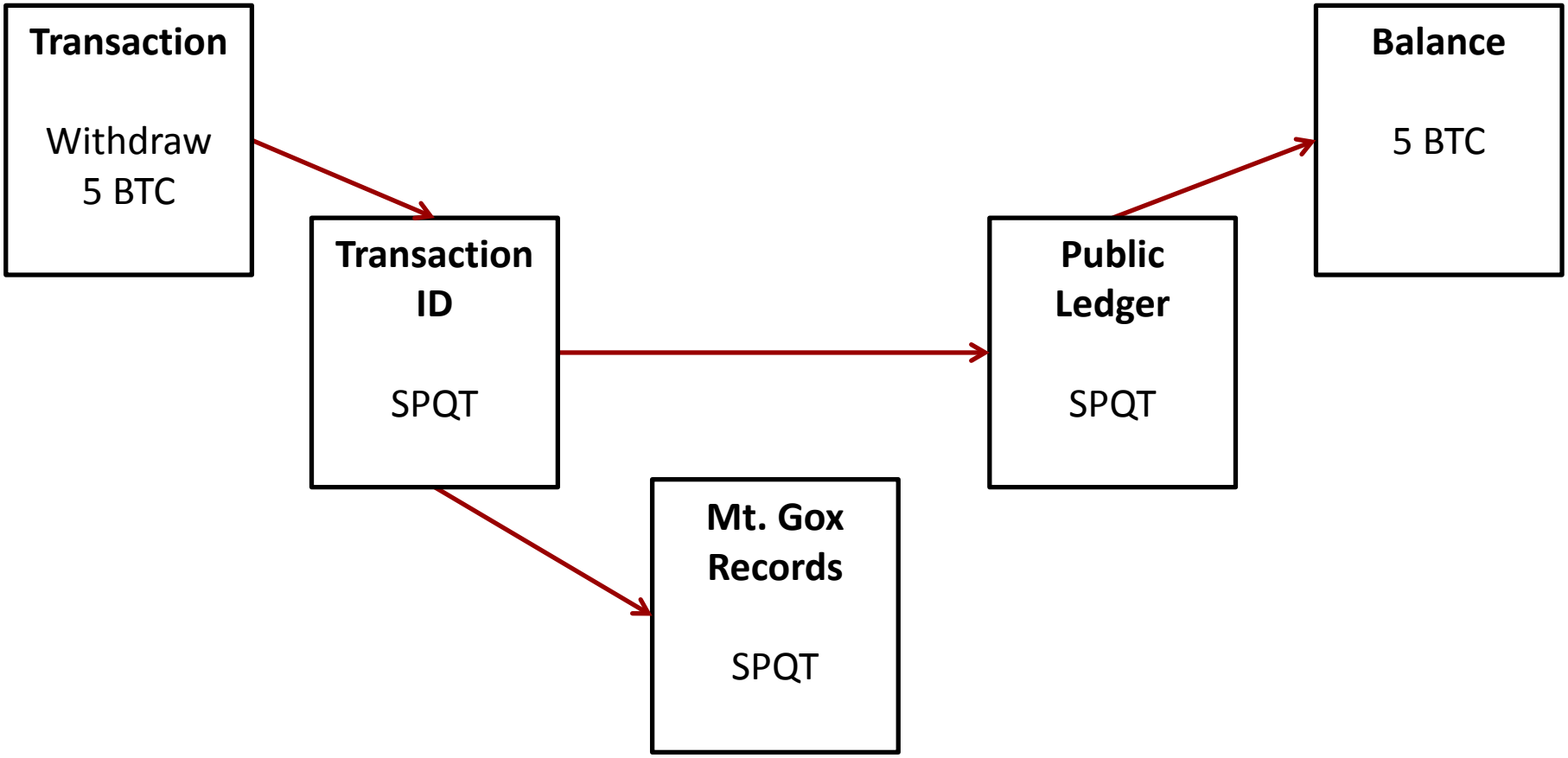
- February 7, 2014, all Bitcoin transactions halted by Mt. Gox, stating the issue was due to transaction malleability

- February 28, 2014, Mt. Gox announced 850,000 bitcoins worth $450 million USD were stolen

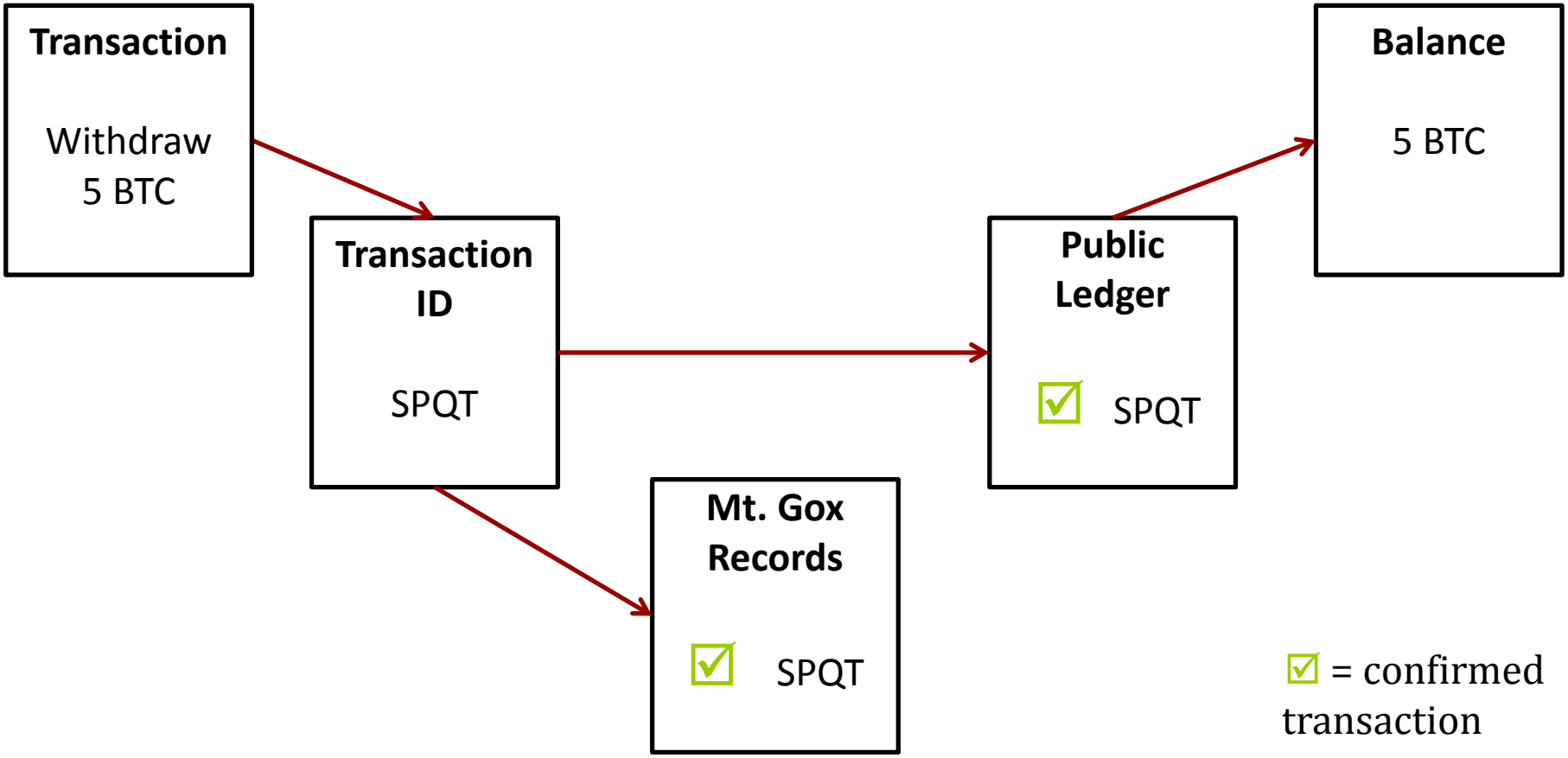
Transaction Malleability… The Basics

- Every transaction is assigned a unique transaction ID, and is recorded in a shared public ledger (blockchain)
- The ledger is maintained by bitcoin **miners**. If you have a well-formed transaction and want it to appear in the ledger, you send the transaction to miners
- "If it appeared in the ledger, you know the funds have been transferred."

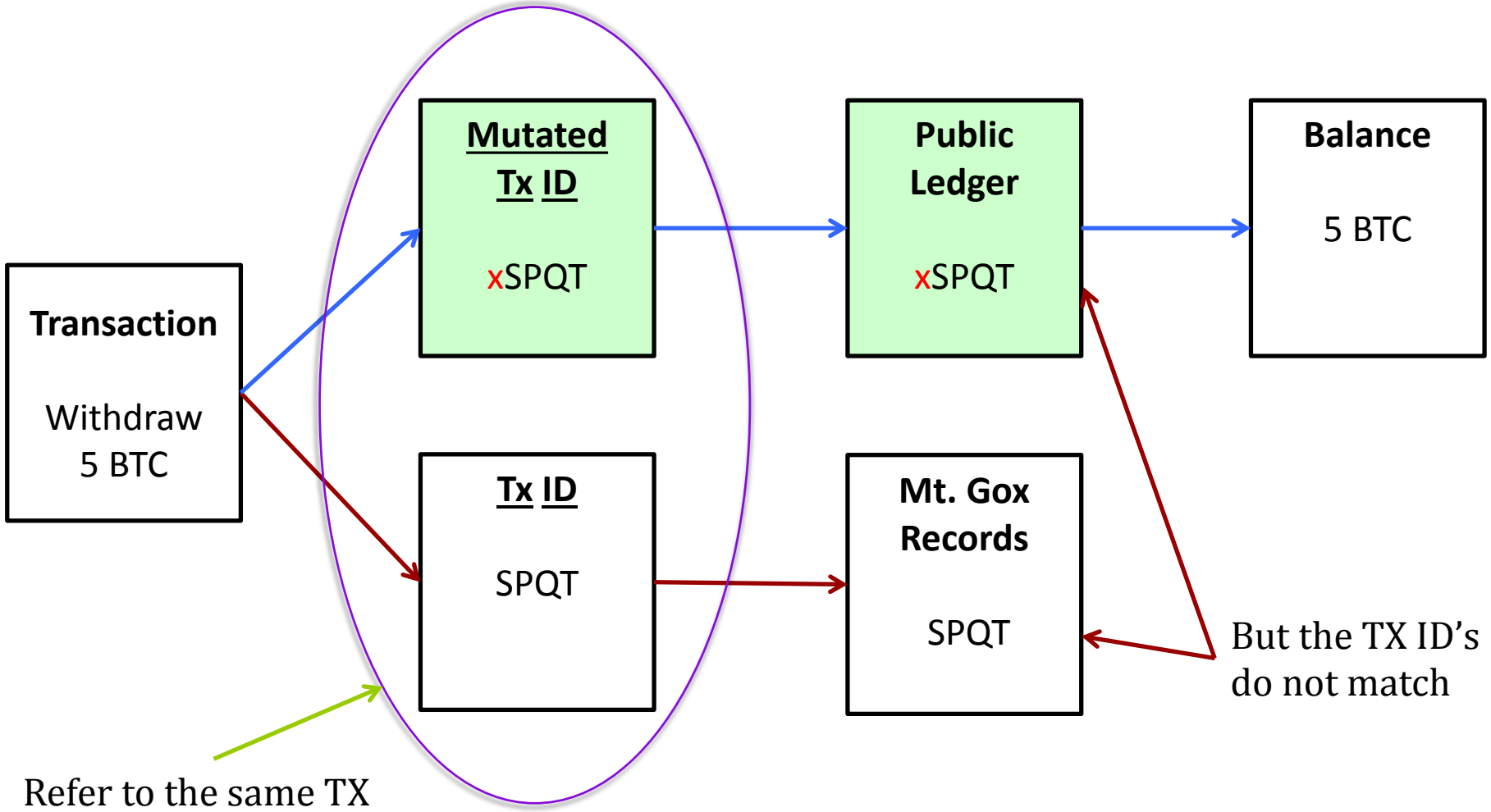
Normal Transaction... Scenario 1



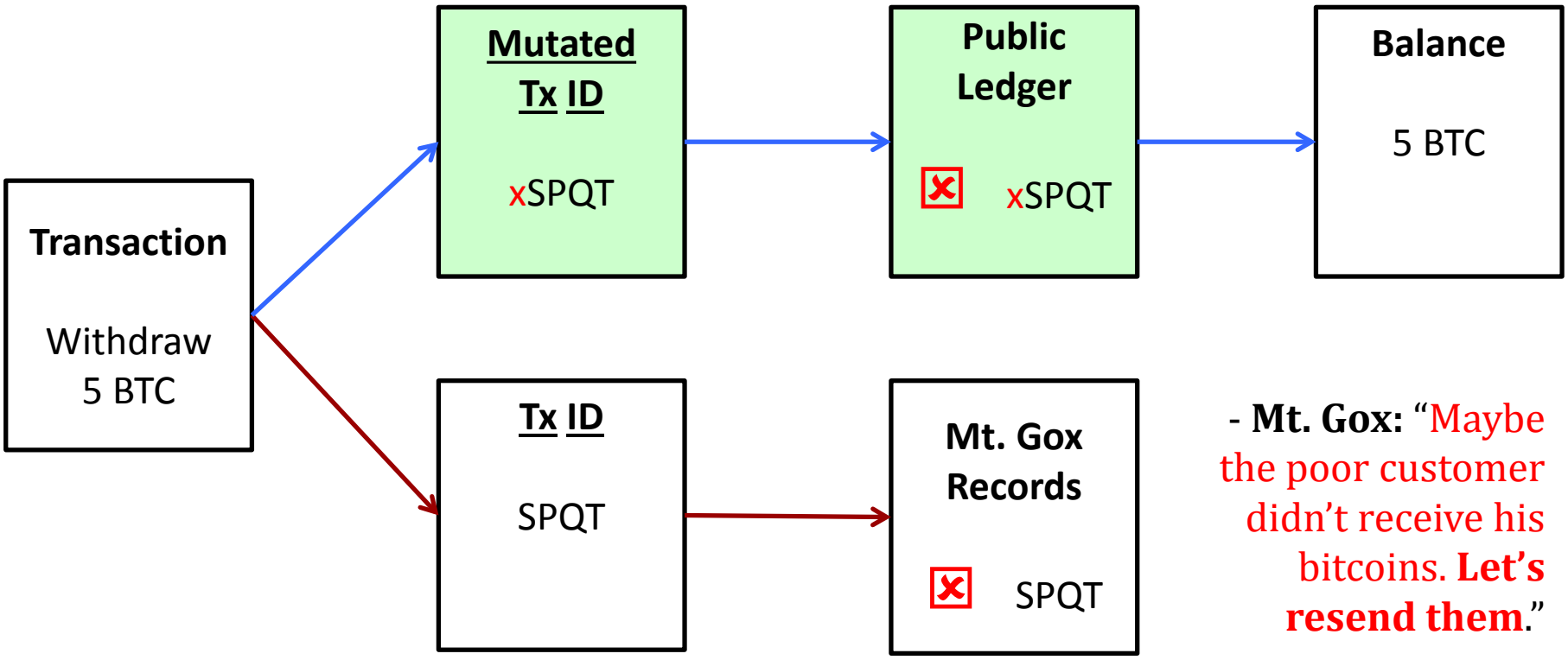
Normal Transaction… Scenario 1



Transaction Malleability… Scenario 2



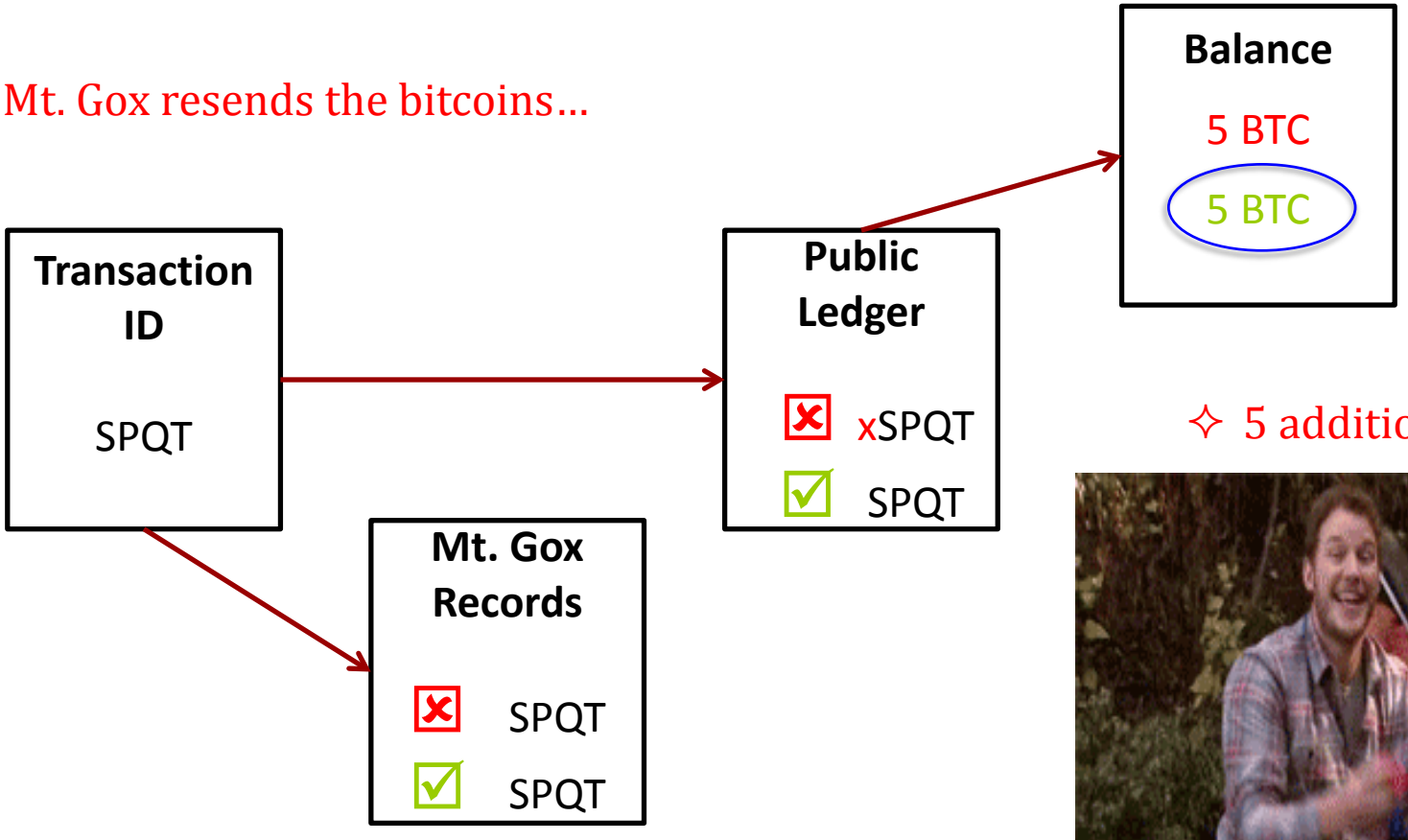
Transaction Malleability… Scenario 2



- **Mt. Gox:** "Maybe the poor customer didn't receive his bitcoins. **Let's resend them**."

Transaction Malleability… Scenario 2

- Mt. Gox resends the bitcoins…



✧ 5 additional Bitcoins.

Who and When Exactly?

- Who?
  - Mark Karpelès?
- When? Two theories…
  - Mt. Gox didn't conduct any audits, so the bitcoins could have been stolen back in 2011
  - February 2014, Mt. Gox was receiving 150,000 DDoS attacks per second (mostly from US and Europe)

How to Secure your Bitcoins…

- Choose a secure and unhacked BTC exchange (check if insurance provided)
- Store bitcoins in a safe environment (i.e. on an external hard drive)
- Encrypt your bitcoin wallet (software: TrueCrypt, Irzip)
- Use up-to-date bitcoin software (software: Bitcoin Core, MultiBit)
- Additional Security:

https://en.bitcoin.it/wiki/Securing_your_wallet

Questions…

1. What is Mt. Gox?

2. List one advantage of using bitcoins over fiat money.

3. List two ways to secure a bitcoin wallet.

Answers…

1. Mt. Gox was a **Bitcoin exchange**. In February 2014, it suspended all its activity owing to the loss of USD $450 million.

1. Minimal to no transaction fee.

1. Secure bitcoins by: 1) using secured exchange (such as Bitfinex), and 2) using latest software (such as MultiBit).

References…

1. Bitcoin Paper: https://bitcoin.org/bitcoin.pdf
2. https://web.archive.org/web/20140210122955/
3. https://www.mtgox.com/press_release_20140210.html
4. http://www.wired.com/2014/03/bitcoin-exchange/
5. http://fortune.com/2015/01/05/bitstamp-bitcoin-freeze-hack/
6. https://bitcointalk.org/index.php?topic=499580
7. http://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency

References…

8. https://en.bitcoin.it/wiki/Securing_your_wallet
9. https://bitcointalk.org/index.php?topic=17240.0
10. https://bitcointalk.org/index.php?topic=497289.0
11. https://gigaom.com/2014/02/28/game-over-for-mtgox-bitcoin-exchange-has-filed-for-bankruptcy-protection-reports-say
12. http://hackingdistributed.com/2014/03/01/what-did-not-happen-at-mtgox/

The End