Blockchain Economics

Joseph Abadi & Markus Brunnermeier

(Preliminary and not for distribution)

March 9, 2018

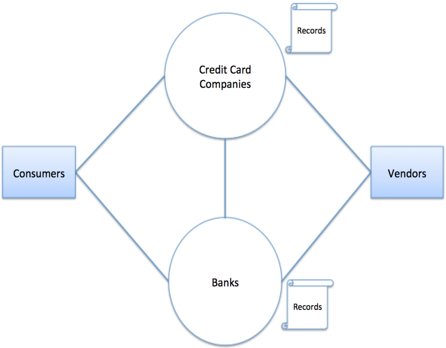
Motivation

Ledgers are "written" and maintained by

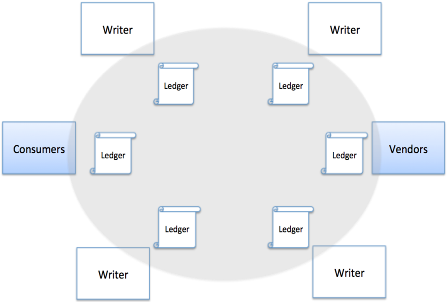
- **Centralized intermediaries** (traditional)
  - maintained by single, centralized agent
  - private
  - trusted because of franchise value
- **Blockchain technology** (new alternative)
  - maintained by many anonymous agents
  - publicly viewable
  - agreed-upon ledger
  - Large computational costs instead of franchise value

When Centralized Intermediary, when Blockchain?

Main question: When is it *cheaper to secure* transactions via blockchain?

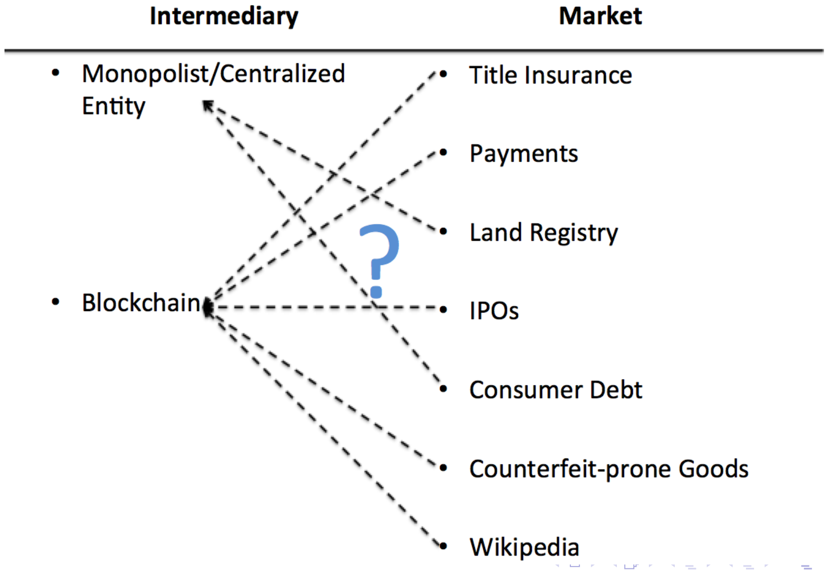


(a) Centralized record-keeping



(b) Decentralized record-keeping

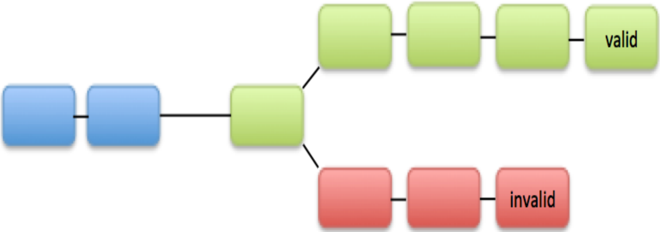
When Centralized Intermediary, when Blockchain?



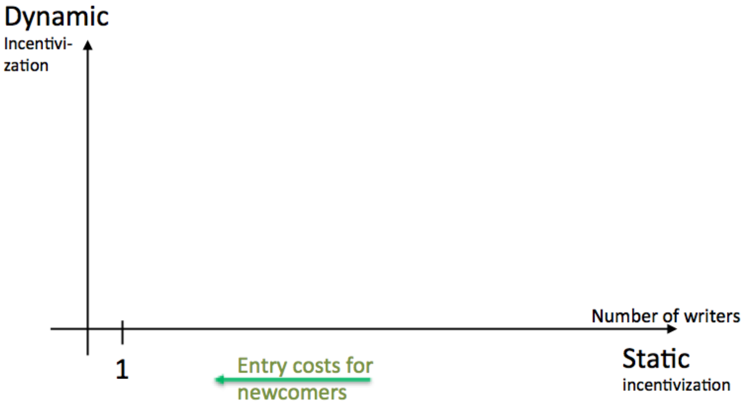
What is a Blockchain?

- Blockchain is a **ledger** in which agents known as writers (or nodes) take turns writing on it.
  - Many ways to choose which writer records the state – discussed later.
- Ledger consists of a **tree of blocks**.
- Current **state** =
  - = longest "valid" chain.
  - = *entire chain* of transactions leading up to that block.
- **Validity** of a chain is determined by **public consensus**
  - Writers signal their acceptance of a block as valid by extending the chain corresponding to that block.
  - Writers earn rewards when their block is on the longest chain, so there are incentives for coordination.

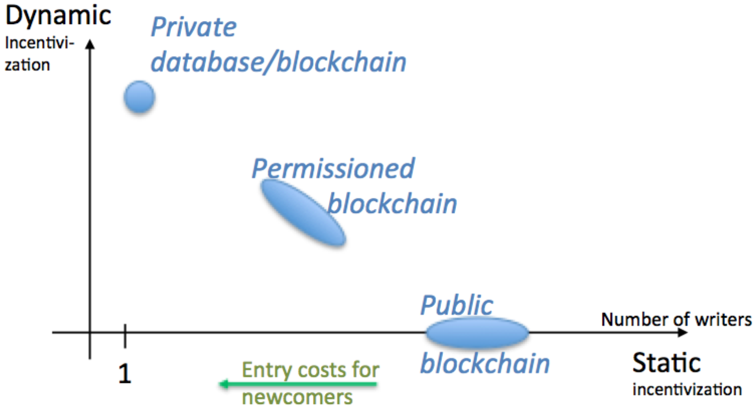
What is a Blockchain? (cont.'d)



Incentives Across the Spectrum



Incentives Across the Spectrum



Types of Blockchains

Private Blockchain:

- *Written* by a centralized entity, but possibly
  Readable in real-time by the public or a regulator.
- Disciplined by readers of ledger (threat to leave blockchain)

Permissioned Blockchain:

- *Write privileges* granted to consortium of entities
  Read privileges may be unrestricted.
- Writers are disciplined by those with read privileges **and other nodes**.

Public Blockchain:

- Write and read privileges are unrestricted $\Rightarrow$ Free entry!
- Writers are disciplined as in permissioned blockchains.
- Needs identity management: **proof-of-work**, proof-of-stake, etc.
  - Otherwise, Sybil attack:
    Create thousands of nodes to write the history you want.
  - real computational resource costs to add block
    (except if useful computations, like DNA decoding)
  - Compensation scheme $\Leftarrow$ free entry condition

When is Proof-of-Work Necessary?

- If readers/users refuse to trade on any ledger that's been attacked
  $\Rightarrow$ Private blockchain
- If writers refuse to build on any invalid block
  $\Rightarrow$ Permissioned blockchain
- Proof-of-Work:
  1. Readers/users can be "fooled" and trade on invalid ledgers.
  2. Writers are able to collude and steal from readers/users.

Relation to Literature

- Rationale of PoW in many CS studies:
  PoW to defend against "double-spending" attacks
  - Writers obtain 51% of the network's computing power and build long chains on which they didn't spend certain coins.
- Most blockchain studies (CS and Econ):
  nobody can steal your assets or create new ones out of thin air.
- This paper:
  - mechanism to defend against arbitrary attacks
    - ★ Writers can write whatever they want (not just double-spending).
    - ★ Readers/users can freely choose (competing) ledger.
  - No need to assume fraction of "honest writers."
  - No need to assume collusion is impossible ex-ante.

Overview of Results

- Basic trade-offs (fee to incentivize writers)
  - Static: writer(s) "distort" $\Rightarrow$ readers/users leave with higher prob.
  - Dynamic: franchise values
- **Security** of blockchain is guaranteed for two reasons:
  1. *Joint attacks* by several writers are unprofitable because writers don't internalize the effects of their actions on others' profits.
  2. *Collusion* in repeated setting is ruled out because of free entry
- **Efficiency** of blockchain $>$ monopolistic intermediation (in static setting) when
  - The sensitivity of consensus to a writer's actions is small;
  - Franchise values are insensitive to deviations by the intermediary.
  - $\Rightarrow$ Optimal number of writers/monitors/miners
- **Ownership vs. Possession**
  - Blockchains don't guarantee secure transfer of possession, just ownership.
  - Blockchains with several writers are unable to discipline issuers of promises when they default.
  - Blockchains can't prevent monopolistic "enforcers" from selectively enforcing contracts.

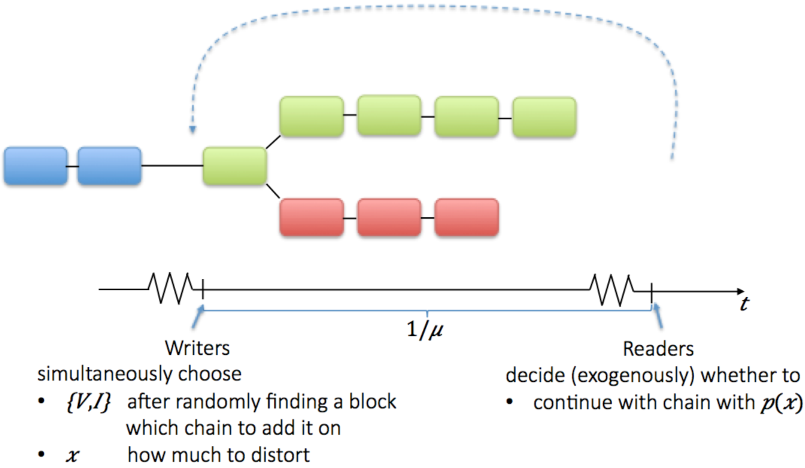
Roadmap

1. What is a blockchain?
2. Fee needed for "trustworthy"/incentivized
   - Blockchain with M miners/writers
   - Intermediary with 1 central record keeper
3. Ownership vs. possession (enforcement)

Public Blockchain– Model Setup

- Agents:
  - Writers, M, who search for blocks
  - Free entry of writers $\Rightarrow$ no dynamic play
  - Readers who "accept" blocks
- Time: continuous, $t \in [0, \infty)$
- Blockchain:
  Tree of blocks $B^t = (B_1, \ldots, B_n)$ with a partial order $\prec_t$ satisfying the usual properties of a tree.
  - There is a minimal block and each block has a unique predecessor.
  - The tree can only be extended; blocks can't be erased or rearranged.
- Sequencing:
  - Writers' actions x (more later)
  - Readers choose chain of blocks
    - At random points in time – Poisson arrival rate μ
    - Readers' acceptance probability $p(x)$,
      = function of writers' actions on a given chain
  - payoff's realize

Summary


t
1/μ
Writers
simultaneously choose
• {V,I} after randomly finding a block which chain to add it on
• x how much to distort
Readers
decide (exogenously) whether to
• continue with chain with p(x)

Blockchains and Funding Limits

- **Lesson 1:**
  Financial frictions are necessary for a blockchain to function!
- Writers exert costly computing power in order to "find" blocks. In each block, writers receive some transaction fees.
- Suppose writers have access to unlimited funding $\Rightarrow$ single writer
  - If M writers each value their computers at Q, a single writer values M computers strictly more than MQ.
  - If a single writer owns all the computers,
    she extracts fees + monopolistic rents.
- *Assumption:*
  Each potential writer can only "afford" the same limited computing power.

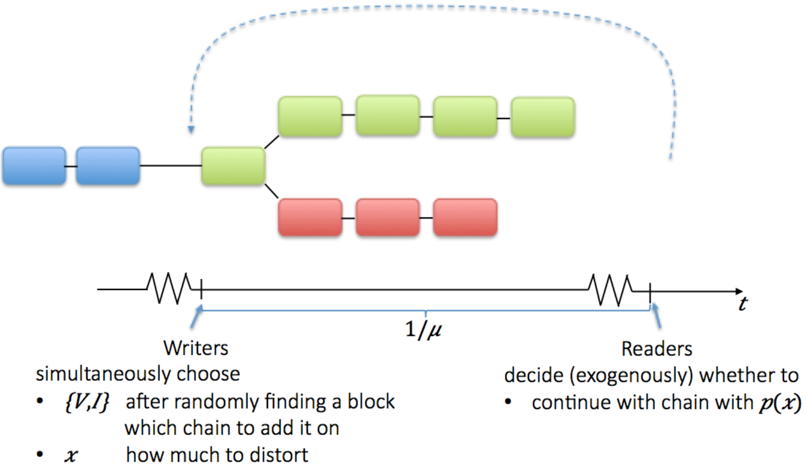
Setup – Writers

- k blocks that randomly arrive within window of random length $1/\mu$
- Writers expend c units of computing resources in order to find blocks
  - arrive at rate $\frac{\eta}{M}$ for an individual writer.
- Assume there are two chains of blocks:
  valid chain V and invalid chain I.
- Writing strategy: $m_i \in \{V, I\}$
- Writer's action strategy: $x_i \in [0, \overline{x}]$
  - x = deviation from truth
- n_V, n_I = number of blocks found on the valid and invalid chains, by a writer who plays action x.
  That writer's payoffs are
  - ϕn_V if the valid chain is accepted
  - $(\phi + x) n_I$ if the invalid chain is accepted
- Free entry to become a writer: $\frac{\eta \phi}{M} = c$

Setup – Readers

- Readers choose whether to accept the valid or invalid chain.
- If valid chain is longer, they accept it automatically.
- If invalid chain is longer, they accept it w/ exogenous prob. $1 - p(\hat{x})$
  - $\hat{x}$ = average action taken by writers
  - $p(\hat{x}) = 0$, readers detect deviation immediately
    $\Rightarrow$ blockchain is automatically secure against any attack even with $M = 1$.
  - Recall at $\hat{x} = \overline{x}$, $p(\overline{x}) = 0$.

Summary


t
1/μ
Writers
simultaneously choose
• {V,I} after randomly finding a block
which chain to add it on
• x how much to distort
Readers
decide (exogenously) whether to
• continue with chain with p(x)

Equilibrium

Lemma

In any equilibrium, all writers play on the same chain.

- Intuition: One writer can always mimic another writer's action and receive at least the same payoff.
- By playing on the same chain as another writer, the chance that the chain is accepted increases.
  - $\Rightarrow$ Higher payoffs for all writers on that chain
- Readers' preference for consensus (long chains) implies writers have an incentive to coordinate.

Static Equilibrium Conditions

In an equilibrium in which all writers play on the invalid chain, a writer's optimization problem is

$$\max_{x}(\phi + x)E\left[\left(1 - p\left(\frac{k-n}{k}x^* + \frac{n}{k}x\right)\right)n\right]$$

The first-order condition in a symmetric equilibrium is

$$1 = \underbrace{\frac{p'(x^*)}{p(x^*)}}_{hazard\ \ rate} \frac{1}{\kappa(M)}(\phi + x^*)$$

where

$$\frac{1}{\kappa(M)} = \frac{1}{M} + \frac{M-1}{M}\frac{1}{E[k]}$$

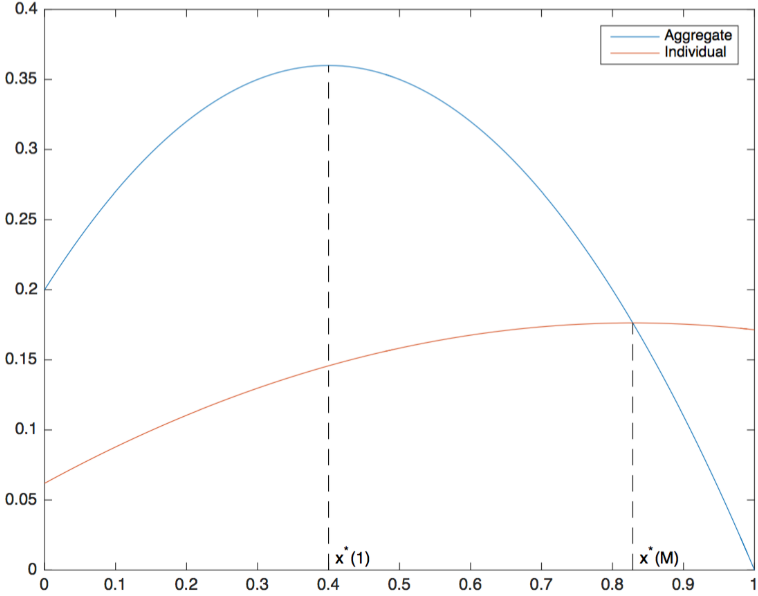
Lemma

When expected number of blocks, $E[k]$, is sufficiently large, there is **no** equilibrium in which writers play on the **invalid chain** for large M.

Why Are Attacks Unprofitable?

1. Each writer doesn't internalize the effect his action has others' profits
2. Writers steal more than is optimal in aggregate;
3. The probability that readers reject the ledger increases;
4. Expected revenues on the invalid chain become lower than revenues on the valid chain;
5. Writers switch to the valid chain.

Why Are Attacks Unprofitable? (cont.'d)



Roadmap

1. What is a blockchain?
2. Model setup
3. Fee needed for "trustworthy"/incentivized
   - Blockchain with M miners/writers
   - Intermediary with 1 central record keeper
4. Ownership vs. possession (enforcement)

Monopolistic Intermediary Benchmark

- no free entry $\Rightarrow$ dynamic incentivization through franchise value
- Consider a monopolist who maintains a ledger and solves
  - Discount factor δ
  - Deviation x discovered with probability $p(x)$
  - Intermediary forgiven with probability q on discovery

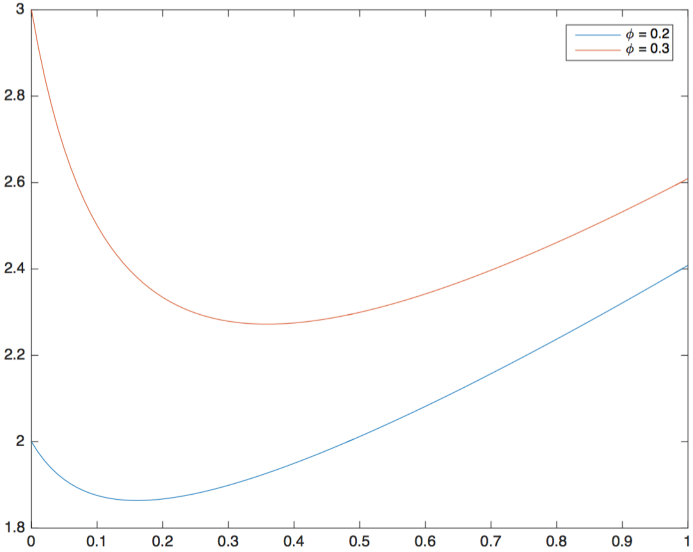
$$\max_x \; (\phi + x) + \delta\big(1 - p(x)(1-q)\big)(\phi + x) + \dots$$

$$\max_x \; \frac{\phi + x}{1 - \delta(1 - p(x)(1-q))}$$

Lemma

The intermediary chooses $x = 0$ iff $\phi \geq \frac{1-\delta}{\delta(1-q)}\overline{x} \equiv \underline{\phi}^I$.

Monopolistic Intermediary Benchmark (cont.'d)



Fee Comparison

- Can writers on a blockchain be incentivized to play $x^* = 0$ for a **lower (aggregate) fee** than a monopolist?
- Let $\overline{M} = \frac{\eta}{c}\underline{\phi}^I$. (How many miners can one afford instead of intermediary?) We want for some $M \leq \overline{M}$, deviation is not profitable, i.e.

$$(\phi(M) + x^*(M))(1 - p(x^*(M))) < \phi(M)$$

- *Example:* With $p(x) = \pi x$, this holds for some $M \leq \overline{M}$ iff

$$\kappa(\overline{M}) < \frac{\delta}{1-\delta}(1-q)$$

Fee Comparison - Optimal Number of Writers

- Approximate $\kappa(\overline{M}) \approx E[k] = \frac{\eta}{\mu}$ (holds for large $\overline{M}$)

$$E[k] \approx \kappa(\overline{M}) < \frac{\delta}{1-\delta}(1-q)$$

$\Rightarrow$ independent of sensitivity π. (Recall $p(x) = \pi x$.)

- $\Rightarrow$ **optimal number of writers:**

$$M^* = \frac{1}{\pi c T}$$

where $T \equiv 1/\mu$ is the average length of a period.

  - High π $\Rightarrow$ Unprofitable theft for low M
  - High cT $\Rightarrow$ Higher costs for the same M

Roadmap

1. What is a blockchain?
2. Model setup
3. Fee needed for stable
    - Blockchain with M miners/writers
    - Intermediary with 1 central record keeper
4. Ownership vs. possession (enforcement)
    - Blockchain with a monopolistic enforcer (government)
    - Blockchain with defaultable promises

Blockchain: Ownership vs. Possession

- Several blockchain proposals involve using blockchains as ownership databases for all kinds of assets– not just cryptocurrencies.
  - E.g. WSJ: "How Blockchain Can End Poverty"
- So far: ignored distinction between **ownership** and **possession**.
  - *Ownership* is traded in the secondary market
  - *Possession* is conferred by the previous possessor and enforced by some entity
- **Currency** is the outlier: no fundamental value.
- Blockchain is good for determining ownership but not possession.
  - No security against an enforcer who selectively enforces contracts.
  - Provides security when issuers want to coordinate with intermediaries.
  - No discipline for issuers who want to default.

Blockchain and Enforcement

- There is an enforcer and M writers.
- The enforcer does not like enforcing contracts and chooses how many to enforce.
- Writers choose how much to cooperate with the enforcer and receive bribes for doing so.
  - E.g. writers could erase ownership records for land the government wants to seize.
  - More bribes $\Rightarrow$ greater probability of detection
- Main result: The equilibrium is independent of the number of miners.
  - More miners $\not\Rightarrow$ more security!
  - The enforcer can control the extent of deviations by choosing how much to bribe.
  - The enforcer makes sure writers never steal too much and get detected.

Intermediation with Defaultable Promises

- M writers
- Continuum of issuers
  - Each wants to default on promise on ledger
  - Try to bribe writers to cooperate with default
    - Example:
      Company bribes an exchange to lie, says shares it issues are authentic
- Two cases for issuers:
  - Issuers want to *coordinate* default with writers
    $\Rightarrow$ Same problem as before
  - Default is *dominant*: can issuers be disciplined?
- Writers may choose to deny service to issuers $\Rightarrow$ zero payoff
  - No denial of service in a static setting
    $\Rightarrow$ Dynamic setting is needed

Discussion

- Our examples follow from two main results:
  1. **Security**:
     Selfish incentives to steal make joint ledger distortion unprofitable.
  2. **No Collusion**:
     Free entry $\Rightarrow$ No off-equilibrium punishments/rewards.
- In contrast to CS literature
  - No need to assume fraction of "honest writers."
  - No need to assume collusion is impossible ex-ante.
    - This emerges naturally from the free entry condition.
    - Ex-ante impossible collusion $\Rightarrow$ No PoW.

When anonymous PoW blockchain

- Markets where reputations are insensitive to deviations
  - E.g., TBTF
- Markets where issuers want to coordinate deviations with intermediaries
  - E.g. Title insurance, counterfeiting, IPOs
- **Not** with monopolistic enforcers.
  - E.g. Land registries
- **Not** when issuers need to be disciplined.
  - E.g. Consumer debt markets

Conclusions