Blockchain
&
Business Application

Lecture:

Community, Politics, and Regulation

Consensus in Bitcoin

- **Consensus about rules.**
  - *Rules*: what makes a transaction or a block valid,
  - the core protocols and data formats
- Required among all different participants
- Talk to each other and agree on things.

Consensus in Bitcoin

- **Consensus about history.**
  - What is and isn't in the block chain,
  - → which transactions have occurred.
  - → which coins — which unspent outputs — exist
  - who owns them.

Consensus in Bitcoin

- **Consensus that coins are valuable**
  - When you give bitcoins, you take sth
  - Now & tomorrow?

- Fiat money: Not by consensus but by fiat
  - What is dollar, what is not?
  - Determined by law, not history

- Cryptocurrency:
  - You believe that tomorrow too people believe that you believe that… Circular!

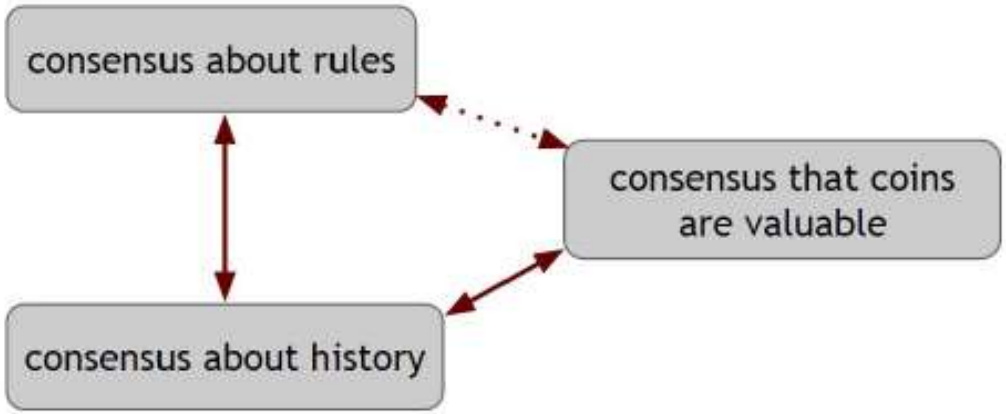


Figure 7.1: Relationships between the three forms of consensus in Bitcoin

- Without knowing which blocks are valid you can't have consensus about the block chain.

- Without consensus about which blocks are in the block chain, you can't know if a transaction is valid or double-spend attempt.

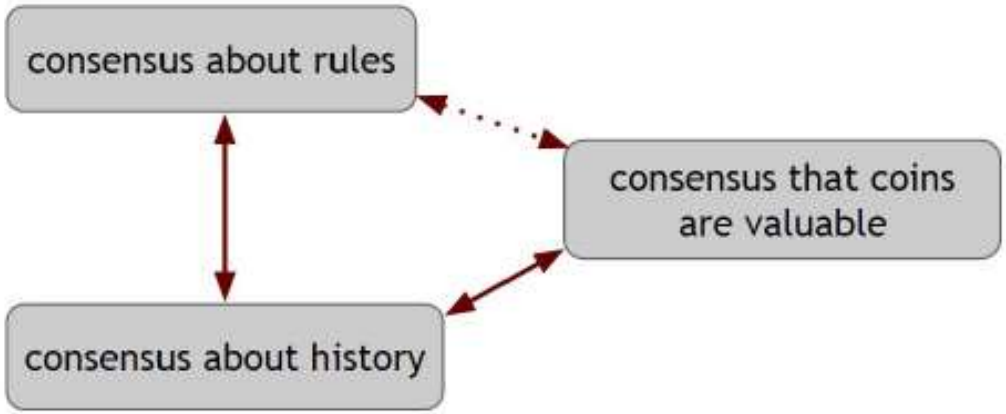


Figure 7.1: Relationships between the three forms of consensus in Bitcoin

– Prerequisite for believing that the coins have value: We agree on who owns which coins

– Consensus about value: motivation for miners

→ maintain block chain: consensus about history

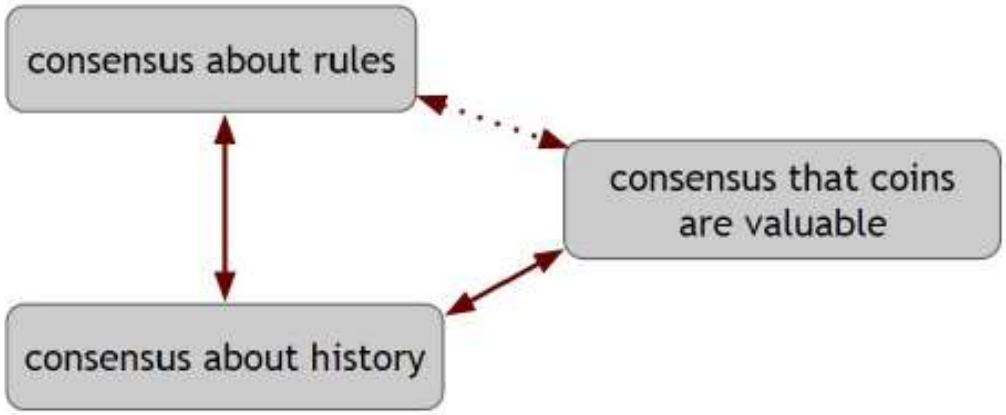


Figure 7.1: Relationships between the three forms of consensus in Bitcoin

– None can be obtained alone.

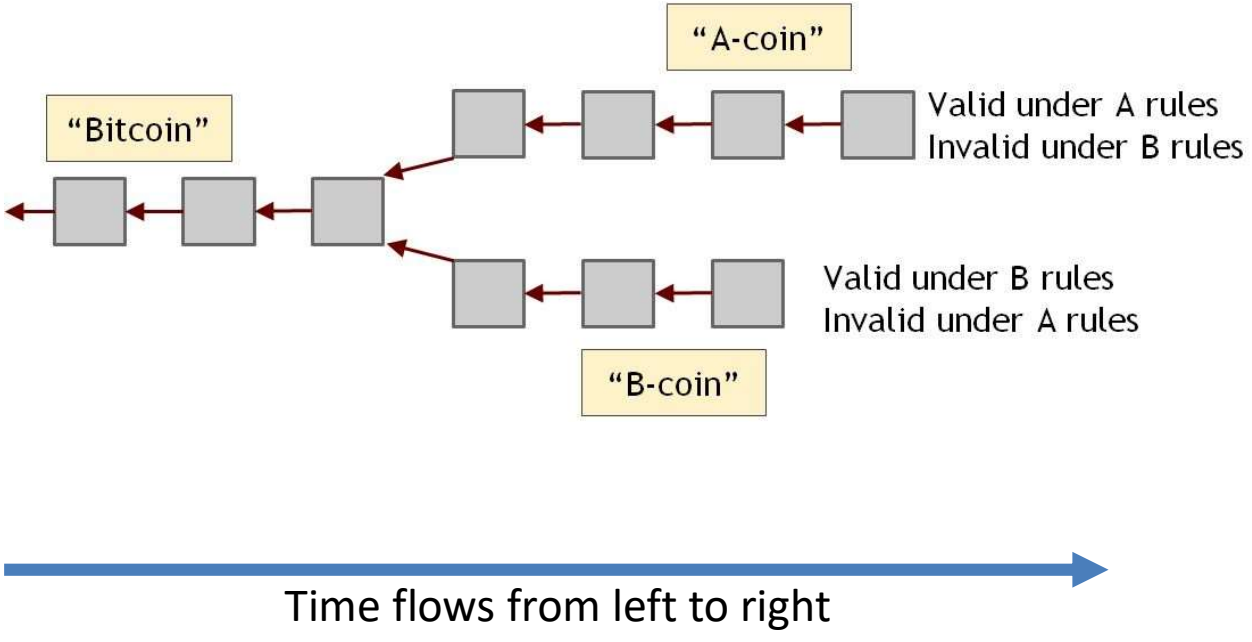
– C. about rules & C. about value are loosely tied

Bitcoin Core Software

- MIT's open-source license
- Core is the de-facto rule book
- Reference for Altcoin developers
- Improvements
  - Pull Requests (as all open-licensed software)
  - Bitcoin Improvement Proposals for big changes

- Bitcoin Core Developers
  - Nakamoto is inactive
  - 5 core developers, powerful?
- Modifying the currency?
  - Fiat money: Nope
  - Cryptocurrency: Possibly

- Disagreement on rules → Can “fork”



Stakeholders: Who's in Charge?

- Core developers (rules)
- Miners (history)
- Investors (value)
- Merchants & customers (demand)
- Payment services

Bitcoin advocacy groups

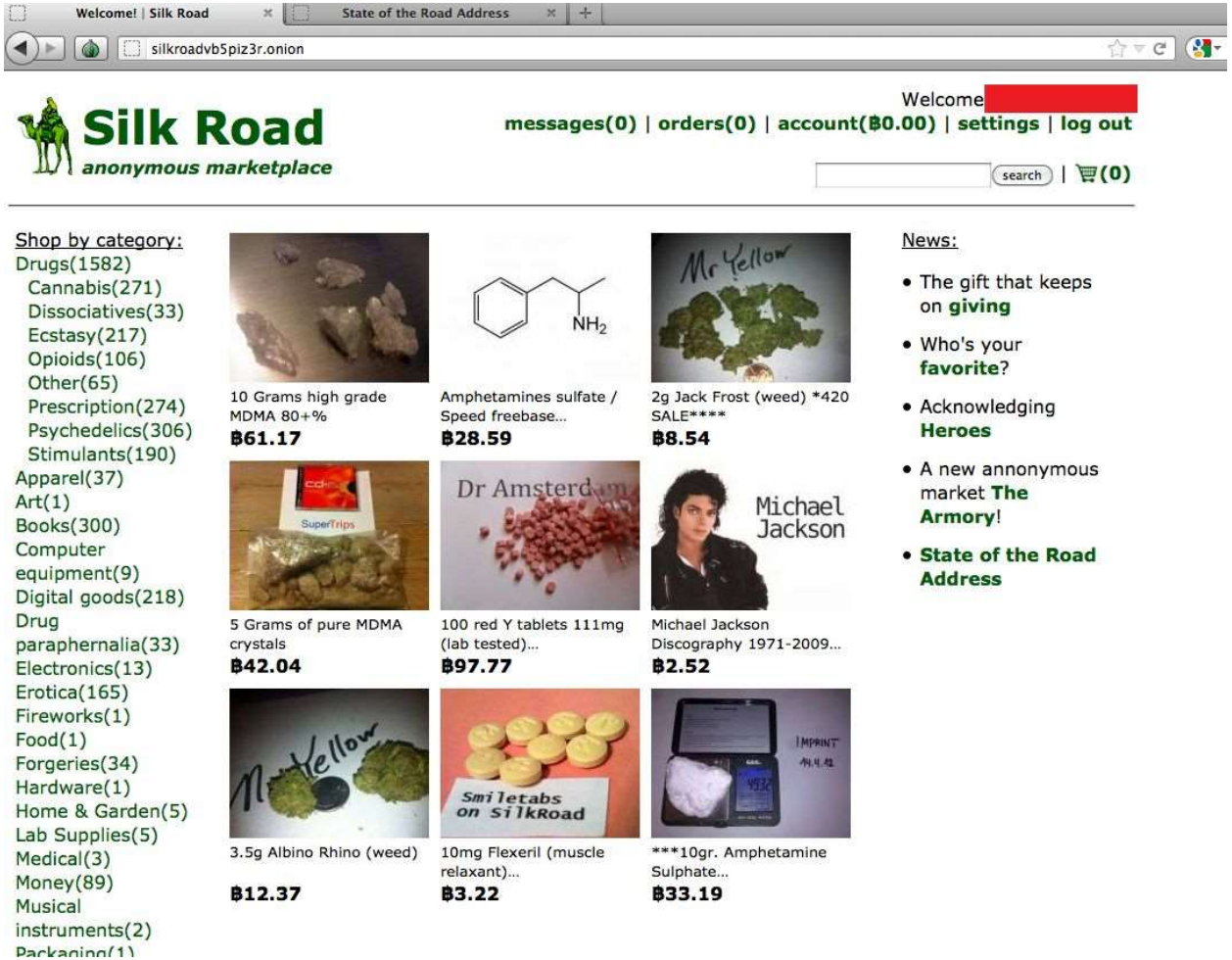
- Bitcoin Foundation (2012, nonprofit)
  - Funding some core developers full-time
  - Talking to governments
- Coin Center (2014, nonprofit)
  - Talking to government
- Should Bitcoin talk to governments?

Roots of Bitcoin

- Libertarian (even anarchist)
  - "Little or no government possible with crypto"
- Satoshi Nakamoto
  - Claimed to be born in 1972; Japanese, male
  - No real information
  - Acquired lots of coins (early mining), never spent
  - Addresses public
  - Cannot exchange to dollar without revealing ID

Governments Notice Bitcoin

- Capital control
  - Transfers between countries
  - Disconnecting with fiat money?
- Crime
  - Ransoms
  - Silk Road “the eBay for illegal drugs”
  - http://silkroad…..onion
    - Escrow
    - 2011-2013, owner arrested


Welcome! | Silk Road
State of the Road Address
silkroadvb5piz3r.onion
Silk Road
anonymous marketplace
Welcome
messages(0) | orders(0) | account(฿0.00) | settings | log out
search | (0)
Shop by category:
Drugs(1582)
Cannabis(271)
Dissociatives(33)
Ecstasy(217)
Opioids(106)
Other(65)
Prescription(274)
Psychedelics(306)
Stimulants(190)
Apparel(37)
Art(1)
Books(300)
Computer equipment(9)
Digital goods(218)
Drug paraphernalia(33)
Electronics(13)
Erotica(165)
Fireworks(1)
Food(1)
Forgeries(34)
Hardware(1)
Home & Garden(5)
Lab Supplies(5)
Medical(3)
Money(89)
Musical instruments(2)
Packaging(1)
10 Grams high grade MDMA 80+%
฿61.17
Amphetamines sulfate / Speed freebase...
฿28.59
2g Jack Frost (weed) *420 SALE****
฿8.54
5 Grams of pure MDMA crystals
฿42.04
100 red Y tablets 111mg (lab tested)...
฿97.77
Michael Jackson Discography 1971-2009...
฿2.52
3.5g Albino Rhino (weed)
฿12.37
10mg Flexeril (muscle relaxant)...
฿3.22
***10gr. Amphetamine Sulphate...
฿33.19
News:
The gift that keeps on giving
Who's your favorite?
Acknowledging Heroes
A new annonymous market The Armory!
State of the Road Address

Anti-Money Laundering

- Try to make organized crime more difficult
- Know your customer laws
  - Identify and authenticate clients
  - Evaluate risk of client
  - Watch for anomalous behavior
- Mandatory reporting
  - Transactions over $10K
  - Structuring clients requested

Regulation

- “Some dumb bureaucrat who doesn't know my business or what I'm trying to do, coming in and messing things up”

- Some can be justified
  - Market failures
  - Pareto improvements: Allocation of goods for all

- Lemons market
  - e.g. Only high&low quality cars
- How to fix?
  - Seller reputation
  - Warranties
- Regulatory fixes
  - Quality labels
  - Quality standards
  - Force the warranties

Reading Assignments

- The economics of information security
- Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace
- Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem
- (Guide) Bitcoin: A primer for policymakers
- (Book) Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age
- Bitcoin: Economics, Technology, and Governance
- How governments can leverage policy and blockchain technology to stunt public corruption