Blockchain Disruption and Smart Contracts

Lin William Cong
University of Chicago

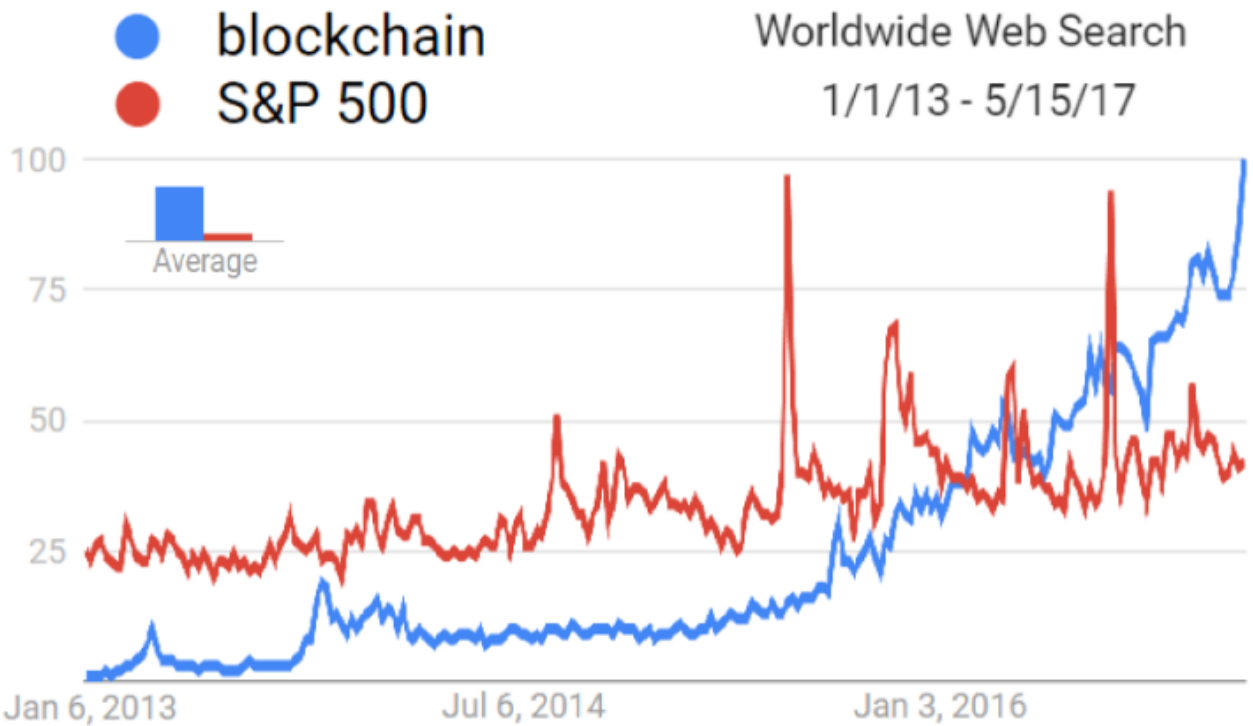
Zhiguo He
University of Chicago and NBER



October 6-7, 2017

Fifty Shades of Blockchain

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



Research Questions

- Economic activities, especially transactions, need tamper-proof consensus
  - Incomplete contracts; frauds; etc
- Unifying features of blockchain: **decentralized consensus** and **distributing information**.
- Economic impact of blockchain and smart contracts, especially on industrial organization and competition.
  - "...the technology really facilitates is *Cartel management* for groups that don't trust each other but which still need to work together....", *Financial Times*, May 2015



Research Questions

- Economic activities, especially transactions, need tamper-proof consensus
  - Incomplete contracts; frauds; etc
- Unifying features of blockchain: **decentralized consensus** and **distributing information**.
- Economic impact of blockchain and smart contracts, especially on industrial organization and competition.
  - "...the technology really facilitates is *Cartel management* for groups that don't trust each other but which still need to work together....", *Financial Times*, May 2015



Outline

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



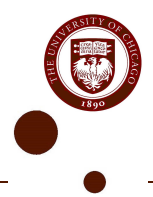
What is Blockchain?

- **Bitcoin** – the underlying blockchain technology
  - Dealing with double-spending of digital currency, distributed ledger.
- A database system in which parties unknown to each other jointly maintain and edit in a decentralized manner, with no individual party exercising central control.
- Decentralized consensus
  - Safe, robust, tamper-proof, & decentralized, that is essential to economic functions.
  - Getting rid of centralized authority (and its hefty rents).
- Distributing Information.
  - Record-keepers, incentives, organization & community.
  - Privacy, transparency, encryption, & informational environment.



What is Blockchain?

- **Bitcoin** – the underlying blockchain technology
  - Dealing with double-spending of digital currency, distributed ledger.
- A database system in which parties unknown to each other jointly maintain and edit in a decentralized manner, with no individual party exercising central control.
- Decentralized consensus
  - Safe, robust, tamper-proof, & decentralized, that is essential to economic functions.
  - Getting rid of centralized authority (and its hefty rents).
- Distributing Information.
  - Record-keepers, incentives, organization & community.
  - Privacy, transparency, encryption, & informational environment.



Two Key Questions

1. How to generate decentralized consensus?
   - Mechanism of decentralized consensus (not just mining games in **Bitcoin**).
   - Achieving it requires distributing information.

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



Smart Contracts

- *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 (at least according to our definition)?
  - Digital contracts with centralized authority; decentralized consnesus.
  - "smart" as in Artificial Intelligence; rather a robotic execution on blockchain.
  - Complete contracts; many contingencies still cannot be contracted upon.



Smart Contracts

- *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 (at least according to our definition)?
  - Digital contracts with centralized authority; decentralized consnesus.
  - "smart" as in Artificial Intelligence; rather a robotic execution on blockchain.
  - Complete contracts; many contingencies still cannot be contracted upon.



Applications of Blockchain and Smart Contracts in Finance

- Trusted payments: **Bitcoin, Lightning, Ripple, Ethereum, Phi, Corda,** etc.
- Trade finance: **R3 CEV, IBM, Wave, HK Blockchain, DTC,** etc.
  - in 2016, **Barclays** and **Wave**, first to complete a global trade transaction using blockchain technology.
  - Exporting almost US$100,000 worth of cheese and butter from Ireland to Seychelles, involving a blockchain-based letter of credit.
- Trading and exchanges: **Nasdaq Linq, Symbiont, NYIAX,** etc.



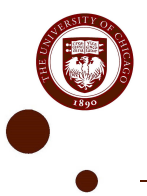
Outline

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



Keepers and Verification

- Validation nodes (**Ripple**/**R3**); Miners (**Bitcoin**/**Ethereum**); etc.
  - **Ripple**: An iterative consensus process, in which transactions are broadcast repeatedly across the network of validating nodes until an agreement is reached.
  - **Bitcoin**: All miners are record keepers (and compete to record transactions/blocks correctly).
- Public information, "oracles", private signals.
  - In the trade-finance application, various ports serve as "oracles" to feed information (about the goods location)
- Verification needs distributing information.
  - No news is news; encrypted data are data.



Keepers and Verification

- Validation nodes (**Ripple**/**R3**); Miners (**Bitcoin**/**Ethereum**); etc.
  - **Ripple**: An iterative consensus process, in which transactions are broadcast repeatedly across the network of validating nodes until an agreement is reached.
  - **Bitcoin**: All miners are record keepers (and compete to record transactions/blocks correctly).
- Public information, "oracles", private signals.
  - In the trade-finance application, various ports serve as "oracles" to feed information (about the goods location)
- Verification needs distributing information.
  - No news is news; encrypted data are data.



Keepers and Verification

- Validation nodes (**Ripple**/**R3**); Miners (**Bitcoin**/**Ethereum**); etc.
  - **Ripple**: An iterative consensus process, in which transactions are broadcast repeatedly across the network of validating nodes until an agreement is reached.
  - **Bitcoin**: All miners are record keepers (and compete to record transactions/blocks correctly).
- Public information, "oracles", private signals.
  - In the trade-finance application, various ports serve as "oracles" to feed information (about the goods location)
- Verification needs distributing information.
  - No news is news; encrypted data are data.



A Simple Model

- A stylized model of decentralized consensus to formulate the way of thinking.
- Contingent state $\tilde{\omega}$; consensus $\tilde{z}$; K keepers.
  - Effectiveness: $-Var\left(\widetilde{\omega}-\widetilde{z}\right)$
- Every keeper, upon contact, sends in report $\widetilde{y}_k$
- Consensus rule: $\widetilde{z}(\mathbf{y})=\frac{1}{K}\sum_k \widetilde{y}_k$.



Information and Keeper's Problem

- Info on blockchain: $\widetilde{x}_i = \widetilde{\omega} + \widetilde{\eta}_i$
- For each keeper, info upon contact: $\widetilde{x}_k = \widetilde{\omega} + \widetilde{\eta}_k$, $\sigma_K \leq \sigma_\eta$
- Potential misreporting to maximize

$$U(y_k; \mathbf{y}) = \widetilde{b}_k \cdot (\widetilde{z}(\mathbf{y}) - \widetilde{x}_k) - \frac{1}{2h}(y_k - \widetilde{x}_k)^2$$

  - Bias: $\widetilde{b}_k \equiv \widetilde{b} + \widetilde{\varepsilon}_k$; with variances σ_ε^2 and σ_b^2
  - $\widetilde{b}$ reflects one transaction party choosing validators; $\widetilde{\varepsilon}_k$ buyer-seller conflict

- Hence the report $\widetilde{y}_k = \widetilde{\omega} + \widetilde{\eta}_k + \frac{h}{K}\left(\widetilde{b} + \widetilde{\varepsilon}_k\right)$.



Information and Keeper's Problem

- Info on blockchain: $\widetilde{x}_i = \widetilde{\omega} + \widetilde{\eta}_i$
- For each keeper, info upon contact: $\widetilde{x}_k = \widetilde{\omega} + \widetilde{\eta}_k$, $\sigma_K \leq \sigma_\eta$
- Potential misreporting to maximize

$$U(y_k; \mathbf{y}) = \widetilde{b}_k \cdot (\widetilde{z}(\mathbf{y}) - \widetilde{x}_k) - \frac{1}{2h}(y_k - \widetilde{x}_k)^2$$

  - Bias: $\widetilde{b}_k \equiv \widetilde{b} + \widetilde{\varepsilon}_k$; with variances σ_ε^2 and σ_b^2
  - $\widetilde{b}$ reflects one transaction party choosing validators; $\widetilde{\varepsilon}_k$ buyer-seller conflict

- Hence the report $\widetilde{y}_k = \widetilde{\omega} + \widetilde{\eta}_k + \frac{h}{K}\left(\widetilde{b} + \widetilde{\varepsilon}_k\right)$.



Information and Keeper's Problem

- Info on blockchain: $\widetilde{x}_i = \widetilde{\omega} + \widetilde{\eta}_i$
- For each keeper, info upon contact: $\widetilde{x}_k = \widetilde{\omega} + \widetilde{\eta}_k$, $\sigma_K \leq \sigma_\eta$
- Potential misreporting to maximize

$$U(y_k; \mathbf{y}) = \widetilde{b}_k \cdot (\widetilde{z}(\mathbf{y}) - \widetilde{x}_k) - \frac{1}{2h}(y_k - \widetilde{x}_k)^2$$

  - Bias: $\widetilde{b}_k \equiv \widetilde{b} + \widetilde{\varepsilon}_k$; with variances σ_ε^2 and σ_b^2
  - $\widetilde{b}$ reflects one transaction party choosing validators; $\widetilde{\varepsilon}_k$ buyer-seller conflict

- Hence the report $\widetilde{y}_k = \widetilde{\omega} + \widetilde{\eta}_k + \frac{h}{K}\left(\widetilde{b} + \widetilde{\varepsilon}_k\right)$.



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

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

- The greater the K, the more effective the consensus.
  - In many real world applications (as well as in later IO model): $\widetilde{z} \approx \widetilde{\omega}$, as $K \to \infty$.
- $K \to \infty$ implies to contact infinitely many keepers on the blockchain (and mere contact can be information).



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.
- Three long-lived sellers: incumbents (A&B) authentic; entrant (C) authentic with prob π.
  - Only authentic sellers can deliver at some small cost μ.
- Quality of service $\mathbf{q} = (q_A, q_B, q_C)$ i.i.d. and public info, $[\underline{q}, \overline{q}]$.
  - Interpreted as probability of success, upon which buyers get unit utility.
  - Charging prices q_i's $\Rightarrow$ no surplus to customers.
- **Aggregate shock**: with probability λ buyers showing up (indicated by $\mathbb{I}_t$).

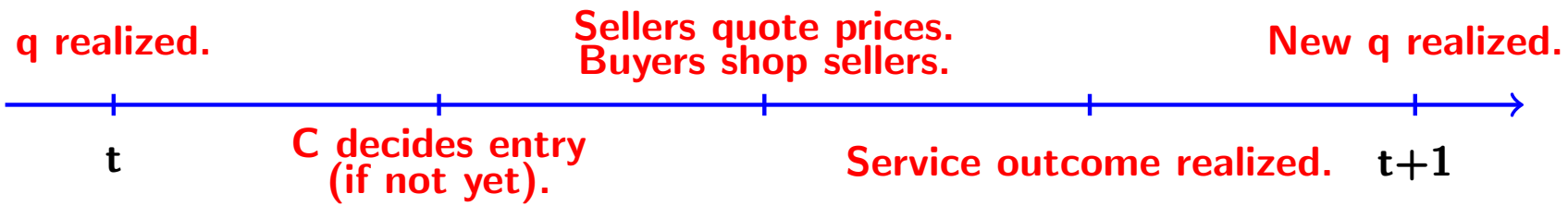


Setup

- Risk-neutral, discrete time $t = 1, 2, \cdots$.
- Buyers: unit measure, short-lived.
- Three long-lived sellers: incumbents (A&B) authentic; entrant (C) authentic with prob π.
  - Only authentic sellers can deliver at some small cost μ.
- Quality of service $\mathbf{q} = (q_A, q_B, q_C)$ i.i.d. and public info, $[\underline{q}, \overline{q}]$.
  - Interpreted as probability of success, upon which buyers get unit utility.
  - Charging prices q_i's $\Rightarrow$ no surplus to customers.
- **Aggregate shock**: with probability λ buyers showing up (indicated by $\mathbb{I}_t$).



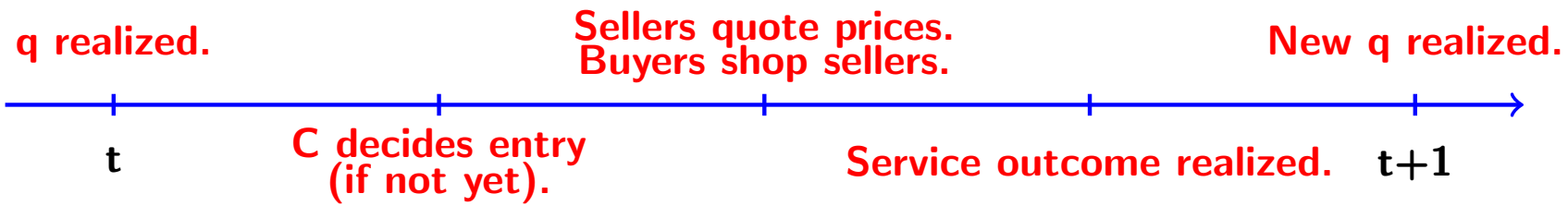
Timeline and Assumption



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* $\pi < \underline{q}/\overline{q}$.

- Reputation π helps but entry still inefficient.
- We focus on the low reputation case $\pi < \underline{q}/\overline{q}$.
  - Will see later smart contracts helps.
- Two incumbents, competitive equilibrium. Say $q_A > q_B$; then A gets all buyers by charging a price $q_A - q_B + \mu$ (B is charging μ).



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* $\pi < \underline{q}/\overline{q}$.

- Reputation π helps but entry still inefficient.
- We focus on the low reputation case $\pi < \underline{q}/\overline{q}$.
  - Will see later smart contracts helps.
- Two incumbents, competitive equilibrium. Say $q_A > q_B$; then A gets all buyers by charging a price $q_A - q_B + \mu$ (B is charging μ).



Collusive Equilibria

- Collusion: Friedman (1971); Green & Porter (1984)
  1. **Collusion** phase: $p_A = q_A$, $p_B = q_B$ so charge full prices; $f(q_A, q_B)$ allocation
  2. **Punishment** phase: triggered by privately observing no buyers, competitive for T periods.
- Repeated game with imperfect public monitoring.
  - Bertrand competition for financial services instead of Cournot.
  - Private observations equivalent to (imperfect) public monitoring.
  - **Imperfect**: cannot distinguish opponent's deviation or aggregate shock (no buyers with prob $1 - \lambda$).

Proposition

Exists discount threshold $\delta_o^{Traditional} < 1$ such that when $\delta < \delta_o^{Traditional}$, no collusion equilibrium exists for any (T, f).



Collusive Equilibria

- Collusion: Friedman (1971); Green & Porter (1984)
  1. **Collusion** phase: $p_A = q_A$, $p_B = q_B$ so charge full prices; $f(q_A, q_B)$ allocation
  2. **Punishment** phase: triggered by privately observing no buyers, competitive for T periods.
- Repeated game with imperfect public monitoring.
  - Bertrand competition for financial services instead of Cournot.
  - Private observations equivalent to (imperfect) public monitoring.
  - **Imperfect**: cannot distinguish opponent's deviation or aggregate shock (no buyers with prob $1 - \lambda$).

Proposition

Exists discount threshold $\delta_o^{Traditional} < 1$ such that when $\delta < \delta_o^{Traditional}$, no collusion equilibrium exists for any (T, f).



Collusive Equilibria

- Collusion: Friedman (1971); Green & Porter (1984)
  1. **Collusion** phase: $p_A = q_A$, $p_B = q_B$ so charge full prices; $f(q_A, q_B)$ allocation
  2. **Punishment** phase: triggered by privately observing no buyers, competitive for T periods.
- Repeated game with imperfect public monitoring.
  - Bertrand competition for financial services instead of Cournot.
  - Private observations equivalent to (imperfect) public monitoring.
  - **Imperfect**: cannot distinguish opponent's deviation or aggregate shock (no buyers with prob $1 - \lambda$).

Proposition

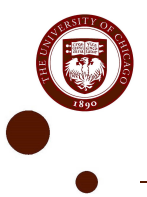
Exists discount threshold $\delta_o^{Traditional} < 1$ *such that when* $\delta < \delta_o^{Traditional}$, *no collusion equilibrium exists for any* (T, f).



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.

- **Ripple**: transactions (not the details of transactions) are broadcast "iteratively" for verification; so aggregate service activities become public information.



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.

- **Ripple**: transactions (not the details of transactions) are broadcast "iteratively" for verification; so aggregate service activities become public information.



Smart Contracts and Enhanced Entry

- Smart contracts in the form of (p^s, p^f) contingent on service delivery becomes available.
- Only the authentic entrant C enters by setting $p^f = -\epsilon$ (i.e., penalty given failure).

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, thanks to decentralized consensus and smart contracts.
- Welfare and consumer (buyer) surplus are higher.



Trust-Machine for Collusion: Explicit Collusion

- Explicit collusion using smart contracts:
  - The same automated execution on certain outcome (with decentralized consensus) can help incumbents.
  - Automatic punishment upon deviation $\rightarrow$ any collusion can be sustained.
- Likely prohibited by anti-trust laws. And easy to detect and enforce.



Trust-Machine for Collusion: Explicit Collusion

- Explicit collusion using smart contracts:
  - The same automated execution on certain outcome (with decentralized consensus) can help incumbents.
  - Automatic punishment upon deviation $\rightarrow$ any collusion can be sustained.
- Likely prohibited by anti-trust laws. And easy to detect and enforce.



Trust-Machine for Collusion: Explicit Collusion

- Explicit collusion using smart contracts:
  - The same automated execution on certain outcome (with decentralized consensus) can help incumbents.
  - Automatic punishment upon deviation $\rightarrow$ any collusion can be sustained.
- Likely prohibited by anti-trust laws. And easy to detect and enforce.



Trust-Machine for Collusion: Tacit Collusion

- Another less explicit but perhaps more profound way to generate hotbed for collusion
- There is greater public information in the economy.
  - In the model, more public information on aggregate service activities.
- Based on the aggregate information, aggregate noises are more likely to be filtered out
  - In the model, public monitoring turns from imperfect to perfect!
- Accurate punishment of deviations becomes more likely.



Trust-Machine for Collusion: Tacit Collusion

- Another less explicit but perhaps more profound way to generate hotbed for collusion
- There is greater public information in the economy.
  - In the model, more public information on aggregate service activities.
- Based on the aggregate information, aggregate noises are more likely to be filtered out
  - In the model, public monitoring turns from imperfect to perfect!
- Accurate punishment of deviations becomes more likely.



Enhanced Tacit Collusion

- Tacit collusion with permissioned blockchain

Proposition

With blockchain, the minimum discount factor to support a collusive equilibrium becomes lower.

Corollary

For a non-trivial range of discount factors, there is no collusion in the traditional world, but could be with blockchain.



Enhanced Tacit Collusion

- Tacit collusion with permissioned blockchain

Proposition

With blockchain, the minimum discount factor to support a collusive equilibrium becomes lower.

Corollary

For a non-trivial range of discount factors, there is no collusion in the traditional world, but could be with blockchain.



Blockchain Disruption

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

Proposition

Exists discount threshold $\delta_o^{Blockchain3} < 1$ such that for all $\delta > \delta_o^{Blockchain3}$, there exists a collusion equilibrium with blockchain resulting in a consumer surplus lower than that in any equilibrium in the traditional world.



Blockchain Disruption

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

Proposition

Exists discount threshold $\delta_o^{Blockchain3} < 1$ *such that for all* $\delta > \delta_o^{Blockchain3}$*, there exists a collusion equilibrium with blockchain resulting in a consumer surplus lower than that in any equilibrium in the traditional world.*



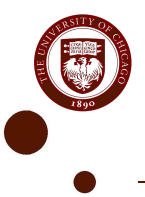
Blockchain Disruption

Theorem

Exists discount threshold $\delta_a^{Blockchain3} < 1$ such that 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

Exists discount threshold $\delta_a^{Blockchain3} < 1$ *such that 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

- Competition among a number of segmented blockchains may mitigate the concern of collusion, as consumers vote by feet.
  - Likely, only few blockchains survive due to network effect
  - What prevent blockchains from collusion?

- Regulatory node and design.
  - Real-time and tamper-proof records on blockchain should help regulators in monitoring collusion-prone behaviors
  - Reserve access to certain encrypted information.

- Separation of keepers from users.
  - Seems to be easiest solution...
  - In **Symbiont**, keepers tend to be a rather separate group from the end users.



Regulatory Measures

- Competition among a number of segmented blockchains may mitigate the concern of collusion, as consumers vote by feet.
  - Likely, only few blockchains survive due to network effect
  - What prevent blockchains from collusion?

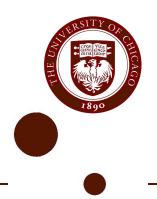
- Regulatory node and design.
  - Real-time and tamper-proof records on blockchain should help regulators in monitoring collusion-prone behaviors
  - Reserve access to certain encrypted information.

- Separation of keepers from users.
  - Seems to be easiest solution...
  - In **Symbiont**, keepers tend to be a rather separate group from the end users.



Regulatory Measures

- Competition among a number of segmented blockchains may mitigate the concern of collusion, as consumers vote by feet.
  - Likely, only few blockchains survive due to network effect
  - What prevent blockchains from collusion?
- Regulatory node and design.
  - Real-time and tamper-proof records on blockchain should help regulators in monitoring collusion-prone behaviors
  - Reserve access to certain encrypted information.
- Separation of keepers from users.
  - Seems to be easiest solution...
  - In **Symbiont**, keepers tend to be a rather separate group from the end users.



Imperfect Consensus

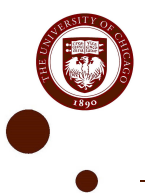
- With probability ψ the blockchain correctly records delivery outcome.
- Authentic type solves:

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

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.

- Still fosters collusion. A better way is to exclude sellers from recordkeeping.



Imperfect Consensus

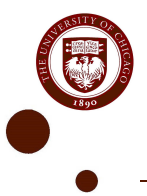
- With probability ψ the blockchain correctly records delivery outcome.
- Authentic type solves:

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

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.

- Still fosters collusion. A better way is to exclude sellers from recordkeeping.



Imperfect Consensus

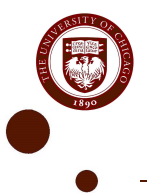
- With probability ψ the blockchain correctly records delivery outcome.
- Authentic type solves:

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

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.

- Still fosters collusion. A better way is to exclude sellers from recordkeeping.



Imperfect Consensus

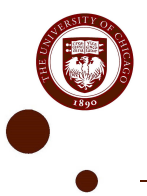
- With probability ψ the blockchain correctly records delivery outcome.
- Authentic type solves:

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

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.

- Still fosters collusion. A better way is to exclude sellers from recordkeeping.



Private Qualities and Allocative (In)efficiency

- $\mathbf{q}$ is privately observed in addition to uncertain authenticity.
- Show that the main economic take-away, i.e., blockchain as a double-edged sword, holds generally.



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: distributing information vs privacy.

- Economic impact on Industrial Organization and 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: distributing information vs privacy.
- Economic impact on Industrial Organization and Competition.
  1. Mitigates information asymmetry; facilitates entry and competition.
  2. More perfect monitoring; enhance collusion.
  3. Regulation; separation of users and keepers.

