

2026 AEA Recent Developments Lecture

The Economics of Cryptocurrencies and Blockchains

Eric Budish
University of Chicago, Booth School of Business

January 4th, 2026

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

- ▶ Satoshi Nakamoto (2008) invented a new kind of economic system that does not need the support of government or laws

Nakamoto's Invention

- ▶ Satoshi Nakamoto (2008) invented a new kind of economic system that does not need the support of government or laws
- ▶ Trust and security instead solely arise from a combination of cryptography and economic incentives. Completely anonymous and decentralized.
 - ▶ CS terminology for Nakamoto's invention: "permissionless consensus"
 - ▶ Large, anonymous, freely-entering and -exiting set of participants collectively maintains a common data set, creating collective trust without any trusted parties
 - ▶ "a new territory of freedom"; "outside the reach of any government"

Nakamoto's Invention

- ▶ Satoshi Nakamoto (2008) invented a new kind of economic system that does not need the support of government or laws
- ▶ Trust and security instead solely arise from a combination of cryptography and economic incentives. Completely anonymous and decentralized.
 - ▶ CS terminology for Nakamoto's invention: "permissionless consensus"
 - ▶ Large, anonymous, freely-entering and -exiting set of participants collectively maintains a common data set, creating collective trust without any trusted parties
 - ▶ "a new territory of freedom"; "outside the reach of any government"
- ▶ Nakamoto's invention enabled cryptocurrencies, including his own, Bitcoin.
 - ▶ A trusted database can keep track of currency balances

Nakamoto's Invention

- ▶ Satoshi Nakamoto (2008) invented a new kind of economic system that does not need the support of government or laws
- ▶ Trust and security instead solely arise from a combination of cryptography and economic incentives. Completely anonymous and decentralized.
 - ▶ CS terminology for Nakamoto's invention: "permissionless consensus"
 - ▶ Large, anonymous, freely-entering and -exiting set of participants collectively maintains a common data set, creating collective trust without any trusted parties
 - ▶ "a new territory of freedom"; "outside the reach of any government"
- ▶ Nakamoto's invention enabled cryptocurrencies, including his own, Bitcoin.
 - ▶ A trusted database can keep track of currency balances
- ▶ More generally: easy to imagine other potential use cases for a trusted public database, called a blockchain
 - ▶ "computer in the sky", Ethereum

Nakamoto's Invention

- ▶ Nakamoto's invention has clearly captured the world's attention
- ▶ Oct 2025 peak: over \$4 trillion
- ▶ Even this figure seems to understate the amount of cultural, political and commercial attention that has been paid to blockchains and cryptocurrencies

Nakamoto's Invention

- ▶ Nakamoto's invention has clearly captured the world's attention
- ▶ Oct 2025 peak: over \$4 trillion
- ▶ Even this figure seems to understate the amount of cultural, political and commercial attention that has been paid to blockchains and cryptocurrencies
- ▶ Yet, economic usefulness remains an open question. To date:

Nakamoto's Invention

- ▶ Nakamoto's invention has clearly captured the world's attention
- ▶ Oct 2025 peak: over \$4 trillion
- ▶ Even this figure seems to understate the amount of cultural, political and commercial attention that has been paid to blockchains and cryptocurrencies
- ▶ Yet, economic usefulness remains an open question. To date:
 - ▶ Largest use case (by far) is financial speculation

Nakamoto's Invention

- ▶ Nakamoto's invention has clearly captured the world's attention
- ▶ Oct 2025 peak: over \$4 trillion
- ▶ Even this figure seems to understate the amount of cultural, political and commercial attention that has been paid to blockchains and cryptocurrencies
- ▶ Yet, economic usefulness remains an open question. To date:
 - ▶ Largest use case (by far) is financial speculation
 - ▶ Next most widely-documented use case is illegal activity (online scams, online casinos, terrorist groups, drugs, etc)

Nakamoto's Invention

- ▶ Nakamoto's invention has clearly captured the world's attention
- ▶ Oct 2025 peak: over \$4 trillion
- ▶ Even this figure seems to understate the amount of cultural, political and commercial attention that has been paid to blockchains and cryptocurrencies
- ▶ Yet, economic usefulness remains an open question. To date:
 - ▶ Largest use case (by far) is financial speculation
 - ▶ Next most widely-documented use case is illegal activity (online scams, online casinos, terrorist groups, drugs, etc)
 - ▶ Sources: Makarov and Schoar, 2021; Yellen, 2021; Gensler, 2021; Buterin, 2022; Faux, 2023

Nakamoto's Invention

- ▶ Nakamoto's invention has clearly captured the world's attention
- ▶ Oct 2025 peak: over \$4 trillion
- ▶ Even this figure seems to understate the amount of cultural, political and commercial attention that has been paid to blockchains and cryptocurrencies
- ▶ Yet, economic usefulness remains an open question. To date:
 - ▶ Largest use case (by far) is financial speculation
 - ▶ Next most widely-documented use case is illegal activity (online scams, online casinos, terrorist groups, drugs, etc)
 - ▶ Sources: Makarov and Schoar, 2021; Yellen, 2021; Gensler, 2021; Buterin, 2022; Faux, 2023
- ▶ Also, a rich irony: most of the financial speculation has been through cryptocurrency exchanges like Coinbase or Binance or exchange-traded products like Bitcoin ETFs ...
 - ▶ That is ... trusted financial intermediaries. Backed by rule of law.

Nakamoto's Invention

- ▶ Nakamoto's invention has clearly captured the world's attention
- ▶ Oct 2025 peak: over \$4 trillion
- ▶ Even this figure seems to understate the amount of cultural, political and commercial attention that has been paid to blockchains and cryptocurrencies
- ▶ Yet, economic usefulness remains an open question. To date:
 - ▶ Largest use case (by far) is financial speculation
 - ▶ Next most widely-documented use case is illegal activity (online scams, online casinos, terrorist groups, drugs, etc)
 - ▶ Sources: Makarov and Schoar, 2021; Yellen, 2021; Gensler, 2021; Buterin, 2022; Faux, 2023
- ▶ Also, a rich irony: most of the financial speculation has been through cryptocurrency exchanges like Coinbase or Binance or exchange-traded products like Bitcoin ETFs ...
 - ▶ That is ... trusted financial intermediaries. Backed by rule of law.
 - ▶ Also: often not even that trustworthy (FTX, many others)

Adam Smith vs. Satoshi Nakamoto

- ▶ Today's talk will have two parts.

Adam Smith vs. Satoshi Nakamoto

- ▶ Today's talk will have two parts.
- ▶ **Part I** will cover my paper “Trust at Scale: The Economic Limits of Cryptocurrencies and Blockchains” (*Quarterly Journal of Economics*, Feb 2025, Pages 1-62).

Adam Smith vs. Satoshi Nakamoto

- ▶ Today's talk will have two parts.
- ▶ **Part I** will cover my paper “Trust at Scale: The Economic Limits of Cryptocurrencies and Blockchains” (*Quarterly Journal of Economics*, Feb 2025, Pages 1-62).
- ▶ Main message: Nakamoto's novel form of trust, while clearly ingenious, is fundamentally economically limited

Adam Smith vs. Satoshi Nakamoto

- ▶ Achilles' heel of permissionless consensus: vulnerability to majority attack

Adam Smith vs. Satoshi Nakamoto

- ▶ Achilles' heel of permissionless consensus: vulnerability to majority attack
- ▶ Many hear the phrase “cryptography” and assume that blockchain data are secure

Adam Smith vs. Satoshi Nakamoto

- ▶ Achilles' heel of permissionless consensus: vulnerability to majority attack
- ▶ Many hear the phrase “cryptography” and assume that blockchain data are secure
- ▶ But really you should think of blockchain data as secured by a combination of:
 1. cryptography, and
 2. an anonymous majority vote by the decentralized participants

Adam Smith vs. Satoshi Nakamoto

- ▶ Achilles' heel of permissionless consensus: vulnerability to majority attack
- ▶ Many hear the phrase “cryptography” and assume that blockchain data are secure
- ▶ But really you should think of blockchain data as secured by a combination of:
 1. cryptography, and
 2. an anonymous majority vote by the decentralized participants
- ▶ This is true for all forms of permissionless consensus: proof of work, stake, etc.
 - ▶ Vulnerability known to Computer Science since the 1980s ...
 - ▶ and literally in the *abstract* of Nakamoto (2008)

Adam Smith vs. Satoshi Nakamoto

- ▶ My approach: model this vulnerability to majority attack as an economic incentive compatibility constraint

Adam Smith vs. Satoshi Nakamoto

- ▶ My approach: model this vulnerability to majority attack as an economic incentive compatibility constraint
- ▶ This in turn allows for eqm reasoning:

Adam Smith vs. Satoshi Nakamoto

- ▶ My approach: model this vulnerability to majority attack as an economic incentive compatibility constraint
- ▶ This in turn allows for eqm reasoning:
 - ▶ If permissionless consensus were to become more economically useful ...

Adam Smith vs. Satoshi Nakamoto

- ▶ My approach: model this vulnerability to majority attack as an economic incentive compatibility constraint
- ▶ This in turn allows for eqm reasoning:
 - ▶ If permissionless consensus were to become more economically useful ...
 - ▶ Then it would have to get implausibly expensive

Adam Smith vs. Satoshi Nakamoto

- ▶ My approach: model this vulnerability to majority attack as an economic incentive compatibility constraint
- ▶ This in turn allows for eqm reasoning:
 - ▶ If permissionless consensus were to become more economically useful ...
 - ▶ Then it would have to get implausibly expensive
- ▶ Costs quickly grow absurd: can be more than all of global GDP

Adam Smith vs. Satoshi Nakamoto

- ▶ My approach: model this vulnerability to majority attack as an economic incentive compatibility constraint
- ▶ This in turn allows for eqm reasoning:
 - ▶ If permissionless consensus were to become more economically useful ...
 - ▶ Then it would have to get implausibly expensive
- ▶ Costs quickly grow absurd: can be more than all of global GDP
- ▶ In contrast: traditional forms of trust have economies of scale.
 - ▶ Ex: pay a fixed cost for a credible legal system, then have trust and safety at low marginal cost, via credible deterrence.

Part II: Open Questions and Directions for Research

Part II of this talk: Open questions and directions for research

- ▶ Taking as our premise that permissionless consensus in its pure form is fundamentally economically limited, per Budish (2025) ...
- ▶ There are many, many interesting questions for research
- ▶ I will sketch 5 topic areas
- ▶ Covering both recent developments and future opportunities

Part II: Open Questions and Directions for Research

Topic 1: Potential solutions to the Budish problem.

- ▶ “Trust frontier”: ways to mix Nakamoto-style trust with traditional forms of trust.
- ▶ Ethereum proof-of-stake plus slashing
- ▶ Leshno et al’s “Stubborn Nakamoto” protocol
- ▶ Facebook’s Libra/Diem approach
- ▶ Layer 1 / Layer 2 paradigm

Part II: Open Questions and Directions for Research

Topic 2: Blockchain and traditional finance.

- ▶ For traditional finance, imagine a permissioned blockchain explicitly backed by rule-of-law
- ▶ CS not impressed. “Just a database.”
 - ▶ (Databases have been around for a while ...)
- ▶ Q: is there anything *economically* interesting that emerges from this particular form of database?
- ▶ Sub-topic: stablecoins.
 - ▶ Lots of confusion in public discussion between permissionless and permissioned versions of the stablecoin idea

Part II: Open Questions and Directions for Research

Topic 3: Crypto as a social and financial phenomenon.

- ▶ Key point: it's a bubble either way!
- ▶ Thus an amazing laboratory to study bubble formation
- ▶ I will pay particular note to Shiller's idea of bubbles as a “naturally occurring Ponzi process”

Part II: Open Questions and Directions for Research

Topic 4: Crypto data for finance research.

- ▶ Opportunity: use crypto data to study questions of interest to traditional academic finance.
- ▶ Ex 1: much of the financial markets regulation that came out of the 1929 crash is not present in crypto markets.
 - ▶ Crypto pump-and-dumps echo 1920s “investor pools” (see Sorkin’s book 1929)
- ▶ Ex 2: amazing lab for market microstructure research (HFT issues on steroids)

Part II: Open Questions and Directions for Research

Topic 5: Crypto and political economy.

- ▶ The core policy conundrum:
 - ▶ Appeal of crypto is anonymity / “outside the reach of any government”
 - ▶ But governments / law provides a lot of explicit and implicit protection for crypto assets
- ▶ The core policy confusion:
 - ▶ Recent crypto legislation confused about permissionless vs. permissioned
 - ▶ And ignores attack risks
- ▶ Crypto and corruption.

Trust at Scale: The Economic Limits of Cryptocurrencies and Blockchains

Eric Budish

University of Chicago, Booth School of Business

Quarterly Journal of Economics, Feb 2025

The Paper's Argument

- ▶ Core of the argument is three equations.

The Paper's Argument

- ▶ Core of the argument is three equations.
- ▶ Equation (1): zero-profits condition, honest play.
 - ▶ The amount of “trust support” devoted to maintaining permissionless consensus reflects the compensation paid by the protocol (work, stake, etc.).

The Paper's Argument

- ▶ Core of the argument is three equations.
- ▶ Equation (1): zero-profits condition, honest play.
 - ▶ The amount of “trust support” devoted to maintaining permissionless consensus reflects the compensation paid by the protocol (work, stake, etc.).
- ▶ Equation (2): incentive compatibility condition, majority attack.
 - ▶ How much security does a given level of trust support produce?
 - ▶ IC: costs of attack must exceed the benefits.

The Paper's Argument

- ▶ Core of the argument is three equations.
- ▶ Equation (1): zero-profits condition, honest play.
 - ▶ The amount of “trust support” devoted to maintaining permissionless consensus reflects the compensation paid by the protocol (work, stake, etc.).
- ▶ Equation (2): incentive compatibility condition, majority attack.
 - ▶ How much security does a given level of trust support produce?
 - ▶ IC: costs of attack must exceed the benefits.
- ▶ Together, (1)+(2) imply:
 - ▶ (3): recurring, “flow” cost of honest trust support must be large relative to the value of attacking the system

The Paper's Argument

- ▶ Core of the argument is three equations.
- ▶ Equation (1): zero-profits condition, honest play.
 - ▶ The amount of “trust support” devoted to maintaining permissionless consensus reflects the compensation paid by the protocol (work, stake, etc.).
- ▶ Equation (2): incentive compatibility condition, majority attack.
 - ▶ How much security does a given level of trust support produce?
 - ▶ IC: costs of attack must exceed the benefits.
- ▶ Together, (1)+(2) imply:
 - ▶ (3): recurring, “flow” cost of honest trust support must be large relative to the value of attacking the system
 - ▶ Very expensive!

The Paper's Argument

- ▶ Core of the argument is three equations.
- ▶ Equation (1): zero-profits condition, honest play.
 - ▶ The amount of “trust support” devoted to maintaining permissionless consensus reflects the compensation paid by the protocol (work, stake, etc.).
- ▶ Equation (2): incentive compatibility condition, majority attack.
 - ▶ How much security does a given level of trust support produce?
 - ▶ IC: costs of attack must exceed the benefits.
- ▶ Together, (1)+(2) imply:
 - ▶ (3): recurring, “flow” cost of honest trust support must be large relative to the value of attacking the system
 - ▶ Very expensive!
 - ▶ Especially as stakes grow! Scales linearly.

The Paper's Argument

- ▶ Core of the argument is three equations.
- ▶ Equation (1): zero-profits condition, honest play.
 - ▶ The amount of “trust support” devoted to maintaining permissionless consensus reflects the compensation paid by the protocol (work, stake, etc.).
- ▶ Equation (2): incentive compatibility condition, majority attack.
 - ▶ How much security does a given level of trust support produce?
 - ▶ IC: costs of attack must exceed the benefits.
- ▶ Together, (1)+(2) imply:
 - ▶ (3): recurring, “flow” cost of honest trust support must be large relative to the value of attacking the system
 - ▶ Very expensive!
 - ▶ Especially as stakes grow! Scales linearly.
- ▶ Intuition: Nakamoto trust relies on anonymous majority voting.
- ▶ Doesn't have the scale economies that come from law + credible deterrence.

Overview of the Talk

Part I: Trust at Scale

- ▶ **Overview of Nakamoto (2008) and Related Concepts**
- ▶ Nakamoto Trust: A Critique in 3 Equations
- ▶ Analysis of Double-Spending Attacks
- ▶ A Way Out: Specific Capital + Collapse
- ▶ Comparison of Nakamoto Trust and Traditional Trust
- ▶ Summary of “Trust at Scale”

Part II: Directions for Research

Conclusion

What is Nakamoto Blockchain?

- ▶ **Transaction:** sender, receiver, amount, signature
- ▶ **Signature:**
 - ▶ Proves sender's identity
 - ▶ Encodes transaction details (amount, recipient)
 - ▶ Standard cryptography techniques

Sender	Receiver	Amount	Signature
Alice	Bob	\$10	<i>Alice</i>

What is Nakamoto Blockchain?

- ▶ **Transaction:** sender, receiver, amount, signature

Sender	Receiver	Amount	Signature
Alice	Bob	\$10	<i>Alice</i>

- ▶ **Signature:**
 - ▶ Proves sender's identity
 - ▶ Encodes transaction details (amount, recipient)
 - ▶ Standard cryptography techniques
- ▶ Imagine transactions on a google spreadsheet
 - ▶ Signature: only Alice can add transactions in which Alice sends money
 - ▶ But:
 - ▶ Alice can send money she doesn't have
 - ▶ Alice can send money she does have but to multiple parties at the same time
 - ▶ Alice can delete previous transactions (her own or others').

What is Nakamoto Blockchain?

- ▶ **Transaction:** sender, receiver, amount, signature

Sender	Receiver	Amount	Signature
Alice	Bob	\$10	<i>Alice</i>

- ▶ **Signature:**
 - ▶ Proves sender's identity
 - ▶ Encodes transaction details (amount, recipient)
 - ▶ Standard cryptography techniques
- ▶ Imagine transactions on a google spreadsheet
 - ▶ Signature: only Alice can add transactions in which Alice sends money
 - ▶ But:
 - ▶ Alice can send money she doesn't have
 - ▶ Alice can send money she does have but to multiple parties at the same time
 - ▶ Alice can delete previous transactions (her own or others').
- ▶ Imagine transactions through a trusted party that keeps track of balances
 - ▶ That works just fine re: security issues listed above
 - ▶ But: requires a trusted party.
 - ▶ (N.B.: central bank digital currency)

What is Nakamoto Blockchain?

Nakamoto (2008) Blockchain Innovation

What is Nakamoto Blockchain?

Nakamoto (2008) Blockchain Innovation

▶ I: Blockchain Data Structure

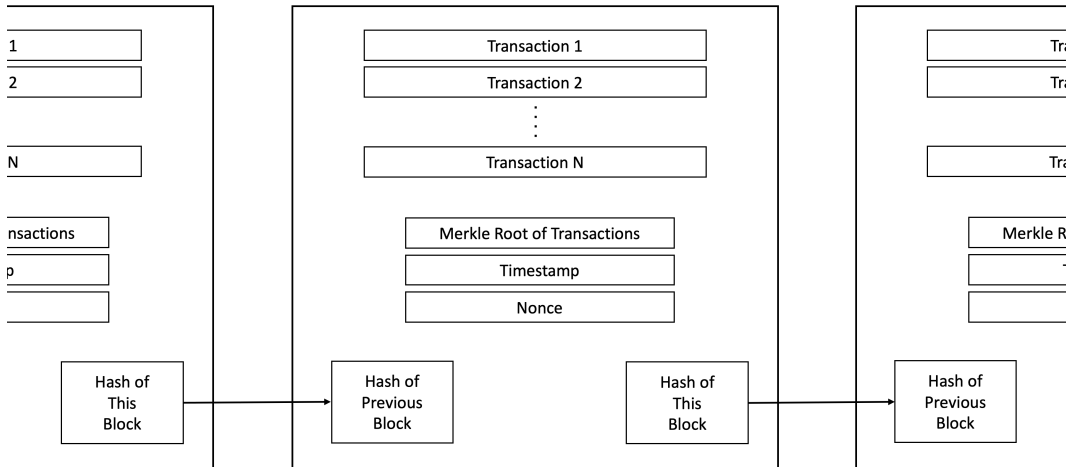
- ▶ Users submit transactions to a pending transactions list, called mempool
- ▶ Computers around the world take turns adding transactions from the mempool to a data structure called the blockchain (will describe turn-taking competition next)
- ▶ Each new block of transactions “chains” to previous block, by including a hash of the data in the previous block (Haber and Stornetta, 1991)

What is Nakamoto Blockchain?

Nakamoto (2008) Blockchain Innovation

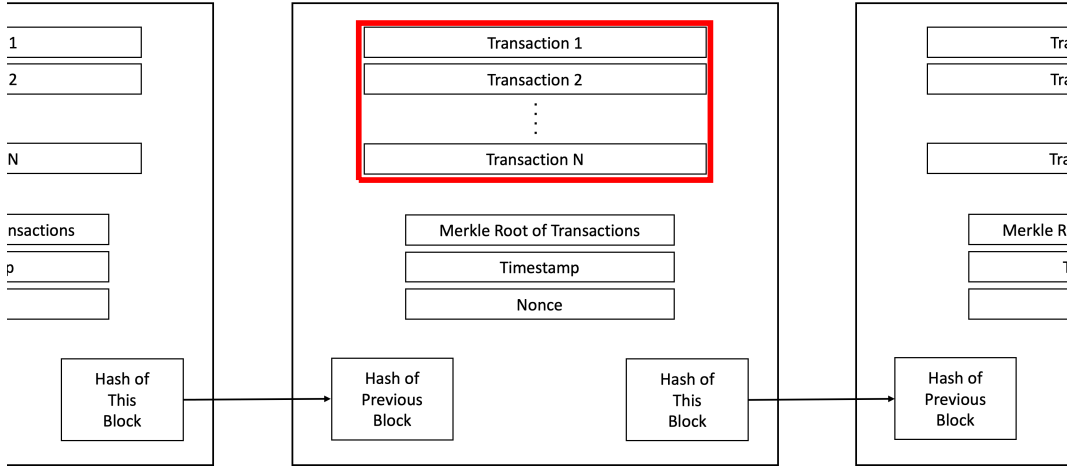
▶ I: Blockchain Data Structure

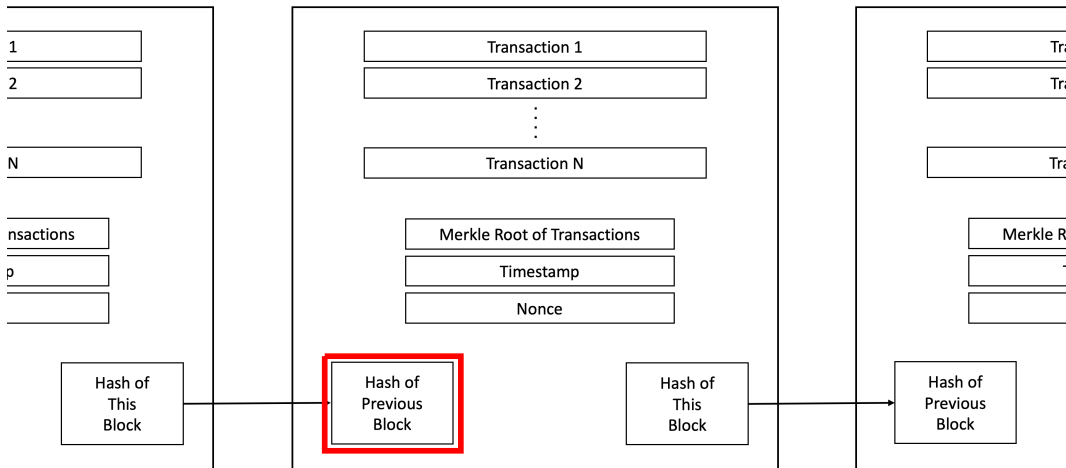
- ▶ Users submit transactions to a pending transactions list, called mempool
- ▶ Computers around the world take turns adding transactions from the mempool to a data structure called the blockchain (will describe turn-taking competition next)
- ▶ Each new block of transactions “chains” to previous block, by including a hash of the data in the previous block (Haber and Stornetta, 1991)
- ▶ Validity: for a block to be valid:
 1. Each individual transaction must be properly signed
 2. Each individual transaction must be funded given previous blocks
 3. No contradictions: there cannot be multiple transactions sending the same funds



Conditions for a Valid Block:

1. Each individual transaction correctly signed,
2. Each individual transaction funded given history,
3. No contradictions in the set of transactions.





Any change to history changes the hash of the previous block.

What is Nakamoto Blockchain?

▶ II: Bitcoin “Mining” Computational Tournament

- ▶ Who gets to add the next block?
- ▶ Boils down to a massive brute-force search for a lucky random alphanumeric string.
- ▶ Free entry, free exit, all anonymous. Anyone can play at any time.

What is Nakamoto Blockchain?

▶ II: Bitcoin “Mining” Computational Tournament

- ▶ Who gets to add the next block?
- ▶ Boils down to a massive brute-force search for a lucky random alphanumeric string.
- ▶ Free entry, free exit, all anonymous. Anyone can play at any time.
- ▶ “Miner” chooses a valid block of transactions from the mempool
- ▶ Then searches for an alphanumeric string (“nonce”), such that, when all of the data is hashed together using SHA-256, the result has a large number of leading zeros.
Example: block 729,999 has the hash

00000000000000000000000008b6f6fb83f8d74512ef1e0af29e642dd20dadd7d318f

What is Nakamoto Blockchain?

▶ II: Bitcoin “Mining” Computational Tournament

- ▶ Who gets to add the next block?
- ▶ Boils down to a massive brute-force search for a lucky random alphanumeric string.
- ▶ Free entry, free exit, all anonymous. Anyone can play at any time.
- ▶ “Miner” chooses a valid block of transactions from the mempool
- ▶ Then searches for an alphanumeric string (“nonce”), such that, when all of the data is hashed together using SHA-256, the result has a large number of leading zeros.
Example: block 729,999 has the hash

00000000000000000000000008b6f6fb83f8d74512ef1e0af29e642dd20daddd7d318f

- ▶ Called “proof of work” – hard to find, easy to check.

What is Nakamoto Blockchain?

▶ II: Bitcoin “Mining” Computational Tournament

- ▶ Who gets to add the next block?
- ▶ Boils down to a massive brute-force search for a lucky random alphanumeric string.
- ▶ Free entry, free exit, all anonymous. Anyone can play at any time.
- ▶ “Miner” chooses a valid block of transactions from the mempool
- ▶ Then searches for an alphanumeric string (“nonce”), such that, when all of the data is hashed together using SHA-256, the result has a large number of leading zeros.
Example: block 729,999 has the hash

00000000000000000000000008b6f6fb83f8d74512ef1e0af29e642dd20daddd7d318f

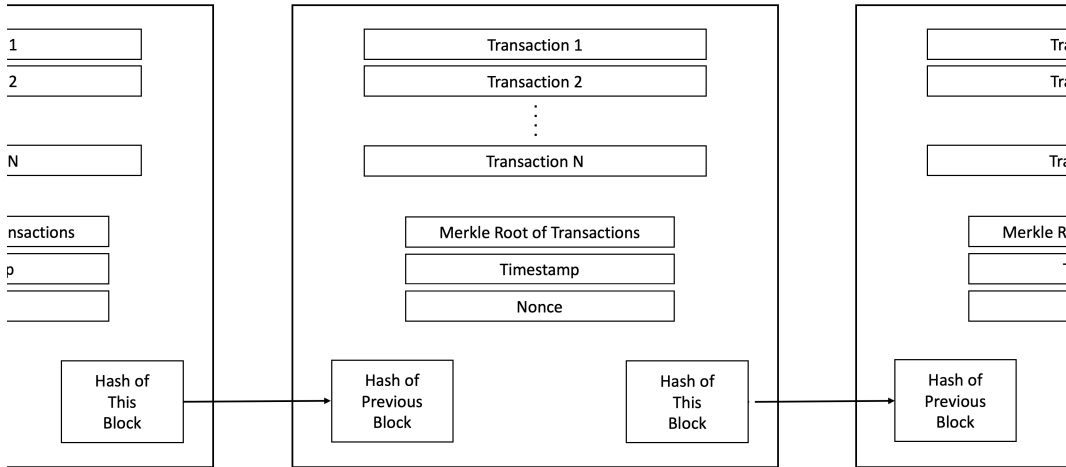
- ▶ Called “proof of work” – hard to find, easy to check.
- ▶ Winner is compensated with newly issued Bitcoins (“mining”) and optional transaction fees (see Huberman, Leshno and Moallemi 2021)
- ▶ Tournament difficulty adjusts every two weeks, calibrated to take about 10 minutes

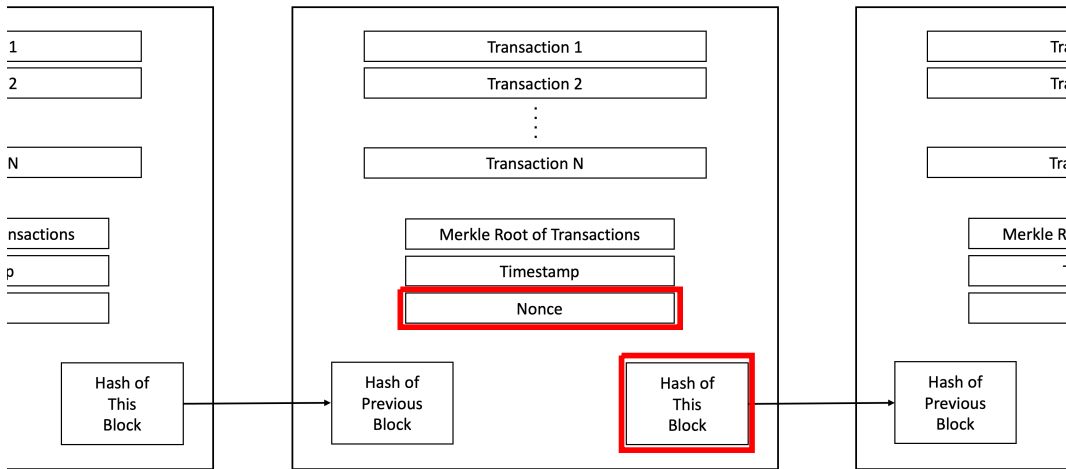
SHA-256 Hash Function: Example

Name	SHA256 Hash	Name	SHA256 Hash
Rodrigo Adao	c43f52b74a1f5424c73f9db2dc9283c6bc5998514c1dcf74dedfed0ddc6daa0f	Harry L. Davis	16bec3fe78ccf3157c0473f5e629d313e363952e9b0589c7eedcd0313e4e522f
Dan Adelman	dd5e6e598a330b24c284a5453b6c39dff4d1c7618fc69393d8e519f74de2e48	Joshua Dean	b01080cb0aa1ff7a2655e0a3ba5f521beda1016e022357a959e316bf06802584
Milena Almagro	27218fcfb01de5f787270d1140e63474b034989c9806d9c05c1da098f2f1a0b1	Levi DeValve	5b46b4f7eb3fb483484e245d01e24144a02b11c264519c2e909547ffeca98c1d
Bryon Aragam	f96deeb5ee3414f9e1354a5c1dc0bd77a29e05d75d269c80d03309372bd34b98	Sanjay K. Dhar	f803ff56de7c6673ba99e7fd9fd548e9ce2b5d925d83aced5e9d8253e272d7ae
Baris Ata	a401e2336dc12710c2c19915cb6032562e625cd69f839dae9ad0e7e438f62e	Douglas W. Diamond	1a7c4d7ea7621974f5d209be0fe70edfa476ca26ea601b3bbf6cc0a076641fb2
Daniel Bartels	d07474851a924a1a12150812e70f73e47fa92ce4904990b1b5e4f3e31cbdcc81	Berkeley J. Dietvorst	2572dca946080e2c36bc7e9ec037b8ae4f2fb9e6ad2a3cbd275e9dd3f07f0328
Francesca Bastianello	bc9fccdce45e25e40900abaeeb0d4421a1fd0553736fb60c980ee0a220fd6c	Jonathan Dinkel	96ca023943b6bf8108e0f520de753625004bed001d4806d976a5a188c97154e9
Philip G. Berger	4b74717d0ac307f003c24129caefdbfb4a69f226be766fb85217ff97cd5381	Rebecca Dizon-Ross	5b22bec6d7ca026cb3fccffdee04fb48494dece486e67331c540228fe85f5962
Marianne Bertrand	0053bc398f704ecd857f6edaac5a8e2ade8c600852dab0e88a85ebf8c787776e	Kristin Donnelly	e3dbe9e581ca5cb81bd48991d5b5562ec74b2bc09d9cdf6f85efd8dc3c286610
John R. Birge	83b8262a785844d002d4d7d9a858572d95a30589f92b624dd6128ff280c6da	Wenxin Du	12af62eea44ad482450d42f443643e5f79a15fca63e1ca9be380e9932e4c4c4
Jonathan Bonham	534c78d299c0f6244b342807d921cd92aded4f3b6093d78d1c13ab37ccab3ec	Jean-Pierre Dubé	65dfa660ab6c36b88c16e4224a7b0f2cc1dae945a4d5143c7326fe74039b98f
Eric Budish	222667cd0f3bb9c5baf1be47ed5f416f6cd2b413c0721a45ad6bae5977867c16	Donald D. Eisenstein	71d8f349834e9c33ce9a0ce9d8f85d9c633044c1667a444f505b39d08fe5b86
Ronald S. Burt	079b2671eaa8a167902cb60c57089a0a3887c9abdb3ba1ed8c912a0807adb6fc2	Nicholas Epley	b7ba97d0003d1194af87f9c6fbc8e542fc634d8d8f8eb43528b3c2947e0b7414
Rene Caldentey	7739ba7a4b39070c733c2d4098ed2e708be374f1b596634d79417121cbc543aa	Merle Erickson	9c781b5004164efc297418ee78548ac0f5a86efbd99641b5e734ff8dfad058c
Christopher Campos	0027d8c4c07cfa45e651340a3537d8ce144b7a986c6d556b9051d5e0f738da	Eugene F. Fama	dfa8a902d7d1c46989702d8a82a6a0abb61e665e2ca9d54bafbc236ca4931185
Ozan Candogan	757600d2582a6ece044e2fb11535ead6ce8d19b44614ba5ba1839fcd1893dc7	Max Farrell	3e04b657a892d71797f816f589a6e182a914954134a7e6f93b22af282a0ce6264
Shereen Chaudhry	d3e486436f351c444240f290f05b451d29958330128297c56e80c02fadfe7376	Ayelet Fishbach	371ca020472baa0cd9e474fda944c1a5eedaaef101ef507ad87add109a6b00
Pradeep K. Chintagunta	2a4fa47da0ff905370af0400f5bd1aa922d423eb952ba305d13d029bbdbbbb7e	Alexander P. Frankel	ada5fe2a27ba40e5a6d17571b35d1d7723f8a762b9565a3fb365b1047ae220c5
Hans B. Christensen	c4b4312f1e29b693c75c4d76f6c00bbb188ec3a23bccb97d77eedc1411ab4c7	Robert H. Gertner	159e8ac6f68530fc786df66bb18e58a4264b4589e37b9c3b300829b5b9d3094d
Emanuele Colonnelli	c7705b0346c15f414e10f0ac38d6dc6d63065881b4387158334945d9cb9c9251	Austan D. Goolsbee	8a41b670e79dfbf787165c19c0052952db44d59b1e7a3e96a3bf4e003905d46
Giovanni Compiani	e8a764369840f37996a3a6ce8521f563be18b44287ef087eaf3600db016bc661	Niels Gormsen	e322ccd5f3095142ace4388412bc2427303b023f1634c1adfa289b72fb39a
George M. Constantinides	f442c6314f9abbfb58566b21f0f8c814fc8eff33ddc02d90f03ed60f7193b221	Joao Granja	4b01bccb1909399c6edff0b89c8854ae67c008ce6690f7c2e3b01ae987557ded
Anna Costello	637fc29b19e98f6a27747e919bd5ad04f374f96194e73b4e7873a16ee8598f04	Veronica Guerrieri	aea43bc44f75d217fd4cbd9c6d0840976403d62bec01cd879216561615b11f
Thomas Covert	b33f79d2ef516c1c0cfe1d0a6e1ad1b9b4ad9fc6195c78fce919685538cd4b2	Varun Gupta	06a075106b1a472fd4db2fab33bf6900772bbec6190192778a49ced4a3f7b50f
Steven J. Davis	1174d6553bf7499383bd3ab7f527cdfac630c229ee75b90e036ff6f60516db0a	Lars Hansen	9ee2fd4f9fce186e157ee9cddee2e2ad28edab2bba1b86edca2d66648e3f9930

SHA-256 Hash Function: Example

Name	SHA256 Hash	Name	SHA256 Hash
Rodrigo Adao	c43f52b74a1f5424c73f9db2dc9283c6bc5998514c1dcf74dedfed0ddc6daa0f	Harry L. Davis	16bec3fe78ccf3157c0473f5e629d313e363952e9b0589c7eedcd0313e4e522f
Dan Adelman	dd5e6e598a330b24c284a5453b6c39dff4d1c7618fc69393d8e519f74de2e48	Joshua Dean	b01080cb0aa1ff7a2655e0a3ba5f21beda1016e022357a959e316bf06802584
Milena Almagro	27218fcb01de5787270d1140e63474b034989c9806d9c05c1da098d2f1a0b1	Levi DeValve	5b46b4f7eb3fb483484e245d01e24144a02b1e2164519c2e909547ffeca98c1d
Bryon Aragam	f96deeb5ee3414f9e1354a5c1dc0bd77a29e05d75d269c80d03309372bd34b98	Sanjay K. Dhar	f803ff56de7c667b3a99e7fd9fd548e9ce2b5d925d83aced5e9d8253e272d7ae
Baris Ata	a401e2336dc12710c2c19915cb6032562e625cd69f839dae9ad0e7e438f62e	Douglas W. Diamond	1a7c4d7ea7621974f5d209be0fe70edfa476ca26ea601b3bbf6cca0076641fb2
Daniel Bartels	d07474851a924a1a12150812e70f73e47fa92ce4904990b1b5e4f3e31cbdccc81	Berkeley J. Dietvorst	2572dca946080e2c36bc7e9ec037b8ae4f2fb9e6ad2a3c3bd275e9dd3f07f0328
Francesca Bastianello	bc9fccdce45e25e40900abaeb0d4421a1fd0553736fb6c980ee0a220fd6c	Jonathan Dingel	96ca023943b6bf8108e0f520de753625004bed001d4806d976a5a188c971514e9
Philip G. Berger	4b74717d0ac307f003c24129caefdbfb4a69f226be766fb85217f9b7cd5381	Rebecca Dizon-Ross	5b22bec6d7ca0263cfccffdee04fb48494dece486e67331c540228f85f5962
* Marianne Bertrand	0053bc398f704ecd857f6edaac5a8e2ade8c600852dab0e88a8ebf86c78776e *	Kristin Donnelly	e3dbe9e581ca5cb81bd48991d5b5562ec74b2bc09d9cdf6f85efd8d3c286610
John R. Birge	83b8262a785844d002d4d7d9a85872d95a30589f92b624dd64128ff280c6da	Wenxin Du	12af62ee44ad482450d42f443643c5f79a15fca63e1ca9be380e9932e4c4c4
Jonathan Bonham	534c78d299c0f6244b342807d921cd92aded4f3b6093d78d1c13ab378ccab3ec	Jean-Pierre Dubé	65dfa660ab6c36b88c16e4224a7b0f2cc1dae945a4d5143c7326fe74039b98f
Eric Budish	222667cd0f3bb9c5baf1be47ed5f416f6cd2b413c0721a45ad6bae5977867c16	Donald D. Eisenstein	71d8f349834e9c33ce9a0ce9d8f85d9c633044c1667a444f505b39d08fe5b86
Ronald S. Burt	079b2671eaa8a167902bc60c57089a0a3887c9abd3ba1ed8c912a0807adb6fc2	Nicholas Epley	b7ba97d0003d1194af87f9c6fbc8e542fc634d8d8f8eb43528b3b2947e0b7414
Rene Caldentey	7739ba7a4b39070c733c2d4098ed2e708be374f1b59d6634d79417121c3c543aa	Merle Erickson	9c781b5004164efc297418ee78548ac0f5a86efbd99641b5e734ff8d1fad058c
* * Christopher Campos	0027d8c4c07cfa45e651340a3537d8ce144b7a986cd556b9051d5e0f738ada * *	Eugene F. Fama	dfa8a902d7d1c46989702d8a82a6a0abb61e6652ca9d54abfc236ca4931185
Ozan Candogan	757600d2582a6ece044e2fb11535ead6ce8d19b44614ba5ba1839cdf1893dc7	Max Farrell	3e04b657a892d717f97816f589a6182a291495413a7e6f93b22af282a0ce6264
Shereen Chaudhry	d3e486436f351c44240f290f05b451d29958330128297c56e80c02fadfe7376	Ayelet Fishbach	371ca020472baa0cd9e474fda944c1a5eedaaef101ef507ad87add109a6b00
Pradeep K. Chintagunta	2a4fa47da0f905370af0400f5bd1aa922d423eb952ba305d13c029b9dbbbb7e	Alexander P. Frankel	ada5fe2a27ba40e5a6d17571b35d1d7723f8a762b9565a3fb365b1047ae220c5
Hans B. Christensen	c4b4312f1e29b693c75c4d76f6c00bbb188ec3a23bccb97d77eedc1411ab4c7	Robert H. Gertner	159e8ac6f68530fc786df6bb18e58a4264b4589e37b9c3b300829b5b9d3094d
Emanuele Colonnelli	c7705b0346c15f414e10f0ac38d6dc60d63065881b4387158334945d9cb9c9251	Austan D. Goolsbee	8a41b670e79dfbf787165c19c0052952db44d59b1e7a3e96a3bf4e0c9305d46
Giovanni Compiani	e8a764369840f37996a3a6ce8521f563be18b44287ef087eaf3600db016bc661	Niels Gormsen	e322ccd5f3095142ace4388412bc2427303b023f1634c1adfa289b72fb39a
George M. Constantinides	f442c6314f9abbfb5856b621f0f8c814fc8eff33ddc02d90f03ed60f7193b221	Joao Granja	4b01bccb1909399c6edff0b89c8854ae67c008ce6690f7c2e3b01ae987557ded
Anna Costello	637fc29b19e98f6a27747e919bd5ad04f374f96194e73b4e7873a16ee8598f04	Veronica Guerrieri	aea43bc44f75d217fd4cbd9c6d0840976403d62bec01cd1789216561615b11f
Thomas Covert	b33f79d2ef516c1c0fce1d0a6e1ad1b9b4ad9f6c195c78fce919685538cd4b2	Varun Gupta	06a075106b1a472f4db2fab33bf69007772bbe6190192778a49ced4a3f7b50f
Steven J. Davis	1174d6553b7499383bd3ab7f527cdfac630c229ee7b590e036ff6f60516db0a	Lars Hansen	9ee2fd49fce186e157ee9cddde2e2ad28edab2bba1b86edca2d66648e3f9930





Hash of block data must have a very large number of leading zeros.

Example from Block 729,999:

- Hash: 00000000000000000000000008b6f6fb83f8d745...

What is Nakamoto Blockchain?

▶ III: Longest-Chain Consensus

- ▶ Once a miner finds a lucky alphanumeric string, all participants are supposed to move on to the next block
- ▶ To induce this, Nakamoto proposed the longest-chain convention: *the official consensus record of transactions is the longest chain, as measured by the amount of computational work*

What is Nakamoto Blockchain?

▶ III: Longest-Chain Consensus

- ▶ Once a miner finds a lucky alphanumeric string, all participants are supposed to move on to the next block
- ▶ To induce this, Nakamoto proposed the longest-chain convention: *the official consensus record of transactions is the longest chain, as measured by the amount of computational work*
- ▶ Intuition #1: as long as a majority of mining power is “honest” and follows the longest chain, then the longest chain will stay longest with probability one
 - ▶ Computing power like “votes” -> enables decentralized adjudication of which is the official chain if there are multiple
- ▶ Intuition #2: need some decentralized way to coordinate miner's efforts
 - ▶ Honest mining is a Nash equilibrium of Nakamoto longest-chain if all miners are “small” (Kroll et al. (2013), Carlsten et al. (2016), Biais et al. (2019))

What is Nakamoto Blockchain?

▶ III: Longest-Chain Consensus

- ▶ Once a miner finds a lucky alphanumeric string, all participants are supposed to move on to the next block
- ▶ To induce this, Nakamoto proposed the longest-chain convention: *the official consensus record of transactions is the longest chain, as measured by the amount of computational work*
- ▶ Intuition #1: as long as a majority of mining power is “honest” and follows the longest chain, then the longest chain will stay longest with probability one
 - ▶ Computing power like “votes” -> enables decentralized adjudication of which is the official chain if there are multiple
- ▶ Intuition #2: need some decentralized way to coordinate miner's efforts
 - ▶ Honest mining is a Nash equilibrium of Nakamoto longest-chain if all miners are “small” (Kroll et al. (2013), Carlsten et al. (2016), Biais et al. (2019))
- ▶ But note: vulnerable to attack by a 51% majority. Can outpace honest miners with probability one.

What is Nakamoto Blockchain: Summary

- ▶ From the Nakamoto (2008) abstract:

What is Nakamoto Blockchain: Summary

- From the Nakamoto (2008) abstract:

"We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain serves not only as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power.

What is Nakamoto Blockchain: Summary

- From the Nakamoto (2008) abstract:

"We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an on-going chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain serves not only as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers." (Emphasis added)

What is Nakamoto Blockchain: Summary

- ▶ From the Nakamoto (2008) abstract:

"We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an on-going chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain serves not only as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers." (Emphasis added)

- ▶ The abstract succinctly summarizes the accomplishment and its vulnerability:

What is Nakamoto Blockchain: Summary

- ▶ From the Nakamoto (2008) abstract:

"We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an on-going chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain serves not only as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers." (Emphasis added)

- ▶ The abstract succinctly summarizes the accomplishment and its vulnerability:
 - ▶ Anonymous, decentralized trust. (A "purely peer-to-peer version of electronic cash" without "a trusted third party ... to prevent double-spending")

What is Nakamoto Blockchain: Summary

- ▶ From the Nakamoto (2008) abstract:

"We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an on-going chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain serves not only as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers." (Emphasis added)

- ▶ The abstract succinctly summarizes the accomplishment and its vulnerability:
 - ▶ Anonymous, decentralized trust. (A "purely peer-to-peer version of electronic cash" without "a trusted third party ... to prevent double-spending")
 - ▶ But, vulnerable to majority attack.

Clarification I: “Permissioned Blockchains”

- ▶ After interest in cryptocurrencies first surged, some started to use the phrase “blockchain” to describe distributed databases among *known, trusted parties supported by rule of law* – that is, *without* the central scientific innovation of Nakamoto (2008)

Clarification I: “Permissioned Blockchains”

- ▶ After interest in cryptocurrencies first surged, some started to use the phrase “blockchain” to describe distributed databases among *known, trusted parties supported by rule of law* – that is, *without* the central scientific innovation of Nakamoto (2008)

“If you announce that you are updating the database software used by a consortium of banks to track derivatives trades, the New York Times will not write an article about it. If you say that you are blockchaining the blockchain software used by a blockchain of blockchains to blockchain blockchain blockchains, the New York Times will blockchain a blockchain about it.” (Matt Levine, 2017)

Clarification I: “Permissioned Blockchains”

- ▶ After interest in cryptocurrencies first surged, some started to use the phrase “blockchain” to describe distributed databases among *known, trusted parties supported by rule of law* – that is, *without* the central scientific innovation of Nakamoto (2008)

“If you announce that you are updating the database software used by a consortium of banks to track derivatives trades, the New York Times will not write an article about it. If you say that you are blockchaining the blockchain software used by a blockchain of blockchains to blockchain blockchain blockchains, the New York Times will blockchain a blockchain about it.” (Matt Levine, 2017)

- ▶ This paper’s critique is of blockchains and permissionless consensus in the sense of Nakamoto (2008)
- ▶ Will come back later to whether there is anything economically interesting about permissioned blockchains.

Clarification II: “Smart Contracts”

- ▶ Notice that Nakamoto's novel form of trust isn't specific to currency transactions

Clarification II: “Smart Contracts”

- ▶ Notice that Nakamoto’s novel form of trust isn’t specific to currency transactions
- ▶ Can replace “Alice sends Bob 10 BTC, signed by Alice” with any executable computer instruction signed by Alice.

Clarification II: “Smart Contracts”

- ▶ Notice that Nakamoto’s novel form of trust isn’t specific to currency transactions
- ▶ Can replace “Alice sends Bob 10 BTC, signed by Alice” with any executable computer instruction signed by Alice.
- ▶ This idea is often called “smart contracts”. Analysis framework of this paper applies analogously
 - ▶ Though attack possibilities will differ (e.g., no such thing as double spending per se if the code is not executing currency transactions).

Clarification III: Proof of Stake

- ▶ “Proof of Stake” as opposed to Proof of Work
- ▶ Roughly: instead of voting for the correct chain with computational work, vote with stake in the cryptocurrency
 - ▶ Ethereum recently switched from proof-of-work to proof-of-stake
 - ▶ Several other blockchains use proof-of-stake

Clarification III: Proof of Stake

- ▶ “Proof of Stake” as opposed to Proof of Work
- ▶ Roughly: instead of voting for the correct chain with computational work, vote with stake in the cryptocurrency
 - ▶ Ethereum recently switched from proof-of-work to proof-of-stake
 - ▶ Several other blockchains use proof-of-stake
- ▶ This paper’s main three-equation critique applies to all forms of permissionless consensus (work, stake, etc.)

Clarification III: Proof of Stake

- ▶ “Proof of Stake” as opposed to Proof of Work
- ▶ Roughly: instead of voting for the correct chain with computational work, vote with stake in the cryptocurrency
 - ▶ Ethereum recently switched from proof-of-work to proof-of-stake
 - ▶ Several other blockchains use proof-of-stake
- ▶ This paper’s main three-equation critique applies to all forms of permissionless consensus (work, stake, etc.)
- ▶ There is a subtle security advantage to stake over work that I will come back to later in the talk
 - ▶ (Recent work of Tas et al, 2023; Budish, Lewis-Pye, and Roughgarden 2024).

Overview of the Talk

Part I: Trust at Scale

- ▶ Overview of Nakamoto (2008) and Related Concepts
- ▶ **Nakamoto Trust: A Critique in 3 Equations**
- ▶ Analysis of Double-Spending Attacks
- ▶ A Way Out: Specific Capital + Collapse
- ▶ Comparison of Nakamoto Trust and Traditional Trust
- ▶ Summary of “Trust at Scale”

Part II: Directions for Research

Conclusion

Zero-Profit Condition (Honest Play)

- ▶ Conceptual question: how much “trust support” will maintain the permissionless consensus if we restrict all to behave honestly?

Zero-Profit Condition (Honest Play)

- ▶ Conceptual question: how much “trust support” will maintain the permissionless consensus if we restrict all to behave honestly?
- ▶ N : amount of trust support (computing power, stake)
 - ▶ Large finite number of honest participants
 - ▶ Follow the permissionless consensus protocol automatically
 - ▶ Player i chooses qty of trust support x_i . Define $N = \sum_i x_i$.
 - ▶ Eqm concept will be zero-profit. Captures permissionless, free entry/exit.

Zero-Profit Condition (Honest Play)

- ▶ Conceptual question: how much “trust support” will maintain the permissionless consensus if we restrict all to behave honestly?
- ▶ N : amount of trust support (computing power, stake)
 - ▶ Large finite number of honest participants
 - ▶ Follow the permissionless consensus protocol automatically
 - ▶ Player i chooses qty of trust support x_i . Define $N = \sum_i x_i$.
 - ▶ Eqm concept will be zero-profit. Captures permissionless, free entry/exit.
- ▶ c : cost per unit time to provide one unit of trust support
 - ▶ For proof-of-work, this would include rental cost of capital and variable costs of electricity ($c = rC + \eta$)
 - ▶ For proof-of-stake, this would be a rental cost of capital

Zero-Profit Condition (Honest Play)

- ▶ Conceptual question: how much “trust support” will maintain the permissionless consensus if we restrict all to behave honestly?
- ▶ N : amount of trust support (computing power, stake)
 - ▶ Large finite number of honest participants
 - ▶ Follow the permissionless consensus protocol automatically
 - ▶ Player i chooses qty of trust support x_i . Define $N = \sum_i x_i$.
 - ▶ Eqm concept will be zero-profit. Captures permissionless, free entry/exit.
- ▶ c : cost per unit time to provide one unit of trust support
 - ▶ For proof-of-work, this would include rental cost of capital and variable costs of electricity ($c = rC + \eta$)
 - ▶ For proof-of-stake, this would be a rental cost of capital
- ▶ p_{block} : compensation per block paid to the player that adds the next block
 - ▶ Assume exogenous. Will derive constraints below.
 - ▶ Proportional rule: player i wins a given block with prob. $\frac{x_i}{N}$

Zero-Profit Condition (Honest Play)

- ▶ D : block difficulty level. Defined as how many units of trust-support-time are needed in expectation to add one new block
- ▶ Definition. A *zero-profit honest Nakamoto trust equilibrium* consists of quantities $\{x_i^*\}_{i=1}^I$ and a difficulty level D^* such that participants (i) add one block per unit time (as a normalization), and (ii) earn zero economic profits in expectation.

Zero-Profit Condition (Honest Play)

- ▶ D : block difficulty level. Defined as how many units of trust-support-time are needed in expectation to add one new block
- ▶ Definition. A *zero-profit honest Nakamoto trust equilibrium* consists of quantities $\{x_i^*\}_{i=1}^I$ and a difficulty level D^* such that participants (i) add one block per unit time (as a normalization), and (ii) earn zero economic profits in expectation.
- ▶ Proposition: Let $N^* = \sum_{i=1}^I x_i^*$. In any zero-profit honest Nakamoto trust equilibrium, $D^* = N^*$ and

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

Zero-Profit Condition (Honest Play)

- ▶ D : block difficulty level. Defined as how many units of trust-support-time are needed in expectation to add one new block
- ▶ Definition. A *zero-profit honest Nakamoto trust equilibrium* consists of quantities $\{x_i^*\}_{i=1}^I$ and a difficulty level D^* such that participants (i) add one block per unit time (as a normalization), and (ii) earn zero economic profits in expectation.
- ▶ Proposition: Let $N^* = \sum_{i=1}^I x_i^*$. In any zero-profit honest Nakamoto trust equilibrium, $D^* = N^*$ and

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

- ▶ Note: (1) widely known (many prior papers). Standard rent-seeking tournament
- ▶ Note: if use Nash eqm, still restrict to honest play, very similar

Incentive Compatibility Condition (Majority Attack)

- ▶ Conceptual question: how much security is generated by the amount of honest trust support in (1)?

Incentive Compatibility Condition (Majority Attack)

- ▶ Conceptual question: how much security is generated by the amount of honest trust support in (1)?
- ▶ Vulnerability: “majority attack”
 - ▶ Well-known Achilles’ heel of permissionless consensus.
 - ▶ Intuition: need majority or super-majority to adjudicate the state if there is a dispute

Incentive Compatibility Condition (Majority Attack)

- ▶ Conceptual question: how much security is generated by the amount of honest trust support in (1)?
- ▶ Vulnerability: “majority attack”
 - ▶ Well-known Achilles’ heel of permissionless consensus.
 - ▶ Intuition: need majority or super-majority to adjudicate the state if there is a dispute
- ▶ In Nakamoto (2008) abstract (as quoted above)
- ▶ Not surprising. Same issues in 1980’s CS literature on what is now called *permissioned* consensus (Lamport et al 1982, Dwork et al 1988)

Incentive Compatibility Condition (Majority Attack)

- ▶ Conceptual question: how much security is generated by the amount of honest trust support in (1)?
- ▶ Vulnerability: “majority attack”
 - ▶ Well-known Achilles’ heel of permissionless consensus.
 - ▶ Intuition: need majority or super-majority to adjudicate the state if there is a dispute
- ▶ In Nakamoto (2008) abstract (as quoted above)
- ▶ Not surprising. Same issues in 1980’s CS literature on what is now called *permissioned* consensus (Lamport et al 1982, Dwork et al 1988)
- ▶ But: with *permissionless* consensus, one has to ask what is an attacker’s *incentive* to become a majority

Incentive Compatibility Condition (Majority Attack)

- ▶ Attack costs
 - ▶ Consider an additional player, the attacker, not restricted to honest play.
 - ▶ Can attack by choosing AN^* units of trust support, $A > 1$, for an $\frac{A}{A+1}$ majority
 - ▶ Cost per unit time: AN^*c
 - ▶ Expected duration of attack: $t(A)$. Timing details of attacks will vary by protocol.
 - ▶ Call $AN^*c \cdot t(A)$ the gross cost of attack.
 - ▶ Attacker can minimize $A \cdot t(A)$: call this $A^* \cdot t(A^*)$

Incentive Compatibility Condition (Majority Attack)

- ▶ Attack costs
 - ▶ Consider an additional player, the attacker, not restricted to honest play.
 - ▶ Can attack by choosing AN^* units of trust support, $A > 1$, for an $\frac{A}{A+1}$ majority
 - ▶ Cost per unit time: AN^*c
 - ▶ Expected duration of attack: $t(A)$. Timing details of attacks will vary by protocol.
 - ▶ Call $AN^*c \cdot t(A)$ the gross cost of attack.
 - ▶ Attacker can minimize $A \cdot t(A)$: call this $A^* \cdot t(A^*)$
- ▶ Attack benefits
 - ▶ Let V_{attack} denote the value of an attack
 - ▶ For now, abstract. Will derive a constraint in relation to p_{block}
 - ▶ Should have in mind that the value of attack will grow as the blockchain's economic usefulness grows.

Incentive Compatibility Condition (Majority Attack)

- ▶ Attack costs
 - ▶ Consider an additional player, the attacker, not restricted to honest play.
 - ▶ Can attack by choosing AN^* units of trust support, $A > 1$, for an $\frac{A}{A+1}$ majority
 - ▶ Cost per unit time: AN^*c
 - ▶ Expected duration of attack: $t(A)$. Timing details of attacks will vary by protocol.
 - ▶ Call $AN^*c \cdot t(A)$ the gross cost of attack.
 - ▶ Attacker can minimize $A \cdot t(A)$: call this $A^* \cdot t(A^*)$
- ▶ Attack benefits
 - ▶ Let V_{attack} denote the value of an attack
 - ▶ For now, abstract. Will derive a constraint in relation to p_{block}
 - ▶ Should have in mind that the value of attack will grow as the blockchain's economic usefulness grows.
- ▶ Definition. Nakamoto trust is *incentive compatible against an outsider attack*, on a *gross-cost basis*, if the gross cost of attack exceeds the benefits of attack:

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

Incentive Compatibility Condition (Majority Attack)

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

► Remarks

Incentive Compatibility Condition (Majority Attack)

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

- ▶ Remarks
- ▶ Inside vs. Outside Attacker
 - ▶ (2) is the IC for an outside attacker.
 - ▶ An attack could also come from the inside — part of the current honest trust support. Cheaper: as little as $\frac{N^* c}{2}$ per unit time
 - ▶ Outside attacker seems more attractive as a conceptual approach. Treats the honest players as “small” which is the Nakamoto ideal. Honest as an atomless continuum that behaves automatically, fluctuates in size with p .
 - ▶ Inside attacker might be more realistic in practice. Cheaper, already have the equipment / stake (Makarov and Schoar; Cong, He and Li)

Incentive Compatibility Condition (Majority Attack)

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

- ▶ Remarks
- ▶ Inside vs. Outside Attacker
 - ▶ (2) is the IC for an outside attacker.
 - ▶ An attack could also come from the inside — part of the current honest trust support. Cheaper: as little as $\frac{N^* c}{2}$ per unit time
 - ▶ Outside attacker seems more attractive as a conceptual approach. Treats the honest players as “small” which is the Nakamoto ideal. Honest as an atomless continuum that behaves automatically, fluctuates in size with p .
 - ▶ Inside attacker might be more realistic in practice. Cheaper, already have the equipment / stake (Makarov and Schoar; Cong, He and Li)
- ▶ Gross vs. Net Cost
 - ▶ (2) is a gross cost. Attacker would earn block rewards for the blocks in their new chain, so Net < Gross. Will come back to this.

Equilibrium Constraint

The Problem

Equilibrium Constraint

The Problem

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

Equilibrium Constraint

The Problem

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

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

Equilibrium Constraint

The Problem

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

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

- Theorem. *The zero-profit condition (1) and gross incentive-compatibility condition (2) together imply the equilibrium constraint:*

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

In words: the equilibrium per-block payment to trust-support providers for maintaining the blockchain (“flow cost of trust”) has to be large relative to the benefits of attacking the blockchain

Equilibrium Constraint

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

► Remarks:

Equilibrium Constraint

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

- ▶ Remarks:
- ▶ 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.

Equilibrium Constraint

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

- ▶ Remarks:
- ▶ 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.
- ▶ Computer Security: security is *linear* in amount of cpu power.
 - ▶ Example: a \$1B attack is 1000x more expensive to prevent than a \$1M attack.
 - ▶ Usual alternatives: cryptography, laws. Convex returns (analogy: lock on a door)
 - ▶ Imagine a company only as secure as the \$ value of its cpu power.

Net Cost of Attack and a “Zero” Theorem

- ▶ What I will call net cost of attack differs from gross costs for three reasons

Net Cost of Attack and a “Zero” Theorem

- ▶ What I will call net cost of attack differs from gross costs for three reasons
 - ▶ Reason 1: Attacker earns block rewards from the attack

Net Cost of Attack and a “Zero” Theorem

- ▶ What I will call net cost of attack differs from gross costs for three reasons
 - ▶ Reason 1: Attacker earns block rewards from the attack
 - ▶ Reason 2: Attacker may face frictions relative to honest trust support

Net Cost of Attack and a “Zero” Theorem

- ▶ What I will call net cost of attack differs from gross costs for three reasons
 - ▶ Reason 1: Attacker earns block rewards from the attack
 - ▶ Reason 2: Attacker may face frictions relative to honest trust support
 - ▶ Reason 3: Attack may harm post-attack value of the cryptocurrency

Net Cost of Attack and a “Zero” Theorem

- ▶ Theorem: *if the attack concludes before difficulty adjusts ($D' = N^*$), the attacker's cost is the same as honest participants ($\kappa = 0$), and the attack does not cause the value of the cryptocurrency to fall ($\Delta_{\text{attack}} = 0$), then the net cost of attack is zero.*

Net Cost of Attack and a “Zero” Theorem

- ▶ Theorem: *if the attack concludes before difficulty adjusts ($D' = N^*$), the attacker's cost is the same as honest participants ($\kappa = 0$), and the attack does not cause the value of the cryptocurrency to fall ($\Delta_{\text{attack}} = 0$), then the net cost of attack is zero.*
- ▶ Proof:
 - ▶ Computational cost of attack: $(1 + \kappa)At \cdot N^*c$
 - ▶ Net value of block rewards: $At \cdot \frac{N^*}{D'} p_{\text{block}}(1 - \Delta_{\text{attack}})$
 - ▶ If $\kappa = \Delta_{\text{attack}} = 0$, $D' = N^*$, and using equation (1), then computational costs less net value of block rewards is

$$At \cdot N^*c - At \cdot N^*c = 0$$

Net Cost of Attack and a “Zero” Theorem

- ▶ Theorem: *if the attack concludes before difficulty adjusts ($D' = N^*$), the attacker's cost is the same as honest participants ($\kappa = 0$), and the attack does not cause the value of the cryptocurrency to fall ($\Delta_{\text{attack}} = 0$), then the net cost of attack is zero.*
- ▶ Proof:
 - ▶ Computational cost of attack: $(1 + \kappa)At \cdot N^*c$
 - ▶ Net value of block rewards: $At \cdot \frac{N^*}{D'} p_{\text{block}}(1 - \Delta_{\text{attack}})$
 - ▶ If $\kappa = \Delta_{\text{attack}} = 0$, $D' = N^*$, and using equation (1), then computational costs less net value of block rewards is

$$At \cdot N^*c - At \cdot N^*c = 0$$

- ▶ Intuition: attacker is fully compensated for their trust-support costs for same reason as honest players are fully compensated for their costs under honest play.
- ▶ Gans and Halaburda (2024): generalize the result, give conditions under which the net cost of attack is in fact negative

A One-Shot Game Version of (1)-(3)

- ▶ Some of the complexity in analysis relates to timing issues and/or conventions specific to Bitcoin
- ▶ Consider instead the following simplified one-shot game

A One-Shot Game Version of (1)-(3)

- ▶ Some of the complexity in analysis relates to timing issues and/or conventions specific to Bitcoin
- ▶ Consider instead the following simplified one-shot game
- ▶ I “nodes”. (Work, stake, etc.)
- ▶ Each node i chooses:
 - ▶ Quantity x_i
 - ▶ Posture $a_i \in \{Honest, Attack\}$

A One-Shot Game Version of (1)-(3)

- ▶ Some of the complexity in analysis relates to timing issues and/or conventions specific to Bitcoin
- ▶ Consider instead the following simplified one-shot game
- ▶ I “nodes”. (Work, stake, etc.)
- ▶ Each node i chooses:
 - ▶ Quantity x_i
 - ▶ Posture $a_i \in \{Honest, Attack\}$
- ▶ Cost is c per unit. Define $N = \sum_i x_i$.

A One-Shot Game Version of (1)-(3)

- ▶ Some of the complexity in analysis relates to timing issues and/or conventions specific to Bitcoin
- ▶ Consider instead the following simplified one-shot game
- ▶ I “nodes”. (Work, stake, etc.)
- ▶ Each node i chooses:
 - ▶ Quantity x_i
 - ▶ Posture $a_i \in \{Honest, Attack\}$
- ▶ Cost is c per unit. Define $N = \sum_i x_i$.
- ▶ Payoffs:

A One-Shot Game Version of (1)-(3)

- ▶ Some of the complexity in analysis relates to timing issues and/or conventions specific to Bitcoin
- ▶ Consider instead the following simplified one-shot game
- ▶ I “nodes”. (Work, stake, etc.)
- ▶ Each node i chooses:
 - ▶ Quantity x_i
 - ▶ Posture $a_i \in \{Honest, Attack\}$
- ▶ Cost is c per unit. Define $N = \sum_i x_i$.
- ▶ Payoffs:
 - ▶ If there is a player i with $x_i > \frac{N}{2}$ and $a_i = Attack$: player i gets V_{attack}

A One-Shot Game Version of (1)-(3)

- ▶ Some of the complexity in analysis relates to timing issues and/or conventions specific to Bitcoin
- ▶ Consider instead the following simplified one-shot game
- ▶ I “nodes”. (Work, stake, etc.)
- ▶ Each node i chooses:
 - ▶ Quantity x_i
 - ▶ Posture $a_i \in \{Honest, Attack\}$
- ▶ Cost is c per unit. Define $N = \sum_i x_i$.
- ▶ Payoffs:
 - ▶ If there is a player i with $x_i > \frac{N}{2}$ and $a_i = Attack$: player i gets V_{attack}
 - ▶ Else: each player i gets $\frac{x_i}{N}p$

A One-Shot Game Version of (1)-(3)

- ▶ Question: under what conditions is there a Nash equilibrium $(x_i^*, a_i^*)_{i=1}^I$ in which all players i choose $a_i^* = \textit{Honest}$?

A One-Shot Game Version of (1)-(3)

- ▶ Question: under what conditions is there a Nash equilibrium $(x_i^*, a_i^*)_{i=1}^I$ in which all players i choose $a_i^* = \textit{Honest}$?
- ▶ Lemma. If there is an honest equilibrium, then $N^*c \leq p$. (Analog of (1))

A One-Shot Game Version of (1)-(3)

- ▶ Question: under what conditions is there a Nash equilibrium $(x_i^*, a_i^*)_{i=1}^I$ in which all players i choose $a_i^* = \textit{Honest}$?
- ▶ Lemma. If there is an honest equilibrium, then $N^*c \leq p$. (Analog of (1))
- ▶ Proposition. A necessary condition for the existence of an honest equilibrium is $p \geq \frac{V_{\textit{attack}}}{1 + \frac{1}{I}}$. As $I \rightarrow \infty$ this becomes $p \geq V_{\textit{attack}}$ (Analog of (3))

A One-Shot Game Version of (1)-(3)

- ▶ Question: under what conditions is there a Nash equilibrium $(x_i^*, a_i^*)_{i=1}^I$ in which all players i choose $a_i^* = \text{Honest}$?
- ▶ Lemma. If there is an honest equilibrium, then $N^*c \leq p$. (Analog of (1))
- ▶ Proposition. A necessary condition for the existence of an honest equilibrium is $p \geq \frac{V_{\text{attack}}}{1 + \frac{1}{I}}$. As $I \rightarrow \infty$ this becomes $p \geq V_{\text{attack}}$ (Analog of (3))
- ▶ Proof of Theorem.
 - ▶ Honest play payoff for i : $\frac{x_i^*}{N^*}p - x_i^*c$
 - ▶ Attack payoff for i : $V_{\text{attack}} - N_{j \neq i}^*c$
 - ▶ Need: $V_{\text{attack}} - N_{j \neq i}^*c \leq \frac{x_i^*}{N^*}p - x_i^*c$. (analog of (2))
 - ▶ Rearrange and use Lemma: $V_{\text{attack}} \leq p + \frac{x_i^*}{N^*}p$
 - ▶ Using smallest x_i^* : $V_{\text{attack}} \leq p(1 + \frac{1}{I})$. QED.

Graphic Novel Version of the Argument



Traditional Trust



Traditional Trust



Traditional Trust



Traditional Trust Model:

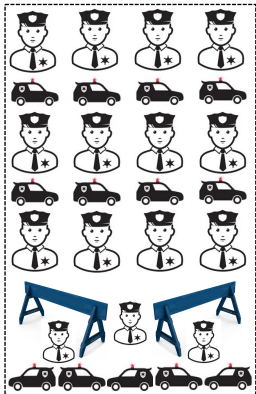
Traditional Trust



Traditional Trust Model:

- ▶ Security Guards

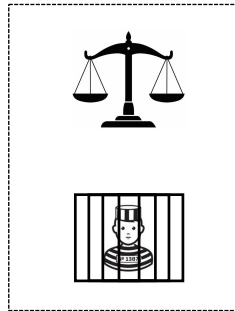
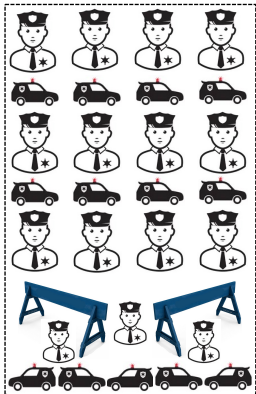
Traditional Trust



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

Overview of the Talk

Part I: Trust at Scale

- ▶ Overview of Nakamoto (2008) and Related Concepts
- ▶ Nakamoto Trust: A Critique in 3 Equations
- ▶ **Analysis of Double-Spending Attacks**
- ▶ A Way Out: Specific Capital + Collapse
- ▶ Comparison of Nakamoto Trust and Traditional Trust
- ▶ Summary of “Trust at Scale”

Part II: Directions for Research

Conclusion

What Can An Attacker Do?

- ▶ A majority attacker can

What Can An Attacker Do?

- ▶ A majority attacker can
 - ▶ Solve computational puzzles faster, in expectation, than the honest minority

What Can An Attacker Do?

- ▶ A majority attacker can
 - ▶ Solve computational puzzles faster, in expectation, than the honest minority
 - ▶ Create an alternative longest chain, replace the honest chain at a strategically opportune moment

What Can An Attacker Do?

- ▶ A majority attacker can
 - ▶ Solve computational puzzles faster, in expectation, than the honest minority
 - ▶ Create an alternative longest chain, replace the honest chain at a strategically opportune moment
- ▶ This allows the attacker to:

What Can An Attacker Do?

- ▶ A majority attacker can
 - ▶ Solve computational puzzles faster, in expectation, than the honest minority
 - ▶ Create an alternative longest chain, replace the honest chain at a strategically opportune moment
- ▶ This allows the attacker to:
 - ▶ Control what transactions get added to the blockchain

What Can An Attacker Do?

- ▶ A majority attacker can
 - ▶ Solve computational puzzles faster, in expectation, than the honest minority
 - ▶ Create an alternative longest chain, replace the honest chain at a strategically opportune moment
- ▶ This allows the attacker to:
 - ▶ Control what transactions get added to the blockchain
 - ▶ Remove recent transactions from the blockchain

What Can An Attacker Do?

- ▶ A majority attacker can
 - ▶ Solve computational puzzles faster, in expectation, than the honest minority
 - ▶ Create an alternative longest chain, replace the honest chain at a strategically opportune moment
- ▶ This allows the attacker to:
 - ▶ Control what transactions get added to the blockchain
 - ▶ Remove recent transactions from the blockchain
- ▶ Canonical attack: “double spend”

What Can An Attacker Do?

- ▶ A majority attacker can
 - ▶ Solve computational puzzles faster, in expectation, than the honest minority
 - ▶ Create an alternative longest chain, replace the honest chain at a strategically opportune moment
- ▶ This allows the attacker to:
 - ▶ Control what transactions get added to the blockchain
 - ▶ Remove recent transactions from the blockchain
- ▶ Canonical attack: “double spend”
- ▶ The attacker also earns the block rewards, for each period of their alternative chain

What Can An Attacker Do?

- ▶ A majority attacker can
 - ▶ Solve computational puzzles faster, in expectation, than the honest minority
 - ▶ Create an alternative longest chain, replace the honest chain at a strategically opportune moment
 - ▶ This allows the attacker to:
 - ▶ Control what transactions get added to the blockchain
 - ▶ Remove recent transactions from the blockchain
 - ▶ Canonical attack: “double spend”
 - ▶ The attacker also earns the block rewards, for each period of their alternative chain
- ▶ A majority attacker cannot
 - ▶ Create new transactions that spend other participants' Bitcoins (“steal all the Bitcoins”)
 - ▶ This would require not just $>50\%$ majority, but breaking modern cryptography

Illustration of Double Spending

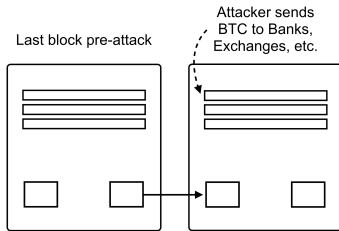


Illustration of Double Spending

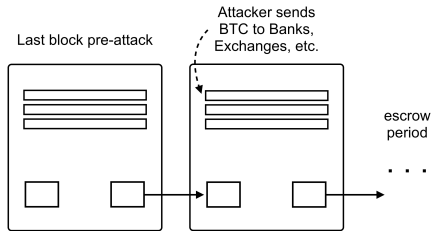


Illustration of Double Spending

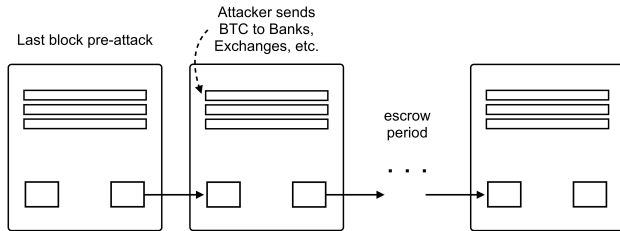


Illustration of Double Spending

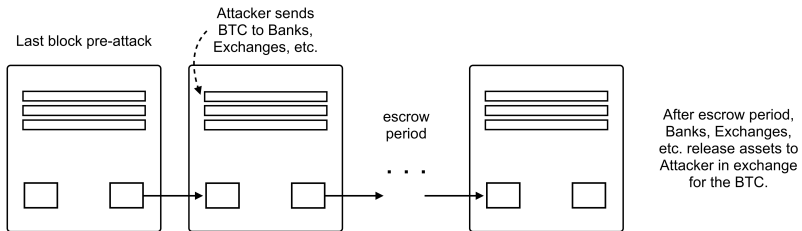


Illustration of Double Spending

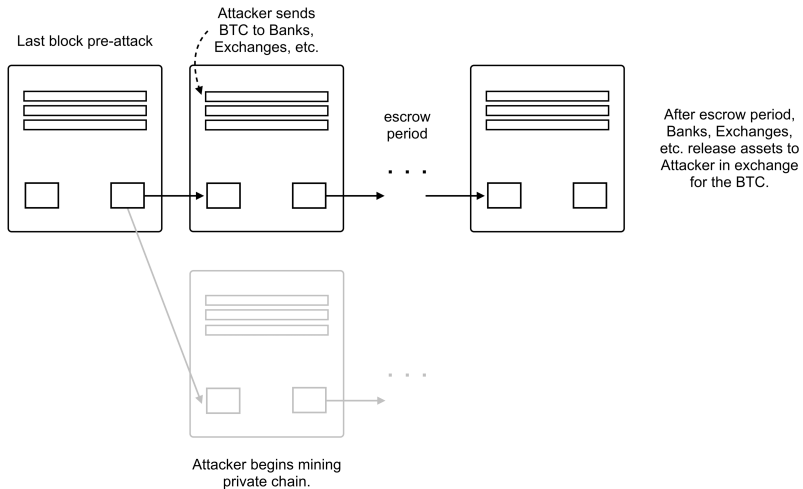


Illustration of Double Spending

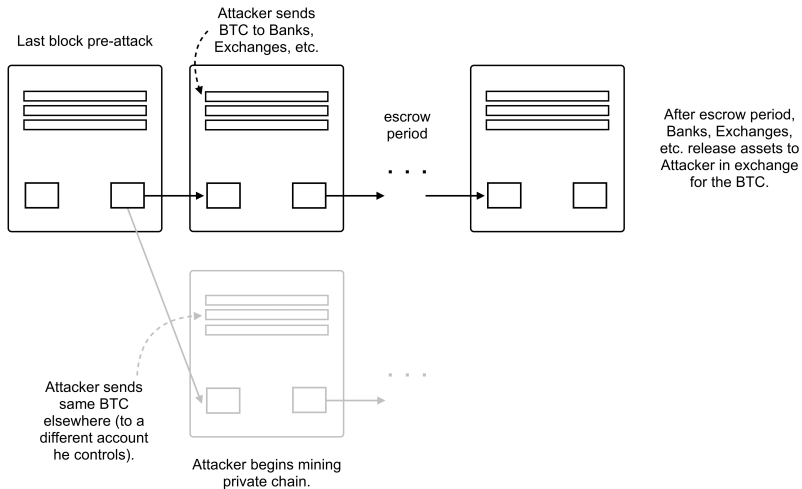


Illustration of Double Spending

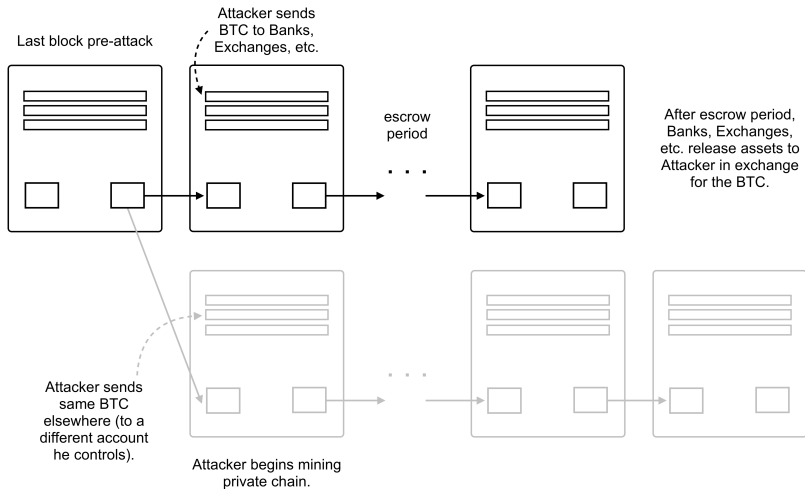
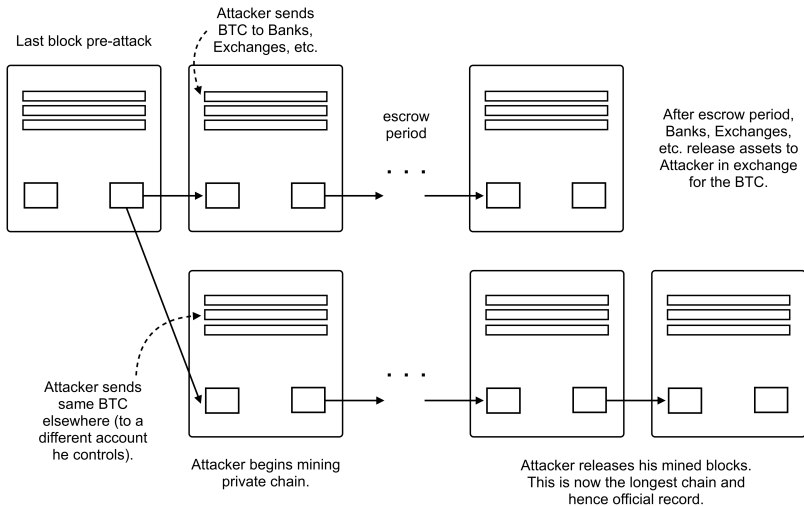


Illustration of Double Spending



Double Spending: Analysis Framework

- ▶ Canonical attack is called “double spending.” Equation (3) tells us that this possibility places an economic limit on Nakamoto trust:

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

Double Spending: Analysis Framework

- ▶ Canonical attack is called “double spending.” Equation (3) tells us that this possibility places an economic limit on Nakamoto trust:

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

- ▶ Duration of attack: $A^* \cdot t(A^*)$
 - ▶ Can compute explicitly for Nakamoto (2008) protocol.
 - ▶ Function of escrow period e and # of blocks the attacker double spends for k .

Double Spending: Analysis Framework

- ▶ Canonical attack is called “double spending.” Equation (3) tells us that this possibility places an economic limit on Nakamoto trust:

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

- ▶ Duration of attack: $A^* \cdot t(A^*)$
 - ▶ Can compute explicitly for Nakamoto (2008) protocol.
 - ▶ Function of escrow period e and # of blocks the attacker double spends for k .
- ▶ Benefits of attack: V_{attack}

Double Spending: Analysis Framework

- ▶ Canonical attack is called “double spending.” Equation (3) tells us that this possibility places an economic limit on Nakamoto trust:

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

- ▶ Duration of attack: $A^* \cdot t(A^*)$
 - ▶ Can compute explicitly for Nakamoto (2008) protocol.
 - ▶ Function of escrow period e and # of blocks the attacker double spends for k .
- ▶ Benefits of attack: V_{attack}
 - ▶ A majority attacker will not double-spend for a cappuccino at Starbucks

Double Spending: Analysis Framework

- ▶ Canonical attack is called “double spending.” Equation (3) tells us that this possibility places an economic limit on Nakamoto trust:

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

- ▶ Duration of attack: $A^* \cdot t(A^*)$
 - ▶ Can compute explicitly for Nakamoto (2008) protocol.
 - ▶ Function of escrow period e and # of blocks the attacker double spends for k .
- ▶ Benefits of attack: V_{attack}
 - ▶ A majority attacker will not double-spend for a cappuccino at Starbucks
 - ▶ They will use their majority to conduct transactions that are as large as possible given current uses of cryptocurrencies

Double Spending: Analysis Framework

- ▶ Canonical attack is called “double spending.” Equation (3) tells us that this possibility places an economic limit on Nakamoto trust:

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

- ▶ Duration of attack: $A^* \cdot t(A^*)$
 - ▶ Can compute explicitly for Nakamoto (2008) protocol.
 - ▶ Function of escrow period e and # of blocks the attacker double spends for k .
- ▶ Benefits of attack: V_{attack}
 - ▶ A majority attacker will not double-spend for a cappuccino at Starbucks
 - ▶ They will use their majority to conduct transactions that are as large as possible given current uses of cryptocurrencies
 - ▶ V_{attack} , therefore, can be understood as a statistic on the economic usefulness of Nakamoto trust. (“Max economic throughput”)

Double Spending: Analysis Framework

- ▶ Canonical attack is called “double spending.” Equation (3) tells us that this possibility places an economic limit on Nakamoto trust:

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

- ▶ Duration of attack: $A^* \cdot t(A^*)$
 - ▶ Can compute explicitly for Nakamoto (2008) protocol.
 - ▶ Function of escrow period e and # of blocks the attacker double spends for k .
- ▶ Benefits of attack: V_{attack}
 - ▶ A majority attacker will not double-spend for a cappuccino at Starbucks
 - ▶ They will use their majority to conduct transactions that are as large as possible given current uses of cryptocurrencies
 - ▶ V_{attack} , therefore, can be understood as a statistic on the economic usefulness of Nakamoto trust. (“Max economic throughput”)
 - ▶ Thought experiment: what is the equilibrium cost of security for a given dollar value of V_{attack} ?

Securing Against an Attack of Size V_{attack} : Base Case

Table 2. Cost to Secure Against Attack: Base Case Analysis

	Per-Block	Per-Day	Per-Year	Per-Transaction
Security Costs as % of Value Secured	5.00%	720%	262,801%	0.0025%
To Secure:				
\$1 thousand	\$50.0 dollars	\$7.2 thousand	\$2.6 million	2.5 cents
\$1 million	\$50.0 thousand	\$7.2 million	\$2.6 billion	\$25.0 dollars
\$1 billion	\$50.0 million	\$7.2 billion	\$2.6 trillion	\$25.0 thousand
\$10 billion	\$500.0 million	\$72.0 billion	\$26.3 trillion	\$250.0 thousand
\$100 billion	\$5.0 billion	\$720.0 billion	\$262.8 trillion	\$2.5 million

Securing Against an Attack of Size V_{attack} : Base Case

Table 2. Cost to Secure Against Attack: Base Case Analysis

	Per-Block	Per-Day	Per-Year	Per-Transaction
Security Costs as % of Value Secured	5.00%	720%	262,801%	0.0025%
To Secure:				
\$1 thousand	\$50.0 dollars	\$7.2 thousand	\$2.6 million	2.5 cents
\$1 million	\$50.0 thousand	\$7.2 million	\$2.6 billion	\$25.0 dollars
\$1 billion	\$50.0 million	\$7.2 billion	\$2.6 trillion	\$25.0 thousand
\$10 billion	\$500.0 million	\$72.0 billion	\$26.3 trillion	\$250.0 thousand
\$100 billion	\$5.0 billion	\$720.0 billion	\$262.8 trillion	\$2.5 million

- Per-block costs follow directly from (3), rewritten as $\frac{P_{block}}{V_{attack}} \geq \frac{1}{At}$

Securing Against an Attack of Size V_{attack} : Base Case

Table 2. Cost to Secure Against Attack: Base Case Analysis

	Per-Block	Per-Day	Per-Year	Per-Transaction
Security Costs as % of Value Secured	5.00%	720%	262,801%	0.0025%
To Secure:				
\$1 thousand	\$50.0 dollars	\$7.2 thousand	\$2.6 million	2.5 cents
\$1 million	\$50.0 thousand	\$7.2 million	\$2.6 billion	\$25.0 dollars
\$1 billion	\$50.0 million	\$7.2 billion	\$2.6 trillion	\$25.0 thousand
\$10 billion	\$500.0 million	\$72.0 billion	\$26.3 trillion	\$250.0 thousand
\$100 billion	\$5.0 billion	\$720.0 billion	\$262.8 trillion	\$2.5 million

- ▶ Per-block costs follow directly from (3), rewritten as $\frac{P_{block}}{V_{attack}} \geq \frac{1}{At}$
- ▶ Major difficulty: how costs scale with size of attack and over time. \$40bn attack requires all of global GDP

Securing Against an Attack of Size V_{attack} : Base Case

Table 2. Cost to Secure Against Attack: Base Case Analysis

	Per-Block	Per-Day	Per-Year	Per-Transaction
Security Costs as % of Value Secured	5.00%	720%	262,801%	0.0025%
To Secure:				
\$1 thousand	\$50.0 dollars	\$7.2 thousand	\$2.6 million	2.5 cents
\$1 million	\$50.0 thousand	\$7.2 million	\$2.6 billion	\$25.0 dollars
\$1 billion	\$50.0 million	\$7.2 billion	\$2.6 trillion	\$25.0 thousand
\$10 billion	\$500.0 million	\$72.0 billion	\$26.3 trillion	\$250.0 thousand
\$100 billion	\$5.0 billion	\$720.0 billion	\$262.8 trillion	\$2.5 million

- ▶ Per-block costs follow directly from (3), rewritten as $\frac{P_{block}}{V_{attack}} \geq \frac{1}{At}$
- ▶ Major difficulty: how costs scale with size of attack and over time. \$40bn attack requires all of global GDP
- ▶ % tax sounds more reasonable per transaction, but even tiny tx's have to pay security costs dictated by large attacks

Securing Against an Attack of Size V_{attack} : Sensitivity Analysis

Table 3. Annual Cost to Secure Against Attack: Sensitivity Analysis

	# Blocks of Double Spending + Escrow Period ($k + e$)					
	1	6	12	36	144	1,008
Per-Block Security Costs as % of V_{attack}	26.74%	8.55%	5.00%	1.99%	0.57%	0.09%
Annual Security Costs if V_{attack} Equals:						
\$1 thousand	\$14.1 M	\$4.5 M	\$2.6 M	\$1.0 M	\$301.3 K	\$47.8 K
\$1 million	\$14.1 B	\$4.5 B	\$2.6 B	\$1.0 B	\$301.3 M	\$47.8 M
\$1 billion	\$14.1 T	\$4.5 T	\$2.6 T	\$1.0 T	\$301.3 B	\$47.8 B
\$10 billion	\$140.5 T	\$44.9 T	\$26.3 T	\$10.5 T	\$3.0 T	\$478.2 B
\$100 billion	\$1.4 Q	\$449.1 T	\$262.8 T	\$104.7 T	\$30.1 T	\$4.8 T

Securing Against an Attack of Size V_{attack} : Sensitivity Analysis

Table 3. Annual Cost to Secure Against Attack: Sensitivity Analysis

	# Blocks of Double Spending + Escrow Period ($k + e$)					
	1	6	12	36	144	1,008
Per-Block Security Costs as % of V_{attack}	26.74%	8.55%	5.00%	1.99%	0.57%	0.09%
Annual Security Costs if V_{attack} Equals:						
\$1 thousand	\$14.1 M	\$4.5 M	\$2.6 M	\$1.0 M	\$301.3 K	\$47.8 K
\$1 million	\$14.1 B	\$4.5 B	\$2.6 B	\$1.0 B	\$301.3 M	\$47.8 M
\$1 billion	\$14.1 T	\$4.5 T	\$2.6 T	\$1.0 T	\$301.3 B	\$47.8 B
\$10 billion	\$140.5 T	\$44.9 T	\$26.3 T	\$10.5 T	\$3.0 T	\$478.2 B
\$100 billion	\$1.4 Q	\$449.1 T	\$262.8 T	\$104.7 T	\$30.1 T	\$4.8 T

- ▶ Long escrow periods (e.g. $k + e = 1$ day or 1 week) improve the picture by 1-2 orders of magnitude, but costs still very high

Securing Against an Attack of Size V_{attack} : Sensitivity Analysis

Table 3. Annual Cost to Secure Against Attack: Sensitivity Analysis

	# Blocks of Double Spending + Escrow Period ($k + e$)					
	1	6	12	36	144	1,008
Per-Block Security Costs as % of V_{attack}	26.74%	8.55%	5.00%	1.99%	0.57%	0.09%
Annual Security Costs if V_{attack} Equals:						
\$1 thousand	\$14.1 M	\$4.5 M	\$2.6 M	\$1.0 M	\$301.3 K	\$47.8 K
\$1 million	\$14.1 B	\$4.5 B	\$2.6 B	\$1.0 B	\$301.3 M	\$47.8 M
\$1 billion	\$14.1 T	\$4.5 T	\$2.6 T	\$1.0 T	\$301.3 B	\$47.8 B
\$10 billion	\$140.5 T	\$44.9 T	\$26.3 T	\$10.5 T	\$3.0 T	\$478.2 B
\$100 billion	\$1.4 Q	\$449.1 T	\$262.8 T	\$104.7 T	\$30.1 T	\$4.8 T

- ▶ Long escrow periods (e.g. $k + e = 1$ day or 1 week) improve the picture by 1-2 orders of magnitude, but costs still very high
- ▶ Even the 1-week case requires 5% of Global GDP to secure against \$100bn attack.

Double Spending Attack: Takeaways

$$p_{block} > \frac{V_{attack}}{At}$$

- Consistent with modest early use cases of Bitcoin—if double-spending worth \$1k, then cost per tx just \$0.025

Double Spending Attack: Takeaways

$$p_{block} > \frac{V_{attack}}{At}$$

- ▶ Consistent with modest early use cases of Bitcoin—if double-spending worth \$1k, then cost per tx just \$0.025
- ▶ Consistent with larger-scale black-market uses of Bitcoin—users willing to pay high tx costs. (Ex: \$1000 per tx secures up to \$40M in base case)

Double Spending Attack: Takeaways

$$p_{block} > \frac{V_{attack}}{A_t}$$

- ▶ Consistent with modest early use cases of Bitcoin—if double-spending worth \$1k, then cost per tx just \$0.025
- ▶ Consistent with larger-scale black-market uses of Bitcoin—users willing to pay high tx costs. (Ex: \$1000 per tx secures up to \$40M in base case)
- ▶ Casts doubt on Bitcoin / Nakamoto trust as major component of mainstream global financial system (too expensive!)

Double Spending Attack: Takeaways

$$p_{block} > \frac{V_{attack}}{At}$$

- ▶ Consistent with modest early use cases of Bitcoin—if double-spending worth \$1k, then cost per tx just \$0.025
- ▶ Consistent with larger-scale black-market uses of Bitcoin—users willing to pay high tx costs. (Ex: \$1000 per tx secures up to \$40M in base case)
- ▶ Casts doubt on Bitcoin / Nakamoto trust as major component of mainstream global financial system (too expensive!)
- ▶ Surprises to the CS community:

Double Spending Attack: Takeaways

$$p_{block} > \frac{V_{attack}}{At}$$

- ▶ Consistent with modest early use cases of Bitcoin—if double-spending worth \$1k, then cost per tx just \$0.025
- ▶ Consistent with larger-scale black-market uses of Bitcoin—users willing to pay high tx costs. (Ex: \$1000 per tx secures up to \$40M in base case)
- ▶ Casts doubt on Bitcoin / Nakamoto trust as major component of mainstream global financial system (too expensive!)
- ▶ Surprises to the CS community:
 1. for the system to be secure for large transactions requires tx costs that are ridiculous for small transactions

Double Spending Attack: Takeaways

$$p_{block} > \frac{V_{attack}}{At}$$

- ▶ Consistent with modest early use cases of Bitcoin—if double-spending worth \$1k, then cost per tx just \$0.025
- ▶ Consistent with larger-scale black-market uses of Bitcoin—users willing to pay high tx costs. (Ex: \$1000 per tx secures up to \$40M in base case)
- ▶ Casts doubt on Bitcoin / Nakamoto trust as major component of mainstream global financial system (too expensive!)
- ▶ Surprises to the CS community:
 1. for the system to be secure for large transactions requires tx costs that are ridiculous for small transactions
 2. that a long-enough escrow period isn't enough

Double Spending Attack: Takeaways

$$p_{block} > \frac{V_{attack}}{A_t}$$

- ▶ Consistent with modest early use cases of Bitcoin—if double-spending worth \$1k, then cost per tx just \$0.025
- ▶ Consistent with larger-scale black-market uses of Bitcoin—users willing to pay high tx costs. (Ex: \$1000 per tx secures up to \$40M in base case)
- ▶ Casts doubt on Bitcoin / Nakamoto trust as major component of mainstream global financial system (too expensive!)
- ▶ Surprises to the CS community:
 1. for the system to be secure for large transactions requires tx costs that are ridiculous for small transactions
 2. that a long-enough escrow period isn't enough
- ▶ Source of both surprises: missed eqm reasoning that one needs to worry about larger and larger attacks if Bitcoin / Nakamoto trust gets more economically useful. Security is not 0-1, but more like a (very high) % tax.

Overview of the Talk

Part I: Trust at Scale

- ▶ Overview of Nakamoto (2008) and Related Concepts
- ▶ Nakamoto Trust: A Critique in 3 Equations
- ▶ Analysis of Double-Spending Attacks
- ▶ **A Way Out: Specific Capital + Collapse**
- ▶ Comparison of Nakamoto Trust and Traditional Trust
- ▶ Summary of “Trust at Scale”

Part II: Directions for Research

Conclusion

Specific Capital + Collapse

- ▶ Nakamoto (2008) envisioned ordinary computers (“one-CPU-one-vote”)

Specific Capital + Collapse

- ▶ Nakamoto (2008) envisioned ordinary computers (“one-CPU-one-vote”)
- ▶ Since 2013, Bitcoin dominated by specialized equipment
 - ▶ ASICs = Application Specific Integrated Circuits
 - ▶ Not just a bit more efficient ... factor of 10,000x or more

Specific Capital + Collapse

- ▶ Nakamoto (2008) envisioned ordinary computers (“one-CPU-one-vote”)
- ▶ Since 2013, Bitcoin dominated by specialized equipment
 - ▶ ASICs = Application Specific Integrated Circuits
 - ▶ Not just a bit more efficient ... factor of 10,000x or more
- ▶ Proof-of-stake: capital is specialized by construction.

Specific Capital + Collapse

- ▶ Nakamoto (2008) envisioned ordinary computers (“one-CPU-one-vote”)
- ▶ Since 2013, Bitcoin dominated by specialized equipment
 - ▶ ASICs = Application Specific Integrated Circuits
 - ▶ Not just a bit more efficient ... factor of 10,000x or more
- ▶ Proof-of-stake: capital is specialized by construction.
- ▶ If (i) capital is specialized, and (ii) attack causes collapse of its value, then the attacker cost model needs to be modified
 - ▶ In addition to charging attacker a flow cost that is $O(N^*c)$, where $c = rC + \eta$
 - ▶ Also need to charge attacker the value of the now-worthless specialized capital: $O(N^*C)$

Specific Capital + Collapse

- ▶ Nakamoto (2008) envisioned ordinary computers (“one-CPU-one-vote”)
- ▶ Since 2013, Bitcoin dominated by specialized equipment
 - ▶ ASICs = Application Specific Integrated Circuits
 - ▶ Not just a bit more efficient ... factor of 10,000x or more
- ▶ Proof-of-stake: capital is specialized by construction.
- ▶ If (i) capital is specialized, and (ii) attack causes collapse of its value, then the attacker cost model needs to be modified
 - ▶ In addition to charging attacker a flow cost that is $O(N^*c)$, where $c = rC + \eta$
 - ▶ Also need to charge attacker the value of the now-worthless specialized capital: $O(N^*C)$
- ▶ This will be my candidate answer to the “Chicago lunch table question”

Antminer



- ▶ Cost per machine
 - ▶ S19j XP: \$4,983
- ▶ # and \$ required to match the Bitcoin hash rate
 - ▶ 2.3 Million machines
 - ▶ \$11.5bn

Note: The numbers are based on data from August 2023 from shop.bitmain.com.

Amazon Web Services



- ▶ AWS Total computational equipment in 2021: \$65 bn
- ▶ Assume ASIC machines are 10000 times more cost effective than AWS machines (conservative)
- ▶ **Devoting all of AWS to Bitcoin mining would yield about .05% of total network hash rate**

Note: Data on Amazon AWS total PP&E are obtained from Amazon's 10-K filing. The cost/efficiency ratio is a conservative estimate based on the data of the hash rate of non-specific mining hardware obtained from the Bitcoin Wiki.

Analysis if Attacker Loses their Capital Value

- ▶ Let $c = rC + \eta$, where C = fixed cost of capital, r = interest rate per unit time, η = variable costs.
- ▶ Honest equilibrium (1) can be written as:

$$N^*(rC + \eta) = p_{block}. \quad (1)$$

Analysis if Attacker Loses their Capital Value

- ▶ Let $c = rC + \eta$, where C = fixed cost of capital, r = interest rate per unit time, η = variable costs.
- ▶ Honest equilibrium (1) can be written as:

$$N^*(rC + \eta) = p_{block}. \quad (1)$$

- ▶ Outside attacker needs N^*C of capital. Assume attacker loses all of their capital value. IC constraint is approximated by

$$N^*C > V_{attack} \quad (2')$$

Analysis if Attacker Loses their Capital Value

- ▶ Let $c = rC + \eta$, where C = fixed cost of capital, r = interest rate per unit time, η = variable costs.
- ▶ Honest equilibrium (1) can be written as:

$$N^*(rC + \eta) = p_{block}. \quad (1)$$

- ▶ Outside attacker needs N^*C of capital. Assume attacker loses all of their capital value. IC constraint is approximated by

$$N^*C > V_{attack} \quad (2')$$

- ▶ We can compute N^*C as a function of p_{block} . Let $\mu = \frac{rC}{rC + \eta}$ denote the capital share of mining. Then:

$$N^*C = \frac{\mu p_{block}}{r}.$$

Analysis if Attacker Loses their Capital Value

- ▶ Hence we can derive a modified version of (3):

$$p_{block} > \frac{r}{\mu} V_{attack} \quad (3')$$

- ▶ MUCH more secure than before, because r is an interest rate per unit time.

Analysis if Attacker Loses their Capital Value

- ▶ Hence we can derive a modified version of (3):

$$p_{block} > \frac{r}{\mu} V_{attack} \quad (3')$$

- ▶ MUCH more secure than before, because r is an interest rate per unit time.
- ▶ Here is an example calculation for Bitcoin:
 - ▶ Assume the capital share of mining is $\mu = 0.4$ (De Vries, 2018, 2022)
 - ▶ Assume annual discount rate for ASICs is 50% (depreciation and risk), which implies that the per-unit-time discount rate is $r \approx 0.0008\%$. So $\frac{r}{\mu} = 0.002\%$.

Analysis if Attacker Loses their Capital Value

- ▶ Hence we can derive a modified version of (3):

$$p_{block} > \frac{r}{\mu} V_{attack} \quad (3')$$

- ▶ MUCH more secure than before, because r is an interest rate per unit time.
- ▶ Here is an example calculation for Bitcoin:
 - ▶ Assume the capital share of mining is $\mu = 0.4$ (De Vries, 2018, 2022)
 - ▶ Assume annual discount rate for ASICs is 50% (depreciation and risk), which implies that the per-unit-time discount rate is $r \approx 0.0008\%$. So $\frac{r}{\mu} = 0.002\%$.
 - ▶ Compare to $\frac{1}{A^* \cdot t(A^*)}$ factor on the right-hand-side of (3) from before. Base case value was $\frac{1}{A^* \cdot t(A^*)} = 5.00\%$
- ▶ So 2500-fold improvement in the cost of security.

Analysis if Attacker Loses their Capital Value

- ▶ Hence we can derive a modified version of (3):

$$p_{block} > \frac{r}{\mu} V_{attack} \quad (3')$$

- ▶ MUCH more secure than before, because r is an interest rate per unit time.
- ▶ Here is an example calculation for Bitcoin:
 - ▶ Assume the capital share of mining is $\mu = 0.4$ (De Vries, 2018, 2022)
 - ▶ Assume annual discount rate for ASICs is 50% (depreciation and risk), which implies that the per-unit-time discount rate is $r \approx 0.0008\%$. So $\frac{r}{\mu} = 0.002\%$.
 - ▶ Compare to $\frac{1}{A^* \cdot t(A^*)}$ factor on the right-hand-side of (3) from before. Base case value was $\frac{1}{A^* \cdot t(A^*)} = 5.00\%$
- ▶ So 2500-fold improvement in the cost of security.
- ▶ (N.B. these same values for μ and r and $p_{block} = \$250k$ imply capital stock of \$12.5B, which about matches retail prices.)

Issue: How Exactly does Attacker Lose their Capital?

Several possibilities, each with problems:

Issue: How Exactly does Attacker Lose their Capital?

Several possibilities, each with problems:

1. Collapse of the cryptocurrency.

- ▶ Ex: a large majority attack on Bitcoin causes the value of Bitcoin to collapse ...
- ▶ ... which in turn causes the value of Bitcoin ASICs to collapse (by even more, factor is $1/\mu$)

Issue: How Exactly does Attacker Lose their Capital?

Several possibilities, each with problems:

1. Collapse of the cryptocurrency.

- ▶ Ex: a large majority attack on Bitcoin causes the value of Bitcoin to collapse ...
- ▶ ... which in turn causes the value of Bitcoin ASICs to collapse (by even more, factor is $1/\mu$)
- ▶ This makes attack expensive, is Bitcoin Wiki's argument why Bitcoin is safe

Issue: How Exactly does Attacker Lose their Capital?

Several possibilities, each with problems:

1. Collapse of the cryptocurrency.

- ▶ Ex: a large majority attack on Bitcoin causes the value of Bitcoin to collapse ...
- ▶ ... which in turn causes the value of Bitcoin ASICs to collapse (by even more, factor is $1/\mu$)
- ▶ This makes attack expensive, is Bitcoin Wiki's argument why Bitcoin is safe
- ▶ But hardly reassuring!
 - ▶ Hurts honest participants
 - ▶ A single attack could cause a collapse of the system

Issue: How Exactly does Attacker Lose their Capital?

Several possibilities, each with problems:

1. Collapse of the cryptocurrency.

- ▶ Ex: a large majority attack on Bitcoin causes the value of Bitcoin to collapse ...
- ▶ ... which in turn causes the value of Bitcoin ASICs to collapse (by even more, factor is $1/\mu$)
- ▶ This makes attack expensive, is Bitcoin Wiki's argument why Bitcoin is safe
- ▶ But hardly reassuring!
 - ▶ Hurts honest participants
 - ▶ A single attack could cause a collapse of the system
- ▶ Also raises the possibility of sabotage
 - ▶ Value of sabotage likely grows with economic usefulness / financial market integration.

Issue: How Exactly does Attacker Lose their Capital?

Several possibilities, each with problems:

Issue: How Exactly does Attacker Lose their Capital?

Several possibilities, each with problems:

2. Internal-to-protocol punishment without collapse

- ▶ Idea: surgically confiscate the attacker's capital, while leaving honest participants unharmed.
- ▶ This is what Ethereum proof-of-stake with “slashing” is trying to accomplish

Issue: How Exactly does Attacker Lose their Capital?

Several possibilities, each with problems:

2. Internal-to-protocol punishment without collapse

- ▶ Idea: surgically confiscate the attacker's capital, while leaving honest participants unharmed.
- ▶ This is what Ethereum proof-of-stake with “slashing” is trying to accomplish
- ▶ But, bumps up against impossibility theorems (Tas et al, 2023; Budish, Lewis-Pye and Roughgarden, 2024)
- ▶ Intuition: a large-enough attacker can prevent the protocol from punishing them, controls the legal system ($\rho = \frac{2}{3}$ the cutoff)

Issue: How Exactly does Attacker Lose their Capital?

Several possibilities, each with problems:

Issue: How Exactly does Attacker Lose their Capital?

Several possibilities, each with problems:

3. External-to-protocol punishment from rule of law

- ▶ Certainly works ...

Issue: How Exactly does Attacker Lose their Capital?

Several possibilities, each with problems:

3. External-to-protocol punishment from rule of law

- ▶ Certainly works ...
- ▶ and is probably operative, especially if the attacker targets large financial institutions.
- ▶ ...

Issue: How Exactly does Attacker Lose their Capital?

Several possibilities, each with problems:

3. External-to-protocol punishment from rule of law

- ▶ Certainly works ...
- ▶ and is probably operative, especially if the attacker targets large financial institutions.
- ▶ ...
- ▶ But the whole question of this paper is whether Nakamoto trust is economically viable without government and rule of law.

Issue: How Exactly does Attacker Lose their Capital?

Several possibilities, each with problems:

3. External-to-protocol punishment from rule of law

- ▶ Certainly works ...
- ▶ and is probably operative, especially if the attacker targets large financial institutions.
- ▶ ...
- ▶ But the whole question of this paper is whether Nakamoto trust is economically viable without government and rule of law.

My best guess is Bitcoin's security to date is a combination of #1 collapse risk and #3 implicit legal protection.

Overview of the Talk

Part I: Trust at Scale

- ▶ Overview of Nakamoto (2008) and Related Concepts
- ▶ Nakamoto Trust: A Critique in 3 Equations
- ▶ Analysis of Double-Spending Attacks
- ▶ A Way Out: Specific Capital + Collapse
- ▶ **Comparison of Nakamoto Trust and Traditional Trust**
- ▶ Summary of “Trust at Scale”

Part II: Directions for Research

Conclusion

Beckerian Deterrence as an Economy of Scale

- ▶ For concreteness, consider a financial transaction between two parties of size V , where one of the parties can cheat and steal the other's assets.
- ▶ Party 1: choose from $\{Engage, Don't Engage\}$
- ▶ Party 2: choose from $\{Honest, Cheat\}$
- ▶ Payoffs

Beckerian Deterrence as an Economy of Scale

- ▶ For concreteness, consider a financial transaction between two parties of size V , where one of the parties can cheat and steal the other's assets.
- ▶ Party 1: choose from $\{Engage, Don't Engage\}$
- ▶ Party 2: choose from $\{Honest, Cheat\}$
- ▶ Payoffs
 - ▶ Party 1 plays *Engage*, Party 2 plays *Honest*: both parties get a payoff of $b > 0$

Beckerian Deterrence as an Economy of Scale

- ▶ For concreteness, consider a financial transaction between two parties of size V , where one of the parties can cheat and steal the other's assets.
- ▶ Party 1: choose from $\{Engage, Don't Engage\}$
- ▶ Party 2: choose from $\{Honest, Cheat\}$
- ▶ Payoffs
 - ▶ Party 1 plays *Engage*, Party 2 plays *Honest*: both parties get a payoff of $b > 0$
 - ▶ Party 1 plays *Engage*, Party 2 plays *Cheat*: Party 2 gets $+V$ and Party 1 gets $-V$

Beckerian Deterrence as an Economy of Scale

- ▶ For concreteness, consider a financial transaction between two parties of size V , where one of the parties can cheat and steal the other's assets.
- ▶ Party 1: choose from $\{Engage, Don't Engage\}$
- ▶ Party 2: choose from $\{Honest, Cheat\}$
- ▶ Payoffs
 - ▶ Party 1 plays *Engage*, Party 2 plays *Honest*: both parties get a payoff of $b > 0$
 - ▶ Party 1 plays *Engage*, Party 2 plays *Cheat*: Party 2 gets $+V$ and Party 1 gets $-V$
 - ▶ Party 1 plays *Don't Engage*: both parties get 0.

Beckerian Deterrence as an Economy of Scale

- ▶ For concreteness, consider a financial transaction between two parties of size V , where one of the parties can cheat and steal the other's assets.
- ▶ Party 1: choose from $\{Engage, Don't Engage\}$
- ▶ Party 2: choose from $\{Honest, Cheat\}$
- ▶ Payoffs
 - ▶ Party 1 plays *Engage*, Party 2 plays *Honest*: both parties get a payoff of $b > 0$
 - ▶ Party 1 plays *Engage*, Party 2 plays *Cheat*: Party 2 gets $+V$ and Party 1 gets $-V$
 - ▶ Party 1 plays *Don't Engage*: both parties get 0.
- ▶ Eqm. One-shot game, as described: clearly only equilibrium is *Don't Engage*.

Beckerian Deterrence as an Economy of Scale

- ▶ Now add a legal system with the power to enforce contracts:

Beckerian Deterrence as an Economy of Scale

- ▶ Now add a legal system with the power to enforce contracts:
- ▶ If Party 2 cheats, Party 1 can pay a cost c_l to bring the matter to court.
- ▶ The court can perfectly observe Party 2's play, and can compel Party 2 to return Party 1's assets and pay a fine of $f > 0$
 - ▶ Payoffs in this scenario:
 - ▶ Party 1's payoff is $-c_l$ and Party 2's payoff is $-f$.

Beckerian Deterrence as an Economy of Scale

- ▶ Now add a legal system with the power to enforce contracts:
- ▶ If Party 2 cheats, Party 1 can pay a cost c_l to bring the matter to court.
- ▶ The court can perfectly observe Party 2's play, and can compel Party 2 to return Party 1's assets and pay a fine of $f > 0$
 - ▶ Payoffs in this scenario:
 - ▶ Party 1's payoff is $-c_l$ and Party 2's payoff is $-f$.
- ▶ Eqm. Clearly, legal system makes it an equilibrium to transact honestly. The credible threat of enforcement deters Player 2 from cheating.

Beckerian Deterrence as an Economy of Scale

- ▶ Now add a legal system with the power to enforce contracts:
- ▶ If Party 2 cheats, Party 1 can pay a cost c_l to bring the matter to court.
- ▶ The court can perfectly observe Party 2's play, and can compel Party 2 to return Party 1's assets and pay a fine of $f > 0$
 - ▶ Payoffs in this scenario:
 - ▶ Party 1's payoff is $-c_l$ and Party 2's payoff is $-f$.
- ▶ Eqm. Clearly, legal system makes it an equilibrium to transact honestly. The credible threat of enforcement deters Player 2 from cheating.
- ▶ Observe: on path, the court need not even involve itself with the transaction.

Beckerian Deterrence as an Economy of Scale

- ▶ Now add a legal system with the power to enforce contracts:
- ▶ If Party 2 cheats, Party 1 can pay a cost c_l to bring the matter to court.
- ▶ The court can perfectly observe Party 2's play, and can compel Party 2 to return Party 1's assets and pay a fine of $f > 0$
 - ▶ Payoffs in this scenario:
 - ▶ Party 1's payoff is $-c_l$ and Party 2's payoff is $-f$.
- ▶ Eqm. Clearly, legal system makes it an equilibrium to transact honestly. The credible threat of enforcement deters Player 2 from cheating.
- ▶ Observe: on path, the court need not even involve itself with the transaction.
- ▶ This is the economy of scale for traditional trust: *A society that pays a fixed cost of operating a court system can facilitate honest transactions that have zero marginal cost of security because of the deterrence effect.*

Complementary Sources of Trust: Reputations, Relationships, Collateral

- ▶ Similar scale economies of trust arise in the private sector from fixed-cost investments in brands, reputations, relationships (Nelson, 1974; Fudenberg, Levine and Maskin, 1994; Tadelis, 1999; Baker, Gibbons and Murphy, 2002; Levin, 2003).

Complementary Sources of Trust: Reputations, Relationships, Collateral

- ▶ Similar scale economies of trust arise in the private sector from fixed-cost investments in brands, reputations, relationships (Nelson, 1974; Fudenberg, Levine and Maskin, 1994; Tadelis, 1999; Baker, Gibbons and Murphy, 2002; Levin, 2003).
- ▶ Remark 1: These often work in conjunction with rule of law.
 - ▶ E.g., can't directly copy a brand's look-and-feel; lower-bound payoffs in Levin 2003.
- ▶ Remark 2: Collateral a particularly important example for finance.
 - ▶ Cost of general-purpose collateral as a source of trust support is zero under the assumptions of the Modigliani-Miller theorem.
 - ▶ And note collateral works in conjunction with rule-of-law.

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

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.

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 U.S. financial industry is about \$800bn. (see Philippon, 2015)

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 U.S. financial industry is about \$800bn. (see Philippon, 2015)
 - ▶ So \$1 trillion is a conservative upper bound for the cost of trust in the U.S. 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 U.S. financial industry is about \$800bn. (see Philippon, 2015)
 - ▶ So \$1 trillion is a conservative upper bound for the cost of trust in the U.S. financial sector (former includes much non-finance, latter includes much non-trust).
 - ▶ Transaction volume in U.S. finance easily exceeds \$1 quadrillion per year (Budish and Sunderam, in progress)

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 U.S. financial industry is about \$800bn. (see Philippon, 2015)
 - ▶ So \$1 trillion is a conservative upper bound for the cost of trust in the U.S. financial sector (former includes much non-finance, latter includes much non-trust).
 - ▶ Transaction volume in U.S. finance easily exceeds \$1 quadrillion per year (Budish and Sunderam, in progress)
- ▶ 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 U.S. financial industry is about \$800bn. (see Philippon, 2015)
 - ▶ So \$1 trillion is a conservative upper bound for the cost of trust in the U.S. financial sector (former includes much non-finance, latter includes much non-trust).
 - ▶ Transaction volume in U.S. finance easily exceeds \$1 quadrillion per year (Budish and Sunderam, in progress)
- ▶ 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.

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 U.S. financial industry is about \$800bn. (see Philippon, 2015)
 - ▶ So \$1 trillion is a conservative upper bound for the cost of trust in the U.S. financial sector (former includes much non-finance, latter includes much non-trust).
 - ▶ Transaction volume in U.S. finance easily exceeds \$1 quadrillion per year (Budish and Sunderam, in progress)
- ▶ 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).

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 U.S. financial industry is about \$800bn. (see Philippon, 2015)
 - ▶ So \$1 trillion is a conservative upper bound for the cost of trust in the U.S. financial sector (former includes much non-finance, latter includes much non-trust).
 - ▶ Transaction volume in U.S. finance easily exceeds \$1 quadrillion per year (Budish and Sunderam, in progress)
- ▶ 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 the comparison with Nakamoto trust is night-and-day.

Overview of the Talk

Part I: Trust at Scale

- ▶ Overview of Nakamoto (2008) and Related Concepts
- ▶ Nakamoto Trust: A Critique in 3 Equations
- ▶ Analysis of Double-Spending Attacks
- ▶ A Way Out: Specific Capital + Collapse
- ▶ Comparison of Nakamoto Trust and Traditional Trust
- ▶ **Summary of “Trust at Scale”**

Part II: Directions for Research

Conclusion

Summary of “Trust at Scale”

- ▶ Anonymous, decentralized trust enabled by Nakamoto (2008) blockchain:
ingenious but expensive

Summary of “Trust at Scale”

- ▶ Anonymous, decentralized trust enabled by Nakamoto (2008) blockchain:
ingenious but expensive
- ▶ Permissionless consensus has to date been of limited usefulness in its pure form
- ▶ My work suggests this is intrinsic to the technology

Summary of “Trust at Scale”

- ▶ Anonymous, decentralized trust enabled by Nakamoto (2008) blockchain:
ingenious but expensive
- ▶ Permissionless consensus has to date been of limited usefulness in its pure form
- ▶ My work suggests this is intrinsic to the technology
- ▶ Emphasize: model consistent with continued use for illegal activity
 - ▶ Black market = willing to pay high implicit fees

Summary of “Trust at Scale”

- ▶ Anonymous, decentralized trust enabled by Nakamoto (2008) blockchain:
ingenious but expensive
- ▶ Permissionless consensus has to date been of limited usefulness in its pure form
- ▶ My work suggests this is intrinsic to the technology
- ▶ Emphasize: model consistent with continued use for illegal activity
 - ▶ Black market = willing to pay high implicit fees
- ▶ Also emphasize: analysis is consistent with the usefulness of the blockchain data structure without Nakamoto's novel form of trust
 - ▶ Example: Central Bank Digital Currencies (CBDCs) take some technical inspiration from cryptocurrencies but are anchored in traditional trust from rule of law and the reputation of central banks

Summary of “Trust at Scale”

- ▶ Anonymous, decentralized trust enabled by Nakamoto (2008) blockchain: *ingenious but expensive*
- ▶ Permissionless consensus has to date been of limited usefulness in its pure form
- ▶ My work suggests this is intrinsic to the technology
- ▶ Emphasize: model consistent with continued use for illegal activity
 - ▶ Black market = willing to pay high implicit fees
- ▶ Also emphasize: analysis is consistent with the usefulness of the blockchain data structure without Nakamoto's novel form of trust
 - ▶ Example: Central Bank Digital Currencies (CBDCs) take some technical inspiration from cryptocurrencies but are anchored in traditional trust from rule of law and the reputation of central banks
- ▶ What this paper highlights is that it is exactly the aspect of Bitcoin and Nakamoto (2008) that is so innovative relative to traditional distributed databases — *the anonymous, decentralized trust* — that is the source of its economic limits

Overview of the Talk

Part I: Trust at Scale

Part II: Directions for Research

- ▶ **Topic 1: Potential Solutions to the Budish Problem**
- ▶ Topic 2: Blockchain and Traditional Finance
- ▶ Topic 3: Crypto as a Social and Financial Phenomenon
- ▶ Topic 4: Crypto Data for Finance Research
- ▶ Topic 5: Crypto and Political Economy

Conclusion

Potential Solutions to the Budish (2025) Problem

- ▶ Is there a “solution” to Budish (2025)’s critique of Bitcoin and Nakamoto trust?

Potential Solutions to the Budish (2025) Problem

- ▶ Is there a “solution” to Budish (2025)’s critique of Bitcoin and Nakamoto trust?
- ▶ Informally: is there a way to generate trust in a public dataset that has some of the anonymity and decentralization aspects of Nakamoto while being significantly less economically constrained by the arguments in this paper?

Potential Solutions to the Budish (2025) Problem

- ▶ Is there a “solution” to Budish (2025)’s critique of Bitcoin and Nakamoto trust?
- ▶ Informally: is there a way to generate trust in a public dataset that has some of the anonymity and decentralization aspects of Nakamoto while being significantly less economically constrained by the arguments in this paper?
- ▶ Many responses to my paper are described in Appendix A (collected since it first circulated in June 2018)

Potential Solutions to the Budish (2025) Problem

- ▶ Is there a “solution” to Budish (2025)’s critique of Bitcoin and Nakamoto trust?
- ▶ Informally: is there a way to generate trust in a public dataset that has some of the anonymity and decentralization aspects of Nakamoto while being significantly less economically constrained by the arguments in this paper?
- ▶ Many responses to my paper are described in Appendix A (collected since it first circulated in June 2018)
- ▶ The most promising responses combine blockchain-based trust with some external source of trust support

Ethereum Proof-of-Stake + “Slashing”

- ▶ In event of a double-spending attack (“finality reversion”): confiscate the attacker’s stake (“slashing”).
- ▶ Takes advantage of two key differences versus Bitcoin proof-of-work

Ethereum Proof-of-Stake + “Slashing”

- ▶ In event of a double-spending attack (“finality reversion”): confiscate the attacker’s stake (“slashing”).
- ▶ Takes advantage of two key differences versus Bitcoin proof-of-work
 1. Capital is stake on-chain not ASICs off-chain (so capital is observable to the protocol - like collateral)

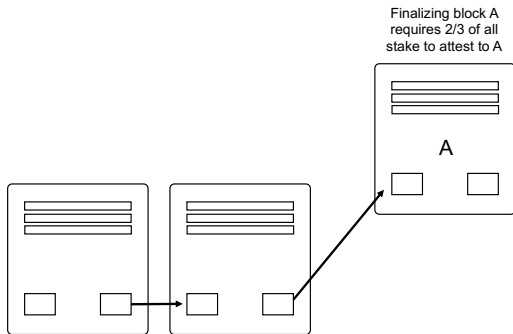
Ethereum Proof-of-Stake + “Slashing”

- ▶ In event of a double-spending attack (“finality reversion”): confiscate the attacker’s stake (“slashing”).
- ▶ Takes advantage of two key differences versus Bitcoin proof-of-work
 1. Capital is stake on-chain not ASICs off-chain (so capital is observable to the protocol - like collateral)
 2. Different consensus mechanism, based on Byzantine Fault Tolerance (BFT) – roughly, all stake votes on all blocks.

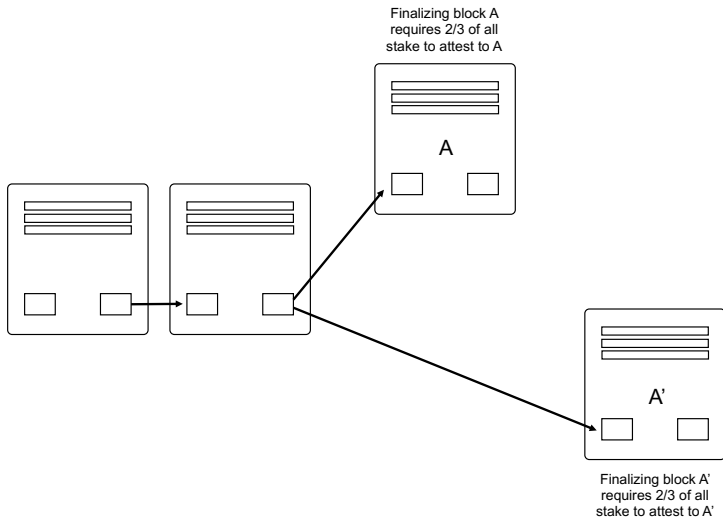
Ethereum Proof-of-Stake + “Slashing”

- ▶ In event of a double-spending attack (“finality reversion”): confiscate the attacker’s stake (“slashing”).
- ▶ Takes advantage of two key differences versus Bitcoin proof-of-work
 1. Capital is stake on-chain not ASICs off-chain (so capital is observable to the protocol - like collateral)
 2. Different consensus mechanism, based on Byzantine Fault Tolerance (BFT) – roughly, all stake votes on all blocks.
- ▶ $1+2 =$
 - ▶ Attacker leaves proof-of-guilt (signs bad votes)
 - ▶ Attacker’s capital can be confiscated (seized like collateral)

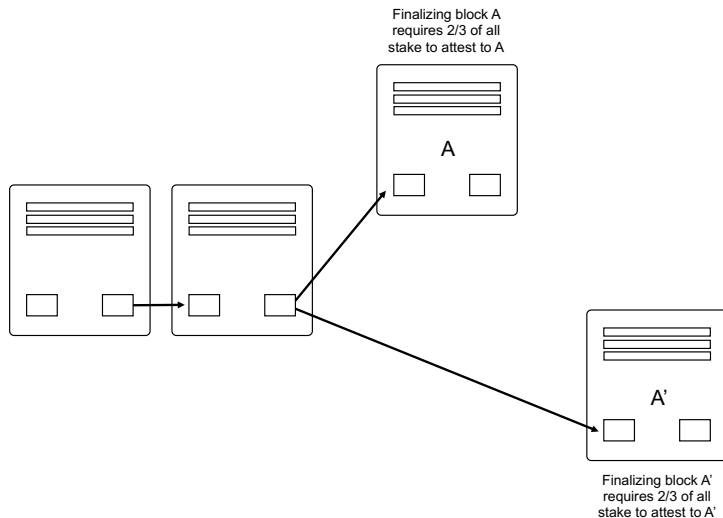
Ethereum PoS: Punishing a Double-Spend Attacker



Ethereum PoS: Punishing a Double-Spend Attacker

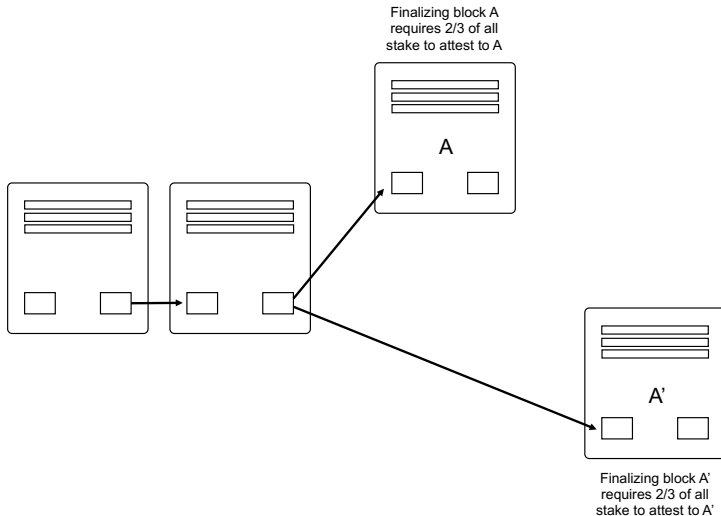


Ethereum PoS: Punishing a Double-Spend Attacker



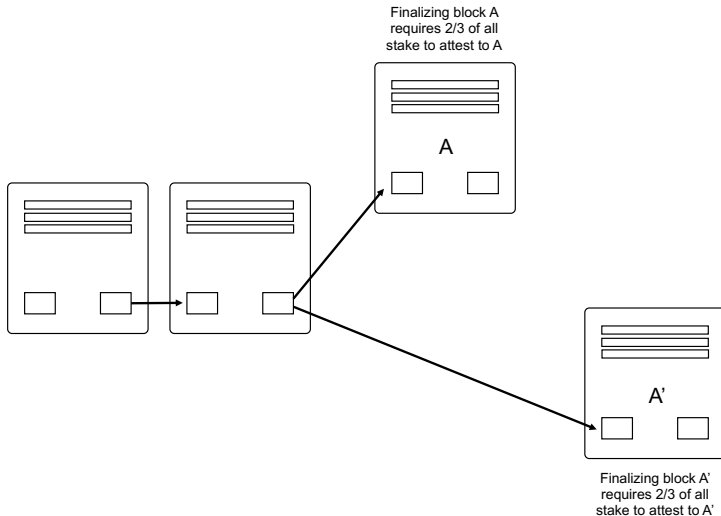
- Therefore, at least 1/3 of all stake signed both A and A'

Ethereum PoS: Punishing a Double-Spend Attacker



- Therefore, at least 1/3 of all stake signed both A and A'
- This stake that signed conflicting transactions is algorithmically destroyed ('slashed')

Ethereum PoS: Punishing a Double-Spend Attacker



- Therefore, at least 1/3 of all stake signed both A and A'
- This stake that signed conflicting transactions is algorithmically destroyed ('slashed')
- The reporter of the conflict earns a small bounty

Does Slashing Work?

- ▶ Recent work joint with Andrew Lewis-Pye and Tim Roughgarden
- ▶ Our formal question: is there a permissionless consensus protocol that is “expensive to attack in the absence of collapse” (EAAC)?
- ▶ EAAC definition (informal): attacker loses their capital but honest participants are not harmed.

Does Slashing Work?

- ▶ Recent work joint with Andrew Lewis-Pye and Tim Roughgarden
- ▶ Our formal question: is there a permissionless consensus protocol that is “expensive to attack in the absence of collapse” (EAAC)?
- ▶ EAAC definition (informal): attacker loses their capital but honest participants are not harmed.
- ▶ Our answers:

Does Slashing Work?

- ▶ Recent work joint with Andrew Lewis-Pye and Tim Roughgarden
- ▶ Our formal question: is there a permissionless consensus protocol that is “expensive to attack in the absence of collapse” (EAAC)?
- ▶ EAAC definition (informal): attacker loses their capital but honest participants are not harmed.
- ▶ Our answers:
 - ▶ No: if the consensus protocol is “fully permissionless” or “dynamically available” (even in the synchronous communications model)

Does Slashing Work?

- ▶ Recent work joint with Andrew Lewis-Pye and Tim Roughgarden
- ▶ Our formal question: is there a permissionless consensus protocol that is “expensive to attack in the absence of collapse” (EAAC)?
- ▶ EAAC definition (informal): attacker loses their capital but honest participants are not harmed.
- ▶ Our answers:
 - ▶ No: if the consensus protocol is “fully permissionless” or “dynamically available” (even in the synchronous communications model)
 - ▶ No: in the partially synchronous communications model (even for permissioned protocols)

Does Slashing Work?

- ▶ Recent work joint with Andrew Lewis-Pye and Tim Roughgarden
- ▶ Our formal question: is there a permissionless consensus protocol that is “expensive to attack in the absence of collapse” (EAAC)?
- ▶ EAAC definition (informal): attacker loses their capital but honest participants are not harmed.
- ▶ Our answers:
 - ▶ No: if the consensus protocol is “fully permissionless” or “dynamically available” (even in the synchronous communications model)
 - ▶ No: in the partially synchronous communications model (even for permissioned protocols)
 - ▶ Yes! In the synchronous communications model, for quasi-permissionless consensus protocols, if the attacker is bounded above by $\frac{2}{3}$ of the total

Does Slashing Work?

- ▶ Recent work joint with Andrew Lewis-Pye and Tim Roughgarden
- ▶ Our formal question: is there a permissionless consensus protocol that is “expensive to attack in the absence of collapse” (EAAC)?
- ▶ EAAC definition (informal): attacker loses their capital but honest participants are not harmed.
- ▶ Our answers:
 - ▶ No: if the consensus protocol is “fully permissionless” or “dynamically available” (even in the synchronous communications model)
 - ▶ No: in the partially synchronous communications model (even for permissioned protocols)
 - ▶ Yes! In the synchronous communications model, for quasi-permissionless consensus protocols, if the attacker is bounded above by $\frac{2}{3}$ of the total
 - ▶ No again, if the attacker can be $> \frac{2}{3}$ (Tas et al, 2023)

Does Slashing Work?

- ▶ Recent work joint with Andrew Lewis-Pye and Tim Roughgarden
- ▶ Our formal question: is there a permissionless consensus protocol that is “expensive to attack in the absence of collapse” (EAAC)?
- ▶ EAAC definition (informal): attacker loses their capital but honest participants are not harmed.
- ▶ Our answers:
 - ▶ No: if the consensus protocol is “fully permissionless” or “dynamically available” (even in the synchronous communications model)
 - ▶ No: in the partially synchronous communications model (even for permissioned protocols)
 - ▶ Yes! In the synchronous communications model, for quasi-permissionless consensus protocols, if the attacker is bounded above by $\frac{2}{3}$ of the total
 - ▶ No again, if the attacker can be $> \frac{2}{3}$ (Tas et al, 2023)
- ▶ Translation
 - ▶ Ethereum slashing works up to a $2/3$ attacker under assumptions about network reliability. Above $2/3$, then some external source of security is needed (e.g., law).

Does Slashing Work?

- ▶ Recent work joint with Andrew Lewis-Pye and Tim Roughgarden
- ▶ Our formal question: is there a permissionless consensus protocol that is “expensive to attack in the absence of collapse” (EAAC)?
- ▶ EAAC definition (informal): attacker loses their capital but honest participants are not harmed.
- ▶ Our answers:
 - ▶ No: if the consensus protocol is “fully permissionless” or “dynamically available” (even in the synchronous communications model)
 - ▶ No: in the partially synchronous communications model (even for permissioned protocols)
 - ▶ Yes! In the synchronous communications model, for quasi-permissionless consensus protocols, if the attacker is bounded above by $\frac{2}{3}$ of the total
 - ▶ No again, if the attacker can be $> \frac{2}{3}$ (Tas et al, 2023)
- ▶ Translation
 - ▶ Ethereum slashing works up to a $2/3$ attacker under assumptions about network reliability. Above $2/3$, then some external source of security is needed (e.g., law).
 - ▶ Consensus protocols like Bitcoin’s cannot be EAAC (they are “fully permissionless”)

Ethereum PoS: “Liveness” Attacks

Table: Cost of “Silence Attack” on Ethereum for Outside Attacker

Duration of Silence Attack	Length of Inactivity in Epochs (X)	$\rho(X)$	Share of Honest Stake Needed for Attack (A^*)	Attacker Slashed Stake as % of Total Honest Stake	Dollar Cost of Attack
1 Hour	10	0.9999	50.00%	0.00%	\$13 thousand
1 Day	225	0.9995	50.03%	0.03%	\$7 million
1 Week	1575	0.9756	51.25%	1.55%	\$388 million
1 Month	6750	0.6359	78.63%	33.98%	\$8.49 billion

Notes: An Epoch consists of 32 blocks (6.4 minutes). $\rho(X)$ represents Ethereum’s slashing function for inactive stakes. It depicts the proportion of an inactive stake that is remaining (not slashed) after X inactive epochs. A^* is computed so that the attacker has at least 1/3 of the total stake (inclusive of honest stakes) throughout the attack. The Attacker Slashed Stake computation accounts for the fact that the attacker’s stake will continue to get slashed, at a declining rate, after the attacker’s inactivity period. The Dollar Cost of Attack is based on \$25bn of value staked on Ethereum, which is roughly the dollar value of stake as of Nov 7, 2022.

Ethereum PoS: “Liveness” Attacks

Table: Cost of “Silence Attack” on Ethereum for Outside Attacker

Duration of Silence Attack	Length of Inactivity in Epochs (X)	$\rho(X)$	Share of Honest Stake Needed for Attack (A^*)	Attacker Slashed Stake as % of Total Honest Stake	Dollar Cost of Attack
1 Hour	10	0.9999	50.00%	0.00%	\$13 thousand
1 Day	225	0.9995	50.03%	0.03%	\$7 million
1 Week	1575	0.9756	51.25%	1.55%	\$388 million
1 Month	6750	0.6359	78.63%	33.98%	\$8.49 billion

Notes: An Epoch consists of 32 blocks (6.4 minutes). $\rho(X)$ represents Ethereum’s slashing function for inactive stakes. It depicts the proportion of an inactive stake that is remaining (not slashed) after X inactive epochs. A^* is computed so that the attacker has at least 1/3 of the total stake (inclusive of honest stakes) throughout the attack. The Attacker Slashed Stake computation accounts for the fact that the attacker’s stake will continue to get slashed, at a declining rate, after the attacker’s inactivity period. The Dollar Cost of Attack is based on \$25bn of value staked on Ethereum, which is roughly the dollar value of stake as of Nov 7, 2022.

Ethereum PoS + Slashing: Conclusion

- ▶ I conclude that Ethereum $>$ Bitcoin in its response to Budish (2025) critique

Ethereum PoS + Slashing: Conclusion

- ▶ I conclude that Ethereum $>$ Bitcoin in its response to Budish (2025) critique
- ▶ But that Ethereum is still reliant on external source of trust support for security.
 - ▶ Both for double-spend attacks and liveness attacks

Ethereum PoS + Slashing: Conclusion

- ▶ I conclude that Ethereum $>$ Bitcoin in its response to Budish (2025) critique
- ▶ But that Ethereum is still reliant on external source of trust support for security.
 - ▶ Both for double-spend attacks and liveness attacks
- ▶ Especially if Ethereum is used for large-stakes traditional financial applications
 - ▶ (Vitalik Buterin to Ezra Klein: "... future where it's just considered normal for there to be trillion dollar assets that are managed on Ethereum")

Leshno et al “Stubborn Nakamoto” Protocol

- ▶ Leshno et al propose roughly the following modification to Nakamoto (2008):
- ▶ Assume that the global internet is reliable in the sense that any message sent from one computer to another arrives within some finite time period Δ (called the “synchronous communications model”)

Leshno et al “Stubborn Nakamoto” Protocol

- ▶ Leshno et al propose roughly the following modification to Nakamoto (2008):
- ▶ Assume that the global internet is reliable in the sense that any message sent from one computer to another arrives within some finite time period Δ (called the “synchronous communications model”)
- ▶ Follow Nakamoto longest-chain as described above

Leshno et al “Stubborn Nakamoto” Protocol

- ▶ Leshno et al propose roughly the following modification to Nakamoto (2008):
- ▶ Assume that the global internet is reliable in the sense that any message sent from one computer to another arrives within some finite time period Δ (called the “synchronous communications model”)
- ▶ Follow Nakamoto longest-chain as described above
- ▶ If a block A is part of the longest-chain, was observed at least 2Δ ago, and you haven't heard anything else that contradicts it: treat A as provisionally confirmed

Leshno et al “Stubborn Nakamoto” Protocol

- ▶ Leshno et al propose roughly the following modification to Nakamoto (2008):
- ▶ Assume that the global internet is reliable in the sense that any message sent from one computer to another arrives within some finite time period Δ (called the “synchronous communications model”)
- ▶ Follow Nakamoto longest-chain as described above
- ▶ If a block A is part of the longest-chain, was observed at least 2Δ ago, and you haven't heard anything else that contradicts it: treat A as provisionally confirmed
- ▶ If a block A “...” 4Δ ago “...”: treat A as final

Leshno et al “Stubborn Nakamoto” Protocol

- ▶ Leshno et al propose roughly the following modification to Nakamoto (2008):
- ▶ Assume that the global internet is reliable in the sense that any message sent from one computer to another arrives within some finite time period Δ (called the “synchronous communications model”)
- ▶ Follow Nakamoto longest-chain as described above
- ▶ If a block A is part of the longest-chain, was observed at least 2Δ ago, and you haven't heard anything else that contradicts it: treat A as provisionally confirmed
- ▶ If a block A “...” 4Δ ago “...”: treat A as final
- ▶ If a block A' is observed that contradicts finalized block A : ignore it

Leshno et al “Stubborn Nakamoto” Protocol

- ▶ Leshno et al propose roughly the following modification to Nakamoto (2008):
- ▶ Assume that the global internet is reliable in the sense that any message sent from one computer to another arrives within some finite time period Δ (called the “synchronous communications model”)
- ▶ Follow Nakamoto longest-chain as described above
- ▶ If a block A is part of the longest-chain, was observed at least 2Δ ago, and you haven't heard anything else that contradicts it: treat A as provisionally confirmed
- ▶ If a block A “...” 4Δ ago “...”: treat A as final
- ▶ If a block A' is observed that contradicts finalized block A : ignore it
- ▶ If a block A' is observed that contradicts provisionally confirmed block A : halt
 - ▶ Given the communications assumption, there must be a bad actor.

Leshno et al “Stubborn Nakamoto” Protocol

- ▶ Stubborn Nakamoto trades a consistency problem for a liveness problem

Leshno et al “Stubborn Nakamoto” Protocol

- ▶ Stubborn Nakamoto trades a consistency problem for a liveness problem
- ▶ Will never revert a finalized block. Once a block is finalized, a node ignores anything that conflicts it, and knows that all other honest participants will do the same.

Leshno et al “Stubborn Nakamoto” Protocol

- ▶ Stubborn Nakamoto trades a consistency problem for a liveness problem
- ▶ Will never revert a finalized block. Once a block is finalized, a node ignores anything that conflicts it, and knows that all other honest participants will do the same.
- ▶ But: will grind to a permanent halt if an attacker inserts a conflicting block at an opportune moment.

Leshno et al “Stubborn Nakamoto” Protocol

- ▶ Stubborn Nakamoto trades a consistency problem for a liveness problem
- ▶ Will never revert a finalized block. Once a block is finalized, a node ignores anything that conflicts it, and knows that all other honest participants will do the same.
- ▶ But: will grind to a permanent halt if an attacker inserts a conflicting block at an opportune moment.
- ▶ Leshno et al argue that external-to-protocol sources of trust can be used to “restart” the protocol in this case.

Related Ideas and Approaches

- ▶ Idea of “Layer 2” protocols
 - ▶ Concede that Bitcoin/Ethereum/etc. are intrinsically very expensive (“Layer 1”)
 - ▶ Build applications that net to Bitcoin/Ethereum/etc. occasionally, but are also partially anchored in traditional trust
 - ▶ What does this combination accomplish?
- ▶ Related Q: Are there ways to tune the level of blockchain trust — and hence the level of cost — to the nature of the transaction?
- ▶ Facebook’s Diem/Libra idea
 - ▶ Instead of “trust Facebook”
 - ▶ Assumption was roughly “trust 20 out of 28 large institutions”
 - ▶ I genuinely like this idea (and think it was unfairly maligned because of where it came from)
 - ▶ But how should we think about it economically?

Overview of the Talk

Part I: Trust at Scale

Part II: Directions for Research

- ▶ Topic 1: Potential Solutions to the Budish Problem
- ▶ **Topic 2: Blockchain and Traditional Finance**
- ▶ Topic 3: Crypto as a Social and Financial Phenomenon
- ▶ Topic 4: Crypto Data for Finance Research
- ▶ Topic 5: Crypto and Political Economy

Conclusion

Blockchain and Traditional Finance

- ▶ Above, I described Ethereum's response to Budish (2025) critique as roughly:
 - ▶ "let's do all we can decentralized, and only rely on external trust support when we absolutely have to"

Blockchain and Traditional Finance

- ▶ Above, I described Ethereum's response to Budish (2025) critique as roughly:
 - ▶ "let's do all we can decentralized, and only rely on external trust support when we absolutely have to"
- ▶ Blockchain for traditional finance I see as coming at the issue from the opposite direction

Blockchain and Traditional Finance

- ▶ Above, I described Ethereum's response to Budish (2025) critique as roughly:
 - ▶ "let's do all we can decentralized, and only rely on external trust support when we absolutely have to"
- ▶ Blockchain for traditional finance I see as coming at the issue from the opposite direction
 - ▶ Rule-of-law and real identities are table stakes for serious traditional finance

Blockchain and Traditional Finance

- ▶ Above, I described Ethereum's response to Budish (2025) critique as roughly:
 - ▶ "let's do all we can decentralized, and only rely on external trust support when we absolutely have to"
- ▶ Blockchain for traditional finance I see as coming at the issue from the opposite direction
 - ▶ Rule-of-law and real identities are table stakes for serious traditional finance
 - ▶ Take inspiration from the data structure ideas in Nakamoto and the smart contracts ideas in Ethereum and elsewhere, while maintaining rule-of-law, including know-your-customer and anti-money-laundering

Blockchain and Traditional Finance

- ▶ This raises a conceptual question

Blockchain and Traditional Finance

- ▶ This raises a conceptual question
- ▶ Computer scientists unimpressed with “permissioned blockchain” / “distributed ledger”
 - ▶ “Just a database”
 - ▶ Nothing intellectually new from a CS perspective

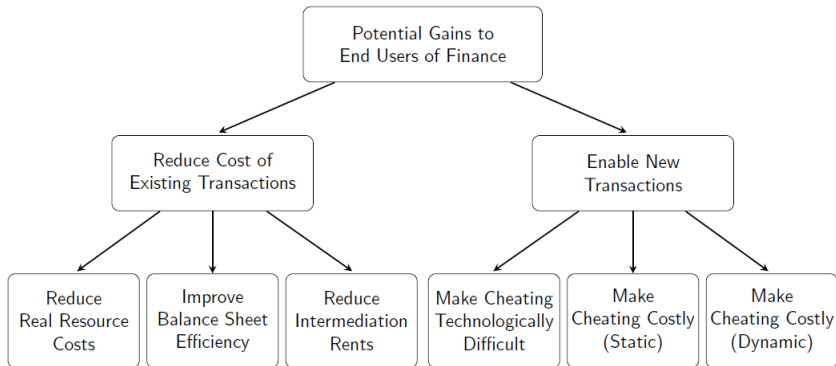
Blockchain and Traditional Finance

- ▶ This raises a conceptual question
- ▶ Computer scientists unimpressed with “permissioned blockchain” / “distributed ledger”
 - ▶ “Just a database”
 - ▶ Nothing intellectually new from a CS perspective
- ▶ The question: is there anything *economically* novel that emerges from this particular form of database?
 - ▶ Features: append-only, secure timestamps, appends pushed to all parties, pre-specified permissions as to who can do what, etc.
 - ▶ But with trust ultimately coming from traditional sources: rule of law, relationships, reputations, etc.

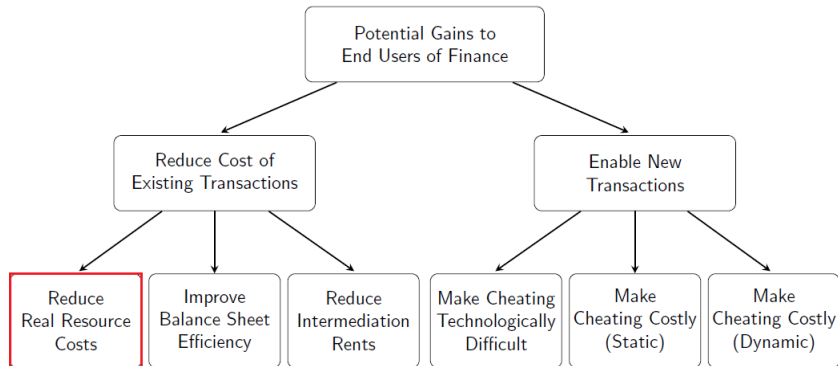
Blockchain and Traditional Finance

- ▶ Work in progress with Adi Sunderam
- ▶ We postulate a perfect blockchain data structure
 - ▶ Protected by rule of law
 - ▶ Not vulnerable to attack
 - ▶ Programmable smart contracts
 - ▶ Easy to use
- ▶ Then we ask: what might the potential social value of such a perfect data structure be for traditional finance

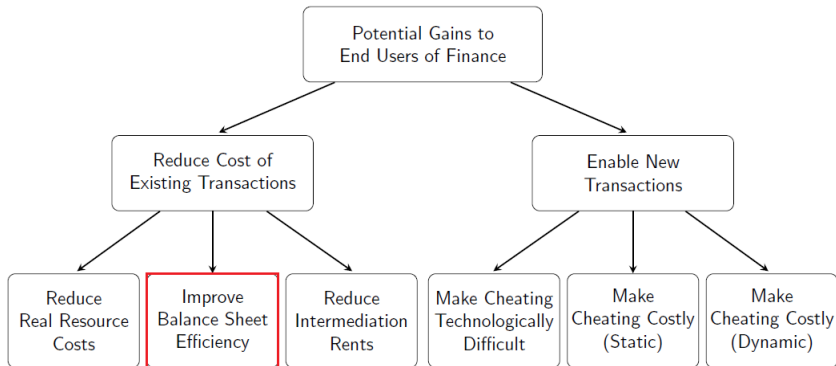
Framework for Analyzing Gains from Idealized Data Structure for Traditional Finance



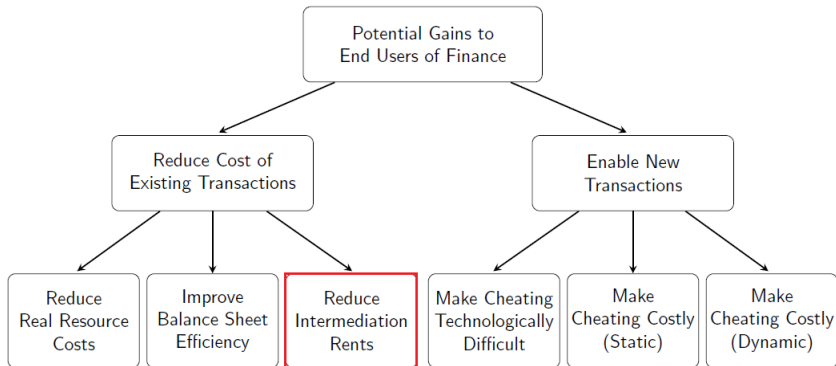
Framework for Analyzing Gains from Idealized Data Structure for Traditional Finance



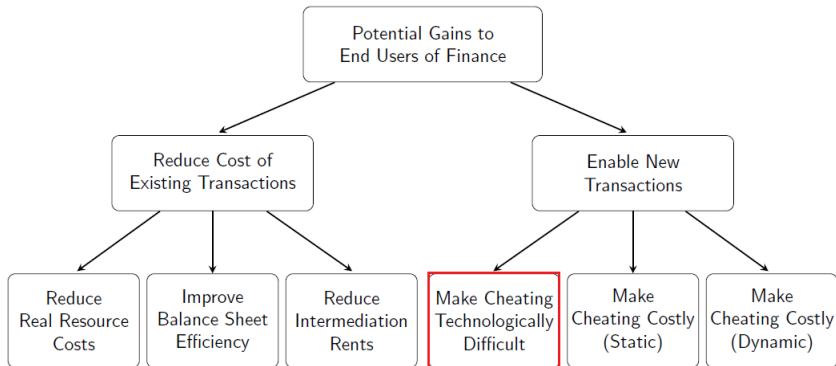
Framework for Analyzing Gains from Idealized Data Structure for Traditional Finance



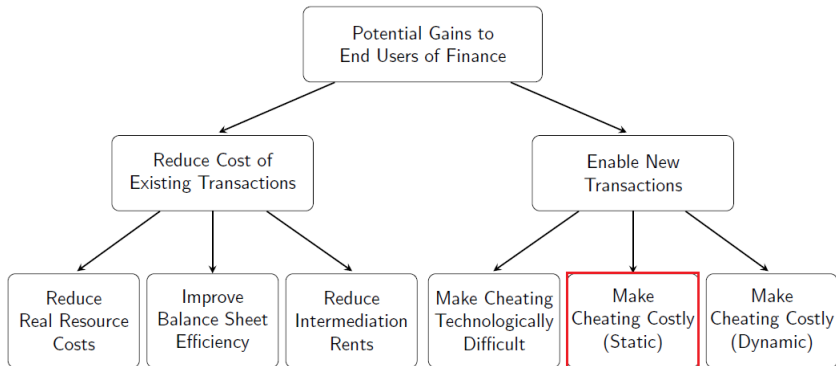
Framework for Analyzing Gains from Idealized Data Structure for Traditional Finance



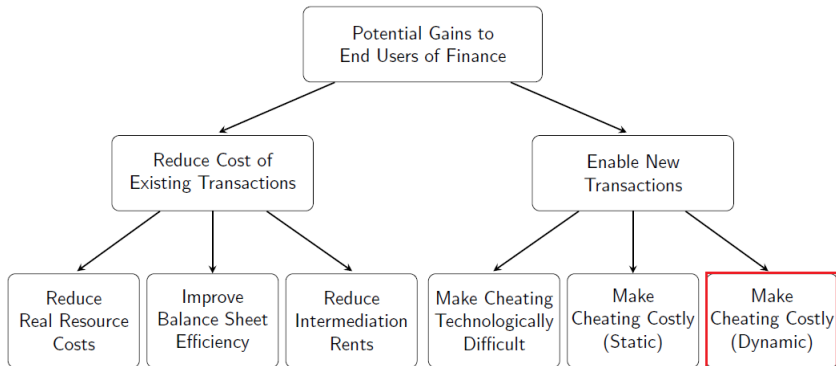
Framework for Analyzing Gains from Idealized Data Structure for Traditional Finance



Framework for Analyzing Gains from Idealized Data Structure for Traditional Finance



Framework for Analyzing Gains from Idealized Data Structure for Traditional Finance



Three Ways an Idealized Blockchain Can Facilitate Cooperation

Panel A: Technology

Player 1	Player 2		
	Engage, Cooperate	Engage, Cheat	Do not Engage
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 1	Player 2		
	Engage, Cooperate	Engage, Cheat	Do not Engage
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 1	Player 2		
	Engage, Cooperate	Engage, Cheat	Do not Engage
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.

Blockchain and Traditional Finance

- ▶ We try to quantify potential gains from addressing:
 1. Reduced real resource costs (ex: backoffice employees)
 2. Improved balance sheet efficiency
 3. Reduced intermediation rents

Blockchain and Traditional Finance

- ▶ We try to quantify potential gains from addressing:
 1. Reduced real resource costs (ex: backoffice employees)
 2. Improved balance sheet efficiency
 3. Reduced intermediation rents
- ▶ Message: transactional inefficiencies are modest \$.
- ▶ Intermediary rents are where the real \$\$\$ are.
 - ▶ (But also where the thorniest political economy is).

Blockchain and Traditional Finance

- ▶ We try to quantify potential gains from addressing:
 1. Reduced real resource costs (ex: backoffice employees)
 2. Improved balance sheet efficiency
 3. Reduced intermediation rents
- ▶ Message: transactional inefficiencies are modest \$.
- ▶ Intermediary rents are where the real \$\$\$ are.
 - ▶ (But also where the thorniest political economy is).
- ▶ New transactions enabled is the hardest to estimate
 - ▶ Insight: high-value tx's are already happening.
 - ▶ But there might be a long tail of small surplus tx's.

Conceptual Question: Multi-Layered 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)

Conceptual Question: Multi-Layered 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?

Conceptual Question: Multi-Layered 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?

Conceptual Question: Multi-Layered 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?
 - ▶ Ex: Ethereum PoS with slashing to punish small attackers and rule-of-law to deter large attackers.
 - ▶ How does this compare to JPMorgan's trust bundle?

An Innovation I'd Like to See

1. Ethereum-style PoS with slashing (to make attacks $< \frac{2}{3}$ expensive)

An Innovation I'd Like to See

1. Ethereum-style PoS with slashing (to make attacks $< \frac{2}{3}$ expensive)
2. Explicit rule-of-law protection (for $\geq \frac{2}{3}$ attackers)

An Innovation I'd Like to See

1. Ethereum-style PoS with slashing (to make attacks $< \frac{2}{3}$ expensive)
2. Explicit rule-of-law protection (for $\geq \frac{2}{3}$ attackers)
3. Ability for law enforcement to de-anonymize transactions with subpoena

An Innovation I'd Like to See

1. Ethereum-style PoS with slashing (to make attacks $< \frac{2}{3}$ expensive)
2. Explicit rule-of-law protection (for $\geq \frac{2}{3}$ attackers)
3. Ability for law enforcement to de-anonymize transactions with subpoena
4. To achieve 3, couldn't be fully permissionless/anonymous. Would need to be at least "gently permissioned" with identity verification as a requirement to participate.

An Innovation I'd Like to See

1. Ethereum-style PoS with slashing (to make attacks $< \frac{2}{3}$ expensive)
 2. Explicit rule-of-law protection (for $\geq \frac{2}{3}$ attackers)
 3. Ability for law enforcement to de-anonymize transactions with subpoena
 4. To achieve 3, couldn't be fully permissionless/anonymous. Would need to be at least "gently permissioned" with identity verification as a requirement to participate.
-
- ▶ Rationale: trade rule-of-law security against large attacks for the ability of the legal system to be able to enforce its laws against ordinary crime. (Can't have your cake and eat it too.)
 - ▶ This might be a superior "computer in the sky" architecture for general use and might be an interesting architecture for finance specifically, to reduce intermediation rents.

Stablecoins

- ▶ Stablecoins are a special case of the “Blockchain for Traditional Finance” question

Stablecoins

- ▶ Stablecoins are a special case of the “Blockchain for Traditional Finance” question
- ▶ Issue: cash leg of TradFi transactions usually quite efficient
 - ▶ TradFi volume literally in the \$quadrillions

Stablecoins

- ▶ Stablecoins are a special case of the “Blockchain for Traditional Finance” question
- ▶ Issue: cash leg of TradFi transactions usually quite efficient
 - ▶ TradFi volume literally in the \$quadrillions
- ▶ So for there to be large benefits they must come from either
 - ▶ Reducing intermediary rents
 - ▶ Ex: credit card tx fees – but what about Zelle/Venmo/etc?

Stablecoins

- ▶ Stablecoins are a special case of the “Blockchain for Traditional Finance” question
- ▶ Issue: cash leg of TradFi transactions usually quite efficient
 - ▶ TradFi volume literally in the \$quadrillions
- ▶ So for there to be large benefits they must come from either
 - ▶ Reducing intermediary rents
 - ▶ Ex: credit card tx fees – but what about Zelle/Venmo/etc?
 - ▶ Enabling new kinds of transactions
 - ▶ Possibly because of programmability (e.g., AI bot micropayments)
 - ▶ Possibly illegal tx's (e.g. online scams, “pig butchering”)
 - ▶ Possibly “sympathetic” illegal tx's (e.g., international remittances)

Overview of the Talk

Part I: Trust at Scale

Part II: Directions for Research

- ▶ Topic 1: Potential Solutions to the Budish Problem
- ▶ Topic 2: Blockchain and Traditional Finance
- ▶ **Topic 3: Crypto as a Social and Financial Phenomenon**
- ▶ Topic 4: Crypto Data for Finance Research
- ▶ Topic 5: Crypto and Political Economy

Conclusion

Bubble Formation

- ▶ One specific topic: crypto seems a fascinating laboratory through which to study bubbles

Bubble Formation

- ▶ One specific topic: crypto seems a fascinating laboratory through which to study bubbles
- ▶ Key observation here: it's a bubble either way!
 - ▶ Whether it persists or collapses!
 - ▶ At least in the narrow sense of price $\gg$ NPV of cash flows

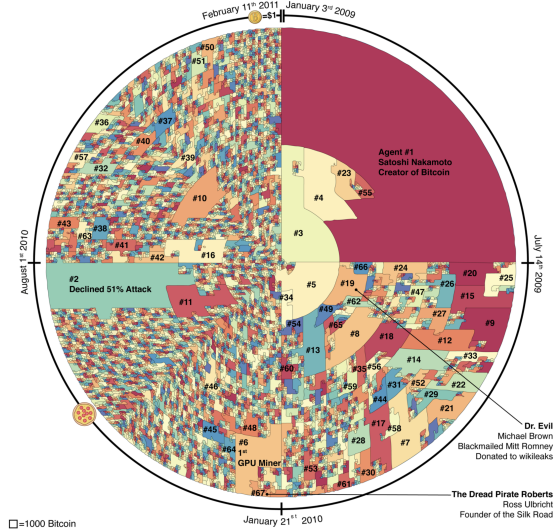
Bubble Formation

- ▶ One specific topic: crypto seems a fascinating laboratory through which to study bubbles
- ▶ Key observation here: it's a bubble either way!
 - ▶ Whether it persists or collapses!
 - ▶ At least in the narrow sense of price $\gg$ NPV of cash flows
- ▶ Delong, Shleifer, Summers and Waldman (1990): noise traders follow positive-feedback investment strategies (extended in Barberis et al, 2018)
- ▶ Shiller (2000): bubbles as a “naturally occurring Ponzi process”
- ▶ Barberis et al: “The fundamental psychological mechanisms of extrapolation remain to be understood.”

Bubble Formation

- ▶ One specific topic: crypto seems a fascinating laboratory through which to study bubbles
- ▶ Key observation here: it's a bubble either way!
 - ▶ Whether it persists or collapses!
 - ▶ At least in the narrow sense of price $\gg$ NPV of cash flows
- ▶ Delong, Shleifer, Summers and Waldman (1990): noise traders follow positive-feedback investment strategies (extended in Barberis et al, 2018)
- ▶ Shiller (2000): bubbles as a “naturally occurring Ponzi process”
- ▶ Barberis et al: “The fundamental psychological mechanisms of extrapolation remain to be understood.”
- ▶ Crypto strikes me as an unusually good potential laboratory to find new data on bubble formation

The Bitcoin 64



Source: Blackburn et al., 2022, "Cooperation among an anonymous group protected Bitcoin during failures of decentralization"

The Crypto Bros



A Naturally-Occurring Ponzi Process?

**KANYE WEST** 
@kanyewest

decentralize

12:01 AM · 16 Feb 2016

10,714 Retweets 40,779 Likes

1.5K 11K 41K



**Gwyneth Paltrow** 
@GwynethPaltrow · Follow

Buying crypto has often felt exclusionary. In order to democratize who can participate, @CashApp is now making it easy to gift Bitcoin. I'm giving out \$500k worth of Bitcoin for the holidays. Follow @cashapp + drop your \$cashtag below w/ #CashAppGifting to enter.

11:02 AM · Dec 20, 2021

19.9K Reply Copy link

Read 48.3K replies

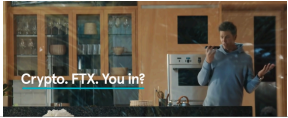
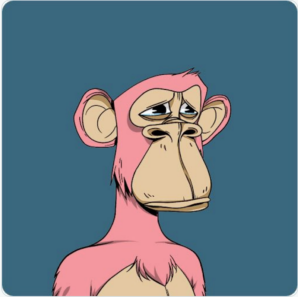


**Reese Witherspoon** 
@ReeseW

Just bought my first ETH! Let's do this #cryptotwitter

**Serena Williams** 
@serenawilliams · Jan 20, 2022

GM



**Mark Cuban** 
@mcuban

The @dallasmavs have done more than 20,000 #Dogecoin in transactions, making us the LARGEST #DOGE COIN MERCHANT IN THE WORLD! We thank all of you and can only say that if we sell another 6,556,000,000 #DOGE COIN worth of Mavs merch, #dogecoin will DEFINITELY HIT \$1 !!! 🚀🚀🚀



A Naturally-Occurring Ponzi Process? Elon Edition.



Elon Musk  @elonmusk · 9h

No highs, no lows, only Doge

 18.7K

 100.4K

 525.7K



Elon Musk  @elonmusk · 9h

Dogecoin is the people's crypto

 16.1K

 97.7K

 395.4K



Elon Musk  @elonmusk · Follow

SpaceX is going to put a literal Dogecoin on the literal moon

5:25 AM · Apr 1, 2021

 514.2K  Reply  Copy link

[Read 24.3K replies](#)



Elon Musk  @elonmusk · Follow

That said, BTC & ETH do seem high lol

1:02 AM · Feb 20, 2021

 17.9K  Reply  Copy link

[Read 2K replies](#)



Elon Musk  @elonmusk · Follow

One word: Doge

3:30 AM · Dec 20, 2020

 209.9K  Reply  Copy link

[Read 10.6K replies](#)



Elon Musk  @elonmusk · Follow

Bitcoin is my safe word

2:21 AM · Dec 20, 2020

[Read the full conversation on Twitter](#)



Elon Musk  @elonmusk · Follow

ur welcome



1:57 AM · Feb 4, 2021

 937.6K  Reply  Copy link



Elon Musk  @elonmusk

Bitcoin is almost as bs as fiat money

10:24 AM · Dec 20, 2020 · Twitter for iPhone

10.3K Retweets 3,487 Quote Tweets 142.2K Likes



Elon Musk  @elonmusk · Follow

I will keep supporting Dogecoin

1:19 AM · Jun 19, 2022

 388.9K  Reply  Copy link

[Read 37.1K replies](#)

A Naturally-Occurring Ponzi Process? Trump Edition.



Donald J. Trump ✓
@realDonaldTrump



I am not a fan of Bitcoin and other Cryptocurrencies, which are not money, and whose value is highly volatile and based on thin air. Unregulated Crypto Assets can facilitate unlawful behavior, including drug trade and other illegal activity....

9:15 AM · Jul 12, 2019



Personal Finance Economy Markets Watchlist Lifestyle Real Estate Tech TV Podcasts More | [Log in](#) [Watch TV](#)

POLITICS · Published 5 hours ago

Trump warns crypto 'potentially a disaster waiting to happen'

The former president argues 'we should be invested in our currency'

By Taha Khatib | FOXBusiness



Markets

Content displayed in real-time



U.S. Politics Media Opinion Business Entertainment Sports Lifestyle TV Fox Nation More | [Log in](#) [Watch TV](#)

Hot Topics: [Hiring](#), [in Business](#), [who potential](#) [experts](#) they will be turned back 'to not come'

MEDIA · Published 5 hours ago

Trump: Bitcoin 'seems like a scam' and should be regulated 'very very high'

Trump said he has 'always' wanted the US dollar to be the currency of the world

By William L. Lewis | Fox News



A Naturally-Occurring Ponzi Process? Trump Edition.



Donald J. Trump
@realDonaldTrump

I am not a fan of Bitcoin and other Cryptocurrencies, which are not money, and whose value is highly volatile and based on thin air. Unregulated Crypto Assets can facilitate unlawful behavior, including drug trade and other illegal activity....

9:15 AM · Jul 12, 2019



Personal Finance Economy Markets Watchlist Lifestyle Real Estate Tech TV Podcasts More

POLITICS Published 5 hours ago

Trump warns crypto 'potentially a disaster waiting to happen'

The former president argues 'we should be invested in our currency'

By Taka Kojima | FOXBusiness



Markets
Content displayed in real-time



U.S. Politics Media Opinion Business Entertainment Sports Lifestyle TV Fox Nation More

NEWS Published 5 hours ago

Trump: Bitcoin 'seems like a scam' and should be regulated 'very very high'

Trump said he has 'always' wanted the US dollar to be the currency of the world

By William Lencioni | Fox News



Donald J. Trump
@realDonaldTrump

VOTE FOR TRUMP! Bitcoin mining may be our last line of defense against a CBDC. Biden's hatred of Bitcoin only helps China, Russia, and the Radical Communist Left. We want all the remaining Bitcoin to be MADE IN THE USA!!! It will help us be ENERGY DOMINANT!!!! [bitcoinmagazine.com/culture/tr](https://bitcoinmagazine.com/culture/trump)

4.34k ReTruths 15.9k Likes

Jun 12, 2024 at 12:57 PM



Donald J. Trump
@realDonaldTrump

Just spoke at the Bitcoin Conference in Nashville, Tennessee on Saturday. It was GREAT! Get your Bitcoin Sneakers now. These are Limited Edition, they are each numbered, and you can now pay with Bitcoin or your favorite Crypto. Have fun — Go to gettrumpsneakers.com/ before they are gone!



2.4k ReTruths 9.65k Likes

Jul 31, 2024 at 11:27 PM

A Naturally-Occurring Ponzi Process? Trump Edition.



Donald J. Trump
@realDonaldTrump

I am not a fan of Bitcoin and other Cryptocurrencies, which are not money, and whose value is highly volatile and based on thin air. Unregulated Crypto Assets can facilitate unlawful behavior, including drug trade and other illegal activity....

9:15 AM · Jul 12, 2019



Trump warns crypto 'potentially a disaster waiting to happen'

The former president argues 'we should be invested in our currency'

By Tasha Knapton / FOXBusiness



Trump: Bitcoin 'seems like a scam' and should be regulated 'very very high'

Trump said he has 'always' wanted the US dollar to be the currency of the world

By William Lian / Fox News



Donald J. Trump
@realDonaldTrump

VOTE FOR TRUMP! Bitcoin mining may be our last line of defense against a CBDC. Biden's hatred of Bitcoin only helps China, Russia, and the Radical Communist Left. We want all the remaining Bitcoin to be MADE IN THE USA!!! It will help us be ENERGY DOMINANT!!!! [bitcoinmagazine.com/culture/tr](https://bitcoinmagazine.com/culture/trump)

4.34k ReTruths 15.9k Likes

Jun 12, 2024 at 12:57 PM



Donald J. Trump
@realDonaldTrump

Just spoke at the Bitcoin Conference in Nashville, Tennessee on Saturday. It was GREAT! Get your Bitcoin Sneakers now. These are Limited Edition, they are each numbered, and you can now pay with Bitcoin or your favorite Crypto. Have fun — Go to gettrumpsneakers.com/ before they are gone!



2.4k ReTruths 9.65k Likes

Jul 31, 2024 at 11:27 PM



MELANIA TRUMP
@MELANIATRUMP

The Official Melania Meme is live!



Donald J. Trump
@realDonaldTrump

You can buy \$MELANIA now.

My NEW Official Trump Meme is HERE! It's time to celebrate everything we stand for: WINNING! Join my very special Trump Community. GET YOUR \$TRUMP NOW. Go to gettrumpmemes.com — Have Fun!



GetTrumpMemes.com
\$TRUMP

6p6xgHyF7AeE6TZkSmFsko444wqoP15icUSqi2jfgIPN

11:44 AM · Jan 18, 2025 · 117.5M Views

\$TRUMP Price Chart

Cryptocurrencies > Official Trump Price

 **Official Trump** TRUMP Price #100

\$4.84 ▼ **83.3% (Max)** ⓘ

0.00005464 BTC ▼ 0.1%



☆ Add to Portfolio • 147,896 added ⓘ

Market Cap ⓘ **\$966,980,786** ▼

Fully Diluted Valuation ⓘ **\$4,834,904,581**

24 Hour Trading Vol ⓘ **\$207,892,115**

Circulating Supply ⓘ **199,999,973** ⓘ

Total Supply ⓘ **1,000,000,000**

Max Supply ⓘ **1,000,000,000**

Overview Markets News Similar Coins Historical Data ⓘ

Price Market Cap Live Chart ⓘ

24H 7D 1M 3M 1Y Max LOG ⓘ ⬇️ ⬆️ ⬇️

📈 📊



A Naturally-Occurring Ponzi Process? Plea for Data.

- ▶ 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 (Ex: 94027, 02138)
 - ▶ 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 (Ex: 60621)

A Naturally-Occurring Ponzi Process? Plea for Data.

- ▶ 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 (Ex: 94027, 02138)
 - ▶ 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 (Ex: 60621)
- ▶ I bet certain kinds of institutional investors more likely to have inflows in 2017, 2020-2021ish
 - ▶ Ex: at GS Digital Asset Conference (June, 2022), there seemed a lot of interest in recruiting pension fund money

A Naturally-Occurring Ponzi Process? Plea for Data.

- ▶ 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 (Ex: 94027, 02138)
 - ▶ 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 (Ex: 60621)
- ▶ I bet certain kinds of institutional investors more likely to have inflows in 2017, 2020-2021ish
 - ▶ Ex: at GS Digital Asset Conference (June, 2022), there seemed a lot of interest in recruiting pension fund money
- ▶ And more traditional wealth managers likely to have inflows in 2024-2025ish
 - ▶ Bitcoin ETFs in Jan 2024
 - ▶ Trump election in Nov 2024

Overview of the Talk

Part I: Trust at Scale

Part II: Directions for Research

- ▶ Topic 1: Potential Solutions to the Budish Problem
- ▶ Topic 2: Blockchain and Traditional Finance
- ▶ Topic 3: Crypto as a Social and Financial Phenomenon
- ▶ **Topic 4: Crypto Data for Finance Research**
- ▶ Topic 5: Crypto and Political Economy

Conclusion

Crypto Data for Finance Research

- ▶ My advice / sense of the research opportunity: Use crypto data to study questions of interest to traditional finance

Crypto Data for Finance Research

- ▶ My advice / sense of the research opportunity: Use crypto data to study questions of interest to traditional finance
- ▶ Financial bubbles: as already discussed

Crypto Data for Finance Research

- ▶ My advice / sense of the research opportunity: Use crypto data to study questions of interest to traditional finance
- ▶ Financial bubbles: as already discussed
- ▶ Financial regulation
 - ▶ Read Andrew Ross Sorkin's 1929
 - ▶ Learn about the financial regulation that came after for US securities markets
 - ▶ Study its absence in crypto markets

Crypto Data for Finance Research

- ▶ My advice / sense of the research opportunity: Use crypto data to study questions of interest to traditional finance
- ▶ Financial bubbles: as already discussed
- ▶ Financial regulation
 - ▶ Read Andrew Ross Sorkin's 1929
 - ▶ Learn about the financial regulation that came after for US securities markets
 - ▶ Study its absence in crypto markets
- ▶ Market microstructure
 - ▶ MEV is HFT on steroids
 - ▶ Publicness of on-chain trading data a goldmine for research

Overview of the Talk

Part I: Trust at Scale

Part II: Directions for Research

- ▶ Topic 1: Potential Solutions to the Budish Problem
- ▶ Topic 2: Blockchain and Traditional Finance
- ▶ Topic 3: Crypto as a Social and Financial Phenomenon
- ▶ Topic 4: Crypto Data for Finance Research
- ▶ **Topic 5: Crypto and Political Economy**

Conclusion

The Core Policy Conundrum

- ▶ Anonymous trust strikes me as a real conundrum for policy makers and legal theorists

The Core Policy Conundrum

- ▶ Anonymous trust strikes me as a real conundrum for policy makers and legal theorists
- ▶ There are lots of implicit “legal puts” to the anonymous trust if you look around

The Core Policy Conundrum

- ▶ Anonymous trust strikes me as a real conundrum for policy makers and legal theorists
- ▶ There are lots of implicit “legal puts” to the anonymous trust if you look around
 - ▶ Ex: if an individual’s crypto wallet is stolen by a mugger -> they can call the cops

The Core Policy Conundrum

- ▶ Anonymous trust strikes me as a real conundrum for policy makers and legal theorists
- ▶ There are lots of implicit “legal puts” to the anonymous trust if you look around
 - ▶ Ex: if an individual’s crypto wallet is stolen by a mugger -> they can call the cops
 - ▶ Ex: if a financial institution gets double spent -> they can call the FBI

The Core Policy Conundrum

- ▶ Anonymous trust strikes me as a real conundrum for policy makers and legal theorists
- ▶ There are lots of implicit “legal puts” to the anonymous trust if you look around
 - ▶ Ex: if an individual’s crypto wallet is stolen by a mugger -> they can call the cops
 - ▶ Ex: if a financial institution gets double spent -> they can call the FBI
- ▶ So, honest users get some implicit legal protection

The Core Policy Conundrum

- ▶ Anonymous trust strikes me as a real conundrum for policy makers and legal theorists
- ▶ There are lots of implicit “legal puts” to the anonymous trust if you look around
 - ▶ Ex: if an individual’s crypto wallet is stolen by a mugger -> they can call the cops
 - ▶ Ex: if a financial institution gets double spent -> they can call the FBI
- ▶ So, honest users get some implicit legal protection
- ▶ Which enhances the value of the system

The Core Policy Conundrum

- ▶ Anonymous trust strikes me as a real conundrum for policy makers and legal theorists
- ▶ There are lots of implicit “legal puts” to the anonymous trust if you look around
 - ▶ Ex: if an individual’s crypto wallet is stolen by a mugger -> they can call the cops
 - ▶ Ex: if a financial institution gets double spent -> they can call the FBI
- ▶ So, honest users get some implicit legal protection
- ▶ Which enhances the value of the system
- ▶ Which provides more cover to black-market users

The Core Policy Conundrum

- ▶ Anonymous trust strikes me as a real conundrum for policy makers and legal theorists
- ▶ There are lots of implicit “legal puts” to the anonymous trust if you look around
 - ▶ Ex: if an individual’s crypto wallet is stolen by a mugger -> they can call the cops
 - ▶ Ex: if a financial institution gets double spent -> they can call the FBI
- ▶ So, honest users get some implicit legal protection
- ▶ Which enhances the value of the system
- ▶ Which provides more cover to black-market users
- ▶ Have your cake and eat it too: anonymous, decentralized trust — unless there is a large attack, then call in the Feds

The Core Policy Confusion

Public Law 119–27
119th Congress

An Act

To provide for the regulation of payment stablecoins, and for other purposes.

July 18, 2025
[S. 1582]

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Guiding and Establishing National Innovation for U.S. Stablecoins Act” or the “GENIUS Act”.

Guiding and
Establishing
National
Innovation for
U.S. Stablecoins
Act.
12 USC 5901
note.
12 USC 5901.

SEC. 2. DEFINITIONS.

In this Act:

(1) **APPROPRIATE FEDERAL BANKING AGENCY.**—The term “appropriate Federal banking agency” has the meaning given that term in section 3 of the Federal Deposit Insurance Act (12 U.S.C. 1813).

(2) **BANK SECRECY ACT.**—The term “Bank Secrecy Act” means—

(A) section 21 of the Federal Deposit Insurance Act (12 U.S.C. 1829b);

(B) chapter 2 of title I of Public Law 91–508 (12 U.S.C. 1951 et seq.); and

(C) subchapter II of chapter 53 of title 31, United States Code.

(3) **BOARD.**—The term “Board” means the Board of Governors of the Federal Reserve System.

(4) **COMPTROLLER.**—The term “Comptroller” means the Office of the Comptroller of the Currency.

(5) **CORPORATION.**—The term “Corporation” means the Federal Deposit Insurance Corporation.

(6) **DIGITAL ASSET.**—The term “digital asset” means any digital representation of value that is recorded on a cryptographically secured distributed ledger.

(7) **DIGITAL ASSET SERVICE PROVIDER.**—The term “digital asset service provider”—

means a person that, for compensation
conducts the business in the United States

The Core Policy Confusion

Public Law 119–27
119th Congress

An Act

To provide for the regulation of payment stablecoins, and for other purposes.

July 18, 2025
[S. 1582]

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Guiding and Establishing National Innovation for U.S. Stablecoins Act” or the “GENIUS Act”.

Guiding and
Establishing
National
Innovation for
U.S. Stablecoins
Act.
12 USC 5901
note.
12 USC 5901.

SEC. 2. DEFINITIONS.

In this Act:

(1) APPROPRIATE FEDERAL BANKING AGENCY.—The term “appropriate Federal banking agency” has the meaning given that term in section 3 of the Federal Deposit Insurance Act (12 U.S.C. 1813).

(2) BANK SECRECY ACT.—The term “Bank Secrecy Act” means—

(A) section 21 of the Federal Deposit Insurance Act (12 U.S.C. 1829b);

(B) chapter 2 of title I of Public Law 91–508 (12 U.S.C. 1951 et seq.); and

(C) subchapter II of chapter 53 of title 31, United States Code.

(6) DIGITAL ASSET.—The term “digital asset” means any digital representation of value that is recorded on a cryptographically secured distributed ledger.

ons a person that, for compensation
he business in the Unit
tame

The Core Policy Confusion: Stablecoins

- ▶ There is a huge distinction between stablecoin tx's on permissionless versus permissioned blockchains.

The Core Policy Confusion: Stablecoins

- ▶ There is a huge distinction between stablecoin tx's on permissionless versus permissioned blockchains.
- ▶ Permissionless
 - ▶ Intrinsically vulnerable to 51% attacks
 - ▶ So need to be very cautious about integration with finance

The Core Policy Confusion: Stablecoins

- ▶ There is a huge distinction between stablecoin tx's on permissionless versus permissioned blockchains.
- ▶ Permissionless
 - ▶ Intrinsically vulnerable to 51% attacks
 - ▶ So need to be very cautious about integration with finance
 - ▶ Intrinsically anonymous at the account level -> so good for illegal activity
 - ▶ Pig butchering (Zeke Faux of Bloomberg reporting)
 - ▶ Funding terrorist groups (WSJ reporting)

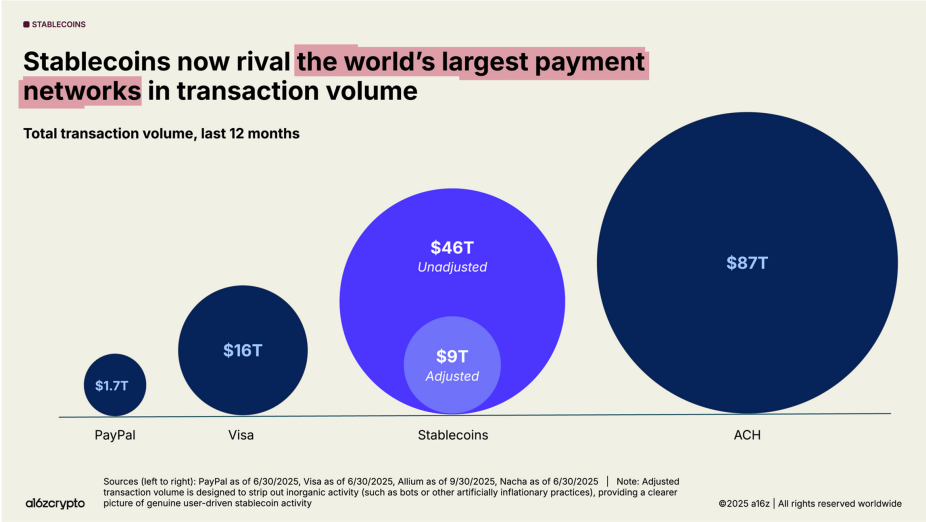
The Core Policy Confusion: Stablecoins

- ▶ There is a huge distinction between stablecoin tx's on permissionless versus permissioned blockchains.
- ▶ Permissionless
 - ▶ Intrinsically vulnerable to 51% attacks
 - ▶ So need to be very cautious about integration with finance
 - ▶ Intrinsically anonymous at the account level -> so good for illegal activity
 - ▶ Pig butchering (Zeke Faux of Bloomberg reporting)
 - ▶ Funding terrorist groups (WSJ reporting)
- ▶ Permissioned rails backed by rule of law do not have these issues
- ▶ Crazy that policy ignores the difference
- ▶ (N.B. there are some sympathetic use cases that take advantage of the anonymity too. This creates tradeoffs that I would like to see researched).

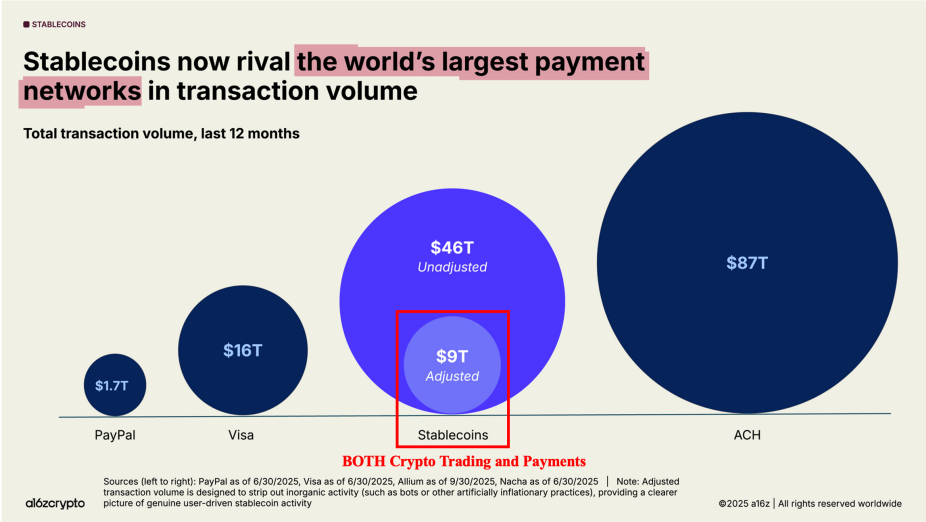
The Core Policy Confusion: Stablecoins

- ▶ An optimistic scenario
 - ▶ Permissionless stablecoins put pressure on TradFi firms and regulators to improve costs / reduce intermediary rents in the traditional, legal financial system
- ▶ A pessimistic scenario
 - ▶ Criminals around the world now have a much more convenient alternative to suitcases of \$100-bills.
 - ▶ Online scammers keep on pig butchering seniors

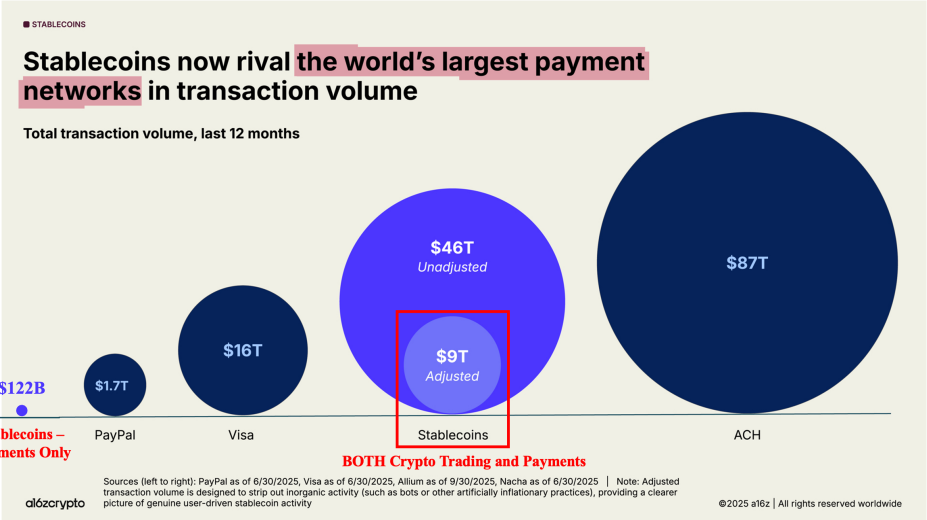
Stablecoins: The Data So Far



Stablecoins: The Data So Far

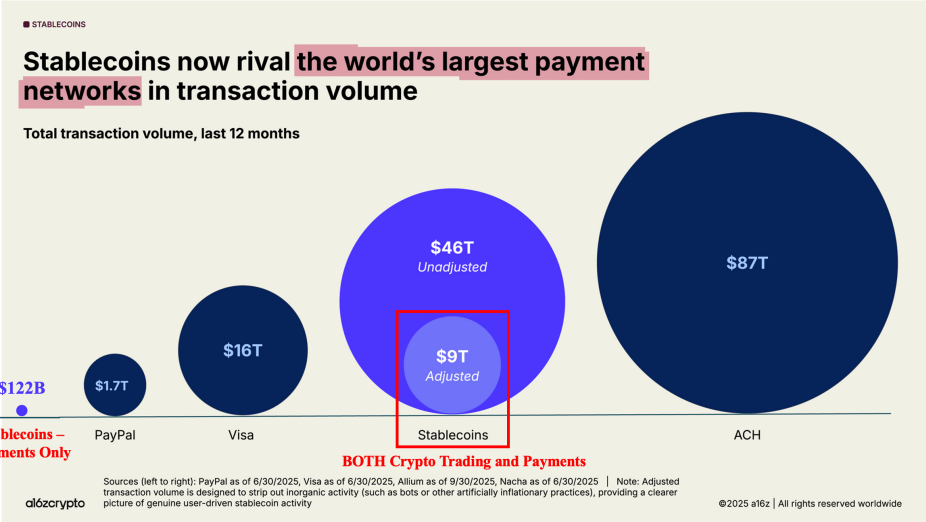


Stablecoins: The Data So Far



Source: Artemis bottoms-up analysis of 33 stablecoin payments companies. Includes P2P, B2B, Card, B2C and Prefunding payments. Artemis's methodology does not attempt to include DIY on-chain payments (e.g., using a MetaMask wallet). \$122B figure in the slide represents annualized run-rate based on most recent month of data (\$10.2B in the month of Aug 2025). This number is of the right order of magnitude when we look at the annualized run-rates of some of the largest stablecoin payments companies including Binance Pay, BVNK, Orbital and Conduit.

Stablecoins: The Data So Far



Source: Visa press release.

Stablecoins: The Data So Far



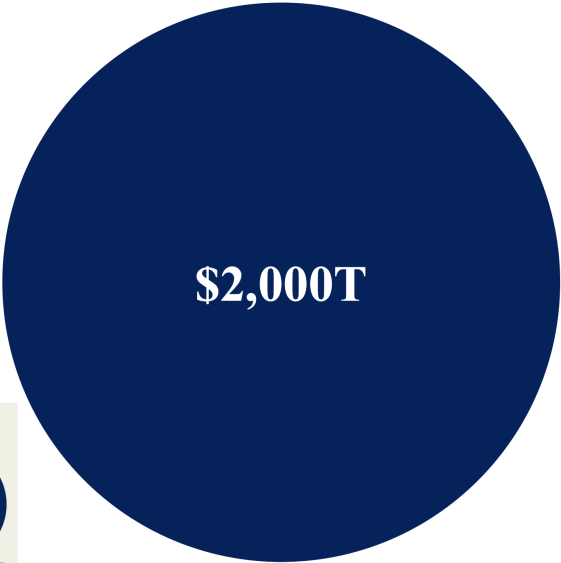
Stablecoins: The Data So Far



Fedwire Funds Service

Source: Federal Reserve Banks.

Stablecoins: The Data So Far



Global Payments Volume



Source: McKinsey 2025 Global Payments Report.

Stablecoins and Politics

Binance Holdings of World Liberty Financial USD (USD1)

Wallet	BNB Smart Chain	Ethereum	Solana	Tron	Total
Binance 28	1,098,981,057	–	–	–	1,098,981,057
Binance: Hot Wallet 20	605,152,926	659,503,932	–	–	1,264,656,858
Binance 51	54,327,678	–	–	–	54,327,678
Binance: Hot Wallet 12	3,928,800	–	–	–	3,928,800
Binance: Withdrawals 7	3,668,123	–	–	–	3,668,123
Binance: Hot Wallet 13	3,558,843	–	–	–	3,558,843
Binance: Hot Wallet 16	2,997,789	–	–	–	2,997,789
Binance: Hot Wallet 11	2,703,702	–	–	–	2,703,702
Binance: Hot Wallet 10	2,330,046	–	–	–	2,330,046
Binance: Binance-Peg Tokens	–	253,891,384	–	–	253,891,384
Binance 14	–	36,343,588	–	–	36,343,588
Binance Deposit	–	20,000,000	–	–	20,000,000
Binance 16	–	5,478,455	–	–	5,478,455
Binance 15	–	4,322,053	–	–	4,322,053
Binance 2	–	–	18,812,424	–	18,812,424
Binance 3	–	–	17,377,186	–	17,377,186
All Binance Wallets	1,777,648,964	979,539,412	36,189,609	–	2,793,377,985
All Non-Binance Holders	139,224,219	253,814,584	81,880,400	19,730,871	494,650,074
Current Total Supply of USD1	1,916,873,184	1,233,353,996	118,070,009	19,730,871	3,288,028,060

Source: Blockchain data from BNB Smart Chain, Ethereum, Solana and Tron, sourced from block explorer websites BscScan, Etherscan, Solscan and Tronscan, respectively. Total Binance holdings calculated as a sum across all Binance wallets in the top 50 holders of USD1 on each blockchain, sourced from each website's top holders section for USD1. The websites indicate which addresses are Binance wallets using public tags associated with each address. Current total USD1 supply for each blockchain sourced directly from each website's overview section for USD1. Aggregate supply across all blockchains matches figures reported by Coinbase, CoinMarketCap, and CoinGecko. Data accessed on January 2, 2026.

Overview of the Talk

Part I: Trust at Scale

Part II: Directions for Research

Conclusion

Overall Conclusion

- ▶ Budish (2025): crypto trust in its pure form doesn't work at scale.

Overall Conclusion

- ▶ Budish (2025): crypto trust in its pure form doesn't work at scale.
- ▶ Crypto trust in combination with rule of law? Jury is still out.

Overall Conclusion

- ▶ Budish (2025): crypto trust in its pure form doesn't work at scale.
- ▶ Crypto trust in combination with rule of law? Jury is still out.
 - ▶ Lots of old-fashioned financial speculation (get your Blackrock ETFs on the NYSE regulated by the SEC)

Overall Conclusion

- ▶ Budish (2025): crypto trust in its pure form doesn't work at scale.
- ▶ Crypto trust in combination with rule of law? Jury is still out.
 - ▶ Lots of old-fashioned financial speculation (get your Blackrock ETFs on the NYSE regulated by the SEC)
 - ▶ Lots of interesting computer science (Eth slashing, stubborn Nakamoto)

Overall Conclusion

- ▶ Budish (2025): crypto trust in its pure form doesn't work at scale.
- ▶ Crypto trust in combination with rule of law? Jury is still out.
 - ▶ Lots of old-fashioned financial speculation (get your Blackrock ETFs on the NYSE regulated by the SEC)
 - ▶ Lots of interesting computer science (Eth slashing, stubborn Nakamoto)
 - ▶ Lots of open conceptual questions (trust frontier)

Overall Conclusion

- ▶ Budish (2025): crypto trust in its pure form doesn't work at scale.
- ▶ Crypto trust in combination with rule of law? Jury is still out.
 - ▶ Lots of old-fashioned financial speculation (get your Blackrock ETFs on the NYSE regulated by the SEC)
 - ▶ Lots of interesting computer science (Eth slashing, stubborn Nakamoto)
 - ▶ Lots of open conceptual questions (trust frontier)
 - ▶ This is where the interesting innovation will be
 - ▶ And a great area for research

Overall Conclusion

- ▶ Budish (2025): crypto trust in its pure form doesn't work at scale.
- ▶ Crypto trust in combination with rule of law? Jury is still out.
 - ▶ Lots of old-fashioned financial speculation (get your Blackrock ETFs on the NYSE regulated by the SEC)
 - ▶ Lots of interesting computer science (Eth slashing, stubborn Nakamoto)
 - ▶ Lots of open conceptual questions (trust frontier)
 - ▶ This is where the interesting innovation will be
 - ▶ And a great area for research
- ▶ Crypto research
 - ▶ Optimistic and supportive
 - ▶ High-level advice: use crypto data / phenomena to study questions of broader interest to economics and finance
 - ▶ (trust, bubbles, crime, financial regulation, political economy, etc.)

Overall Conclusion

- ▶ Crypto prices?

Overall Conclusion

- ▶ Crypto prices?
 - ▶ No idea

Overall Conclusion

- ▶ Crypto prices?
 - ▶ No idea
 - ▶ I'm confident in continued low economic usefulness of crypto in its pure form.

Overall Conclusion

- ▶ Crypto prices?
 - ▶ No idea
 - ▶ I'm confident in continued low economic usefulness of crypto in its pure form.
 - ▶ A lot of the activity looks to me like a naturally occurring Ponzi process

Overall Conclusion

- ▶ Crypto prices?
 - ▶ No idea
 - ▶ I'm confident in continued low economic usefulness of crypto in its pure form.
 - ▶ A lot of the activity looks to me like a naturally occurring Ponzi process
 - ▶ But I've been saying that for a while

Overall Conclusion

- ▶ Crypto prices?
 - ▶ No idea
 - ▶ I'm confident in continued low economic usefulness of crypto in its pure form.
 - ▶ A lot of the activity looks to me like a naturally occurring Ponzi process
 - ▶ But I've been saying that for a while
- ▶ Two final words

Overall Conclusion

- ▶ Crypto prices?
 - ▶ No idea
 - ▶ I'm confident in continued low economic usefulness of crypto in its pure form.
 - ▶ A lot of the activity looks to me like a naturally occurring Ponzi process
 - ▶ But I've been saying that for a while
- ▶ Two final words
- ▶ First, while there hasn't been a majority attack of Bitcoin or another major cryptocurrency yet, there have been a LOT of attacks of smaller cryptocurrencies, large-\$ thefts of crypto projects, and collapses of crypto financial entities.

51% Attacks of Bitcoin and Ethereum Forks

Name of Coin	Date of Attack	Amount Stolen	Length of Largest Reorganization	Market Cap at Time of Attack	Market Cap at Peak
Bitcoin SV	8/3/2021	Unknown	Unknown	\$2.7 billion	\$8.3 billion
	6/24/2021	Unknown	Unknown	\$2.4 billion	
Ethereum Classic	8/29/2020	Unknown	7,000 Blocks	\$760 million	\$15.6 billion
	8/6/2020	\$1.7 million	4,200 Blocks	\$840 million	
	8/1/2020	\$5.6 million	3,700 Blocks	\$860 million	
	1/5/2019	\$1.1 million	140 Blocks	\$560 million	
Bitcoin Gold	1/23/2020	\$72 thousand	16 Blocks	\$190 million	\$7.6 billion
	5/16/2018	\$18.6 million	22 Blocks	\$1.0 billion	

Sources: Bitcoin Gold Forum, Bloomberg, CCN, Coinbase, CoinDesk, Cointelegraph, Decrypt, GitHub, Twitter, and <https://dci.mit.edu/51-attacks>. For a list of all articles consulted with URLs please see the author's website or the paper's online appendix. For interpreting length of longest reorganization, note that for Bitcoin SV and Bitcoin Gold there are typically 6 blocks per hour. For Ethereum Classic there are typically 275 blocks per hour. Amount Stolen is based on press reports of the dollar value stolen. Market cap data is from CoinMarketCap. The market cap at the time of attack is based on the day prior to the date of attack.

Attacks of Crypto Financial Entities (I/III)

Name	Type of Business	Date of Attack	Amount Stolen	Attack Vector
Poloniex	Centralized Exchange	November 2023	\$120 Million	Unknown
Mixin Network	Decentralized Exchange and Lending Protocol	September 2023	\$200 Million	Compromised Cloud Database
Multichain	DeFi Bridge	July 2023	\$230 Million	Compromised Private Keys or Rug Pull
Euler Finance	DeFi Lending Protocol	March 2023	\$197 Million	Flash Loan Attack + Flawed Code
FTX	Centralized Exchange	November 2022	\$477 Million	Compromised Private Keys
		March-April 2021	\$600 Million	Price Manipulation
Mango Markets	Decentralized Exchange	October 2022	\$100 Million	Price Manipulation
BNB Chain	DeFi Bridge	October 2022	\$568 Million	Flawed Code

Sources: BitMart, Bloomberg, Chainalysis, Coinbase, CoinDesk, CoinMarketCap, Cointelegraph, Elliptic Inc, Forbes, Going Infinite by Michael Lewis, Kraken Blog, Mango Markets, Medium Blog, Mixin Network, PolyNetwork, Reuters, The Verge, Twitter, Unchained Crypto, and WSJ. For a list of all articles consulted with URLs please see the author's website or the paper's online appendix. Amount Stolen is based on press reports of the dollar value stolen where available or based on press reports of the amount of cryptocurrency stolen converted into dollars using price data from CoinMarketCap.

Attacks of Crypto Financial Entities (II/III)

Name	Type of Business	Date of Attack	Amount Stolen	Attack Vector
Wintermute	DeFi Market Maker	September 2022	\$160 Million	Compromised Hot Wallet
Nomad	DeFi Bridge	August 2022	\$190 Million	Flawed Code
Horizon Bridge	DeFi Bridge	June 2022	\$100 Million	Compromised Private Keys + Governance Control
Beanstalk Farms	DeFi Stablecoin	April 2022	\$182 Million	Flash Loan Attack + Governance Control
Ronin Network	DeFi Bridge	March 2022	\$625 Million	Compromised Private Keys + Governance Control
Wormhole	DeFi Bridge	February 2022	\$320 Million	Flawed Code
Qubit Finance	DeFi Lending Protocol	January 2022	\$80 Million	Flawed Code
BitMart	Centralized Exchange	December 2021	\$150 Million	Compromised Private Keys

Sources: BitMart, Bloomberg, Chainalysis, Coinbase, CoinDesk, CoinMarketCap, Cointelegraph, Elliptic Inc, Forbes, Going Infinite by Michael Lewis, Kraken Blog, Mango Markets, Medium Blog, Mixin Network, PolyNetwork, Reuters, The Verge, Twitter, Unchained Crypto, and WSJ. For a list of all articles consulted with URLs please see the author's website or the paper's online appendix. Amount Stolen is based on press reports of the dollar value stolen where available or based on press reports of the amount of cryptocurrency stolen converted into dollars using price data from CoinMarketCap.

Attacks of Crypto Financial Entities (III/III)

Name	Type of Business	Date of Attack	Amount Stolen	Attack Vector
C.R.E.A.M. Finance	DeFi Lending Protocol	October 2021	\$130 Million	Flash Loan Attack + Price Manipulation
PolyNetwork	DeFi Bridge	August 2021	\$600 Million	Flawed Code
KuCoin	Centralized Exchange	September 2020	\$281 Million	Compromised Private Keys
BitGrail	Centralized Exchange	February 2018	\$170 Million	Unknown
Coincheck	Centralized Exchange	January 2018	\$530 Million	Unknown
The DAO	Decentralized Venture Capital	June 2016	\$55 Million	Flawed Code
Mt. Gox	Centralized Exchange	2011-2014	\$480 Million	Compromised Private Keys

Sources: BitMart, Bloomberg, Chainalysis, Coinbase, CoinDesk, CoinMarketCap, Cointelegraph, Elliptic Inc, Forbes, Going Infinite by Michael Lewis, Kraken Blog, Mango Markets, Medium Blog, Mixin Network, PolyNetwork, Reuters, The Verge, Twitter, Unchained Crypto, and WSJ. For a list of all articles consulted with URLs please see the author's website or the paper's online appendix. Amount Stolen is based on press reports of the dollar value stolen where available or based on press reports of the amount of cryptocurrency stolen converted into dollars using price data from CoinMarketCap.

Collapses of Crypto Financial Entities

Name	Type of Business	Date of Collapse	Entity Size
Genesis	Lending Firm	January 2023	\$5.1 billion
BlockFi	Lending Firm	November 2022	\$3.9 billion
FTX	Centralized Exchange	November 2022	\$8.9 billion - \$32 billion
Three Arrows Capital	Hedge Fund	June 2022	\$3.4 billion - \$10 billion
Voyager	Lending Firm	July 2022	\$5.8 billion
Celsius	Lending Firm	July 2022	\$5.5 billion - \$19.1 billion
Terra + Luna	Blockchain + Stablecoin	May 2022	\$40 billion
Africrypt	Investment Firm	April 2021	\$3.6 billion
Thodex	Centralized Exchange	April 2021	\$2 billion
Mt. Gox	Centralized Exchange	February 2014	\$480 million

Sources: BlockFi Blog, Bloomberg, Chainalysis, CoinDesk, Cointelegraph, Forbes, PR Newswire, Reuters, WSJ, and bankruptcy filings. For Celsius: the \$19.1 billion figure is Celsius's balance sheet size as of August 13, 2021 based on an investment memorandum provided to the author and reported in the Wall Street Journal in June 2022; the \$5.5 billion figure is Celsius's balance sheet size when it filed for bankruptcy. For FTX: the \$8.9 billion figure is FTX's customer assets at the time of its bankruptcy filing; the \$32 billion is its peak market valuation. For Three Arrows Capital: the \$10 billion figure is based on reports of the hedge funds size as of March 2022 and the \$3.4 billion figure is based on reports of claims from creditors. For Mt. Gox: the \$480 million figure is the reported value of customer Bitcoins reported lost by the exchange when it filed for bankruptcy. For a list of all articles consulted with URLs please see the author's website or the paper's online appendix.

Overall Conclusion

- ▶ Crypto prices?
 - ▶ No idea
 - ▶ I'm confident in continued low economic usefulness of crypto in its pure form.
 - ▶ A lot of the activity looks to me like a naturally occurring Ponzi process
 - ▶ But I've been saying that for a while
- ▶ Two final words
- ▶ First, while there hasn't been a majority attack of Bitcoin or another major cryptocurrency yet, there have been a LOT of attacks of smaller cryptocurrencies, large-\$ thefts of crypto projects, and collapses of crypto financial entities.

Overall Conclusion

- ▶ Crypto prices?
 - ▶ No idea
 - ▶ I'm confident in continued low economic usefulness of crypto in its pure form.
 - ▶ A lot of the activity looks to me like a naturally occurring Ponzi process
 - ▶ But I've been saying that for a while
- ▶ Two final words
- ▶ First, while there hasn't been a majority attack of Bitcoin or another major cryptocurrency yet, there have been a LOT of attacks of smaller cryptocurrencies, large-\$ thefts of crypto projects, and collapses of crypto financial entities.
- ▶ Second, let me leave you with the Bitcoin community's opinion of my research.
Big fans!

The Bitcoin Community



Pedro
@pedromvpg

Replying to @alexoimas
Have fun staying poor
4:51 PM · May 15, 2022



Pomp
@APompliano

Replying to @alexoimas
Sir, too much school is bad for thinking skills
5:29 PM · May 14, 2022



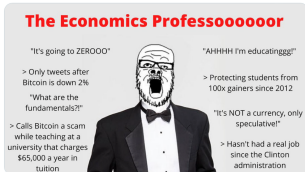
Dr Tufty Sylvestris
@tuftythecat

Replying to @alexoimas
TL;DR: Bitcoin incentivizes work in the real world, but don't work in Budish's theoretical world, therefore the real world must be wrong. QED.
12:02 PM · May 16, 2022



Cantillonaire Disrespector
@ToxicBitcoiner

Replying to @alexoimas
Fucking morons

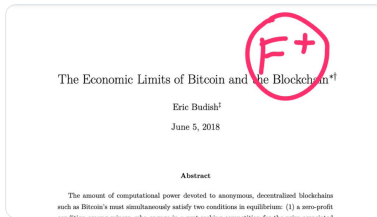


8:51 PM · May 14, 2022



Peter McCormack
@PeterMcCormack

Replying to @alexoimas

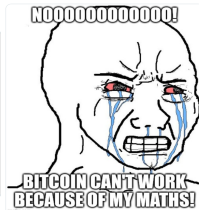


7:40 PM · May 14, 2022



J. Gatt, BTC Psychopath
@jgatt

Replying to @alexoimas



13% Monetary Mulligan
@MichaelPestura

Replying to @alexoimas



1:46 AM · May 15, 2022



Bitcoin Bergkamp
@BergkampBitcoin

Replying to @alexoimas

I read one paper by an economics professor and never took the profession or their opinions seriously again.

6:47 PM · May 14, 2022



Shayne in the Blockchayne
@ShayneOnChayne

Replying to @alexoimas

Oh wow, an academic paper. Imagine if your degree and theories actually produced something of actual value in the real world, would be good to get the mathematical limits of that.

6:35 PM · May 14, 2022



Ari Paul
@AriDavidPaul

Replying to @alexoimas

It was a decent stab at the game theory of PoW, but was a few years out of date by the time it was published. Wrote about it in real-time. Every idea in Budish's paper had already been covered by 2012.

6:27 AM · May 15, 2022



Darin Feinstein
@DarinFeinstein

Replying to @DarinFeinstein and @alexoimas

Lets say you were a behavioral economist and predicting behavior is what you are being paid to teach

why would you post your 2017 prediction ...that was so massively wrong, that every student now discredits your ability to make accurate predictions into the future?

6:23 PM · May 14, 2022