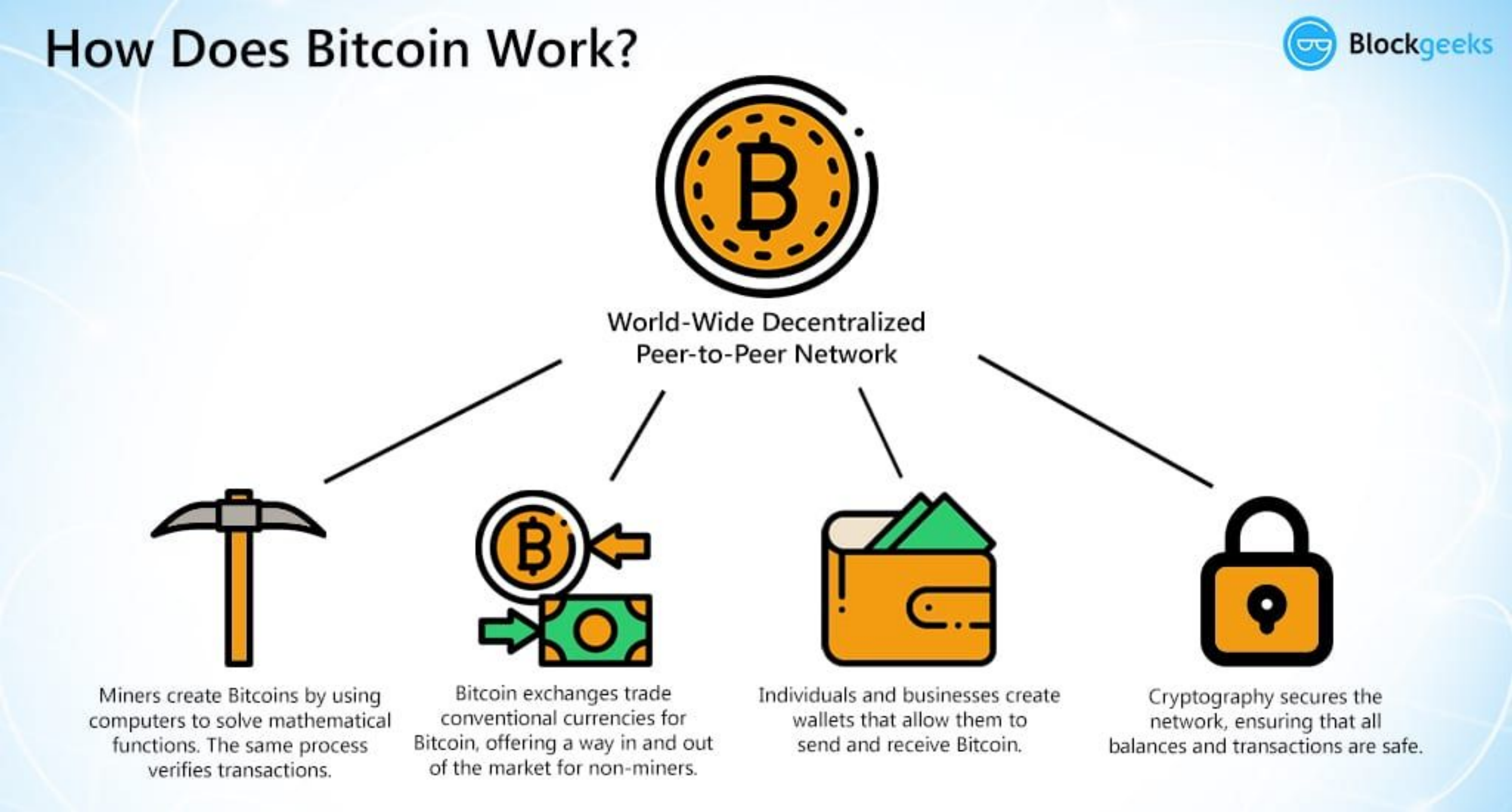
Mt. Gox Bitcoin Heist

Gousia Sultana
Dave Marshall
Yae Jin Park

Cryptocurrency and Bitcoin

- Means of Peer-to-Peer transaction of online payment: electronic cash
  - No middleman (e.g. centralized banks)
- Bitcoin is the first cryptocurrency that was fully developed that can be exchanged like real currencies
- Highly complex application of cryptography to ensure authenticity of transaction



How Does Bitcoin Work?

World-Wide Decentralized Peer-to-Peer Network

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

Bitcoin exchanges trade conventional currencies for Bitcoin, offering a way in and out of the market for non-miners.

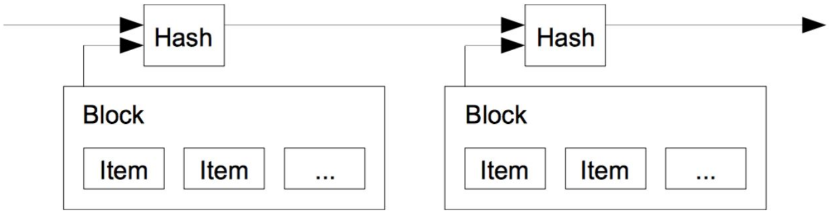
Individuals and businesses create wallets that allow them to send and receive Bitcoin.

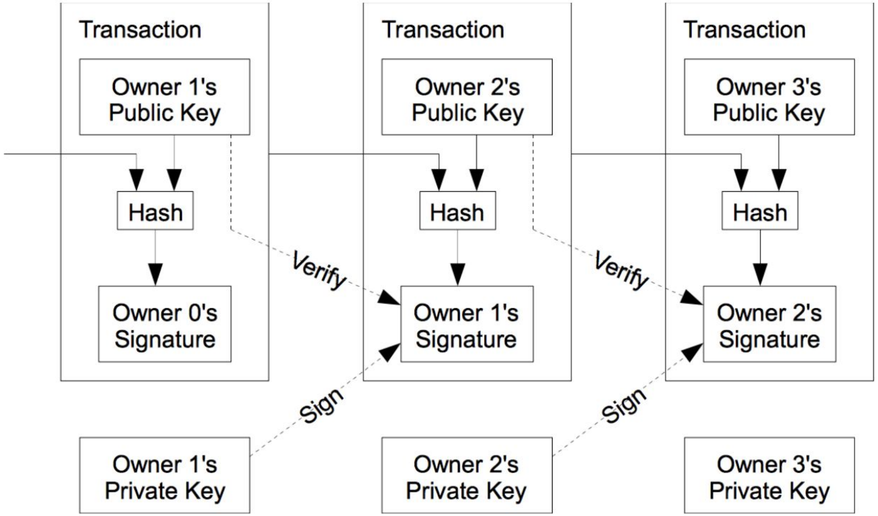
Cryptography secures the network, ensuring that all balances and transactions are safe.

Image: https://blockgeeks.com/guides/what-is-bitcoin/

Blockchain and Bitcoin Wallet

- Decentralized system, no regulating party, in need of security for transaction: Blockchain
- Bitcoin is a part of the blockchain, so technically not able to be “stored” in a place





Images: https://medium.com/crypto-currently/what-exactly-is-bitcoin-3d5417bff390

Blockchain and Bitcoin Wallet

A wallet is a collection of the keys to access bitcoin

- Hot wallet (online)
- Cold wallet (offline)

Mt. Gox exchange had both, and their hot wallets were hacked.

Cryptocurrencies are risky because no global regulation on exists at the moment.

- Some countries enforce regulations within their own jurisdiction. Not all do.
- Some countries only issue warnings about the dangers of bitcoin exchange.

Mt. Gox Heist Overview

Mt. Gox was the biggest bitcoin exchange - handled up to 70% of all BTC transactions

Failure with security maintenance allowed the biggest bitcoin theft known

Image: https://www.businessinsider.com/bitcoin-price-traders-angry-over-mt-gox-trustees-bitcoin-sales-2018-3

Before the Incident - Timeline

2007

- In July, Jed McCaleb started the online site “Magic: The Gathering ”

2010

- He repurposed it as “Mt.Gox: The gathering for online exchange "

2011

- Finally in 2011, he sold it to Mark Karpeles. Karpeles rewrote the backend software and made it into the world famous bitcoin exchange platform

2013

- By 2013 it was handling 70% of the world’s bitcoin trading

Before the Incident - Vulnerabilities

Lack of 2FA

Weak encryption technique

MD5 hash algorithm

The programming language PHP

No Test Environment

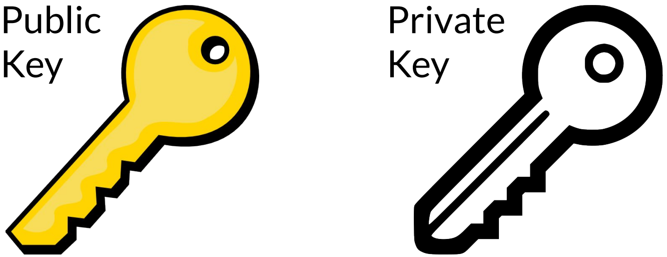
Before the Incident - Vulnerabilities Cont’d

Accessibility rights

Leak in hot wallet

Flawed BTC Tracking

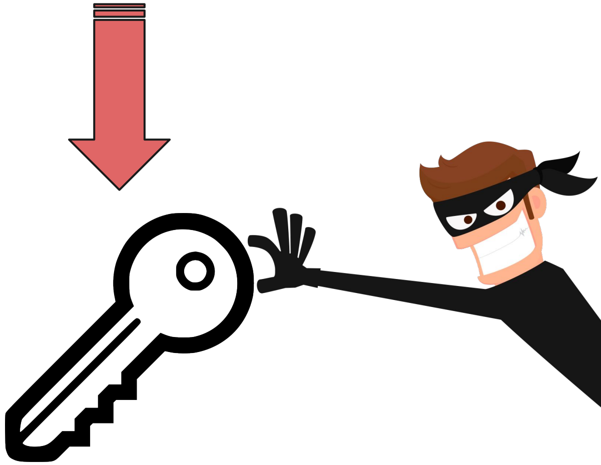
The Attack



Hot wallet private key copied around September 2011

Duplicate Hot wallet set up externally

Funds siphoned off until Feb. 2014



The Attack

Funds laundered through many wallets and exchanges

More was stolen as BTC was moved from cold to hot wallets

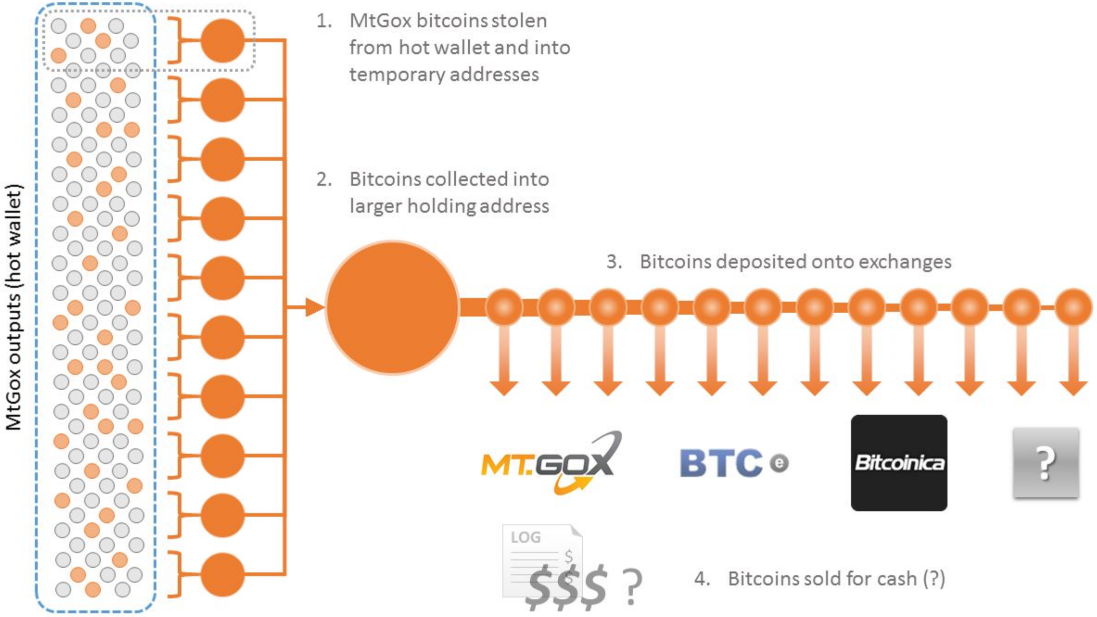

MtGox outputs (hot wallet)
1. MtGox bitcoins stolen from hot wallet and into temporary addresses
2. Bitcoins collected into larger holding address
3. Bitcoins deposited onto exchanges
MT.GOX
BTC e
Bitcoinica
?
LOG
$
$$$?
4. Bitcoins sold for cash (?)

Image: https://blog.wizsec.jp/2015/04/the-missing-mtgox-bitcoins.html

Aftermath

650,000 BTC =

$39,000	on	July 17, 2010
$3,250,000	in	September 2011
$357,500,000	on	Feb. 28, 2014
$4,771,000,000	on	Dec. 3, 2019

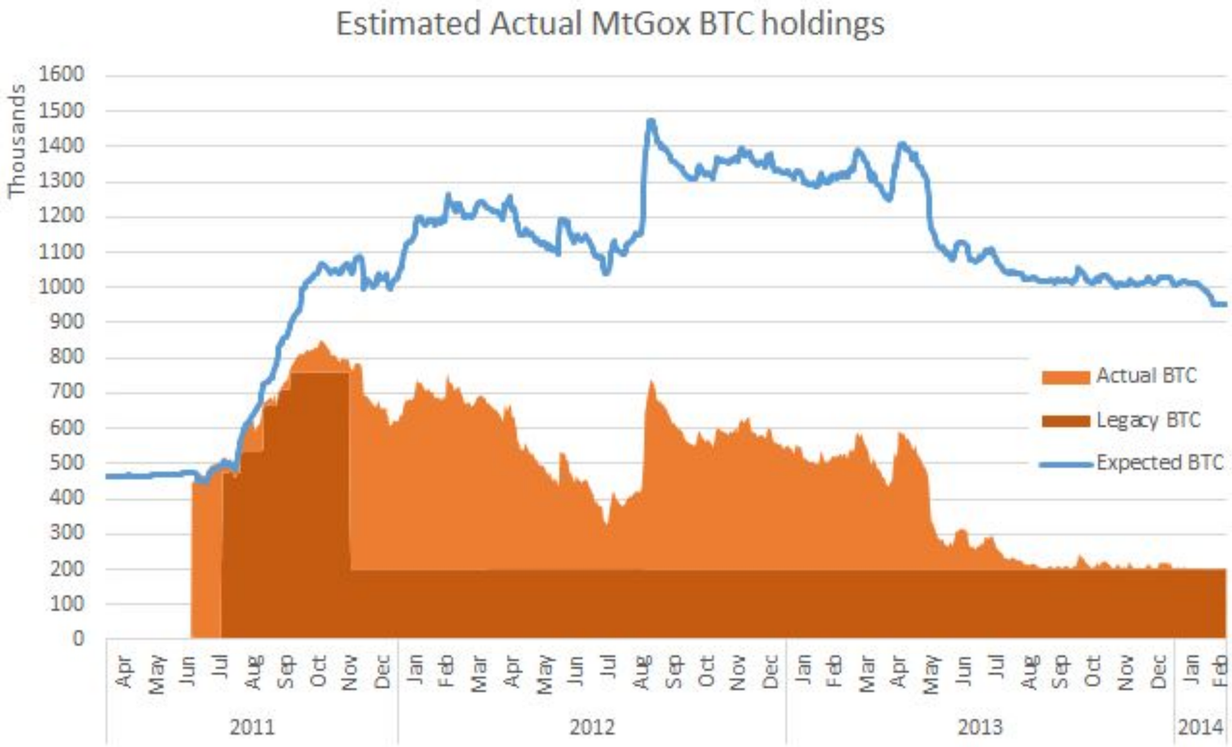


Image: https://blog.wizsec.jp/2015/04/the-missing-mtgox-bitcoins.html

Aftermath

February 28th, 2014: bankruptcy declared

Mt. Gox never recovered

Russian man arrested in 2017 for money laundering

Fin.