Virtual Currencies: Obstacles and Applications Beyond Currency

Sarah Meiklejohn (University College London)
ECB categories of virtual currencies
ECB categories of virtual currencies
ECB categories of virtual currencies

- "closed"
- "one direction"
ECB categories of virtual currencies

- **“closed”**
  - $x$
  - £
  - €

- **“convertible”**
  - $x$
  - £
  - €

- **“one direction”**
  - £
  - €

- **“convertible”**
  - £
  - €
  - $x$
ECB categories of virtual currencies

- "closed"
- "convertible" centralized
- "one direction"
- "convertible"
ECB categories of virtual currencies

- **“closed”**
  - $x
  - £
  - €

- **“convertible” centralized**
  - $x
  - £
  - €

- **“convertible” decentralized**
  - $x
  - £
  - €

- **“one direction”**
  - $x
  - £
  - €
ECB categories of virtual currencies

- "closed"
- "convertible" centralized
- "one direction"
- "convertible" decentralized
decentralized consensus
decentralized consensus
decentralized consensus

updatable
decentralized consensus

updatable

globally visible
decentralized consensus

- updatable
- globally visible
- immutable
decentralized consensus

“mining”

updatable

globally visible

immutable
decentralized consensus

“mining”

updatable

globally visible

immutable
the hype cycle of cryptocurrencies
the **hype cycle** of cryptocurrencies
the **hype cycle** of cryptocurrencies

“technology trigger”
2009  2010  2011  2012  2013  2014

Bitcoin paper
Bitcoin paper
2009

Bitcoin deployed
2010

$1 = 0.0007
2011

time

2012

2013

2014
Bitcoin paper

2009

Bitcoin deployed

$1 = $0.0007

2010

MtGox opens

2011

2012

2013

2014

time
2009: Bitcoin paper
2010: $1 = $0.0007
2011: Bitcoin deployed
2011: MtGox opens
2013: first mining pool block
Bitcoin deployed

2009

Bitcoin paper

$0.0007

2010

MtGox opens

2011

Silk Road opens

2012

first mining pool block

2013

2014

$1
Bitcoin paper
Bitcoin deployed
MtGox opens
Silk Road opens
first mining pool block

\[ B_1 = 0.0007 \]

\[ B_1 = 1 \]

\[ B_1 = 32 \]
“peak of inflated expectations”
new businesses
new businesses
new cryptocurrencies ("altcoins")

- **2009**: Bitcoin paper
- **2010**: Bitcoin deployed
- **2011**: Silk Road opens
- **2012**: MtGox opens, B1 = $1
- **2013**: B1 = $32
- **2014**: New cryptocurrencies ("altcoins")
new cryptocurrencies ("altcoins")

- **2009**
  - Bitcoin paper
  - Bitcoin deployed
  - \( B_1 = \$0.0007 \)

- **2010**
  - MtGox opens

- **2011**
  - Silk Road opens
  - \( B_1 = \$1 \)
  - Namecoin

- **2012**
  - \( B_1 = \$32 \)
  - Litecoin
  - Peercoin

- **2013**
  - Ripple
  - Feathercoin
  - Mastercoin
  - Quark
  - Dogecoin
  - Primecoin
  - Nxt

- **2014**
  - Darkcoin
<table>
<thead>
<tr>
<th></th>
<th>Coin</th>
<th>Value (USD)</th>
<th>Price (USD)</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin</td>
<td>$4,321,327,369</td>
<td>$316.03</td>
<td>13,673,875 BTC</td>
</tr>
<tr>
<td>2</td>
<td>Ripple</td>
<td>$753,476,625</td>
<td>$0.024323</td>
<td>30,978,075,200 XRP *</td>
</tr>
<tr>
<td>3</td>
<td>PayCoin</td>
<td>$100,507,953</td>
<td>$8.15</td>
<td>12,325,837 XPY **</td>
</tr>
<tr>
<td>4</td>
<td>Litecoin</td>
<td>$95,072,164</td>
<td>$2.70</td>
<td>35,218,304 LTC</td>
</tr>
<tr>
<td>5</td>
<td>BitShares</td>
<td>$40,746,199</td>
<td>$0.016312</td>
<td>2,497,973,773 BTS *</td>
</tr>
<tr>
<td>6</td>
<td>MaidSafeCoin</td>
<td>$23,192,451</td>
<td>$0.051248</td>
<td>452,552,412 MAID *</td>
</tr>
<tr>
<td>7</td>
<td>Stellar</td>
<td>$19,533,919</td>
<td>$0.005492</td>
<td>3,557,060,725 STR *</td>
</tr>
<tr>
<td>8</td>
<td>Dogecoin</td>
<td>$17,889,012</td>
<td>$0.000184</td>
<td>97,204,400,153 DOGE</td>
</tr>
<tr>
<td>9</td>
<td>Nxt</td>
<td>$17,504,849</td>
<td>$0.017505</td>
<td>999,997,096 NXT *</td>
</tr>
<tr>
<td></td>
<td>Symbol</td>
<td>Value 1</td>
<td>Value 2</td>
<td>Value 3</td>
</tr>
<tr>
<td>---</td>
<td>----------</td>
<td>---------</td>
<td>---------</td>
<td>------------------</td>
</tr>
<tr>
<td>28</td>
<td>Quark</td>
<td>$1,324,931</td>
<td>$0.005331</td>
<td>248,529,548 QRK</td>
</tr>
<tr>
<td>29</td>
<td>CoinoUSD</td>
<td>$1,208,710</td>
<td>$1.05</td>
<td>1,154,584 COINO *</td>
</tr>
<tr>
<td>30</td>
<td>InstantDEX</td>
<td>$1,208,630</td>
<td>$1.21</td>
<td>1,000,000 DEX *</td>
</tr>
<tr>
<td>31</td>
<td>DNotes</td>
<td>$1,140,315</td>
<td>$0.012011</td>
<td>94,940,826 NOTE</td>
</tr>
<tr>
<td>32</td>
<td>Pangea Poker</td>
<td>$1,102,710</td>
<td>$1.10</td>
<td>999,402 PANGEA *</td>
</tr>
<tr>
<td>33</td>
<td>Feathercoin</td>
<td>$1,051,275</td>
<td>$0.015819</td>
<td>66,455,200 FTC</td>
</tr>
<tr>
<td>34</td>
<td>ReddCoin</td>
<td>$1,042,389</td>
<td>$0.000038</td>
<td>27,310,972,002 RDD</td>
</tr>
<tr>
<td>35</td>
<td>BitUSD</td>
<td>$917,585</td>
<td>$1.05</td>
<td>873,433 BITUSD *</td>
</tr>
<tr>
<td>36</td>
<td>Primecoin</td>
<td>$823,269</td>
<td>$0.097423</td>
<td>8,450,498 XPM</td>
</tr>
</tbody>
</table>
soaring exchange rate
soaring exchange rate
soaring exchange rate
soaring exchange rate
soaring exchange rate
regulatory interest

Bitcoin.de and Fidor Bank AG Agree on Large-Scale Partnership

Bitcoin-Central becomes first Bitcoin exchange licensed to operate like a bank

New Money Laundering Guidelines Are A Positive Sign For Bitcoin

This Senate hearing is a Bitcoin lovefest
news media

YC-Backed Buttercoin Uses Bitcoin To Attack The $500B-A-Year Remittances Economy

Silicon Valley catches Bitcoin fever

2013: Year Of The Bitcoin

Why Bitcoin Is Poised To Change Society Much More Than The Internet Did
“trough of disillusionment”
Bitcoin might not be as \_\_\_\_\_\_\_\_ as we hoped.
Bitcoin might not be as decentralized as we hoped.
Bitcoin might not be as decentralized as we hoped.
Bitcoin might not be as **decentralized** as we hoped.
Bitcoin might not be as decentralized as we hoped.
Bitcoin might not be as secure as we hoped.

decentralized

Elliptic Curve Cryptography in Practice

Joppe W. Bos\(^1\), J. Alex Halderman\(^2\), Nadia Heninger\(^3\), Jonathan Moore, Michael Naehrig\(^1\), and Eric Wustrow\(^2\)

Android bug batters Bitcoin wallets
Bitcoin might not be as **secure** as we hoped.

---

**Elliptic Curve Cryptography in Practice**

Joppe W. Bos¹, J. Alex Halderman², Nadia Heninger³, Jonathan Moore, Michael Naehrig¹, and Eric Wustrow²

---

**Android bug batters Bitcoin wallets**

Deterministic Wallets, Their Advantages and their Understated Flaws
Bitcoin might not be as secure as we hoped.

decentralized

Elliptic Curve Cryptography in Practice

Joppe W. Bos¹, J. Alex Halderman², Nadia Heninger³, Jonathan Moore, Michael Naehrig¹, and Eric Wustrow²

Android bug batters Bitcoin wallets

Deterministic Wallets, Their Advantages and their Understated Flaws

Bitcoin “Brainwallets” and why they are a bad idea
Bitcoin might not be as anonymous as we hoped. Decentralized secure.
Bitcoin might not be as **anonymous** as we hoped.

decentralized

secure

[RH, RS, A+, M+, M13, SMZ14]
Bitcoin might not be as anonymous as we hoped. It is not decentralized and secure.

[RH, RS, A+, M+, M13, SMZ14] [A14, MO15]
Bitcoin might not be as stable as we hoped.
Bitcoin might not be as stable as we hoped.

- decentralized
- secure
- anonymous

$1000 $881 $640 $650 $420 $320

Jan Apr Oct Dec Jan Apr Jun Dec
Bitcoin might not be as useful as we hoped.

decentralized
secure
anonymous
stable
Bitcoin might not be as useful as we hoped.

decentralized
secure
anonymous
stable

The 'Killer Bitcoin App' Has Yet To Arrive

Bitcoin Is Still Adrift

CoinSummit Venture Capitalists Seek 'Killer' Bitcoin App
Bitcoin might not be as **useful** as we hoped.

- stable
- decentralized
- secure
- anonymous
- stable

---

**The 'Killer Bitcoin App' Has Yet To Arrive**

**Bitcoin Is Still Adrift**

**CoinSummit Venture Capitalists Seek 'Killer' Bitcoin App**

**Is Apple Pay a bitcoin killer?**
Bitcoin might not be as useful as we hoped.

decentralized
secure
anonymous
stable

IN-DEPTH: BANGLADESH BANS BITCOIN

Russia Proposes Monetary Penalties for Bitcoin Use and Promotion
“slope of enlightenment”
how to timestamp
how to timestamp

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn  Marjori Pomarole  Grant Jordan
Kirill Levchenko  Damon McCoy  Geoffrey M. Voelker  Stefan Savage
how to timestamp

\( H(\text{addr}) \)

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn  Marjorie Pomarole  Grant Jordan
Kirill Levchenko  Damon McCoy  Geoffrey M. Voelker  Stefan Savage
how to timestamp

\[ H(\text{addr} \rightarrow \text{btc} \rightarrow \text{addr}) \]

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, Stefan Savage
how to timestamp

\[ H(\text{addr}) \]

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn  Marjori Pomarole  Grant Jordan
Kirill Levchenko  Damon McCoy  Geoffrey M. Voelker  Stefan Savage

addr \rightarrow\text{btc} \rightarrow addr
how to timestamp

H(addr) → btc → addr

“21/8/13 @ 11:08”
how to timestamp

\( H(\text{addr} \rightarrow \text{btc} \rightarrow \text{addr}) \)

"21/8/13 @ 11:08"
H( )

addr → btc → addr

“21/8/13 @ 11:08”
$$H(\text{addr} \rightarrow \text{btc} \rightarrow \text{addr})$$

TIME

“20/7/69 @ 20:18”

updatable
H(  )

addr → btc → addr

“20/7/69 @ 20:18”

updatable

globally visible
H(addr)  (addr)  “20/7/69 @ 20:18”

updatable
globally visible
immutable
notary publics

Select a document and have it certified in the Bitcoin blockchain

Click here or drag and drop your document in the box.
The file will NOT be uploaded. The cryptographic proof is calculated client-side.

Sign a document
Upload a document and sign it or get it signed.

Verify a document
Check the authenticity of a document signed on BlockSign.
how to **claim ownership**

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn  Marjori Pomarole  Grant Jordan
Kirill Levchenko  Damon McCoy  Geoffrey M. Voelker  Stefan Savage

H

addr -> btc -> addr

[Diagram showing a network of addresses and transactions]
how to **claim ownership**

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn  Marjori Pomarole  Grant Jordan
Kirill Levchenko  Damon McCoy  Geoffrey M. Voelker  Stefan Savage

**H**

$\text{addr} \xrightarrow{\text{btc}} \text{addr}$

eprint
how to **claim ownership**

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn  Marjori Pomarole  Grant Jordan
Kirill Levchenko  Damon McCoy  Geoffrey M. Voelker  Stefan Savage

\[ \text{addr} \xrightarrow{\text{btc}} \text{addr} + \text{signature} \xrightarrow{\text{eprint}} \]
how to **claim ownership**

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn Marjorie Pomarole Grant Jordan
Kirill Levchenko Damon McCoy Geoffrey M. Voelker Stefan Savage

\[ H(\text{addr} + \text{signature}) \rightarrow \text{eprint} \]
how to claim ownership

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn  Marjori Pomarole  Grant Jordan
Kirill Levchenko  Damon McCoy  Geoffrey M. Voelker  Stefan Savage

H(addr + signature)

eprint

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn  Marjori Pomarole  Grant Jordan
Kirill Levchenko  Damon McCoy  Geoffrey M. Voelker  Stefan Savage
how to **claim ownership**

\[ H(\text{addr} + \text{signature}) \]

\[ H(\text{eprint}) \]
"file":"http://static.mccoyspace.com/gifs/cars.gif", "post":"https://twitter.com/mccoyspace/status/462455439930966016", "hash":"f3969884355163f4d336fdef318d671d1d12616e60bb1dcb6be67f3a177a63d4", "title":"I hereby assert title to the file at the URL listed. It was originally published at the post URL. The file whose SHA265 hash is as indicated herein is the file in question. Title to file transfers to whoever controls this blockchain entry"
"file":"http://static.mccoyspace.com/gifs/cars.gif", "post":"https://twitter.com/mccoyspace/status/462455439930966016", "hash":"f3969884355163f4d336def318d671d11d12616e60bb1dcb6be67f3a177a63d4", "title":"I hereby assert title to the file at the URL listed. It was originally published at the post URL. The file whose SHA265 hash is as indicated herein is the file in question. Title to file transfers to whoever controls this blockchain entry"}
how to prove history

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn  Marjori Pamarole  Grant Jordan
Kirill Levchenko  Damon McCoy  Geoffrey M. Voelker  Stefan Savage

H((addr) → btc → addr) +signature → eprint
how to prove history

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn  Marjori Pomarole  Grant Jordan
Kirill Levchenko  Damon McCoy  Geoffrey M. Voelker  Stefan Savage
how to prove history
how to prove history

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn  Marjori Pomarole  Grant Jordan
Kirill Levchenko  Damon McCoy†  Geoffrey M. Voelker  Stefan Savage

Characterising

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn  Marjori Pomarole  Grant Jordan
Kirill Levchenko  Damon McCoy†  Geoffrey M. Voelker  Stefan Savage

Characterising
The Future of Wine Provenance Is Bitcoin
The Future of Wine Provenance Is Bitcoin

no blood diamonds!

belonged to a queen!
county records office / land registry
county records office / land registry
county records office / land registry
ethereum
proof of existence
proof of ownership
proof of existence
proof of history
proof of ownership
proof of existence
proof of history
proof of ownership
proof of existence

updatable
globally visible
immutable
Bitcoin might not be as \underline{decentralized} as we hoped.

\underline{Secure} \underline{Anonymous} \underline{Stable} \underline{Useful}

\underline{Proof of ownership} \underline{Proof of history} \underline{Proof of existence}
Bitcoin might not be as \underline{stable} as we hoped.

\underline{Anonymous} \underline{Secure} \underline{Decentralized} \underline{Useful}

\underline{Proof of ownership} \underline{Proof of history} \underline{Proof of existence}

\underline{Updatable} \underline{Globally visible} \underline{Immutable}
Bitcoin might not be as [ ] as we hoped.

- decentralized
- secure
- anonymous
- stable
- useful

Less crucial in these contexts?

- proof of history
- proof of ownership
- proof of existence

- updatable
- globally visible
- immutable
“plateau of productivity”
what can real world cryptographers do?
what can real world cryptographers do?

increase usability to improve security
what can real world cryptographers do?

increase \textit{usability} to improve \textit{security}

enforce \textit{decentralization}
what can real world cryptographers do?

increase **usability** to improve **security**

enforce **decentralization**

( solutions for **burn transactions**

( solutions for **bloat problem** )

what can real world cryptographers do?

increase **usability** to improve **security**

enforce **decentralization**

( solutions for **burn transactions**

( solutions for **bloat problem**

**audit** software)
what can real world cryptographers do?

increase **usability** to improve **security**

enforce **decentralization**

(solutions for **burn transactions**)

(solutions for **bloat problem**)

**audit** software

apply **proofs of history/ownership** to crypto
Thanks! Any questions?