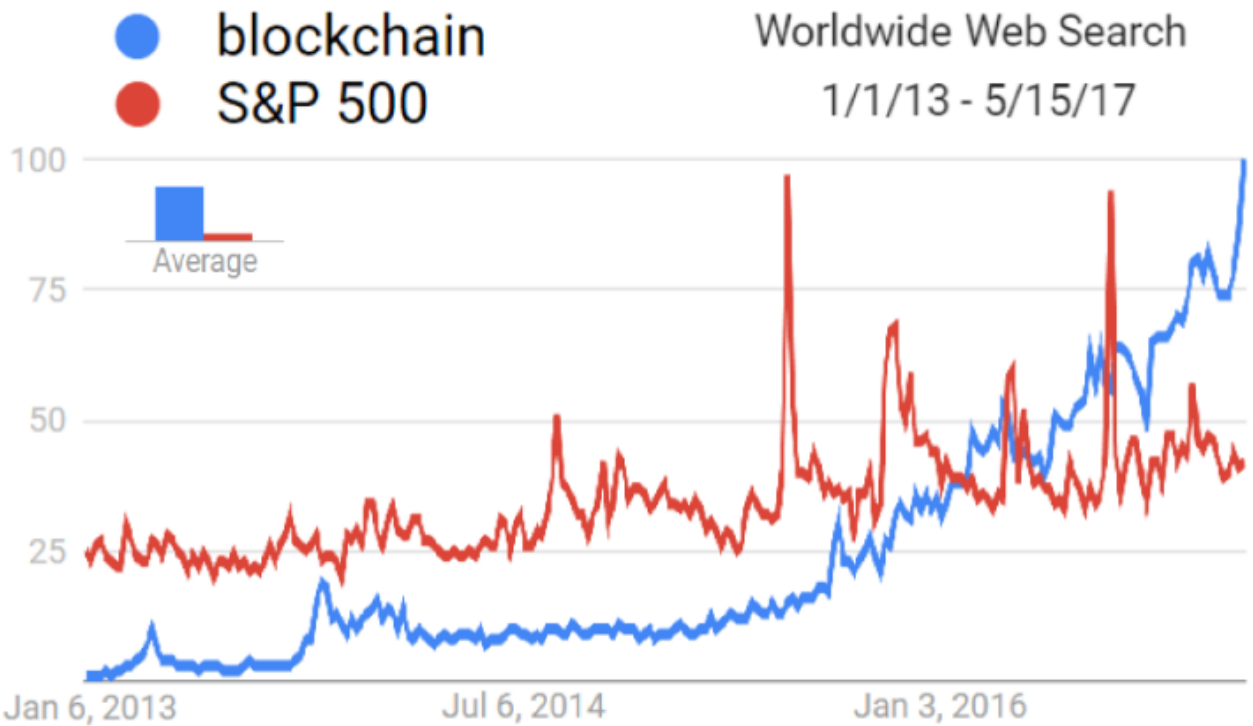
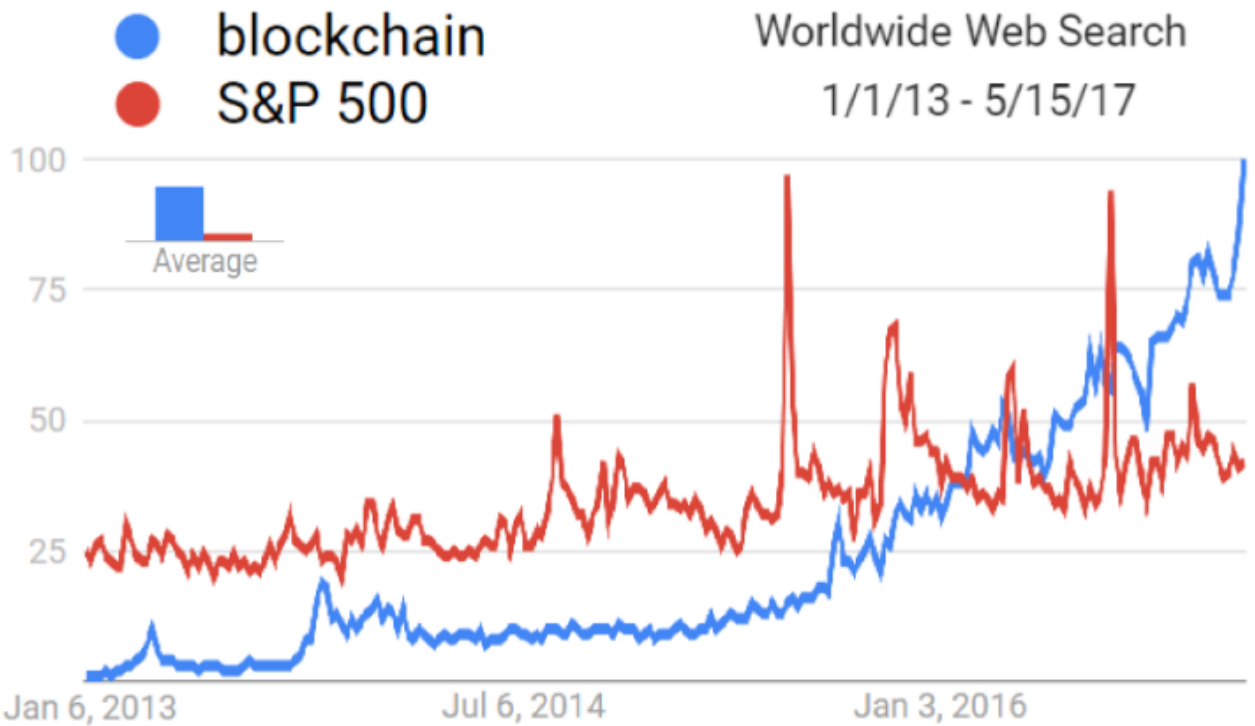
Fifty Shades of Blockchain

"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 and sharper definitions of blockchain and smart contracts.
- Economic impact of blockchain, especially on competition.

Research Questions

- Unifying features and sharper definitions of blockchain and smart contracts.
- Economic impact of blockchain, especially on competition.

What is Blockchain?

- Bitcoin – the original blockchain
  - Double-spending, public distributed ledger
  - Blockchain not defined by Bitcoin.

- 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.

- Cheaply maintain a robust consensus.
  - Decentralized: no need to trust or rely on a centralized authority.
  - A community to maintain consensus.

What is Blockchain?

- Bitcoin – the original blockchain
  - Double-spending, public distributed ledger
  - Blockchain not defined by Bitcoin.

- 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.

- Cheaply maintain a robust consensus.
  - Decentralized: no need to trust or rely on a centralized authority.
  - A community to maintain consensus.

What is Blockchain?

- Bitcoin – the original blockchain
  - Double-spending, public distributed ledger
  - Blockchain not defined by Bitcoin.
- 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.
- Cheaply maintain a robust consensus.
  - Decentralized: no need to trust or rely on a centralized authority.
  - A community to maintain consensus.

What is Blockchain?

- Bitcoin – the original blockchain
  - Double-spending, public distributed ledger
  - Blockchain not defined by Bitcoin.
- 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.
- Cheaply maintain a robust consensus.
  - Decentralized: no need to trust or rely on a centralized authority.
  - A community to maintain consensus.

Two Important Questions

1. 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, ...
   - Achieving decentralized consensus requires distribution of information.

2. What are the economic implications of decentralized consensus?
   - Greater contractibility: rise of smart contracts
   - Greater public information: information economics, repeated games with monitoring....

Two Important Questions

1. 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, ...
   - Achieving decentralized consensus requires distribution of information.

2. What are the economic implications of decentralized consensus?
   - Greater contractibility: rise of smart contracts
   - Greater public information: information economics, repeated games with monitoring....

Two Important Questions

1. 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, ...
   - Achieving decentralized consensus requires distribution of information.

2. What are the economic implications of decentralized consensus?
   - Greater contractibility: rise of smart contracts
   - Greater public information: information economics, repeated games with monitoring....

What is Smart Contract?

- *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?
  - Merely digital contracts.
  - Centralized authority or consensus.
  - Primarily human-intermediated execution
  - Truly smart (AI).
  - Complete contract.

Fundamental Tension and Applications

- Information in Decentralized Consensus
  - Micro: privacy; Macro: more public information.
  - Verification; Zero-knowledge Proof.
  - No news is news; encrypted data are information.
- Applications
  - Payments: Lightning, Ripple, Phi, etc.
  - Trade Finance: R3 CEV, IBM, Wave, DTC.
  - Trading and exchanges: Nasdaq Linq, Symbiont, NYIAX, etc.

Fundamental Tension and Applications

- Information in Decentralized Consensus
  - Micro: privacy; Macro: more public information.
  - Verification; Zero-knowledge Proof.
  - No news is news; encrypted data are information.
- Applications
  - Payments: Lightning, Ripple, Phi, etc.
  - Trade Finance: R3 CEV, IBM, Wave, DTC.
  - Trading and exchanges: Nasdaq Linq, Symbiont, NYIAX, etc.

Fundamental Tension and Applications

- Information in Decentralized Consensus
  - Micro: privacy; Macro: more public information.
  - Verification; Zero-knowledge Proof.
  - No news is news; encrypted data are information.
- Applications
  - Payments: Lightning, Ripple, Phi, etc.
  - Trade Finance: R3 CEV, IBM, Wave, DTC.
  - Trading and exchanges: Nasdaq Linq, Symbiont, NYIAX, etc.

Fundamental Tension and Applications

- Information in Decentralized Consensus
  - Micro: privacy; Macro: more public information.
  - Verification; Zero-knowledge Proof.
  - No news is news; encrypted data are information.
- Applications
  - Payments: Lightning, Ripple, Phi, etc.
  - Trade Finance: R3 CEV, IBM, Wave, DTC.
  - Trading and exchanges: Nasdaq Linq, Symbiont, NYIAX, etc.

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.
- 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.
- Service production cost k.

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.
- 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.
- Service production cost k.

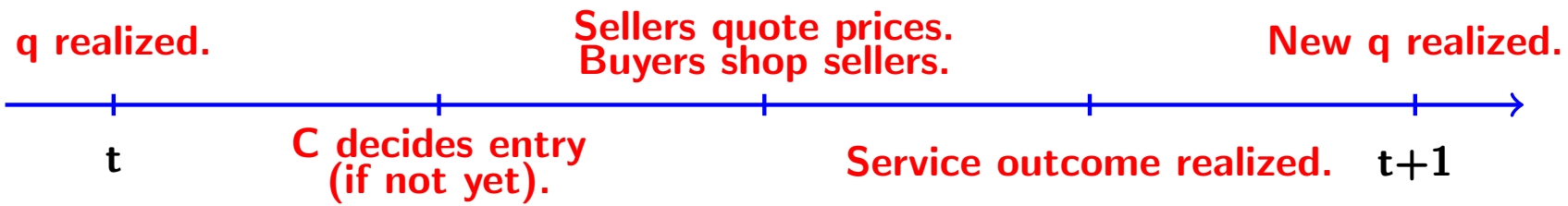
Setup

- 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.
- 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.
- Service production cost k.

Setup

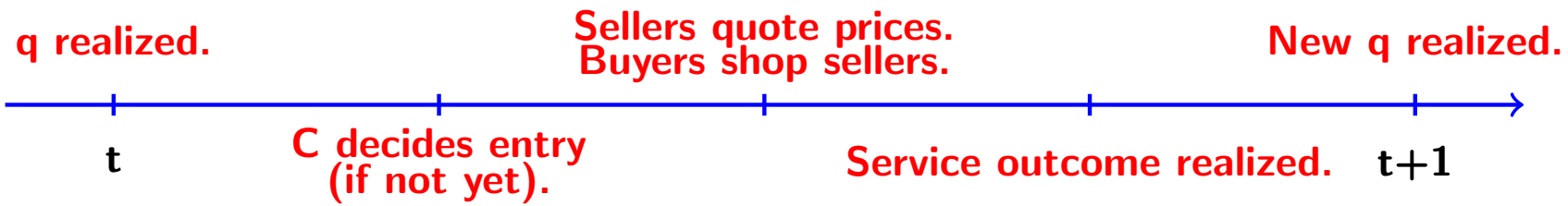
- Risk-neutral, discrete time $t = 1, 2, \cdots$.
- Buyers: unit measure, short-lived;
  Aggregate shock: probability λ showing up (indicated by $\mathbb{I}_t$).
- Three long-lived sellers: incumbents (A&B) authentic; entrant (C) authentic with prob π.
  Only authentic sellers deliver.
- Quality of service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

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



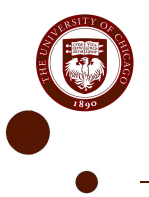
Assumption 1: In traditional world, no payment can be contingent on whether service delivery occurs or not. Each seller can only observe his own buyers and associated transaction information.

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)*.*

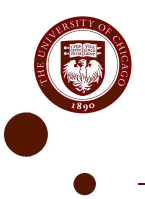
The Trust Machine

- **Assumption 2**: **New Informational Environment** Blockchain enables decentralized consensus, and buyers and sellers can write smart contracts that are contingent on the service outcome associated with their own transaction. In order to reach decentralized consensus, aggregate service activities are publicly observable on blockchain.

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.



The Trust Machine

- **Assumption 2**: **New Informational Environment** Blockchain enables decentralized consensus, and buyers and sellers can write smart contracts that are contingent on the service outcome associated with their own transaction. In order to reach decentralized consensus, aggregate service activities are publicly observable on blockchain.

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

- 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

- 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

- 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

- 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

- 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 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.*

Enhanced 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

Proposition

For $m \geq n \geq 2$, if $\lambda < \frac{n-1}{n}$, then $\delta_o^{Traditional,n} > \delta_o^{Blockchain,m}$, where m and n indicate the number of colluding sellers with and without blockchain respectively. Consequently for all $\delta \in [\delta_o^{Blockchain,m}, 1)$, there is no collusion in the traditional world with n incumbents, while there can be collusion with blockchain with m sellers that reduces consumer surplus.

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.

Private Qualities and Allocative Inefficiency

q is privately observed in addition to uncertain authenticity.

Lemma

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

Private Qualities and Allocative Inefficiency

q is privately observed in addition to uncertain authenticity.

Lemma

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

Equilibrium Contracts and Economic Outcomes

q is privately observed in addition to uncertain authenticity.

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

q is privately observed in addition to uncertain authenticity.

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.

Regulation and Blockchain Competition

- Noise injection on service activities.
- Making monitoring more imperfect.

- Blockchain competition: a number of segmented blockchains
- No customer if offering collusive price.
- Only tacit collusion across platforms.

Regulation and Blockchain Competition

- Noise injection on service activities.
- Making monitoring more imperfect.

- Blockchain competition: a number of segmented blockchains
- No customer if offering collusive price.
- Only tacit collusion across platforms.

Smart Contract Design

- Improving consumer surplus conditional on maximizing welfare.
- Smart contract design: $p^f = 0$.
- General Symmetric Mechanism design
- Optimal smart contract and market mechanism implements the optimal mechanism.

Smart Contract Design

- Improving consumer surplus conditional on maximizing welfare.
- Smart contract design: $p^f = 0$.
- General Symmetric Mechanism design
- Optimal smart contract and market mechanism implements the optimal mechanism.

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 and smart contract design

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 and smart contract design