BITCOIN FORENSICS

Peter Theobald

peter@TCForensics.com
BITCOIN FORENSICS

PART I: Bitcoin overview

• 1) Why is Bitcoin worth anything?
• 2) Cryptography, blockchain ledger and incentives
• 3) Bitcoin ecosystem today
• 4) Altcoins - Bitcoin 2.0 or snake oil?
BITCOIN FORENSICS

PART II: Cryptocurrency Forensics

• 1) Common forensic goals
• 2) Weaknesses and attack surface
• 3) Examining the blockchain directly
• 4) Searching a computer
• 5) Case Study: How Many Bitcoins?
• 6) Case study: Wikileaks
Why is Bitcoin worth anything?

Bitcoin is similar in ways to Gold:

• There’s a fixed supply. It costs time and money to find gold, usually a huge investment in a gold mine; you have a chance at both profit and loss.

• It’s easy to transport. A little gold represents a significant enough portion of the world’s supply that $5,000 worth fits easily in your pocket.

• It’s completely “fungible” - if it’s in your hand - whether you earned it, stole it, or mined it - you can go spend it.

• It’s durable. You can bury some in the wilderness and leave a map for your grand-kids to find it. It stores value.

• It is impervious to politics. The government could fall into collapse or communism and - so long as you can hide it - you can still spend it around the world.

• People began accepting it as payment at some point in history. This caused more people to accept it - since it could always be sold to the original group. This created a self-reinforcing cycle which rapidly led to gold being valued universally (even though it’s not accepted as payment for most simple purchases.)
BITCOIN FORENSICS

Cryptography, blockchain ledger and incentives


• Digital assets: music, movies, photography, journalism, publishing. Easily copied, hard to prove ownership, lowered value.

• Solution:
  • Distributed transparent ledger (blockchain) of transactions.
  • Mining coins as “proof-of-work”. Signing transactions.
  • Public Key cryptography. Private keys to public addresses.
BITCOIN FORENSICS

Bitcoin ecosystem today

• Massive mining ‘farms’ in China and locations with cheap electricity
• Local wallets vs. exchanges
• Miners, Holders, Speculators and Whales
• Wall St., banks, governments and tech startups
• IRS and Coinbase
BITCOIN FORENSICS

Altcoins - Bitcoin 2.0 or snake oil?

- "Better Tech"
- Scaling, transaction fees (Litecoin, Bitcoin Cash)
- Energy efficiency (Proof of work, proof of stake)
- Privacy coins (Dash, Monero)
- Programmable contracts (Ethereum)
- ICOs (Initial Coin Offerings)
- Scams (Dogecoin: Is a coin a scam if it holds and rises in value? Only time will tell)
BITCOIN FORENSICS

Common forensic goals

• Stolen or lost cryptocurrency
  • Wallets and the vulnerable private key.
  • Hackers, viruses, spy-ware. Security 2FA, Phone SMS intercepts.
  • Locked-out addresses.

• Hidden cash, assets, transactions
  • The Dark Web. Illegal purchases. Hiding cash.
  • Wallet software. Cold Wallets, Hot Wallets, Hardware Wallets, Exchange vaults.
  • Fraud/ extortion payments.
BITCOIN FORENSICS

Weaknesses and attack surface

• Public ledger
  • + Every BTC transaction ever made is public, in every detail, forever. Complex tracing is possible.
  • - Account numbers are anonymous like swiss bank accounts
  • - Account numbers are disposable, “burner by design”.

• Exchange with fiat
  • Exchanges (Coinbase and the IRS, subpoenas)
  • Bank deposits KYC
  • Trace: follow the transactions until it exits the system as fiat

• Known addresses
  • Donations, public projects, publicized addresses.
  • Blockchain.info
BITCOIN FORENSICS
Examining the blockchain directly

• Tools
  • Running a node: direct access to all transactions
  • Blockchain.info, blockexplorer.com: view information about any block, address, transaction by numeric-address. Some counterparty information where known.
  • Coinmarketcap: BTC and alt coin price data, historical prices
    • https://coinmarketcap.com/currencies/bitcoin/historical-data/
  • Computer science professor Sara Meiklejohn while at UCSD researched methods of analyzing and de-anonymizing blockchain transactions
    • (input clustering, change address identifying, exchange known addresses, etc)
  • Chainalysis ‘Reactor’ tool has compiled massive database cross-referencing identified people and organizations with known bitcoin addresses, and offers analysis of webs of linked transactions.
BITCOIN FORENSICS

Searching a computer

• Forensic artifacts of Wallets, Mining software

• Email, web artifacts of transactions, exchanges
  • Make list of cryptocurrency terminology, websites and exchanges. Search computer for emails, chats, web pages related to cryptocurrency holdings and transactions.

• Tools: Magnet Internet Evidence Finder, FTK, EnCase etc.
BITCOIN FORENSICS
A blockchain transaction

• Blockchain: The entire history of every transaction ever as a series of linked blocks.
• Block: A single block holding approx. 2000 transactions. A new block is assembled and signed (confirmed) by a miner approx. every 10 minutes. Yes, 3+ per second.
• Transaction: A list of addresses (inputs) with coins being spent, and a list of addresses (outputs) and the amounts of coins sent to each address.
• Input addresses are signed cryptographically to prove ownership and the right to spend them.
• Input addresses are spent in their entirety every time. Unspent coins “change” are explicitly sent back to the input address or to a new “change” address.
• The miner who assembles the block and confirms the transactions gets a transaction fee which is not explicitly listed but is the difference between the total of inputs and the total of outputs (what’s left on the table)
BITCOIN FORENSICS

Case Study: How Many Bitcoins?

• Matrimonial, quick phone consult. Husband had approx. $40k in Bitcoins bought a year earlier, can I help wife set up wallet to receive half?

• I walk them through setting up a wallet, cautioning them NOT to reveal the private keys and to move to a safer hardware wallet later.

• Husband transfers approx. $20K in Bitcoins. I confirm receipt in wife’s wallet.

• I get curious and follow the transaction back. I find the previous day he transferred $40K to his address from a different address holding $200K.

• See: attached transactions, and follow the coins...
BITCOIN FORENSICS

Case Study: WikiLeaks

• When WikiLeaks was blocked by Visa and Mastercard in 2010, they published a Bitcoin address for donations. On one day in December 2013 they moved around 3,000 Bitcoin worth approx. $800 each into a series of other accounts. In December 2017 3,000 Bitcoins would be worth $57 million.

• See: attached transactions...
Thank you!

Peter Theobald
peter@TCForensics.com
(516) 762-3187
Transaction View information about a bitcoin transaction

Summary
- Size: 226 (bytes)
- Weight: 904
- Received Time: 2017-07-15 18:58:14
- Lock Time: Block: 475949
- Included In Blocks: 475950 (2017-07-15 18:58:28 + 0 minutes)
- Confirmations: 28645 Confirmations

Inputs and Outputs
- Total Input: 20 BTC
- Total Output: 19.9984334 BTC
- Fees: 0.0015666 BTC
- Fee per byte: 693.186 sat/B
- Fee per weight unit: 173.296 sat/WU
- Estimated BTC Transacted: 9.9992167 BTC

Visualize
- View Tree Chart

Transaction details:
- Hub address: 1JbK2r9xcg7GRck9B7vBx5VisimtnYrwQf
- Wife's receiving address: 1JnaFsHP1hLvSvtYY9Zsatc2e61zzWRB1g
- Presumed Hub change address: 178QJwMeGKkZKRBuJYGAm9YdCaKfqCNHJQ

7/15/2017 price ≈ $2000/BTC

≈ $20K each
≈ $40K total
Transaction View information about a bitcoin transaction

<table>
<thead>
<tr>
<th>Summary</th>
<th>Inputs and Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size 226 (bytes)</td>
<td>Total Input 108.1081081 BTC</td>
</tr>
<tr>
<td>Weight 904</td>
<td>Total Output 108.09338856 BTC</td>
</tr>
<tr>
<td>Received Time 2017-07-14 05:50:34</td>
<td>Fees 0.01471954 BTC</td>
</tr>
<tr>
<td>Included In Blocks 475752 (2017-07-14 05:51:50 + 1 minutes)</td>
<td>Fee per byte 6,513.071 sat/B</td>
</tr>
<tr>
<td>Confirmations 28838 Confirmations</td>
<td>Fee per weight unit 1,628.268 sat/WU</td>
</tr>
</tbody>
</table>

Visualize View Tree Chart

Inputs and Outputs

<table>
<thead>
<tr>
<th>Total Input</th>
<th>Total Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>108.1081081 BTC</td>
<td>108.09338856 BTC</td>
</tr>
</tbody>
</table>

Fees 0.01471954 BTC

Fee per byte 6,513.071 sat/B

Fee per weight unit 1,628.268 sat/WU

Estimated BTC Transacted 20 BTC

Approximately $40K

7/14/2017 price $2000/BTC

J ust the day before!

CoinCola Start Trading BTC, ETH, and BCH | Global OTC Marketplace | 0% trading fee | Perfect time to invest

Start Trading
### Transaction

**View information about a bitcoin transaction**

- **Transaction ID**: 2817f3d8813e02b6ccbb2c9e017cf79036eb64d491e8dbf2cc3e7b74ca291353
- **Input 1**: 1Gp5DWXLCKzEbDZUygzZUoCuopS1kmHiX5
- **Output 1**: 1KQWYc2XMKCoK96T38EYLS9DAt8Chp2RY

### Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>226 (bytes)</td>
</tr>
<tr>
<td>Weight</td>
<td>904</td>
</tr>
<tr>
<td>Received Time</td>
<td>2016-02-08 17:30:21</td>
</tr>
<tr>
<td>Lock Time</td>
<td>Block: 397400</td>
</tr>
<tr>
<td>Included In Blocks</td>
<td>397412 (2016-02-08 17:38:07 + 8 minutes)</td>
</tr>
<tr>
<td>Confirmations</td>
<td>107176 Confirmations</td>
</tr>
</tbody>
</table>

**Visualize**: View Tree Chart

### Inputs and Outputs

- **Total Input**: 398.00002184 BTC
- **Total Output**: 397.9999981 BTC
- **Fees**: 0.00002374 BTC
- **Fee per byte**: 10.504 sat/B
- **Fee per weight unit**: 2.626 sat/WU
- **Estimated BTC Transacted**: 289.89189 BTC

### Scripts

- **Coinbase**: Show scripts & coinbase

---

**Start Trading BTC, ETH, and BCH | Global OTC Marketplace**

| 0% trading fee | Perfect time to invest | Start Trading |

---

**2/8/2016 price is $370/BTC**

**approx $40K in 2/8/2016**
### WikiLeaks

#### Summary

<table>
<thead>
<tr>
<th>Address</th>
<th>1HB5XML.mzFVj8ALj6mfBsbfRoD4miY36v</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash 160</td>
<td>b169f2b0b866db05900b93a5d76345f18d3afb24</td>
</tr>
<tr>
<td>Tools</td>
<td>Related Tags - Unspent Outputs</td>
</tr>
</tbody>
</table>

#### Transactions

- **No. Transactions**: 26346
- **Total Received**: 4,041.90513436 BTC
- **Final Balance**: 1.74286901 BTC

If they still have all this, it would be worth $76 million in donations as of Dec 2017.

They've cleared out all but $30K worth.

---

https://blockchain.info/address/1HB5XML.mzFVj8ALj6mfBsbfRoD4miY36v
Bitcoin Address 1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v

1/17/2018

Start Trading BTC, ETH, and BCH | Global OTC Marketplace
| 0% trading fee | Perfect time to invest

WALLET | DATA | API | ABOUT

658e071f08d38b24c6c1a810511a93286d856932010...
16rHgdqLK3hNKqSSMy6cGxFBFZTQpbLgT

WikiLeaks
0.00001007 BTC
82 Confirmations
0.00001007 BTC

9a6dce69a7b9fe02cc51536da88cf8b206a6defbbda3...
1DxrPg52T5EoYCVLHJYYd7hc3odiqwPDh

WikiLeaks
0.02 BTC

f4bfc316a25ec2b72df0cdd0271c2540abf5e2c48eb...
1JqXh59iYVYgXefFPuZ7hGTaLU8ktVBQr8

WikiLeaks
0.00174287 BTC

0.00174287 BTC

c869263674ef16ce5daae83ef42a0d0935b3d16c5354...

18fyEQxAZQgCb... (HUMAN RIGHTS FOUNDATION )

WikiLeaks
0.00006974 BTC

0.00006974 BTC

c869263674ef16ce5daae83ef42a0d0935b3d16c5354...

1DxrPg52T5EoYCVLHJYYd7hc3odiqwPDh

WikiLeaks
0.02 BTC

f4bfc316a25ec2b72df0cdd0271c2540abf5e2c48eb...
1JqXh59iYVYgXefFPuZ7hGTaLU8ktVBQr8

WikiLeaks
0.00174287 BTC

0.00174287 BTC

https://blockchain.info/address/1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v

2/10
1/17/2018

Bitcoin Address 1HB5XMLmzFVj8ALj6mfBsbfIRoD4miY36v

4fe206008012c2d84d4fba8c0d8a78be706e98a7624... 2018-01-05 18:46:49
1QHEyeSzqpeGtx6JcvKpkw8sMDTq6HHjbn  WikiLeaks 0.0001 BTC

3e4db391643c15f38e2d1ab3423ec655de592fba10... 2018-01-05 18:16:17
38Lxu26qKqsYAL834DUBCSchIMQHx1M34d  WikiLeaks 0.08381841 BTC

557aae7d0c17ec053ec710cb6e5ff5ab6bacf2611ea3... 2018-01-04 05:33:22
18SfuL9vEe5SEQzCWppmirUNEjhUdfYBP  WikiLeaks 0.01666667 BTC

f3d1ce07ff2a74d1cbb5f914c16b55c9f66f70b1a4fa... 2018-01-01 23:09:18
3FnNn2XCRdYP7x7gzUhKTooPETmYxqNnx85  WikiLeaks 0.015 BTC

ea019fc054bce735d31f0c935987d46fca3b30266b3b... 2017-12-30 20:44:46
1E5H3sS42yNEUf7kCyJvKXqph6SZo5VnGX  WikiLeaks 0.00050225 BTC

https://blockchain.info/address/1HB5XMLmzFVj8ALj6mfBsbfIRoD4miY36v
<table>
<thead>
<tr>
<th>Transaction ID</th>
<th>Amount</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>419cd332f57033ad2b17acf27b121af4e39731b1134b...</td>
<td>0.00117594 BTC</td>
<td>2017-12-30 07:08:17</td>
</tr>
<tr>
<td>1KifNP9mZXXPhonJKT3pjXueeZScwpPPaK</td>
<td>0.01 BTC</td>
<td>2017-12-29 03:56:32</td>
</tr>
<tr>
<td>9633f4b24eab108bf4a930352f949e4370e71c8c2c1b...</td>
<td>0.001 BTC</td>
<td>2017-12-28 23:11:49</td>
</tr>
<tr>
<td>3QcMX9XeAxVDbovgdCmjFYrx9oi3G6wGL</td>
<td>0.01622 BTC</td>
<td>2017-12-27 22:11:56</td>
</tr>
<tr>
<td>ce4e9f4d9fa374166855b318500f9071d4ce35ce1e...</td>
<td>0.00024068 BTC</td>
<td>2017-12-27 21:58:03</td>
</tr>
<tr>
<td>1G7oyvioiBCKDgwKya2MAoSfQ3A1ucD43Xk</td>
<td>0.002 BTC</td>
<td>2017-12-07 06:43:17</td>
</tr>
<tr>
<td>4e36f34bdf9d51567ac6309b4a44ad118b43c59b2a...</td>
<td>0.00024068 BTC</td>
<td></td>
</tr>
<tr>
<td>18C5QCMEQzX1oLyqes1cqvneJZRTGQNMsv</td>
<td>0.012 BTC</td>
<td>2017-12-07 06:43:17</td>
</tr>
<tr>
<td>377eb7376e834e548439561b208d18ae09544e8c31...</td>
<td>0.002 BTC</td>
<td>2017-12-07 06:43:17</td>
</tr>
<tr>
<td>1MqvL5vHYFsCDwGDiJFvrSk3CzlQjGhyCj</td>
<td>0.002 BTC</td>
<td>2017-12-07 06:43:17</td>
</tr>
<tr>
<td>Hash</td>
<td>Label</td>
<td>Amount</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------</td>
<td>------------</td>
</tr>
<tr>
<td>ac4aaed830817f995f61b4e5d22ec5102202d1af86e54...</td>
<td>WikiLeaks</td>
<td>0.0006137 BTC</td>
</tr>
<tr>
<td>13fSCKPGqbnPvPXvQyowrfGhrWmVmp6mB</td>
<td>WikiLeaks</td>
<td>0.0006137 BTC</td>
</tr>
<tr>
<td>1d36682754b4ca4a58dcdfe9e6b81e02d22de777a03...</td>
<td>WikiLeaks</td>
<td>0.00010171 BTC</td>
</tr>
<tr>
<td>1D1hBKlf6KLP3cPHlteYCAuwxZgBFQsWHY</td>
<td>WikiLeaks</td>
<td>0.00010171 BTC</td>
</tr>
<tr>
<td>a8d7d3703204c1b274fa97f8c50f7d77c62b2349e424...</td>
<td>WikiLeaks</td>
<td>0.007 BTC</td>
</tr>
<tr>
<td>17yaXc9qkTu2qo6hAzkR2XsbrK503n5</td>
<td>WikiLeaks</td>
<td>0.007 BTC</td>
</tr>
<tr>
<td>b947440d03e7c2708d9cf22a3c7252e97dca35a0848...</td>
<td>WikiLeaks</td>
<td>0.00081824 BTC</td>
</tr>
<tr>
<td>1Cx7gzcQ7vYmxJPbqXE8pEavoGirMrJEP</td>
<td>WikiLeaks</td>
<td>0.00081824 BTC</td>
</tr>
<tr>
<td>294c4a7432597cb0d7c7f1416324eff30a011396a199...</td>
<td>WikiLeaks</td>
<td>0.0006869 BTC</td>
</tr>
<tr>
<td>1E09HZ2YntR3HMTgTdb1SJkLpjNu4yCUna</td>
<td>WikiLeaks</td>
<td>0.0006869 BTC</td>
</tr>
</tbody>
</table>
lots of transactions clearing donations out. Is this a regular December thing?
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Amount (BTC)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-12-15</td>
<td>12:21:20</td>
<td>-0.50961262BTC</td>
<td>WikiLeaks to 3PcWHnWbhkdEUHXpYADXdZJysPZnPphvgc</td>
</tr>
<tr>
<td>2017-12-15</td>
<td>12:19:59</td>
<td>-1.03078727BTC</td>
<td>WikiLeaks to 3PcWHnWbhkdEUHXpYADXdZJysPZnPphvgc</td>
</tr>
<tr>
<td>2017-12-15</td>
<td>12:18:07</td>
<td>-1.0133938BTC</td>
<td>WikiLeaks to 3PcWHnWbhkdEUHXpYADXdZJysPZnPphvgc</td>
</tr>
<tr>
<td>2017-12-15</td>
<td>12:17:22</td>
<td>-3.05234004BTC</td>
<td>WikiLeaks to 3PcWHnWbhkdEUHXpYADXdZJysPZnPphvgc</td>
</tr>
<tr>
<td>2017-12-15</td>
<td>12:16:09</td>
<td>-0.6264594BTC</td>
<td>WikiLeaks to 3PcWHnWbhkdEUHXpYADXdZJysPZnPphvgc</td>
</tr>
</tbody>
</table>

Lots of transactions clearing donations out. Is this a regular December thing?
<table>
<thead>
<tr>
<th>Date</th>
<th>Hash</th>
<th>Address</th>
<th>Amount</th>
<th>Transaction ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-12-15</td>
<td>1ef18517d1d3f2a75645c383c68ed067986c2aa7698b...</td>
<td>32kdimWbEGXLKANCBBAVTgxbQyb2NgVjL</td>
<td>10.18357123 BTC</td>
<td>10.18517193 BTC</td>
</tr>
<tr>
<td>2017-12-14</td>
<td>49acc4fa0da4ffeea93aca3a62458138bd3e2e2203c...</td>
<td>1AemMmBM9pXwEFjDW2JgQZtW5tHukrYrH</td>
<td>0.00182371 BTC</td>
<td>0.00182371 BTC</td>
</tr>
</tbody>
</table>