MIT Media Lab

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

Condominium Systems

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

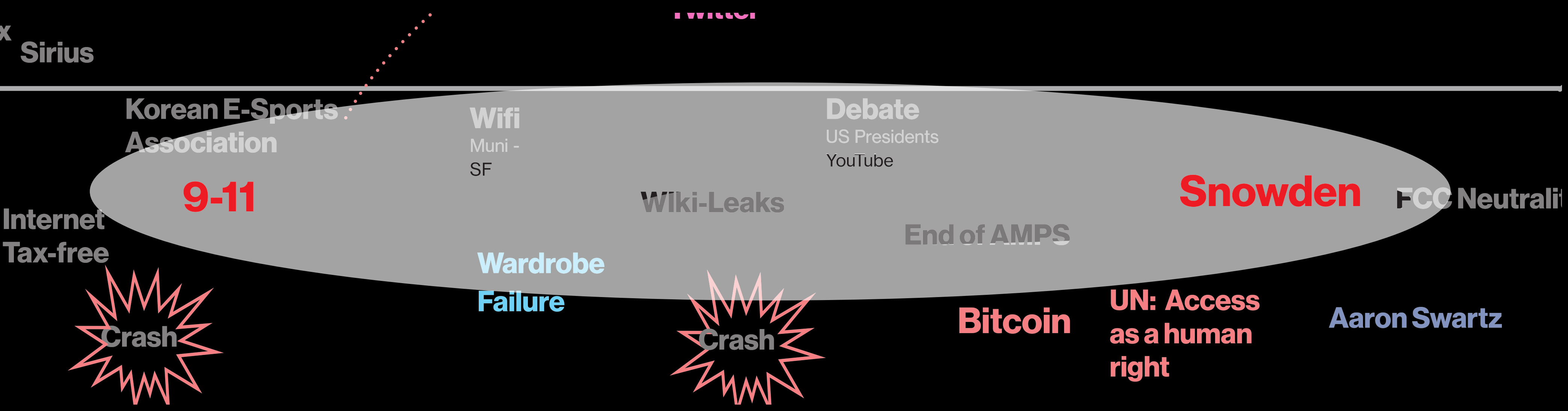
Distributed

Trustless

Time-stamped

Append-only list

Decentralization



x

Sirius

Twitter

Korean E-Sports Association

Internet Tax-free

9-11

Crash

Wifi
Muni - SF

Wardrobe Failure

Wiki-Leaks

Crash

Debate
US Presidents
YouTube

End of AMPS

Bitcoin

UN: Access as a human right

Snowden

FCC Neutralit

Aaron Swartz

End

Fun stuff follows

Perspective: Paypal, Square, ApplePay

Paypal, 1998
4.9billion payments in 2015
$228Billion in 2014
179million 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

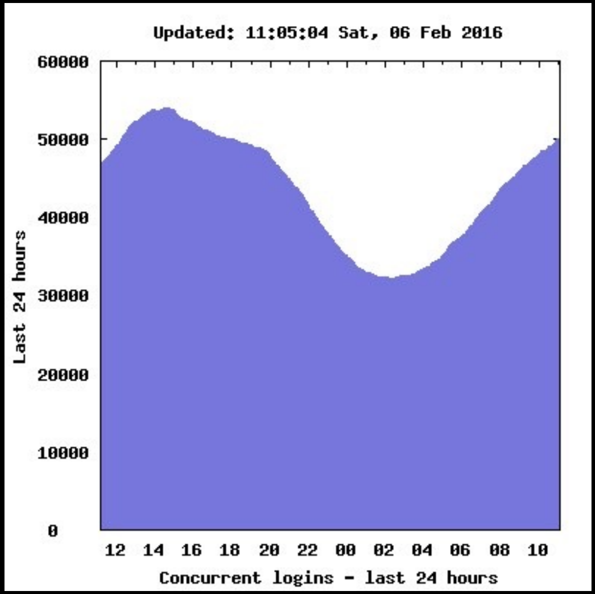
Miners get a reward for creating a block

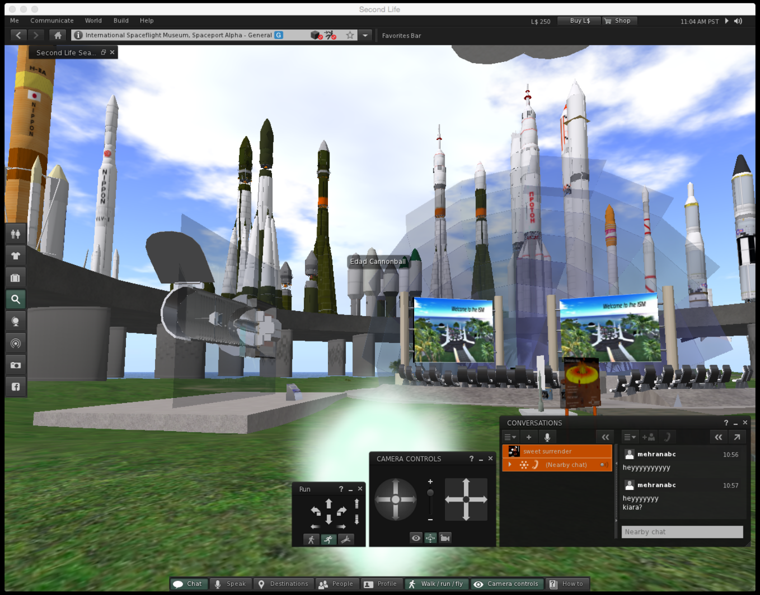
Cost is ~ $7500/block in lost energy and capital

Perspective: Second Life

Linden Labs, 1999
Second Life, 2002
Linden Dollar, 2003

L$240 = US$1.00





mehranabc 10:56
heyyyyyyyyyy

mehranabc 10:57
heyyyyyyy
kiara?

Still crazy after all those years

The new money

Bitcoin	6,036
Ethereum	918
Ripple	268
Litecoin	140
MaidSafeCoin	43
Dash	31
Dogecoin	23
Monero	14

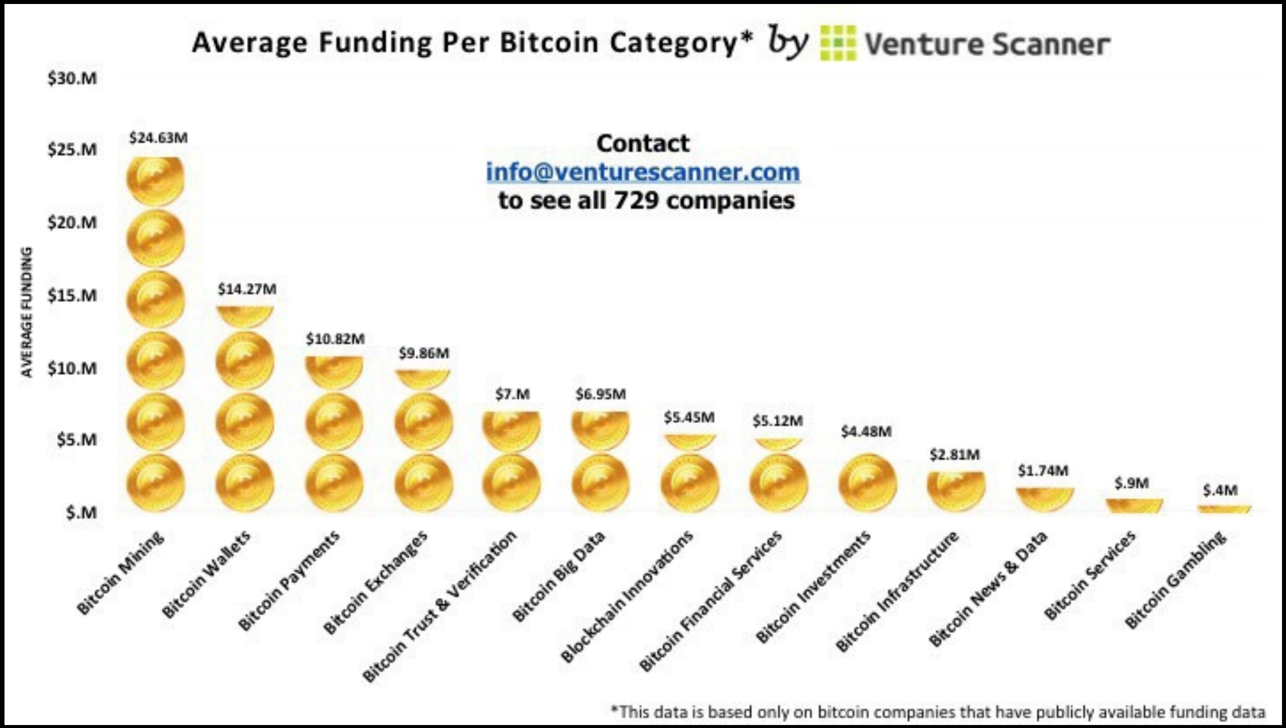
Market cap in $Millions

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

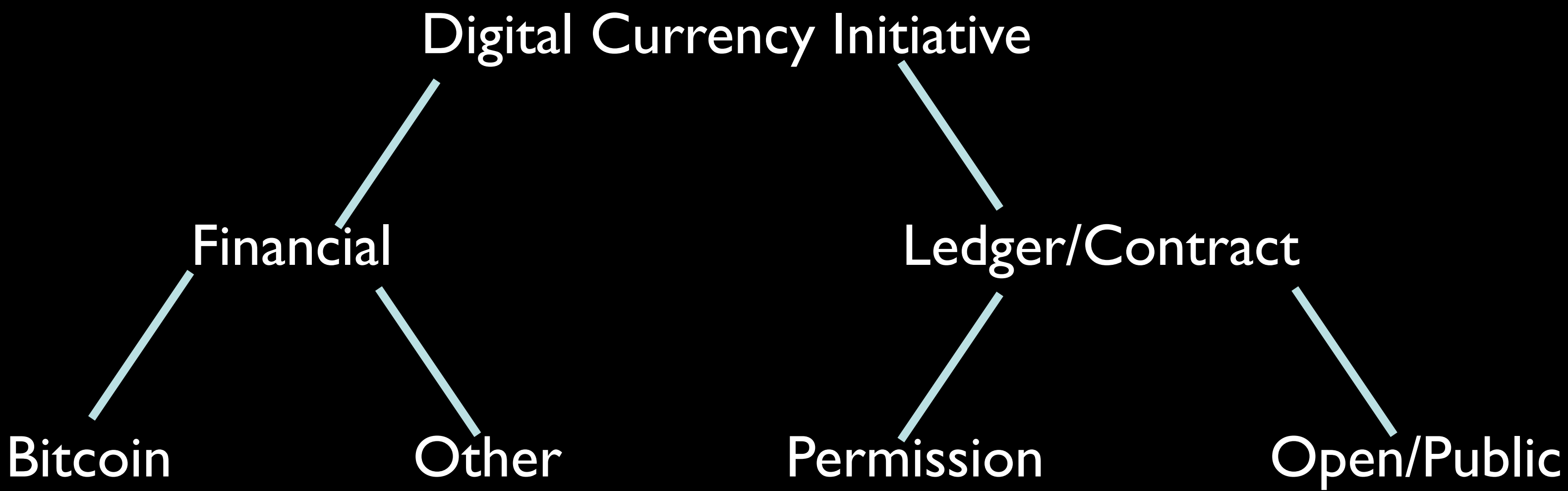


Average Funding Per Bitcoin Category* by Venture Scanner

*This data is based only on bitcoin companies that have publicly available funding data

$1Billion invested; $5Billion in value

Viral Money



Digital Currency Initiative

Financial

Ledger/Contract

Bitcoin

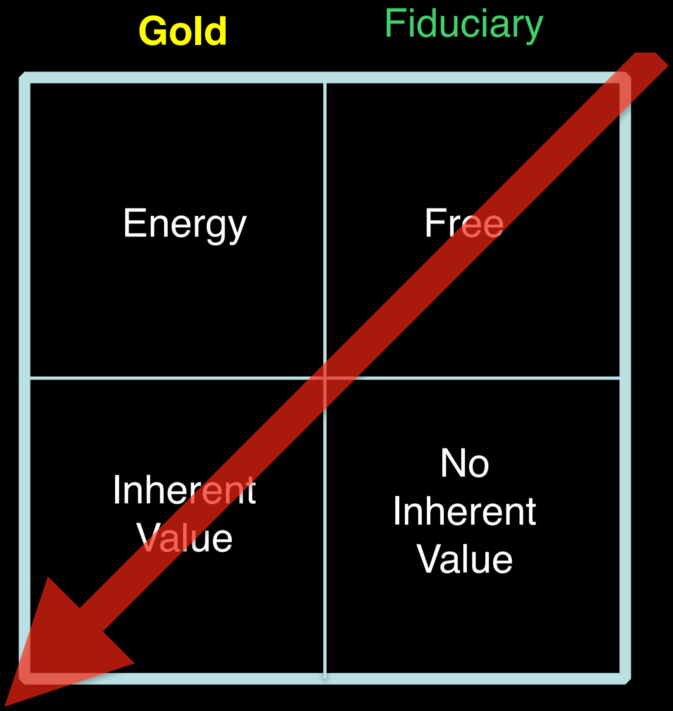
Other

Permission

Open/Public

Ripple, Stellar, Etheruem, ML Certs

Rates of Exchange



	Gold	Fiduciary
	Energy	Free
	Inherent Value	No Inherent Value

Easy to create, agree and inherent value

Rates of Exchange

Contrast two currencies, gold and fiduciary.

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

Gold	Fiduciary
Energy	Free
Inherent Value	No Inherent Value

Rates of Exchange

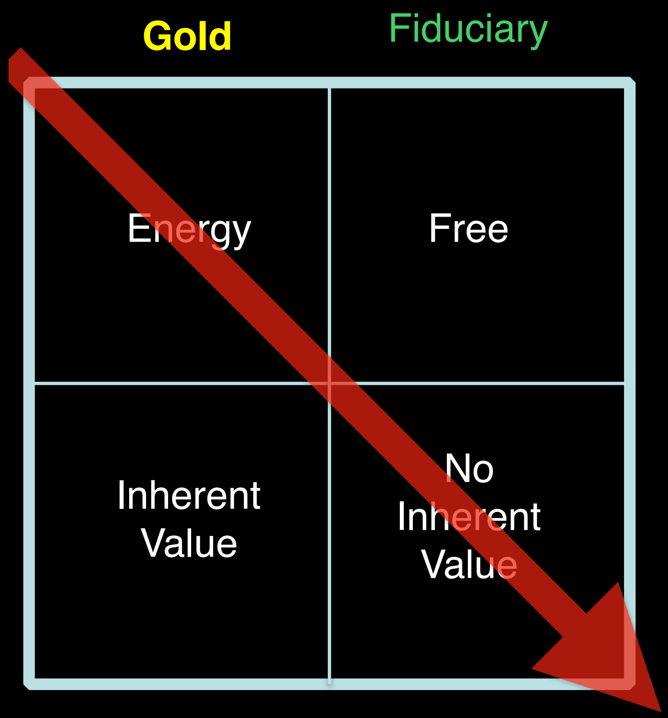
What are the problems we want to solve?

Remittances? Unbanked? Credit? Loans? Transactions?

Gold	Fiduciary
Energy	Free
Inherent Value	No Inherent Value

Generational change versus evolution

Rates of Exchange

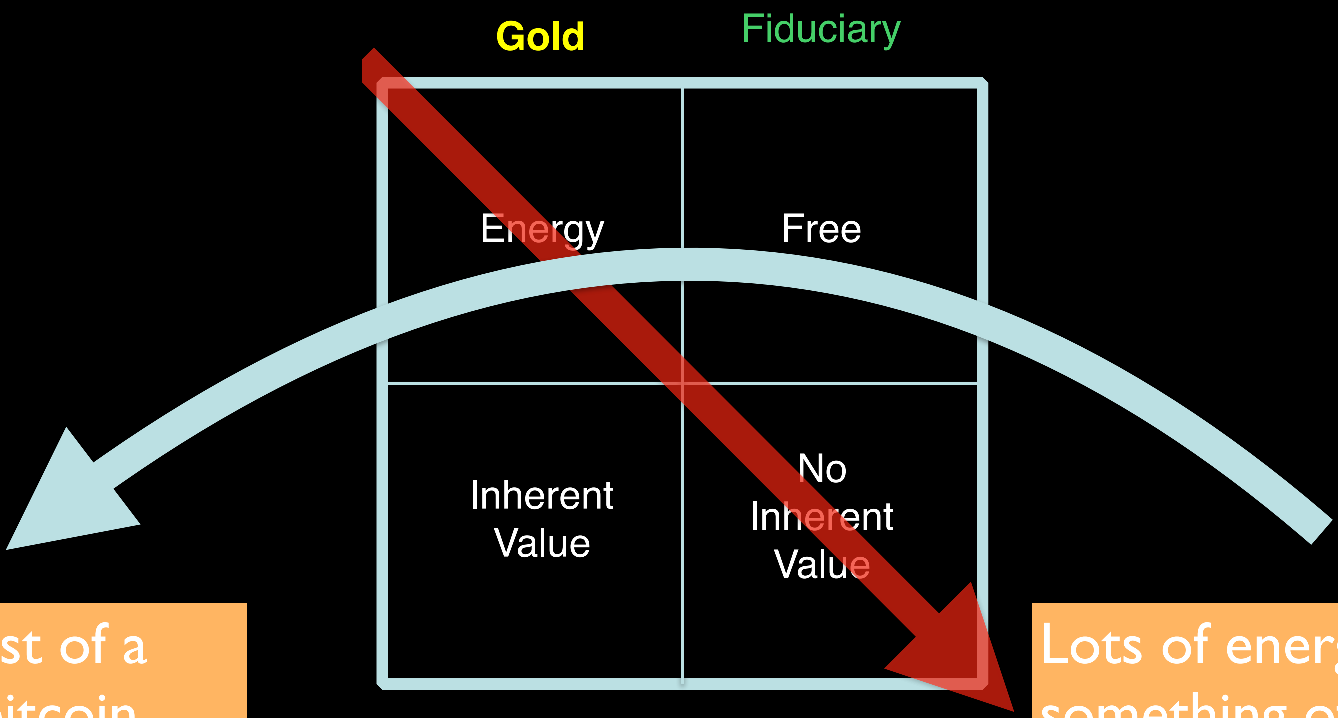


Gold	Fiduciary
Energy	Free
Inherent Value	No Inherent Value

Lots of energy for something of no inherent value

Rates of Exchange

MIT Media Lab



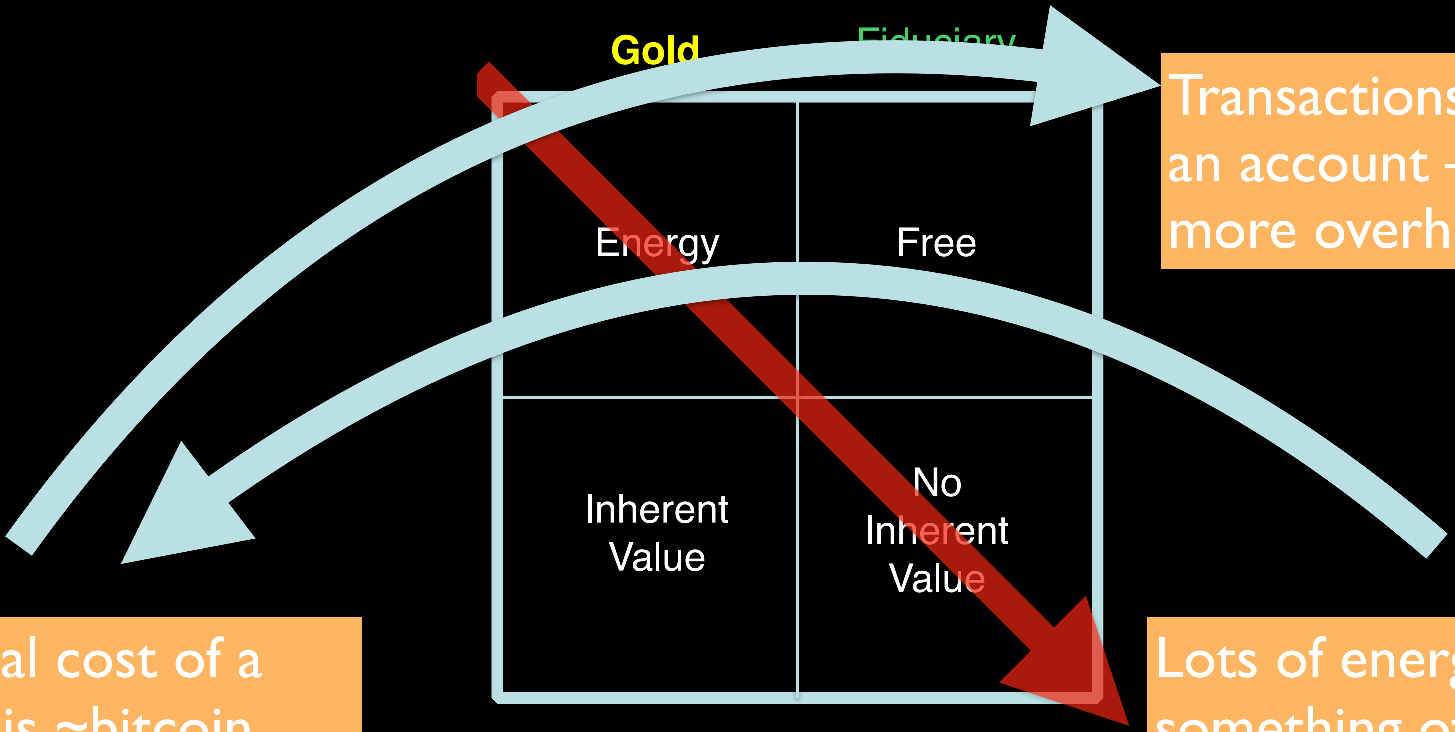
Gold	Fiduciary
Energy	Free
Inherent Value	No Inherent Value

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

Lots of energy for something of no inherent value

Rates of Exchange

MIT Media Lab



Gold	Fiduciary
Energy	Free
Inherent Value	No Inherent Value

Transactions require an account — yet more overhead

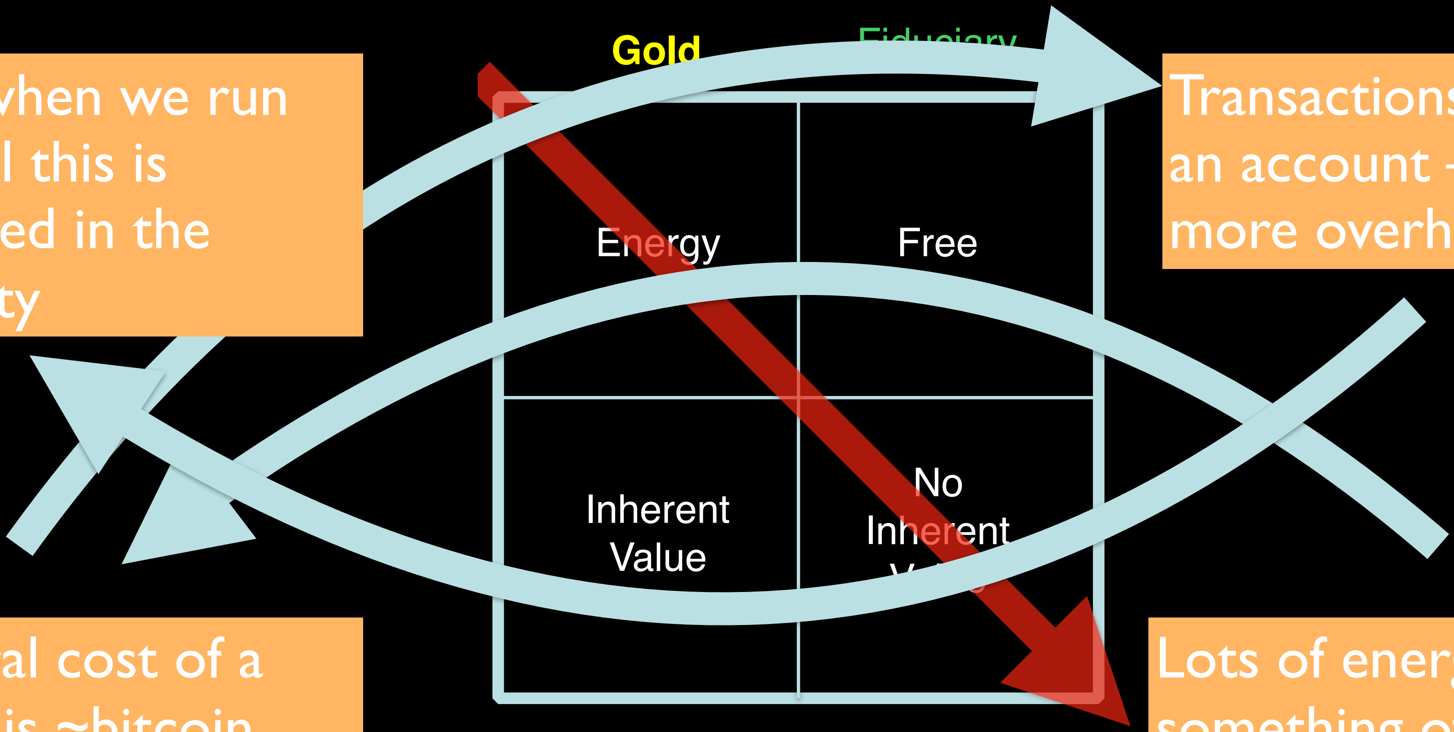
Natural cost of a block is ~bitcoin, about $240 (x25)

Lots of energy for something of no inherent value

There are only 21 million Bitcoin

Rates of Exchange

And when we run out, all this is included in the velocity

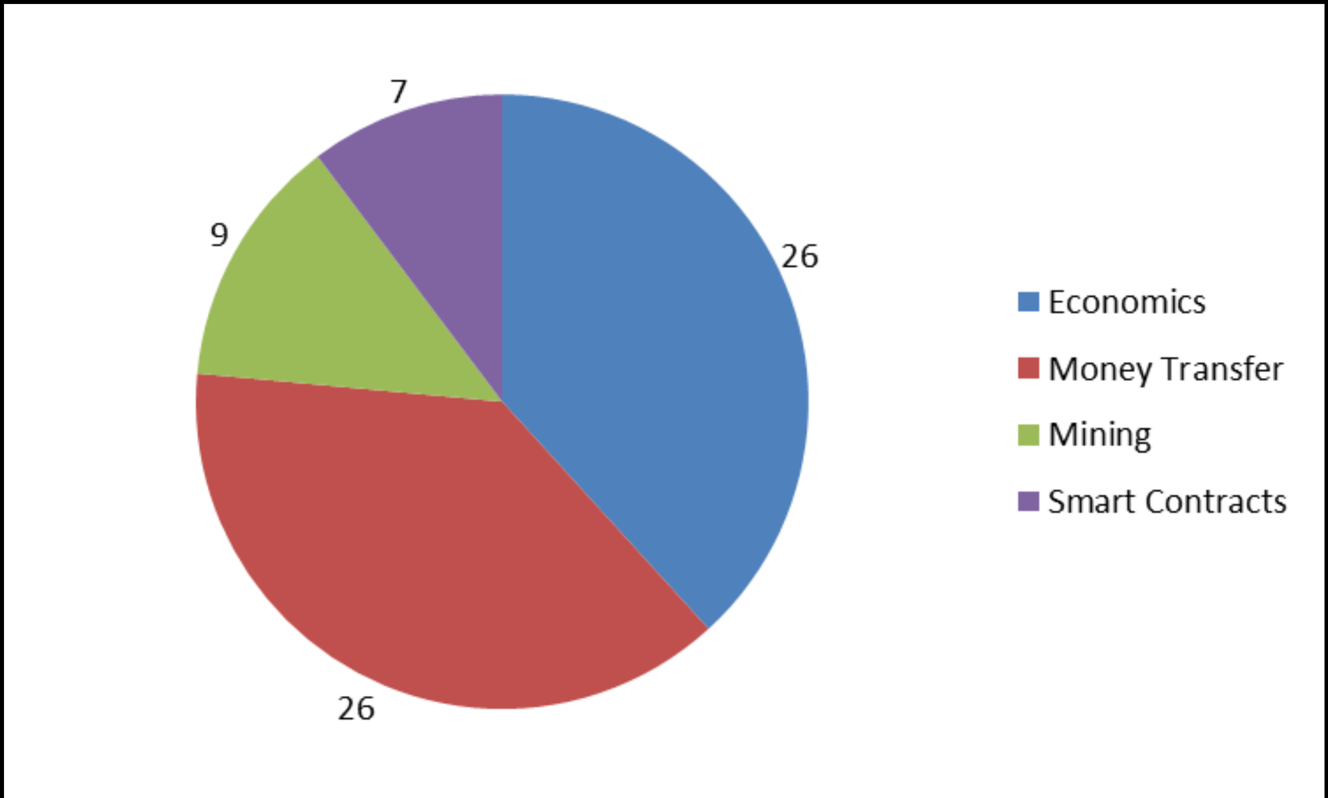


Transactions require an account — yet more overhead

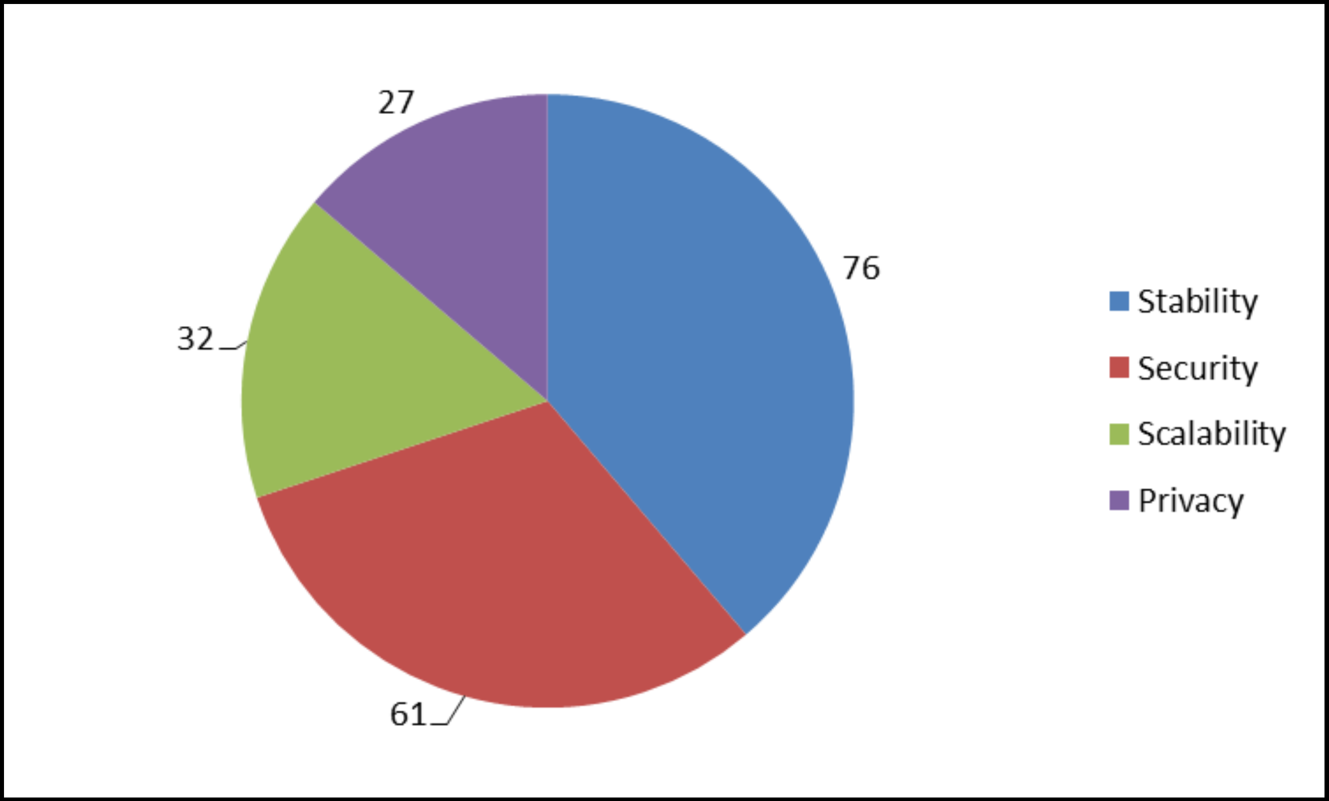
Natural cost of a block is ~bitcoin, about $240 (x25)

Lots of energy for something of no inherent value

Viral Money



Viral Money



Viral Money

Bitcoin is the extreme of a viral system:

Distributed
Trustless
Time-stamped
Irrevocable
(Valuable)

But it burns $36000/hour for security