Part 2 – Security

• Unbelievable security of core system
• The mining industry
• Classical attacks
• Centralization
• Misaligned incentives:
  • Transactions
  • Mining
• Reducing pool sizes
• User-side security
Core System Availability

Almost always on.

Despite no shortage of attack motivation.
The March 2013 Fork

- Miner with version 0.8.0 generated a large block.
- Old versions rejected it.

Solution:
1. Major miners downgraded to pre-0.8.0.
2. Upgrade to 0.8.1 prevented large blocks.
3. 5 months later: Upgrade done right.
The Mining Industry
Mining

Difficulty rise:

Total Network Hash Rate

Hash Rate [TH/sec]

20,000
2,000
200
20

Mar’13   Jul’13   Jan’14

[Blockchain.info]
Mining Industry
Mining Industry
Mining Industry
Mining Industry

- Avalon
- ASIC Miner
- BitMine
- Butterfly Labs
- CoinTerra
- GAW Miners
- HashFast
- KnC Miner
- Spondoolies
Mining Industry

- Avalon
- ASIC Miner
- BitMine
- Butterfly Labs
- CoinTerra
- GAW Miners
- HashFast
- KnC Miner
- Spondoolies
Mining Industry

- Avalon
- ASIC Miner
- BitMine
- **Butterfly Labs**
- CoinTerra
- GAW Miners
- HashFast
- KnC Miner
- Spondoolies
Mining Industry
Mining Industry

This is what makes Bitcoin secure.
Classical Attacks
Double Spending

Eve buys coffee from Bob but keeps her money:

1. Eve buys coffee from Bob.

2. Bob provides product to Eve.

3. Eve spends the same money again.

Similar, but more feasible: The Finney attack
Majority Attacker, aka 51%

Attacker produces the longest chain.

Attacker cannot steal.
Attacker can:
• Require excessive transaction fees,
• take ransom from a single user, or
• prevent all transactions (DoS).
Centralization
Centralization

One entity gains control of the blockchain:
• Single majority miner
• Consortium of pools

Breaks Bitcoin’s essential premise.
Centralization

Pool GHash.IO (w/ CEX.IO) surpassed 50%. Community raged. DoS attacks on pool. GHash promptly reduced its rate.
Centralization

Pool GHash.IO (w/ CEX.IO) surpassed 50%. Community raged. DoS attacks on pool. GHash promptly reduced its rate.

(Almost) no good reason for such large pools.
• Nice interface.
• Good uptime.
Misaligned Incentives: Transaction Propagation
Transaction Propagation [1]

Nodes should propagate transactions. But why would they?

Actual incentive: don’t propagate.

Transaction Propagation [1]

DARPA Network Challenge ’09: Find 10 red balloons in US.

**Winner**: MIT Group

**Technique**:
- $2000 to finder
- $1000 to recruiter
- $500 to 2\textsuperscript{nd} recruiter
...

Transaction Propagation [1]

DARPA Network Challenge ’09: Find 10 red balloons in US.

Winner: MIT Group Technique:
$2000 to finder
$1000 to recruiter
$500 to 2\textsuperscript{nd} recruiter
...

Applicable to Bitcoin?

Red balloons technique not applicable to Bitcoin.

- Why recruit your own competition?
  Unlike balloons case where you recruit far away.

- Can masquerade as your own recruits.
  Unlike balloons case where you physically show up.

Transaction Propagation [1]

Solution sketch:

Set integers $H$ and $\beta$ according to topology. Then, for a chain of length $l$:

If $l > H$

- no reward.

Otherwise,

- miner gets $1 + (H - l + 1)\beta$,
- others get $1$.

Misaligned Incentives: Selfish Mining
Nakamoto’s Bitcoin mining protocol is incentive compatible (assuming an honest majority)

1. Best strategy: being honest

2. Revenue proportional to compute power
Selfish Mining [1]

Goal: Get more than fair share.
How: Maintain secret blocks, publish judiciously.

Intuition: Risk some work, others waste a lot.

[1] Eyal and Sirer: *Majority is not Enough: Bitcoin Mining is Vulnerable*, FC’14
Selfish Mining Algorithm

(a) Any state but two branches of length 1. Pool finds a block. Keep it secret. No revenue.
Selfish Mining Algorithm

(h) Lead more than 2. Others find a block. Publish one block. Selfish gets 1.
Selfish Mining Algorithm

(g) Lead of 2.
Others find a block.
Publish secret chain. Selfish gets 2.
Selfish Mining Algorithm

(f) Lead of 1.
Others find a block.
Publish secret block. No revenue.

\[ \gamma \]: Ratio of others that follow pool

\[ \gamma \]: Ratio of others that follow pool
Selfish Mining Algorithm

(b) Two branches of length 1.
Pool finds a block.
Publish branch. Selfish gets 2.
Selfish Mining Algorithm

(c) Two branches of length 1. Others find a block after pool head. Revenue: Each get 1.
(d) Two branches of length 1. Others find a block after others’ head. Revenue: Others get 2.
Selfish Mining Algorithm

(e) No private branch.
Others find a block.
Revenue: Others get 1.
Selfish Mining: Analysis
Selfish Mining – Probabilities

\[(1 - \gamma)(1 - \alpha)\]
\[\gamma(1 - \alpha)\]
\[\frac{\alpha}{1 - \alpha}\]

\[0'\]
\[1 - \alpha\]
\[1\]
\[\alpha\]
\[2\]
\[\alpha\]
\[3\]
\[\alpha\]
\[4\]
\[\alpha\]

\[(1 - \gamma)(1 - \alpha)\]
\[\gamma(1 - \alpha)\]
\[\frac{\alpha}{1 - \alpha}\]

\[0\]
\[1 - \alpha\]
\[1\]
\[\alpha\]
\[2\]
\[\alpha\]
\[3\]
\[\alpha\]
\[4\]
\[\alpha\]

\[\ldots\]
Selfish Mining – Probabilities

\[
\begin{align*}
\alpha p_0 &= (1 - \alpha)p_1 + (1 - \alpha)p_2 \\
p_0' &= (1 - \alpha)p_1 \\
\alpha p_1 &= (1 - \alpha)p_2 \\
\forall k \geq 2 : \alpha p_k &= (1 - \alpha)p_{k+1} \\
\sum_{k=0}^{\infty} p_k + p_0' &= 1
\end{align*}
\]
Selfish Mining – Revenue

\[
\begin{align*}
(1-\gamma)(1-\alpha) & \gamma(1-\alpha) \\
(1-\alpha) & \alpha \\
1 & 2 \\
2 & 3 \\
3 & 4 \\
4 & \cdots
\end{align*}
\]

Case (c)
\[
r_{\text{others}} = p_0' \cdot \gamma(1-\alpha) \cdot 1 + p_0' \cdot (1-\gamma)(1-\alpha) \cdot 2 + p_0 \cdot (1-\alpha) \cdot 1
\]

Case (d)
\[
r_{\text{pool}} = p_0' \cdot \alpha \cdot 2 + p_0' \cdot \gamma(1-\alpha) \cdot 1 + p_2 \cdot (1-\alpha) \cdot 2 + P[i > 2](1-\alpha) \cdot 1
\]
Auto-adjusting difficulty, so:

\[ R_{pool} = \frac{r_{pool}}{r_{pool} + r_{others}} \]
Selfish Mining – Analysis

![Graph showing the relationship between relative pool revenue and pool size. The graph demonstrates a linear increase in relative pool revenue as pool size increases. The line labeled "Honest mining" illustrates the trend.]
Selfish Mining – Analysis

- Honest mining
- $\gamma = 0$
- $\gamma = 0$ (sim)

Relative pool revenue vs Pool size graph.
Selfish Mining – Analysis

![Graph showing the relationship between relative pool revenue and pool size for different values of \( \gamma \). The graph includes lines and markers for Honest mining and two different values of \( \gamma \): \( \gamma = 0 \) and \( \gamma = 1 \).]
Selfish Mining – Analysis

![Graph showing relative pool revenue vs. pool size for different values of γ (0, 1/2, 1) and simulation results.

- Honest mining
- γ = 0
- γ = 1/2
- γ = 1
- γ = 0 (sim)
- γ = 1/2 (sim)
- γ = 1 (sim)
Selfish Mining: Implications
Attack Feasible

~February 2014

unknown

Ghash.IO

unknown

P2Pool

Slush

BTC Guild

Eligius

BTC Guild: 17%

Relative pool revenue

Pool size

Honest mining

γ = 0

γ = 0 (sim)

γ = 1/2

γ = 1/2 (sim)

γ = 1

γ = 1 (sim)
Catastrophe Scenario

After threshold:

Rational miners want to join selfish pool.
Catastrophe Scenario

Superlinear growth:
Selfish pool wants to grow.
Catastrophe Scenario

Rational miners want to join selfish pool.

+ Selfish pool wants to grow.

= Selfish pool may grow towards 50% NOT GOOD.
Attack Happening Now?

~February 2014

April 16, 2014

Selfish Mining Monitor

Threat Level: Low
Hardening the protocol

Algorithm change:
• Propagate all blocks of longest chain.
• Choose one at random to mine on.
Hardening the protocol

Algorithm change:
• Propagate all blocks of longest chain.
• Choose one at random to mine on.

Benefits:
• Proved threshold
• Backward compatible
• Progressive
• Simple
Reducing Pool Sizes
P2Pool [1]

A peer to peer distributed pool.

- A separate blockchain with Easy PoW
- Blocks distribute potential revenue among miners.
- Actual revenue on full PoW.

Pool Limiting

• Non-outsourcable PoW [1]
Cryptographic technique: A miner can steal from the pool when it finds a block.
  • Pool cannot outsource differently.
  • Block does not reveal secret.

• Permacoin [2]
Proof of storage rather than work.
Storage should not be outsourceable.

2-Phase Proof of Work

Split the proof of work.
- Phase 1: Standard Bitcoin, but easier.
- Phase 2: Requires coinbase secret key.

Benefits:
- Existing infrastructure controlled phase-out. HW, datacenters.
- Pool must trust miners to outsource phase 2. Miner could try and steal the coinbase.
User-side security
User-side Security

Client must keep private keys secret.

High availability vs. security

Individual and large organizations security differs only in scale.

Unprecedented security requirements from commodity systems.
Individuals

Tools:
• Standard client
• Software wallets (for phone)
• Online wallets
• Brain wallets
• Hardware wallets

Practice:
• Limited amount on phone
• Cold storage – replicated
• Use correct cryptography [1]

Large services

Tools:
- Plenty of firewalls
- Bullet proof front-end systems
- Bullet proof back-end systems

Practice:
- Cold storage
- Auditing

Powered by MongoDB

Flexcoin is shutting down.
On March 2nd 2014 Flexcoin was attacked and robbed of all coins in the hot wallet. The attacker made off with 896 BTC, dividing them into these two addresses:
1NDkevapt4SWYFEmquCDBif7DLMTNVggdu
1QFcC5JitGwpFKqRDd9QNH3eGN56dCNgy6
As Flexcoin does not have the resources, assets, or otherwise to come back from this loss, we are closing our doors immediately.
Transaction Malleability

Transaction hash used to track transactions. But it’s possible to change a transaction:

<table>
<thead>
<tr>
<th>input 1</th>
<th>output 1, amount 1</th>
</tr>
</thead>
</table>

Change scriptSig:
Still valid, for same content, different bits.
1. Change signature. (Crypto trick)
2. Change script. (Protocol trick)
Transaction Malleability

The MtGox con:
Transaction Malleability

The MtGox con:

1. Issue withdraw command.
2. Generate malformed txn, place in public buffer.
3. Change txn and publish it; get the money.
4. Call Mt.Gox to complain.
5. Pay again with new txn.
6. Get money again.
Miners and Pools

- The BGP attack
Miners and Pools

- The BGP attack
Miners and Pools

• The BGP attack

Get work, Send PoW

Get work, Send PoW
Miners and Pools

- The BGP attack
- Block Withholding
  Miner sends pool PoW
  Unless it’s an actual solution
Bitcoin: Concepts, Practice, and Research Directions

Part III
Other Research

Ittay Eyal, Emin Gün Sirer

Computer Science, Cornell University
DISC Bitcoin Tutorial, October 2014
Part 2 – Other Research

- Alt-coins
- Extensions
- Privacy
- Contemporary issues
Alt-coins & Extensions
Parameter changing

- Block frequency
  - Faster confirmation
  - More forks

- PoW choice
  - More green? (no)
  - More fair? (no)

- Difficulty adjustment rate
  - Defense against flash miners
Goal:
• Save some trees.
• Power to the users! (rather than miners)

Method:
• Proof of Stake (PoS) instead of Proof of Work: Lock coins to create block.

Goal:
- Save some trees.
- Power to the users! (rather than miners)

Method:
- Proof of Stake (PoS) instead of Proof of Work: Lock coins to create block.

But nothing is at stake!

Merged mining

Bitcoin PoW contains:
- Useless transaction (alt-coin header hash $x$)

Alt-coin PoW contains:
- Alt-coin header with hash $x$
- Bitcoin header with transaction $x$
Merged mining

Miners benefit from mining both chains together. So they do.

Alt-coin gets mining power from day one.
Smart Contracts

- Smart Contracts:
  - $m$ out of $n$ signatures.
  - Time-locked transactions:
    - Time to place in blockchain.
    - Time to use outputs.

- Ethereum: outsource distributed computing (got 31k BTC, at $18 million)
  - Transactions generate transactions.
  - Transactions activate one another.
Extensions

• Colored coins:
  Associate assets to individual Bitcoins.

• Side chains:
  • Faster
  • backed by main blockchain
  • less secure
Privacy
Transaction Tracking

All transactions remain in Blockchain forever.
Transaction Tracking

All transactions remain in Blockchain forever. One can associate addresses by **detective work**.

- For large scale crime? Not great.
- For somewhat secret activity? Pretty good.

[1] Ron and Shamir, FC’14
Zerocoin and Zerocash

Zerocash [2]:
Privacy preserving alt-coin on top of Bitcoin.
(preceded by Zerocoin [1])

The key:
The key: To move funds: prove* that “I know the secret for moving certain coins”.

Without revealing the sources or the value. But still preventing double-spending.

*Zero-knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARKs)

Stealth Addresses

The goal:
Untrackable transactions to public address.

The method:
1. Bob publishes address template $x$.
2. Alice sends Bitcoin to augmented address $x'$.
3. Bob finds $x'$ and controls it.

• No one but Alice and Bob know $x'$.
Need either Alice’s secrets or Bob’s.
• Only Alice controls $x'$. 
Contemporary Issues
Scalability

Initialization:
• Blockchain over 22GB. Linear growth.
• Long time for bootstrapping

Running (at 7 txn/sec):
  **CPU**: Insignificant
  **Memory**: ~100MB
  **Network**: ~30Kb/sec

Scalability

Lightweight clients: **Simple Proof Verification**

Initialization speedup: [1]
- Headers first
- UTXO first

UTXO and Mempool Maintenance

UTXO set becoming large.
Miners can choose to skip transaction verification.

Mempool becoming large
Miners can publish empty blocks.
Block Propagation Time

Block propagation time:
• Too long.
• Depends on block size.

Suggested solutions:
• Transaction set reconciliation.
• Header first.
BIP 70 – Payment Protocol

Customer

Wallet App

Merchant Server

Bitcoin P2P Network

click: "Pay Now"

Authorize?

click: "OK"

(optional) message

PaymentRequest

Payment

PaymentACK

transaction

transactions
Bitcoin: Concepts, Practice, and Research Directions

Part IV
Non-technical

Ittay Eyal, Emin Gün Sirer
Computer Science, Cornell University
DISC Bitcoin Tutorial, October 2014
Economy

- Deflationary (21 million total)

- What is it?
  - Store of value?
  - Method to transact USD?

- So what’s the potential value (USD/BTC)?
  - Function of mining cost? No! Rate is set.
  - Ratio of world economy?
  - Ratio of world transactions, and a function of the time it needs to store value?
Reasons for Volatility

• Regulation
  • Anti Money Laundering (US/Europe)
  • Adoption / rejection (China, Russia)
  • Fiat regulation (Cyprus, greece)
• Adoption
  • Large companies (Dell, PayPal)
  • Illegal (Silk Road)
• Security
  • Mt. Gox
• Technical
  • Not really
Tax

Commodity or currency? Something else?

Revenue in Bitcoin

Exchange

Mining?
Legal

• Payment for illicit goods.

<table>
<thead>
<tr>
<th>Shop by category:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannabis(203)</td>
</tr>
<tr>
<td>Ecstasy(35)</td>
</tr>
<tr>
<td>Psychedelics(127)</td>
</tr>
<tr>
<td>Opioids(39)</td>
</tr>
<tr>
<td>Stimulants(68)</td>
</tr>
<tr>
<td>Dissociatives(9)</td>
</tr>
<tr>
<td>Other(197)</td>
</tr>
<tr>
<td>Benzos(43)</td>
</tr>
</tbody>
</table>

1 hit of LSD (blotter) $0.58
1/8 oz high quality cannabis $2.05
1 g pure MDMA (white) $1.28

Step-by-step:
1. Get anonymous money
2. Buy something here
3. Enjoy it when it arrives!

Vacation mode. Important info for sellers...

• Money laundering
  • Tumblers
  • w/ pool fees
  • Bitcoin ATMs
Community

Diverse – a lot of players

• Community health
  • Maturing

• Governance
  Mostly the Bitcoin Foundation
  • Protocol changes
  • Interaction with state regulation
  • Bitcoin central bank?

• Large service auditing
Conclusion
Conclusion

input 1
input 2
input 3
output 1, amount 1
output 2, amount 2

B
C

GET STRATUM

Copyright © 2014 Ittay Eyal, Emin Gün Sirer