Crypto Hacks & Exploits

by John, Arya, and Harrison

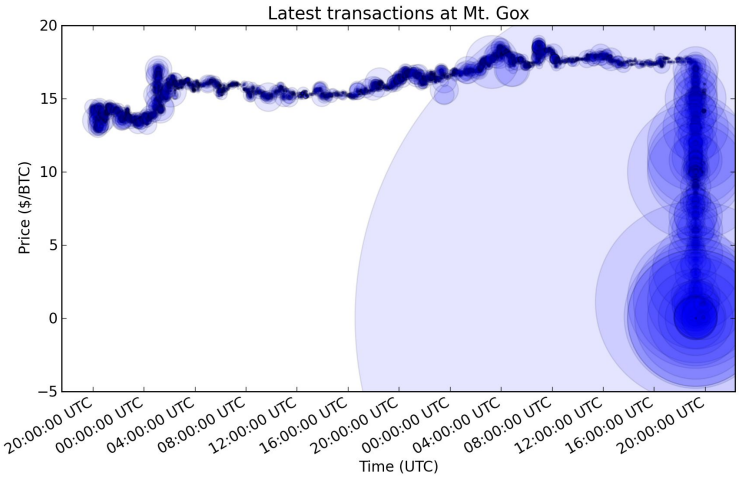
Pizza Sponsor

- https://lucylabs.io/
- Cryptocurrency Merchant Bank

lucylabs

Mt. Gox

- Mt. Gox, a bitcoin exchange in Japan, was the largest bitcoin exchange in the world
- The hack lost 740,000 BTC (6% of all bitcoin at that time)
- Only 200,000 BTC have been recovered to date



History of Mt. Gox

- Launched in 2010 by US programmer Jed McCaleb
- Mt. Gox stands for “Magic: The Gathering Online eXchange”
- First hack was in June 2011
  - Auditor’s computer was hacked
  - Bitcoin value was artificially altered to be $0.01
  - Hacker stole 2000 BTC
- This hack led to Mt. Gox being more careful and put BTC into cold storage

Mt. Gox Continued

- At its peak, Mt. Gox handled 70% - 80% of all of Bitcoin's volume
  - Mt. Gox pricing basically determined the value of BTC
- Before the big 2014 hack, customers were having troubles withdrawing funds
  - Due to "Transaction Malleability" - when someone changes the unique ID of a bitcoin before it is confirmed on the bitcoin network
- On February 2014, the exchange suspended withdrawals after discovering "suspicious activity in its digital wallets"
- The suspension alone dropped the value of BTC by 20%
- The company discovered it had "lost" 750,000 BTC, losing 6% of BTC's total supply at the time
- How did this happen?

Dear MtGox Customers,

During our efforts to resolve the issue being encountered by some bitcoin withdrawals it was determined that the increase in withdrawal traffic is hindering our efforts on a technical level. As to get a better look at the process the system needs to be in a static state.

In order for our team to resolve the withdrawal issue it is necessary to temporarily pause all withdrawal traffic to obtain a clear technical view of the current processes.

We apologize for the extremely short notice, but as of now all bitcoin withdrawals will be paused, and withdrawals in the queue will returned to your MtGox wallet and can be re-intiated once the issue is resolved. Customers can still use the trading platform as usual.

Our team will be working hard through the weekend and will provide an update on Monday, February 10, 2014 (JST).

Again, we apologize for the inconvenience, and ask for your continued patience and support while we work to resolve this issue.

Best regards,

The MtGox Team

Mt. Gox Hack Explained - Blockchain Basics

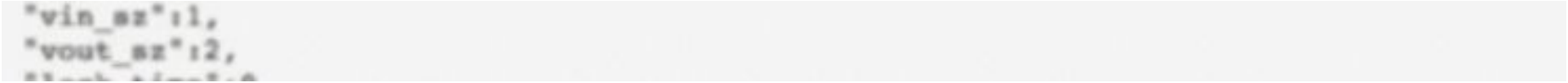
- A transaction malleability attack
- Data of a transaction in code form
- For this code, pretend Jim wants to send 0.0015 BTC to Anne
- In order to send 0.0015 BTC, Jim sends inputs worth 0.0015770 BTC

Dissecting Mt. Gox - Blockchain Basics


```
{
  "hash":"13aaf3df20b9ec99b5c253f9cd3c784c39275083b9fca884e0767b88419bca28",
```


- This is the transaction ID or “hash” of the transaction

Dissecting Mt. Gox - Blockchain Basics



- Vin_sz is the number of input data
  - Since the data is being sent using only 1 of the previous transaction in this case the vin_sz = 1
- Vout_sz is the number of outputs
  - In this case, vout_sz = 2 since some BTC is sent to 1 person and the remaining BTC is sent back as change

Dissecting Mt. Gox - Blockchain Basics


```
  "in":[
    {
      "prev_out":{
        "hash":"84c2424f312f0887f0d82aecc8000c635f8f0f8169806bff4f9a4d4652c3098f",
        "n":0
      },

"scriptSig":"3045022100c51d512928e13d61a30ceb77db70e5d0b565d559f5491edb7cf2312ae84ae06f022050f0710d436a6dc8bf415dc3b86c7b66b0be5342e257b86cb5fcb203f693632801
0438c73f3ba716a2b214141da57eb60f6fdbe8652bb5a05944010087a51460a16dcdad7bf71608e0cba3125d00c94656c18b130150bd92cbc1eaa73fd266b04c85"
    }
  ],
```


- This is the input data of the code
- “scriptSig” is the Jim’ signature data
  - Keep Note of this. Will be very important later

Dissecting Mt. Gox - Blockchain Basics


```
"out":[
  {
    "value":"0.00150000",
    "scriptPubKey":"OP_DUP OP_HASH160 49eab6c1e49d65aa03a3deac4b25de4b3a6c41ec OP_EQUALVERIFY OP_CHECKSIG"
  },
  {
    "value":"0.00005120",
    "scriptPubKey":"OP_DUP OP_HASH160 08f9982d6b663d5ab5b44d8a9008f7c501db57e5 OP_EQUALVERIFY OP_CHECKSIG"
  }
]
```


- This is the output of the transaction
- The first part signifies how much BTC is getting sent out
  - In this case 0.0015 BTC
- The second part signifies the change the sender is getting back
  - In this case 0.0005120 BTC

Dissecting Mt. Gox - Blockchain Basics

- In the previous slide, Anne is getting 0.0015 BTC and Jim is getting back 0.00005120 BTC as change
- Remember Jim sent out **0.0015770 BTC** as input data. This means that **0.0015512** (0.0015 + 0.000051200) BTC is returned yet Jim's input data was **0.0015770 BTC** > **0.0015512 BTC**. How is this possible?
- The remaining BTC is sent sent to miners as a transaction fee

Dissecting Mt. Gox - Blockchain Basics

- Now you know the code of a simple transaction
- The Bitcoin blockchain is completely immutable via cryptographic hash functions and Proof of Work
  - Once data is inside the blockchain, it is impossible to tamper with
- There is a loophole to the immutability of the blockchain

Dissecting Mt. Gox - Transaction Malleability

- Remember the “scriptSig” in the input data?


```
  "in":[
    {
      "prev_out":{
        "hash":"84c2424f312f0887f0d82aecc8000c635f8f0f8169806bff4f9a4d4652c3098f",
        "n":0
      },

"scriptSig":"3045022100c51d512928e13d61a30ceb77db70e5d0b565d559f5491edb7cf2312ae84ae06f022050f0710d436a6dc8bf415dc3b86c7b66b0be5342e257b86cb5fcb203f693632801
0438c73f3ba716a2b214141da57eb60f6fdbe8652bb5a05944010087a51460a16dcdad7bf71608e0cba3125d00c94656c18b130150bd92cbc1eaa73fd266b04c85"
    }
  ],
```


- This signature that goes along with the input data can be manipulated, which can change the transaction ID
- How is this possible?

Transaction Malleability Example

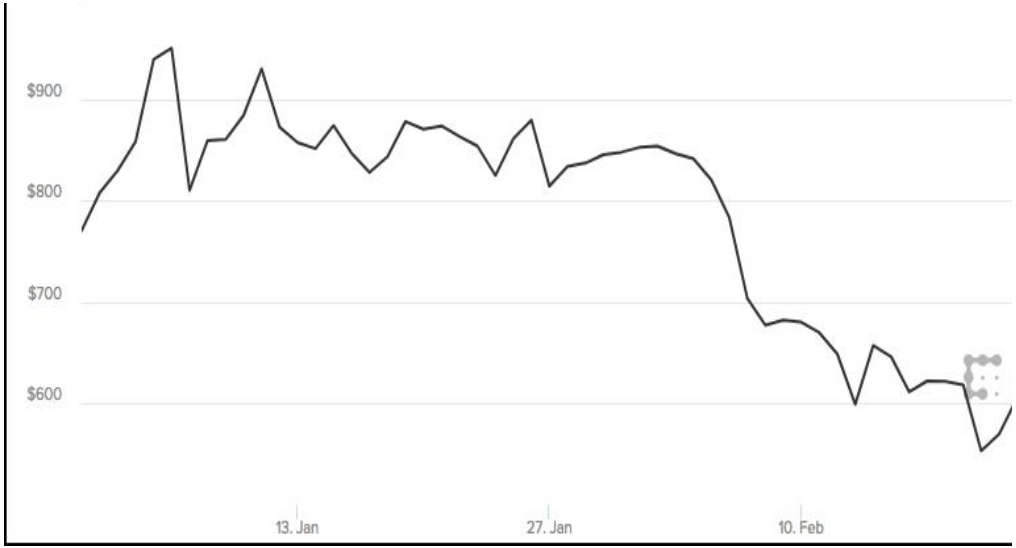
- Suppose Anne wants Jim to send her 0.025 BTC
- Jim initiates a 0.025 BTC transaction to Anne's public address and broadcasts it for miner approval
- While the transaction is waiting in the queue (mempool), Anne uses transaction malleability to alter Jim's signature, thus changing the transaction ID
- If this tampered transaction gets approved before Jim's transaction does, this will overwrite Jim's transaction

Transaction Malleability Example

- Why does it matter if Anne overwrote Jim's transaction?
- Anne can will still get the 0.025 BTC, but she can tell Jim she didn't get it
- Jim would see that his transaction didn't go through and thus resend the 0.025 BTC
- This means Anne now has 0.050 BTC instead of the 0.025 BTC she was supposed to get
- This is what happened at Mt. Gox on a much larger scale
- In the end, Mt. Gox lost at least 750,000 BTC

Aftermath of Mt. Gox

- Worst possible time for a vulnerability with Bitcoin
- Bitcoin was just becoming mainstream, and the fear of another attack like Mt. Gox put the faith in Bitcoin back for 4-5 years

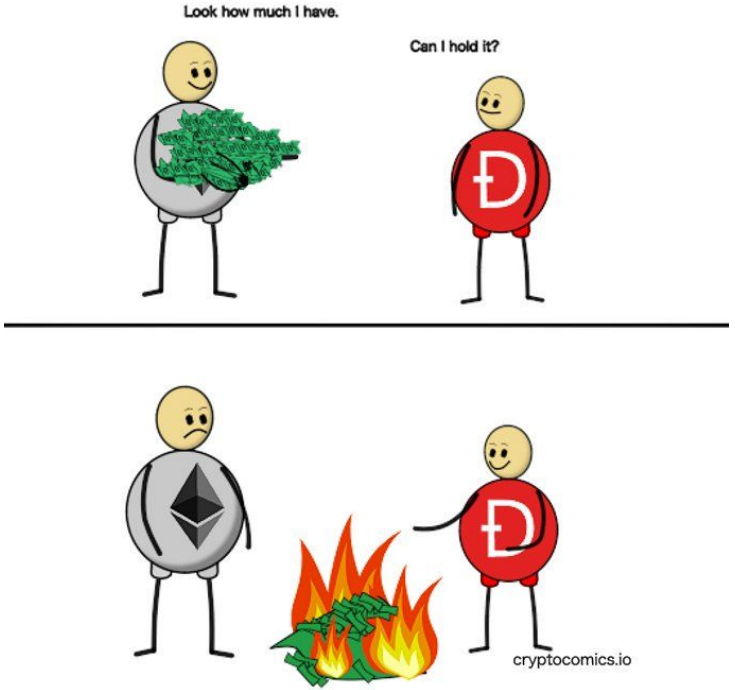


Aftermath of Mt. Gox

- Mt. Gox then declared bankruptcy
- The stolen funds were being laundered through BTC-e
- This led to the arrest of the owner of BTC-e, Alexander Vinnik, in Greece where he is going to be extradited to the US

Ethereum: DAO Hack (June 2016)

- *Decentralized Autonomous Organization*
- Smart contract
- Controlled ~14% of Ethereum
- ~$50 million stolen by attacker



Aftermath of the DAO exploit

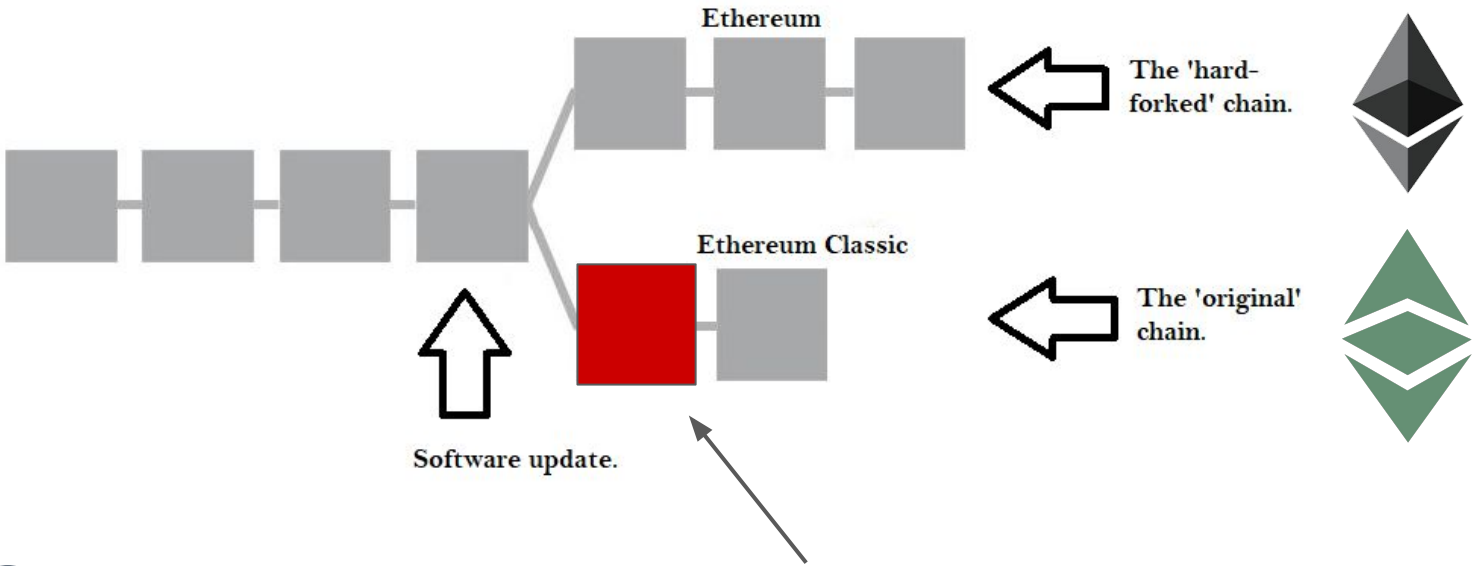
Ethereum

Hack is reverted and blockchain is forked

Ethereum Classic

Hack is not reverted. Blockchain must be immutable

Hard Fork


Ethereum
The 'hard-forked' chain.
Ethereum Classic
The 'original' chain.
Software update.
DAO Hack

Bitfinex

Bitfinex is a Hong Kong based crypto exchange, similar to coinbase and Gemini.

In 2015 it was hacked and 1500 bitcoin were stolen, this was only a small amount of their total bitcoin reserves but it prompted them to look for more secure ways to protect people's money.

This lead them to partner with BitGo and use their multisignature security method...

Hot wallets / Cold storage

Many exchanges use “hot wallets” which is essentially just when your private key is kept online and not offline like on a piece of paper for example.

Offline wallets are said to be in “Cold storage” this means that they can be sent money just as easily but it is more difficult to send money from them.

Having a hot wallet means that your private key can be vulnerable. If your computer is attacked by a hacker your private key can be stolen

Multi-signature wallet

A multi-signature wallet is designed to protect hot wallets by issuing three (or more) private keys instead of one. This protects you if either you lose your private key or if a hacker gets hold of it.

2 out of the 3 keys are needed for a transaction to occur.

One is kept by the company that issues them and the other two are kept by you.

Bitfinex

In BitFinex's case your two private keys are kept "securely" on their network and BitGo kept the other one.

BitFinex believed that this would be more secure than their previous security system and so they kept more money available, increasing liquidity.

Since Bitgo had a key they were supposed to look at transactions and verify that they didn't look suspicious and then approve the transaction.

BitFinex hack

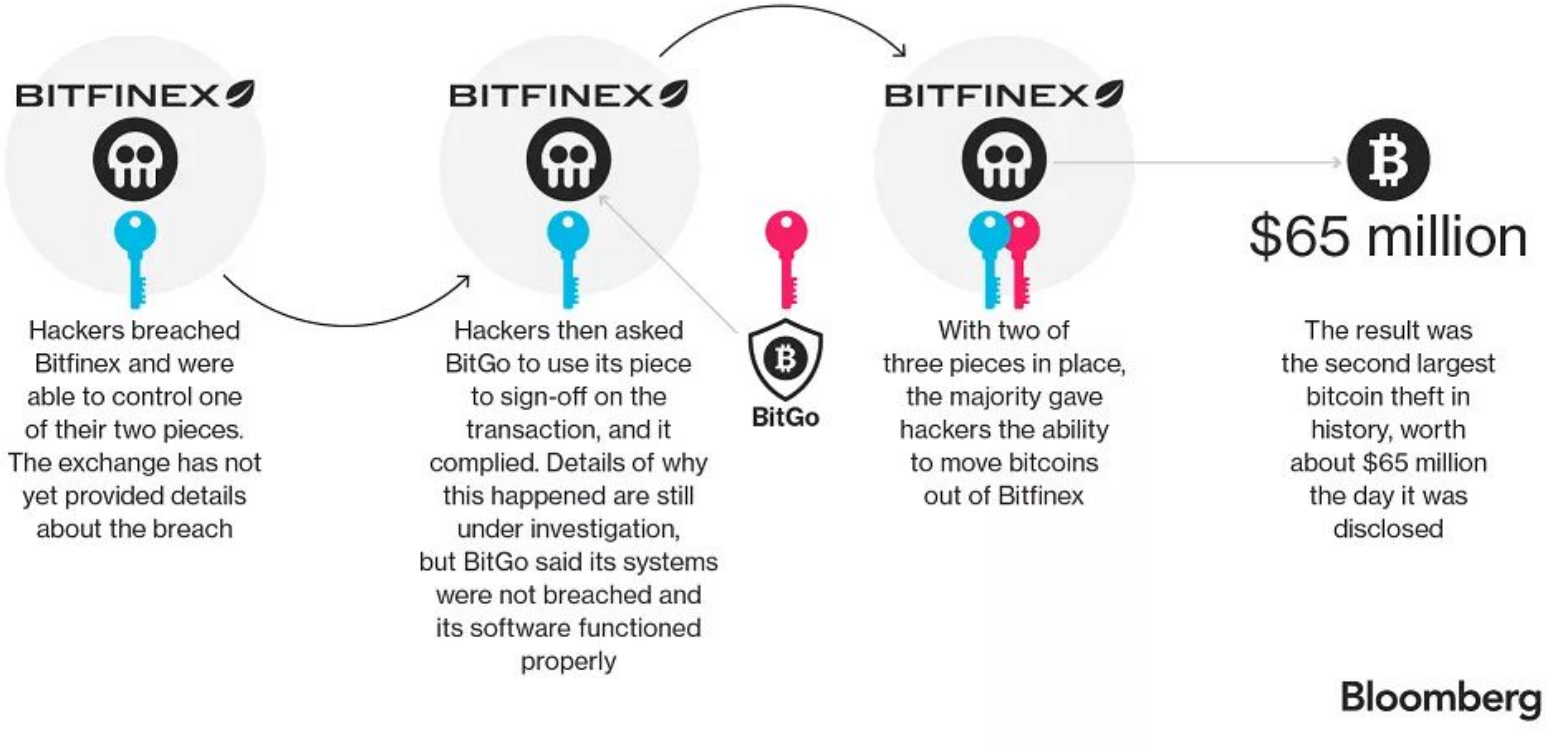
So then how did 120,000 Bitcoin worth $72 million at the time get stolen?

No one knows exactly what happened and a lot of theories are out there about what happened but most people agree with one theory.

This theory suggests that hackers were able to gain one private key from the server and pass off lots of fake transactions as real ones. Bitfinex servers allowed this to happen. Bitgo should have been able to stop this but Bitgo was doing whatever Bitfinex said to do and validating all of the transactions.

This caused the price of bitcoin to drop by 20%

How Hackers Pulled Off a $65 Million Dollar Heist



Bloomberg

Pitt Crypto

What happened after

Bitfinex issued BFX tokens to everyone who has lost money that were worth $1 each.

They promised to allow these to be refundable for real money of other currencies eventually.

After a while all the BFX tokens were able to be cashed in and people got their money back.

Sources

- https://coincentral.com/ethereum-classic-vs-ethereum/
- https://medium.com/@QUOINE/timeline-of-significant-crypto-exchange-hacks-621f4993b625
- https://altcointoday.com/how-bitfinex-was-hacked/
- https://blockgeeks.com/guides/cryptocurrency-hacks/