# CAN CRYPTOCURRENCIES BECOME MONEY?

**Nicolás Cachanosky**
Metropolitan State University of Denver
ncachano@msudenver.edu

# Contents

- How does Bitcoin work?
- Is Bitcoin money?
- Three monetary challenges to Bitcoin
- Three generations of cryptocurrencies
- The future: Divergent paths

# HOW DOES BITCOIN WORK?

# How does Bitcoin work?

- Historical context
  - Bitcoin launches during the 2008 crisis
    - Movement against central bank
    - Movement against private banks
    - Motivation: Bank-less digital transactions and anonymity
  - Even if Bitcoin was not created to become money, the possibility of cryptocurrencies becoming a CAMOE is an important question in the literature
    - Is this possible?

# How does Bitcoin work?

- How is transacting with Bitcoin different than an online transfer?
  - Transactions can be
    - Cash (easy to trust)
    - Electronic transaction (i.e. bank transfer)
  - Bitcoin is a *peer-to-peer* electronic transaction with no need of intermediaries
    - Save transactions costs of asymmetric information
  - Bitcoin: Money or payment technology?
    - Do individuals hold Bitcoin, or just use to move money around?
    - If they hold Bitcoin, is for liquidity or speculative purposes?

# How does Bitcoin work?

- Nakamoto (p. 1, emphasis added):

> 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.

# How does Bitcoin work?

- The case of Bitcoin
  - Creation of bitcoins is **predefined** by the *constitution* of the network
  - Public ledger information should match the history “attached” to each bitcoin
  - Miners check the legitimacy of a bitcoin transaction
  - Bitcoins are created as a compensation to miners
- Some popular cryptocurrencies
  - Bitcoin / Litecoin / Ether / Ripple / Tether / Etc… (it is a long list)

# How does Bitcoin work?

- Creation of bitcoins is predefined by the network constitution
  - Public ledgers record all transactions where a bitcoin is involved
    - A ledger cannot be modified without being noticed by the network (all ledgers must have the same information)
    - Each bitcoin gets an attachment with all its historical transactions
  - Transaction
    - Miners check that the historical record of a bitcoin matches the public ledger
    - For this work, miners are compensated with newly created bitcoins
  - Miners as intermediaries
    - Miners are paid by the network (not the parties) and do not held bitcoins as deposits
  - Anonymity
    - Miners, and each party, doe not need to know who each actor is

# IS BITCOIN MONEY?

# Is Bitcoin Money?

- What type of asset is Bitcoin?
  - Scarcity is absolute
  - Does not have a non-monetary use?
  - It is not commodity money (gold)
  - It is not fiat money

| | | NON-MONETARY USE? | |
|---|---|---|---|
| | | Yes | No |
| SCARCITY | Absolute | Commodity | Synthetic Commodity |
| | Contingent | Coase Durable | Fiat |

# Is Bitcoin Money?

- What is money?
  - A common means of exchange
- Functions of money?
  - A common means of exchange
  - Unit of account
  - Store of value

# Is Bitcoin Money?

| | U.S. dollar | Argentine peso | Bitcoin | Gold |
|---|---|---|---|---|
| Commonly accepted | YES | YES | NO | NO |
| Unit of account | YES | YES | NO | NO |
| Store of value | YES | NO | ? | YES |
| **MONEY?** | **YES** | **YES** | **NO** | **NO** |

# THREE MONETARY CHALLENGES TO BITCOIN

# Three monetary challenges of Bitcoin

- Challenge 1: Network effects
  - Be careful: Money **is not** a *public good*, money is a *network good*
  - Network goods compete in *contestable markets* (all or nothing)
  - Can Bitcoin break the network effect?
    - No monetary substitution after the collapse of the Somali government

# Three monetary challenges of Bitcoin

- Challenge 1: Network effects (cont…)
  - Let $u$ be the utility provided by a network good, then:
    - $u(N) = \frac{a+b\cdot\ln(\theta N)}{r}; \theta \in [0,1]$
    - $a$: non-monetary services ($a \geq 0$)
    - $b$: network effect ($b > 0$)
    - $N$: Size of the network
    - $r$: Discount rate
  - Consider an alternative network good
    - $\mu = \frac{\alpha+\beta\cdot\ln[(1-\theta)N]}{r}$

# Three monetary challenges of Bitcoin

- Challenge 1: Network effects (cont…)
  - Switch to $u$ if new network good utility beats the switching cost ($s$)
    - Let $a = \alpha$
    - $\frac{b \cdot \ln(\theta N) - \beta \cdot \ln[(1-\theta)N]}{r} > s$
  - Contestant network good must
    - Design a strategy to increase the **size** of the network ($\theta N$)
    - Increase network benefits such that $b - \beta$ as large enough to trigger a switch of network
      - Anonymity: $b \uparrow$
      - Scalability constraints: $b \downarrow$
      - Network of middle-men: $b \uparrow$
      - Legislation risk: $b \downarrow$

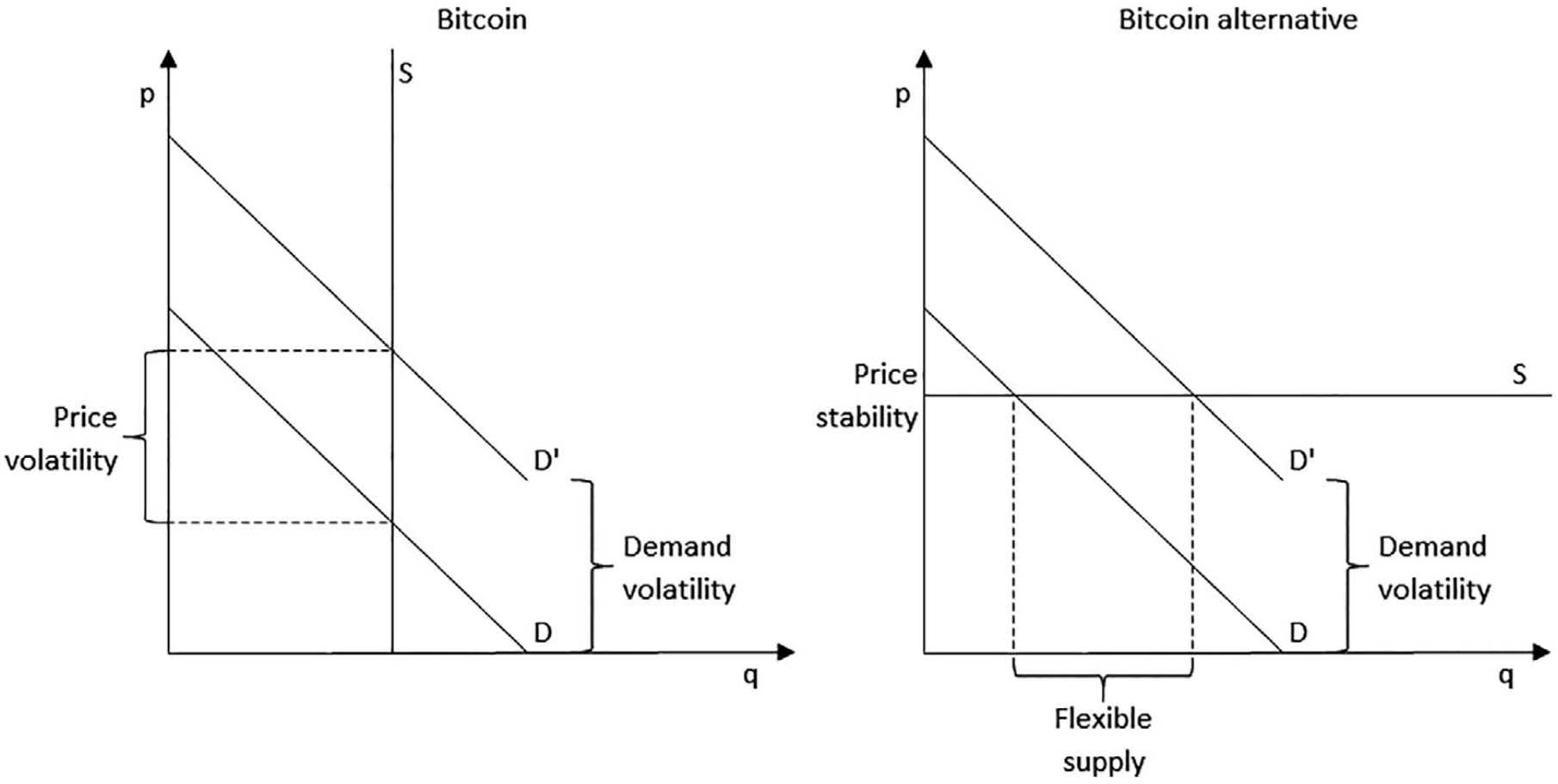
# Three monetary challenges of Bitcoin

- Challenge 1: Network effects (cont…)
  - Network goods
    - Classic examples
      - Telephones
      - Fax machines
    - Contemporary examples
      - Facebook (remember Google+?)
      - Twitter (do you know what mastodon.org is?)
      - Instragram
      - Etc…
  - Having a product of higher quality is not enough
  - Potential solution
    - Entrepreneurs as middle-men

# Three monetary challenges of Bitcoin

- Challenge 2: The monetary rule problem
  - How does a good monetary rule look like?
    - Convention: Price stability
    - Even better: Money supply = Money demand
      - $M^D = M^S \nrightarrow \bar{P}$
      - $\overline{MV} = PY$
      - $\Delta P = -\Delta Y$ (real/productivity shocks)

# Three monetary challenges of Bitcoin



# Three monetary challenges of Bitcoin

- Challenge 2: The monetary rule problem (cont…)
  - Can Bitcoin evolve to have a good monetary rule?
    - Incomplete inspiration in the Gold Standard?
    - Where are the banks?

| Monetary regime | Equation of exchange |
|---|---|
| Free banking | $GmV = Py$ |
| Classic gold standard | $GmV = Py$ |
| Fiat money | $FmV = Py$ |
| Bitcoin | $\bar{B}V = Py$ |

# Three monetary challenges of Bitcoin

- Challenge 2: The monetary rule problem (cont…)
  - Potential solution: Banks should be able to issue convertible notes on Bitcoin
    - Too risky
    - What is the pragmatic benefit of depositing a bitcoin in a bank?
    - The supply of Bitcoin does not respond to changes in demand, as was the case with commodity money under gold standard or free banking

# Three monetary challenges of Bitcoin

- Challenge 3: The scalability constraint
  - Transactions are recorded in the blockchain
    - Security measure:
      - Each **block** stores information for the last 10 minutes
      - Each **block** has a size limit of 1MB
    - This capacity is a constrain for the actual size of the Bitcoin network
      - Long waiting lines
      - Miners charge fees during peak times (*sounds like a bank..?*)
    - Transactions per second (TPS) for competitive payment technologies

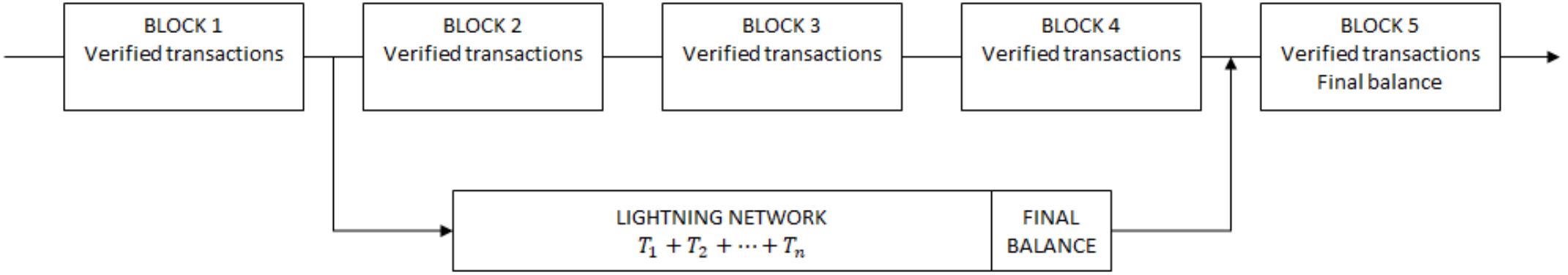
| VISA | PayPal | Bitcoin |
|---|---|---|
| 24,000 | 193 | 7 |

# Three monetary challenges of Bitcoin

- Challenge 3: The scalability constraint (cont…)
  - The 1M information cap
    - The larger the block size, the more space for a dishonest miner to either log a fake transaction
  - The 10-minute window
    - The propagation time of a new block (how long it takes to be seen by the network) should be **short with respect to** how long it takes to add the block to the chain
    - If blocks are immediately added to the chain, then a dishonest miner can log fake transactions
  - In a **decentralized** network there is trade-off between TPS and security

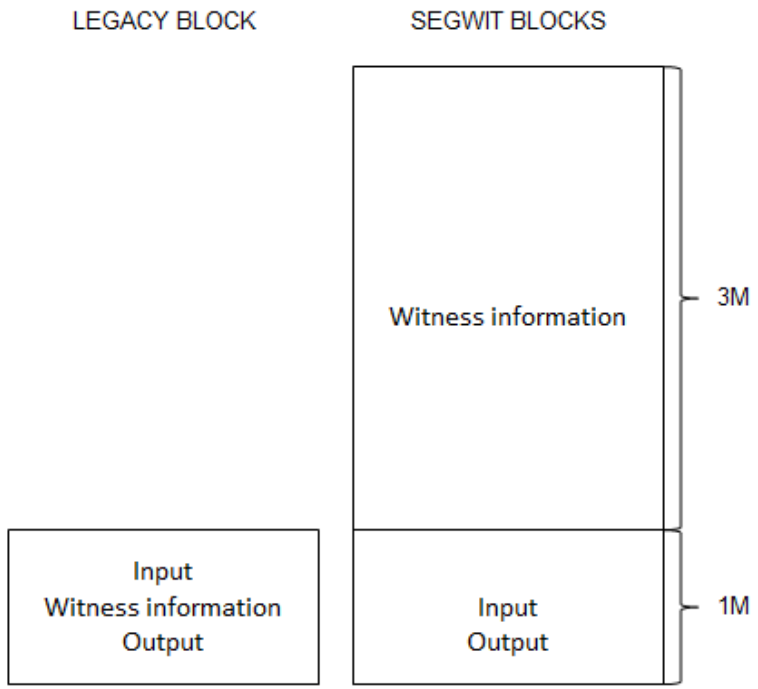
# Three monetary challenges of Bitcoin

- Challenge 3: The scalability constraint
  - Potential solution 2: The lightning network (+ smart contract?)



# Three monetary challenges of Bitcoin

- Challenge 3: The scalability constraint
  - Potential solution 2: SegWit



# THREE GENERATIONS OF CRYPTOCURRENCIES

# Three generations of cryptocurrencies

- Generation 1
  - Fixed supply cryptocurrencies
    - Bitcoin / Litecoin
- Generation 2
  - Stable coins
    - Tether / Sagacoin / Basis
- Generation 3
  - Monetary equilibrium
    - *Quahl* (formerly *Initiative Q*)
- Problem:
  - Fixing the supply is easy
  - Fixing the exchange rate is doable
  - But how you code monetary equilibrium?

# THE FUTURE: DIVERGENT PATHS

# The future: Divergent paths

- Central bank digital currency (CBDC)
  - Move towards a cash-less economy
  - Charge negative interest rates
  - Centralize commercial banking
- Cryptocurrencies
  - Currency competition *a la* Hayek
  - But Hayek's model is unstable
  - Unless cryptocurrencies facilitate a separation between (1) banking and (2) transaction services
    - Again: Is Bitcoin money or a transaction technology?

# Q&A