Viral Money

Independent, distributed, computational currencies
and their byproducts and implications

March, 2016
The Simple Stuff: an independent currency

Bitcoin solves double spending via
• distributed ledger
• proof of work consensus

It also features
• Scripting (e.g., checklocktimeverify)

Also withstands “51% attacks”
Grownups: the blockchain

Blockstack: Private blockchain (PWC)
Ethereum: Turing Complete
Namecoin: DNS on the blockchain
Ripple and Stellar: Programmable money

Contracts: Digital rights
Identity: Enigma
Certified mail: MIT Thesis
Medrec: Records access and validation
But

Remember the metaphor: It doesn’t have to be Bitcoin to be inspirational and disruptive. But that’s what got us started.

Maybe we think about trust in a new way.

Legacy systems are potentially challengeable
Asleep at the switch systems can be challenged
What is the law, anyway?

You might smell tulips, but they are still around
Grownups: the blockchain

Public
Distributed
Trustless
Time-stamped
Append-only list
Decentralization

9-11

Wiki-Leaks

End of AMPS

Snowden

Bitcoin

UN: Access as a human right

Aaron Swartz

FCC Neutral

Korean E-Sports Association

Wifi
Muni - SF

Debate
US Presidents
YouTube

Wardrobe Failure

Crash

Crash

Viral Communications
March, 2016

Andrew Lippman
End

Fun stuff follows
Perspective: Paypal, Square, ApplePay

Paypal, 1998
4.9 billion payments in 2015
$228 Billion in 2014
179 million accounts
200 markets, 100 currencies
paypal.me: via web link

Square, 2008
Web link

ApplePay, 2014
Essentially NFC credit card

Paypal was Confinity; Blackberry service
The Simple Stuff: an independent currency

Bitcoin is a political and a technical statement.

It has a permanent, distributed, trustless, time-stamped, append-only list of transactions (for 6 years)

It is a deflationary currency

It is unpegged and floating

It is decentralized

It does not guarantee anonymity

Open source, has miners, developers and exchanges
How it works

submit a transaction with payers and payees to the network
“Miners” amalgamate a “block” every ten minutes
Valid blocks propagate to miners and full nodes
If there are simultaneous solutions, longest chain wins

Software is maintained by core developers and others
Proof of work difficulty is updated periodically
Miners get a reward for creating a block

Cost is ~ $7500/block in lost energy and capital
Perspective: Second Life

Linden Labs, 1999
Second Life, 2002
Linden Dollar, 2003
L$240 = US$1.00

Still crazy after all those years
## The new money

<table>
<thead>
<tr>
<th>Cryptocurrency</th>
<th>Market cap in $Millions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitcoin</td>
<td>6,036</td>
</tr>
<tr>
<td>Ethereum</td>
<td>918</td>
</tr>
<tr>
<td>Ripple</td>
<td>268</td>
</tr>
<tr>
<td>Litecoin</td>
<td>140</td>
</tr>
<tr>
<td>MaidSafeCoin</td>
<td>43</td>
</tr>
<tr>
<td>Dash</td>
<td>31</td>
</tr>
<tr>
<td>Dogecoin</td>
<td>23</td>
</tr>
<tr>
<td>Monero</td>
<td>14</td>
</tr>
</tbody>
</table>

Market cap in $Millions
Take-away

The blockchain can only be supported by a currency that is independent of any other and inherently wasteful to create.

Governance is a serious problem

Scaling is the forcing function

$1 Billion invested; $5 Billion in value
Viral Money

Digital Currency Initiative

Financial
- Bitcoin
- Other

Ledger/Contract
- Permission
- Open/Public

Ripple, Stellar, Ethereum, ML Certs
Rates of Exchange

Easy to create, agree and inherent value
Contrast two currencies, gold and fiduciary.

Gold has 5000 years of inherent value.

Gold

Fiduciary

Energy

Free

Inherent Value

No Inherent Value

Gold has 5000 years of inherent value
# Rates of Exchange

A good currency has
- no real use
- is valued by all
- is rare

<table>
<thead>
<tr>
<th>Gold</th>
<th>Fiduciary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy</td>
<td>Free</td>
</tr>
<tr>
<td>Inherent Value</td>
<td>No Inherent Value</td>
</tr>
</tbody>
</table>
What are the problems we want to solve?


Rates of Exchange

Generational change versus evolution
Rates of Exchange

Lots of energy for something of no inherent value
Rates of Exchange

- **Gold**
  - Energy
  - Inherent Value

- **Fiduciary**
  - Free
  - No Inherent Value

Natural cost of a block is ~bitcoin, about $390 (x25)

Lots of energy for something of no inherent value
Rates of Exchange

Transactions require an account — yet more overhead

Lots of energy for something of no inherent value

Natural cost of a block is ~bitcoin, about $240 (x25)

There are only 21 million Bitcoin
And when we run out, all this is included in the velocity.

Transactions require an account — yet more overhead.

Lots of energy for something of no inherent value.

Natural cost of a block is ~bitcoin, about $240 (x25).
Viral Money

- Economics
- Money Transfer
- Mining
- Smart Contracts

9
26
26
7
Viral Money

![Pie chart showing distribution of values for Stability, Security, Scalability, and Privacy.]

- Stability: 76
- Security: 61
- Scalability: 32
- Privacy: 27
Viral Money

Bitcoin is the extreme of a viral system:

- Distributed
- Trustless
- Time-stamped
- Irrevocable
  (Valuable)

But it burns $36000/hour for security