

# Cryptocurrencies and Blockchains

Eric Budish

University of Chicago, Booth School of Business

Clark Center Finance Experts Panel Conference  
October 3-4, 2024

# “Trust at Scale: The Economic Limits of Cryptocurrencies and Blockchains”

Eric Budish

*Quarterly Journal of Economics*, Forthcoming

# Nakamoto's Invention

- ▶ Economists have long widely agreed that the market system requires some form of government and rule of law for support
- ▶ Uncontroversial among even the most free-market oriented thinkers
  - ▶ Smith (1776): “Commerce and manufactures can seldom flourish long in any state” without a legal system, property rights and contract enforcement.
  - ▶ Hayek (1960): to maximize freedom, defined as absence of coercion, it is necessary to have a government with the power to coerce
  - ▶ Friedman (1962): government sets “rules of the game” and serves as “umpire”

## Nakamoto's Invention

- ▶ Core scientific innovation behind cryptocurrencies and blockchains is what computer science calls “permissionless consensus”
  - ▶ Create consensus on the state of a dataset
  - ▶ Without the need for any trusted party or support from rule of law
- ▶ Trust arises from a combination of cryptography and economic incentives, instead of traditional sources (law, and also reputation, relationships, collateral, etc.)
  - ▶ All anonymous, decentralized: large, freely-entering and -exiting set of participants collectively maintains the trust
  - ▶ (“a new territory of freedom,” “outside the reach of any government”)
- ▶ For a currency: a trusted dataset can keep track of currency balances (Bitcoin)
- ▶ More generally: easy to imagine other potential use cases for a trusted public database (“computer in the sky”, Ethereum)

## Adam Smith vs. Satoshi Nakamoto

- ▶ I show that Nakamoto's novel form of trust, while clearly ingenious, is seriously economically limited

## Adam Smith vs. Satoshi Nakamoto

- ▶ I show that Nakamoto's novel form of trust, while clearly ingenious, is seriously economically limited
- ▶ Achilles' heel of permissionless consensus: vulnerability to majority attack
  - ▶ Many hear the phrase "cryptography" and assume that blockchain data is secure
  - ▶ But really you should think of blockchain data as secured by a combination of cryptography and a majority vote by the decentralized participants
  - ▶ This is true for all forms of permissionless consensus: proof of work, stake, etc.
- ▶ Computer science has understood this vulnerability since the 1980s
  - ▶ And it's literally in the abstract of the Nakamoto (2008) paper

# Adam Smith vs. Satoshi Nakamoto

- ▶ I show that Nakamoto's novel form of trust, while clearly ingenious, is seriously economically limited
- ▶ Achilles' heel of permissionless consensus: vulnerability to majority attack
  - ▶ Many hear the phrase "cryptography" and assume that blockchain data is secure
  - ▶ But really you should think of blockchain data as secured by a combination of cryptography and a majority vote by the decentralized participants
  - ▶ This is true for all forms of permissionless consensus: proof of work, stake, etc.
- ▶ Computer science has understood this vulnerability since the 1980s
  - ▶ And it's literally in the abstract of the Nakamoto (2008) paper
- ▶ My approach: model this vulnerability to majority attack as an incentive compatibility constraint
  - ▶ This in turn allows for eqm reasoning: if permissionless consensus were to become more economically useful, then it will get more expensive to secure against attack
  - ▶ Costs quickly grow absurd: more than global GDP in some scenarios

## Nakamoto Trust: Three-Equation Critique

**Free-Entry Condition on Blockchain “Trust Support” (Work, Stake, etc.)**

$$N^* c = p_{block} \quad (1)$$

**Incentive Compatibility Condition (Majority Attack)**

$$A^* N^* c \cdot t(A^*) > V_{attack} \quad (2)$$

**Equilibrium Constraint**

$$p_{block} > \frac{V_{attack}}{A^* \cdot t(A^*)} \quad (3)$$

*In words: the equilibrium per-block payment to honest participants for providing trust support (“flow cost of trust”) must be large relative to the value of an attack*

## Remarks on the Equilibrium Constraint

$$p_{block} > \frac{V_{attack}}{A^* \cdot t(A^*)} \quad (3)$$

- ▶ Economics: *very expensive* form of trust.
  - ▶ Imagine if users of the Visa network had to pay fees to Visa, every ten minutes, that were large relative to the value of a successful one-off attack on the Visa network.
  - ▶ Imagine a brand only as trustworthy as its flow investment in advertising.
  - ▶ Imagine a country only as secure as its flow expenditure on soldiers at the border.
  - ▶ Base case analysis: it takes all of global GDP to secure against  $V_{attack}$  of \$40Bn.
- ▶ Computer Security: security is *linear* in amount of blockchain trust support.
  - ▶ Example: a \$1B attack is 1000x more expensive to prevent than a \$1M attack.
  - ▶ Usual alternatives: cryptography, laws. Convex returns
  - ▶ Imagine a company only as secure as the \$ value of its cpu power.

## Graphic Novel Version of the Argument



## Traditional Trust



# Traditional Trust



# Traditional Trust



Traditional Trust Model:

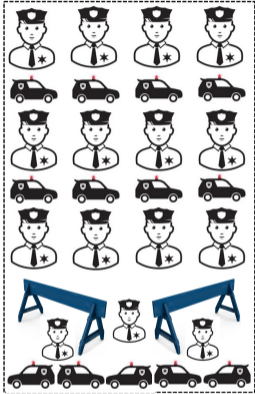
# Traditional Trust



Traditional Trust Model:

- ▶ Security Guards

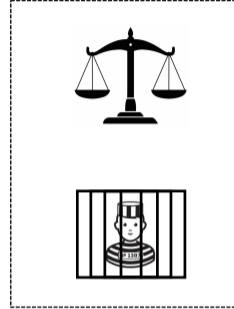
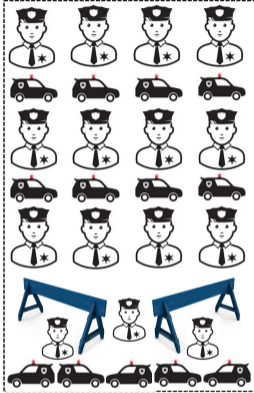
# Traditional Trust



Traditional Trust Model:

- ▶ Security Guards
- ▶ Police Reinforcements

# Traditional Trust



## Traditional Trust Model:

- ▶ Security Guards
- ▶ Police Reinforcements
- ▶ Punishment via Rule of Law

## Nakamoto Trust (Permissionless Consensus)



## Nakamoto Trust (Permissionless Consensus)



# Nakamoto Trust (Permissionless Consensus)



# Nakamoto Trust (Permissionless Consensus)



Nakamoto Trust Model:

# Nakamoto Trust (Permissionless Consensus)



Nakamoto Trust Model:

- ▶ Large amount of Security Guards

# Nakamoto Trust (Permissionless Consensus)



Nakamoto Trust Model:

- ▶ Large amount of Security Guards
- ▶ But no additional layers (Police, Rule of Law)

# Nakamoto Trust (Permissionless Consensus)



## Nakamoto Trust Model:

- ▶ Large amount of Security Guards
- ▶ But no additional layers (Police, Rule of Law)
- ▶ So, guards alone must deter attack

# Comparison of Trust Models

	Cost to Break Trust	Variable Cost of Honest Play	Fixed Cost Investments that Support Honest Play
Nakamoto Trust in its original form (Nakamoto, 2008)	Flow. Attacker pays cost of honest trust support $p_{block} = N^*c$ for a short period of time.	$p_{block}$ per period.	–
Repeated Interaction (Schelling, 1956; Aumann, 1959)	Stock. Attacker loses the net present value of the trust relationship $V_{trust} = \frac{1}{1-\delta}\tau$ .	0, given pre-existing trust relationship.	Investment in trust relationship, brand, reputation.
Credible Deterrence (Hayek, 1960; Becker, 1968)	Arbitrarily high up to value of life and assets. Attacker can be punished by the state.	“Security guards” in Figure 1. Variable costs of monitoring and enforcement associated with specific locations or transactions.	Investment in government and legal system.
Collateral	Stock + Punishment. Attacker loses the value of their collateral plus any additional punishment.	0, under conditions of Modigliani-Miller theorem. Requires legal enforcement mechanism which entails fixed costs.	Collateral value.
Nakamoto with Collapse	Stock. Attacker loses specialized capital worth $N^*C$ .	$p_{block}$ per period.	ASICs or other specialized computational equipment.
Proof-of-Stake in its original form	Flow. Attacker pays opportunity cost of capital $p_{block} = N^*c$ for a short period of time.	$p_{block}$ per period.	Cryptocurrency stake.
Proof-of-Stake with Slashing (Idealized)	Stock. Attacker loses specialized capital worth $N^*C$ .	$p_{block}$ per period.	Cryptocurrency stake.

# Comparison of Trust Models

	Cost to Break Trust	Variable Cost of Honest Play	Fixed Cost Investments that Support Honest Play
Nakamoto Trust in its original form (Nakamoto, 2008)	Flow. Attacker pays cost of honest trust support $p_{block} = N * c$ for a short period of time.	$p_{block}$ per period.	–
Repeated Interaction (Schelling, 1956; Aumann, 1959)	Stock. Attacker loses the net present value of the trust relationship $V_{trust} = \frac{1}{1-\delta} \tau$ .	0, given pre-existing trust relationship.	Investment in trust relationship, brand, reputation.
Credible Deterrence (Hayek, 1960; Becker, 1968)	Arbitrarily high up to value of life and assets. Attacker can be punished by the state.	“Security guards” in Figure 1. Variable costs of monitoring and enforcement associated with specific locations or transactions.	Investment in government and legal system.
Collateral	Stock + Punishment. Attacker loses the value of their collateral plus any additional punishment.	0, under conditions of Modigliani-Miller theorem. Requires legal enforcement mechanism which entails fixed costs.	Collateral value.
Nakamoto with Collapse	Stock. Attacker loses specialized capital worth $N * C$ .	$p_{block}$ per period.	ASICs or other specialized computational equipment.
Proof-of-Stake in its original form	Flow. Attacker pays opportunity cost of capital $p_{block} = N * c$ for a short period of time.	$p_{block}$ per period.	Cryptocurrency stake.
Proof-of-Stake with Slashing (Idealized)	Stock. Attacker loses specialized capital worth $N * C$ .	$p_{block}$ per period.	Cryptocurrency stake.

# Comparison of Trust Models

	Cost to Break Trust	Variable Cost of Honest Play	Fixed Cost Investments that Support Honest Play
Nakamoto Trust in its original form (Nakamoto, 2008)	Flow. Attacker pays cost of honest trust support $p_{block} = N * c$ for a short period of time.	$p_{block}$ per period.	–
Repeated Interaction (Schelling, 1956; Aumann, 1959)	Stock. Attacker loses the net present value of the trust relationship $V_{trust} = \frac{1}{1-\delta} \tau$ .	0, given pre-existing trust relationship.	Investment in trust relationship, brand, reputation.
Credible Deterrence (Hayek, 1960; Becker, 1968)	Arbitrarily high up to value of life and assets. Attacker can be punished by the state.	“Security guards” in Figure 1. Variable costs of monitoring and enforcement associated with specific locations or transactions.	Investment in government and legal system.
Collateral	Stock + Punishment. Attacker loses the value of their collateral plus any additional punishment.	0, under conditions of Modigliani-Miller theorem. Requires legal enforcement mechanism which entails fixed costs.	Collateral value.
Nakamoto with Collapse	Stock. Attacker loses specialized capital worth $N * C$ .	$p_{block}$ per period.	ASICs or other specialized computational equipment.
Proof-of-Stake in its original form	Flow. Attacker pays opportunity cost of capital $p_{block} = N * c$ for a short period of time.	$p_{block}$ per period.	Cryptocurrency stake.
Proof-of-Stake with Slashing (Idealized)	Stock. Attacker loses specialized capital worth $N * C$ .	$p_{block}$ per period.	Cryptocurrency stake.

# Comparison of Trust Models

	Cost to Break Trust	Variable Cost of Honest Play	Fixed Cost Investments that Support Honest Play
Nakamoto Trust in its original form (Nakamoto, 2008)	Flow. Attacker pays cost of honest trust support $p_{block} = N * c$ for a short period of time.	$p_{block}$ per period.	–
Repeated Interaction (Schelling, 1956; Aumann, 1959)	Stock. Attacker loses the net present value of the trust relationship $V_{trust} = \frac{1}{1-\delta} \tau$ .	0, given pre-existing trust relationship.	Investment in trust relationship, brand, reputation.
Credible Deterrence (Hayek, 1960; Becker, 1968)	Arbitrarily high up to value of life and assets. Attacker can be punished by the state.	“Security guards” in Figure 1. Variable costs of monitoring and enforcement associated with specific locations or transactions.	Investment in government and legal system.
Collateral	Stock + Punishment. Attacker loses the value of their collateral plus any additional punishment.	0, under conditions of Modigliani-Miller theorem. Requires legal enforcement mechanism which entails fixed costs.	Collateral value.
Nakamoto with Collapse	Stock. Attacker loses specialized capital worth $N * C$ .	$p_{block}$ per period.	ASICs or other specialized computational equipment.
Proof-of-Stake in its original form	Flow. Attacker pays opportunity cost of capital $p_{block} = N * c$ for a short period of time.	$p_{block}$ per period.	Cryptocurrency stake.
Proof-of-Stake with Slashing (Idealized)	Stock. Attacker loses specialized capital worth $N * C$ .	$p_{block}$ per period.	Cryptocurrency stake.

# Comparison of Trust Models

	Cost to Break Trust	Variable Cost of Honest Play	Fixed Cost Investments that Support Honest Play
Nakamoto Trust in its original form (Nakamoto, 2008)	Flow. Attacker pays cost of honest trust support $p_{block} = N * c$ for a short period of time.	$p_{block}$ per period.	–
Repeated Interaction (Schelling, 1956; Aumann, 1959)	Stock. Attacker loses the net present value of the trust relationship $V_{trust} = \frac{1}{1-\delta} \tau$ .	0, given pre-existing trust relationship.	Investment in trust relationship, brand, reputation.
Credible Deterrence (Hayek, 1960; Becker, 1968)	Arbitrarily high up to value of life and assets. Attacker can be punished by the state.	“Security guards” in Figure 1. Variable costs of monitoring and enforcement associated with specific locations or transactions.	Investment in government and legal system.
Collateral	Stock + Punishment. Attacker loses the value of their collateral plus any additional punishment.	0, under conditions of Modigliani-Miller theorem. Requires legal enforcement mechanism which entails fixed costs.	Collateral value.
Nakamoto with Collapse	Stock. Attacker loses specialized capital worth $N * C$ .	$p_{block}$ per period.	ASICs or other specialized computational equipment.
Proof-of-Stake in its original form	Flow. Attacker pays opportunity cost of capital $p_{block} = N * c$ for a short period of time.	$p_{block}$ per period.	Cryptocurrency stake.
Proof-of-Stake with Slashing (Idealized)	Stock. Attacker loses specialized capital worth $N * C$ .	$p_{block}$ per period.	Cryptocurrency stake.

# Comparison of Trust Models

	Cost to Break Trust	Variable Cost of Honest Play	Fixed Cost Investments that Support Honest Play
Nakamoto Trust in its original form (Nakamoto, 2008)	Flow. Attacker pays cost of honest trust support $p_{block} = N * c$ for a short period of time.	$p_{block}$ per period.	–
Repeated Interaction (Schelling, 1956; Aumann, 1959)	Stock. Attacker loses the net present value of the trust relationship $V_{trust} = \frac{1}{1-\delta} \tau$ .	0, given pre-existing trust relationship.	Investment in trust relationship, brand, reputation.
Credible Deterrence (Hayek, 1960; Becker, 1968)	Arbitrarily high up to value of life and assets. Attacker can be punished by the state.	“Security guards” in Figure 1. Variable costs of monitoring and enforcement associated with specific locations or transactions.	Investment in government and legal system.
Collateral	Stock + Punishment. Attacker loses the value of their collateral plus any additional punishment.	0, under conditions of Modigliani-Miller theorem. Requires legal enforcement mechanism which entails fixed costs.	Collateral value.
Nakamoto with Collapse	Stock. Attacker loses specialized capital worth $N * C$ .	$p_{block}$ per period.	ASICs or other specialized computational equipment.
Proof-of-Stake in its original form	Flow. Attacker pays opportunity cost of capital $p_{block} = N * c$ for a short period of time.	$p_{block}$ per period.	Cryptocurrency stake.
Proof-of-Stake with Slashing (Idealized)	Stock. Attacker loses specialized capital worth $N * C$ .	$p_{block}$ per period.	Cryptocurrency stake.

# Comparison of Trust Models

	Cost to Break Trust	Variable Cost of Honest Play	Fixed Cost Investments that Support Honest Play
Nakamoto Trust in its original form (Nakamoto, 2008)	Flow. Attacker pays cost of honest trust support $p_{block} = N * c$ for a short period of time.	$p_{block}$ per period.	–
Repeated Interaction (Schelling, 1956; Aumann, 1959)	Stock. Attacker loses the net present value of the trust relationship $V_{trust} = \frac{1}{1-\delta} \tau$ .	0, given pre-existing trust relationship.	Investment in trust relationship, brand, reputation.
Credible Deterrence (Hayek, 1960; Becker, 1968)	Arbitrarily high up to value of life and assets. Attacker can be punished by the state.	“Security guards” in Figure 1. Variable costs of monitoring and enforcement associated with specific locations or transactions.	Investment in government and legal system.
Collateral	Stock + Punishment. Attacker loses the value of their collateral plus any additional punishment.	0, under conditions of Modigliani-Miller theorem. Requires legal enforcement mechanism which entails fixed costs.	Collateral value.
Nakamoto with Collapse	Stock. Attacker loses specialized capital worth $N * C$ .	$p_{block}$ per period.	ASICs or other specialized computational equipment.
Proof-of-Stake in its original form	Flow. Attacker pays opportunity cost of capital $p_{block} = N * c$ for a short period of time.	$p_{block}$ per period.	Cryptocurrency stake.
Proof-of-Stake with Slashing (Idealized)	Stock. Attacker loses specialized capital worth $N * C$ .	$p_{block}$ per period.	Cryptocurrency stake.

# Comparison of Trust Models

	Cost to Break Trust	Variable Cost of Honest Play	Fixed Cost Investments that Support Honest Play
Nakamoto Trust in its original form (Nakamoto, 2008)	Flow. Attacker pays cost of honest trust support $p_{block} = N * c$ for a short period of time.	$p_{block}$ per period.	–
Repeated Interaction (Schelling, 1956; Aumann, 1959)	Stock. Attacker loses the net present value of the trust relationship $V_{trust} = \frac{1}{1-\delta} \tau$ .	0, given pre-existing trust relationship.	Investment in trust relationship, brand, reputation.
Credible Deterrence (Hayek, 1960; Becker, 1968)	Arbitrarily high up to value of life and assets. Attacker can be punished by the state.	“Security guards” in Figure 1. Variable costs of monitoring and enforcement associated with specific locations or transactions.	Investment in government and legal system.
Collateral	Stock + Punishment. Attacker loses the value of their collateral plus any additional punishment.	0, under conditions of Modigliani-Miller theorem. Requires legal enforcement mechanism which entails fixed costs.	Collateral value.
Nakamoto with Collapse	Stock. Attacker loses specialized capital worth $N * C$ .	$p_{block}$ per period.	ASICs or other specialized computational equipment.
Proof-of-Stake in its original form	Flow. Attacker pays opportunity cost of capital $p_{block} = N * c$ for a short period of time.	$p_{block}$ per period.	Cryptocurrency stake.
Proof-of-Stake with Slashing (Idealized)	Stock. Attacker loses specialized capital worth $N * C$ .	$p_{block}$ per period.	Cryptocurrency stake.

## Sense of Magnitudes: Traditional Trust vs. Nakamoto Trust

- ▶ Sense of magnitudes for finance
  - ▶ Total annual spending in the US on police, prisons and courts is about \$300bn.
  - ▶ Real value added in the US financial sector is about \$800bn. (see Philippon, 2015)
  - ▶ So \$1 trillion is a conservative upper bound for the cost of trust in the US financial sector (former includes much non-finance, latter includes much non-trust).

# Sense of Magnitudes: Traditional Trust vs. Nakamoto Trust

- ▶ Sense of magnitudes for finance
  - ▶ Total annual spending in the US on police, prisons and courts is about \$300bn.
  - ▶ Real value added in the US financial sector is about \$800bn. (see Philippon, 2015)
  - ▶ So \$1 trillion is a conservative upper bound for the cost of trust in the US financial sector (former includes much non-finance, latter includes much non-trust).
  - ▶ Transaction volume in US finance easily exceeds \$1 quadrillion per year (Budish and Sunderam, 2024)

## Sense of Magnitudes: Traditional Trust vs. Nakamoto Trust

- ▶ Sense of magnitudes for finance
  - ▶ Total annual spending in the US on police, prisons and courts is about \$300bn.
  - ▶ Real value added in the US financial sector is about \$800bn. (see Philippon, 2015)
  - ▶ So \$1 trillion is a conservative upper bound for the cost of trust in the US financial sector (former includes much non-finance, latter includes much non-trust).
  - ▶ Transaction volume in US finance easily exceeds \$1 quadrillion per year (Budish and Sunderam, 2024)
- ▶ So we can conservatively upper bound  $\frac{F}{V_{honest}} + c$  for the financial sector by 0.1%

## Sense of Magnitudes: Traditional Trust vs. Nakamoto Trust

- ▶ Sense of magnitudes for finance
  - ▶ Total annual spending in the US on police, prisons and courts is about \$300bn.
  - ▶ Real value added in the US financial sector is about \$800bn. (see Philippon, 2015)
  - ▶ So \$1 trillion is a conservative upper bound for the cost of trust in the US financial sector (former includes much non-finance, latter includes much non-trust).
  - ▶ Transaction volume in US finance easily exceeds \$1 quadrillion per year (Budish and Sunderam, 2024)
- ▶ So we can conservatively upper bound  $\frac{F}{V_{honest}} + c$  for the financial sector by 0.1%
- ▶ Many fees in traditional finance, especially for large transactions, are 0.01% or less of transaction volume.
- ▶ Not meant to be an apology for traditional finance (see Greenwood and Scharfstein, 2013; Philippon, 2015; Zingales, 2015). But comparison with Nakamoto trust is night-and-day.

# “The Economic Limits of Permissionless Consensus”

Eric Budish, Andrew Lewis-Pye, Tim Roughgarden

*The Twenty-Fifth ACM Conference on Economics and Computation (EC'24)*

## Our Question

- ▶ Context: if the attack costs the attacker the “stock” value of their capital (computers, stake, etc.) in addition to the “flow” costs of attack, then the blockchain is much more secure (2500x improvement)
- ▶ There are in principle three different ways this could happen
  1. Collapse.
    - ▶ Currency collapses because of the majority attack. So specialized capital loses its value (ASICs, stake, etc.)
    - ▶ Works, but (a) harms honest participants too, (b) vulnerable to sabotage
  2. Legal punishment of the attacker. External to protocol.
    - ▶ Works, but the question is whether Nakamoto trust is viable without rule of law
  3. Algorithmic, in-protocol punishment of the attacker.
    - ▶ E.g., confiscate/destroy/nullify the attacker’s specialized computers in the case of proof-of-work, or the attacker’s stake in proof-of-stake.
- ▶ Our question: does targeted algorithmic punishment actually work?

## Our Results

- ▶ Targeted punishment of the attacker is:
- ▶ Impossible for a large class of permissionless consensus protocols that includes
  - ▶ Bitcoin
  - ▶ Earliest versions of proof-of-stake (based on longest chain)
- ▶ Possible for proof-of-stake consensus based on Byzantine Fault Tolerance (BFT). First positive result of its kind, but comes with some big restrictions, which we show are necessary:
  - ▶ Strong assumption about network reliability
  - ▶ Long unlock/escrow periods. Issue is that an attacker would want to unlock their funds before they can be punished
  - ▶ Attacker can't be too large ...  $\frac{2}{3}$  bound. Issue is that attacker can stall the legal system.
- ▶ Implication:
  - ▶ Ethereum's approach (PoS with slashing) improves security if the attacker is between 51-66%. Successfully mimics collateral + rule-of-law
  - ▶ But once an attacker is incentivized to reach 67%, no longer works

# “Blockchain Technology in Traditional Finance”

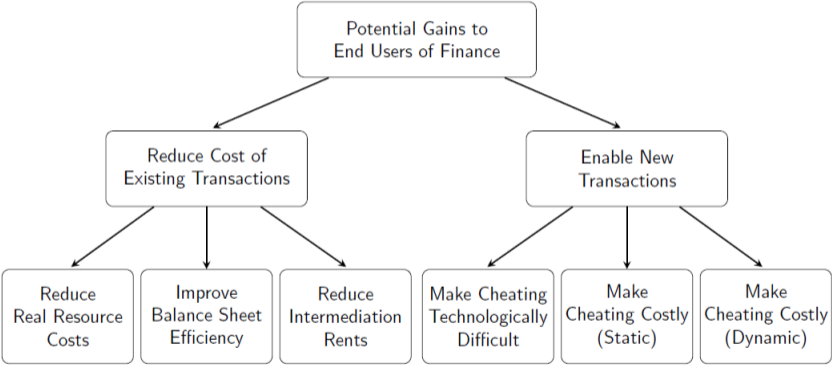
Eric Budish, Adi Sunderam

*Sveriges Riksbank 7th Annual Macprudential Conference*

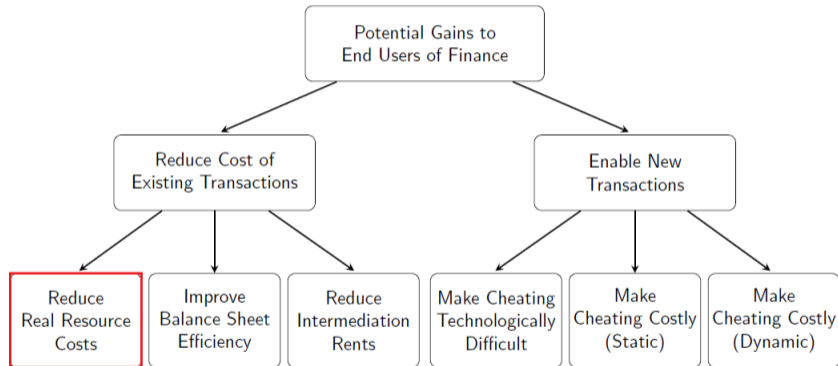
## Motivation

- ▶ Economic Limits papers leave us deeply skeptical about permissionless consensus in its pure form.
- ▶ Our question: is combining the ideas developed in the CS literature on permissionless consensus with old-fashioned rule-of-law economically useful relative to alternatives.
- ▶ We postulate a perfect blockchain data structure — not vulnerable to attack, protected by rule of law in the background.
- ▶ Then we ask, what might be the potential social value of such a data structure for traditional finance.

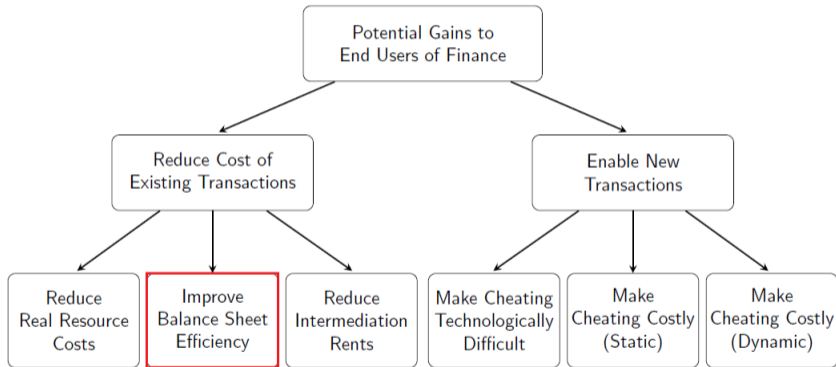
# Framework for Analyzing Gains from Idealized Data Structure for Traditional Finance



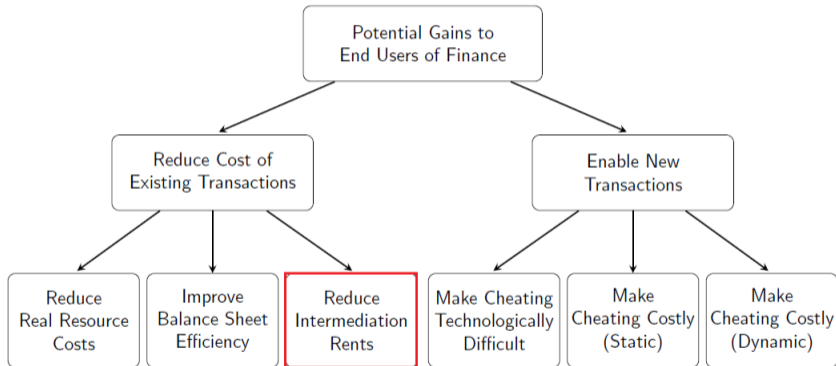
# Framework for Analyzing Gains from Idealized Data Structure for Traditional Finance



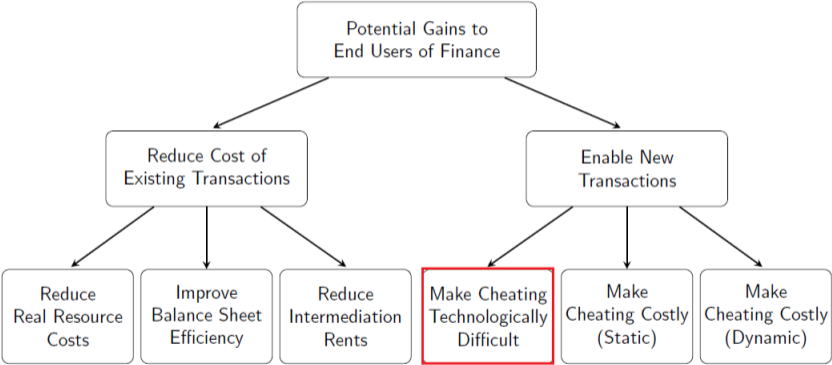
# Framework for Analyzing Gains from Idealized Data Structure for Traditional Finance



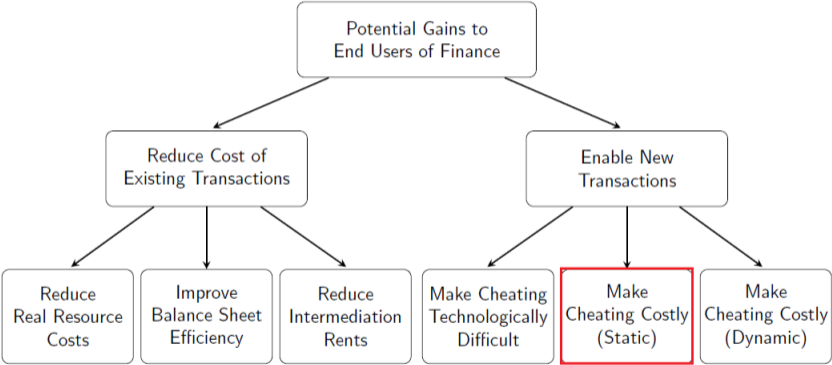
# Framework for Analyzing Gains from Idealized Data Structure for Traditional Finance



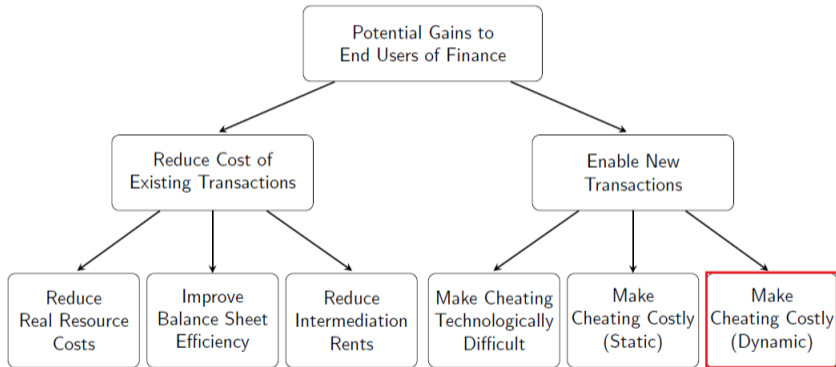
# Framework for Analyzing Gains from Idealized Data Structure for Traditional Finance



# Framework for Analyzing Gains from Idealized Data Structure for Traditional Finance



# Framework for Analyzing Gains from Idealized Data Structure for Traditional Finance



# Three Ways a Blockchain Can Facilitate Cooperation

Panel A: Technology

		Player 2		
		Engage, Cooperate	Engage, Cheat	Do not Engage
Player 1	Engage, Cooperate	$+f$	$+V$	0
	Engage, Cheat	$-V$	$-P$	0
Do not Engage		0	0	0

If a blockchain eliminates the technological possibility of cheating, then {Cooperate, Cooperate} becomes the unique static equilibrium.

Panel B: Punishment

		Player 2		
		Engage, Cooperate	Engage, Cheat	Do not Engage
Player 1	Engage, Cooperate	$+f$	$-P$	0
	Engage, Cheat	0	$-\epsilon$	0
Do not Engage		0	0	0

If a blockchain makes cheating detectable and punishable via rule-of-law, then {Cooperate, Cooperate} becomes the unique static equilibrium.

Panel C: Reputation

		Player 2		
		Engage, Cooperate	Engage, Cheat	Do not Engage
Player 1	Engage, Cooperate	$+f$	$+V$	0
	Engage, Cheat	$-V$	$-\epsilon$	0
Do not Engage		0	0	0

If a blockchain makes past play widely observable across the financial sector, then {Cooperate, Cooperate} can become an equilibrium of the *dynamic* game even if in the one-shot game there remains a possibility to cheat.

## Closing Questions and Directions

- ▶ Econ + CS question: is there something new and better on the “production possibilities frontier for trust”?
- ▶ Traditional trust is often “multi-layered”: law, reputations, relationships, brands, collateral, technology, etc., often working together in the same transaction, without even drawing much notice
  - ▶ Ex: JPMorgan combination of reputation, collateral, laws
  - ▶ Ex: local coffee shop (reputation, relational contracts, food safety laws)
- ▶ Q1: How do we model the production possibilities frontier for trust?
- ▶ Q2: Does permissionless consensus expand the frontier? Are there combinations of permissionless consensus protocols + traditional sources of trust that are superior to existing alternatives?
- ▶ Q3: What about permissioned consensus protocols? Do they create new points on the frontier? (Facebook’s Diem project)

## Closing Questions and Directions

- ▶ Policy conundrum
- ▶ There is a lot of implicit legal support for crypto.
  - ▶ Ex 1: majority attack against a major financial institution
  - ▶ Ex 2: criminal steals crypto password at gunpoint
- ▶ Which puts policy in a bind because dominant use case to date is criminal activity.
- ▶ Question: is there a useful way to make the trade more explicit
  - ▶ Explicit legal support for permissionless consensus
  - ▶ Identities that are non-anonymous or can be easily de-anonymized by the courts

## Closing Questions and Directions

- ▶ Market power in traditional finance
- ▶ Huberman, Leshno and Moallemi (2021) point to \$2Trn global payments revenues
- ▶ Could a better blockchain reduce these and other rents in traditional finance?
- ▶ As flagged, this is the source of potential gains that Sunderam and I are most unsure about how to model.
- ▶ Financial institutions that earn rents from the status quo have a lot of incentive to preserve these rents
- ▶ CBDC seems like a good idea — Fed's 2022 white paper on CBDCs surprisingly cautious about effects on banks' profits from deposits

## Closing Questions and Directions

- ▶ Crypto as a social/financial phenomenon
- ▶ Observe: It's a bubble either way!
- ▶ Great setting to study financial bubbles — likely better and different data than in past contexts
- ▶ One empirical pattern I bet would obtain if someone can find the data:
  - ▶ In early years of crypto takeoff (2010-2016ish): investment inflows disproportionately from wealthy, educated, high-tech zip codes
  - ▶ In peak-speculative-frenzy years of crypto takeoff (2017, 2020-2021): that is where you will see comparatively more investment inflows from poorer, low-SES zip codes
- ▶ Also interesting to study institutional investors inflows
  - ▶ Ex: at Goldman Sachs Digital Asset Conference (June, 2022), there seemed a lot of interest in recruiting pension fund money
  - ▶ Optimal portfolio allocation or next layer of the pyramid?