

CRACKING MT.GOX

Investigating one of the biggest
digital heists in history – from the outside

KIM NILSSON



WIZSEC
Bitcoin Security Specialists

- Brief history reminder
- Basics of blockchain analysis
- Acquiring the missing pieces
- Findings so far

Early 2014



BREAKING NEWS

WITHDRAWALS HALTED AT MTGOX



MTGOX CUSTOMERS DEMAND ANSWERS





MTGOX CEO ANNOUNCES BANKRUPTCY



ALSO IN THE NEWS

- MtGox data leaked (March 2014)
- The “Willy Report” (May 2014)
- First creditor meeting (July 2014)
- Kraken selected to assist bankruptcy (November 2014)

BEHIND THE NEWS

- Multiple creditor initiatives
 - Acquire and/or rehabilitate MtGox
 - Lawsuits to recover funds
 - Gain access to investigate



- “Will this get handled properly?”
- Individual efforts < focused group effort
 - ✓ Competence
 - ✓ Local presence
 - ✓ Determination
 - ✓ Wannabe hacker group name

PUBLIC AUDIT?

- First-of-a-kind opportunity
- Audit and forensic investigation using public data
 - Blockchain + additional leaked data
- $(\text{Deposits}) + (\text{buys}) - (\text{withdrawals}) - (\text{sells}) = (\text{final balance})$
- Reconcile deposits and withdrawals against blockchain
- $(\text{All MtGox spends}) - (\text{valid withdrawals}) = \text{theft} ?$

OBJECTIVES

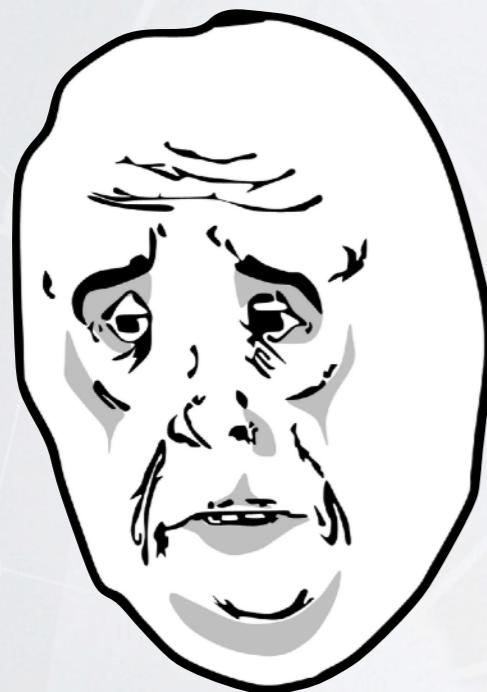
- Verify existing research
- Approach insiders
- Get better data
- Dig deeper
- Assist official investigations

OBJECTIVES

- Verify existing research
- Approach insiders
- Get better data
- Dig deeper
- Assist official investigations

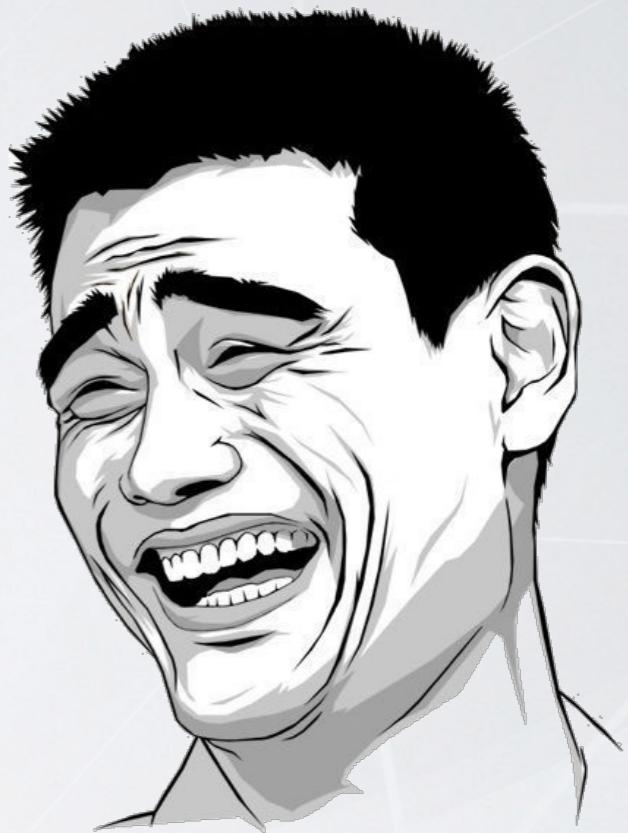


*“Hey Mark, can we get a copy
of the MtGox database?”*



OKAY

LOL NO



RECONCILING DATA

- Leaked log of deposits and withdrawals
 - Date and amount
- Match blockchain outputs to logged events
- Problem: too large for naive approach

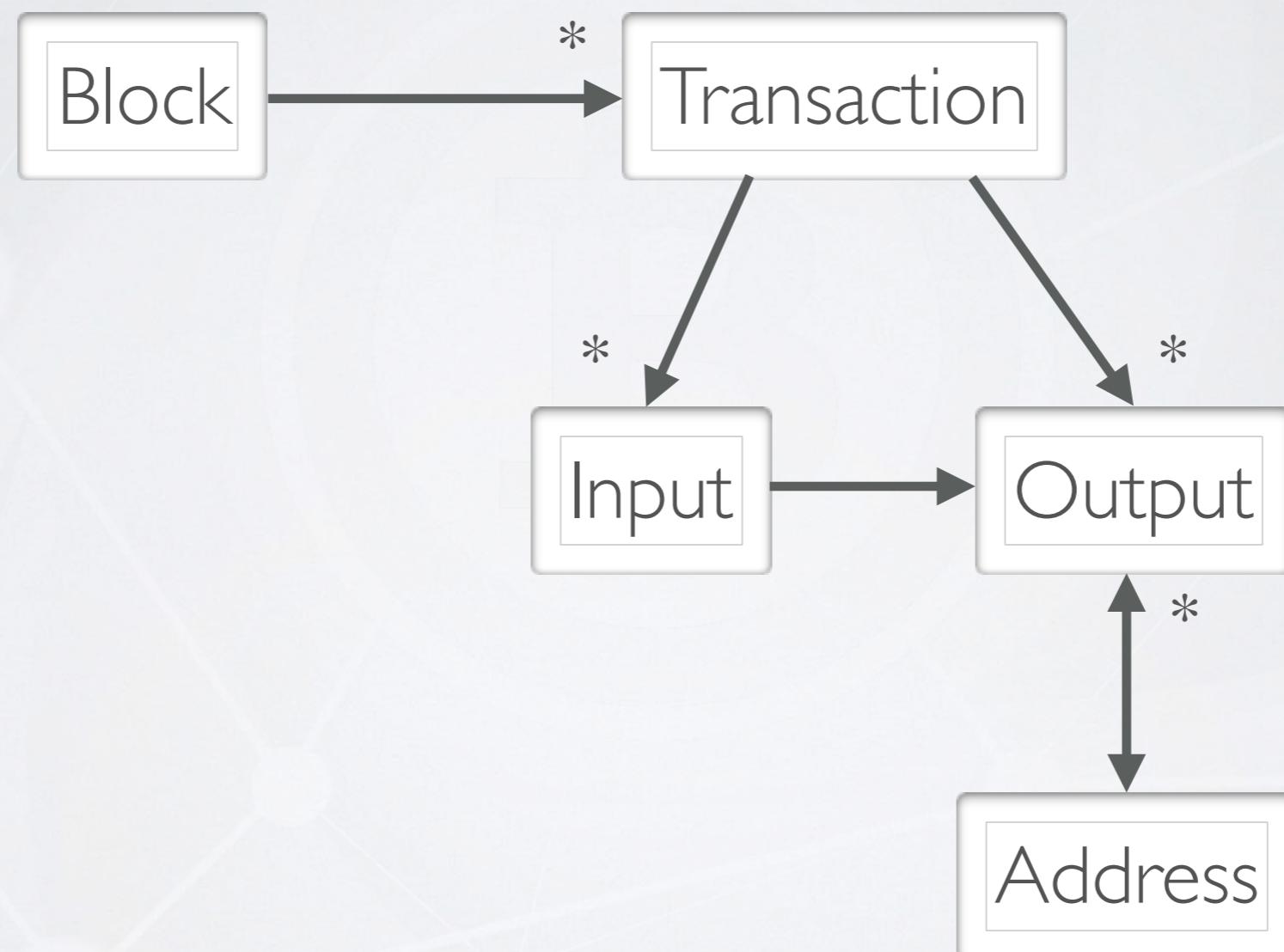
PARSING THE BLOCKCHAIN

- About 30–40 GB of blockchain at the time
- Approach 1: Scan entire blockchain, beginning to end, while looking for target outputs to match
 - Slow: 30m~8h depending on query complexity
- Approach 2: Build a fast index of the blockchain entities and relationships

BLOCKCHAIN DATA

- Block: previous hash, merkle root, timestamp, ...
 - + list of transactions
- Transaction: version, locktime
 - + list of inputs
 - + list of outputs
- Output: value, scriptPubKey
- Input: transaction hash, output index, seq#, scriptSig

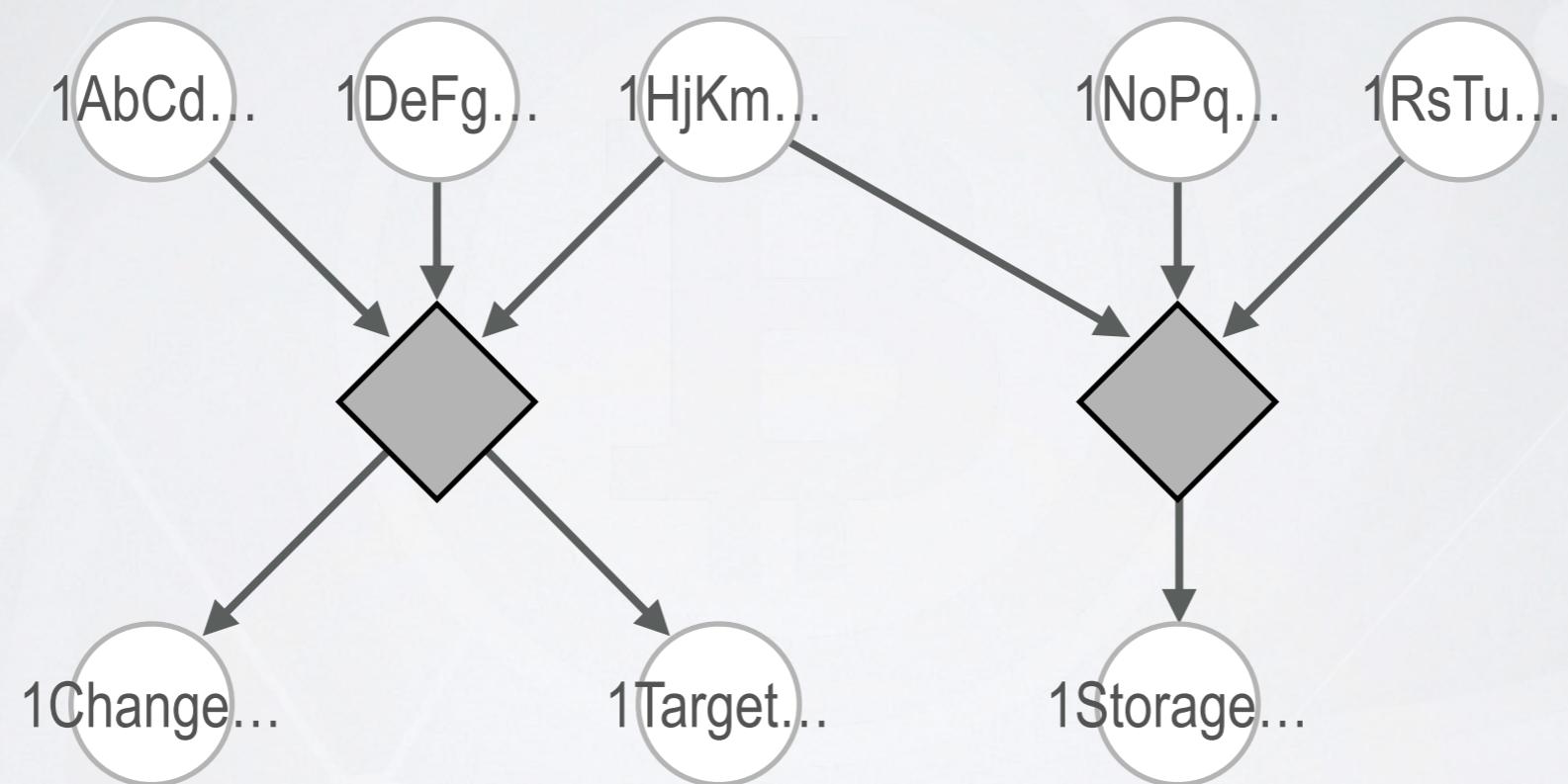
BLOCKCHAIN RELATIONS



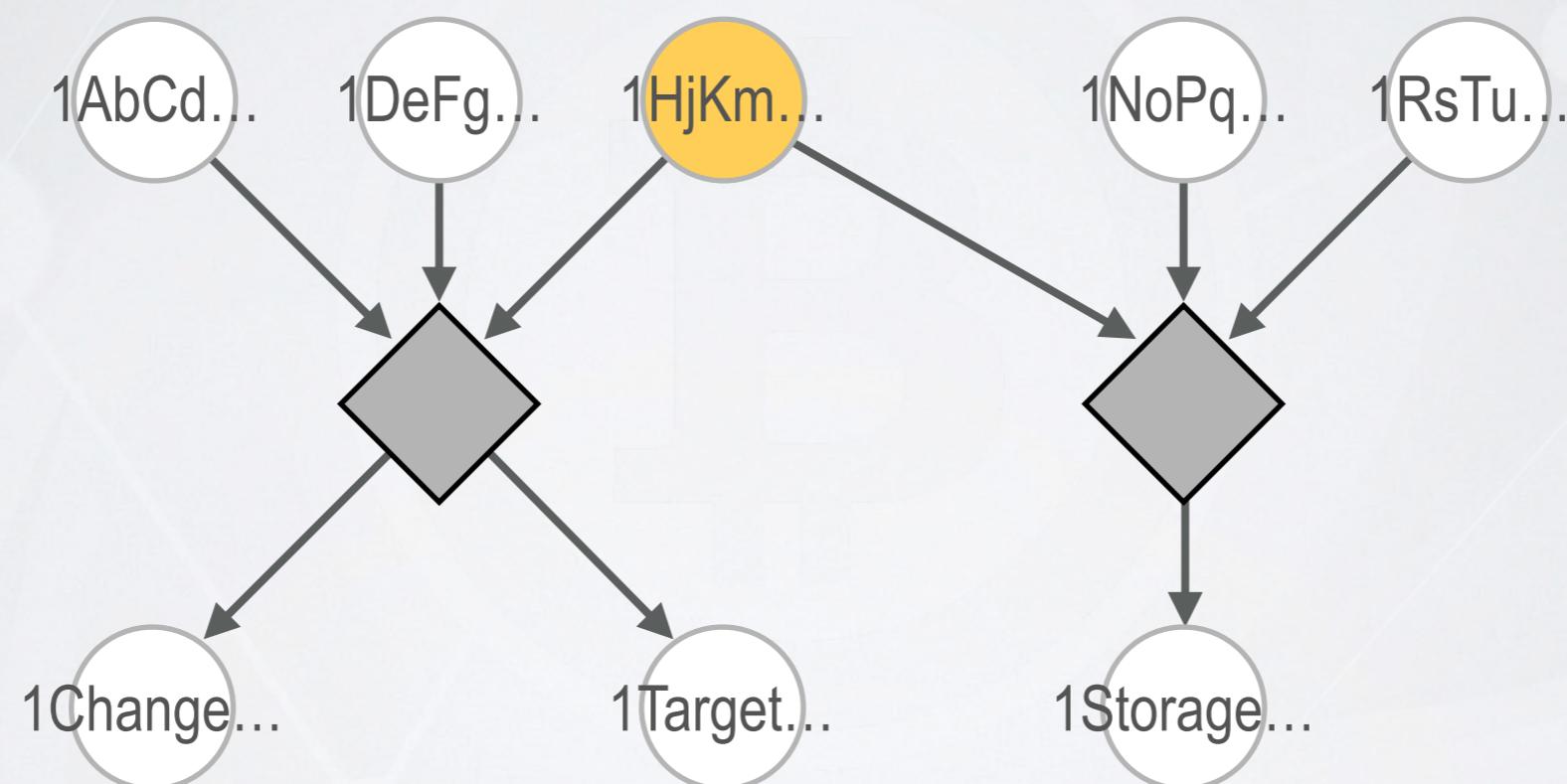
BLOCKCHAIN INDEX

- Keep only essential data: identifiers, relationships, amounts
- Optimize for fast lookups and traversal
 - $O(\log n)$ to look up something by identifier
 - $O(l)$ to get related entities
- Compact representation suitable for memory mapping
- 35 GB → 5 GB

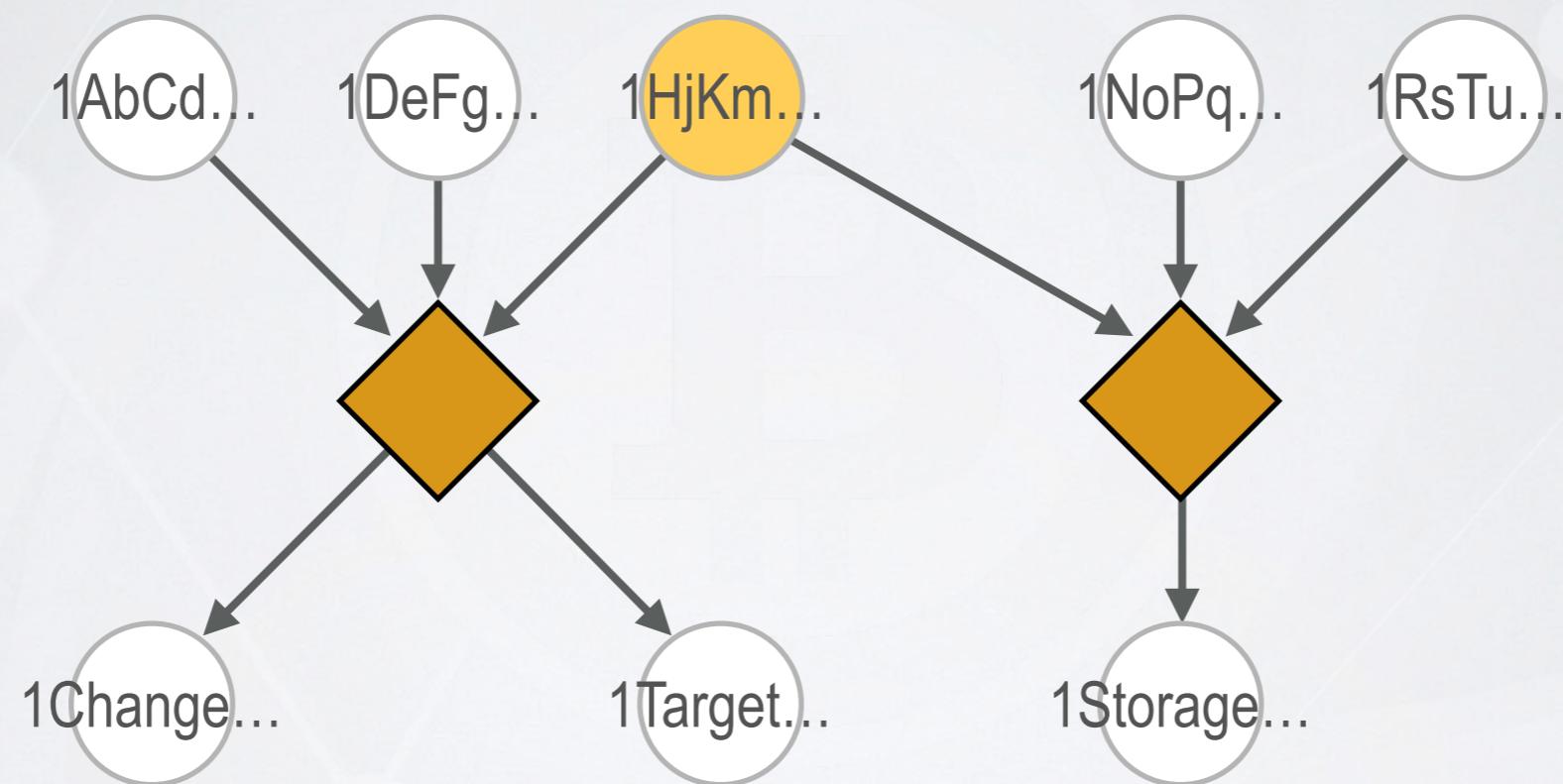
RECONSTRUCTING WALLETS



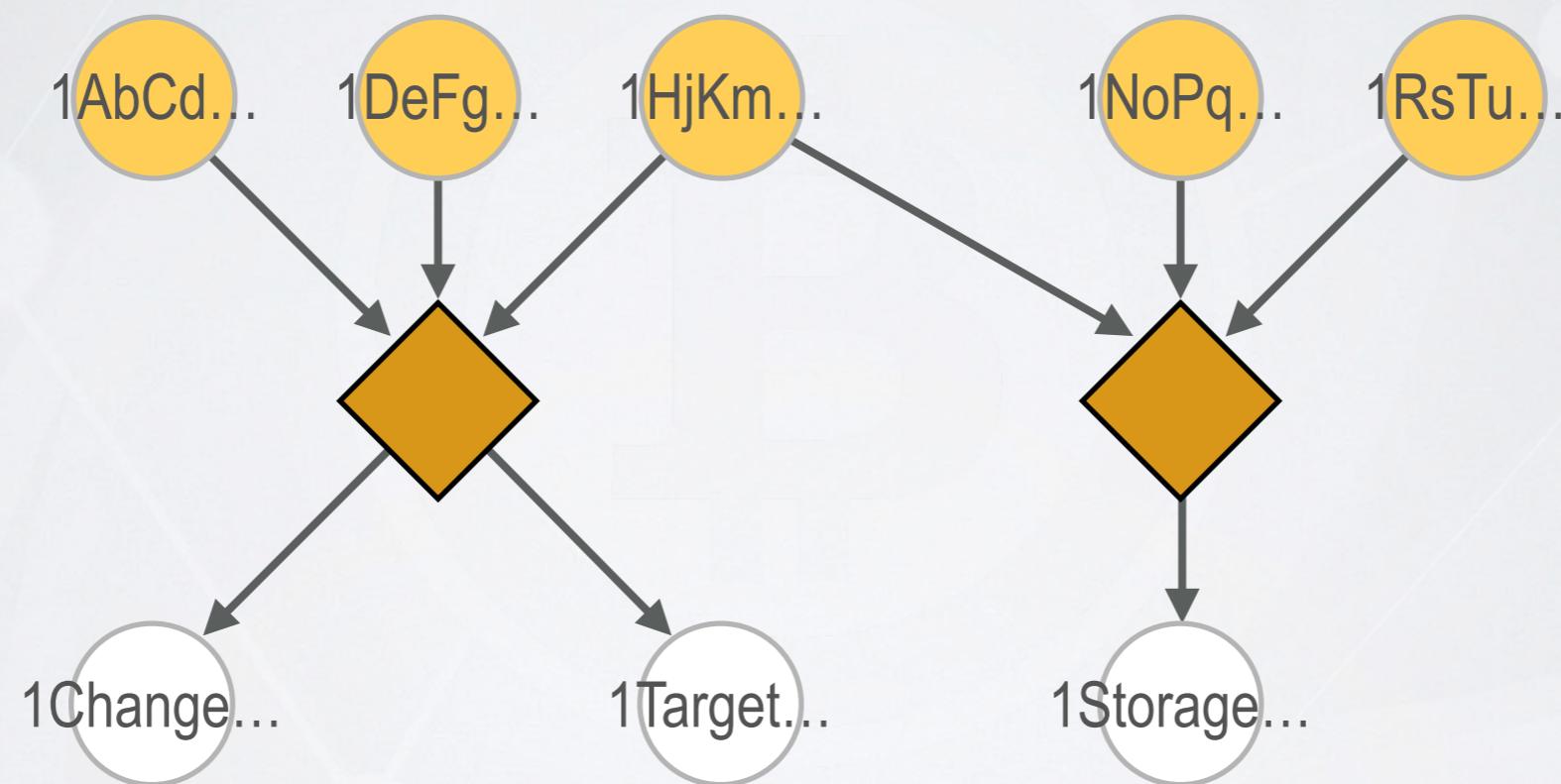
RECONSTRUCTING WALLETS



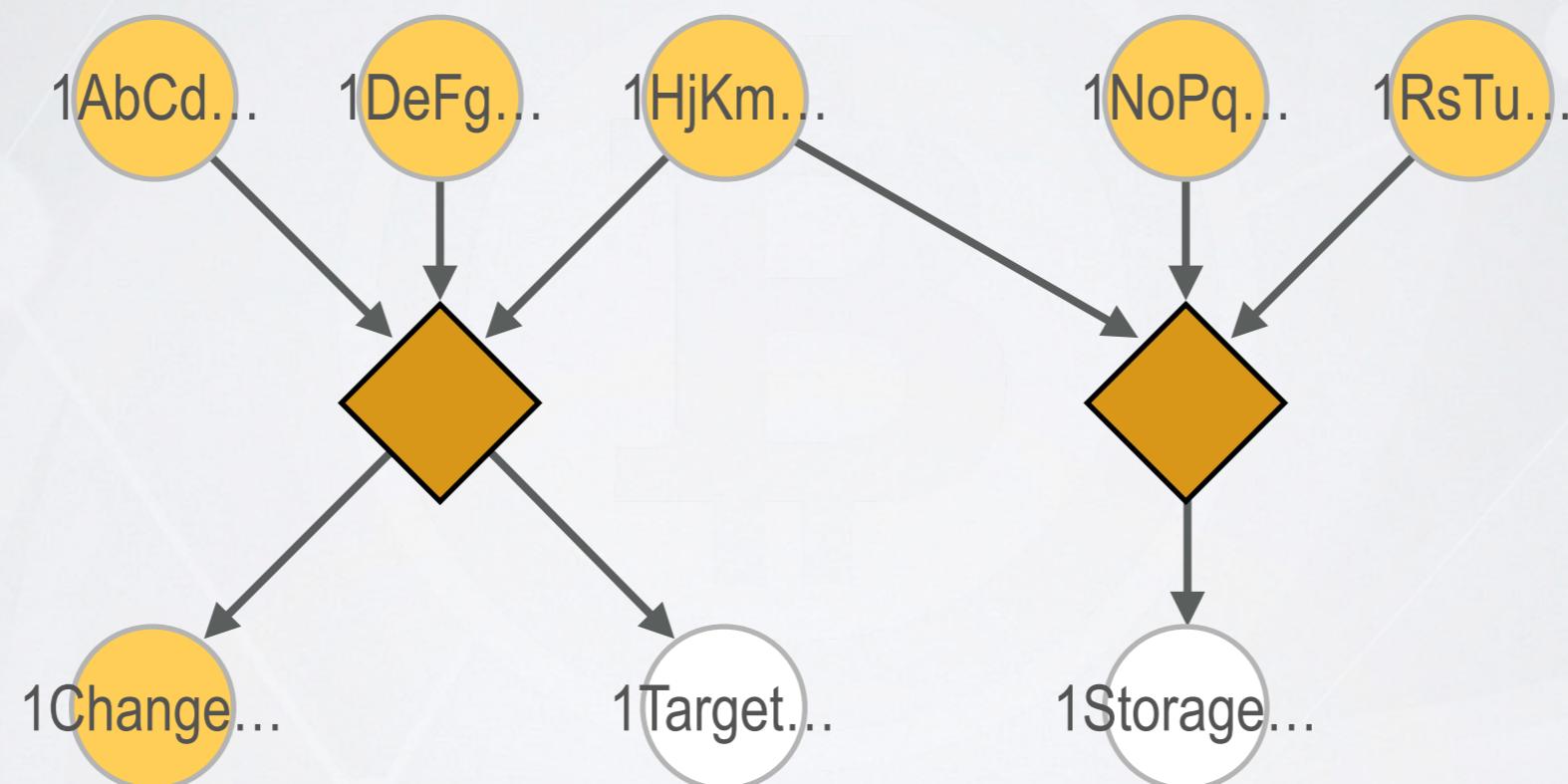
RECONSTRUCTING WALLETS



RECONSTRUCTING WALLETS



RECONSTRUCTING WALLETS

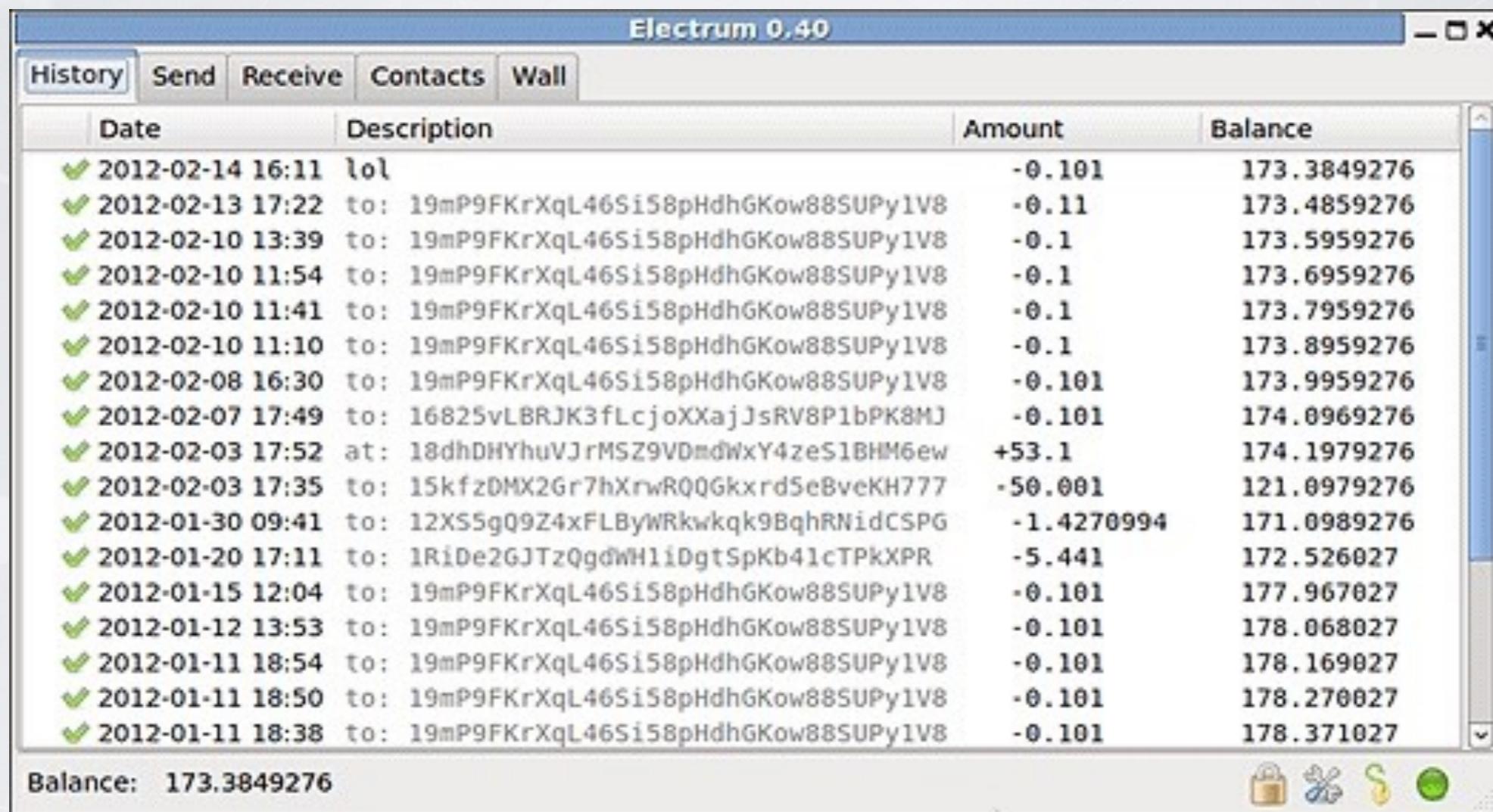


RECONSTRUCTING WALLETS

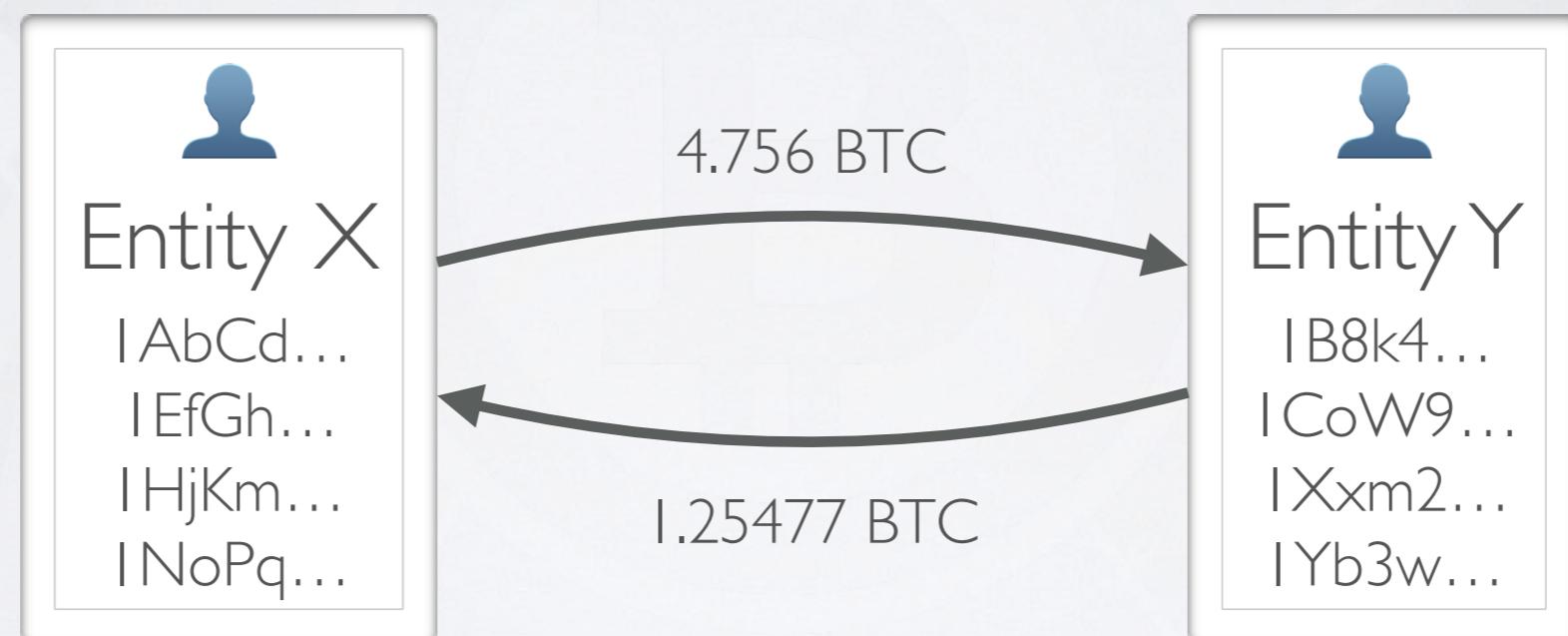
Electrum 0.40

Date	Description	Amount	Balance
✓ 2012-02-14 16:11	lol	-0.101	173.3849276
✓ 2012-02-13 17:22	to: 19mP9FKrXqL46Si58pHdhGKow88SUPy1V8	-0.11	173.4859276
✓ 2012-02-10 13:39	to: 19mP9FKrXqL46Si58pHdhGKow88SUPy1V8	-0.1	173.5959276
✓ 2012-02-10 11:54	to: 19mP9FKrXqL46Si58pHdhGKow88SUPy1V8	-0.1	173.6959276
✓ 2012-02-10 11:41	to: 19mP9FKrXqL46Si58pHdhGKow88SUPy1V8	-0.1	173.7959276
✓ 2012-02-10 11:10	to: 19mP9FKrXqL46Si58pHdhGKow88SUPy1V8	-0.1	173.8959276
✓ 2012-02-08 16:30	to: 19mP9FKrXqL46Si58pHdhGKow88SUPy1V8	-0.101	173.9959276
✓ 2012-02-07 17:49	to: 16825vLBRJK3fLcjoXXajJsRV8P1bPK8MJ	-0.101	174.0969276
✓ 2012-02-03 17:52	at: 18dhDHYhuVJrMSZ9VDmdWxY4zeS1BHM6ew	+53.1	174.1979276
✓ 2012-02-03 17:35	to: 15kfvDMX2Gr7hXrwRQQGkxrd5eBveKH777	-50.001	121.0979276
✓ 2012-01-30 09:41	to: 12XS5gQ9Z4xFLByWRkwkqk9BqhRNidCSPG	-1.4270994	171.0989276
✓ 2012-01-20 17:11	to: 1RiDe2GJTzQgdWH1iDgtSpKb41cTPkXPR	-5.441	172.526027
✓ 2012-01-15 12:04	to: 19mP9FKrXqL46Si58pHdhGKow88SUPy1V8	-0.101	177.967027
✓ 2012-01-12 13:53	to: 19mP9FKrXqL46Si58pHdhGKow88SUPy1V8	-0.101	178.068027
✓ 2012-01-11 18:54	to: 19mP9FKrXqL46Si58pHdhGKow88SUPy1V8	-0.101	178.169027
✓ 2012-01-11 18:50	to: 19mP9FKrXqL46Si58pHdhGKow88SUPy1V8	-0.101	178.270027
✓ 2012-01-11 18:38	to: 19mP9FKrXqL46Si58pHdhGKow88SUPy1V8	-0.101	178.371027

Balance: 173.3849276



IDENTIFYING WALLETS





btc0inr

Help: deposit not showing up in account

Apr 27, 2016, 06:39:14 PM

I sent 0.123456 BTC to Exchange A, as I write this the transaction has 20 confirmations already but it hasn't shown up in my account yet, and support isn't answering... what do I do?



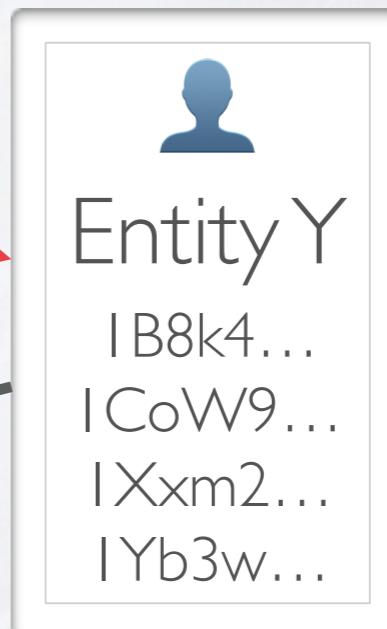
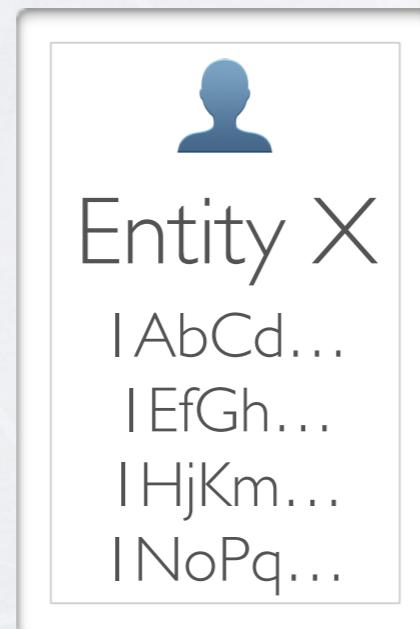
Help: deposit not showing up in account

Apr 27, 2016, 06:39:14 PM

btcinr

I sent [0.123456 BTC](#) to Exchange A, as I write this the transaction has [20 confirmations](#) already but it hasn't shown up in my account yet, and support isn't answering... what do I do?

TXID: 01234567789abcdef...





Help: deposit not showing up in account

Apr 27, 2016, 06:39:14 PM

btc0inr

I sent [0.123456 BTC](#) to Exchange A, as I write this the transaction has [20 confirmations](#) already but it hasn't shown up in my account yet, and support isn't answering... what do I do?

TXID: 01234567789abcdef...



btc0inr

| AbCd...
| EfGh...
| HjKm...
| NoPq...



Exchange A

| B8k4...
| CoW9...
| Xxm2...
| Yb3w...

EARLY RESULTS

- ~2 million addresses identified as MtGox
- False positives when clustering! (shared keys)
- Growing discrepancy between real and expected bitcoin holdings, suspected theft transactions
- Acquire better data to clean up results

April 19, 2015

The missing MtGox bitcoins

We received a lot of positive feedback on our release of our preliminary investigation into the Willy bot, even though it was already quite old (written circa August 2014). We also said we hoped to release more of our information over time, even though we have to take some care doing so. But while we have good relations to responsibly acquire and exchange information and share efforts, and reception from people online has been very encouraging, official interest has been pretty low.

In recent weeks, there has been a lot of news surrounding the U.S. agents accused of large bitcoin thefts in early 2013, and their interactions with Silk Road as well as MtGox. In the wake of this, there has been intense speculation that what happened at MtGox may have been related to these agents.

With the next creditors' meeting also on the horizon, this seems like a pretty good time for me to step in and share a bit more of what we know. First of all: no, we don't think these agents are main characters in the story of the missing MtGox bitcoins, and the story doesn't begin in 2013 either.

— Kim Nilsson, lead investigator (*available for comments: kim@wizsec.com*)

Updates since initial publication:

- The proper term for MtGox's financial status would have been "insolvency", not "fractional reserve". Thanks for pointing this out.
- The graphs related to MtGox's BTC holdings have been updated to include older, heuristically identified outputs, filling in most of the "gap" and giving a clearer picture of holdings over time.
- Minor language cleanups.

Executive summary

Most or all of the missing bitcoins were stolen straight out of the MtGox hot wallet over time, beginning in late 2011. As a result, MtGox was technically insolvent for years (knowingly or not), and was practically depleted of bitcoins by 2013. A significant number of stolen bitcoins were deposited onto various exchanges, including MtGox itself, and probably sold for cash (which at the bitcoin prices of the day would have been substantially less than the hundreds of millions of dollars they were worth at the time of MtGox's collapse).

Background

After a string of reported problems with bitcoin withdrawals, the MtGox exchange made big news when it collapsed in early 2014 and declared bankruptcy. Ever since then it has been the topic of vivid speculation what

Labels

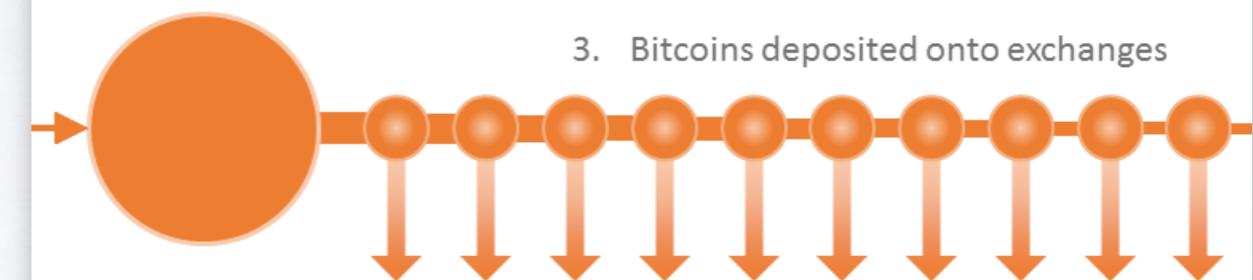
- [MtGox](#) (4)

Blog Archive

- [2017](#) (2)
- ▼ [2015](#) (2)
 - ▼ [April](#) (1) [The missing MtGox bitcoins](#)
 - [February](#) (1)



2. Bitcoins collected into larger holding address



4. Bitcoins sold for cash (?)

PROGRESS BY 2015

- Limited interest from bankruptcy trustee or law enforcement
- Mark more cooperative after all the work so far

<nikuhodai> hey word on the street is
that they're going to arrest you

<MagicalTux> just a rumor

8 HOURS LATER



FINDINGS BY 2016

- There were multiple thefts
(as far back as the beginning of 2011)
- MtGox was insolvent for most of its existence
- MtGox traded its own liabilities on itself
- Connected to other bitcoin thefts

WAITING...

- Known suspect for handling stolen coins
- Ongoing law enforcement investigations
- Delay publishing to avoid interfering
- Keep investigating details

ONE YEAR LATER

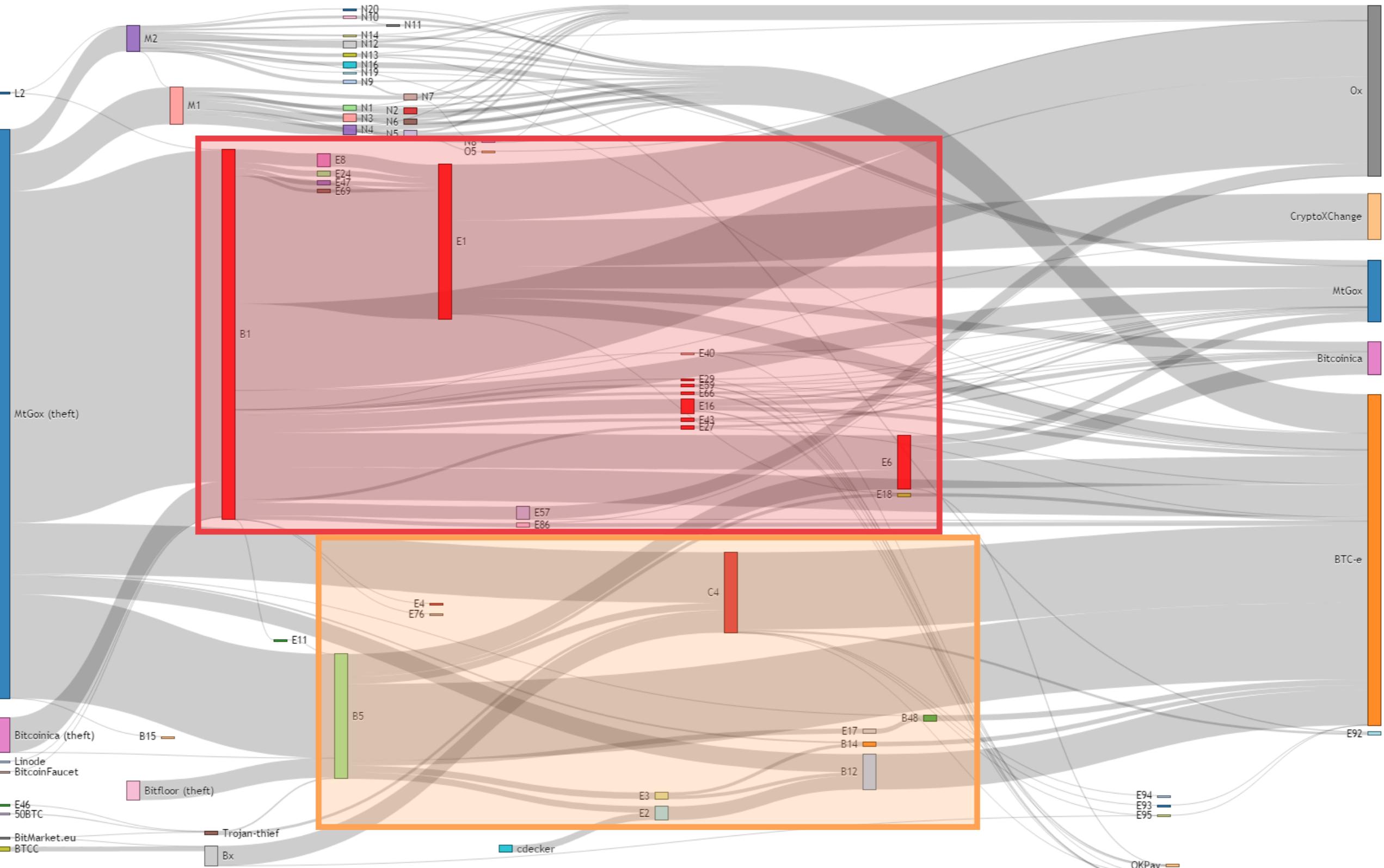




- Alexander Vinnik a.k.a. “WME”
- Received over half a million stolen bitcoins from MtGox and other thefts
- Deposited the stolen coins onto BTC-e, TradeHill, MtGox etc.
- Probably sold most bitcoins (including via “money codes”)
- Alleged by US to be a BTC-e administrator

THE TRAIL TO VINNIK

- Didn't use tumblers/mixers
- Spent coins from multiple sources together
- Deposited coins back to MtGox accounts ("WME")
- Used his real name online (to complain about his stolen funds being confiscated)



LAUNDERER ≠ THIEF ?

- All evidence pointing to Vinnik are for the wallet(s) that receive and move the stolen bitcoins
- The thief had possession of MtGox's private keys, could have sent the coins anywhere
- Unlikely a single person carried out this many thefts
- Sending coins to Vinnik without intermediate steps suggests involvement or prior arrangement

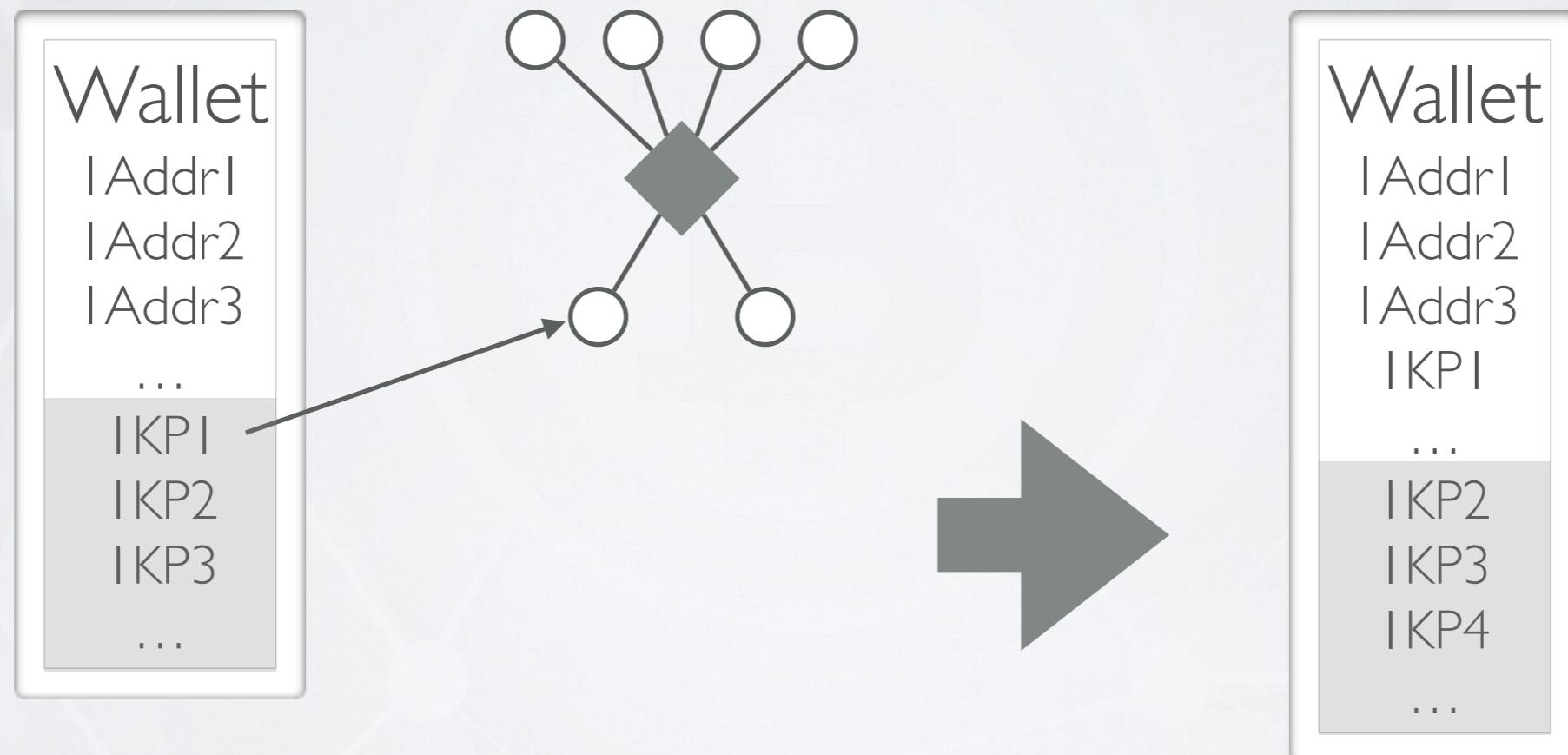
STOLEN PRIVATE KEYS?

- How do we know the thief stole the private keys?
- Running a second Bitcoin wallet on top of a copied wallet.dat file leaves blockchain fingerprints

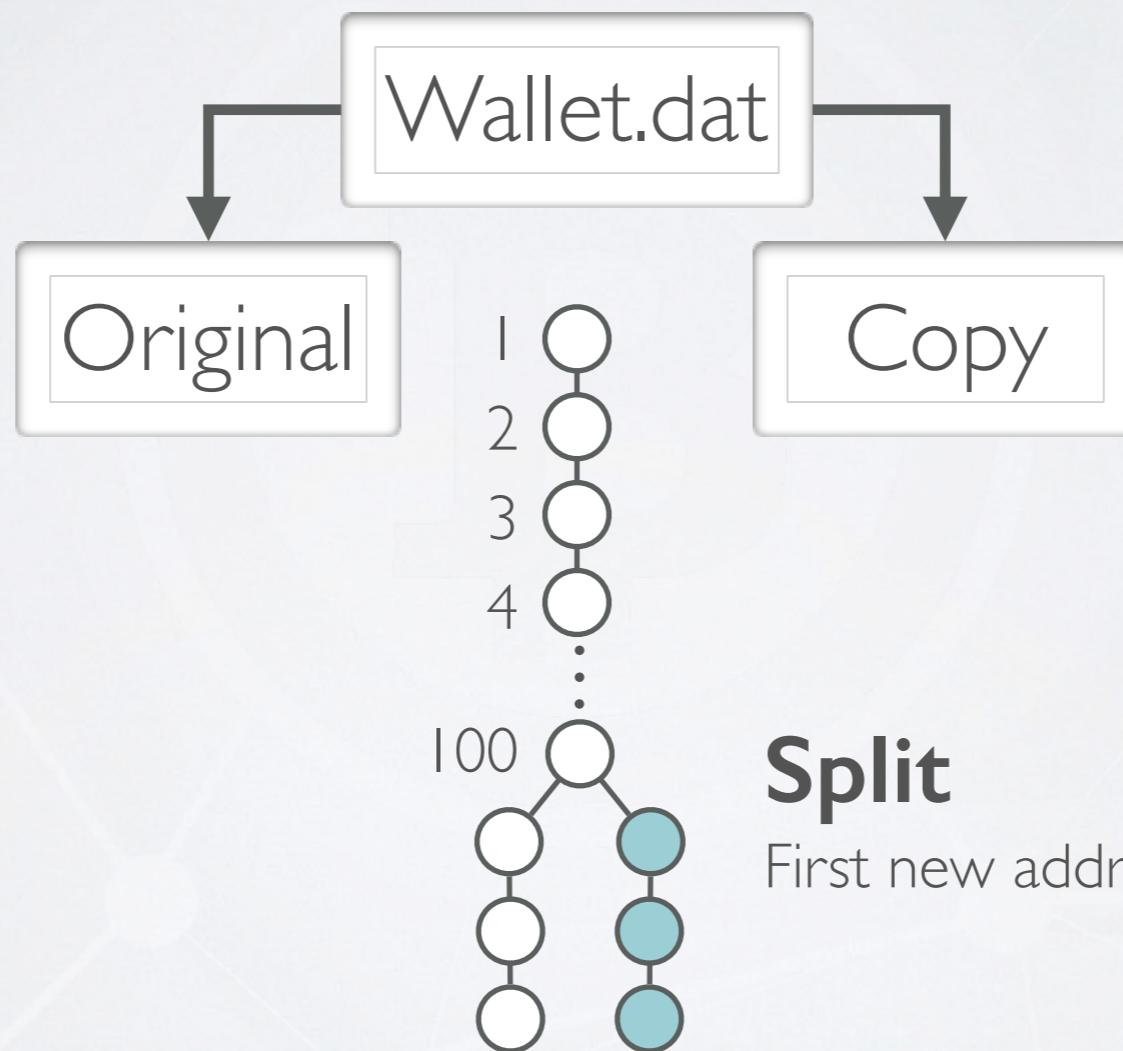
KEYPOOL

- In the original Bitcoin wallet, 100 “next” private keys are already pre-generated
- Lower chance of losing funds when restoring from a backup
- Largely superseded by deterministic wallets

KEYPOOL



KEYPOOL



MTGOX'S KEYPOOL

- First 100 theft transactions have change addresses perfectly matching MtGox's keypool as of **September 11, 2011, ~21:30 UTC**
- Some of those addresses were allocated as deposit addresses on MtGox's side
 - Thief steals coins, MtGox sees change as deposit

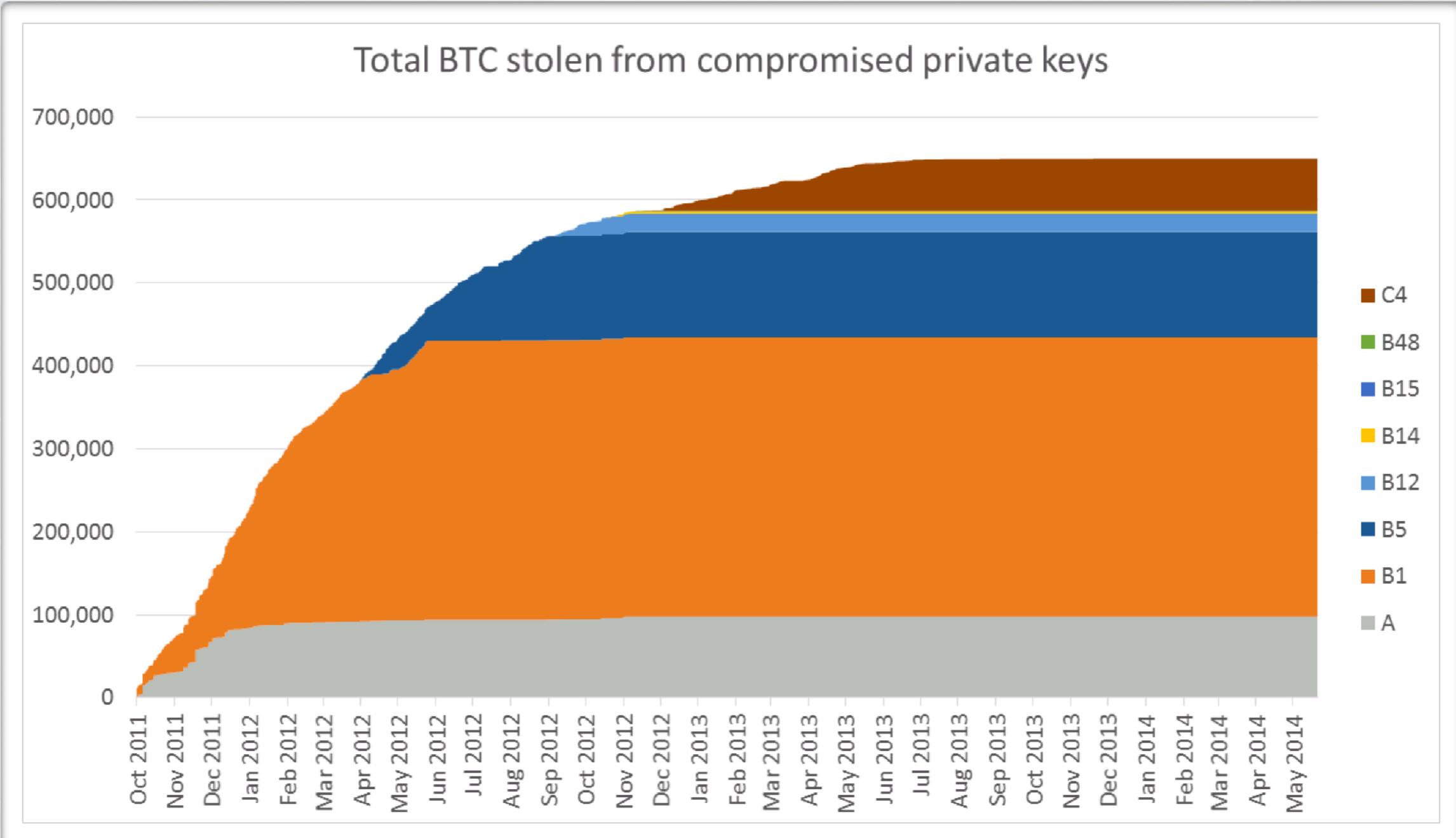
WHAT WAS TAKEN?

- Compromised hot wallet, up to 100,000 keys
- Over time, relatively smaller share of total keys
(eventually MtGox had ~4 million keys)

THEFT PATTERN

- Each transaction steals similar amounts
- Longer and longer time between transactions
- Restarts with same stolen wallet.dat file

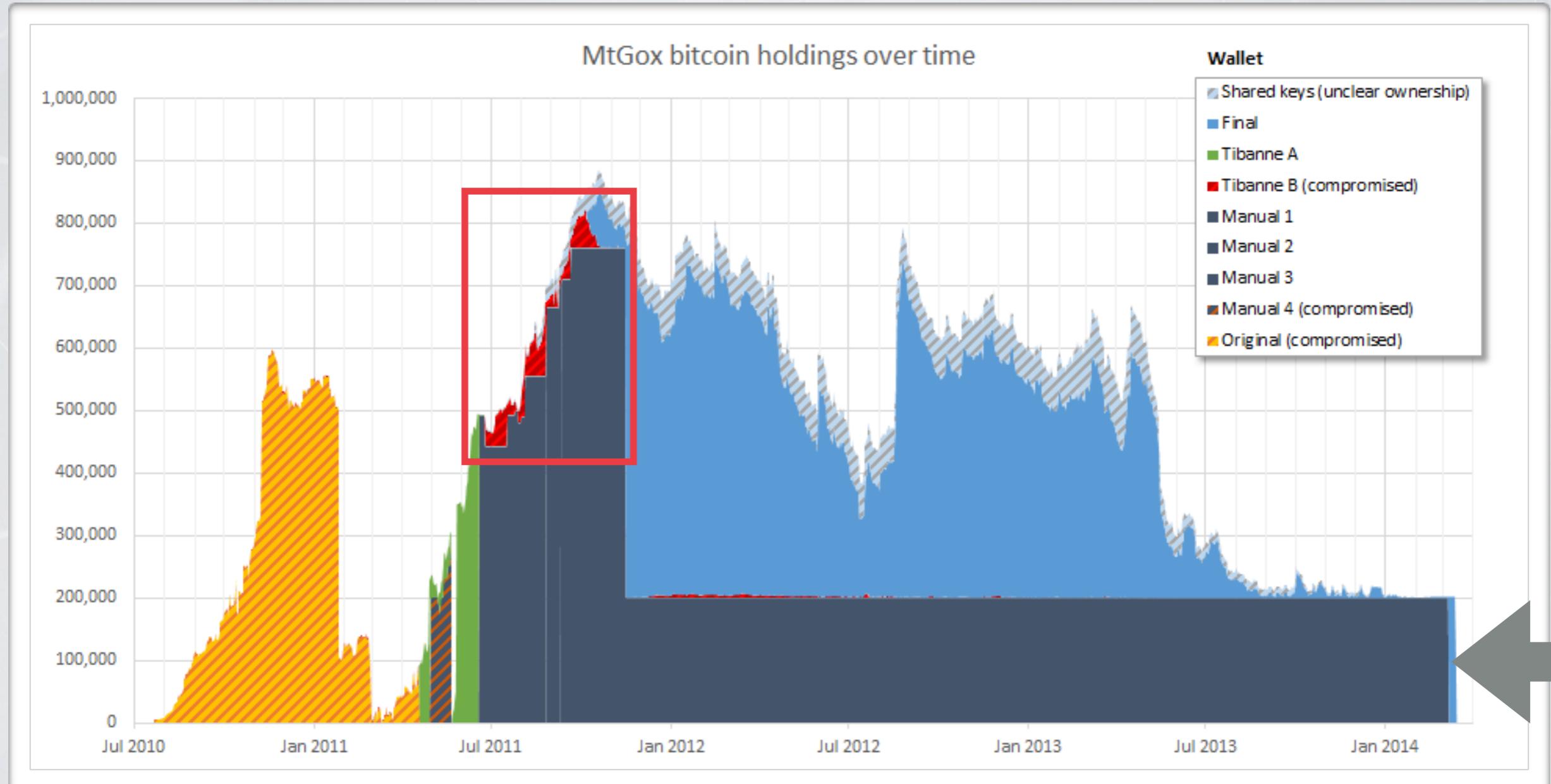
THEFT PATTERN



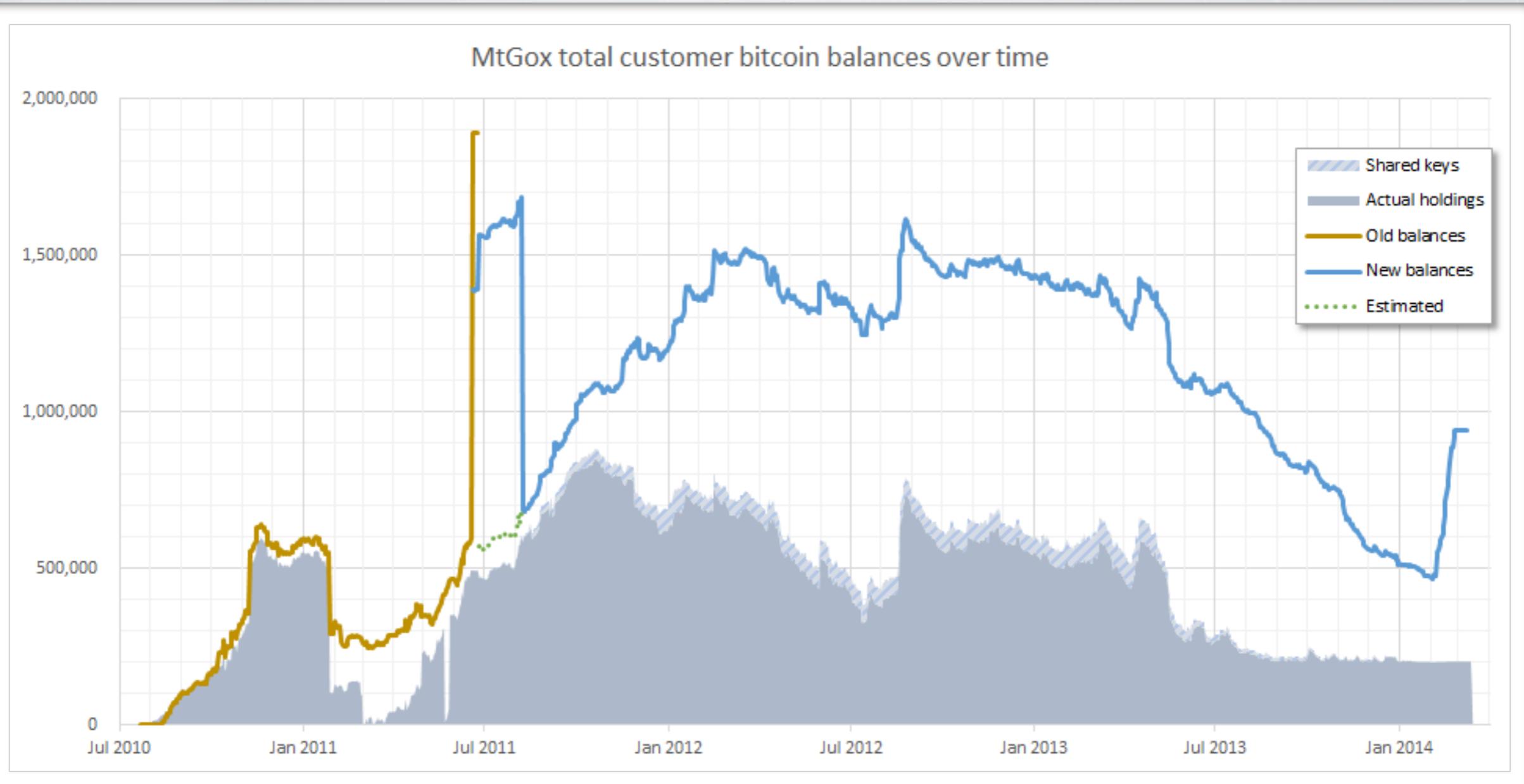
THE FULL MTGOX HISTORY

- Founded by Jed McCaleb in 2010
- Sold to Mark Karpeles in March 2011
 - Already insolvent when sold
 - Numerous incidents

BITCOIN HOLDINGS



...AND LIABILITIES



INCIDENTS

Liberty Reserve withdrawal exploit

(January 20–23, 2011)

- Unsanitized input → XML injection
- Override with custom amount
- 50,000 USD lost



Total losses

50,000 USD

0 BTC

INCIDENTS

Liberty Reserve withdrawal exploit #2

(January 30, 2011)

- Forgot to check for negative amounts
- User “withdrew” -\$2,147,483.647,
got credited to their account
- Fixed without permanent damage?



Total losses
50,000 USD
0 BTC

INCIDENTS

Hot wallet stolen

(March 1, 2011)

- Thieves copied wallet.dat from server
- 80,000 BTC lost
- Stolen bitcoins never moved
- Spawned idea of trading debts to recover

Total losses
50,000 USD
80,000 BTC

INCIDENTS

Off-site wallet stolen

(May 22, 2011)

- 300,000 BTC temporarily kept on an unsecured publicly accessible network drive
- Thief got nervous; gave coins back in return for 1% keeper's fee



Total losses

50,000 USD

83,000 BTC

INCIDENTS

Public hack via compromised accounts

(June 19, 2011)

- Hacker gained access to Jed's admin account
- Manipulated balances and crashed market
- Got about 2,000 BTC out



Total losses

50,000 USD

85,000 BTC

INCIDENTS

Absorbed Bitomat's debts

(August 11, 2011)

- Bitomat collapsed after they accidentally deleted their private keys
- MtGox offered to absorb the company
- About 17,000 BTC of debts



Total losses
50,000 USD
102,000 BTC

INCIDENTS

Compromised database

(September, 2011)

- Hacker gained read-write access to database
- Inflated account balances and withdrew funds
- Deleted (most) evidence
- About 77,500 BTC of withdrawals



Total losses

50,000 USD

179,500 BTC

INCIDENTS

Hot wallet stolen (again)

(Between September 11 and October 1, 2011)

- Thief got a copy of MtGox's main wallet.dat
- Didn't begin stealing funds until October 1
- In total, over 630,000 BTC stolen
- Seemingly never noticed...



INCIDENTS

Incorrectly detected deposits

(October 1, 2011 and onwards)

- Thief wallet's change seen by MtGox as deposits
- 48 MtGox users received a total of 44,300 BTC
- Some BTC recovered;
about 30,000 BTC lost



Total losses
50,000 USD
839,500 BTC

INCIDENTS

Accidentally destroyed bitcoins

(October 28, 2011)

- A bug in Mark's new wallet software caused it to send 2,609 BTC to an unspendable null key



INCIDENTS

US seizures

(May and August, 2013)

- Two law enforcement related seizures of a total of 5 million dollars



INCIDENTS

CoinLab dispute

(May, 2013)

- After a deal to become MtGox's US processor fell through, CoinLab allegedly refused to return 5 million dollars



Total losses

10,050,000 USD
841,509 BTC

INCIDENTS

“Willy”— the MtGox obligation exchange (2011–2013)

- Internal MtGox program to shift debts between different currencies by injecting fake currency
- Intended to recover from insolvency, but actually made it worse:
 - 51,600,000 USD
 - 22,800 BTC



Total losses

61,650,000 USD
864,309 BTC

TOTAL IMPACT

- Over 60 million dollars and 865,000 BTC lost
 - ~950,000 BTC in customer balances
 - ~100,000 BTC in company revenues
 - ~200,000 BTC left when MtGox collapsed
- Multiple compromises, not survivable
- Made worse by decision to keep quiet

FAILURES

- Didn't disclose early thefts
- Tried to dig their way out of a hole
- Proper auditing and monitoring prevented by the need to keep the secret
 - Increased risk

ANYTHING LEFT?

- Coins from the June 2011 hack are moving
- Track 300,000 BTC thief-with-a-conscience?
- Possible connection with BTC-e?
- Additional traces connecting the thefts

QUESTIONS?

kim@wizsec.com
@wizsecurity / @nikuhodai



1nikuYD1PUhAkhJaQWzLiLahuJBe9a2sZ