Bitcoin and Cryptocurrencies
and what they mean for cybersecurity research

Andrew Miller
Dec 7, 2015

http://www.cs.umd.edu/~amiller/
https://twitter.com/socrates1024
The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of

bitcoin-0.1.0.rar
bitcoin-0.1.0.tgz
Silk Road Creator Ross Ulbricht Sentenced to Life in Prison

Wired - May 29, 2015
On Friday Ulbricht was sentenced to life in prison without the possibility of parole for his role in creating and running Silk Road's billion-dollar, ...

Corrupt DEA Agent Pleads Guilty To Extorting Bitcoin From

Forbes - Jul 1, 2015
Carl Mark Force IV, 46, served on the Baltimore Silk Road Task Force from 2012 to 2014 as the lead agent in charge of investigating and ... Former Silk Road DEA Agent Pleads Guilty to Bitcoin Theft

VIP at illegal-drug site Silk Road nabbed in Thailand, police say - CNET

CNET - 1 day ago
The right-hand man of Ross Ulbricht -- convicted mastermind of Silk Road, the notorious ...
$5B Total Market Cap
Bitcoin Still Small Compared to Major Currencies

<table>
<thead>
<tr>
<th>Country</th>
<th>M1 Money Supply (USD Bli)</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>2,705</td>
</tr>
<tr>
<td>Australia</td>
<td>255</td>
</tr>
<tr>
<td>Guatemala</td>
<td>8</td>
</tr>
<tr>
<td>Bitcoin</td>
<td>7</td>
</tr>
</tbody>
</table>

Source: Fitch, Federal Reserve, Reserve Bank of Australia, Banco de Guatemala, blockchain.info, CoinDesk.com
Cryptology ePrint Archive: Search Results

2015/1164  2015/702  (PDF)
Beyon  Demystifying inc
Pasqua  Loi Luu and Jason
2015/1019  2015/607  (PDF)
Speed  Fast and
Aggelos  Alex Bird
2015/1015  2015/578  (PDF)
On Bi  Authent
Joseph  Patrick M
2015/1008  2015/518  (PDF)
Provis  Eclipse
Gaby C  Ethan He
2015/1007  2015/482  (PDF)
How t  Research
Zhichao  Joseph B
2015/946  2015/478  (PDF)
Asym  On Pow
Alex B  Loi Luu
2015/796  2015/469  (PDF)
Stubb  Hierarch
Kartik  Gus Guta
2015/792  2015/464  (PDF)
Shadow-Bitcoin:  A Denia
Andrew Miller and  Jethro Bu
2014/886  (PDF)
Stubb  Account
Kartik  Giuseppe

ACM CCS 2015

Session 3A
Using Cryptocurrency
Session 7A
CryptoCurrency
## Distribution of (Reachable) Nodes

<table>
<thead>
<tr>
<th>RANK</th>
<th>COUNTRY</th>
<th>NODES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>United States</td>
<td>2685 (41.81%)</td>
</tr>
<tr>
<td>2</td>
<td>Germany</td>
<td>519 (8.08%)</td>
</tr>
<tr>
<td>3</td>
<td>Canada</td>
<td>412 (6.42%)</td>
</tr>
<tr>
<td>4</td>
<td>France</td>
<td>360 (5.61%)</td>
</tr>
<tr>
<td>5</td>
<td>United Kingdom</td>
<td>353 (5.50%)</td>
</tr>
<tr>
<td>6</td>
<td>Netherlands</td>
<td>271 (4.22%)</td>
</tr>
<tr>
<td>7</td>
<td>Russian Federation</td>
<td>221 (3.44%)</td>
</tr>
<tr>
<td>8</td>
<td>China</td>
<td>161 (2.51%)</td>
</tr>
</tbody>
</table>
Bitcoin is not alone

Between 150-500 altcoins launched to date

Data from mapofcoins.com
Bitcoin is a legitimately novel approach to distributed system design.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ever-growing chain of
Ideal Bank Account Functionality

Public Bank

Alice: $08
Bob: $22

Account Balances

-2
+2

“Alice: Send $2 from my account to Bob.”

“Bob: You’ve got Money! $2 from Alice.”

A single transaction: Ledger -> Ledger’ (or failure)
Valid transactions don’t spend more money than they have.

(note: privacy is not provided)
What are the security goals?

- Money supply is conserved
  Alice can’t spend more money than she has

- Transactions are “authorized”
  Alice can’t spend Bob’s money

- The service is “available”
  Bob can’t prevent Alice from spending her money

- Transactions are consistent, permanent
  Alice can’t send Bob money, and then take it back
1. Implement the Bank as a trusted third party (e.g., Paypal)

- Digitally signed messages, or password authentication

"Send $2 from my account to Bob."
2. Implement the Bank as a multi-party computation

- Standard results in fault-tolerance apply here, (e.g. paxos, bft)

- PKI or similar is assumed
Why not just include everyone?

- Protocols are unscalable
- How to prevent Sybil attacks without administrators?
From Ideal to Bitcoin in 5 Steps

3. Suppose we have a magic token that chooses parties at random.

Whoever has the token gets to broadcast *once*.

If \( t \) parties are malicious, \( \Pr[\text{honest selected}] = \frac{n-t}{t} \)

Thm. *If majority are honest, transaction log converges*
From Ideal to Bitcoin in 5 Steps

4. Replace the token with computational puzzle
   - Solvable by independent participants
   - No advantage over brute force

$$\text{Scratch}_d^{(puz, m)}: \ r \leftarrow \{0,1\}^k; \ \text{if} \ H(puz \ || \ m \ || \ r) < 2^{k-d} \ \text{then} \ \text{return} \ r$$
From Ideal to Bitcoin in 5 Steps

5. Finally, provide participation incentives

- give each “lottery winner” a reward
- also solves the problem of initial allocation
How mining works

How mining works

prev: \( H(\ ) \)
mrkl_root: \( H(\ ) \)
nonce: \( 0x7a83 \)
hash: \( 0x0000 \)

prev: \( H(\ ) \)
mrkl_root: \( H(\ ) \)
nonce: \( 0xf77e\ldots \)
hash: \( 0x0000\ldots \)

25.0→A
coinbase: \( 0x3df5\ldots65 \)

transaction
transaction
transaction
Alice: $10
Bob: $20

anyone

Alice: $08
Bob: $22

volunteers

Alice

Bob
Bitcoin miners earn ~$1M per day
Mining difficulty adjusts over time
GPU mining

- GPUs designed for high-performance graphics
  - high parallelism
  - high throughput
- First used for Bitcoin ca. October 2010
- Implemented in OpenCL
  - Later: hacks for specific cards
FPGA mining

- Field Programmable Gate Area
- First used for Bitcoin ca. June 2011
- Implemented in Verilog
Bitcoin ASICs

TerraMiner™ IV – 2TH/s Networked ASIC Miner

$5,999

Shipping June 2014

300 GH Bitcoin Mining Card
The Monarch BPU 300 C

$1,497.00

Pre-Order Terms: This is a pre-order. 28nm ASIC bitcoin mining hardware products are shipped according to placement in the order queue, and delivery may take 3 months or more after order. All sales are final.
Professional mining centers

Needs:
- cheap power
- good network
- cool climate
Evolution of mining

CPU
GPU
FPGA
ASIC

gold pan
sluice box
placer mining
pit mining
Whirlwind tour of cryptocurrency research topics

*SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies.*
Cryptocurrencies are at the cutting edge of usable security
Bitcoin UX is Cryptography COME ALIVE
Ad-hoc cryptographic marketplaces

**Bitcoin-OTC**: 12,000 users with PGP keys

“Web-of-Trust” reputation tracking tool
Bitcoin sidestepped 30+ years of research in E-Cash

“First Generation” cryptocurrencies:
- Blind Signatures and untraceable payments. David Chaum, 1982
- Payword and Micromint. Rivest and Shamir. 2001

Many of these old ideas can be seen in new light
It is a surprise that Bitcoin has survived this long.

Science is needed.
Attack Modeling --- Example: 51% attacks

Goldfinger Attack?
Alice: $08
Bob: $22

Is mining needed at all?
Competition from Bitcoin is forcing financial institutions to upgrade.
The potential future of Programmable Money
Example: 2-player lottery

&Alice, &Bob  (hardcoded pubkeys)
wait to receive $10 from &Alice
wait to receive $10 from &Bob
pick a random bit x
if x == 0: send $20 to &Alice
    else: send $20 to &Bob
Possible Applications

- Games: board games, gambling, etc
- Global services
  - Domain Name Registration
- Financial coordination
  - Auctions
  - Crowdfunding (reach the target, or get refunded)
  - Risk swaps / betting / prediction markets
- Service Level Agreement enforcement
  - Is the server computing the right results?
  - Is the server storing the data? With redundancy?
  - Has the server provisioned enough resources?
  - Does the server have insurance?
Cryptocurrencies are an “upbeat” theme for cybersecurity --- an opportunity to “build security in”
Use smart contracts to teach applied cryptography: signatures, Merkle trees, proofs-of-retrievability, ZK proofs

Towards Safe Smart Contracts

- Virtual machine images (to simplify setup)
- Self-contained guide, notes
- Recorded lectures from 1-day workshop
Nonoutsourceable puzzles to discourage Bitcoin mining coalitions

Andrew Miller / University of Maryland
+ Ahmed Kosba, Elaine Shi, Jonathan Katz

CCS 2015
Decentralized  Robust, Trustworthy
Incentive Structure → Decentralized → Robust, Trustworthy
June 12, 2014
GHash.IO large mining pool crisis

GHash Commits to 40% Hashrate Cap at Bitcoin Mining Summit

Stan Higgins | Published on July 16, 2014 at 18:40 GMT
In counting there is strength.
How do coalitions form?

Can we fix the incentive mechanism to discourage them?
Typical Bitcoin mining pool

Pool Operator

Solution!

“shares”

Payout divided among members

Pool Members
Encouraging *defection* from pools

Pool Operator

“shares”

Pool Members

Solution found!

Take the money and run!