

Trust at Scale: The Economic Limits of Cryptocurrencies and Blockchains

Eric Budish
University of Chicago, Booth School of Business

October 28th, 2023
NBER Market Design

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
- ▶ Trust and security instead arise from a combination of cryptography and economic incentives. Completely anonymous and decentralized.
 - ▶ CS terminology: “permissionless consensus.” Agree on the truth w/out a trusted party.
 - ▶ “a new territory of freedom,” “outside the reach of any government”
- ▶ Nakamoto's invention enabled cryptocurrencies, including his own, Bitcoin
- ▶ The specific data structure maintained is called a blockchain

Nakamoto's Invention

- ▶ Nakamoto's invention captured the world's attention
- ▶ Recent peak: \$3 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, majority of volume appears speculative, with other widely-documented use case being black market (Makarov and Schoar, 2021; Foley et al., 2019; Yellen, 2021; Gensler, 2021; Buterin, 2022)
- ▶ Moreover, most of the speculative volume has been through cryptocurrency exchanges — which are, at least in principle, centralized, trusted financial intermediaries
 - ▶ So the largest volume use to date does not even take advantage of the novel form of trust

Adam Smith vs. Satoshi Nakamoto

- ▶ So which view is correct?
- ▶ Can trust and security be engineered from cryptography and incentives alone?
- ▶ Or is rule of law essential for the market system?

This Paper's Argument

- ▶ The paper shows that Nakamoto's novel form of trust — while undeniably ingenious — is economically implausible (at least in its literal form without implicit support from rule of law)
 - ▶ It is too expensive in absolute terms relative to the stakes involved
 - ▶ Its expense *scales linearly* with the stakes
- ▶ Put differently: if Nakamoto trust were to become more economically useful, then the costs of securing its trust would become preposterous
- ▶ Analysis serves as both
 1. an explanation for why cryptocurrencies and blockchains have not been very economically useful to date, and
 2. a reason to be skeptical that Nakamoto's anonymous, decentralized trust will play a major role in the global economy and financial system in the future.
- ▶ The paper will also sharpen our conceptual understanding of what is special about traditional forms of trust
 - ▶ Key distinction will be *economies of scale in the production of trust*

The Paper's Argument

- ▶ Core of the argument is just 3 equations.
- ▶ Equation (1): zero-profits condition.
 - ▶ The amount of computing power devoted to maintaining Nakamoto trust reflects the compensation paid to this computing power (called “miners”).
- ▶ Equation (2): incentive compatibility condition.
 - ▶ How much trust does a given level of computing power produce?
 - ▶ Vulnerability: “majority attack”.
 - ▶ IC: costs of attack must exceed the benefits.
- ▶ Together, (1)+(2) imply:
 - ▶ (3): recurring, “flow” payments to miners for maintaining the blockchain must be large relative to the one-off benefits of attacking the blockchain (“stock”-like).
 - ▶ Very expensive!
 - ▶ Especially as stakes grow! Scales linearly.
- ▶ Intuition: Nakamoto trust is “memoryless,” no scale economies.
- ▶ Under idealized attack circumstances, get an even stronger result:
 - ▶ “Zero net attack cost theorem”

The Paper's Argument

- ▶ So ... why hasn't Bitcoin already been attacked? (Chicago lunch table)
- ▶ A way out of the “extremely expensive” argument:
 - ▶ (i) mining technology is specialized/non-repurposable, and
 - ▶ (ii) majority attack causes collapse
- ▶ Why? Makes attack much more expensive.
 - ▶ Attacker pays not just the “flow” cost of attack, but the “stock” value of the now-worthless specialized mining computers.
 - ▶ 3-4 orders of magnitude difference in costs.
- ▶ This is good news about security costs, but vulnerability to collapse is itself a serious problem.
 - ▶ Especially if thinking about cryptocurrencies playing a meaningful role in global financial system.
 - ▶ “Pick your poison”
- ▶ Analysis points to specific collapse scenarios.
- ▶ Note: Ethereum PoS + “Slashing” is trying to make cost of attack a stock not a flow, but only works if attacker is small. (Tas et al, 2023; Lewis-Pye, Roughgarden and Budish, 2023).

Overview of the Talk

- ▶ Overview of the Nakamoto Blockchain
- ▶ Nakamoto Blockchain: A Critique in 3 Equations
- ▶ Analysis of Double Spending Attacks
- ▶ Analysis of Sabotage Attacks
- ▶ Collapse Scenarios
- ▶ Comparison of Nakamoto Trust and Traditional Trust
- ▶ Conclusion

Overview of the Talk

- ▶ **Overview of the Nakamoto Blockchain**
- ▶ Nakamoto Blockchain: A Critique in 3 Equations
- ▶ Analysis of Double Spending Attacks
- ▶ Analysis of Sabotage Attacks
- ▶ Collapse Scenarios
- ▶ Comparison of Nakamoto Trust and Traditional Trust
- ▶ Conclusion

What is Nakamoto Blockchain (1/4)

- ▶ **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'). Called "double spending."

- ▶ 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 (2/4)

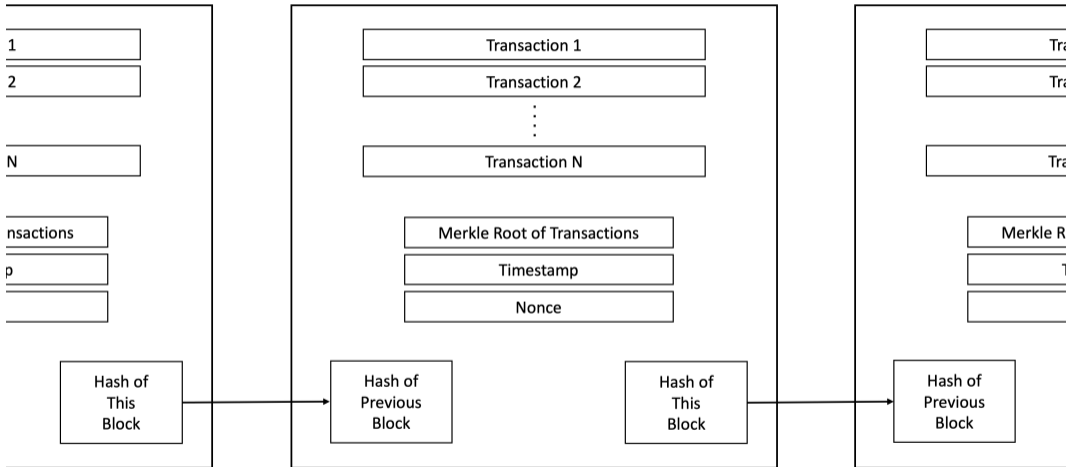
Nakamoto (2008) Blockchain Innovation

▶ I: Pending Transactions List

- ▶ Users submit transactions to a pending transactions list, called mempool
- ▶ Like a google spreadsheet — not considered official yet

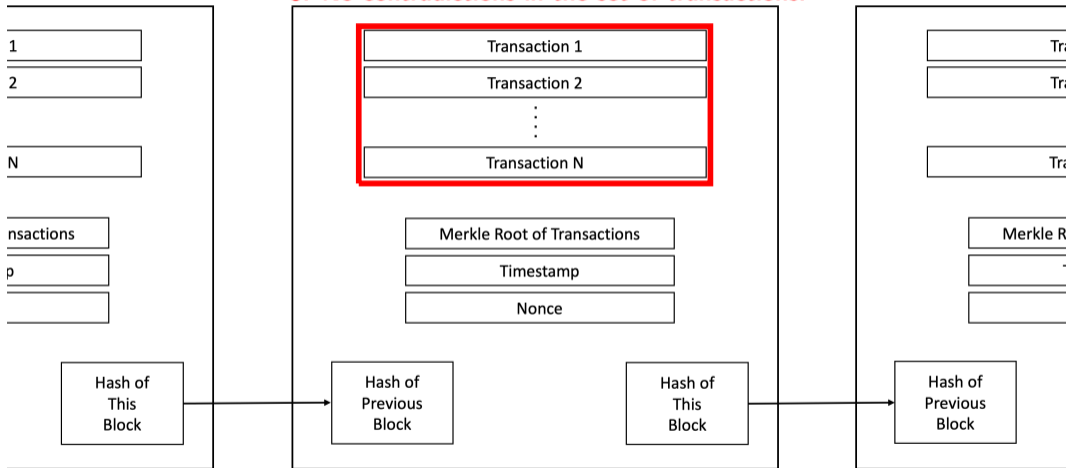
▶ II: Valid Blocks

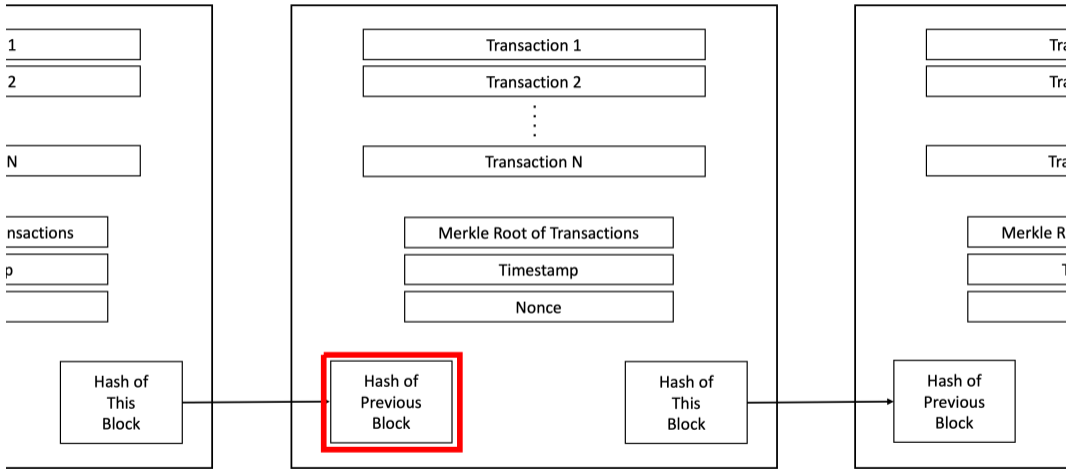
- ▶ Any computer around the world can compete for the right to add transactions from the mempool to a data structure called the blockchain. (Will describe competition next)
- ▶ Each new block of transactions "chains" to previous block, by including a hash of the data in the previous block (Haber and 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 (3/4)

▶ III: Bitcoin “Mining” Computational Tournament

- ▶ 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. Because cryptographic hash functions like SHA-256 are:
 - ▶ Deterministic
 - ▶ Non-invertible (other than brute force)
 - ▶ Pseudo-random (small changes to input lead to completely different output)
- ▶ Bitcoin’s current hash rate: about 350 million TH/s (3.5×10^{20})

SHA-256 Hash Function: Example

Name	SHA256 Hash	Name	SHA256 Hash
Nikhil Agarwal	534dab9b320deb919af5c902a1863ba7e2e9a28997ab09407be0a47543109f6	Patrick Agte	793f05667a13ab6f15c8e08bd2d91b478cc80c105f3a180f30b02f87c400d820
Claudia Allende	50f2a93835480197a4d9b640724e48713bbd856a71bf9dfb979397e204f85da85	Daniel Aronoff	3bc90109fc906b8663b793bb6081f9c15b335709afdbec830981c1b14dadcb81
Lawrence Ausubel	f951cda93b6cd470992226c29540d46f35f96d49f6db3094b93b9c8ca85cc131	Ian S. Ball	a5bc5ce30546125f6af983c9779dfba632683a8da54fe5aa81e9f85b9c4ef0fb
Martino Banchio	a2fe70e1f172657b7f56621ad55f9b02a249a957b9961f3396420d818e7728285	Dirk Bergemann	35e9b858dbff6dc82c30298dabb6251bfed7c402971e4a9e1666295e3400928
Eric Budish	2266d7c0f93bb9c5baf1be47ed5f416f6cd2b41c30721a45ad6bae5977867c16	Juan Camilo Castillo	0ba4c82457382286a8d7cf68204e12cc38d02a5c38335f08349f82244168
Oguzhan Celebi	2bda967c9d50a6f194404d16cc7bf3a32eccc984bd8e5b2993109a7b17c1411c	Alex Chan	58f3a5d47e59e1071155956ffa2abd200c6acd86c2b2f84a8d204836172d19
Daniel Chen	4aea1aabadbcb812454ca74e6dfbe1ac230b21878be14505ab39d1c34dc5f38a7	Peter Cramton	1bf69cecc7b693529b9987c30429e1176ab15471a166d99023708281861dca91
Luciano I. de Castro	6190e2c96ce94fd7414bf35fde4761dddd21bb2bdcf574c2809213371df28af	David Delacretaz	a4ef8e22724a06983d504c5047a2d4008be6d63827cd7e341a865ed5a3c05cc4
Wouter Dessen	798b1ce13d029e0442138592f9941753fba4bec77be34ecf051007106365c1	Laura Doval	cdc39475e56c574291a10bbecc7657e699727a6c1fb63cd646036d1eb6a0ed04e
Jeremy T. Fox	d7080b5a442d7f55eb5d7aa5a1f8cd87e0f2cc7720294aabf1aed50dfb09732	Drew Fudenberg	cf4d1c5217f762ac6d80986227e259356d3bd5326cec3bbfe4a3a454512f4eeb
Diego Gentile Passaro	5c1d006ae7d55701920ba0d7e8e639ddbe4c12b19dc9617dfbc4f78a11202ccb	Yannai A. Gonczarowski	b74591c331c6f8a2a500541182861005c99662e09354c20acc84072fa3ed63
Alexander Haberman	cd4a8ae98472ecc327a87516be0bd605aa68cc454b386fed34519239a75f15	Guillaume Haeringer	cd91749f996992a25f5c1dc6926239a7186a624c7c7f4c5a24c7c07f550
Dong Woo Hahn	061d8dbddaf1fb74022a931e0c2fcb2e0246a7e8707774a6c8d8cfe51d8e3adc	YingHua He	abd8a67d3d67db74a265d8a9a818bedd615eeb0597f9b04e311d09a4ff959a1
Clemence M. Idoux	b5a018630f1773b7d9d2a7f5057107a8a6c0aa753489a7ffad0db0db51780474	Nicole Immorlica	5f0539de379f9d5c85c57d4a874e988f6995a17027a31d23e077000e15d3b43
Ravi Jagadeesan	714fa2c238c88a1558f9dc5cd9a86aa2d0934466030e9ed55cc3ba47ec09a28	Zi Yang Kang	d1654d7a6b22cd3e35d5222b904c5ba5019525b846703778c5e98f66163a37d
Adam Kapur	0fb39f06629908f13419dd1d0c2d51aaef8166a3cd714b75d5f4e56966814e	Navin Kartik	85f06b56461ee6a8105fb40d590ffe36751c34ec37bd52d9477d5594428b774
Jakub Kastl	985c369f70241c3274edc5e3a766935cc3d1031a11f862c2191a9c2319ce0e9	Judd B. Kessler	03da2b35489614cf68c82fa5c32c0bd3e91e6f7054c6f524a57de1cfc580be44
John Lazarev	ccfc7fb7fec9390e0cad3ad7ab7bdb599edc05f2a70479d0154a085c14825b	Kwok Hao Lee	048c26b7e83c7f6c22e6b8d42209ac4aaf53ffccf80985978e40a75f2b6a0967
Jacob D. Leshno	01bd9ab65ee8287602a609813a4753c8fed80f1d349a98deb3bae57e82c1699	Hao Li	0fad5e498f675f36af215749086dccc8deb3aa77c37e5bd7a0420e2fca8b3350
Shengwu Li	62f63590404c5e685054d86895a3e958294d8133708f085716d87541b9e863c	Irene Y. Lo	ede5b47e6e946a4c3b0e8a5d688130ad0beca38b9edad3a66c6c1b79022d70
Brendan Lucier	d9718ba2be14660259f31b6ea73f26425c9f88f81843dce57646d7549c373fa	Hongyao Ma	02777df6ca202fa754affb6ea01d203e337c2d0a6eb0373633466733fa9a21
Stephen Morris	c06e286b4aa7fd112ac6f8a3f2c6ad888093628f63d5ecc3aee3305f1ec4	Ellen Muir	e456bd9f5e68b580b773b9770846d68ab295ef49277a6f2ae0b3cdd366bbad5
Christopher Neilson	e83c3888fae096982365ef8650d4584e297c0fdb6ad9a600174c0f393bf70	Fernando Ochoa	6ea25ae7de95e602bd0ae82ebdb4a0e651f102200a9dd2d0a0c072d41b5b48
Michael Ostrovsky	b7bdbdf42ecbe53b2e296e22ef9d1d1623de256e6b702c317990767a7e518b56	Bobak Pakzad-Hurson	dda782a93600045b6e7e093e630e5af75ca5ae2f1b35716db03987200b203800
Parag A. Pathak	c8021373539106531edcb265ba65b94f6d6aed37879db4da312bca8788cfe35	Daniel Quint	f3c08c5b3228accf520b9f7210ef0ae782eed51216440039d3caca01c0dd0d57
Alex Rees-Jones	e4032f22812ba31ad427610bcd94890b42e30bc4895cfee812b9c83353	Eric Richert	8d39b8c92a80b91a0262c70b44dc3b0f0d8973e85ca0266336604e05987fd9dd6
Marzena Rostek	0e68efa4ab8cb0e0b597199dd20e3543e650608641a884cf6ca350a739c9be	Anna Russo	f04ba03a5692f8cd561195b81da26143ec9751a64094c864ef12f3ba4017a3
Tobias Salz	4b3b784be4c54edcfc6c56c0e93d00bb12d443bc842b1495406146f61b3131b1	Tayfun Sonmez	df70c49f6a9b873c9ee2b8899a230238286aadd116bd1855becce5a80ff1db54
Alexander Teytelboym	db2da1117c1fc1662090fee690083c15b72b9d966ba29b241b8e74b0778a72	Juuso Toikka	6c18efab6056df6e36ef9bfe7a12f982dc76696cba3b17c7dc446833ac36d6
M. Utku Ünver	be21c48db12dbb2551c677036f1e4cb39e18d983897f11347488d9ed6bfff50f7	Quitze Valenzuela-Stookey	bf8dd3e74d84c462a67e996ccdad0c6c197c5ef381c1d2c0cc480a3839d452

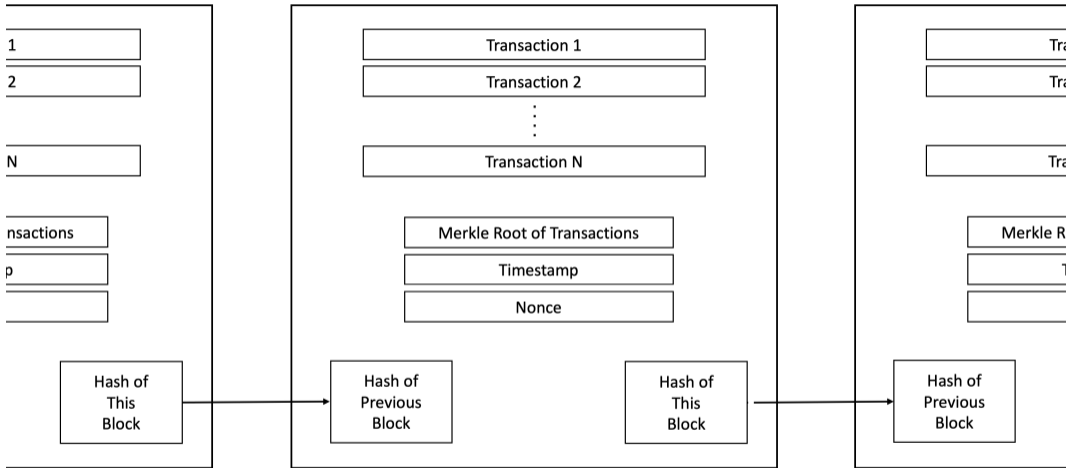
SHA-256 Hash Function: Example

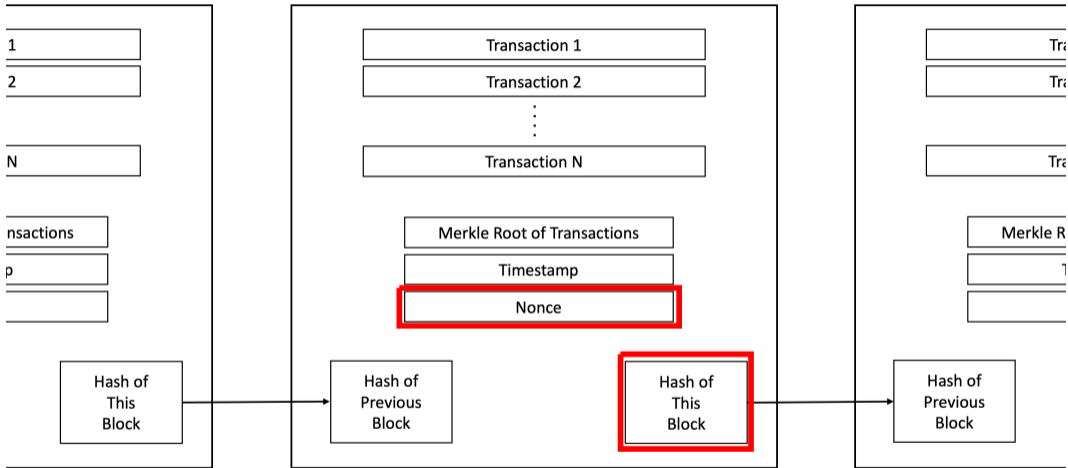
Name	SHA256 Hash	Name	SHA256 Hash
Nikhil Agarwal	534dab9b320deb919af5c902a1863ba7e2e9a28997ab09407be0a47543109f6	Patrick Agte	793f05667a13ab6f15c8e08bd2d91b478cc80c105f3a180f30b02f87c400d820
Claudia Allende	50f2a93835480197a4d9b6407242e48713bbd856a71df9bf9397e204f85da85	Daniel Aronoff	3bc90109fc906b8663b793bb6081f9c15b335709afdbec830981c1b14dadcb81
Lawrence Ausubel	f951cda93b6cd470992226c29540d46f35f96d49f6db3094b93b9c8ca83c131	Ian S. Ball	a5bc5ce30546125f6af983c9779dfba632683a8da54fe5aa81e9f85b9c4ef0fb
Martino Banchio	a2fe70e1f72657b7f56621ca55f9b02a249a957b9961f3396420d818e7728285	Dirk Bergemann	35e9b858dbf6dc82c30298dabb6251bfed7c402971e4a9e1666295e3400928
Eric Budish	2266c7d0f3b99c5baf1be47ed5f416f6c2b41c30721a45ad6fbae597f867c16	Juan Camilo Castillo	0ab4c8245738f2286a8d7cf68204e12cc38d02a5c383835a0834af82244168
Oguzhan Celebi	2bba967cd95a6ff194404d16cc7bf3a23eccc984bd8e5b2993109a7b71c1411c	Alex Chan	58f3a5d47e59e107115595dff2a2add200cc6acd8fba2b84a8d204836172d19
Daniel Chen	4aea1aabadbcb812454ca74e6dbfe1ac230b21878be14505ab39d1c34dc5f38a7	Peter Cramton	1bf69c8cc7b693529b9987c30429e1176ab15471a166d99023708281861dca91
Luciano I. de Castro	6190e2c96ce94fd7414bf35fde4761ddddd21bb2bdcf574c2809213371df28af	David Delacretaz	a4ef8e22724a06983d504c5047a2d4008be6d63827cd7e341a865ed5a3c05cc4
Wouter Dessen	798b1ce13d029e0442138592f0941753fba4bec77be34ecf05107106365c1	Laura Doval	cdc39475e56c574291a10bbecc7657e699727a6c1fb63cd64d036d1eb6a0e0de4
Jeremy T. Fox	d7080b5a442d7f55eb5d7aa5a1f8cd87e0f2cc7720294aabf1aed50dfb09732	Drew Fudenberg	cf4d1c5217b762ac6d80986227e259356d3bd5326cc3bbfe4a3a454512f4eeb
Diego Gentile Passaro	5c1d006ae7d557019208a0d7e8e639ddbe4c12b19dc9617dfbc4f78a11202ccb	Yannai A. Gonczarowski	b74591c331c6f8a2a500541182861005c99662e09354c20acc84072a3ed63
Alexander Haberman	cd4a8ae98472ecc327a87516be0bd605aa68cc454b386fed34519239a75f15	Guillaume Haeringer	cd91749f969992a25f5c1dc6926239a7186a624c7c7f4c5a24c7c07f550
Dong Woo Hahn	061d8dbddaf1fb74022a931e0c2fcb2e0246a7e8707774a6c8d8cfe51d8e3adc	YingHua He	abd8a67d3d67db74a265d8a9a818bedd615ee0b9597f9b04e311d09a4b4ff59a1
Clemence M. Idoux	b5a018630f1773b7d9d2a7f5057107a8a60caa753489a7ffad0db0d51780474	Nicole Immorlica	5f0539de379f9d5c85c57d4a874e988f6995a17027a31d23e077000e15d3b43
Ravi Jagadeesan	714fa6c2c38c88a1558f9dc5cd9a86aa2d0934466030e9ed553ca4b7ec09a28	Zi Yang Kang	d1654d7a6b22cd3e35d5222b904c5ba5019525b846703778e5e98f66163a37d
Adam Kapor	0fb39f06629908f13419dd1d0cd251aaef8166a3cd714ba75df54e5696e814e	Navin Kartik	85f06b5641ee6a8105fb40d590ffe36751c34ec37bd52d947d55944228b774
Jakub Kastl	985c369f70241c3274edc5e3a766935cc3d1031a11f862c2191a9e2319ce0e9	Judd B. Kessler	03da2b35489614c6f8c2fa5c32c0bd3e91e6f7054c6f524a57de1cfc580b0e44
John Lazarev	ccfc7fb7ef9390e0cad3ad7ab7bdb599edc05f2a70479d0154a085c14825b	Kwok Hao Lee	048c26b7e83c7f6c22e6b8d42209ac4aaf53ffcc80985978e40a75f2b6a0967
Jacob D. Leshno	01bd9ab65ee82760a2a609813a4753c8df80f1d349a98deb3bae57e82c1699	Hao Li	0fad5e98f675f36af215749086dc8deb3aa77c37e5bd7a0420e2fca8b3350
Shengwu Li	62f63590404c5e685054d86895a3e958294d8133708f085716d87541b9e863c	Irene Y. Lo	eed547e6e946a4c3b0e8a5d688130ad0beca8b9edad3a66c6c1b79022de70
Brendan Lucier	d9718ba2be14660259f31b6ea73f26425c9f88f81843dce5766d7549c373fa	Hongyao Ma	02777df6ca202fa754affb6ea01d203c337c2c0a4be0b837363346673a9a21
Stephen Morris	c06e286b4aa7fd112ac6f8a3f2c6ad888093628f5632ecc3aee3305f1ec4	Ellen Muir	e456bd9f5e68b580b773b9770846d68ab295ef49277a6f2ae0b3cdd366bbad5
Christopher Neilson	e83c3888fae096982365ef8650d4584e297cc0fdb6ad9a600174c0f393bf70	Fernando Ochoa	6ea5ae7de95e602b0daeb28dd4ba0e651f102200a9dd2d0a0c072d41b5b48
Michael Ostrovsky	b7bdbdf42ecbe53b2e296c22ef9d1d1623de256e6b702c317990767a7e518b56	Bobak Pakzad-Hurson	dda782a93600045b6e70093630e5af75ca5ae2f1b35716db03987200b203800
Parag A. Pathak	c8021373539106531edcb265ba65b94f6d6aed37879db4da312bca87886ce35	Daniel Quint	f3c08c5b322a8ac5f20b9f7210ef0ae782eed51216440039c3caaa01c0dd0d57
Alex Rees-Jones	e4032f2281281a2ba31ad427610bcd94890b42e303bc4895cfce812b9c83353	Eric Richert	8d396b8c92a80b91a0262c70b44dc3b0fd08973e85ca0266336604e05987d9dd6
Marzena Rostek	0e68fa4ab8bb0e0b597199dd20e3543e650608641a884cfbca350a7739cde	Anna Russo	f04ba03a5692f8cd561195b81da26143ec9751a64094c864af12f3ba4017a3
Tobias Szal	4b3b784be4c54edcfc6c56c0e93d0bb12d4ba3c842b1495046164bf6131b1	Tayfun Sonmez	df70c49f6a9b873c9ee2b8899a230238286add116bd1855bec5a80eff1db54
Alexander Teytelboym	db2da11177c1fc1662090fee690083c15b72b9d966ba29b241b8e74b0778a72	Juuso Toikka	6c18efab6056df6e36ef9bfe7a12f982dc76696cba3b17c7dc4db46833ac36d6
M. Utku Ünver	be21c48db12dbb2551c677036f1e4cb39e18d983897f11347488d9ed6bf50f7	Quitze Valenzuela-Stookey	bf8dd3e74d8c462a67e996ccdad0c6c197c5ef381c1d2c0cc480a38394452

What is Nakamoto Blockchain (3/4)

▶ III: Bitcoin “Mining” Computational Tournament

- ▶ Miner who finds a lucky hash broadcasts their new block
- ▶ Other miners check validity (fast), then start working on the next block (will describe why on next slide)
- ▶ Winner is compensated
 - ▶ Paid in newly issued Bitcoins.
 - ▶ Initially 50 Bitcoins per block.
 - ▶ Currently 6.25. Halves every four years. Zero by 2140.
 - ▶ Winner also earns small transaction fees.
 - ▶ Currently small as a fraction of total compensation. I will ignore for the purpose of this talk.
 - ▶ See Huberman, Leshno and Moallemi (2021) on the economics.
- ▶ Tournament difficulty adjusts every two weeks, calibrated to take about 10 minutes





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

Example from Block 729,999:

- Hash: 00000000000000000000000008b6f6fb83f8d745...

What is Nakamoto Blockchain (4/4)

▶ IV Longest-Chain Convention

- ▶ Once a miner finds a lucky alphanumeric string, all miners are supposed to move on to mining 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
 - ▶ What makes the Bitcoin blockchain real and the “Budish blockchain” (run from my laptop) an imposter? Answer: the work.
- ▶ 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.
 - ▶ (Not surprising that it is vulnerable. Decentralized consensus that pre-dates Nakamoto, based on Byzantine Fault Tolerance, vulnerable to $\frac{1}{3}$ attack)

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.

Overview of the Talk

- ▶ Overview of the Nakamoto Blockchain
- ▶ **Nakamoto Blockchain: A Critique in 3 Equations**
- ▶ Analysis of Double Spending Attacks
- ▶ Analysis of Sabotage Attacks
- ▶ Collapse Scenarios
- ▶ Comparison of Nakamoto Trust and Traditional Trust
- ▶ Conclusion

Zero-Profit Condition (Blockchain Miners)

- ▶ Conceptual question: how much computational power will maintain Nakamoto's anonymous, decentralized trust, if we restrict all to behave honestly?
- ▶ Treat time as continuous
- ▶ N : amount of computational power
 - ▶ Large finite number of honest miners
 - ▶ Follow longest chain protocol automatically
 - ▶ Player i chooses qty of computing power x_i . Define $N = \sum_i x_i$.
 - ▶ Eqm concept will be zero-profit. Captures permissionless, free entry/exit.
- ▶ p_{block} : compensation per block paid to the miner that wins the computational tournament
 - ▶ Assume exogenous. Will derive constraints below.
 - ▶ Proportional rule: player i wins a given block with prob. $\frac{x_i}{N}$
- ▶ c : cost per unit time to run one unit of computing power
 - ▶ Includes rental cost of capital and variable costs ($c = rC + \eta$)
 - ▶ Can generalize to have an upward sloping supply curve

Zero-Profit Condition (Blockchain Miners)

- ▶ D : block difficulty level. Defined as how many units of compute-time are needed in expectation to solve one block (assume Poisson arrivals)
- ▶ Honest miner profits: if N units of computing power, D difficulty
 - ▶ Some miner solves a block every $\frac{D}{N}$ time in expectation.
 - ▶ Profits per unit of compute per unit time are thus

$$\frac{1}{N} \frac{D}{N} p_{block} - c$$

- ▶ Definition. A zero-profit honest mining equilibrium consists of quantities $\{x_i^*\}_{i=1}^I$ and a difficulty level D^* such that miners (i) solve one block per unit time (as a normalization), and (ii) earn zero economic profits in expectation.
- ▶ Result: Let $N^* = \sum_i x_i^*$. In any zero-profit honest mining equilibrium, $D^* = N^*$ and

$$N^* c = p_{block} \tag{1}$$

- ▶ Note: (1) widely known (many papers, Bitcoin Wiki).
- ▶ Note: if use Nash eqm for entry, still restrict to honest play, then $N^* c < p_{block}$

Incentive Compatibility (Majority Attack)

- ▶ Conceptual question: how much security is generated by the amount of honest mining in (1)?
- ▶ Vulnerability: an attacker with $> 50\%$ of total computational power can double-spend with probability one.
- ▶ Attack costs
 - ▶ Consider an additional player, the attacker, not restricted to honest play.
 - ▶ Can attack by choosing AN^* units of computing power, $A > 1$, for an $\frac{A}{A+1}$ majority
 - ▶ Cost per unit time: AN^*c
 - ▶ Expected duration of attack: $t(A)$. Will derive closed form in next section under assumptions.
 - ▶ Call $AN^*c \cdot t(A)$ the gross cost of attack.
- ▶ Attacker can minimize $A \cdot t(A)$: call this $A^* \cdot t(A^*)$
- ▶ 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 Bitcoin's importance / usefulness grow.

Incentive Compatibility (Majority Attack)

- ▶ Definition. The blockchain is incentive compatible against an outsider attack, on a gross-cost basis, if the gross cost of attack exceeds the benefits of attack:

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

- ▶ 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 mining. Cheaper: as little as $\frac{N^*c}{2}$ per unit time
 - ▶ Outside attacker seems more attractive as a conceptual approach. Treats the honest miners 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, and miners are concentrated (Makarov and Schoar; Cong, He and Li)
- ▶ Gross vs. Net Cost
 - ▶ (2) is a gross cost. In Bitcoin, attacker would earn block rewards for the blocks in their new chain, so Net < Gross. Will come back to this.

Critique in 3 Equations

The Problem

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

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

- ▶ Proposition. *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 miners for maintaining the blockchain has to be large relative to the one-off benefits of attacking it*
- ▶ Flow payment to miners > Stock-like value of attack

Critique in 3 Equations

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

- ▶ Remarks:
- ▶ Economics: *very expensive* form of trust. Memoryless.
 - ▶ Usual alternatives: reputations, relationships, collateral, rule-of-law.
 - ▶ Imagine a brand only as trustworthy as its flow investment in advertising. Or a military only as secure as # of soldiers on border.
 - ▶ 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.
- ▶ 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, force, laws.
 - ▶ 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
- ▶ Reason 1: Attacker earns block rewards from the attack
 - ▶ An A attacker who mines for t time performs $At \cdot N^*$ compute-units of work.
 - ▶ If difficulty stays constant at $D' = D^* = N^*$, earns At block rewards in expectation
- ▶ Reason 2: Attacker may face frictions relative to honest miners
 - ▶ Ex: attacker compute power may be less energy efficient, start/stop costs
 - ▶ Let $\kappa \geq 0$ parameterize cost inefficiency, s.t. cost is $(1 + \kappa)At \cdot N^*c$
- ▶ Reason 3: Attack may harm post-attack value of Bitcoin
 - ▶ This reduces value of block rewards, value of Bitcoins kept in double-spend attack. (Assume for now capital is repurposable and retains its value.)
 - ▶ Let $\Delta_{attack} \geq 0$ parameterize decline.
 - ▶ Reduces block rewards by $\Delta_{attack}At \cdot N^*c$
 - ▶ Reduces benefit of attack by $\Delta_{attack}V_{attack}$

Net Cost of Attack and a “Zero” Theorem

- ▶ Theorem: *if the attacker’s cost is the same as honest miners ($\kappa = 0$), the attack concludes before difficulty adjusts ($D' = N^*$), and the attack does not cause the value of Bitcoin to fall ($\Delta_{attack} = 0$), then the net cost of attack is zero.*
- ▶ Proof:
 - ▶ Computational cost of attack: $(1 + \kappa)At \cdot N^*c$
 - ▶ Net value of block rewards: $At \cdot \frac{N^*}{D'} p_{block}(1 - \Delta_{attack})$
 - ▶ If $\kappa = \Delta_{attack} = 0$, $D' = N^*$, 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 computational costs for same reason as honest miners are fully compensated for their costs under honest play.
- ▶ Implication: Bitcoin’s security relies on either attacker cost frictions or the presumption that attacks would cause a large decline in the value of Bitcoin.
- ▶ (To be clear: zero frictions and zero decline seem unrealistic, but are useful as a benchmark case.)

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

- ▶ Some of the complexity in analysis relates to timing issues and/or conventions specific to Bitcoin
 - ▶ Costs are per unit time
 - ▶ Payments are per block – stochastic arrivals
 - ▶ Attack duration is stochastic
 - ▶ Difficulty adjustment
- ▶ 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 in which all players i choose $a_i = \text{Honest}$ (and some x_i^* consistent with NE)
- ▶ Lemma. If there is an honest equilibrium, then $N^*c \leq p$. (1)
- ▶ Theorem. Necessary condition for no player to have a profitable attack: $p \geq \frac{V_{\text{attack}}}{1 + \frac{1}{l}}$ (3)
- ▶ Proof of Theorem.
 - ▶ Honest play payoff for i : $\frac{x_i^*}{N^*}p - x_i^*c$
 - ▶ Attack payoff for i : $V_{\text{attack}} - N_{j \neq i}^*c$ (where $N_{j \neq i}^* = \sum_{j \neq i} x_j^*$)
 - ▶ Need: $V_{\text{attack}} - N_{j \neq i}^*c \leq \frac{x_i^*}{N^*}p - x_i^*c$. (If $x_i^* = 0$, this is $N^*c \geq V_{\text{attack}}$, which corresponds to (2))
 - ▶ Rearrange and use Lemma: $V_{\text{attack}} \leq p + \frac{x_i^*}{N^*}p$
 - ▶ Using smallest x_i^* : $V_{\text{attack}} \leq p(1 + \frac{1}{l})$. QED.
- ▶ As l goes to infinity, condition is $p \geq V_{\text{attack}}$
- ▶ Interpretation: p, c , now both represent a unit of time commensurate with duration of attack. (Analog of $A^* \cdot t(A^*)$ in (3))

The Flow-Stock Problem, Illustrated



Traditional Security Model



Traditional Security Model



Traditional Security Model



Traditional Security Model:

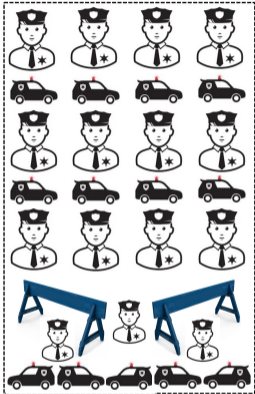
Traditional Security Model



Traditional Security Model:

- ▶ Security Guards

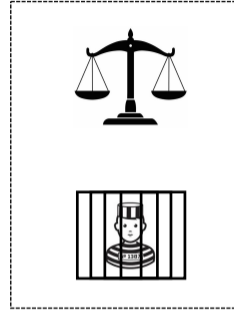
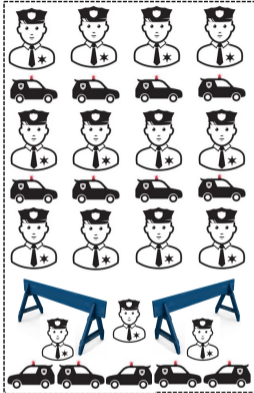
Traditional Security Model



Traditional Security Model:

- ▶ Security Guards
- ▶ Police Reinforcements

Traditional Security Model



Traditional Security Model:

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

Bitcoin Security Model



Bitcoin Security Model



Bitcoin Security Model



Bitcoin Security Model



Bitcoin Security Model:

Bank Security Model



Bitcoin Security Model:

- ▶ Large amount of Security Guards

Bank Security Model



Bitcoin Security Model:

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

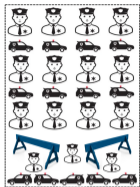
Bank Security Model



Bitcoin Security Model:

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

Comparison of Security Models



Traditional Security



Bitcoin Security

cost of overcoming guards +
cost of overcoming police reinforcements + $> V_{attack}$
risk \times punishment if caught

cost of overcoming guards $> V_{attack}$

Key contrast:

- ▶ Traditional security benefits from economies of scale, from police, and Beckerian deterrence from punishment.
- ▶ Bitcoin security only as strong as number of guards at the front of the bank.
- ▶ This works, but it's dramatically more expensive and scales badly.

Overview of the Talk

- ▶ Overview of the Nakamoto Blockchain
- ▶ Nakamoto Blockchain: A Critique in 3 Equations
- ▶ **Analysis of Double Spending Attacks**
- ▶ Analysis of Sabotage Attacks
- ▶ Collapse Scenarios
- ▶ Comparison of Nakamoto Trust and Traditional Trust
- ▶ Conclusion

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
 - ▶ 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

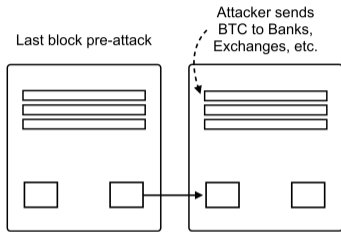


Illustration of Double Spending

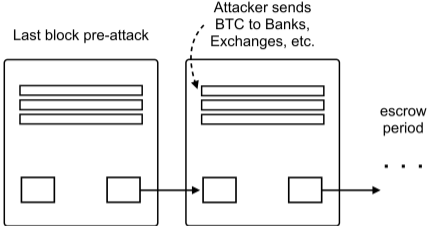


Illustration of Double Spending

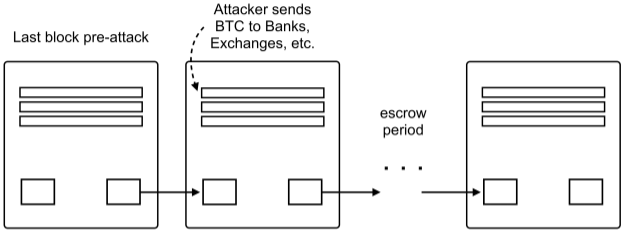


Illustration of Double Spending

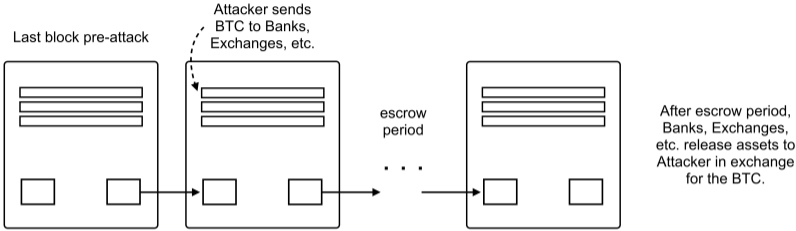


Illustration of Double Spending

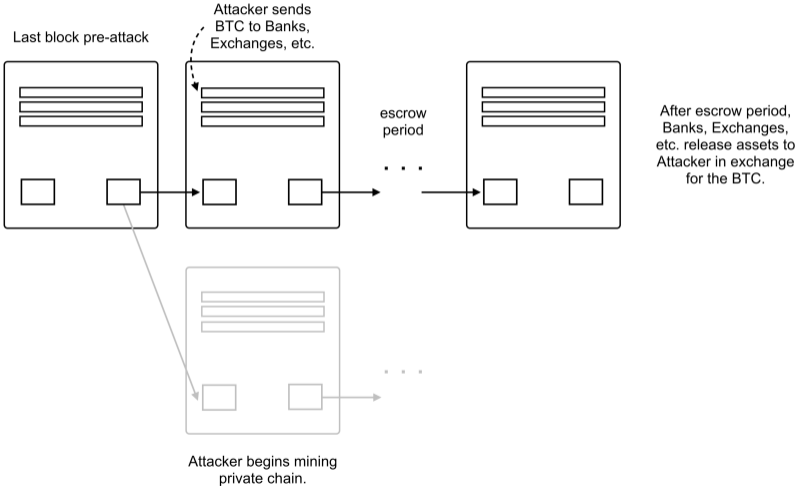


Illustration of Double Spending

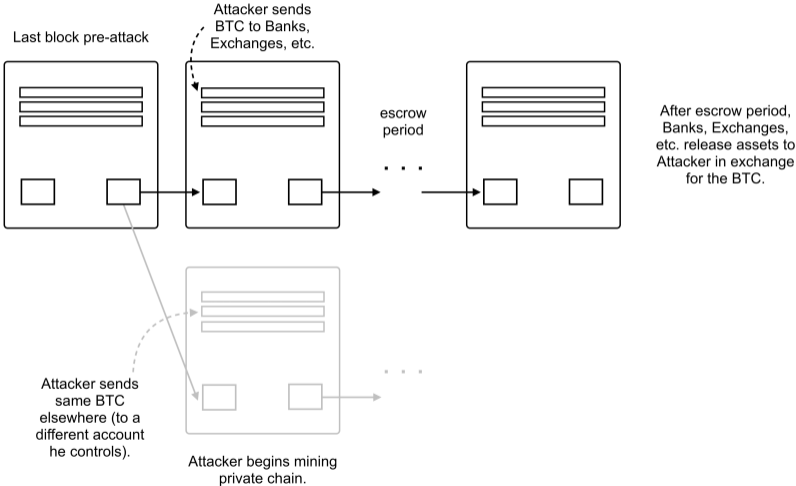


Illustration of Double Spending

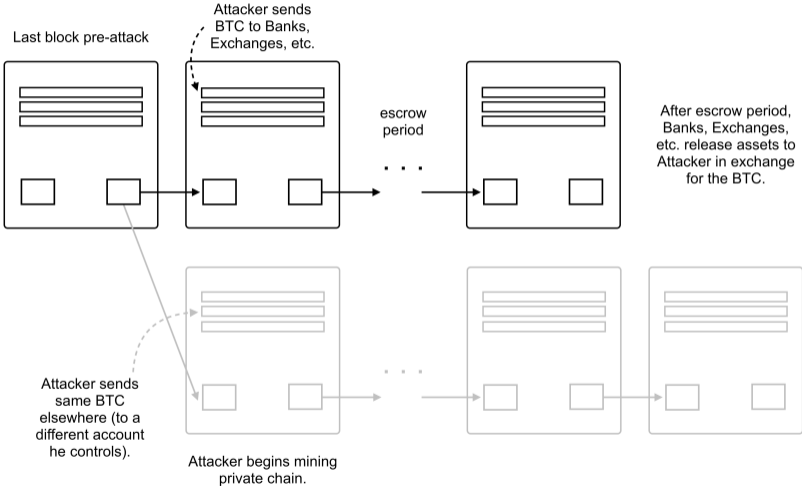
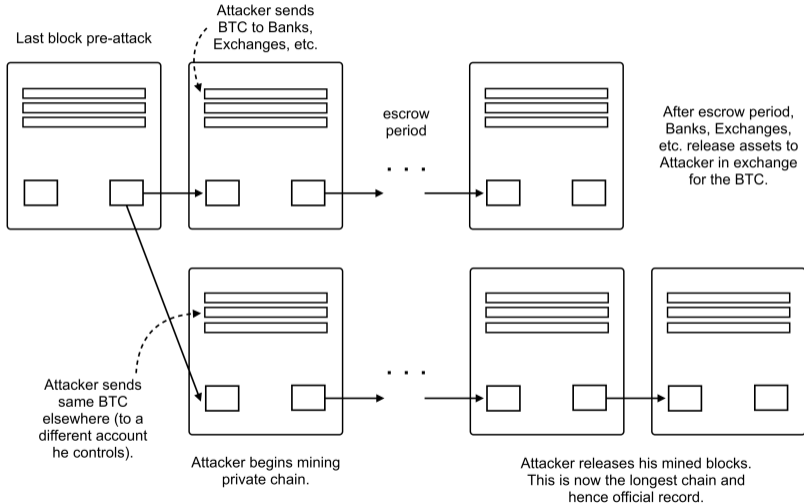


Illustration of Double Spending



Double Spending: Analysis Framework

- ▶ Equation (3) tells us that the possibility of a double-spending attack places an economic limit on Nakamoto trust:

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

- ▶ 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 Nakamoto blockchain (potentially, many such transactions using many addresses)
 - ▶ Interpretation: V_{attack} represents the maximum amount of transaction volume that *honest users* of Bitcoin can conduct (“max economic throughput”)
 - ▶ I consider a range from \$1000 (pizza) to \$100bn (global finance)
- ▶ Duration of attack: $A^* \cdot t(A^*)$
 - ▶ Can compute explicitly. Then will consider a range informed by the computations.
- ▶ Then ask: how big need p_{block} be for a given desired amount to secure, V_{attack}

Double Spending: Attack Duration in Closed Form

- ▶ Let $t(A, e)$ denote the expected time it takes an A attacker to over-take honest miners if there is an e escrow period
- ▶ Proposition. Closed form expression:

$$t(A, e) = (1 + e) + \left[\sum_{i=0}^{1+e} \left(\frac{i+1}{A-1} \right) \cdot \frac{(1+2e-i)!}{(1+e-i)!e!} \left(\frac{A}{1+A} \right)^{1+e-i} \left(\frac{1}{1+A} \right)^{1+e} \right].$$

- ▶ Intuition for the expression
 - ▶ The attacker must wait for the honest chain to reach $1 + e$ blocks due to the escrow condition no matter what — even if attacker's chain is much longer by then.
 - ▶ What if the attacker's chain is *shorter* than the honest chain at time $1 + e$? Call this difference in attacker and honest chain length the 'attacker deficit', i
 - ▶ The sum considers, for each possible attacker deficit at the end of the escrow period,
 - ▶ The expected time to overcome the attack deficit i : $\left(\frac{i+1}{A-1} \right)$
 - ▶ The probability of facing attack deficit i : $\frac{(1+2e-i)!}{(1+e-i)!e!} \left(\frac{A}{1+A} \right)^{1+e-i} \left(\frac{1}{1+A} \right)^{1+e}$

Double Spending Attack: Simulation Details I

Table 1, Panel A. Expected Duration of Attack (t)

	$e = 0$	$e = 1$	$e = 6$	$e = 10$	$e = 100$	$e = 1000$
$A = 1.05$	25.51	29.77	45.06	54.44	181.32	1,067.82
$A = 1.1$	13.02	15.42	24.48	30.35	125.81	1,004.04
$A = 1.2$	6.79	8.28	14.37	18.65	105.13	1,001.0
$A = 1.25$	5.54	6.86	12.41	16.44	102.79	1,001.0
$A = 1.33$	4.34	5.49	10.57	14.40	101.47	1,001.0
$A = 1.5$	3.08	4.07	8.77	12.49	101.03	1,001.0
$A = 2$	1.89	2.78	7.39	11.23	101.0	1,001.0
$A = 5$	1.12	2.06	7.00	11.00	101.0	1,001.0

Double Spending Attack: Simulation Details I

Table 1, Panel A. Expected Duration of Attack (t)

	$e = 0$	$e = 1$	$e = 6$	$e = 10$	$e = 100$	$e = 1000$
$A = 1.05$	25.51	29.77	45.06	54.44	181.32	1,067.82
$A = 1.1$	13.02	15.42	24.48	30.35	125.81	1,004.04
$A = 1.2$	6.79	8.28	14.37	18.65	105.13	1,001.0
$A = 1.25$	5.54	6.86	12.41	16.44	102.79	1,001.0
$A = 1.33$	4.34	5.49	10.57	14.40	101.47	1,001.0
$A = 1.5$	3.08	4.07	8.77	12.49	101.03	1,001.0
$A = 2$	1.89	2.78	7.39	11.23	101.0	1,001.0
$A = 5$	1.12	2.06	7.00	11.00	101.0	1,001.0

Double Spending Attack: Simulation Details II

Table 1, Panel B. Gross Cost of Attack (At)

	$e = 0$	$e = 1$	$e = 6$	$e = 10$	$e = 100$	$e = 1000$
$A = 1.05$	26.78	31.26	47.31	57.17	190.38	1,121.22
$A = 1.1$	14.32	16.96	26.92	33.39	138.39	1,104.35
$A = 1.2$	8.14	9.93	17.24	22.38	126.15	1,201.20
$A = 1.25$	6.93	8.57	15.51	20.55	128.49	1,251.25
$A = 1.33$	5.78	7.31	14.06	19.15	134.96	1,331.33
$A = 1.5$	4.62	6.11	13.15	18.73	151.54	1,501.5
$A = 2$	3.78	5.56	14.78	22.45	202.0	2,002.0
$A = 5$	5.59	10.29	35.01	55.00	505.0	5,005.0

Double Spending Attack: Simulation Details II

Table 1, Panel B. Gross Cost of Attack (A_t)

	$e = 0$	$e = 1$	$e = 6$	$e = 10$	$e = 100$	$e = 1000$
$A = 1.05$	26.78	31.26	47.31	57.17	190.38	1,121.22
$A = 1.1$	14.32	16.96	26.92	33.39	138.39	1,104.35
$A = 1.2$	8.14	9.93	17.24	22.38	126.15	1,201.20
$A = 1.25$	6.93	8.57	15.51	20.55	128.49	1,251.25
$A = 1.33$	5.78	7.31	14.06	19.15	134.96	1,331.33
$A = 1.5$	4.62	6.11	13.15	18.73	151.54	1,501.5
$A = 2$	3.78	5.56	14.78	22.45	202.0	2,002.0
$A = 5$	5.59	10.29	35.01	55.00	505.0	5,005.0

Double Spending Attack: Simulation Details II

Table 1, Panel B. Gross Cost of Attack (A_t)

	$e = 0$	$e = 1$	$e = 6$	$e = 10$	$e = 100$	$e = 1000$
$A = 1.05$	26.78	31.26	47.31	57.17	190.38	1,121.22
$A = 1.1$	14.32	16.96	26.92	33.39	138.39	1,104.35
$A = 1.2$	8.14	9.93	17.24	22.38	126.15	1,201.20
$A = 1.25$	6.93	8.57	15.51	20.55	128.49	1,251.25
$A = 1.33$	5.78	7.31	14.06	19.15	134.96	1,331.33
$A = 1.5$	4.62	6.11	13.15	18.73	151.54	1,501.5
$A = 2$	3.78	5.56	14.78	22.45	202.0	2,002.0
$A = 5$	5.59	10.29	35.01	55.00	505.0	5,005.0

Note: circles indicate approximate cost-minimizing choice of A . For exact formula see the appendix.

Securing Against an 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	7.61%	1,096%	400,129%	0.004%
To Secure:				
\$1 thousand	\$76.1 dollars	\$11.0 thousand	\$4.0 million	3.8 cents
\$1 million	\$76.1 thousand	\$11.0 million	\$4.0 billion	\$38.1 dollars
\$1 billion	\$76.1 million	\$11.0 billion	\$4.0 trillion	\$38.1 thousand
\$100 billion	\$7.6 billion	\$1.1 trillion	\$400.1 trillion	\$3.8 million

Securing Against an 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	7.61%	1,096%	400,129%	0.004%
To Secure:				
\$1 thousand	\$76.1 dollars	\$11.0 thousand	\$4.0 million	3.8 cents
\$1 million	\$76.1 thousand	\$11.0 million	\$4.0 billion	\$38.1 dollars
\$1 billion	\$76.1 million	\$11.0 billion	\$4.0 trillion	\$38.1 thousand
\$100 billion	\$7.6 billion	\$1.1 trillion	\$400.1 trillion	\$3.8 million

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

Securing Against an 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	7.61%	1,096%	400,129%	0.004%
To Secure:				
\$1 thousand	\$76.1 dollars	\$11.0 thousand	\$4.0 million	3.8 cents
\$1 million	\$76.1 thousand	\$11.0 million	\$4.0 billion	\$38.1 dollars
\$1 billion	\$76.1 million	\$11.0 billion	\$4.0 trillion	\$38.1 thousand
\$100 billion	\$7.6 billion	\$1.1 trillion	\$400.1 trillion	\$3.8 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. \$100bn attack requires 4 times global GDP annually

Securing Against an 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	7.61%	1,096%	400,129%	0.004%
To Secure:				
\$1 thousand	\$76.1 dollars	\$11.0 thousand	\$4.0 million	3.8 cents
\$1 million	\$76.1 thousand	\$11.0 million	\$4.0 billion	\$38.1 dollars
\$1 billion	\$76.1 million	\$11.0 billion	\$4.0 trillion	\$38.1 thousand
\$100 billion	\$7.6 billion	\$1.1 trillion	\$400.1 trillion	\$3.8 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. \$100bn attack requires 4 times global GDP annually

Securing Against an 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	7.61%	1,096%	400,129%	0.004%
To Secure:				
\$1 thousand	\$76.1 dollars	\$11.0 thousand	\$4.0 million	3.8 cents
\$1 million	\$76.1 thousand	\$11.0 million	\$4.0 billion	\$38.1 dollars
\$1 billion	\$76.1 million	\$11.0 billion	\$4.0 trillion	\$38.1 thousand
\$100 billion	\$7.6 billion	\$1.1 trillion	\$400.1 trillion	\$3.8 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. \$100bn attack requires 4 times global GDP annually
- ▶ % tax looks more reasonable per transaction, but even tiny tx's have to pay security costs dictated by large attacks

Securing Against an Attack: Sensitivity Analysis

Table 3, Panel A. Securing Against an Attack: Sensitivity Analysis

Attack Scenarios	Per-Block	Per-Day	Per-Year	Per-Transaction
Base Case	7.61 %	1,096 %	400,129 %	0.004 %
Expensive	0.57 %	82.0 %	29,939 %	0.0003 %
Very Expensive	0.09 %	13.1 %	4,777.9 %	0.00005 %

Securing Against an Attack: Sensitivity Analysis

Table 3, Panel A. Securing Against an Attack: Sensitivity Analysis

Attack Scenarios	Per-Block	Per-Day	Per-Year	Per-Transaction
Base Case	7.61 %	1,096 %	400,129 %	0.004 %
Expensive	0.57 %	82.0 %	29,939 %	0.0003 %
Very Expensive	0.09 %	13.1 %	4,777.9 %	0.00005 %

- ▶ Expensive and very expensive cases improve the picture by 1-2 orders of magnitude, but costs still very high

Securing Against an Attack: Sensitivity Analysis

Table 3, Panel A. Securing Against an Attack: Sensitivity Analysis

Attack Scenarios	Per-Block	Per-Day	Per-Year	Per-Transaction
Base Case	7.61 %	1,096 %	400,129 %	0.004 %
Expensive	0.57 %	82.0 %	29,939 %	0.0003 %
Very Expensive	0.09 %	13.1 %	4,777.9 %	0.00005 %

- ▶ Expensive and very expensive cases improve the picture by 1-2 orders of magnitude, but costs still very high
- ▶ Even at a 1-week escrow period (very expensive), require an annual expense of \$48bn, per-transaction cost of \$450, to keep Bitcoin secure up to \$1bn attack.
 - ▶ 5% of Global GDP, \$45k per tx, to secure against \$100bn attack.

Double Spending Attack: Takeaways

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

- ▶ Consistent with modest early use cases of Bitcoin (computer parts, silk road, online gambling)—if double-spending worth \$1k, then cost per tx just \$0.04
- ▶ Consistent with larger-scale black-market uses of Bitcoin—users willing to pay high tx costs (Ex: \$100 per tx secures up to \$3M base case, \$35M exp. 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 % tax).

Overview of the Talk

- ▶ Overview of the Nakamoto Blockchain
- ▶ Nakamoto Blockchain: A Critique in 3 Equations
- ▶ Analysis of Double Spending Attacks
- ▶ **Analysis of Sabotage Attacks**
- ▶ Collapse Scenarios
- ▶ Comparison of Nakamoto Trust and Traditional Trust
- ▶ Conclusion

Attack II: Sabotage

- ▶ Obvious response: double spending attack would be “noticed”
- ▶ Cause decline in value of Bitcoin, which attacker will be left with after a double spend (V_{attack} worth)
- ▶ Bitcoin Wiki classifies majority attack “Probably Not a Problem” for this reason
- ▶ As above, suppose attack causes Bitcoin value to decline by proportion Δ_{attack} . Attacker cost frictions κ . Equation (3) becomes:

$$p_{block} > \frac{(1 - \Delta_{attack})}{At(\kappa + \Delta_{attack})} V_{attack}$$

- ▶ Proposition. For any potential value of a double-spending attack V_{attack} , and any level of block reward p_{block} , the Bitcoin blockchain is secure against the double-spending attack if Δ_{attack} is sufficiently large.
- ▶ This may sound reassuring about security ...
 - ▶ But the argument concedes that an attack would cause collapse of the trust
 - ▶ Raises worry about attacker motivated by collapse per se (“sabotage”)
 - ▶ **Pick your poison: high implicit tax rates or risk of collapse**

Attack II: Sabotage

- ▶ How big is V_{attack} from a sabotage?
- ▶ Hard to say, but seems likely to already be large relative to the Base, Expensive, and maybe even Very Expensive gross costs of attack (\$4M - \$250M at recent values)
- ▶ Would be larger still if Bitcoin / Nakamoto trust becomes more integrated into global financial system
- ▶ Futures markets
 - ▶ CME: \$2bn of open interest
 - ▶ Crypto Exchanges: \$20bn of open interest
- ▶ Bitcoin market capitalization: as high as \$1 trillion (Peter Thiel: \$100 trillion)
- ▶ Vitalik Buterin: “if blockchains do become successful enough, and they survive long enough, they have a good enough track record of actually being the base layer for many kinds of interactions, and we fast-forward a couple of decades into a future where it’s **just considered normal for there to be trillion dollar assets that are managed on Ethereum ...**” (Ezra Klein podcast, Sept 30, 2022)

Sabotage and Blockchain-Specific Capital

- ▶ Why would a sabotage attack cost a stock, not a flow?
- ▶ 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
- ▶ If capital is specialized, and attack causes collapse, 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: $O(N^*C)$

Antminer



- ▶ Cost per machine
 - ▶ S19 Pro: \$3769 (March 2021)
 - ▶ S19 Pro: \$7700 (May 2022)
- ▶ Mining power: 104-110 TH/s
- ▶ Cost to match the Bitcoin hash rate:
 - ▶ Mar 2021: \$5bn
 - ▶ May 2022: \$15bn

Note: The numbers are based on data from March 2021 and May 2022. Data from shop.bitmain.com.

Amazon Web Services



- ▶ AWS Total computation 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 will get about .05% of total network hash rate**

Note: The numbers are based on data from early 2022. Data of Amazon AWS total PP&E and potential equipment lease are obtained from Amazon 10-K. The cost/efficiency ratio is a conservative estimate based on the data of the hash rate of non-specific mining hardware obtained from Bitcoin Wiki.

Cost to Secure Against Sabotage, Derivation

- ▶ Write per-unit-time compute cost as $c = rC + \eta$. Honest mining equilibrium (1) can be written as:

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

- ▶ Outside attacker needs N^*C of capital. Assume attack causes total collapse of the trust. IC constraint to secure against outsider sabotage 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:

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

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

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

Cost to Secure Against Sabotage, Derivation

- ▶ MUCH more secure than before, because of r (interest rate per block!). So relative to original, improve security by several orders of magnitude.
- ▶ Sense of magnitudes
 - ▶ The change in the IC constraint is a factor of $At \frac{r}{\mu}$
 - ▶ If we use base case of $At = 13.14$, use $r = 50\%$ annually which is $\sim 0.001\%$ per block, and $\mu = 0.4$, we have $At \frac{r}{\mu} = 0.0004$. A 2500x reduction in the rewards necessary for security.
 - ▶ (N.B. these values of r and μ , with 2022 avg. values of p_{block} , imply $N^*C = \$10B$ which roughly matches observed prices.)
- ▶ Current capital stock and miner payments suggests Bitcoin is secure up to sabotages worth roughly \$10bn for an outsider, \$5bn for an insider

Overview of the Talk

- ▶ Overview of the Nakamoto Blockchain
- ▶ Nakamoto Blockchain: A Critique in 3 Equations
- ▶ Analysis of Double Spending Attacks
- ▶ Analysis of Sabotage Attacks
- ▶ **Collapse Scenarios**
- ▶ Comparison of Nakamoto Trust and Traditional Trust
- ▶ Conclusion

Collapse Scenarios

- ▶ So we have a candidate answer to the Chicago Lunch Table question: Bitcoin hasn't been attacked yet because of (i) specialized equipment, and (ii) attackers would lose the stock value of their specialized equipment in an attack, because an attack will cause the system to collapse. And this stock cost of attack is larger than the current attack possibilities.
- ▶ Suppose this is right. That is:
 - ▶ Bitcoin blockchain *does not* satisfy (2): $A^* N^* c \cdot t(A^*) > V_{attack}$
 - ▶ Bitcoin blockchain *does* satisfy (2'): $N^* C > V_{attack}$
 - ▶ Attack would cause collapse, hence (2') not (2) is operative
- ▶ Question: what changes to the economic environment could cause the binding constraint to change from (2') to (2)? Or cause (2') no longer to hold?

Attack Scenario 1. Cheap-enough Specialized Chips

- ▶ Suppose there are previous-generation ASIC chips that are not economically efficient for mining, but are powerful enough for the purpose of attack and exist in large quantity
 - ▶ Formally, suppose per-unit-compute electricity cost is $\eta' > c$. So in honest mining equilibrium, old chips are not economical to use even if the chips themselves are free.
- ▶ Observation: If there are $\geq N^*$ compute units of old chips, and these chips are approximately free, then attacker can attack at flow cost of $N^*\eta'$.
- ▶ Currently no reason to think $\geq N^*$ compute units of old chips exist
 - ▶ Both quantity and quality have been growing dramatically
- ▶ But ASIC market continues to mature, so this could change.
- ▶ More generally, if security depends on specialized chips, then Bitcoin is vulnerable to changes in the chip market.

Attack Scenario 2. Sufficient Fall in Mining Rewards

- ▶ Recall $N^*(rC + \eta) = p_{block}$ and $\mu :=$ the capital share of mining cost.
- ▶ If p_{block} falls to $\alpha \cdot p_{block}$, with $\alpha < (1 - \mu)$, then $N^*\eta > \alpha \cdot p_{block}$ and some capital will be “mothballed”. Not worth the variable costs even if treat capital as free.
- ▶ If enough capital is mothballed for a sufficiently long period of time, this would seem to raise the vulnerability to attack
- ▶ Additionally, Bitcoin halvings will decrease p_{block} over time.
 - ▶ By 2032, reward is <1 Bitcoin
 - ▶ By 2044, reward is <0.1 Bitcoin
 - ▶ (This is the reason the total supply of Bitcoins that will ever be mined is finite. 21 million total, the last epsilon mined in about 2140.)
- ▶ Hence: either Bitcoin value must grow significantly, transaction costs must grow significantly, or there will be significant mothballed capital

Attack Scenario 3. Bitcoin Grows in Economic Importance (Relative to Cost)

- ▶ Previous two scenarios identify conditions under which the cost of attack changes from a stock cost to a flow cost
- ▶ The other logical possibility: Bitcoin grows in economic importance enough to tempt a saboteur despite the cost
 - ▶ That is, (2') fails to hold: $V_{attack} > N * C$.
- ▶ Speculatively, this seems most likely to occur if Bitcoin becomes more fully integrated into the global financial system.
 - ▶ \$10bn is small in the scheme of global finance

Examples of 51% Attacks

Name	Date of First Attack	Amount Stolen	Length of Largest Reorganization
Bitcoin SV	8/3/2021	Unknown	14 Blocks
	6/24/2021	Unknown	Unknown
Verge	2/15/2021	Unknown	560,000 Blocks
	5/22/2018	\$1.8 million	NA
	4/4/2018	\$1 million	NA
Æternity	12/3/2020	\$2.9 million	Unknown
Grin	11/8/2020	Unknown	Unknown
Ethereum Classic	8/29/2020	Unknown	7,000 Blocks
	8/6/2020	\$1.7 million	4,200 Blocks
	7/29/2020	\$5.6 million	3,700 Blocks
	1/5/2019	\$1.1 million	Unknown
Bitcoin Gold	1/23/2020	\$100 thousand	29 Blocks
	5/16/2018	\$18 million	22 Blocks
Firo	1/18/2019	\$5 million	300 Blocks
Vertcoin	12/2/2018	\$100 thousand	307 Blocks
Zencash	6/2/2018	\$700 thousand	38 Blocks
Litecoin Cash	5/30/2018	Unknown	Unknown
Monacoin	5/13/2018	\$90 thousand	Unknown

Sources: Bloomberg, Coindesk, Bitcoinist, CCN, Cointelegraph, bitquery, GitHub Gist and Medium. Often there is an ambiguity of whether several block reorganizations should be considered as 1 attack or several attacks. Because of this, only the date of the first attack/reorganization is mentioned.

Examples of 51% Attacks

Name	Date of First Attack	Amount Stolen	Length of Largest Reorganization
Bitcoin SV	8/3/2021	Unknown	14 Blocks
	6/24/2021	Unknown	Unknown
Verge	2/15/2021	Unknown	560,000 Blocks
	5/22/2018	\$1.8 million	NA
	4/4/2018	\$1 million	NA
Æternity	12/3/2020	\$2.9 million	Unknown
Grin	11/8/2020	Unknown	Unknown
Ethereum Classic	8/29/2020	Unknown	7,000 Blocks
	8/6/2020	\$1.7 million	4,200 Blocks
	7/29/2020	\$5.6 million	3,700 Blocks
	1/5/2019	\$1.1 million	Unknown
Bitcoin Gold	1/23/2020	\$100 thousand	29 Blocks
	5/16/2018	\$18 million	22 Blocks
Firo	1/18/2019	\$5 million	300 Blocks
Vertcoin	12/2/2018	\$100 thousand	307 Blocks
Zencash	6/2/2018	\$700 thousand	38 Blocks
Litecoin Cash	5/30/2018	Unknown	Unknown
Monacoin	5/13/2018	\$90 thousand	Unknown

Sources: Bloomberg, Coindesk, Bitcoinist, CCN, Cointelegraph, bitquery, GitHub Gist and Medium. Often there is an ambiguity of whether several block reorganizations should be considered as 1 attack or several attacks. Because of this, only the date of the first attack/reorganization is mentioned.

Attacks of Crypto Financial Entities

Name	Type of Business	Date of Attack	Amount Stolen	Attack Vector
Euler Finance	Decentralized Lending Firm	January 2023	\$197	Flashloan Attack + Flawed Code
Mango Market	Decentralized Exchange	October 2022	\$100 million	Price Manipulation
BNB Chain	DeFi Bridge	October 2022	\$568 million	Flawed Code
Wintermute	DeFi Market Maker	September 2022	\$160 million	Compromised Wallet Generator
Nomad	DeFi Bridge	August 2022	\$200 million	Flawed Code
Horizon Bridge	DeFi Bridge	July 2022	\$100	Compromised Private Keys + Governance Control
Beanstalk Farms	DeFi Stablecoin	April 2022	\$182 million	Flashloan 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	Lending Firm	January 2022	\$80	Flawed Code
BitMart	Centralized Exchange	December 2021	\$150 million	Compromised Private Keys
C.r.e.a.m. Finance	DeFi Lending Protocol	October 2021	\$130 million	Flashloan 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	February 2014	\$480 million	Compromised Private Keys

Sources: Bloomberg, WSJ, Elliptic Inc. Amounts calculated based on fund values at the time of theft.

Attacks of Crypto Financial Entities

Name	Type of Business	Date of Attack	Amount Stolen	Attack Vector
Euler Finance	Decentralized Lending Firm	January 2023	\$197	Flashloan Attack + Flawed Code
Mango Market	Decentralized Exchange	October 2022	\$100 million	Price Manipulation
BNB Chain	DeFi Bridge	October 2022	\$568 million	Flawed Code
Wintermute	DeFi Market Maker	September 2022	\$160 million	Compromised Wallet Generator
Nomad	DeFi Bridge	August 2022	\$200 million	Flawed Code
Horizon Bridge	DeFi Bridge	July 2022	\$100	Compromised Private Keys + Governance Control
Beanstalk Farms	DeFi Stablecoin	April 2022	\$182 million	Flashloan 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	Lending Firm	January 2022	\$80	Flawed Code
BitMart	Centralized Exchange	December 2021	\$150 million	Compromised Private Keys
C.r.e.a.m. Finance	DeFi Lending Protocol	October 2021	\$130 million	Flashloan 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	Juny 2016	\$55 million	Flawed Code
Mt. Gox	Centralized Exchange	February 2014	\$480 million	Compromised Private Keys

Sources: Bloomberg, WSJ, Elliptic Inc. Amounts calculated based on fund values at the time of theft.

Collapses of Crypto Financial Entities

Name	Type of Business	Date of Collapse	Entity Size (or Loss Amt)
Genesis	Lending Firm	January 2023	\$1 billion - \$10 billion
BlockFi	Lending Firm	November 2022	\$1 billion - \$10 billion
FTX	Centralized Exchange	November 2022	\$32 billion
Three Arrows Capital	Hedge Fund	July 2022	\$3 billion
Voyager	Lending Firm	July 2022	\$1 billion - \$10 billion
Celsius	Lending Firm	July 2022	\$4 billion - \$19 billion
Terra + Luna	Blockchain + Stablecoin	March 2022	\$40 billion
Coincheck	Centralized Exchange	January 2018	\$530 million (loss amt)
Mt. Gox	Centralized Exchange	February 2014	\$480 million (loss amt)

Sources: Bloomberg, WSJ, Coinmarketcap.

Collapses of Crypto Financial Entities

Name	Type of Business	Date of Collapse	Entity Size (or Loss Amt)
Genesis	Lending Firm	January 2023	\$1 billion - \$10 billion
BlockFi	Lending Firm	November 2022	\$1 billion - \$10 billion
FTX	Centralized Exchange	November 2022	\$32 billion
Three Arrows Capital	Hedge Fund	July 2022	\$3 billion
Voyager	Lending Firm	July 2022	\$1 billion - \$10 billion
Celsius	Lending Firm	July 2022	\$4 billion - \$19 billion
Terra + Luna	Blockchain + Stablecoin	March 2022	\$40 billion
Coincheck	Centralized Exchange	January 2018	\$530 million (loss amt)
Mt. Gox	Centralized Exchange	February 2014	\$480 million (loss amt)

Sources: Bloomberg, WSJ, Coinmarketcap.

Overview of the Talk

- ▶ Overview of the Nakamoto Blockchain
- ▶ Nakamoto Blockchain: A Critique in 3 Equations
- ▶ Analysis of Double Spending Attacks
- ▶ Analysis of Sabotage Attacks
- ▶ Collapse Scenarios
- ▶ **Comparison of Nakamoto Trust and Traditional Trust**
- ▶ 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 $\{Honest, Cheat\}$
 - ▶ If Party 1 plays *Engage* and Party 2 plays *Honest*, both parties get a payoff of $b > 0$
 - ▶ If Party 1 plays *Engage* and Party 2 plays *Cheat*, Party 2 gets $+V$ and Party 1 gets $-V$
 - ▶ If Party 1 plays *Don't Engage*, both parties get 0.
- ▶ One-shot game, as described: clearly only equilibrium is *Don't Engage*.
- ▶ 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 $f > 0$
 - ▶ In this scenario, Party 1's payoff is $-c_l$ and Party 2's payoff is $-f$.
- ▶ 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

- ▶ 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.*
- ▶ 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)
- ▶ Collateral an 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

Beckerian Deterrence as an Economy of Scale

- ▶ Simple mathematical comparison
 - ▶ Consider the stripped-down one-shot game model from earlier
 - ▶ Let V_{honest} represent average volume per period by honest users of the system if trust is secured
 - ▶ Model Nakamoto trust as earlier
 - ▶ Model traditional trust as costing a fixed cost F plus a variable cost per unit transacted of c
- ▶ The two trust models' costs per unit volume are thus:

$$\textit{Traditional Trust} : \frac{F}{V_{honest}} + c$$

$$\textit{Nakamoto Trust} : \frac{V_{attack}}{V_{honest}}$$

Beckerian Deterrence as an Economy of Scale

- ▶ Sense of magnitudes
 - ▶ 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 exceeds \$1 quadrillion per year
- ▶ So we can conservatively upper bound $\frac{F}{V_{honest}} + c$ for the financial sector by 0.1% (clearly very rough)
- ▶ Many fees in traditional finance, especially for large transactions, are 0.01% less of transaction volume.
- ▶ Bitcoin Gold attack: $\frac{V_{attack}}{V_{honest}}$ of about 1800%. (Attacker engages in transactions as large as possible given the typical level of transaction volume).
- ▶ Not meant to be an apology for traditional finance (see Greenwood and Scharfstein, 2013; Philippon, 2015; Zingales, 2015). But comparison with Nakamoto trust is night-and-day.

Overview of the Talk

- ▶ Overview of the Nakamoto Blockchain
- ▶ Nakamoto Blockchain: A Critique in 3 Equations
- ▶ Analysis of Double Spending Attacks
- ▶ Analysis of Sabotage Attacks
- ▶ Collapse Scenarios
- ▶ Comparison of Nakamoto Trust and Traditional Trust
- ▶ **Conclusion**

Conclusion: Summary

- ▶ Anonymous, decentralized trust enabled by Nakamoto (2008) blockchain: *ingenious but expensive*
- ▶ Eq. (3): for trust to be meaningful, flow cost of running the blockchain $>$ one-shot value of attacking it
 - ▶ To prevent double spending: payments to miners must be large relative to the max economic throughput of Bitcoin
 - ▶ Like a large implicit tax: from \$450 to \$76k per tx to secure against \$1bn attack
 - ▶ All grows linearly: if attack can be \$100bn, annual cost is 4x global GDP
- ▶ Argument that attack costs more than this flow cost requires one to concede both
 1. Security relies on use of scarce, specialized chips (contra Nakamoto ideal)
 2. Vulnerable to sabotage, collapse (“pick your poison”)
- ▶ The analysis then points to specific collapse scenarios
- ▶ Overall message: there are intrinsic economic limits to how economically important crypto and blockchains can become.

Conclusion: Summary

- ▶ Emphasize: model consistent with earliest uses of Bitcoin and blockchain: hobbyists and black market
 - ▶ 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 ("permissioned blockchain" or "distributed ledger technology")
 - ▶ 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 emerges from proof-of-work* — that also may make it so economically limited

Directions for Future Research

- ▶ Direction 1: Is there a “solution” to this paper’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 decentralized aspects of Nakamoto while being significantly less economically constrained by the arguments in this paper
- ▶ Formally: Lewis-Pye, Roughgarden and Budish (2023) define “economically secure permissionless consensus” as a permissionless consensus protocol that makes it expensive to attack in the sense of costing a stock not a flow, without honest participants suffering impairment of their capital (i.e., without collapse)
- ▶ Many responses to the paper are described in Appendix A.
- ▶ The most promising responses combine blockchain-based trust with some external source of trust support (including Jacob Leshno’s paper, up next!)
- ▶ This in turn begs the next question

Directions for Future Research

- ▶ Direction 2: How should we model trust that comes from a combination of technology and rule of law?
- ▶ And more generally, how should we understand trust when it comes from multiple sources in the same transaction that work in complement with each other?
- ▶ 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 (Budish and Sunderam, 2023)
- ▶ Consider the completely ordinary transaction of buying a cup of coffee at the local coffee shop ...
- ▶ As one appreciates how many sources of trust work together in even the most ordinary of economic transactions, it is hard not to regard the traditional market system with a sense of wonder

The Friendly Colleague



Alex Imas
@alexoimas

...

IMHO, this is only paper on cryptocurrency that you need to read (by colleague Eric Budish)

Saw it presented in 2017 and didn't take crypto seriously again.

faculty.chicagobooth.edu/eric.budish/re..

TL'DR mathematically shows why it cannot become economically important as store of value 1/3

The Economic Limits of Bitcoin and the Blockchain*†

Eric Budish†

June 5, 2018

Abstract

The amount of computational power devoted to anonymous, decentralized blockchains such as Bitcoin's must simultaneously satisfy two conditions in equilibrium: (1) a zero-profit condition among miners, who engage in a rent-seeking competition for the prize associated with adding the next block to the chain; and (2) an incentive compatibility condition on the system's vulnerability to a "majority attack", namely that the computational costs of such an attack must exceed the benefits. Together, these two equations imply that (3) the recurring, "flow", payments to miners for running the blockchain must be large relative to the one-off, "stock", benefits of attacking it. This is very expensive! The constraint is softer (i.e., stock versus stock) if both (i) the mining technology used to run the blockchain is both scarce and non-repurposable, and (ii) any majority attack is a "sabotage" in that it causes a collapse in the economic value of the blockchain; however, reliance on non-repurposable technology for security and vulnerability to sabotage each raise their own concerns, and point to specific collapse scenarios. In particular, the model suggests that Bitcoin would be majority attacked if it became sufficiently economically important — e.g., if it became a "store of value" akin to gold — which suggests that there are intrinsic economic limits to how economically important it can become in the first place.

10:58 AM · May 14, 2022

696 Retweets 90 Quotes 3,798 Likes 2,320 Bookmarks

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 Disrespecter
@ToxicBitcoiner


Replying to @alexoimas
Fucking morons

The Economics Professoooooo

"It's going to ZEROOO"

> Only tweets after Bitcoin is down 2%
"What are the fundamentals?!"

> Calls Bitcoin a scam while teaching at a university that charges \$65,000 a year in tuition



"AHHHH I'm educatingggg!"

> Protecting students from 100x gainers since 2012

"It's NOT a currency, only speculative!"

> Hasn't had a real job since the Clinton administration

8:51 PM · May 14, 2022



Peter McCormack
@PeterMcCormack

Replying to @alexoimas

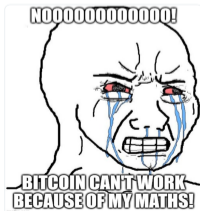


7:40 PM · May 14, 2022



J. Gett, BTC Psychopath
@gettj

Replying to @alexoimas



10% Monetary Mulligan
@MichaelPonore

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

The Wise Son

- ▶ U.S. Treasury Secretary, Janet Yellen, in Feb. 2021:

"I don't think that bitcoin ... is widely used as a transaction mechanism ... To the extent it is used I fear it's often for illicit finance. ... It is a highly speculative asset."

- ▶ U.S. SEC Chair, Gary Gensler, in Aug. 2021:

"Primarily, crypto assets provide digital, scarce vehicles for speculative investment. ... These assets haven't been used much as a unit of account. We also haven't seen crypto used much as a medium of exchange. To the extent that it is used as such, it's often to skirt our laws ..."

- ▶ Nathan Budish, June 2022:

"So daddy, is crypto using fake money to take your real money?"