Blockchain Disruption and Smart Contracts

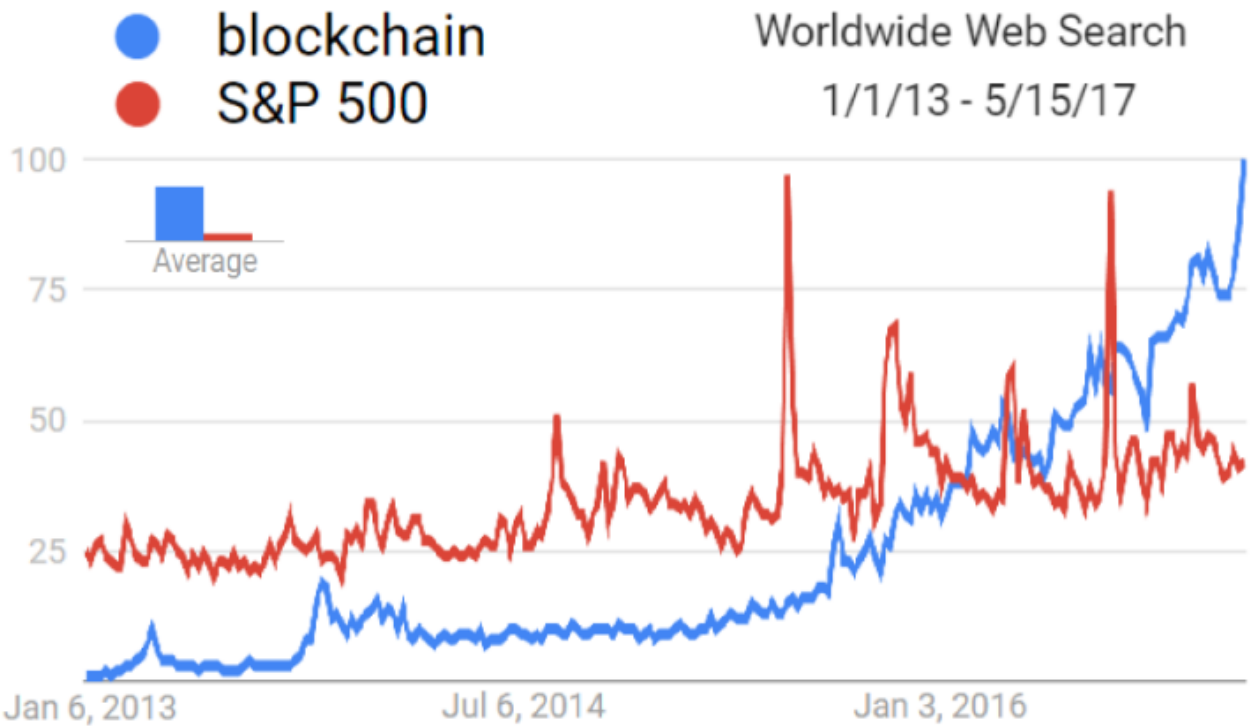
Lin William Cong
University of Chicago

Zhiguo He
University of Chicago

September 28-29, 2017

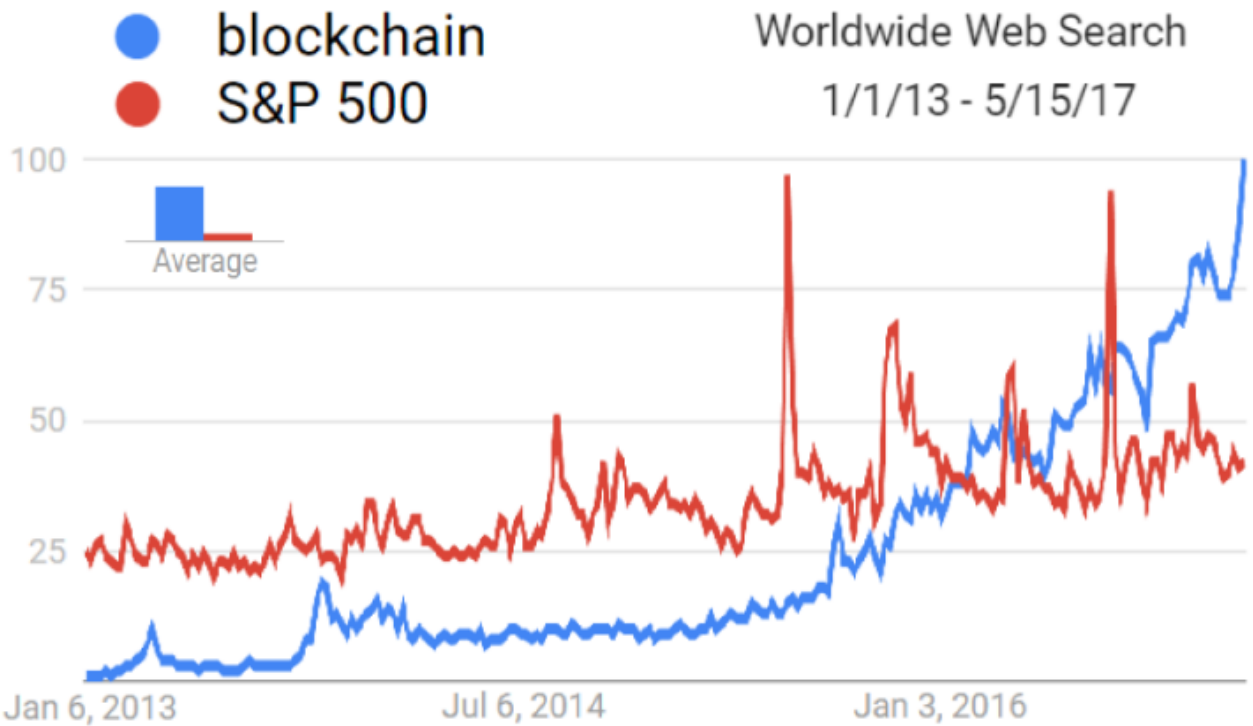
Fifty Shades of Blockchain

"The Trust Machine", "Distributed Trust Network",
"Bitcoin", "Ethereum", "Distributed Ledger"...
Smart Contracts



Fifty Shades of Blockchain

"The Trust Machine", "Distributed Trust Network",
"Bitcoin", "Ethereum", "Distributed Ledger"...
Smart Contracts



Research Questions

- Unifying features of blockchain: decentralized consensus and information.
- Economic impact of blockchain and smart contracts, especially on industrial organization and competition.

Research Questions

- Unifying features of blockchain: decentralized consensus and information.
- Economic impact of blockchain and smart contracts, especially on industrial organization and competition.

Outline

- **Introduction & Institutional Background**
- Decentralized Consensus & Information Distribution
- Blockchain Disruption & Industrial Organization
- Regulation & Discussion
- Conclusion

What is Blockchain?

- Bitcoin – the original blockchain: double-spending, distributed ledger.
- A database system in which parties unknown to each other can jointly maintain and edit in a decentralized manner, with no individual party exercising central control.
- Decentralized consensus
  - Safe, robust, cheap, & decentralized.
  - Errors, manipulations, & attacks.
- Information Distribution.
  - Record-keepers, incentives, organization & community.
  - Privacy, transparency, encryption, & informational environment.

What is Blockchain?

- Bitcoin – the original blockchain: double-spending, distributed ledger.
- A database system in which parties unknown to each other can jointly maintain and edit in a decentralized manner, with no individual party exercising central control.
- Decentralized consensus
  - Safe, robust, cheap, & decentralized.
  - Errors, manipulations, & attacks.
- Information Distribution.
  - Record-keepers, incentives, organization & community.
  - Privacy, transparency, encryption, & informational environment.

What is Blockchain?

- Bitcoin – the original blockchain: double-spending, distributed ledger.
- A database system in which parties unknown to each other can jointly maintain and edit in a decentralized manner, with no individual party exercising central control.
- Decentralized consensus
  - Safe, robust, cheap, & decentralized.
  - Errors, manipulations, & attacks.
- Information Distribution.
  - Record-keepers, incentives, organization & community.
  - Privacy, transparency, encryption, & informational environment.

What is Blockchain?

- Bitcoin – the original blockchain: double-spending, distributed ledger.
- A database system in which parties unknown to each other can jointly maintain and edit in a decentralized manner, with no individual party exercising central control.
- Decentralized consensus
  - Safe, robust, cheap, & decentralized.
  - Errors, manipulations, & attacks.
- Information Distribution.
  - Record-keepers, incentives, organization & community.
  - Privacy, transparency, encryption, & informational environment.

What is Blockchain?

- Bitcoin – the original blockchain: double-spending, distributed ledger.
- A database system in which parties unknown to each other can jointly maintain and edit in a decentralized manner, with no individual party exercising central control.
- Decentralized consensus
  - Safe, robust, cheap, & decentralized.
  - Errors, manipulations, & attacks.
- Information Distribution.
  - Record-keepers, incentives, organization & community.
  - Privacy, transparency, encryption, & informational environment.

What is Blockchain?

- Bitcoin – the original blockchain: double-spending, distributed ledger.
- A database system in which parties unknown to each other can jointly maintain and edit in a decentralized manner, with no individual party exercising central control.
- Decentralized consensus
  - Safe, robust, cheap, & decentralized.
  - Errors, manipulations, & attacks.
- Information Distribution.
  - Record-keepers, incentives, organization & community.
  - Privacy, transparency, encryption, & informational environment.

Two Important Questions

1. Why and how to create decentralized consensus?
   - Compensation for miners: Kiayias et al (2016), Baldimtsi et al (2017)
   - Mining as a game: Eyal and Sirer (2014), Nayak et al (2016), Biais et al (2017).
   - Proof-of-work, proof-of-stake, proof-of-burn, ...
   - Benefits of decentralized consensus.
   - Achieving it requires distribution of information.

2. What are its economic implications?
   - Greater contractibility: rise of smart contracts.
   - Greater information distribution: more sustainable dynamic equilibria.

Two Important Questions

1. Why and how to create decentralized consensus?
   - Compensation for miners: Kiayias et al (2016), Baldimtsi et al (2017)
   - Mining as a game: Eyal and Sirer (2014), Nayak et al (2016), Biais et al (2017).
   - Proof-of-work, proof-of-stake, proof-of-burn, ...
   - Benefits of decentralized consensus.
   - Achieving it requires distribution of information.

2. What are its economic implications?
   - Greater contractibility: rise of smart contracts.
   - Greater information distribution: more sustainable dynamic equilibria.

Two Important Questions

1. Why and how to create decentralized consensus?
   - Compensation for miners: Kiayias et al (2016), Baldimtsi et al (2017)
   - Mining as a game: Eyal and Sirer (2014), Nayak et al (2016), Biais et al (2017).
   - Proof-of-work, proof-of-stake, proof-of-burn, ...
   - Benefits of decentralized consensus.
   - Achieving it requires distribution of information.
2. What are its economic implications?
   - Greater contractibility: rise of smart contracts.
   - Greater information distribution: more sustainable dynamic equilibria.

Smart Contracts & Applications

- *Smart contracts are digital contracts allowing terms contingent on decentralized consensus and are self-enforcing and tamper-proof through automated execution.*
- What smart contract is NOT? Digital contracts, centralized authority, human-intermediation/execution, "smart"/AI, complete contract.
- Applications in the Financial Industry:
  - Trusted payments: Bitcoin, Lightning, Ripple, Ethereum, Phi, Corda, etc.
  - Trade finance: R3 CEV, IBM, Wave, HK Blockchain, DTC, etc.
  - Trading and exchanges: Nasdaq Linq, Symbiont, NYIAX, etc.

Smart Contracts & Applications

- *Smart contracts are digital contracts allowing terms contingent on decentralized consensus and are self-enforcing and tamper-proof through automated execution.*
- What smart contract is NOT? Digital contracts, centralized authority, human-intermediation/execution, "smart"/AI, complete contract.
- Applications in the Financial Industry:
  - Trusted payments: Bitcoin, Lightning, Ripple, Ethereum, Phi, Corda, etc.
  - Trade finance: R3 CEV, IBM, Wave, HK Blockchain, DTC, etc.
  - Trading and exchanges: Nasdaq Linq, Symbiont, NYIAX, etc.

Outline

- Introduction & Institutional Background
- **Decentralized Consensus & Information Distribution**
- Blockchain Disruption & Industrial Organization
- Regulation & Discussion
- Conclusion

Keepers and Verification

- Miners (Bitcoin/Ethereum), validation nodes (Ripple/R3), etc.
- Public information, "oracles", private signals.
- Fundamental tension in information distribution
- No news is news; encrypted data are data.

Keepers and Verification

- Miners (Bitcoin/Ethereum), validation nodes (Ripple/R3), etc.
- Public information, "oracles", private signals.
- Fundamental tension in information distribution
- No news is news; encrypted data are data.

Keepers and Verification

- Miners (Bitcoin/Ethereum), validation nodes (Ripple/R3), etc.
- Public information, "oracles", private signals.
- Fundamental tension in information distribution
- No news is news; encrypted data are data.

Keepers and Verification

- Miners (Bitcoin/Ethereum), validation nodes (Ripple/R3), etc.
- Public information, "oracles", private signals.
- Fundamental tension in information distribution
- No news is news; encrypted data are data.

A Simple Model

- Contingent state $\tilde{\omega}$; consensus $\tilde{z}$; K keepers.
- Effectiveness: $-Var\left(\widetilde{\omega}-\widetilde{z}\right)$
- Consensus rule: $\widetilde{z}(\mathbf{y})=\frac{1}{K}\sum_k \widetilde{y}_k$.
- Info on blockchain: $\widetilde{x}_i=\widetilde{\omega}+\widetilde{\eta}_i$
- Info upon contact: $\widetilde{x}_k=\widetilde{\omega}+\widetilde{\eta}_k$, $\sigma_K \leq \sigma_\eta$
- Misreporting:
  $U(y_k;\mathbf{y})=\widetilde{b}_k\cdot\left(\widetilde{z}(\mathbf{y})-\widetilde{x}_k\right)-\frac{1}{2h}\left(y_k-\widetilde{x}_k\right)^2$
- Bias: $\widetilde{b}_k\equiv\widetilde{b}+\widetilde{\varepsilon}_k$

A Simple Model

- Contingent state $\tilde{\omega}$; consensus $\tilde{z}$; K keepers.
- Effectiveness: $-Var\left(\widetilde{\omega}-\widetilde{z}\right)$
- Consensus rule: $\widetilde{z}(\mathbf{y})=\frac{1}{K}\sum_k \widetilde{y}_k$.
- Info on blockchain: $\widetilde{x}_i=\widetilde{\omega}+\widetilde{\eta}_i$
- Info upon contact: $\widetilde{x}_k=\widetilde{\omega}+\widetilde{\eta}_k$, $\sigma_K \leq \sigma_\eta$
- Misreporting:
  $U(y_k;\mathbf{y})=\widetilde{b}_k\cdot\left(\widetilde{z}(\mathbf{y})-\widetilde{x}_k\right)-\frac{1}{2h}\left(y_k-\widetilde{x}_k\right)^2$
- Bias: $\widetilde{b}_k\equiv\widetilde{b}+\widetilde{\varepsilon}_k$

A Simple Model

- Contingent state $\tilde{\omega}$; consensus $\tilde{z}$; K keepers.
- Effectiveness: $-Var\left(\widetilde{\omega}-\widetilde{z}\right)$
- Consensus rule: $\widetilde{z}(\mathbf{y})=\frac{1}{K}\sum_k \widetilde{y}_k$.
- Info on blockchain: $\widetilde{x}_i=\widetilde{\omega}+\widetilde{\eta}_i$
- Info upon contact: $\widetilde{x}_k=\widetilde{\omega}+\widetilde{\eta}_k$, $\sigma_K \leq \sigma_\eta$
- Misreporting:
  $U(y_k;\mathbf{y})=\widetilde{b}_k\cdot\left(\widetilde{z}(\mathbf{y})-\widetilde{x}_k\right)-\frac{1}{2h}\left(y_k-\widetilde{x}_k\right)^2$
- Bias: $\widetilde{b}_k\equiv\widetilde{b}+\widetilde{\varepsilon}_k$

A Simple Model

- Contingent state $\tilde{\omega}$; consensus $\tilde{z}$; K keepers.
- Effectiveness: $-Var\left(\widetilde{\omega}-\widetilde{z}\right)$
- Consensus rule: $\widetilde{z}(\mathbf{y})=\frac{1}{K}\sum_k \widetilde{y}_k$.
- Info on blockchain: $\widetilde{x}_i=\widetilde{\omega}+\widetilde{\eta}_i$
- Info upon contact: $\widetilde{x}_k=\widetilde{\omega}+\widetilde{\eta}_k$, $\sigma_K \leq \sigma_\eta$
- Misreporting:
  $U(y_k;\mathbf{y})=\widetilde{b}_k\cdot\left(\widetilde{z}(\mathbf{y})-\widetilde{x}_k\right)-\frac{1}{2h}\left(y_k-\widetilde{x}_k\right)^2$
- Bias: $\widetilde{b}_k\equiv\widetilde{b}+\widetilde{\varepsilon}_k$

A Simple Model

- Contingent state $\tilde{\omega}$; consensus $\tilde{z}$; K keepers.
- Effectiveness: $-Var\left(\widetilde{\omega}-\widetilde{z}\right)$
- Consensus rule: $\widetilde{z}(\mathbf{y})=\frac{1}{K}\sum_k \widetilde{y}_k$.
- Info on blockchain: $\widetilde{x}_i=\widetilde{\omega}+\widetilde{\eta}_i$
- Info upon contact: $\widetilde{x}_k=\widetilde{\omega}+\widetilde{\eta}_k$, $\sigma_K \leq \sigma_\eta$
- Misreporting:
  $U(y_k;\mathbf{y})=\widetilde{b}_k\cdot\left(\widetilde{z}(\mathbf{y})-\widetilde{x}_k\right)-\frac{1}{2h}\left(y_k-\widetilde{x}_k\right)^2$
- Bias: $\widetilde{b}_k\equiv\widetilde{b}+\widetilde{\varepsilon}_k$

A Simple Model

- Contingent state $\tilde{\omega}$; consensus $\tilde{z}$; K keepers.
- Effectiveness: $-Var\left(\widetilde{\omega}-\widetilde{z}\right)$
- Consensus rule: $\widetilde{z}(\mathbf{y})=\frac{1}{K}\sum_k \widetilde{y}_k$.
- Info on blockchain: $\widetilde{x}_i=\widetilde{\omega}+\widetilde{\eta}_i$
- Info upon contact: $\widetilde{x}_k=\widetilde{\omega}+\widetilde{\eta}_k$, $\sigma_K \leq \sigma_\eta$
- Misreporting:
  $U(y_k;\mathbf{y})=\widetilde{b}_k\cdot\left(\widetilde{z}(\mathbf{y})-\widetilde{x}_k\right)-\frac{1}{2h}\left(y_k-\widetilde{x}_k\right)^2$
- Bias: $\widetilde{b}_k\equiv\widetilde{b}+\widetilde{\varepsilon}_k$

A Simple Model

- Contingent state $\tilde{\omega}$; consensus $\tilde{z}$; K keepers.
- Effectiveness: $-Var\left(\widetilde{\omega}-\widetilde{z}\right)$
- Consensus rule: $\widetilde{z}(\mathbf{y})=\frac{1}{K}\sum_k \widetilde{y}_k$.
- Info on blockchain: $\widetilde{x}_i=\widetilde{\omega}+\widetilde{\eta}_i$
- Info upon contact: $\widetilde{x}_k=\widetilde{\omega}+\widetilde{\eta}_k$, $\sigma_K \leq \sigma_\eta$
- Misreporting:
  $U(y_k;\mathbf{y})=\widetilde{b}_k\cdot\left(\widetilde{z}(\mathbf{y})-\widetilde{x}_k\right)-\frac{1}{2h}\left(y_k-\widetilde{x}_k\right)^2$
- Bias: $\widetilde{b}_k\equiv\widetilde{b}+\widetilde{\varepsilon}_k$

Equilibrium Consensus

- $\widetilde{z} = \frac{1}{K}\sum_k \widetilde{y}_k = \widetilde{\omega} + \frac{1}{K}\sum_k \widetilde{\eta}_k + \frac{h}{K}\left(\widetilde{b} + \frac{1}{K}\sum_k \widetilde{\varepsilon}_k\right)$
- Effectiveness

$$-Var(\widetilde{\omega} - \widetilde{z}) = -\left[\underbrace{\frac{\sigma_K^2}{K}}_{\text{signal quality}} + \underbrace{\frac{h^2}{K^2}\left[\sigma_b^2 + \frac{\sigma_\varepsilon^2}{K}\right]}_{\text{manipulation}}\right]$$

- $\widetilde{z} \approx \widetilde{\omega}$, as $K \to \infty$

Equilibrium Consensus

- $\widetilde{z} = \frac{1}{K}\sum_k \widetilde{y}_k = \widetilde{\omega} + \frac{1}{K}\sum_k \widetilde{\eta}_k + \frac{h}{K}\left(\widetilde{b} + \frac{1}{K}\sum_k \widetilde{\varepsilon}_k\right)$
- Effectiveness

$$-Var(\widetilde{\omega} - \widetilde{z}) = -\left[\underbrace{\frac{\sigma_K^2}{K}}_{\text{signal quality}} + \underbrace{\frac{h^2}{K^2}\left[\sigma_b^2 + \frac{\sigma_\varepsilon^2}{K}\right]}_{\text{manipulation}}\right]$$

- $\widetilde{z} \approx \widetilde{\omega}$, as $K \to \infty$

Equilibrium Consensus

- $\widetilde{z} = \frac{1}{K}\sum_k \widetilde{y}_k = \widetilde{\omega} + \frac{1}{K}\sum_k \widetilde{\eta}_k + \frac{h}{K}\left(\widetilde{b} + \frac{1}{K}\sum_k \widetilde{\varepsilon}_k\right)$
- Effectiveness

$$-Var(\widetilde{\omega} - \widetilde{z}) = -\left[\underbrace{\frac{\sigma_K^2}{K}}_{\text{signal quality}} + \underbrace{\frac{h^2}{K^2}\left[\sigma_b^2 + \frac{\sigma_\varepsilon^2}{K}\right]}_{\text{manipulation}}\right]$$

- $\widetilde{z} \approx \widetilde{\omega}$, as $K \to \infty$

Outline

- Introduction & Institutional Background
- Decentralized Consensus & Information Distribution
- **Blockchain Disruption & Industrial Organization**
- Regulation & Discussion
- Conclusion

Setup

- Risk-neutral, discrete time $t = 1, 2, \cdots$.
- Buyers: unit measure, short-lived;
  Aggregate shock: probability λ showing up (indicated by $\mathbb{I}_t$).
- Three long-lived sellers: incumbents (A&B) authentic; entrant (C) authentic with prob π.
  Only authentic sellers deliver at cost μ.
- Quality of service $\mathbf{q} = (q_A, q_B, q_C)$ i.i.d. and public, $[\underline{q}, \overline{q}]$.
  Interpreted as probability of success, upon which buyers get unit utility.

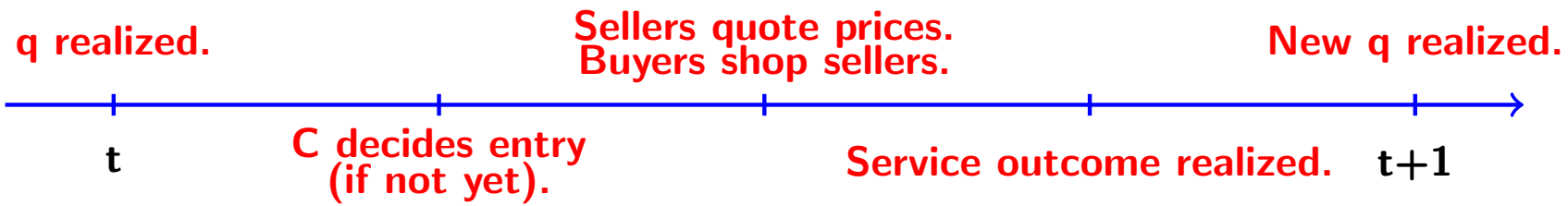
Setup

- Risk-neutral, discrete time $t = 1, 2, \cdots$.
- Buyers: unit measure, short-lived;
  Aggregate shock: probability λ showing up (indicated by $\mathbb{I}_t$).
- Three long-lived sellers: incumbents (A&B) authentic; entrant (C) authentic with prob π.
  Only authentic sellers deliver at cost μ.
- Quality of service $\mathbf{q} = (q_A, q_B, q_C)$ i.i.d. and public, $[\underline{q}, \overline{q}]$.
  Interpreted as probability of success, upon which buyers get unit utility.

Setup

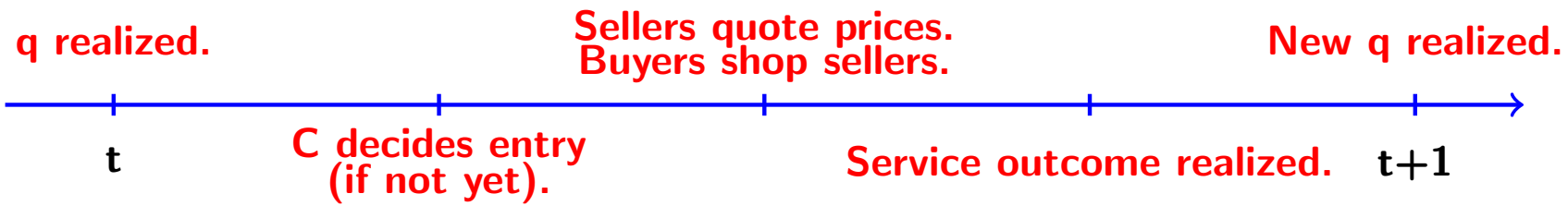
- Risk-neutral, discrete time $t = 1, 2, \cdots$.
- Buyers: unit measure, short-lived;
  Aggregate shock: probability λ showing up (indicated by $\mathbb{I}_t$).
- Three long-lived sellers: incumbents (A&B) authentic; entrant (C) authentic with prob π.
  Only authentic sellers deliver at cost μ.
- Quality of service $\mathbf{q} = (q_A, q_B, q_C)$ i.i.d. and public, $[\underline{q}, \overline{q}]$.
  Interpreted as probability of success, upon which buyers get unit utility.

Timeline and Assumption



Assumption 1: In traditional world, no payment can be contingent on whether service delivery occurs or not. Each seller can only observe his own buyers and associated transaction information.

Timeline and Assumption



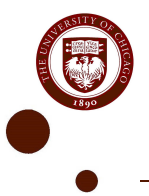
Assumption 1: In traditional world, no payment can be contingent on whether service delivery occurs or not. Each seller can only observe his own buyers and associated transaction information.

Reputation and Entry

Proposition

In a competitive equilibrium, the first time C can serve customers is in period $\tau \equiv \min\{t \geq 0 | \pi q_{C,t} \mathbb{I}_t \geq \max\{q_{A,t}, q_{B,t}\}\}$ *or later. Consequently, C never enters if* $\pi \overline{q} < \underline{q}$.

- Reputation π helps but entry still inefficient.
- We focus on $\underline{q} > \pi \overline{q}$. .

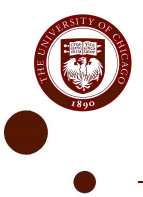


Collusive Equilibria

- Collusion (f, T): Green and Porter (1984); Friedman (1971)
- Collusion phase: $f(q_A, q_B)$, $p_A = q_A$, $p_B = q_B$
- Punishment phase: triggered by deviation or aggregate shock
  seeing no buyer (imperfect public monitoring), punish T periods.
- $M_1 = E[f(q)(q-k)]$, $M_2 = E[(q_i - \max_{j\neq i} q_j)^+]$, $M_3 = \max_q\{(1-f(q))(q-k)\}$, then

Proposition

The discount threshold $\delta_o^{Traditional} \equiv \inf_f \frac{1}{\lambda}\frac{M_3}{M_1+M_3-M_2}$ *is well-defined and positive. When* $\delta < \delta_o^{Traditional}$*, no collusion equilibrium exists for any* (T, f)*.*



Collusive Equilibria

- Collusion (f, T): Green and Porter (1984); Friedman (1971)
- Collusion phase: $f(q_A, q_B)$, $p_A = q_A$, $p_B = q_B$
- Punishment phase: triggered by deviation or aggregate shock
  seeing no buyer (imperfect public monitoring), punish T periods.
- $M_1 = E[f(q)(q-k)]$, $M_2 = E[(q_i - \max_{j\neq i} q_j)^+]$, $M_3 = \max_q\{(1-f(q))(q-k)\}$, then

Proposition

The discount threshold $\delta_o^{Traditional} \equiv \inf_f \frac{1}{\lambda}\frac{M_3}{M_1+M_3-M_2}$ *is well-defined and positive. When* $\delta < \delta_o^{Traditional}$*, no collusion equilibrium exists for any* (T, f)*.*

Blockchain World & Trust Machine

- **Assumption 2**: **New Informational Environment**
  The blockchain contacts all participants (including the sellers and the continuum of consumers) to generate effective decentralized consensus. More specifically, the blockchain consensus $\widetilde{z} = \widetilde{\omega}$ and a seller upon being contacted infers that customers are present.

Proposition

With smart contracts, the entrant C enters almost surely, and first gets customers in period
$\tau = \min\{t \geq 0 | q_{C,t}\mathbb{I}_t \geq \max\{q_{A,t}, q_{B,t}\}\}$ *or earlier.*

- Greater entry and competition:
  $\mathbb{E}[q^{(1)}] > \mathbb{E}[\max\{q_A, q_B\}]$.
- Welfare and consumer (buyer) surplus are higher.

Blockchain World & Trust Machine

- **Assumption 2**: **New Informational Environment**
  The blockchain contacts all participants (including the sellers and the continuum of consumers) to generate effective decentralized consensus. More specifically, the blockchain consensus $\widetilde{z} = \widetilde{\omega}$ and a seller upon being contacted infers that customers are present.

Proposition

With smart contracts, the entrant C enters almost surely, and first gets customers in period
$\tau = \min\{t \geq 0 | q_{C,t}\mathbb{I}_t \geq \max\{q_{A,t}, q_{B,t}\}\}$ *or earlier.*

- Greater entry and competition:
  $\mathbb{E}[q^{(1)}] > \mathbb{E}[\max\{q_A, q_B\}]$.
- Welfare and consumer (buyer) surplus are higher.

Trust-Machine for Collusion

- Explicit collusion using smart contract:
  - The same consensus and automated execution can help incumbents.
  - Punishment upon deviation
    $\rightarrow$ any collusion can be sustained.
- Likely prohibited by anti-trust laws.
- Greater public information on service activities.
- Based on the aggregate information, aggregate noise can be filtered out.
- Can more accurately punish deviations using continuation value.

Trust-Machine for Collusion

- Explicit collusion using smart contract:
  - The same consensus and automated execution can help incumbents.
  - Punishment upon deviation
    $\rightarrow$ any collusion can be sustained.
- Likely prohibited by anti-trust laws.
- Greater public information on service activities.
- Based on the aggregate information, aggregate noise can be filtered out.
- Can more accurately punish deviations using continuation value.

Trust-Machine for Collusion

- Explicit collusion using smart contract:
  - The same consensus and automated execution can help incumbents.
  - Punishment upon deviation
    $\rightarrow$ any collusion can be sustained.
- Likely prohibited by anti-trust laws.
- Greater public information on service activities.
- Based on the aggregate information, aggregate noise can be filtered out.
- Can more accurately punish deviations using continuation value.

Trust-Machine for Collusion

- Explicit collusion using smart contract:
  - The same consensus and automated execution can help incumbents.
  - Punishment upon deviation
    $\rightarrow$ any collusion can be sustained.
- Likely prohibited by anti-trust laws.
- Greater public information on service activities.
- Based on the aggregate information, aggregate noise can be filtered out.
- Can more accurately punish deviations using continuation value.

Trust-Machine for Collusion

- Explicit collusion using smart contract:
  - The same consensus and automated execution can help incumbents.
  - Punishment upon deviation
    $\rightarrow$ any collusion can be sustained.
- Likely prohibited by anti-trust laws.
- Greater public information on service activities.
- Based on the aggregate information, aggregate noise can be filtered out.
- Can more accurately punish deviations using continuation value.

Enhanced Tacit Collusion

- Tacit collusion with permissioned blockchain

Proposition

Compare the thresholds above which the specified collusion strategy is an equilibrium. We have

$$\delta^{Blockchain2}_{(T,f)} < \delta^{Traditional}_{(T,f)}$$

Corollary

When $\delta \in \left[\inf_f\{\delta^{Blockchain2}_{(\infty,f)}\}, \delta^{Traditional}_{o}\right)$*, there cannot be collusion without blockchain, but there could be with blockchain.*

Enhanced Tacit Collusion

- Tacit collusion with permissioned blockchain

Proposition

Compare the thresholds above which the specified collusion strategy is an equilibrium. We have

$$\delta_{(T,f)}^{Blockchain2} < \delta_{(T,f)}^{Traditional}$$

Corollary

When $\delta \in \left[\inf_f\{\delta_{(\infty,f)}^{Blockchain2}\}, \delta_o^{Traditional}\right)$*, there cannot be collusion without blockchain, but there could be with blockchain.*

Blockchain Disruption

- Public blockchain: entry and collusion
- Collusion phase: $\hat{f}(q_i, q_j, q_k)$ allocation function
- Punishment phase: no buyers conditional on buyers' presence.

Proposition

The discount threshold $\delta_o^{Blockchain3} \equiv \inf_{\hat{f}}\{\delta_{(\infty,\hat{f})}^{Blockchain3}\}$ *is well-defined and satisfies* $\delta_o^{Blockchain3} < 1$. *For all* $\delta > \delta_o^{Blockchain3}$, *there exists a collusion equilibrium with blockchain such that the consumer surplus is lower than that in any equilibrium in the traditional world.*

Blockchain Disruption

- Public blockchain: entry and collusion
- Collusion phase: $\hat{f}(q_i, q_j, q_k)$ allocation function
- Punishment phase: no buyers conditional on buyers' presence.

Proposition

The discount threshold $\delta_o^{Blockchain3} \equiv \inf_{\hat{f}}\{\delta_{(\infty,\hat{f})}^{Blockchain3}\}$ *is well-defined and satisfies* $\delta_o^{Blockchain3} < 1$. *For all* $\delta > \delta_o^{Blockchain3}$, *there exists a collusion equilibrium with blockchain such that the consumer surplus is lower than that in any equilibrium in the traditional world.*

Blockchain Disruption

Theorem

The discount threshold $\delta_a^{Blockchain3} \equiv \sup_f \{\delta_{(\infty,\hat{f})}^{Blockchain3}\}$ *is well-defined and satisfies* $\delta_a^{Blockchain3} < 1$. *For all* $\delta > \delta_a^{Blockchain3}$, *any consumer surplus and welfare attainable in the traditional world can be attained with blockchain, and some additional equilibria with higher or lower consumer surplus or welfare can also be sustained.*

Corollary

The most collusive equilibrium with blockchain, which generates the highest payoff to the sellers, improves social welfare but results in strictly lower consumer surplus, compared to any equilibrium outcome in the traditional world.

Blockchain Disruption

Theorem

The discount threshold $\delta_a^{Blockchain3} \equiv \sup_f \{\delta_{(\infty,\hat{f})}^{Blockchain3}\}$ *is well-defined and satisfies* $\delta_a^{Blockchain3} < 1$. *For all* $\delta > \delta_a^{Blockchain3}$, *any consumer surplus and welfare attainable in the traditional world can be attained with blockchain, and some additional equilibria with higher or lower consumer surplus or welfare can also be sustained.*

Corollary

The most collusive equilibrium with blockchain, which generates the highest payoff to the sellers, improves social welfare but results in strictly lower consumer surplus, compared to any equilibrium outcome in the traditional world.

Outline

- Introduction & Institutional Background
- Decentralized Consensus & Information Distribution
- Blockchain Disruption & Industrial Organization
- **Regulation & Discussion**
- Conclusion

Regulatory Measures

- Blockchain competition: a number of segmented blockchains.
- Regulatory node and design.
- Separation of keepers of users.
- Blockchain and smart contract design.

Regulatory Measures

- Blockchain competition: a number of segmented blockchains.
- Regulatory node and design.
- Separation of keepers of users.
- Blockchain and smart contract design.

Regulatory Measures

- Blockchain competition: a number of segmented blockchains.
- Regulatory node and design.
- Separation of keepers of users.
- Blockchain and smart contract design.

Regulatory Measures

- Blockchain competition: a number of segmented blockchains.
- Regulatory node and design.
- Separation of keepers of users.
- Blockchain and smart contract design.

Imperfect Consensus

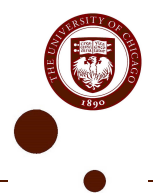
- With probability ψ the blockchain correctly records delivery outcome.
- Authentic type solves:

$$\max_{(p^s,p^f)} \quad \psi p^s + (1-\psi)p^f$$
$$s.t. \quad \psi p^s + (1-\psi)p^f \geq \mu, \quad -p^f \leq L,$$
$$and \quad (1-\psi)p^s + \psi p^f < 0,$$

Proposition

As long as the consensus quality is not too low ($\psi \geq \frac{\mu+L}{\mu+2L}$), the use of smart contract facilitates entry of the authentic type.

- Collusion and exclusion of sellers from recordkeeping.



Imperfect Consensus

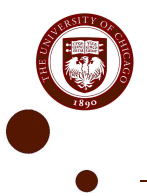
- With probability ψ the blockchain correctly records delivery outcome.
- Authentic type solves:

$$\max_{(p^s,p^f)} \quad \psi p^s + (1-\psi)p^f$$
$$s.t. \quad \psi p^s + (1-\psi)p^f \geq \mu, \quad -p^f \leq L,$$
$$and \quad (1-\psi)p^s + \psi p^f < 0,$$

Proposition

As long as the consensus quality is not too low ($\psi \geq \frac{\mu+L}{\mu+2L}$), the use of smart contract facilitates entry of the authentic type.

- Collusion and exclusion of sellers from recordkeeping.



Imperfect Consensus

- With probability ψ the blockchain correctly records delivery outcome.
- Authentic type solves:

$$\max_{(p^s,p^f)} \quad \psi p^s + (1-\psi)p^f$$
$$s.t. \quad \psi p^s + (1-\psi)p^f \geq \mu, \quad -p^f \leq L,$$
$$and \quad (1-\psi)p^s + \psi p^f < 0,$$

Proposition

As long as the consensus quality is not too low ($\psi \geq \frac{\mu+L}{\mu+2L}$), the use of smart contract facilitates entry of the authentic type.

- Collusion and exclusion of sellers from recordkeeping.

Imperfect Consensus

- With probability ψ the blockchain correctly records delivery outcome.
- Authentic type solves:

$$\max_{(p^s,p^f)} \quad \psi p^s + (1-\psi)p^f$$
$$s.t. \quad \psi p^s + (1-\psi)p^f \geq \mu, \quad -p^f \leq L,$$
$$and \quad (1-\psi)p^s + \psi p^f < 0,$$

Proposition

As long as the consensus quality is not too low ($\psi \geq \frac{\mu+L}{\mu+2L}$), the use of smart contract facilitates entry of the authentic type.

- Collusion and exclusion of sellers from recordkeeping.

Private Qualities and Allocative (In)efficiency

q is privately observed in addition to uncertain authenticity.

Lemma

In the traditional world, sellers will post the same price $p_i = u$, and the buyer will select (randomly) one of them for transaction need. The expected buyer's surplus and social welfare per period is $\mathbb{E}[q] - \mu$.

Private Qualities and Allocative (In)efficiency

q is privately observed in addition to uncertain authenticity.

Lemma

In the traditional world, sellers will post the same price $p_i = u$, and the buyer will select (randomly) one of them for transaction need. The expected buyer's surplus and social welfare per period is $\mathbb{E}[q] - \mu$.

Equilibrium Contracts and Economic Outcomes

Proposition

The smart contracts the sellers offer in equilibrium are all of the form $(p, p-1)$, where p is the price a buyer pays upon success, and $1-p$ is the compensation a buyer receives upon failure.

Corollary

Smart contracts fully resolve informational asymmetry in any market equilibrium, and welfare and consumer surplus are independent of whether seller qualities are private or not.

Welfare and consumer surplus improve.

Equilibrium Contracts and Economic Outcomes

Proposition

The smart contracts the sellers offer in equilibrium are all of the form $(p, p-1)$, where p is the price a buyer pays upon success, and $1-p$ is the compensation a buyer receives upon failure.

Corollary

Smart contracts fully resolve informational asymmetry in any market equilibrium, and welfare and consumer surplus are independent of whether seller qualities are private or not.

Welfare and consumer surplus improve.

Conclusion

- Blockchain and Smart Contract
  1. Decentralized consensus, low-cost, tamper-proof algorithmic execution.
  2. Greater information distribution and contractibility: Smart Contracts.
  3. Consensus generation: information distribution vs privacy.

- Economic impact on competition.
  1. Mitigates information asymmetry; facilitates entry and competition.
  2. More perfect monitoring; enhance collusion.
  3. Regulation; separation of users and keepers.

Conclusion

- Blockchain and Smart Contract
  1. Decentralized consensus, low-cost, tamper-proof algorithmic execution.
  2. Greater information distribution and contractibility: Smart Contracts.
  3. Consensus generation: information distribution vs privacy.
- Economic impact on competition.
  1. Mitigates information asymmetry; facilitates entry and competition.
  2. More perfect monitoring; enhance collusion.
  3. Regulation; separation of users and keepers.