Lecture 7

Community, Politics, and Regulation

Lecture 7.1:

Consensus in Bitcoin

Consensus about Rules

Agree on:

- what makes a transaction valid
- what makes a block valid
- how P2P nodes should behave
- protocols and formats

Consensus about History

Agree on contents of the blockchain

therefore: which transactions have occurred

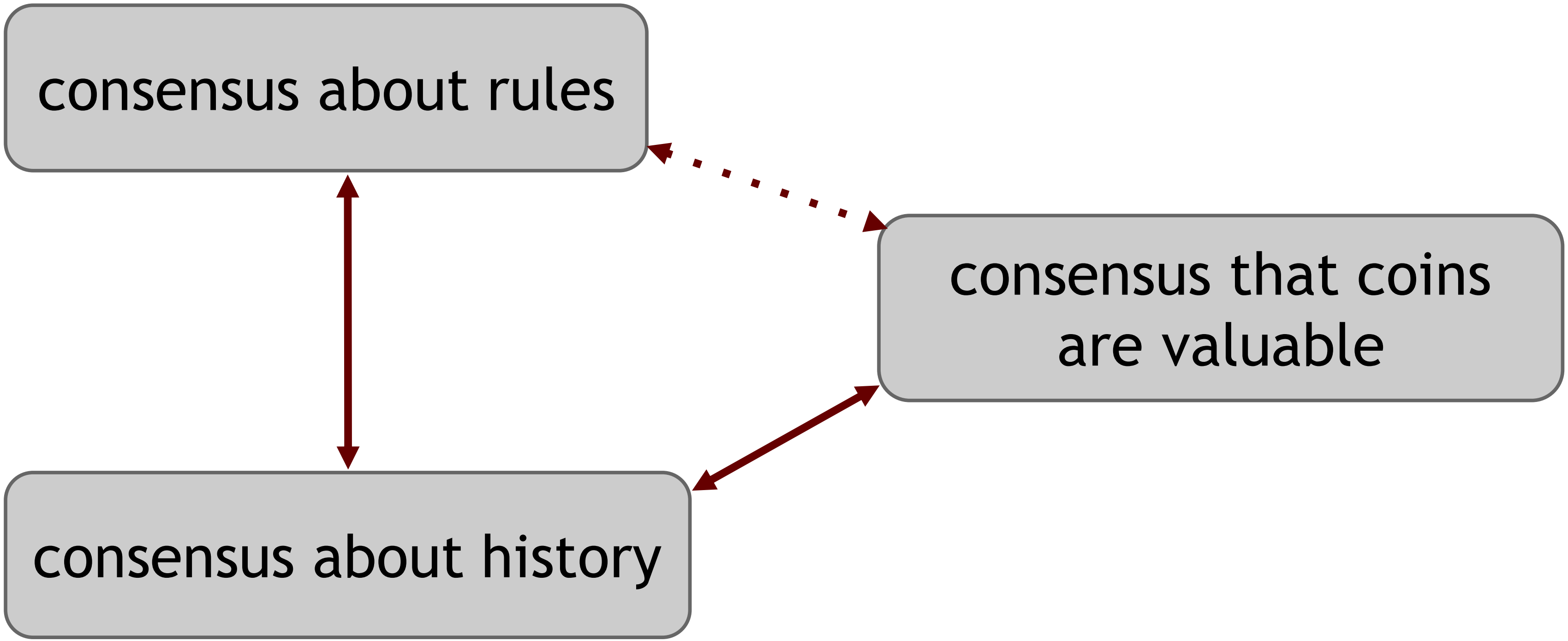
therefore: which coins exist and who owns them

Consensus that Coins are Valuable

General agreement that coins have value

Any currency needs this

“Tinkerbell effect”



consensus about rules

consensus that coins are valuable

consensus about history

Lecture 7.2:

Bitcoin Core Software

Bitcoin Core software

open source (MIT license)

the most widely used Bitcoin software

those who don’t use it follow its lead on rules

Bitcoin Core is the de facto rule book of Bitcoin

Bitcoin Improvement Proposals (BIPs)

“formal” proposal for changes to Bitcoin

includes technical spec and rationale

published in a numbered series

each BIP has a champion to evangelize / coordinate

also: informational BIPs, process-oriented BIPs

Core developers:

Wladimir van der Laan

Gavin Andresen

Jeff Garzik

Gregory Maxwell

Satoshi Nakamoto

Pieter Wuille

How powerful are the lead developers?

their rule changes will be followed by default

but anyone can fork the software at any time

Lead devs are “leading the parade”.

If users don’t like a rule change:

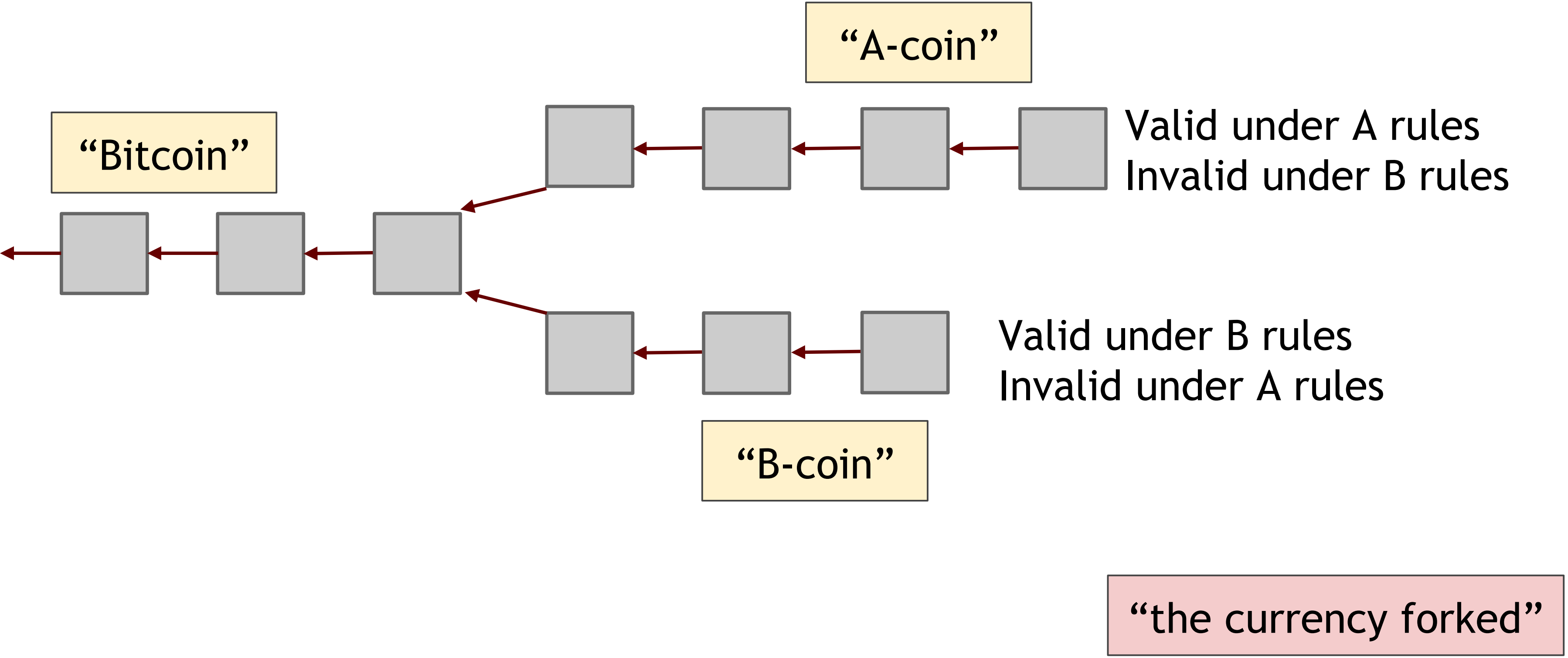
Centralized currency: Users have the right to exit.

Bitcoin: Users have the right to fork the rules.

Right to fork is more empowering than right to exit.

⇒ community retains more power

If there's a (hard) fork in the rules:



"A-coin"

"Bitcoin"

Valid under A rules
Invalid under B rules

Valid under B rules
Invalid under A rules

"B-coin"

"the currency forked"

After a hard fork:

(If fork was meant to start an altcoin:
altcoin goes its separate way
branches coexist nicely)

If fork reflected a fight over future of Bitcoin:
branches fight for market share
branches fight to be seen as “the real Bitcoin”
probably one branch wins, one melts away

Lecture 7.3:

Stakeholders : Who’s in Charge?

Who has the power in the Bitcoin ecosystem?

Suppose there is a negotiation about rule-setting.
Who controls the outcome?

Depends who would win the fight if they fail to agree.

Claim: Bitcoin Core developers have the power.

They write the rulebook.

Almost everybody uses their code, follows their rules.

Claim: Miners have the power.

Miners write the history.

History will be consistent with miners’ consensus rules.

Claim: Investors have the power.

Investors determine whether Bitcoin has any value.

In case of hard-fork, investors decide which branch wins.

Claim: Merchants and their customers have the power.

They generate the primary demand for Bitcoins.

They drive the long-term price of Bitcoin.

Investors are just guessing where merchants and customers will go.

Claim: Payment services have the power.

They are the ones that really handle transactions.

So they drive primary demand.

Merchants, customers, and investors will follow them.

The Bitcoin Foundation (founded 2012)

pays core developers

talk to governments as “voice of Bitcoin”

some controversy ...

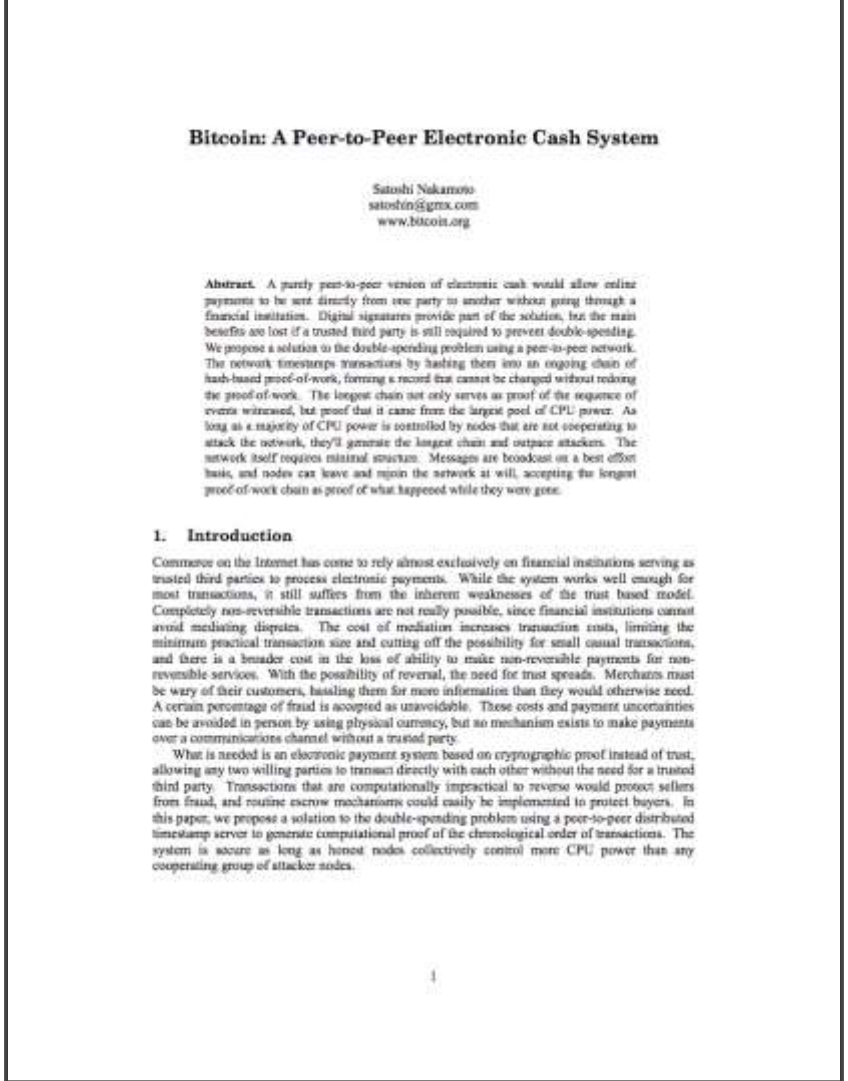
Lecture 7.4:

Roots of Bitcoin

Precursors to Bitcoin:

- Cypherpunk movement
- Early digital cash (Chaum et al.)

2008



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 hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

Satoshi Nakamoto

author of white paper and original Bitcoin software

almost certainly a pseudonym

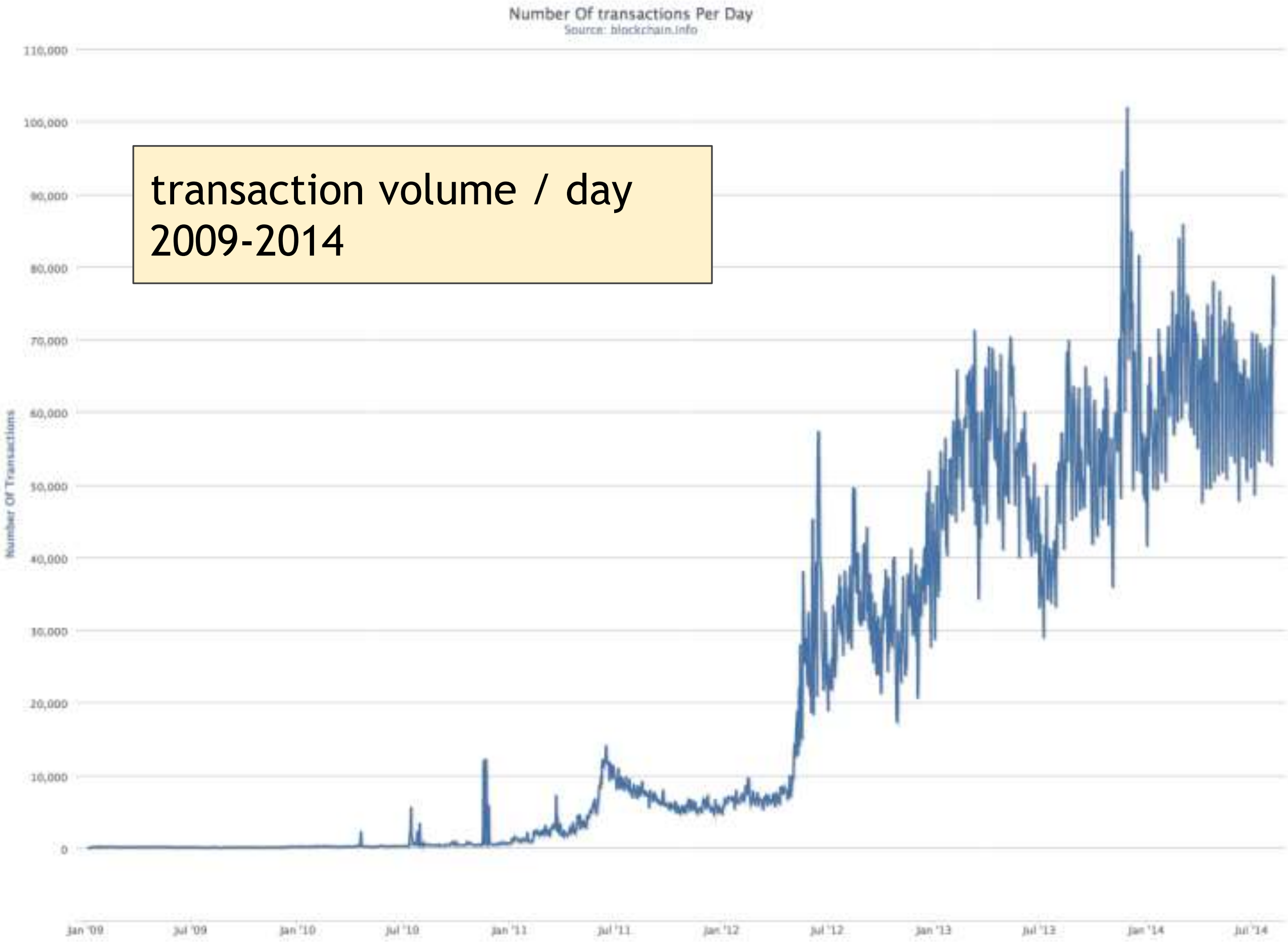
identity associated with certain public keys

writes fairly well in English

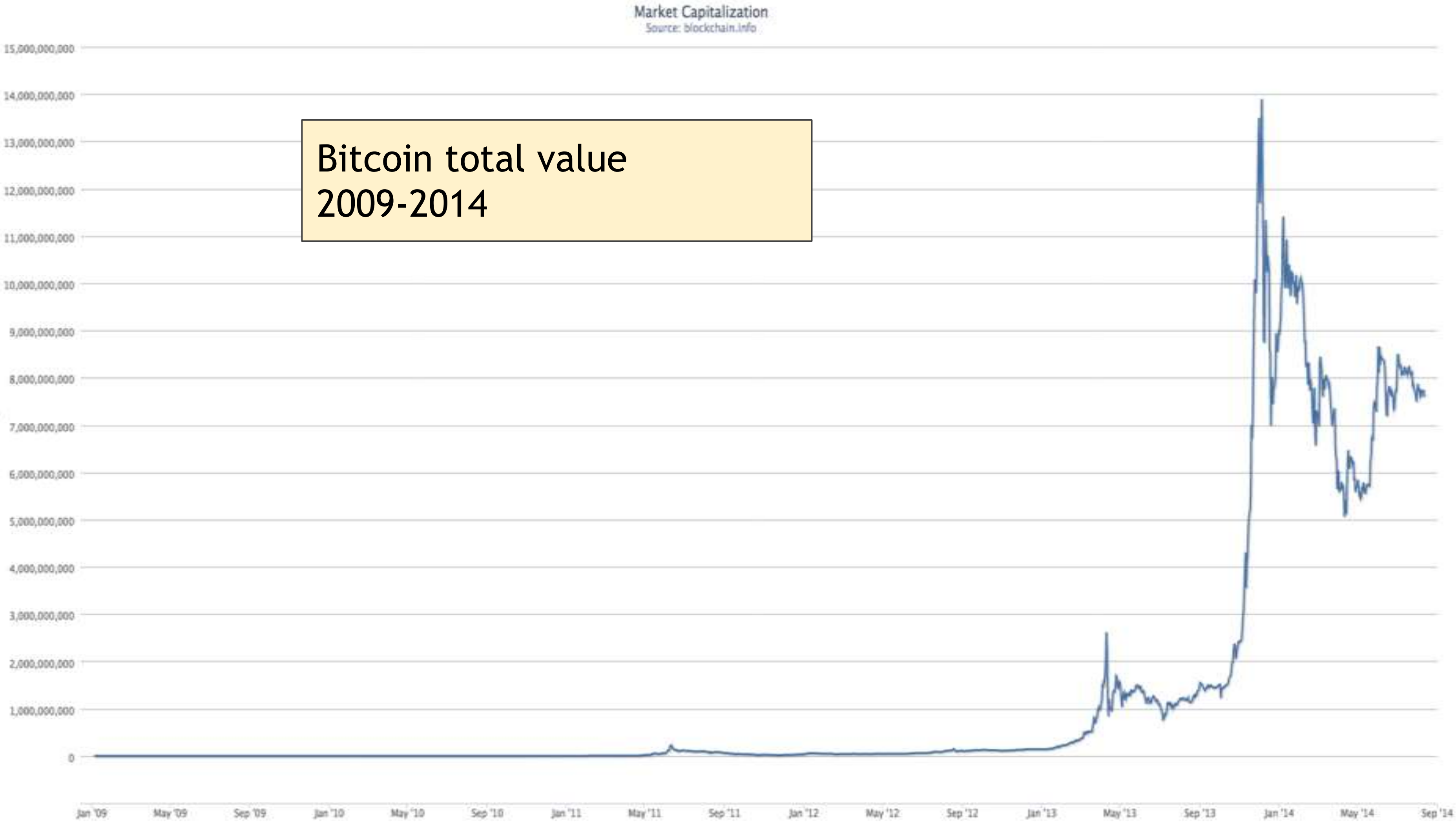
has barely been heard from since 2010

owns lots of Bitcoins from early mining

Real identity unknown.



transaction volume / day
2009-2014



Market Capitalization

Source: blockchain.info

Bitcoin total value
2009-2014

Lecture 7.5:

Governments Notice Bitcoin

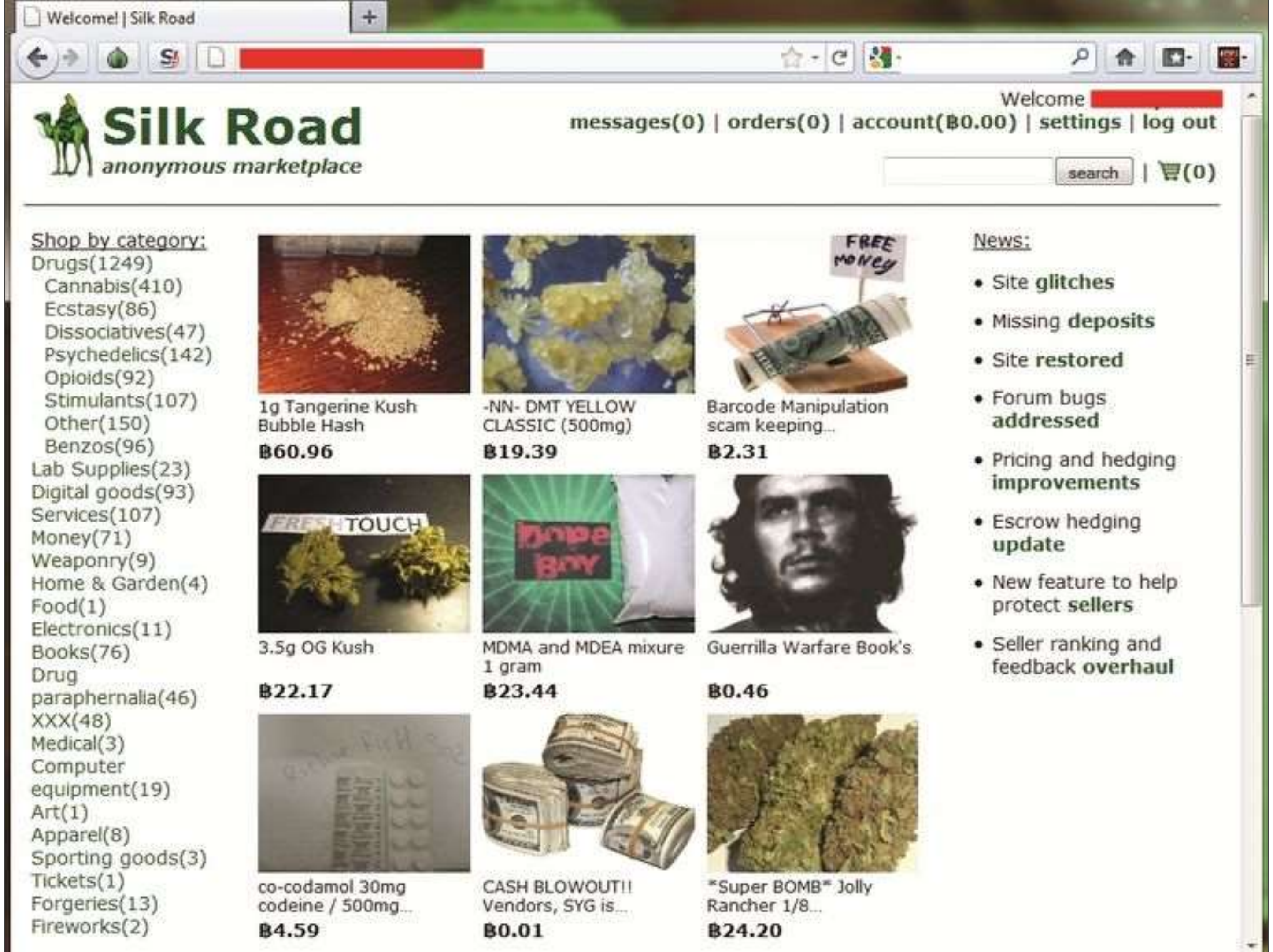
Untraceable digital cash defeats capital controls:

country can’t stop Bitcoin value from flowing in or out

government countermeasure: disconnect BTC world
from fiat currency financial institutions
example: China

Untraceable digital cash facilitates some crimes:

- kidnapping and extortion
- tax evasion
- sale of illegal items



Welcome! | Silk Road

[redacted]

Welcome [redacted]

messages(0) | orders(0) | account(Ƀ0.00) | settings | log out

|

Silk Road

anonymous marketplace

Shop by category:

- Drugs(1249)
  - Cannabis(410)
  - Ecstasy(86)
  - Dissociatives(47)
  - Psychedelics(142)
  - Opioids(92)
  - Stimulants(107)
  - Other(150)
  - Benzos(96)
- Lab Supplies(23)
- Digital goods(93)
- Services(107)
- Money(71)
- Weaponry(9)
- Home & Garden(4)
- Food(1)
- Electronics(11)
- Books(76)
- Drug paraphernalia(46)
- XXX(48)
- Medical(3)
- Computer equipment(19)
- Art(1)
- Apparel(8)
- Sporting goods(3)
- Tickets(1)
- Forgeries(13)
- Fireworks(2)

1g Tangerine Kush Bubble Hash
Ƀ60.96

-NN- DMT YELLOW CLASSIC (500mg)
Ƀ19.39

Barcode Manipulation scam keeping...
Ƀ2.31

3.5g OG Kush
Ƀ22.17

MDMA and MDEA mixure 1 gram
Ƀ23.44

Guerrilla Warfare Book's
Ƀ0.46

co-codamol 30mg codeine / 500mg...
Ƀ4.59

CASH BLOWOUT!! Vendors, SYG is...
Ƀ0.01

Super BOMB Jolly Rancher 1/8...
Ƀ24.20

News:

- Site **glitches**
- Missing **deposits**
- Site **restored**
- Forum bugs **addressed**
- Pricing and hedging **improvements**
- Escrow hedging **update**
- New feature to help protect **sellers**
- Seller ranking and feedback **overhaul**

Silk Road

- largest online market for illegal drugs
- ran as a Tor hidden service
- payment in Bitcoins
- site held BTC in escrow while goods shipped
- eBay-like reputation system
- run by “Dread Pirate Roberts”

operated February 2011 to October 2013

Ross Ulbricht
alleged operator of Silk Road

arrested October 2013
awaiting trial

government says he tried to cover his tracks,
but they connected the dots

government seized 174,000 BTC
auctioned them to the public

lessons:

hard to keep real and virtual separate
hard to stay anonymous for a long time
Feds can “follow the money”
⇒ money becomes untouchable

Lecture 7.6:

Anti Money-Laundering

goal of AML: stop large amounts of money from

(1) crossing borders, or
(2) moving from underground to legitimate economy

without detection

Know Your Customer (KYC):

(1) identify and authenticate clients,
(2) evaluate risk of client,
(3) watch for anomalous behavior.

Mandatory reporting in U.S.:

Must report currency transactions over $10,000.
⇒ file “currency transaction report”

Must watch for clients “structuring” transactions to avoid reporting.
⇒ file “suspicious activity report”

Requirements differ by country; consult your lawyer.

Note well: government takes this very seriously!

Bitcoin businesses have been shut down.

Businesspeople have been arrested.

Lecture 7.7:

Regulation

Argument against regulation is common, well understood.

Argument for regulation not as well understood.

When markets fail and produce bad outcomes,
regulation can address the failure.

Market failure example: Lemons market

Market for widgets, can be low-quality or high-quality

High-quality (HQ)

- costs a bit more to make
- consumers like them much better

Efficient market would deliver mostly HQ

What if consumers can’t tell HQ apart from LQ?

⇒ consumers won’t pay extra for HQ

⇒ sellers won’t sell HQ

Fixing a lemons market

Market-based approaches

- seller reputation
- warranties

Regulation

- required disclosure, with penalties for lying
- quality standards, with enforcement
- required warranties, with enforcement

Market failure example: Price fixing

Sellers agree to raise prices

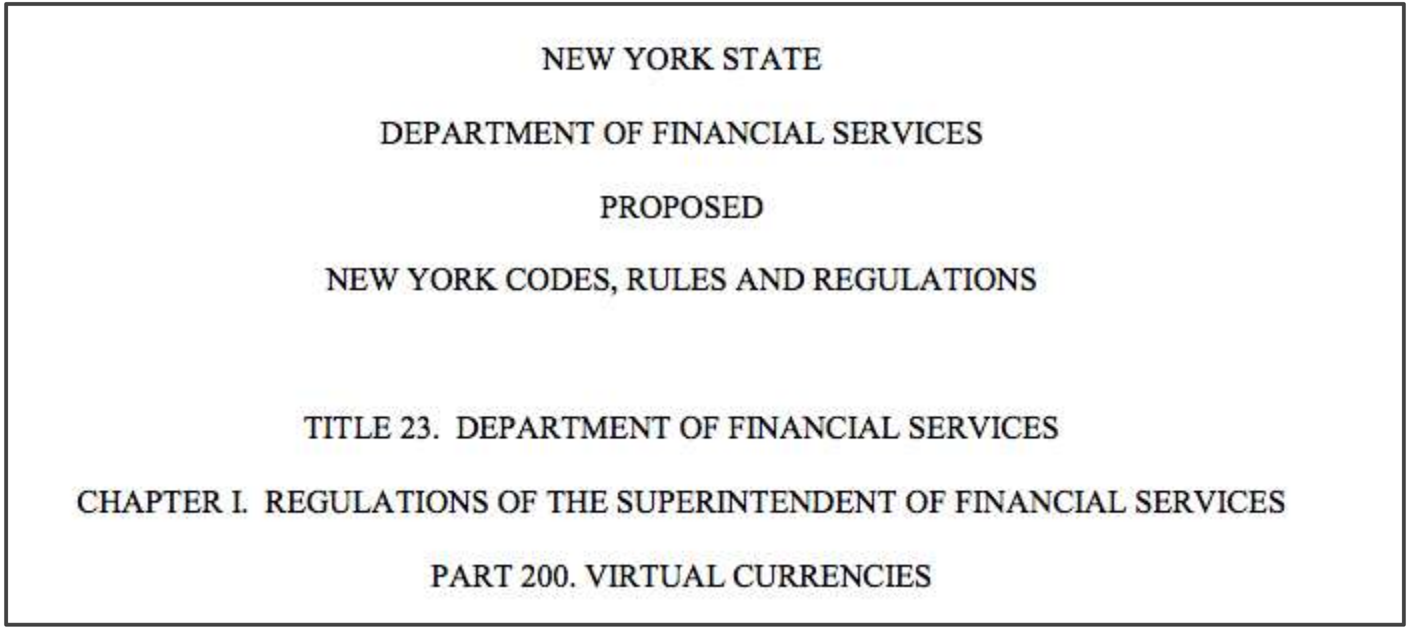
related: agreement not to compete

These are illegal in most jurisdictions.

part of “antitrust” or “competition” law

Lecture 7.8:

New York’s BitLicense Proposal



NEW YORK STATE

DEPARTMENT OF FINANCIAL SERVICES

PROPOSED

NEW YORK CODES, RULES AND REGULATIONS

TITLE 23. DEPARTMENT OF FINANCIAL SERVICES

CHAPTER I. REGULATIONS OF THE SUPERINTENDENT OF FINANCIAL SERVICES

PART 200. VIRTUAL CURRENCIES

New York “BitLicense” proposal
July 2014
http://www.dfs.ny.gov/about/press2014/pr1407171-vc.pdf

Would need a "BitLicense" from NYDFS to do any of these things:

Virtual Currency Business Activity means the conduct of any one of the following …
involving New York or a New York Resident:

(1) receiving Virtual Currency for transmission or transmitting the same;
(2) securing, storing, holding, or maintaining custody or control of Virtual Currency on behalf of others;
(3) buying and selling Virtual Currency as a customer business;
(4) performing retail conversion services, including the conversion or exchange of Fiat Currency or other value into Virtual Currency, the conversion or exchange of Virtual Currency into Fiat Currency or other value, or the conversion or exchange of one form of Virtual Currency into another form of Virtual Currency; or
(5) controlling, administering, or issuing a Virtual Currency

Applying for a licence

Provide information on

- ownership
- finances and insurance
- business plan

Pay an application fee

Licensees must:

Provide updated information to NYDFS

- including periodic financial statements

Maintain a financial reserve

- amount set by NYDFS

Follow rules on

- custody of consumer assets
- anti money laundering
- cybersecurity and disaster recovery
- recordkeeping

Designate a compliance officer, have written policies

Disclose risks to consumers

Status of BitLicense proposal [August 2014]

Proposed by NYDFS
Public comments solicited by NYDFS
After comments are in, NYDFS will decide what to do

Prediction: some kind of BitLicense will be put in place