Monopoly without a Monopolist: Economics of the Bitcoin Payment System

Gur Huberman, Jacob D. Leshno, Ciamac Moallemi
Columbia Business School

Two Known Forms of Money

- Coins, paper bills
  - Originate with a mint that makes them immune to forgery
  - Possession is proof of ownership
  - Payments are final
  - Receipt is proof of payment; optional
- Ledger-based
  - MONOLITIC ledger
  - Trusted third party maintains the ledger
  - Trusted third party guarantees veracity
  - Trusted third party always involved in payments
  - Monopoly/Market power

Bitcoin: A Peer-to-Peer Electronic Cash System

- 10/2008: Satoshi Nakamoto floats the original 9 page white paper
- 1/2009: Releases the first software
  - Mines the genesis block & earns 50btc for that

- Electronic payment systems
  - Bitcoin being the first
  - ~25 systems have total balances of over $1B; agg val ~$380Bn
  - New systems developed, offering new functionality

Cryptocurrencies

- Decentralized, two-sided platform
  - Users receive similar services to PayPal, Fedwire; Miners provide infrastructure
  - Object viable only on platform
  - Platform viable only if expected to remain viable in the future
  - Market design enabled by blockchain protocol

- Miners maintain the system
- Users make payments
  - Recipients accord value

Cryptocurrencies

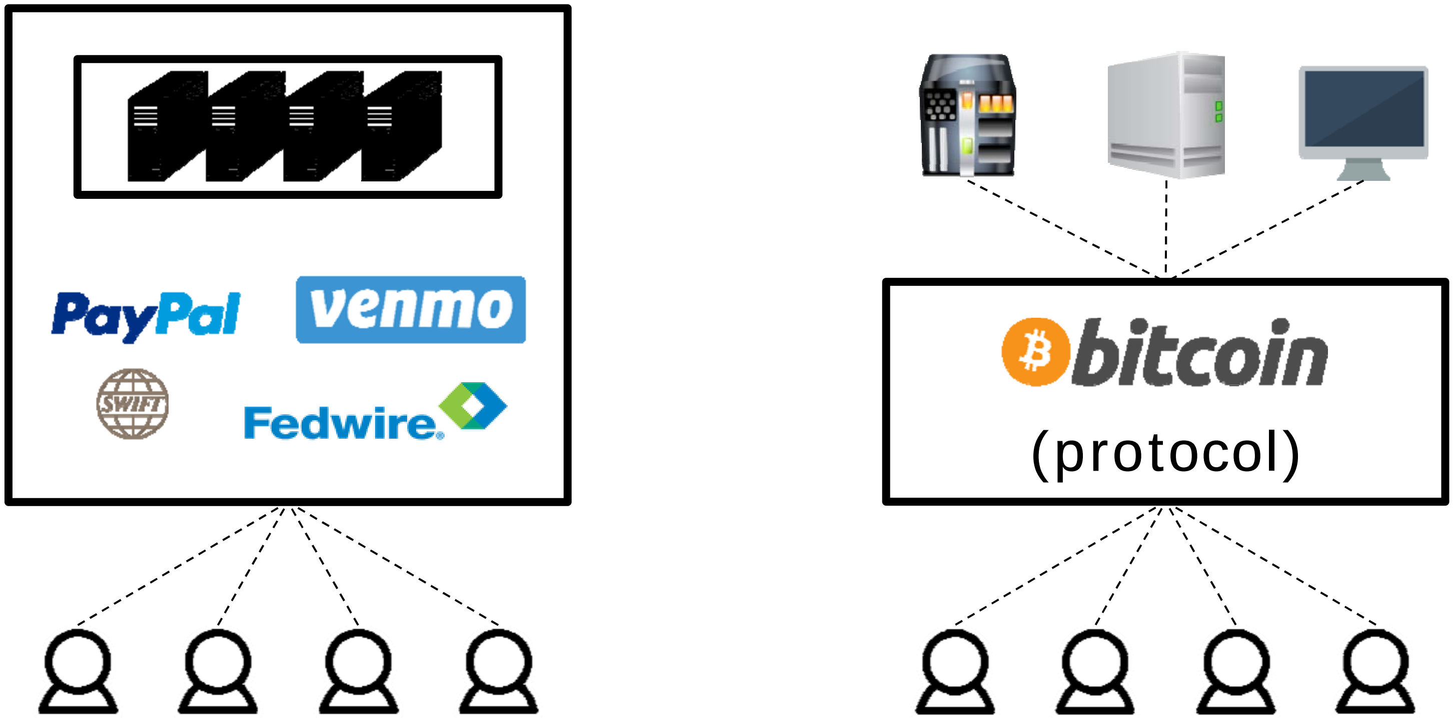
- Novel economic structure
  - Owned by no one
  - Rules fixed by a computer protocol
  - A single agent's action doesn't affect others (~price taking)

Traditional Electronic Payment Systems

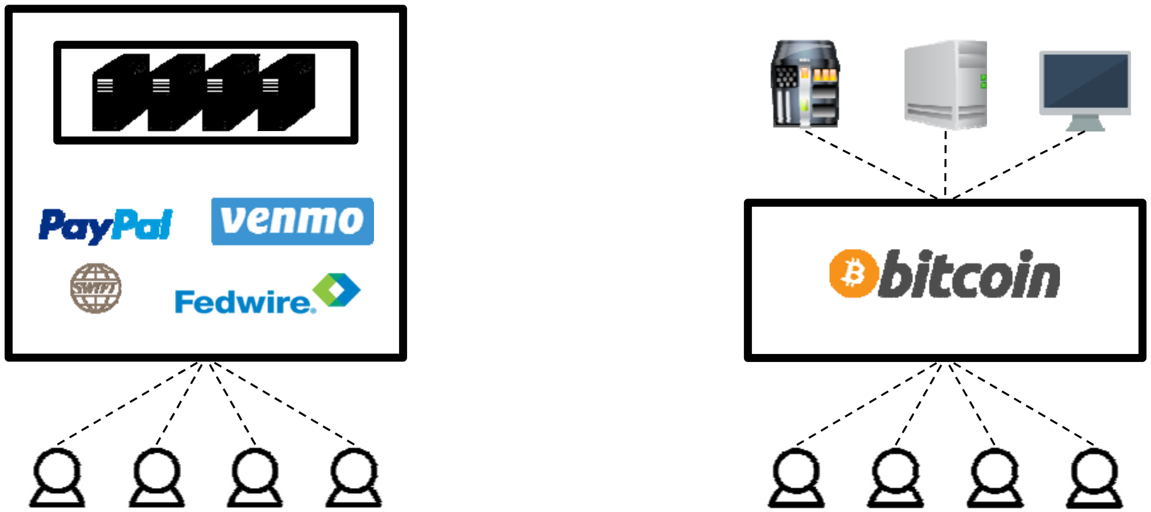
- Allows users to hold balances and make transfers
- Controlling authority
  - Provide trust, maintain infrastructure, sets usage fees, changes them when circumstances change.
- Natural monopoly
  - Monolithic ledger
  - Network externalities, fixed costs
  - Often requires regulation

- Examples: Fedwire, Venmo, PayPal, SWIFT, M-Pesa

Traditional Payment Systems vs. Bitcoin

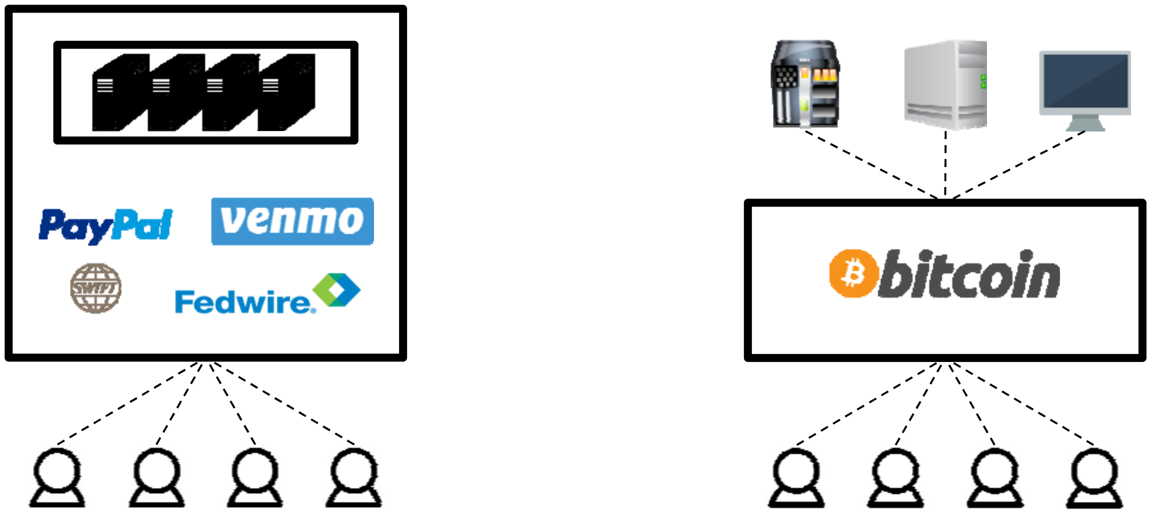


Traditional Payment Systems vs. Bitcoin



Rules	Set by firm/org	Fixed by protocol
Infrastructure	Procured by firm/org	
Revenue	Fees set by firm/org	

Traditional Payment Systems vs. Bitcoin



Rules	Set by firm/org	Fixed by protocol
Infrastructure	Procured by firm/org	*Revenue, entry/exit*
Revenue	Fees set by firm/org	*Equilibrium congestion pricing, all agents served*

Sketch of Main Results

- Miners
- Users and congestion
- Stability, waste and (absence of) self-correction

Analysis of Miners

- In equilibrium, active miners maximize reward by procession K transactions with highest fees
  - Cannot affect the behavior of users or set transaction fees
  - Can observe pending transactions and their fees
  - Create block with highest fee transactions, up to block capacity

- Total system revenue, payments to miners (per unit time) is equal to total transaction fees (per unit time)

- Miners – system providers! – make zero profit.

Analysis of Users

- System congested; delays
- Users offer transaction fees to gain queuing priority

Analysis of Users/Transactions

- Users play a congestion queueing game
  - Transaction fees $b(c_i)$ are bids for priority
- Blocks mined/added at rate μ, each processes K highest fee transactions
  - Independently of number of miners
- Equilibrium transaction fees $b_i = b(c_i)$ maximize

$$u(c_i) = \mathrm{R} - c_i \cdot W(b_i|G) - b_i$$

where $W(b_i|G)$ is the expected delay for a user who bids b_i given distribution of others bids G

An Auction w/o an Auctioneer

- Nobody imposes transaction fees
- Equilibrium transaction fees $b_i = b(c_i)$ maximize

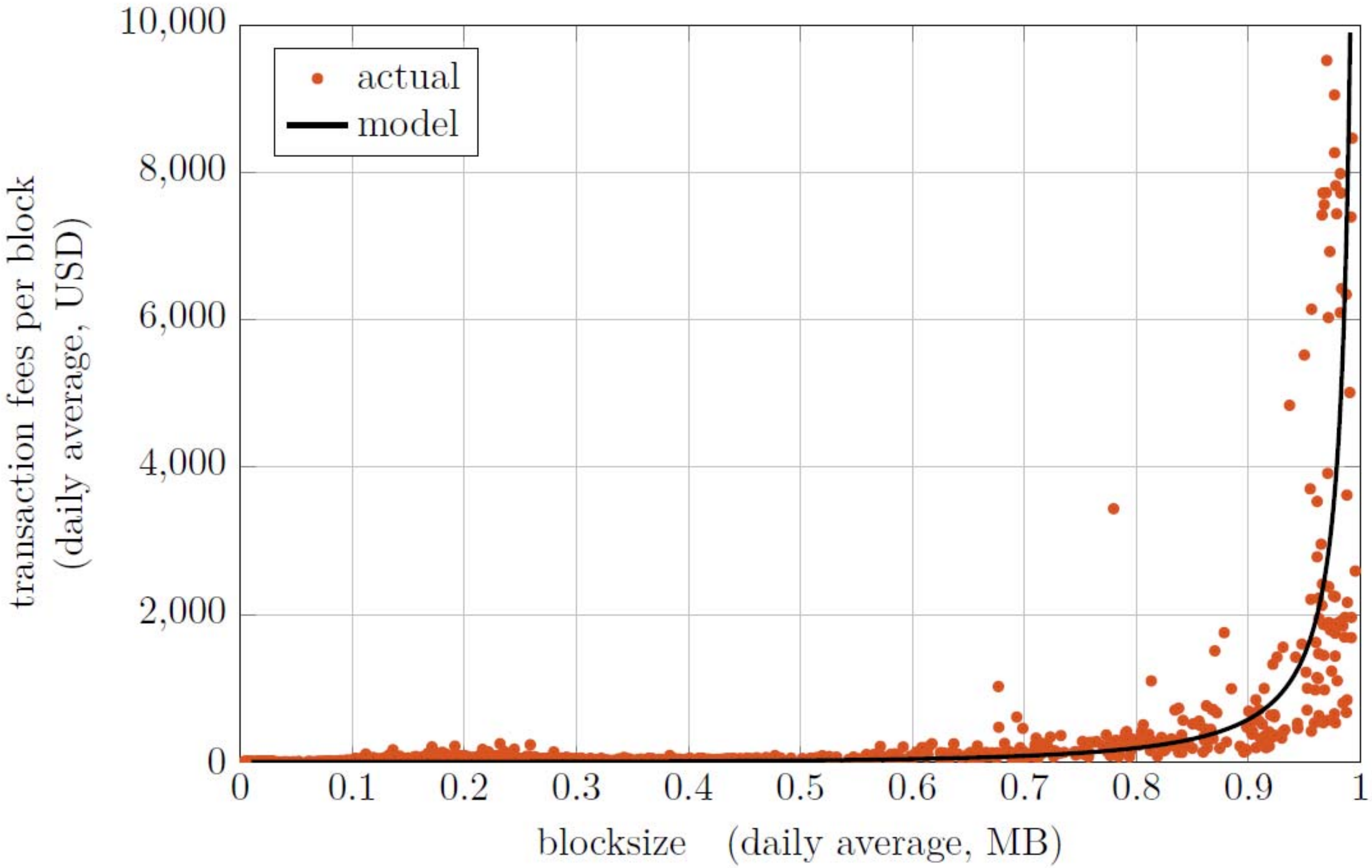
$$u(c_i) = \mathrm{R} - c_i \cdot W(b_i|G) - b_i$$

where $W(b_i|G)$ is the expected delay for a user who bids b_i given distribution of others bids G

In Equilibrium,

- Users with higher delay costs pay higher transaction fees, receive higher priority and lower delay
- Transaction fee paid by a user is equal to the externality imposed on other transactions

Data: Total Transaction Fees vs Congestion



- Model curve parameters: $K = 2{,}000$, and delay costs $c \sim U[0, 0.1]$ for 10min.

Revenue and infrastructure

- Infrastructure provided at cost
  - Free entry/exit, competition of miners
- Revenue determines infrastructure level
- Revenue varies with congestion
  - Infrastructure level can be too low or too high
  - Congestion and delay costs are necessary for positive revenue

Potential Instability

Corollary: *No Delays ⇒ No Revenues*

- Low utilization ρ implies low revenue, miners exit
- Miners exit does not generate congestion
  - System throughput is independent of number of miners
- System becomes unreliable with low number of miners (latency, vulnerability)
  - Potentially reducing user demand and ρ
  - Bad dynamics, leads to system collapse

Costs, Potential Waste

- Costly design
  - Redundancies
  - Tournament for random selection of miners
- Delay costs are necessary to incentivize payment
- Infrastructure level (number of miners) may not be optimal
  - Determined by transaction fee payments due to congestion, not the need for more miners
- Potential instability
  - Entry/Exit does not help balance the system

Summary

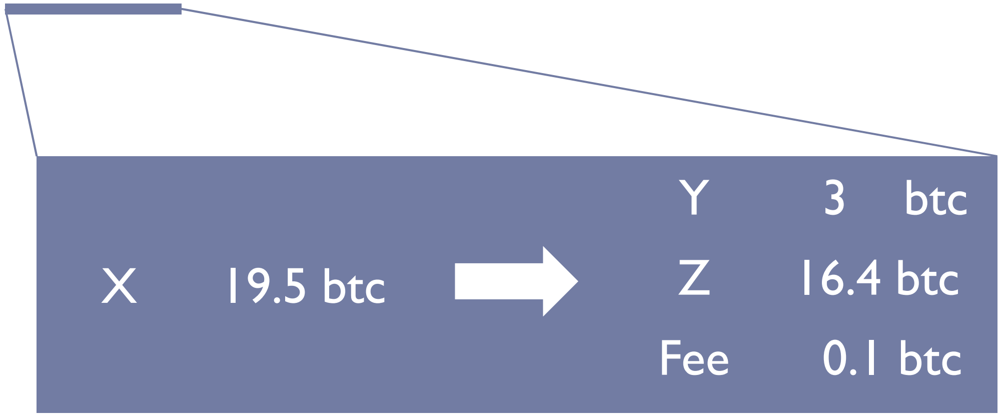
- Economic innovation of Blockchain technology
  - No owner
  - Competitive pricing, even if the platform is a monopoly
  - Fees determined in equilibrium

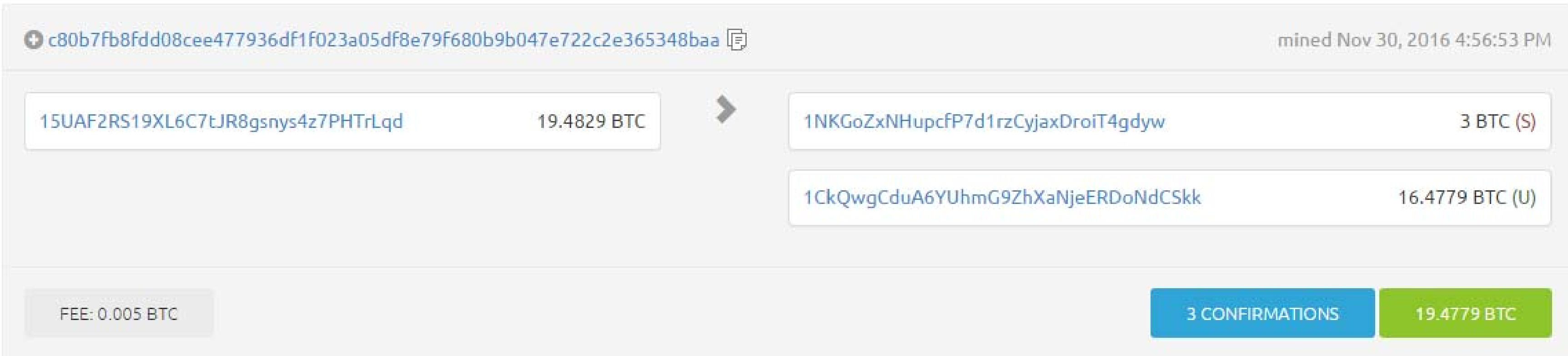
- Congestion as a revenue generating mechanism
  - System can raise revenue while serving all potential users
  - Requires congestion, delay costs

- Design of revenue generating rules
  - Control congestion to target revenue
  - Benefit of smaller block size
  - Future work – what revenue generating rules are implementable?

The Blockchain ledger

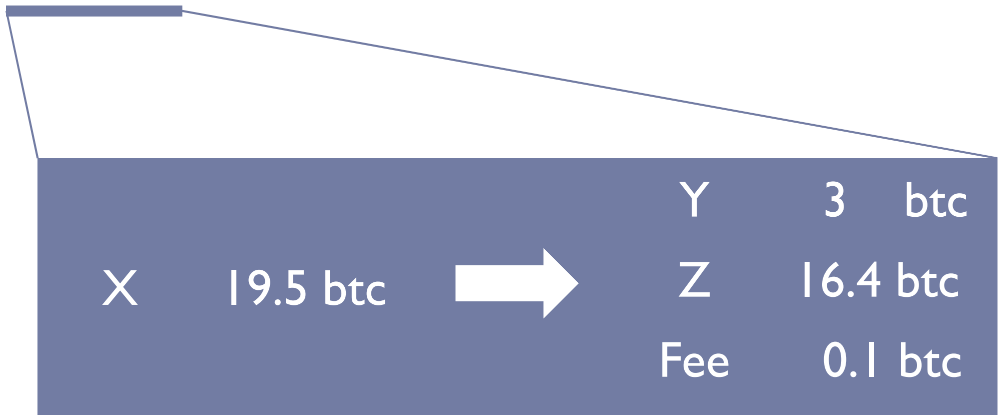
- A bitcoin transaction is a balance transfer between addresses
- Sent publicly (to the mempool)





The Blockchain ledger

- A bitcoin transaction is a balance transfer between addresses

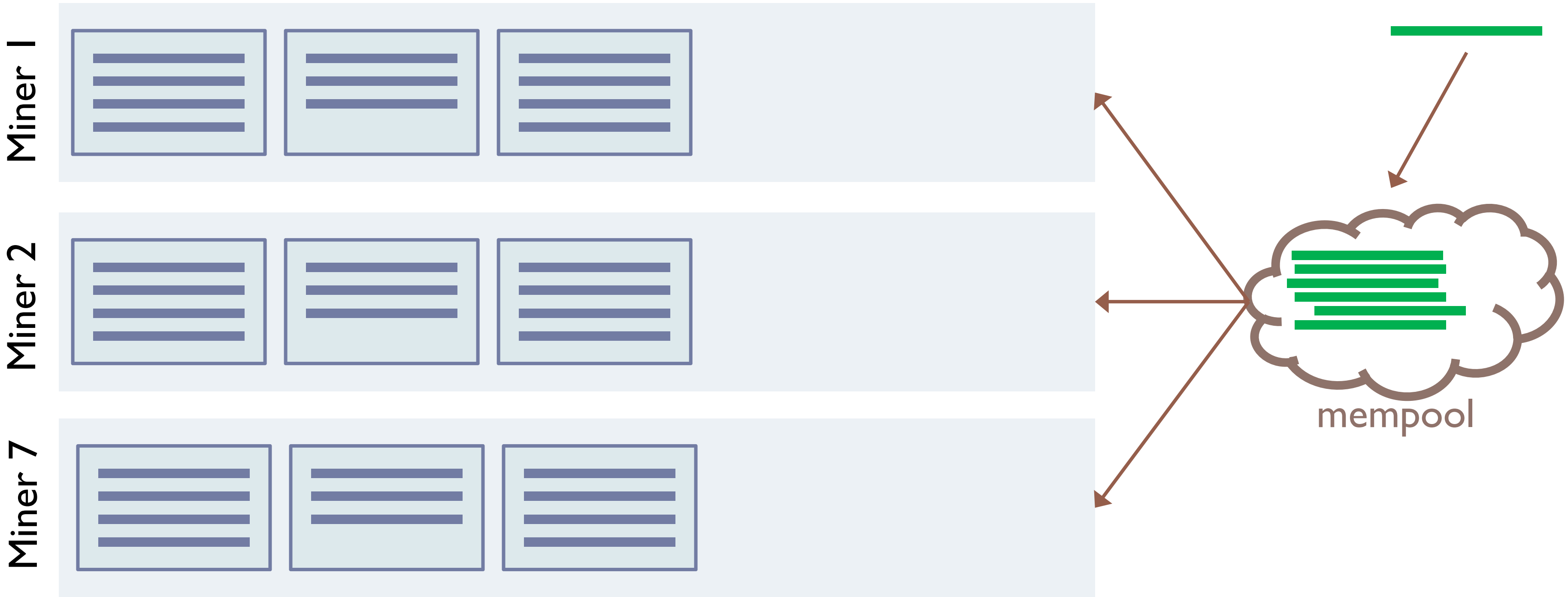


- The Blockchain ledger is a list of all past transactions, organized into blocks

Blockchain

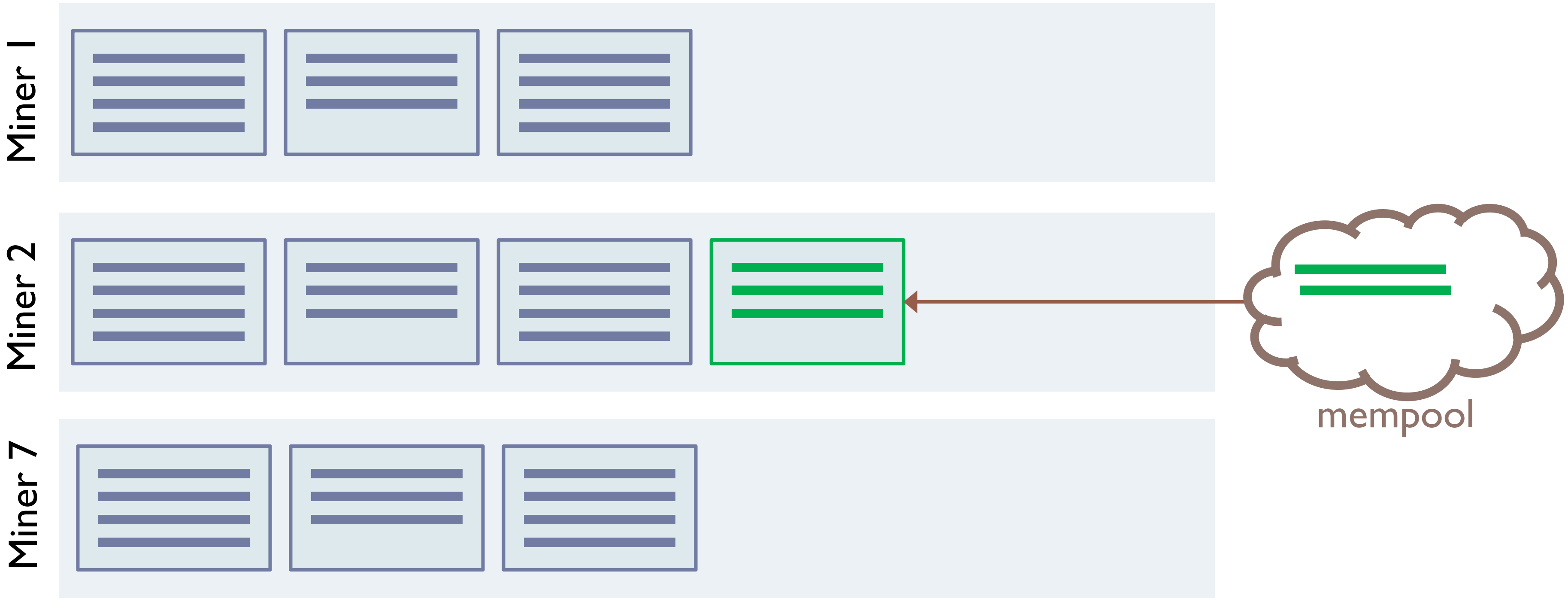
- Many Miners, free entry
- All hold identical copies of the blockchain

Blockchain



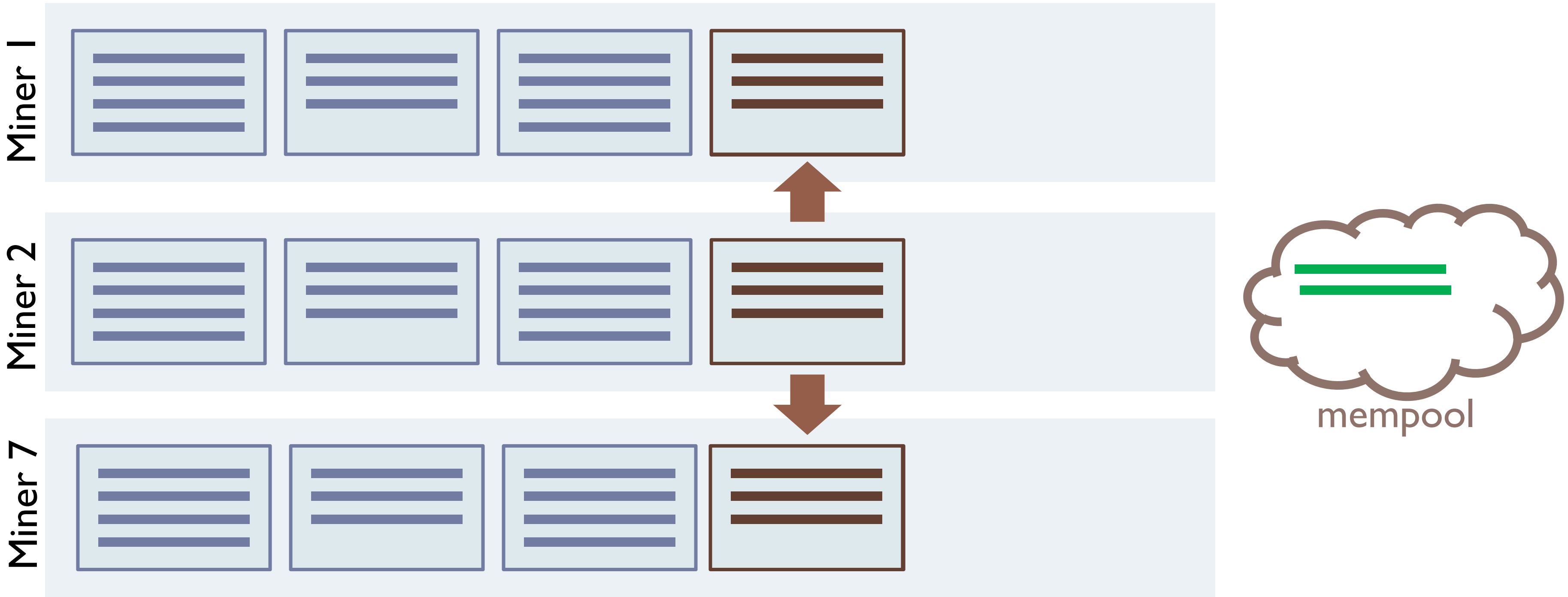
- New transactions transmitted to all miners

Blockchain



- Every 10 min (on avg), one randomly selected miner creates/mines a new block
- Maximal block size is 1MB (approx. 2000 transactions)
  - Unprocessed transactions remain, wait for next block

Blockchain



- New mined block transmitted to all miners
- Vetted by others, becomes part of the blockchain

Blockchain

- Miners rewarded when mine a block:
  1. Fixed amount of newly minted coins
     - Majority of current reward
     - Only short term, halved every 4 years
  2. Transactions fees from transactions within the mined block
     - Long term

- Decentralized random selection by a tournament
  - Avoids the need for a trusted randomization device
  - Requires costly effort from each miner
  - Arrival of new blocks follows a Poisson process

Blockchain

- Equilibrium for (small) miners to follow the consensus blockchain
  (Nakamoto 2008, Eyal & Sirer 2013)
  - Only valid transactions – verification using cryptography
  - Accept others' blocks – follow the longest chain
  - With sufficiently many miners the system is secure

Blockchain – Properties

- Users choose transaction fees
- (Small) Miners are price takers
  - Provide computational infrastructure, rewarded by transaction fees and newly minted coins
  - Cannot block transactions, affect user behavior or transaction fees
- Free entry and exit of miners
- System's throughput independent of number of miners
  - Set by protocol parameters ($1MB$, 10min)

A Simplified Economic Model

- N (small) miners
  - Equal computing power, equal cost of mining c_m
  - Many potential miners, free entry/exit
- Blocks mined at Poisson rate μ
  - Up to K transactions processed per block
- Users/transactions arrive at Poisson rate $\lambda < K \cdot \mu$
  - Each user has a single transaction, selects fee $b \geq 0$
  - Heterogeneous delay cost $c \sim F[\,0, \overline{c}\,]$

Simplified Economic Model

- Assumptions:
  - Unobservable queue
  - Sufficiently high value for service R, all users served
  - No new coins minted
  - Sufficiently many miners for the system to operate securely