The Economics of Cryptocurrencies

Eric Budish
University of Chicago, Booth School of Business

November 9th, 2022
Harvard University Harris Lecture

Nakamoto's Invention

- Satoshi Nakamoto invented a new kind of trust
- Completely anonymous and decentralized
- Without support from traditional sources: rule of law, reputations, relationships, collateral, trusted intermediaries

Nakamoto's Invention

- Satoshi Nakamoto invented a new kind of trust
- Completely anonymous and decentralized
- Without support from traditional sources: rule of law, reputations, relationships, collateral, trusted intermediaries

- At a high level: Nakamoto invented an elaborate scheme, combining ideas from CS+Econ, to incentivize a large, anonymous, freely-entering and -exiting mass of computing power around the world to pay attention to and collectively maintain a common data set
- Enabling trust in this data set
  - (CS terminology for the invention: "permissionless consensus")

Nakamoto's Invention

- Satoshi Nakamoto invented a new kind of trust
- Completely anonymous and decentralized
- Without support from traditional sources: rule of law, reputations, relationships, collateral, trusted intermediaries

- At a high level: Nakamoto invented an elaborate scheme, combining ideas from CS+Econ, to incentivize a large, anonymous, freely-entering and -exiting mass of computing power around the world to pay attention to and collectively maintain a common data set
- Enabling trust in this data set
  - (CS terminology for the invention: "permissionless consensus")

- This invention enabled cryptocurrencies — including Nakamoto's 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

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)
  - Ironically, most of the speculative volume is through cryptocurrency exchanges — which are trusted financial intermediaries

- 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 ..."

The Economic Limits of Bitcoin and Anonymous, Decentralized Trust on the Blockchain

Eric Budish, June 2022

The Paper's Argument

- The paper argues that Bitcoin and Nakamoto's novel form of trust — while undeniably ingenious — have serious economic limitations

The Paper's Argument

- The paper argues that Bitcoin and Nakamoto's novel form of trust — while undeniably ingenious — have serious economic limitations
- Analysis ultimately suggests skepticism that Bitcoin and the Nakamoto blockchain will play a major role in the global economy and financial system

The Paper's Argument

- Core of the argument is just 3 equations.

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 the trust reflects the compensation paid to this computing power (called "miners").

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 the 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.

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 the 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).

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 the 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!

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 the 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.

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 the 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"

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 the 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"
- 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)

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

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.

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"

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.

Overview of the Talk

A General Introduction:

- What is Nakamoto Blockchain?

The Economic Limits of Bitcoin and Anonymous, Decentralized Trust:

- Nakamoto Blockchain: A Critique in 3 Equations
  - Flow vs. Stock Problem
  - Zero Net Attack Cost Theorem
- Analysis of Double Spending Attacks
- A Way Out: Specialized Capital + Risk of Collapse
  - A Softer Constraint: Stock vs. Stock. Collapse Scenarios.

Open Questions for Future Research:

- Q1: Permissionless trust beyond Nakamoto
- Q2: Economics of permissioned blockchains
- Many other open q's related to theory, finance, policy

Overview of the Talk

A General Introduction:

- **What is Nakamoto Blockchain?**

The Economic Limits of Bitcoin and Anonymous, Decentralized Trust:

- Nakamoto Blockchain: A Critique in 3 Equations
  - Flow vs. Stock Problem
  - Zero Net Attack Cost Theorem
- Analysis of Double Spending Attacks
- A Way Out: Specialized Capital + Risk of Collapse
  - A Softer Constraint: Stock vs. Stock. Collapse Scenarios.

Open Questions for Future Research:

- Q1: Permissionless trust beyond Nakamoto
- Q2: Economics of permissioned blockchains
- Many other open q's related to theory, finance, policy

What is Nakamoto Blockchain (1/4)

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

Sender	Receiver	Amount	Signature
Alice	Bob	$10	*Alice*

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

What is Nakamoto Blockchain (1/4)

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

Sender	Receiver	Amount	Signature
Alice	Bob	$10	*Alice*

- **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."

What is Nakamoto Blockchain (1/4)

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

Sender	Receiver	Amount	Signature
Alice	Bob	$10	*Alice*

- **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

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

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)

What is Nakamoto Blockchain (2/4)

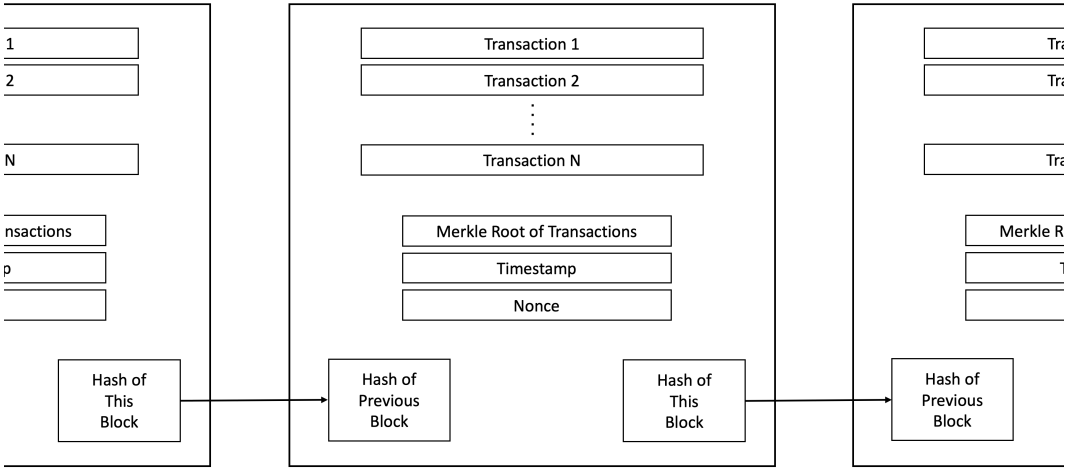
Nakamoto (2008) Blockchain Innovation

- **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)

What is Nakamoto Blockchain (2/4)

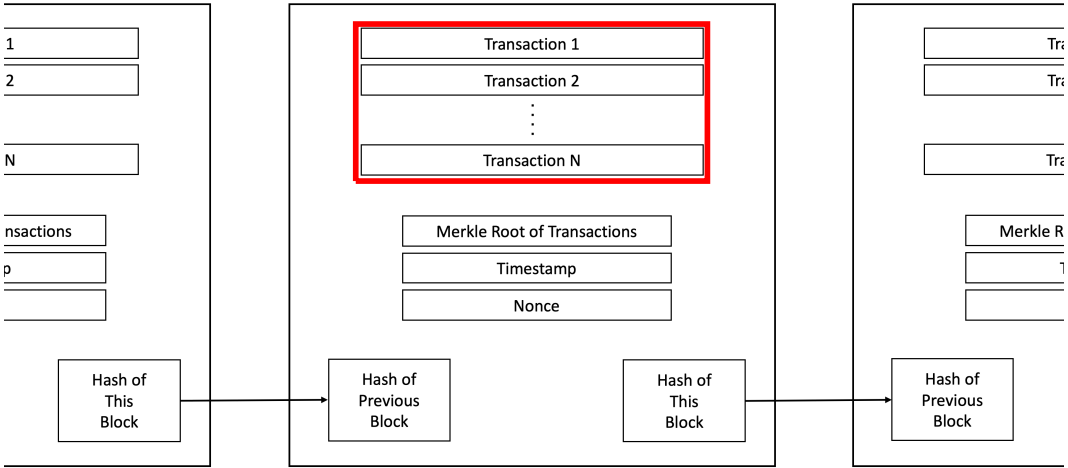
Nakamoto (2008) Blockchain Innovation

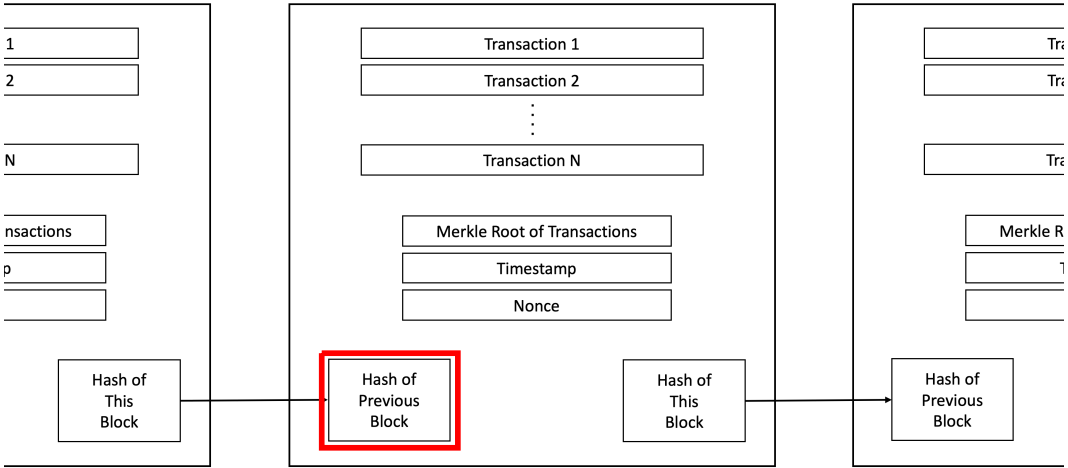
- **I: Pending Transactions List**
  - Users submit transactions to a pending transactions list, called mempool
  - Like a google spreadsheet — not considered official yet
- **II: Valid Blocks**
  - Any computer around the world can compete for the right to add transactions from the mempool to a data 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


1
2
N
nsactions
p
Transaction 1
Transaction 2
Transaction N
Merkle Root of Transactions
Timestamp
Nonce
Tra
Tra
Tra
Merkle R
Hash of This Block
Hash of Previous Block
Hash of This Block
Hash of Previous Block

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.

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

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

    $$0000000000000000008b6f6fb83f8d74512ef1e0af29e642dd20daddd7d318f$$

  - 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)

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

    $$000000000000000000008b6f6fb83f8d74512ef1e0af29e642dd20daddd7d318f$$

  - 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 250 million TH/s (2.5×10^{20})

SHA-256 Hash Function: Example

Name	SHA256 Hash	Name	SHA256 Hash
Isaiah Andrews	ecf88ddb2fae9c572d533a8e2b2734bdf5c176c40e6a4b6bfaaaeadf80115c38	Gabriel Kreindler	1dbb7fec624a48bfa3d7480e8a4e42c8b919ff5395e826e8607c46cacf2228f2
Pol Antràs	a811ca78d06d8ae91b47a0a0f430f9a21f696ce0036b3ba94110d1727fe6e8c4	David Laibson	1a2dc2210c41abb4d2d9da44ca78cab915df2c5849b9e9513b5b5b1e10d7c2df
Robert Barro	a811ca78d06d8ae91b47a0a0f430f9a21f696ce0036b3ba94110d1727fe6e8c4	Robin Lee	e1503dd738a8a02bc054a739eca92a9e7400fe47eed8a876d72b5313d9048a72
Adrien Bilal	dbe079b1595c74595b6a9afa8c9af2bca4685986c3650e083d4f20895e818c20	Shengwu Li	62f63590404ce5685054d86895a3e958294d8133f708f085716d87541b9e863c
Emily Breza	2d31773d6da6d54818c24a5f3477ae6e7021e778395e1b409595ac6177fbf726	N. Gregory Mankiw	574834d3cda09cd66a4f7a2f0e3361f9e5578ea686425e0fede15a73868cd35d
John Y. Campbell	62696d13b16650d3743198ac70d4c31f4315ad25e2e174c186c7f505cfe824fe	Stephen Marglin	fe782870a17292c82ce218839c848d9699a342bc54c790ad0b97312da2553767
Raj Chetty	ab4129898166640da51dd836249a57741c2ccae8a7615165604e313b6b17f18	Eric S. Maskin	9e691095bc808b7ffbbce0e3742e376a3bfb98107cecf6a412fa937aa16f9e65
Gabriel Chodorow-Reich	e700d6114da87852f4ef997763e9a47d17c3ff379cde9fa5dd0cf225536e9ae6f	Marc Melitz	5c6181e634b8b69b3505d7d8e2d37f136f5f245b306594f71ef0c5d0a75858c4
David M. Cutler	cd4fe428e0021379cdb6262db10147757bc509efdcad0ee3a7d417ab67db5c8a	Jeffrey Miron	425bde3f650d9f85145f702503105d09b83e6c25dd1ed5ec6708673716cc9614
Melissa Dell	dceab6bcdf4f3a8288c4d4a8b97a3752c64d28bc0912ca2aaeda21111d1887a1	Ariel Pakes	5997223f684c40600214017c54f69757581bde73ff88d7b3c1a38c582c01ae1d
Karen Dynan	c4d5d04b5f15d60da4c97318576a66603b832c3579831db993f0ce8b6321261a	Amanda Pallais	89cfb6f19d19d3260081afbf4dac942ccebc885de200f98a94eeae25e69349b7
Benjamin Enke	6326a164b172d62689d240effefc8e104e9d565eda1de3c9c6076615266e16bd	Matthew Rabin	2d42411c07ccf10194873b772ea64cbca21dfe70527ec25ca3985641f7c48ec7
Christopher Foote	d03fa5fcf873d7bc9d5bd8541b2a8bb817b5b893cec6d12ad9f6608aecf5d14d	Gautam Rao	a7af4444426021253504623f12dd71a4c99542b414b27f1993794fa61e08e93c
Richard B. Freeman	6e8ada6cc9f64dcfd274425ef25d533888c4d48edd4804e330ac04c43bdbcf34	Kenneth Rogoff	14084190b01c773da377ed70b74df3a54c894b236cd888c10d4f7f0e05d22bcc
Benjamin Friedman	97dc15f1334e801950f9b3c8f11e0f382306c3f20a53c5a3b4dc2f504cb9968f	Amartya Sen	5c18512379dc8b4e48ad391ebbd12993ac8802ee979cf6755a825e64a024b8d8
Roland Fryer	c13cedf6c198852aa83964a79a32ae9e38612b911425918c659d607d706cdfc3	Jesse Shapiro	da09c60a6adf01f8bf76a75ff46e4f98a92b1a53c9708351838703f29e016ca
Jason Furman	652f58ab028efb7dd70cea45a5535704514cb47ab1fac2e67fee2d832d1042b9	Neil Shephard	76f2a1bd0b6885048c87330c66e64840b1c7527865eb63b6e247136786fa9e3f
Xavier Gabaix	ed761b207277542d5ea469a3cab49e3483a5c36435927387eac63c7fb7631718	Andrei Shleifer	e45a2bb1c5411cb3e759f78cf9d0274210d717e14916618dcbd058d8b23d29be
Edward Glaeser	dd7151d697aad5182d61582088a6d3a3b44a567f8a486fdf7ebbd985bd6f9c19	Stefanie Stantcheva	df5259157fa05ad7466dd2b609f2db19b9dae01db7d0f6f8b3d65cfd7285ee98
Claudia Goldin	507674e1362e2b9849093431baf6b0eccad8d8badcd7eb7a8b2069179c92830028	Jeremy Stein	663b54c0870519d41f65e4d0f463513790280 9de9a3c4f8827361e4514b4ea5
Yannai Gonczarowski	ed05f26a688d3153a9c54264065f57f71b0d1bd9e3d4105526b9781e85d1f0d6	James Stock	0937e137ef6983c49e9f89fa0ec9ba9dbe89ec386a6d8affd6ca5e4175a0792e
Jerry Green	cbe7708cc1fdc8c1132decbd0ed617691b8e44c9d22c68b5ef83f020379c6e96	Ludwig Straub	fd0fb6fcdbf13d9bb97801219339 24d5d501e796be7b99660a8cb2dbaeeb23e7
Oliver Hart	e66791e61e542f9f4ac35f9b45a52f480a661cb9c2899680466dacdc556b67dc	Tomasz Strzalecki	3dd00df7e76cd517a8e51effef0422c02d9582b5ff9b2c77ba805c359d5c9baa
Elhanan Helpman	2a923d5edb959dff23e9ccb6913e620352e526eec4ae1e72ee8b1d72b56e6c7d	Lawrence Summers	3ef1b83556faa89305aedfa4ba24d35b1a78909d027d54515f14d06e85f6aee0
Nathaniel Hendren	1d9ee59d60289a376e7ed2bcf3e0e1266a06381ce1a53c343a3747777f694806b	Elie Tamer	28f5c81700bd1174d4ddeb4390388d8b63fa82e9aec3de6a6af721c8b15083d0
Myrto Kalouptsidi	edabed5b8c9a439e5216030c7ff9d4fa40161094a7aa5740c093794075114729	Winnie van Dijk	69cc8effebd1f54fb04db2e1a1a1978e81f8ffcf269d16785aa4b0c7362d0dc0
Lawrence Katz	77f7bd7f506968fa458bc0c7f6bc5ae79930045c98da9389ad5e3fdf0fc0e4a1	David Yang	9c81af6c507eec0493601faad3d83546418be18e9946e5b1484d97dec2655ef4

SHA-256 Hash Function: Example

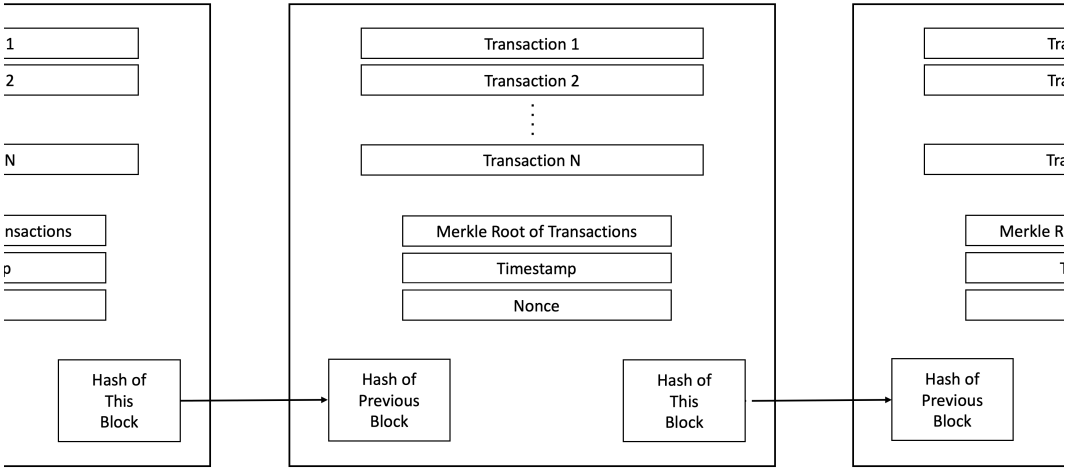
Name	SHA256 Hash	Name	SHA256 Hash
Isaiah Andrews	ecf88ddb2fae9c572d533a8e2b2734bdf5c176c40e6a4b6bfaaaeadf80115c38	Gabriel Kreindler	1dbb7fec624a48bfa3d7480e8a4e42c8b919ff5395e826e8607c46cacf2228f2
Pol Antràs	a811ca78d06d8ae91b47a0a0f430f9a21f696ce0036b3ba94110d1727fe6e8c4	David Laibson	1a2dc2210c41abb4d2d9da44ca78cab915df2c5849b9e9513b5b5b1e10d7c2df
Robert Barro	a811ca78d06d8ae91b47a0a0f430f9a21f696ce0036b3ba94110d1727fe6e8c4	Robin Lee	e1503dd738a8a02bc054a739eca92a9e7400fe47eed8a876d72b5313d9048a72
Adrien Bilal	dbe079b1595c74595b6a9afa8c9af2bca4685986c3650e083d4f20895e818c20	Shengwu Li	62f63590404ce5685054d86895a3e958294d8133f708f085716d87541b9e863c
Emily Breza	2d31773d6da6d54818c24a5f3477ae6e7021e778395e1b4095954ac6177bf726	N. Gregory Mankiw	574834d3cda09cd66a4f7a2f0e3361f9e5578ea686425e0fede15a73868cd35d
John Y. Campbell	62696d13b16650d3743198ac70d4c31f4315ad25e2e174c186c7f505cfe824fe	Stephen Marglin	fe782870a17292c82ce218839c848d9699a342bc54c790ad0b97312da2553767
Raj Chetty	ab4129898166640da51dd836249a57741c2ccae8a7615165604e313b6b17f18	Eric S. Maskin	9e691095bc808b7ffbbce0e3742e376a3bfb98107cecf6a412fa937aa16f9e65
Gabriel Chodorow-Reich	e700d6114da87852f4ef997763e9a47d17c3ff379cde9fa5dd0cf225536e9ae6f	Marc Melitz	5c6181e634b8b69b3505d7d8e2d37f136f5f245b306594f71ef0c5d0a75858c4
David M. Cutler	cd4fe428e0021379cdb6262db10147757bc509efdcad0ee3a7d417ab67db5c8a	Jeffrey Miron	425bde3f650d9f85145f702503105d09b83e6c25dd1ed5ec6708673716cc9614
Melissa Dell	dceab6bcdf4f3a8288c4d4a8b97a3752c64d28bc0912ca2aaeda21111d1887a1	Ariel Pakes	5997223f684c40600214017c54f69757581bde73ff88d7b3c1a38c582c01ae1d
Karen Dynan	c4d5d04b5f15d60da4c97318576a66603b832c3579831db993f0ce8b6321261a	Amanda Pallais	89cfb6f19d19d3260081afbf4dac942ccebc885de200f98a94eeae25e69349b7
Benjamin Enke	6326a164b172d62689d240effefc8e104e9d565eda1de3c9c6076615266e16bd	Matthew Rabin	2d42411c07ccf10194873b772ea64cbca21dfe70527ec25ca3985641f7c48ec7
Christopher Foote	d03fa5fcf873d7bc9d5bd8541b2a8bb817b5b893cec6d12ad9f6608aecf5d14d	Gautam Rao	a7af4444426021253504623f12dd71a4c99542b414b27f1993794fa61e08e93c
Richard B. Freeman	6e8ada6cc9f64dcfd274425ef25d533888c4d48edd4804e330ac04c43bdbcf34	Kenneth Rogoff	14084190b01c773da377ed70b74df3a54c894b236cd888c10d4f7f0e05d22bcc
Benjamin Friedman	97dc15f1334e801950f9b3c8f11e0f382306c3f20a53c5a3b4dc2f504cb9968f	Amartya Sen	5c18512379dc8b4e48ad391ebbd12993ac8802ee979cf6755a825e64a024b8d8
Roland Fryer	c13cedf6c198852aa83964a79a32ae9e38612b911425918c659d607d706cdfc3	Jesse Shapiro	da09c60a6adf01f8bf76a75ff46e4f98a92b1a53c9708351838703f29e016ca
Jason Furman	652f58ab028efb7dd70cea45a5535704514cb47ab1fac2e67fee2d832d1042b9	Neil Shephard	76f2a1bd0b6885048c87330c66e64840b1c7527865eb63b6e247136786fa9e3f
Xavier Gabaix	ed761b207277542d5ea469a3cab49e3483a5c36435927387eac63c7fb7631718	Andrei Shleifer	e45a2bb1c5411cb3e759f78cf9d0274210d717e14916618dcbd058d8b23d29be
Edward Glaeser	dd7151d697aad5182d61582088a6d3a3b44a567f8a486fdf7ebbd985bd6f9c19	Stefanie Stantcheva	df5259157fa05ad7466dd2b609f2db19b9dae01db7d0f6f8b3d65cfd7285ee98
Claudia Goldin	507674e1362e2b9849093431baf6b0eccad8dbacd7eb7a8b2069179c92830028	Jeremy Stein	663b54c0870519d41f65e4d0f463513790280 9de9a3c4f8827361e4514b4ea5
Yannai Gonczarowski	ed05f26a688d3153a9c54264065f57f71b0d1bd9e3d4105526b9781e85d1f0d6	James Stock	0937e137ef6983c49e9f89fa0ec9ba9dbe89ec386a6d8affd6ca5e4175a0792e
Jerry Green	cbe7708cc1fdc8c1132decbd0ed617691b8e44c9d22c68b5ef83f020379c6e96	Ludwig Straub	fd0fb6fcdbf13d9bb97801219339 24d5d501e796be7b99660a8cb2dbaeeb23e7
Oliver Hart	e66791e61e542f9f4ac35f9b45a52f480a661cb9c2899680466dacdc556b67dc	Tomasz Strzalecki	3dd00df7e76cd517a8e51effef0422c02d9582b5ff9b2c77ba805c359d5c9baa
Elhanan Helpman	2a923d5edb959dff23e9ccb6913e620352e526eec4ae1e72ee8b1d72b56e6c7d	Lawrence Summers	3ef1b83556faa89305aedfa4ba24d35b1a78909d027d54515f14d06e85f6aee0
Nathaniel Hendren	1d9ee59d60289a376e7ed2bcf3e0e1266a06381ce1a53c343a3747777f694806b	Elie Tamer	28f5c81700bd1174d4ddeb4390388d8b63fa82e9aec3de6a6af721c8b15083d0
Myrto Kalouptsidi	edabed5b8c9a439e5216030c7ff9d4fa40161094a7aa5740c093794075114729	Winnie van Dijk	69cc8effebd1f54fb04db2e1a1a1978e81f8ffcf269d16785aa4b0c7362d0dc0
Lawrence Katz	77f7bd7f506968fa458bc0c7f6bc5ae79930045c98da9389ad5e3fdf0fc0e4a1	David Yang	9c81af6c507eec0493601faad3d83546418be18e9946e5b1484d97dec2655ef4

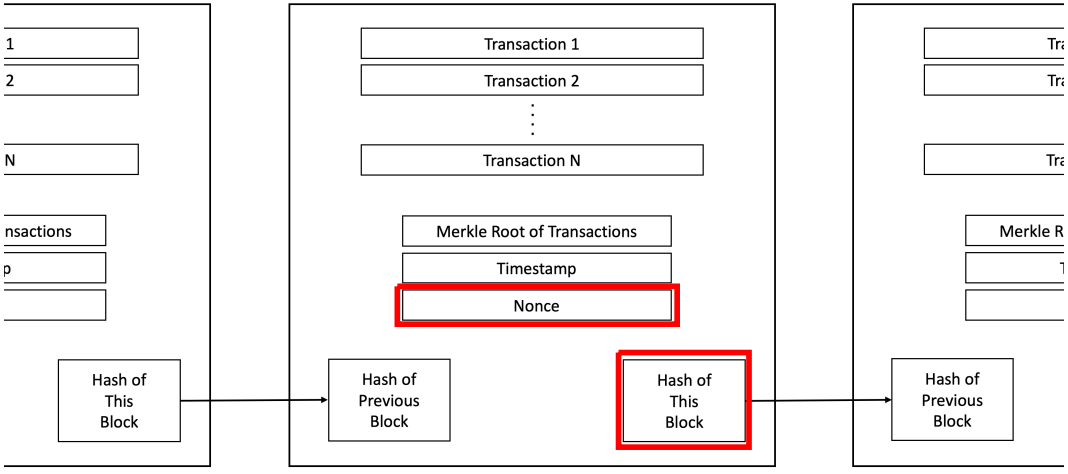
What is Nakamoto Blockchain (3/4)

- **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)

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.
    - Will ignore tx fees for the purpose of this talk. (see Huberman, Leshno and Moallemi, 2021)
- Tournament difficulty adjusts every two weeks, calibrated to take about 10 minutes


1
2
N
nsactions
p
Hash of This Block
Transaction 1
Transaction 2
Transaction N
Merkle Root of Transactions
Timestamp
Nonce
Hash of Previous Block
Hash of This Block
Tra
Tra
Tra
Merkle R
Hash of Previous Block



Hash of block data must have a very large number of leading zeros.
Example from Block $729,999$**:**
- **Hash:** $0000000000000000008b6f6fb83f8d745\ldots$

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*

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))

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:

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.

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"

- As interest in Bitcoin and its blockchain have surged, some have started to use the phrase "blockchain" to describe distributed databases among *known, trusted parties* – that is, *without* the central innovation of Nakamoto (2008)

Clarification I: "Permissioned Blockchains"

- As interest in Bitcoin and its blockchain have surged, some have started to use the phrase "blockchain" to describe distributed databases among *known, trusted parties* – that is, *without* the central 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"

- As interest in Bitcoin and its blockchain have surged, some have started to use the phrase "blockchain" to describe distributed databases among *known, trusted parties* – that is, *without* the central 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)

- My critique is of blockchain in the sense of Nakamoto (2008), not of distributed databases / ledgers
- A very interesting open question is whether the blockchain data structure is economically valuable in contexts where the trust is grounded in traditional sources. Will return to this at the end.

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
- Usual motiviation: reduce mining expense and environmental harm ("Ethereum reduces its energy use by 99.95%")
- Environmental issue is orthogonal to the concerns raised in this paper

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
- Usual motiviation: reduce mining expense and environmental harm ("Ethereum reduces its energy use by 99.95%")
- Environmental issue is orthogonal to the concerns raised in this paper
- What's interesting re: this paper's argument is that stakes have *memory*. This opens up new possibilities for making attacks more expensive
  - Will return to this at the end.
  - So far, no PoS that makes "all" attacks more expensive. (Ex: Ethereum PoS makes double-spending attacks much more expensive, but is vulnerable to "liveness attacks" which are cheap. Where "expensive" = stock, "cheap" = flow.).

Overview of the Talk

A General Introduction:

- What is Nakamoto Blockchain?

The Economic Limits of Bitcoin and Anonymous, Decentralized Trust:

- **Nakamoto Blockchain: A Critique in 3 Equations**
  - **Flow vs. Stock Problem**
  - **Zero Net Attack Cost Theorem**
- Analysis of Double Spending Attacks
- A Way Out: Specialized Capital + Risk of Collapse
  - A Softer Constraint: Stock vs. Stock. Collapse Scenarios.

Open Questions for Future Research:

- Q1: Permissionless trust beyond Nakamoto
- Q2: Economics of permissioned blockchains
- Many other open q's related to theory, finance, policy

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?

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

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

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 $\{x_i^*\}_{i \in I}$ 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.

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 $\{x_i^*\}_{i \in I}$ 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)?

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.

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 $A^* \cdot t(A^*)$

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:

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

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:

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

- Remarks

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:

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

- 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)

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:

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

- 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

Critique in 3 Equations

The Problem

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

Critique in 3 Equations

The Problem

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

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

Critique in 3 Equations

The Problem

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

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

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

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

Critique in 3 Equations

The Problem

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

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

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

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

- *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*

Critique in 3 Equations

The Problem

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

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

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

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

- *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:

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.

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

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

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 $(1 + \kappa)At \cdot N^* c$

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.*

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.

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

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 $N = \sum x_i$.
- 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 $a_i = \textit{Honest}$ (and some x_i^* consistent with NE)
  - Lemma. If there is an honest equilibrium, then $N^* c \leq p$. (1)
  - Theorem. A necessary condition for no player to have a profitable attack is $p \geq \frac{V_{attack}}{1+\frac{1}{f}}$ (3)

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

- Question: under what conditions is there a Nash equilibrium in which all players i choose $a_i = \textit{Honest}$ (and some x_i^* consistent with NE)
  - Lemma. If there is an honest equilibrium, then $N^* c \leq p$. (1)
  - Theorem. A necessary condition for no player to have a profitable attack is $p \geq \frac{V_{attack}}{1+\frac{1}{l}}$ (3)
- Proof of Theorem.
  - Honest play payoff for i: $\frac{x_i^*}{N^*} p - x_i^* c$
  - Attack payoff for i: $V_{attack} - N_{j \neq i}^* c$ (where $N_{j \neq i}^* = \sum_{j \neq i} x_i^*$)
  - Need: $V_{attack} - N_{j \neq i}^* c \leq \frac{x_i^*}{N^*} p - x_i^* c$. (If $x_i^* = 0$, this is $N^* c \geq V_{attack}$, which corresponds to (2))
  - Rearrange: $V_{attack} \leq N_{j \neq i}^* c - x_i^* c + \frac{x_i^*}{N^*} p$
  - Using Lemma: $V_{attack} \leq p + \frac{x_i^*}{N^*} p$
- Using smallest x_i^*: $V_{attack} \leq p(1 + \frac{1}{l})$. QED.

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

- Question: under what conditions is there a Nash equilibrium in which all players i choose $a_i = \textit{Honest}$ (and some x_i^* consistent with NE)
  - Lemma. If there is an honest equilibrium, then $N^* c \leq p$. (1)
  - Theorem. A necessary condition for no player to have a profitable attack is $p \geq \frac{V_{attack}}{1+\frac{1}{I}}$ (3)
- Proof of Theorem.
  - Honest play payoff for i: $\frac{x_i^*}{N^*} p - x_i^* c$
  - Attack payoff for i: $V_{attack} - N_{j \neq i}^* c$ (where $N_{j \neq i}^* = \sum_{j \neq i} x_i^*$)
  - Need: $V_{attack} - N_{j \neq i}^* c \leq \frac{x_i^*}{N^*} p - x_i^* c$. (If $x_i^* = 0$, this is $N^* c \geq V_{attack}$, which corresponds to (2))
  - Rearrange: $V_{attack} \leq N_{j \neq i}^* c - x_i^* c + \frac{x_i^*}{N^*} p$
  - Using Lemma: $V_{attack} \leq p + \frac{x_i^*}{N^*} p$
- Using smallest x_i^*: $V_{attack} \leq p(1 + \frac{1}{I})$. QED.

- As I goes to infinity, condition is $p \geq V_{attack}$
- 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

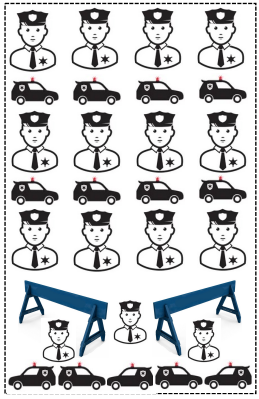
Traditional Security Model:

Traditional Security Model

Traditional Security Model:

- Security Guards

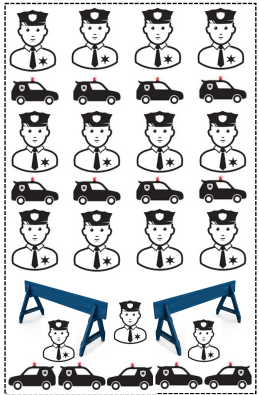
Traditional Security Model

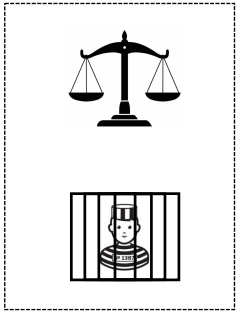


Traditional Security Model:

- 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:

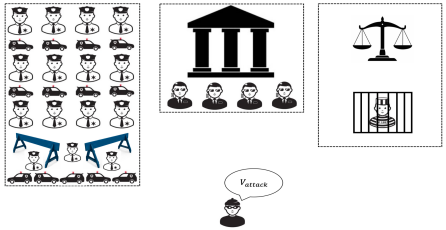
- Large amount of Security Guards
- But no additional layers (Police, Rule of Law)

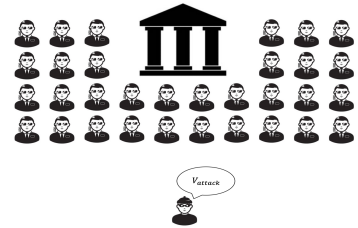
Bank Security Model

Bitcoin Security Model:

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

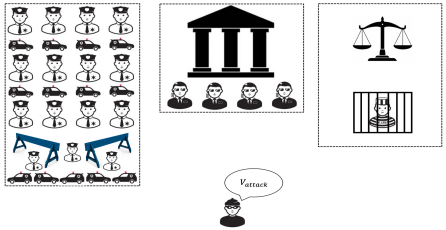
Comparison of Security Models

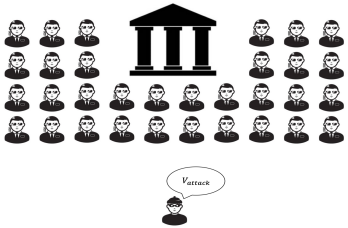




Traditional Security	Bitcoin Security
cost of overcoming guards + cost of overcoming police reinforcements + risk × punishment if caught $> V_{attack}$	cost of overcoming guards $> V_{attack}$

Comparison of Security Models



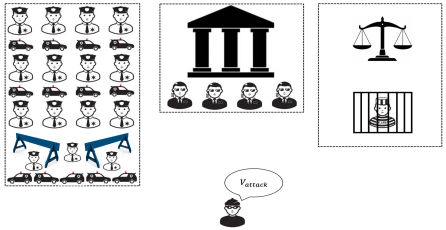


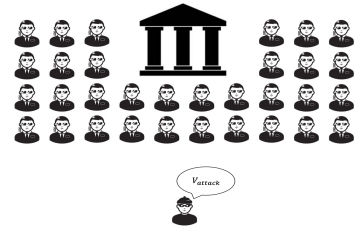
Traditional Security	Bitcoin Security
cost of overcoming guards + cost of overcoming police reinforcements + risk × punishment if caught $> V_{attack}$	cost of overcoming guards $> V_{attack}$

Key contrast:

- Traditional security benefits from economies of scale, from police, and Beckerian deterrence from punishment.

Comparison of Security Models



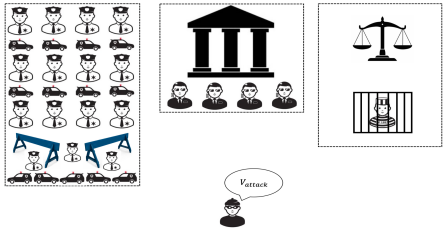


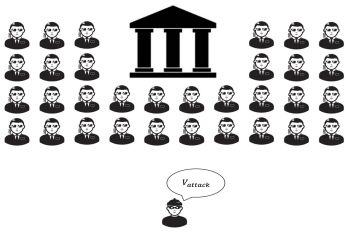
Traditional Security	Bitcoin Security
cost of overcoming guards + cost of overcoming police reinforcements + risk × punishment if caught $> V_{attack}$	cost of overcoming guards $> V_{attack}$

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.

Comparison of Security Models





Traditional Security	Bitcoin Security
cost of overcoming guards + cost of overcoming police reinforcements + risk × punishment if caught $> V_{attack}$	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

A General Introduction:

- What is Nakamoto Blockchain?

The Economic Limits of Bitcoin and Anonymous, Decentralized Trust:

- Nakamoto Blockchain: A Critique in 3 Equations
  - Flow vs. Stock Problem
  - Zero Net Attack Cost Theorem
- **Analysis of Double Spending Attacks**
- A Way Out: Specialized Capital + Risk of Collapse
  - A Softer Constraint: Stock vs. Stock. Collapse Scenarios.

Open Questions for Future Research:

- Q1: Permissionless trust beyond Nakamoto
- Q2: Economics of permissioned blockchains
- Many other open q's related to theory, finance, policy

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

Attack I: Double Spending

- Attacker can double spend:
  - (i) spend Bitcoins — i.e., engage in a transaction in which he sends Bitcoins to a merchant in exchange for goods or assets
  - (ii) allow that transaction to be added to the blockchain
  - (iii) the attacker works in secret to create an alternative longest chain (in which those same Bitcoins are sent to other accounts they control)
  - (iv) the attacker waits for any escrow periods to elapse, so they receive the goods or assets in (i)
  - (v) the attacker then releases their alternative longest chain. They now have the goods or assets received in (iv), and also the Bitcoins they sent to themselves in (iii)
- Recall, this is the canonical attack Nakamoto (2008) worries about ("We propose a solution to the double-spending problem using a peer-to-peer ...")

Illustration of Double Spending

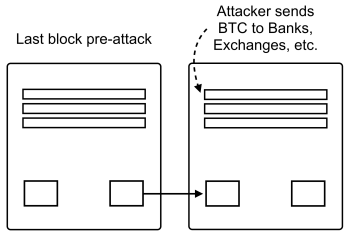


Illustration of Double Spending

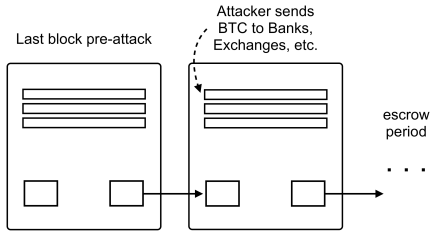


Illustration of Double Spending

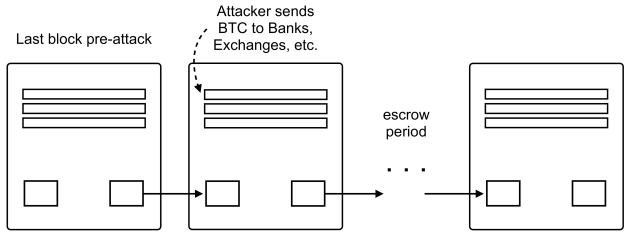


Illustration of Double Spending

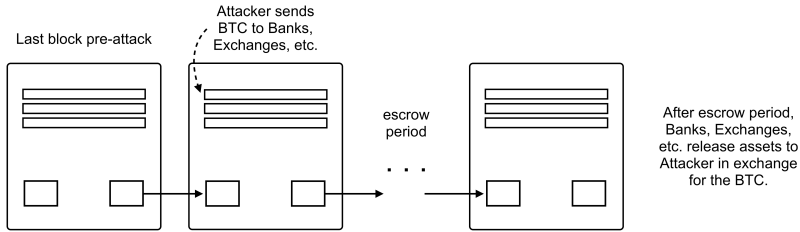


Illustration of Double Spending

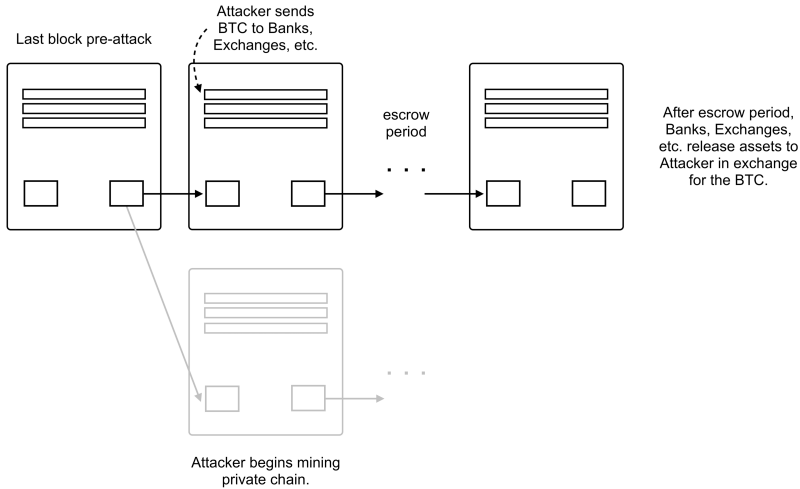


Illustration of Double Spending

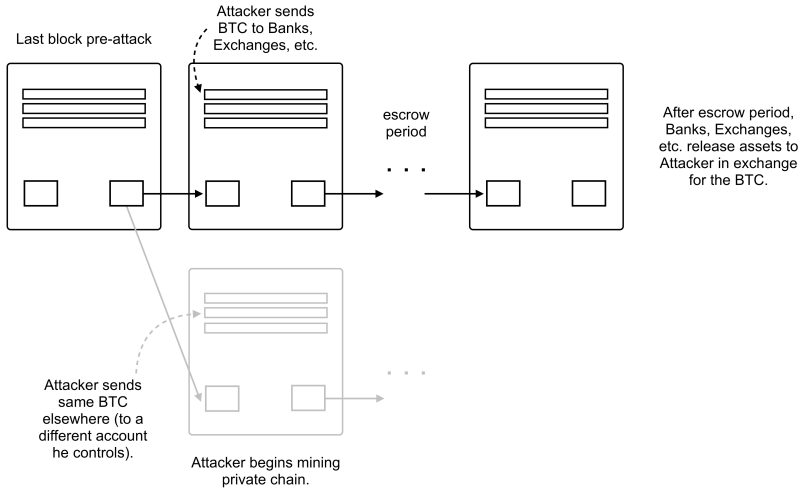


Illustration of Double Spending

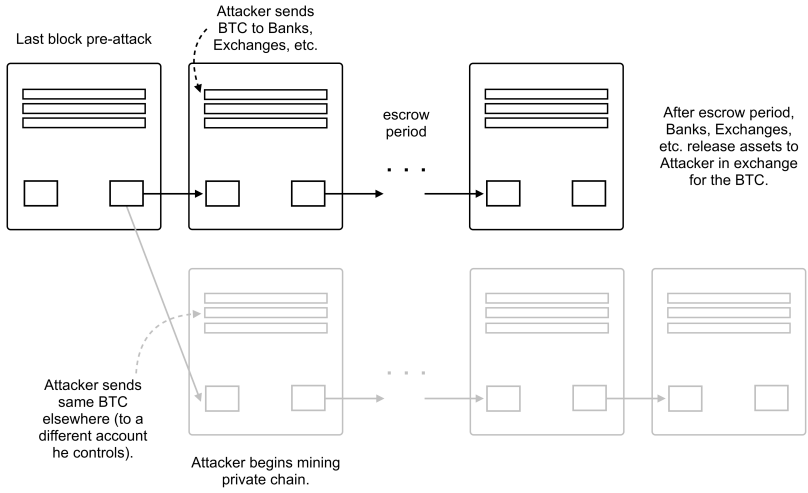
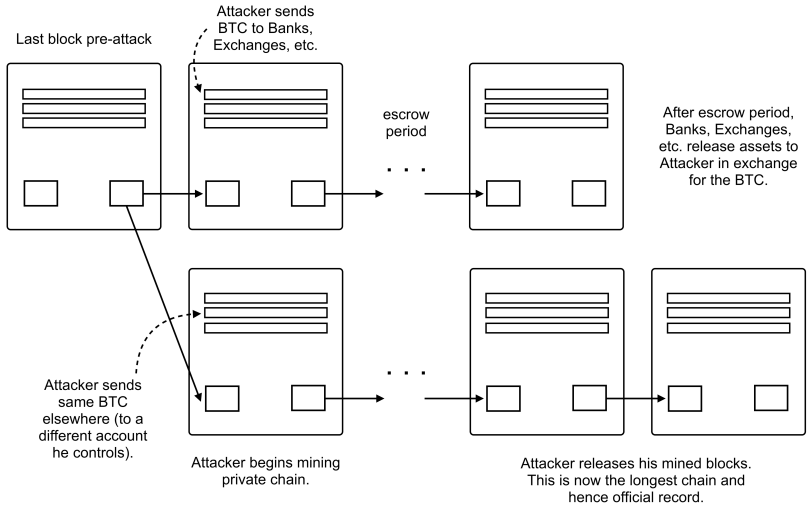


Illustration of Double Spending



Double Spending: Analysis Framework

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

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

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 amount of transaction volume that *honest users* of Bitcoin can conduct in a modest amount of time ("max economic throughput")
  - I consider a range from \$1000 (pizza) to \$100bn (global finance)

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 amount of transaction volume that *honest users* of Bitcoin can conduct in a modest amount of time ("max economic throughput")
  - I consider a range from \$1000 (pizza) to \$100bn (global finance)
- Duration of attack: $A^* \cdot t(A^*)$
  - Can compute explicitly

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 amount of transaction volume that *honest users* of Bitcoin can conduct in a modest amount of time ("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 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

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:

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

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:

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

- 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

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:

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

- 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	1,104.45
$A = 1.2$	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 (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	1,104.45
$A = 1.2$	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 (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	1,104.45
$A = 1.2$	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.

Double Spending Attack: Cases and Sensitivity

- I consider a range of cases for At informed by the computations
- **Base case,** $At = 16$. Corresponds to gross costs under current escrow period $e = 6$ and attacker majority $A = 1.25$ (55%).
  - Net costs if $\kappa = 1$ (frictions cancel block rewards) and $\Delta_{attack} = 0$.
- **Expensive attack case**, $At = 150$. Corresponds to one full day of block-compute-costs.
  - Appropriate if escrows longer for higher-value transactions.
  - Or, base case with higher attack frictions.
- **Very expensive attack case** $At = 1000$. One full week of block-compute-costs

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	6.25%	900%	328,500%	0.003%
To Secure:				
$1 thousand	$62.5 dollars	$9.0 thousand	$3.3 million	3.1 cents
$1 million	$62.5 thousand	$9.0 million	$3.3 billion	$31.3 dollars
$1 billion	$62.5 million	$9.0 billion	$3.3 trillion	$31.3 thousand
$100 billion	$6.3 billion	$900.0 billion	$328.5 trillion	$3.1 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	6.25%	900%	328,500%	0.003%
To Secure:				
$1 thousand	$62.5 dollars	$9.0 thousand	$3.3 million	3.1 cents
$1 million	$62.5 thousand	$9.0 million	$3.3 billion	$31.3 dollars
$1 billion	$62.5 million	$9.0 billion	$3.3 trillion	$31.3 thousand
$100 billion	$6.3 billion	$900.0 billion	$328.5 trillion	$3.1 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	6.25%	900%	328,500%	0.003%
To Secure:				
$1 thousand	$62.5 dollars	$9.0 thousand	$3.3 million	3.1 cents
$1 million	$62.5 thousand	$9.0 million	$3.3 billion	$31.3 dollars
$1 billion	$62.5 million	$9.0 billion	$3.3 trillion	$31.3 thousand
$100 billion	$6.3 billion	$900.0 billion	$328.5 trillion	$3.1 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	6.25%	900%	328,500%	0.003%
To Secure:				
$1 thousand	$62.5 dollars	$9.0 thousand	$3.3 million	3.1 cents
$1 million	$62.5 thousand	$9.0 million	$3.3 billion	$31.3 dollars
$1 billion	$62.5 million	$9.0 billion	$3.3 trillion	$31.3 thousand
$100 billion	$6.3 billion	$900.0 billion	$328.5 trillion	$3.1 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	6.25%	900%	328,500%	0.003%
To Secure:				
\$1 thousand	\$62.5 dollars	\$9.0 thousand	\$3.3 million	3.1 cents
\$1 million	\$62.5 thousand	\$9.0 million	\$3.3 billion	\$31.3 dollars
\$1 billion	\$62.5 million	\$9.0 billion	\$3.3 trillion	\$31.3 thousand
\$100 billion	\$6.3 billion	\$900.0 billion	\$328.5 trillion	\$3.1 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 B. Securing Against an Attack: Sensitivity Analysis

Attack Scenarios	Per-Block	Per-Day	Per-Year	Per-Transaction
Base Case	6.25 %	900 %	328,500 %	0.003 %
Expensive	0.67 %	96 %	35,040 %	0.0003 %
Very Expensive	0.10 %	14 %	5,256 %	0.00005 %

Securing Against an Attack: Sensitivity Analysis

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

Attack Scenarios	Per-Block	Per-Day	Per-Year	Per-Transaction
Base Case	6.25 %	900 %	328,500 %	0.003 %
Expensive	0.67 %	96 %	35,040 %	0.0003 %
Very Expensive	0.10 %	14 %	5,256 %	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 B. Securing Against an Attack: Sensitivity Analysis

Attack Scenarios	Per-Block	Per-Day	Per-Year	Per-Transaction
Base Case	6.25 %	900 %	328,500 %	0.003 %
Expensive	0.67 %	96 %	35,040 %	0.0003 %
Very Expensive	0.10 %	14 %	5,256 %	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 attack duration (very expensive), require an annual expense of $52bn, per-transaction cost of $500, to keep Bitcoin secure up to $1bn attack.
  - 5% of Global GDP, $50k per tx, to secure against $100bn attack.

Double Spending Attack: Takeaways

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

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 \$0.03

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 \$0.03
- 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, \$30M exp. case)

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 \$0.03
- 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, \$30M exp. 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 (computer parts, silk road, online gambling)—if double-spending worth \$1k, then cost per tx just \$0.03
- 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, \$30M 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

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 \$0.03
- 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, \$30M 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

Overview of the Talk

A General Introduction:

- What is Nakamoto Blockchain?

The Economic Limits of Bitcoin and Anonymous, Decentralized Trust:

- Nakamoto Blockchain: A Critique in 3 Equations
  - Flow vs. Stock Problem
  - Zero Net Attack Cost Theorem
- Analysis of Double Spending Attacks
- **A Way Out: Specialized Capital + Risk of Collapse**
  - **A Softer Constraint: Stock vs. Stock. Collapse Scenarios.**

Open Questions for Future Research:

- Q1: Permissionless trust beyond Nakamoto
- Q2: Economics of permissioned blockchains
- Many other open q's related to theory, finance, policy

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

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.*

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 ...

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

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")

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?

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

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

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)

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?

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")

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

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:

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

Cost to Secure Against Sabotage, Derivation

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

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

- 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

$$N^* C > V_{attack} \tag{2'}$$

Cost to Secure Against Sabotage, Derivation

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

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

- 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

$$N^* C > V_{attack} \tag{2'}$$

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

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

Cost to Secure Against Sabotage, Derivation

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

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

- 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

$$N^* C > V_{attack} \tag{2'}$$

- 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):

$$p_{block} > \frac{r}{\mu} V_{attack} \tag{3'}$$

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.

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 $At = 16$, 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 $N^*C = \$12B$ which roughly matches observed prices.)

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 $At = 16$, 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 $N^*C = \$12B$ which roughly matches observed prices.)
- Annual cost to secure $1bn:
  - Original model without collapse: $3.3 trillion
  - Sabotage model with collapse: $1.25 billion ($2.5 bn for insider sabotage)
- Current capital stock and miner payments suggests Bitcoin is secure up to sabotages worth roughly $10bn for an outsider, $5bn for an insider

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.

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:

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

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'): $N^* C > V_{attack}$

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

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 $N^*\eta'$.

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.

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

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

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: $V_{attack} > N^* C$.

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.
  - $12bn is small in the scheme of global finance

Examples of 51% Attacks

Name	Hash function	Date of First Attack	Amount Stolen
Bitcoin SV	SHA-256	8/3/2021	Unknown
Verge	Scrypt, X17, Lyra2rev2, Myr-groestl, Blake2s	2/15/2021	Unknown
		4/4/2018	$2.8 million
Grin	Cuckoo Cycle	11/8/2020	Unknown
Ethereum Classic	Ethash	8/29/2020	Unknown
		8/6/2020	$1.7 million
		7/29/2020	$5.6 million
		1/5/2019	$1.1 million
Bitcoin Gold	Equihash	1/23/2020	$100 thousand
		5/16/2018	$18 million
Firo	MTP	1/19/2019	$4 million
Vertcoin	Lyra2rev2	10/12/2018	$100 thousand
Zencash	Equihash	6/2/2018	$700 thousand
Litecoin Cash	SHA-256	5/30/2018	Unknown
Monacoin	Lyra2rev2	5/13/2018	$100 thousand

Sources: Bloomberg, Coindesk, Bitcoinist, CCN, Cointelegraph, bitquery, GitHub Gist and Medium. The hash functions listed here are the hash functions at the time of the attack. 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	Hash function	Date of First Attack	Amount Stolen
Bitcoin SV	SHA-256	8/3/2021	Unknown
Verge	Scrypt, X17, Lyra2rev2, Myr-groestl, Blake2s	2/15/2021	Unknown
		4/4/2018	$2.8 million
Grin	Cuckoo Cycle	11/8/2020	Unknown
Ethereum Classic	**Ethash**	**8/29/2020**	**Unknown**
		8/6/2020	**$1.7 million**
		7/29/2020	**$5.6 million**
		1/5/2019	**$1.1 million**
Bitcoin Gold	**Equihash**	1/23/2020	$100 thousand
		5/16/2018	**$18 million**
Firo	MTP	1/19/2019	$4 million
Vertcoin	Lyra2rev2	10/12/2018	$100 thousand
Zencash	Equihash	6/2/2018	$700 thousand
Litecoin Cash	SHA-256	5/30/2018	Unknown
Monacoin	Lyra2rev2	5/13/2018	$100 thousand

Sources: Bloomberg, Coindesk, Bitcoinist, CCN, Cointelegraph, bitquery, GitHub Gist and Medium. The hash functions listed here are the hash functions at the time of the attack. 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 Crypto Thefts

Name	Type of Business	Date of Attack	Amount Stolen
Mango Market	Decentralized Exchange	October 2022	$100 million
BNB Chain	DeFi Bridge	October 2022	$568 million
Wintermute	DeFi Market Maker	September 2022	$160 million
Nomad	DeFi Bridge	August 2022	$200 million
Beanstalk Farms	DeFi Stablecoin	April 2022	$182 million
Ronin Network	DeFi Bridge	March 2022	$625 million
Wormhole	DeFi Bridge	February 2022	$320 million
BitMart	Centralized Exchange	December 2021	$150 million
C.r.e.a.m. Finance	DeFi Lending Protocol	October 2021	$130 million
PolyNetwork	DeFi Bridge	August 2021	$600 million
KuCoin	Centralized Exchange	September 2020	$281 million
BitGrail	Centralized Exchange	February 2018	$170 million
Coincheck	Centralized Exchange	January 2018	$530 million
Mt. Gox	Centralized Exchange	February 2014	$480 million

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

Examples of Crypto Thefts

Name	Type of Business	Date of Attack	Amount Stolen
Mango Market	Decentralized Exchange	October 2022	$100 million
BNB Chain	DeFi Bridge	October 2022	$568 million
Wintermute	DeFi Market Maker	September 2022	$160 million
Nomad	DeFi Bridge	August 2022	$200 million
Beanstalk Farms	**DeFi Stablecoin**	**April 2022**	**$182 million**
Ronin Network	DeFi Bridge	March 2022	$625 million
Wormhole	DeFi Bridge	February 2022	$320 million
BitMart	Centralized Exchange	December 2021	$150 million
C.r.e.a.m. Finance	DeFi Lending Protocol	October 2021	$130 million
PolyNetwork	DeFi Bridge	August 2021	$600 million
KuCoin	Centralized Exchange	September 2020	$281 million
BitGrail	Centralized Exchange	February 2018	$170 million
Coincheck	Centralized Exchange	January 2018	$530 million
Mt. Gox	Centralized Exchange	February 2014	$480 million

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

Beanstalk Attack Case Study

April 16th:

- Attacker submits a malicious proposal to the Beanstalk protocol
  - Called "Donate to Ukraine" – code did send $250,000 to Ukraine
  - Code also would send all of Beanstalk's funds to Attacker

Beanstalk Attack Case Study

April 16th:

- Attacker submits a malicious proposal to the Beanstalk protocol
  - Called "Donate to Ukraine" – code did send $250,000 to Ukraine
  - Code also would send all of Beanstalk's funds to Attacker

April 17th:

- Attacker, in a single block:

Beanstalk Attack Case Study

From	Aave: aDAI Token ...	To	Beanstalk Flashlo...	For	350,000,000 ($349,782,650.00) Dai Stableco... (DAI)
From	Aave: aUSDC Tok...	To	Beanstalk Flashlo...	For	500,000,000 ($500,000,000.00) USD Coin (USDC)
From	Aave: aUSDT Tok...	To	Beanstalk Flashlo...	For	150,000,000 ($149,955,300.00) Tether USD (USDT)
From	Uniswap V2: BEAN 3	To	Beanstalk Flashlo...	For	32,100,950.626687 Bean (BEAN)
From	SushiSwap: LUSD...	To	Beanstalk Flashlo...	For	11,643,065.703498478902362927 ($12,071,466.14) LUSD Stablec... (LUSD)
From	Beanstalk Flashlo...	To	Curve.fi: DAI/USD...	For	350,000,000 ($349,782,650.00) Dai Stableco... (DAI)
From	Beanstalk Flashlo...	To	Curve.fi: DAI/USD...	For	500,000,000 ($500,000,000.00) USD Coin (USDC)
From	Beanstalk Flashlo...	To	Curve.fi: DAI/USD...	For	150,000,000 ($149,955,300.00) Tether USD (USDT)
From	Null Address: 0x00...	To	Beanstalk Flashlo...	For	979,691,328.662155074401448409 Curve.fi DAI... (3Crv)
From	Beanstalk Flashlo...	To	0xed279fdd11ca84...	For	15,000,000 Curve.fi DAI... (3Crv)
From	0xed279fdd11ca84...	To	Beanstalk Flashlo...	For	15,251,318.119203242266294685 ($15,812,482.30) LUSD Stablec... (LUSD)
From	Beanstalk Flashlo...	To	Beanstalk: BEAN3...	For	964,691,328.662155074401448409 Curve.fi DAI... (3Crv)
From	Null Address: 0x00...	To	Beanstalk Flashlo...	For	795,425,740.813818200295323741 Curve.fi Fac... (BEAN3C...)
From	Beanstalk Flashlo...	To	Beanstalk: BEANL...	For	32,100,950.626687 Bean (BEAN)
From	Beanstalk Flashlo...	To	Beanstalk: BEANL...	For	26,894,383.822701721168657777 ($27,883,948.44) LUSD Stablec... (LUSD)
From	Null Address: 0x00...	To	Beanstalk Flashlo...	For	58,924,887.872471876761750555 Curve.fi Fac... (BEANLU...)
From	Beanstalk Flashlo...	To	Beanstalk: Beanst...	For	795,425,740.813818200295323741 Curve.fi Fac... (BEAN3C...)
From	Beanstalk Flashlo...	To	Beanstalk: Beanst...	For	58,924,887.872471876761750555 Curve.fi Fac... (BEANLU...)
From	Beanstalk: Beanst...	To	Beanstalk Flashlo...	For	36,084,584.376516 Bean (BEAN)
From	Beanstalk: Beanst...	To	Beanstalk Flashlo...	For	0.540716100968756904 ($3,977,050.97) Uniswap V2 (UNI-V2)
From	Beanstalk: Beanst...	To	Beanstalk Flashlo...	For	874,663,982.237419391168556425 Curve.fi Fac... (BEAN3C...)
From	Beanstalk: Beanst...	To	Beanstalk Flashlo...	For	60,562,844.064129085666723423 Curve.fi Fac... (BEANLU...)
From	Null Address: 0x00...	To	Beanstalk Flashlo...	For	100 Bean (BEAN)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	874,663,982.237419391168556425 Curve.fi Fac... (BEAN3C...)
From	Beanstalk: BEAN3...	To	Beanstalk Flashlo...	For	1,007,734,729.918865110952432204 Curve.fi DAI... (3Crv)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	60,562,844.064129085666723423 Curve.fi Fac... (BEANLU...)
From	Beanstalk: BEANL...	To	Beanstalk Flashlo...	For	28,149,504.988150028822680438 ($29,185,251.12) LUSD Stablec... (LUSD)
From	Beanstalk Flashlo...	To	SushiSwap: LUSD...	For	11,678,100.003509005920123297 ($12,107,789.51) LUSD Stablec... (LUSD)
From	Beanstalk Flashlo...	To	Uniswap V2: BEAN 3	For	32,197,543.256457 Bean (BEAN)
From	Beanstalk Flashlo...	To	0xed279fdd11ca84...	For	16,471,404.984641022902557141 ($17,077,461.61) LUSD Stablec... (LUSD)
From	0xed279fdd11ca84...	To	Beanstalk Flashlo...	For	16,184,690.442370661651972 Curve.fi DAI... (3Crv)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	511,959,710.180617886302214702 Curve.fi DAI... (3Crv)
From	Curve.fi: DAI/USD...	To	Beanstalk Flashlo...	For	522,487,380.233548 ($522,487,380.23) USD Coin (USDC)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	358,371,797.126432520411550291 Curve.fi DAI... (3Crv)
From	Curve.fi: DAI/USD...	To	Beanstalk Flashlo...	For	365,758,059.846650868575584745 ($365,530,924.09) Dai Stableco... (DAI)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	153,587,913.054185365890664411 Curve.fi DAI... (3Crv)
From	Curve.fi: DAI/USD...	To	Beanstalk Flashlo...	For	156,732,232.49236 ($156,685,526.29) Tether USD (USDT)
From	Null Address: 0x00...	To	Aave: Aave Collec...	For	192.544598265969491594 ($193.12) Aave interes... (aDAI)
From	Beanstalk Flashlo...	To	Aave: aDAI Token ...	For	350,315,000 ($350,097,454.39) Dai Stableco... (DAI)
From	Null Address: 0x00...	To	Aave: Aave Collec...	For	30.364909 ($30.49) Aave interes... (aUSDC)
From	Beanstalk Flashlo...	To	Aave: aUSDC Tok...	For	500,450,000 ($500,450,000.00) USD Coin (USDC)
From	Null Address: 0x00...	To	Aave: Aave Collec...	For	89.259866 ($89.97) Aave interes... (aUSDT)
From	Beanstalk Flashlo...	To	Aave: aUSDT Tok...	For	150,135,000 ($150,090,259.77) Tether USD (USDT)
From	Beanstalk Flashlo...	To	Uniswap V2: BEAN 3	For	0.540716100968756904 ($3,977,050.97) Uniswap V2 (UNI-V2)
From	Uniswap V2: BEAN 3	To	Null Address: 0x00...	For	0.540716100968756904 ($3,977,050.97) Uniswap V2 (UNI-V2)
From	Uniswap V2: BEAN 3	To	Beanstalk Flashlo...	For	10,883.105341079068109889 ($17,879,853.76) Wrapped Ethe... (WETH)
From	Uniswap V2: BEAN 3	To	Beanstalk Flashlo...	For	32,511,085.804104 Bean (BEAN)
From	Beanstalk Flashlo...	To	Ukraine Crypto Do...	For	250,000 ($250,000.00) USD Coin (USDC)
From	Uniswap V3: DAI-...	To	Beanstalk Flashlo...	For	15,441,256.987216 ($15,441,256.99) USD Coin (USDC)
From	Beanstalk Flashlo...	To	Uniswap V3: DAI-...	For	15,443,059.846650868575584745 ($15,433,469.71) Dai Stableco... (DAI)
From	Uniswap V3: USD...	To	Beanstalk Flashlo...	For	11,822.158690514861161013 ($19,422,624.51) Wrapped Ethe... (WETH)
From	Beanstalk Flashlo...	To	Uniswap V3: USD...	For	37,228,637.220764 ($37,228,637.22) USD Coin (USDC)
From	Uniswap V3: USDT	To	Beanstalk Flashlo...	For	2,124.852878868396961413 ($3,490,920.79) Wrapped Ethe... (WETH)
From	Beanstalk Flashlo...	To	Uniswap V3: USDT	For	6,597,232.49236 ($6,595,266.52) Tether USD (USDT)

Source: etherscan.io

Beanstalk Attack Case Study

April 16th:

- Attacker submits a malicious proposal to the Beanstalk protocol
  - Called "Donate to Ukraine" – code did send $250,000 to Ukraine
  - Code also would send all of Beanstalk's funds to Attacker

April 17th:

- Attacker, in a single block:
  - Gets flash loans worth $1 billion.

Beanstalk Attack Case Study

From	Aave: aDAI Token ...	To	Beanstalk Flashlo...	For	350,000,000 ($349,782,650.00) Dai Stableco... (DAI)
From	Aave: aUSDC Tok...	To	Beanstalk Flashlo...	For	500,000,000 ($500,000,000.00) USD Coin (USDC)
From	Aave: aUSDT Tok...	To	Beanstalk Flashlo...	For	150,000,000 ($149,955,300.00) Tether USD (USDT)
From	Uniswap V2: BEAN 3	To	Beanstalk Flashlo...	For	32,100,950.626687 Bean (BEAN)
From	SushiSwap: LUSD...	To	Beanstalk Flashlo...	For	11,643,065.703498478902362927 ($12,071,466.14) LUSD Stablec... (LUSD)
From	Beanstalk Flashlo...	To	Curve.fi: DAI/USD...	For	350,000,000 ($349,782,650.00) Dai Stableco... (DAI)
From	Beanstalk Flashlo...	To	Curve.fi: DAI/USD...	For	500,000,000 ($500,000,000.00) USD Coin (USDC)
From	Beanstalk Flashlo...	To	Curve.fi: DAI/USD...	For	150,000,000 ($149,955,300.00) Tether USD (USDT)
From	Null Address: 0x00...	To	Beanstalk Flashlo...	For	979,691,328.662155074401448409 Curve.fi DAI... (3Crv)
From	Beanstalk Flashlo...	To	0xed279fdd11ca84...	For	15,000,000 Curve.fi DAI... (3Crv)
From	0xed279fdd11ca84...	To	Beanstalk Flashlo...	For	15,251,318.119203242266294685 ($15,812,482.30) LUSD Stablec... (LUSD)
From	Beanstalk Flashlo...	To	Beanstalk: BEAN3...	For	964,691,328.662155074401448409 Curve.fi DAI... (3Crv)
From	Null Address: 0x00...	To	Beanstalk Flashlo...	For	795,425,740.813818200295323741 Curve.fi Fac... (BEAN3C...)
From	Beanstalk Flashlo...	To	Beanstalk: BEANL...	For	32,100,950.626687 Bean (BEAN)
From	Beanstalk Flashlo...	To	Beanstalk: BEANL...	For	26,894,383.822701721168657777 ($27,883,948.44) LUSD Stablec... (LUSD)
From	Null Address: 0x00...	To	Beanstalk Flashlo...	For	58,924,887.872471876761750555 Curve.fi Fac... (BEANLU...)
From	Beanstalk Flashlo...	To	Beanstalk: Beanst...	For	795,425,740.813818200295323741 Curve.fi Fac... (BEAN3C...)
From	Beanstalk Flashlo...	To	Beanstalk: Beanst...	For	58,924,887.872471876761750555 Curve.fi Fac... (BEANLU...)
From	Beanstalk: Beanst...	To	Beanstalk Flashlo...	For	36,084,584.376516 Bean (BEAN)
From	Beanstalk: Beanst...	To	Beanstalk Flashlo...	For	0.540716100968756904 ($3,977,050.97) Uniswap V2 (UNI-V2)
From	Beanstalk: Beanst...	To	Beanstalk Flashlo...	For	874,663,982.237419391168556425 Curve.fi Fac... (BEAN3C...)
From	Beanstalk: Beanst...	To	Beanstalk Flashlo...	For	60,562,844.064129085666723423 Curve.fi Fac... (BEANLU...)
From	Null Address: 0x00...	To	Beanstalk Flashlo...	For	100 Bean (BEAN)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	874,663,982.237419391168556425 Curve.fi Fac... (BEAN3C...)
From	Beanstalk: BEAN3...	To	Beanstalk Flashlo...	For	1,007,734,729.918865110952432204 Curve.fi DAI... (3Crv)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	60,562,844.064129085666723423 Curve.fi Fac... (BEANLU...)
From	Beanstalk: BEANL...	To	Beanstalk Flashlo...	For	28,149,504.988150028822680438 ($29,185,251.12) LUSD Stablec... (LUSD)

From	Beanstalk Flashlo...	To	SushiSwap: LUSD...	For	11,678,100.003509005920123297 ($12,107,789.51) LUSD Stablec... (LUSD)
From	Beanstalk Flashlo...	To	Uniswap V2: BEAN 3	For	32,197,543.256457 Bean (BEAN)
From	Beanstalk Flashlo...	To	0xed279fdd11ca84...	For	16,471,404.984641022902557141 ($17,077,461.61) LUSD Stablec... (LUSD)
From	0xed279fdd11ca84...	To	Beanstalk Flashlo...	For	16,184,690.442370661651972 Curve.fi DAI... (3Crv)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	511,959,710.180617886302214702 Curve.fi DAI... (3Crv)
From	Curve.fi: DAI/USD...	To	Beanstalk Flashlo...	For	522,487,380.233548 ($522,487,380.23) USD Coin (USDC)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	358,371,797.126432520411550291 Curve.fi DAI... (3Crv)
From	Curve.fi: DAI/USD...	To	Beanstalk Flashlo...	For	365,758,059.846650868575584745 ($365,530,924.09) Dai Stableco... (DAI)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	153,587,913.054185365890664411 Curve.fi DAI... (3Crv)
From	Curve.fi: DAI/USD...	To	Beanstalk Flashlo...	For	156,732,232.49236 ($156,685,526.29) Tether USD (USDT)
From	Null Address: 0x00...	To	Aave: Aave Collec...	For	192.544598265969491594 ($193.12) Aave interes... (aDAI)
From	Beanstalk Flashlo...	To	Aave: aDAI Token ...	For	350,315,000 ($350,097,454.39) Dai Stableco... (DAI)
From	Null Address: 0x00...	To	Aave: Aave Collec...	For	30.364909 ($30.49) Aave interes... (aUSDC)
From	Beanstalk Flashlo...	To	Aave: aUSDC Tok...	For	500,450,000 ($500,450,000.00) USD Coin (USDC)
From	Null Address: 0x00...	To	Aave: Aave Collec...	For	89.259866 ($89.97) Aave interes... (aUSDT)
From	Beanstalk Flashlo...	To	Aave: aUSDT Tok...	For	150,135,000 ($150,090,259.77) Tether USD (USDT)
From	Beanstalk Flashlo...	To	Uniswap V2: BEAN 3	For	0.540716100968756904 ($3,977,050.97) Uniswap V2 (UNI-V2)
From	Uniswap V2: BEAN 3	To	Null Address: 0x00...	For	0.540716100968756904 ($3,977,050.97) Uniswap V2 (UNI-V2)
From	Uniswap V2: BEAN 3	To	Beanstalk Flashlo...	For	10,883.105341079068109889 ($17,879,853.76) Wrapped Ethe... (WETH)
From	Uniswap V2: BEAN 3	To	Beanstalk Flashlo...	For	32,511,085.804104 Bean (BEAN)
From	Beanstalk Flashlo...	To	Ukraine Crypto Do...	For	250,000 ($250,000.00) USD Coin (USDC)
From	Uniswap V3: DAI-...	To	Beanstalk Flashlo...	For	15,441,256.987216 ($15,441,256.99) USD Coin (USDC)
From	Beanstalk Flashlo...	To	Uniswap V3: DAI-...	For	15,443,059.846650868575584745 ($15,433,469.71) Dai Stableco... (DAI)
From	Uniswap V3: USD...	To	Beanstalk Flashlo...	For	11,822.158690514861161013 ($19,422,624.51) Wrapped Ethe... (WETH)
From	Beanstalk Flashlo...	To	Uniswap V3: USD...	For	37,228,637.220764 ($37,228,637.22) USD Coin (USDC)
From	Uniswap V3: USDT	To	Beanstalk Flashlo...	For	2,124.852878868396961413 ($3,490,920.79) Wrapped Ethe... (WETH)
From	Beanstalk Flashlo...	To	Uniswap V3: USDT	For	6,597,232.49236 ($6,595,266.52) Tether USD (USDT)

Source: etherscan.io

Gets flash loans worth $1 billion

Beanstalk Attack Case Study

April 16th:

- Attacker submits a malicious proposal to the Beanstalk protocol
  - Called "Donate to Ukraine" – code did send $250,000 to Ukraine
  - Code also would send all of Beanstalk's funds to Attacker

April 17th:

- Attacker, in a single block:
  - Gets flash loans worth $1 billion.
  - Buys enough governance tokens to gain $>67\%$ voting power.

Beanstalk Attack Case Study

From	Aave: aDAI Token ...	To	Beanstalk Flashlo...	For	350,000,000 ($349,782,650.00) Dai Stableco... (DAI)
From	Aave: aUSDC Tok...	To	Beanstalk Flashlo...	For	500,000,000 ($500,000,000.00) USD Coin (USDC)
From	Aave: aUSDT Tok...	To	Beanstalk Flashlo...	For	150,000,000 ($149,955,300.00) Tether USD (USDT)
From	Uniswap V2: BEAN 3	To	Beanstalk Flashlo...	For	32,100,950.626687 Bean (BEAN)
From	SushiSwap: LUSD...	To	Beanstalk Flashlo...	For	11,643,065.703498478902362927 ($12,071,466.14) LUSD Stablec... (LUSD)
From	Beanstalk Flashlo...	To	Curve.fi: DAI/USD...	For	350,000,000 ($349,782,650.00) Dai Stableco... (DAI)
From	Beanstalk Flashlo...	To	Curve.fi: DAI/USD...	For	500,000,000 ($500,000,000.00) USD Coin (USDC)
From	Beanstalk Flashlo...	To	Curve.fi: DAI/USD...	For	150,000,000 ($149,955,300.00) Tether USD (USDT)
From	Null Address: 0x00...	To	Beanstalk Flashlo...	For	979,691,328.662155074401448409 Curve.fi DAI... (3Crv)
From	SushiSwap: LUSD...	To	Beanstalk Flashlo...	For	11,643,065.703498478902362927 ($12,071,466.14) LUSD Stablec... (LUSD)
From	Beanstalk Flashlo...	To	Curve.fi: DAI/USD...	For	350,000,000 ($349,782,650.00) Dai Stableco... (DAI)
From	Beanstalk Flashlo...	To	Curve.fi: DAI/USD...	For	500,000,000 ($500,000,000.00) USD Coin (USDC)
From	Beanstalk Flashlo...	To	Curve.fi: DAI/USD...	For	150,000,000 ($149,955,300.00) Tether USD (USDT)
From	Null Address: 0x00...	To	Beanstalk Flashlo...	For	979,691,328.662155074401448409 Curve.fi DAI... (3Crv)
From	Null Address: 0x00...	To	0xed279fdd11ca84...	For	15,000,000 Curve.fi DAI... (3Crv)
From	0xed279fdd11ca84...	To	Beanstalk Flashlo...	For	15,251,318.119203242266294685 ($15,812,482.30) LUSD Stablec... (LUSD)
From	Beanstalk Flashlo...	To	Beanstalk: BEAN3...	For	964,691,328.662155074401448409 Curve.fi DAI... (3Crv)
From	Null Address: 0x00...	To	Beanstalk Flashlo...	For	795,425,740.813818200295323741 Curve.fi Fac... (BEAN3C...)
From	Beanstalk Flashlo...	To	Beanstalk: BEANL...	For	32,100,950.626687 Bean (BEAN)
From	Beanstalk Flashlo...	To	Beanstalk: BEANL...	For	26,894,383.822701721168657777 ($27,883,948.44) LUSD Stablec... (LUSD)
From	Null Address: 0x00...	To	Beanstalk Flashlo...	For	58,924,887.872471876761750555 Curve.fi Fac... (BEANLU...)
From	Beanstalk Flashlo...	To	Beanstalk: Beanst...	For	795,425,740.813818200295323741 Curve.fi Fac... (BEAN3C...)
From	Beanstalk Flashlo...	To	Beanstalk: Beanst...	For	58,924,887.872471876761750555 Curve.fi Fac... (BEANLU...)
From	Beanstalk: Beanst...	To	Beanstalk Flashlo...	For	36,084,584.376516 Bean (BEAN)
From	Beanstalk: Beanst...	To	Beanstalk Flashlo...	For	0.540716100968756904 ($3,977,050.97) Uniswap V2 (UNI-V2)
From	Beanstalk: Beanst...	To	Beanstalk Flashlo...	For	874,663,982.237419391168556425 Curve.fi Fac... (BEAN3C...)
From	Beanstalk: Beanst...	To	Beanstalk Flashlo...	For	60,562,844.064129085666723423 Curve.fi Fac... (BEANLU...)
From	Null Address: 0x00...	To	Beanstalk Flashlo...	For	100 Bean (BEAN)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	874,663,982.237419391168556425 Curve.fi Fac... (BEAN3C...)
From	Beanstalk: BEAN3...	To	Beanstalk Flashlo...	For	1,007,734,729.918865110952432204 Curve.fi DAI... (3Crv)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	60,562,844.064129085666723423 Curve.fi Fac... (BEANLU...)
From	Beanstalk: BEANL...	To	Beanstalk Flashlo...	For	28,149,504.988150028822680438 ($29,185,251.12) LUSD Stablec... (LUSD)

From	Beanstalk Flashlo...	To	SushiSwap: LUSD...	For	11,678,100.003509005920123297 ($12,107,789.51) LUSD Stablec... (LUSD)
From	Beanstalk Flashlo...	To	Uniswap V2: BEAN 3	For	32,197,543.256457 Bean (BEAN)
From	Beanstalk Flashlo...	To	0xed279fdd11ca84...	For	16,471,404.984641022902557141 ($17,077,461.61) LUSD Stablec... (LUSD)
From	0xed279fdd11ca84...	To	Beanstalk Flashlo...	For	16,184,690.442370661651972 Curve.fi DAI... (3Crv)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	511,959,710.180617886302214702 Curve.fi DAI... (3Crv)
From	Curve.fi: DAI/USD...	To	Beanstalk Flashlo...	For	522,487,380.233548 ($522,487,380.23) USD Coin (USDC)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	358,371,797.126432520411550291 Curve.fi DAI... (3Crv)
From	Curve.fi: DAI/USD...	To	Beanstalk Flashlo...	For	365,758,059.846650868575584745 ($365,530,924.09) Dai Stableco... (DAI)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	153,587,913.054185365890664411 Curve.fi DAI... (3Crv)
From	Curve.fi: DAI/USD...	To	Beanstalk Flashlo...	For	156,732,232.49236 ($156,685,526.29) Tether USD (USDT)
From	Null Address: 0x00...	To	Aave: Aave Collec...	For	192.544598265969491594 ($193.12) Aave interes... (aDAI)
From	Beanstalk Flashlo...	To	Aave: aDAI Token ...	For	350,315,000 ($350,097,454.39) Dai Stableco... (DAI)
From	Null Address: 0x00...	To	Aave: Aave Collec...	For	30.364909 ($30.49) Aave interes... (aUSDC)
From	Beanstalk Flashlo...	To	Aave: aUSDC Tok...	For	500,450,000 ($500,450,000.00) USD Coin (USDC)
From	Null Address: 0x00...	To	Aave: Aave Collec...	For	89.259866 ($89.97) Aave interes... (aUSDT)
From	Beanstalk Flashlo...	To	Aave: aUSDT Tok...	For	150,135,000 ($150,090,259.77) Tether USD (USDT)
From	Beanstalk Flashlo...	To	Uniswap V2: BEAN 3	For	0.540716100968756904 ($3,977,050.97) Uniswap V2 (UNI-V2)
From	Uniswap V2: BEAN 3	To	Null Address: 0x00...	For	0.540716100968756904 ($3,977,050.97) Uniswap V2 (UNI-V2)
From	Uniswap V2: BEAN 3	To	Beanstalk Flashlo...	For	10,883.105341079068109889 ($17,879,853.76) Wrapped Ethe... (WETH)
From	Uniswap V2: BEAN 3	To	Beanstalk Flashlo...	For	32,511,085.804104 Bean (BEAN)
From	Beanstalk Flashlo...	To	Ukraine Crypto Do...	For	250,000 ($250,000.00) USD Coin (USDC)
From	Uniswap V3: DAI-...	To	Beanstalk Flashlo...	For	15,441,256.987216 ($15,441,256.99) USD Coin (USDC)
From	Beanstalk Flashlo...	To	Uniswap V3: DAI-...	For	15,443,059.846650868575584745 ($15,433,469.71) Dai Stableco... (DAI)
From	Uniswap V3: USD...	To	Beanstalk Flashlo...	For	11,822.158690514861161013 ($19,422,624.51) Wrapped Ethe... (WETH)
From	Beanstalk Flashlo...	To	Uniswap V3: USD...	For	37,228,637.220764 ($37,228,637.22) USD Coin (USDC)
From	Uniswap V3: USDT	To	Beanstalk Flashlo...	For	2,124.852878868396961413 ($3,490,920.79) Wrapped Ethe... (WETH)
From	Beanstalk Flashlo...	To	Uniswap V3: USDT	For	6,597,232.49236 ($6,595,266.52) Tether USD (USDT)

Source: etherscan.io

Buys enough governance tokens for >67%

Beanstalk Attack Case Study

April 16th:

- Attacker submits a malicious proposal to the Beanstalk protocol
  - Called "Donate to Ukraine" – code did send $250,000 to Ukraine
  - Code also would send all of Beanstalk's funds to Attacker

April 17th:

- Attacker, in a single block:
  - Gets flash loans worth $1 billion.
  - Buys enough governance tokens to gain $>67\%$ voting power.
  - Votes the malicious proposal in and transfers all of Beanstalk's assets to their wallet. These assets were worth $182 million just before the attack.

Beanstalk Attack Case Study

Source: etherscan.io

Votes in proposal and empties Beanstalk's assets

Beanstalk Attack Case Study

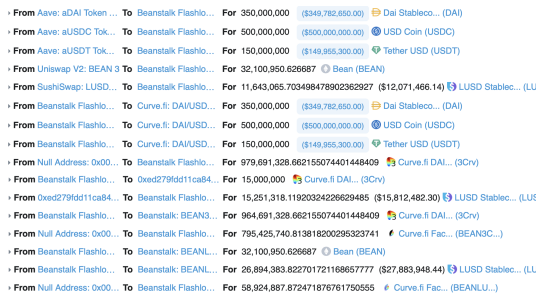
April 16th:

- Attacker submits a malicious proposal to the Beanstalk protocol
  - Called "Donate to Ukraine" – code did send $250,000 to Ukraine
  - Code also would send all of Beanstalk's funds to Attacker

April 17th:

- Attacker, in a single block:
  - Gets flash loans worth $1 billion.
  - Buys enough governance tokens to gain $>67\%$ voting power.
  - Votes the malicious proposal in and transfers all of Beanstalk's assets to their wallet. These assets were worth $182 million just before the attack.
  - Repays flash loans,

Beanstalk Attack Case Study



Source: etherscan.io

Repays flash loans

Beanstalk Attack Case Study

April 16th:

- Attacker submits a malicious proposal to the Beanstalk protocol
  - Called "Donate to Ukraine" – code did send $250,000 to Ukraine
  - Code also would send all of Beanstalk's funds to Attacker

April 17th:

- Attacker, in a single block:
  - Gets flash loans worth $1 billion.
  - Buys enough governance tokens to gain $>67\%$ voting power.
  - Votes the malicious proposal in and transfers all of Beanstalk's assets to their wallet. These assets were worth $182 million just before the attack.
  - Repays flash loans, sends $250,000 to Ukraine,

Beanstalk Attack Case Study

From	Aave: aDAI Token ...	To	Beanstalk Flashlo...	For	350,000,000 ($349,782,650.00) Dai Stableco... (DAI)
From	Aave: aUSDC Tok...	To	Beanstalk Flashlo...	For	500,000,000 ($500,000,000.00) USD Coin (USDC)
From	Aave: aUSDT Tok...	To	Beanstalk Flashlo...	For	150,000,000 ($149,955,300.00) Tether USD (USDT)
From	Uniswap V2: BEAN 3	To	Beanstalk Flashlo...	For	32,100,950.626687 Bean (BEAN)
From	SushiSwap: LUSD...	To	Beanstalk Flashlo...	For	11,643,065.703498478902362927 ($12,071,466.14) LUSD Stablec... (LUSD)
From	Beanstalk Flashlo...	To	Curve.fi: DAI/USD...	For	350,000,000 ($349,782,650.00) Dai Stableco... (DAI)
From	Beanstalk Flashlo...	To	Curve.fi: DAI/USD...	For	500,000,000 ($500,000,000.00) USD Coin (USDC)
From	Beanstalk Flashlo...	To	Curve.fi: DAI/USD...	For	150,000,000 ($149,955,300.00) Tether USD (USDT)
From	Null Address: 0x00...	To	Beanstalk Flashlo...	For	979,691,328.662155074401448409 Curve.fi DAI... (3Crv)
From	Beanstalk Flashlo...	To	0xed279fdd11ca84...	For	15,000,000 Curve.fi DAI... (3Crv)
From	0xed279fdd11ca84...	To	Beanstalk Flashlo...	For	15,251,318.119203242266294685 ($15,812,482.30) LUSD Stablec... (LUSD)
From	Beanstalk Flashlo...	To	Beanstalk: BEAN3...	For	964,691,328.662155074401448409 Curve.fi DAI... (3Crv)
From	Null Address: 0x00...	To	Beanstalk Flashlo...	For	795,425,740.813818200295323741 Curve.fi Fac... (BEAN3C...)
From	Beanstalk Flashlo...	To	Beanstalk: BEANL...	For	32,100,950.626687 Bean (BEAN)
From	Beanstalk Flashlo...	To	Beanstalk: BEANL...	For	26,894,383.822701721168657777 ($27,883,948.44) LUSD Stablec... (LUSD)
From	Null Address: 0x00...	To	Beanstalk Flashlo...	For	58,924,887.872471876761750555 Curve.fi Fac... (BEANLU...)
From	Beanstalk Flashlo...	To	Beanstalk: Beanst...	For	795,425,740.813818200295323741 Curve.fi Fac... (BEAN3C...)
From	Beanstalk Flashlo...	To	Beanstalk: Beanst...	For	58,924,887.872471876761750555 Curve.fi Fac... (BEANLU...)
From	Beanstalk: Beanst...	To	Beanstalk Flashlo...	For	36,084,584.376516 Bean (BEAN)
From	Beanstalk: Beanst...	To	Beanstalk Flashlo...	For	0.540716100968756904 ($3,977,050.97) Uniswap V2 (UNI-V2)
From	Beanstalk: Beanst...	To	Beanstalk Flashlo...	For	874,663,982.237419391168556425 Curve.fi Fac... (BEAN3C...)
From	Beanstalk: Beanst...	To	Beanstalk Flashlo...	For	60,562,844.064129085666723423 Curve.fi Fac... (BEANLU...)
From	Null Address: 0x00...	To	Beanstalk Flashlo...	For	100 Bean (BEAN)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	874,663,982.237419391168556425 Curve.fi Fac... (BEAN3C...)
From	Beanstalk: BEAN3...	To	Beanstalk Flashlo...	For	1,007,734,729.918865110952432204 Curve.fi DAI... (3Crv)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	60,562,844.064129085666723423 Curve.fi Fac... (BEANLU...)
From	Beanstalk: BEANL...	To	Beanstalk Flashlo...	For	28,149,504.988150028822680438 ($29,185,251.12) LUSD Stablec... (LUSD)

From	Beanstalk Flashlo...	To	SushiSwap: LUSD...	For	11,678,100.003509005920123297 ($12,107,789.51) LUSD Stablec... (LUSD)
From	Beanstalk Flashlo...	To	Uniswap V2: BEAN 3	For	32,197,543.256457 Bean (BEAN)
From	Beanstalk Flashlo...	To	0xed279fdd11ca84...	For	16,471,404.984641022902557141 ($17,077,461.61) LUSD Stablec... (LUSD)
From	0xed279fdd11ca84...	To	Beanstalk Flashlo...	For	16,184,690.442370661651972 Curve.fi DAI... (3Crv)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	511,959,710.180617886302214702 Curve.fi DAI... (3Crv)
From	Curve.fi: DAI/USD...	To	Beanstalk Flashlo...	For	522,487,380.233548 ($522,487,380.23) USD Coin (USDC)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	358,371,797.126432520411550291 Curve.fi DAI... (3Crv)
From	Curve.fi: DAI/USD...	To	Beanstalk Flashlo...	For	365,758,059.846650868575584745 ($365,530,924.09) Dai Stableco... (DAI)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	153,587,913.054185365890664411 Curve.fi DAI... (3Crv)
From	Curve.fi: DAI/USD...	To	Beanstalk Flashlo...	For	156,732,232.49236 ($156,685,526.29) Tether USD (USDT)
From	Null Address: 0x00...	To	Aave: Aave Collec...	For	192.544598265969491594 ($193.12) Aave interes... (aDAI)
From	Beanstalk Flashlo...	To	Aave: aDAI Token ...	For	350,315,000 ($350,097,454.39) Dai Stableco... (DAI)
From	Null Address: 0x00...	To	Aave: Aave Collec...	For	30.364909 ($30.49) Aave interes... (aUSDC)
From	Beanstalk Flashlo...	To	Aave: aUSDC Tok...	For	500,450,000 ($500,450,000.00) USD Coin (USDC)
From	Null Address: 0x00...	To	Aave: Aave Collec...	For	89.259866 ($89.97) Aave interes... (aUSDT)
From	Beanstalk Flashlo...	To	Aave: aUSDT Tok...	For	150,135,000 ($150,090,259.77) Tether USD (USDT)
From	Beanstalk Flashlo...	To	Uniswap V2: BEAN 3	For	0.540716100968756904 ($3,977,050.97) Uniswap V2 (UNI-V2)
From	Uniswap V2: BEAN 3	To	Null Address: 0x00...	For	0.540716100968756904 ($3,977,050.97) Uniswap V2 (UNI-V2)
From	Uniswap V2: BEAN 3	To	Beanstalk Flashlo...	For	10,883.105341079068109889 ($17,879,853.76) Wrapped Ethe... (WETH)
From	Uniswap V2: BEAN 3	To	Beanstalk Flashlo...	For	32,511,085.804104 Bean (BEAN)
From	Beanstalk Flashlo...	To	Ukraine Crypto Do...	For	250,000 ($250,000.00) USD Coin (USDC)
From	Uniswap V3: DAI-...	To	Beanstalk Flashlo...	For	15,441,256.987216 ($15,441,256.99) USD Coin (USDC)
From	Beanstalk Flashlo...	To	Uniswap V3: DAI-...	For	15,443,059.846650868575584745 ($15,433,469.71) Dai Stableco... (DAI)
From	Uniswap V3: USD...	To	Beanstalk Flashlo...	For	11,822.158690514861161013 ($19,422,624.51) Wrapped Ethe... (WETH)
From	Beanstalk Flashlo...	To	Uniswap V3: USD...	For	37,228,637.220764 ($37,228,637.22) USD Coin (USDC)
From	Uniswap V3: USDT	To	Beanstalk Flashlo...	For	2,124.852878868396961413 ($3,490,920.79) Wrapped Ethe... (WETH)
From	Beanstalk Flashlo...	To	Uniswap V3: USDT	For	6,597,232.49236 ($6,595,266.52) Tether USD (USDT)

Source: etherscan.io

Sends $250,000 to Ukraine (as promised!)

Beanstalk Attack Case Study

April 16th:

- Attacker submits a malicious proposal to the Beanstalk protocol
  - Called "Donate to Ukraine" – code did send $250,000 to Ukraine
  - Code also would send all of Beanstalk's funds to Attacker

April 17th:

- Attacker, in a single block:
  - Gets flash loans worth $1 billion.
  - Buys enough governance tokens to gain $>67\%$ voting power.
  - Votes the malicious proposal in and transfers all of Beanstalk's assets to their wallet. These assets were worth $182 million just before the attack.
  - Repays flash loans, sends $250,000 to Ukraine, and cashes out $\sim$25,000 ETH worth $\sim$$75 million at the time.

Beanstalk Attack Case Study

From	Aave: aDAI Token ...	To	Beanstalk Flashlo...	For	350,000,000 ($349,782,650.00) Dai Stableco... (DAI)
From	Aave: aUSDC Tok...	To	Beanstalk Flashlo...	For	500,000,000 ($500,000,000.00) USD Coin (USDC)
From	Aave: aUSDT Tok...	To	Beanstalk Flashlo...	For	150,000,000 ($149,955,300.00) Tether USD (USDT)
From	Uniswap V2: BEAN 3	To	Beanstalk Flashlo...	For	32,100,950.626687 Bean (BEAN)
From	SushiSwap: LUSD...	To	Beanstalk Flashlo...	For	11,643,065.703498478902362927 ($12,071,466.14) LUSD Stablec... (LUSD)
From	Beanstalk Flashlo...	To	Curve.fi: DAI/USD...	For	350,000,000 ($349,782,650.00) Dai Stableco... (DAI)
From	Beanstalk Flashlo...	To	Curve.fi: DAI/USD...	For	500,000,000 ($500,000,000.00) USD Coin (USDC)
From	Beanstalk Flashlo...	To	Curve.fi: DAI/USD...	For	150,000,000 ($149,955,300.00) Tether USD (USDT)
From	Null Address: 0x00...	To	Beanstalk Flashlo...	For	979,691,328.662155074401448409 Curve.fi DAI... (3Crv)
From	Beanstalk Flashlo...	To	0xed279fdd11ca84...	For	15,000,000 Curve.fi DAI... (3Crv)
From	0xed279fdd11ca84...	To	Beanstalk Flashlo...	For	15,251,318.119203242266294685 ($15,812,482.30) LUSD Stablec... (LUSD)
From	Beanstalk Flashlo...	To	Beanstalk: BEAN3...	For	964,691,328.662155074401448409 Curve.fi DAI... (3Crv)
From	Null Address: 0x00...	To	Beanstalk Flashlo...	For	795,425,740.813818200295323741 Curve.fi Fac... (BEAN3C...)
From	Beanstalk Flashlo...	To	Beanstalk: BEANL...	For	32,100,950.626687 Bean (BEAN)
From	Beanstalk Flashlo...	To	Beanstalk: BEANL...	For	26,894,383.822701721168657777 ($27,883,948.44) LUSD Stablec... (LUSD)
From	Null Address: 0x00...	To	Beanstalk Flashlo...	For	58,924,887.872471876761750555 Curve.fi Fac... (BEANLU...)
From	Beanstalk Flashlo...	To	Beanstalk: Beanst...	For	795,425,740.813818200295323741 Curve.fi Fac... (BEAN3C...)
From	Beanstalk Flashlo...	To	Beanstalk: Beanst...	For	58,924,887.872471876761750555 Curve.fi Fac... (BEANLU...)
From	Beanstalk: Beanst...	To	Beanstalk Flashlo...	For	36,084,584.376516 Bean (BEAN)
From	Beanstalk: Beanst...	To	Beanstalk Flashlo...	For	0.540716100968756904 ($3,977,050.97) Uniswap V2 (UNI-V2)
From	Beanstalk: Beanst...	To	Beanstalk Flashlo...	For	874,663,982.237419391168556425 Curve.fi Fac... (BEAN3C...)
From	Beanstalk: Beanst...	To	Beanstalk Flashlo...	For	60,562,844.064129085666723423 Curve.fi Fac... (BEANLU...)
From	Null Address: 0x00...	To	Beanstalk Flashlo...	For	100 Bean (BEAN)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	874,663,982.237419391168556425 Curve.fi Fac... (BEAN3C...)
From	Beanstalk: BEAN3...	To	Beanstalk Flashlo...	For	1,007,734,729.918865110952432204 Curve.fi DAI... (3Crv)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	60,562,844.064129085666723423 Curve.fi Fac... (BEANLU...)
From	Beanstalk: BEANL...	To	Beanstalk Flashlo...	For	28,149,504.988150028822680438 ($29,185,251.12) LUSD Stablec... (LUSD)
From	Beanstalk Flashlo...	To	SushiSwap: LUSD...	For	11,678,100.003509005920123297 ($12,107,789.51) LUSD Stablec... (LUSD)
From	Beanstalk Flashlo...	To	Uniswap V2: BEAN 3	For	32,197,543.256457 Bean (BEAN)
From	Beanstalk Flashlo...	To	0xed279fdd11ca84...	For	16,471,404.984641022902557141 ($17,077,461.61) LUSD Stablec... (LUSD)
From	0xed279fdd11ca84...	To	Beanstalk Flashlo...	For	16,184,690.442370661651972 Curve.fi DAI... (3Crv)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	511,959,710.180617886302214702 Curve.fi DAI... (3Crv)
From	Curve.fi: DAI/USD...	To	Beanstalk Flashlo...	For	522,487,380.233548 ($522,487,380.23) USD Coin (USDC)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	358,371,797.126432520411550291 Curve.fi DAI... (3Crv)
From	Curve.fi: DAI/USD...	To	Beanstalk Flashlo...	For	365,758,059.846650868575584745 ($365,530,924.09) Dai Stableco... (DAI)
From	Beanstalk Flashlo...	To	Null Address: 0x00...	For	153,587,913.054185365890664411 Curve.fi DAI... (3Crv)
From	Curve.fi: DAI/USD...	To	Beanstalk Flashlo...	For	156,732,232.49236 ($156,685,526.29) Tether USD (USDT)
From	Null Address: 0x00...	To	Aave: Aave Collec...	For	192.544598265969491594 ($193.12) Aave interes... (aDAI)
From	Beanstalk Flashlo...	To	Aave: aDAI Token ...	For	350,315,000 ($350,097,454.39) Dai Stableco... (DAI)
From	Null Address: 0x00...	To	Aave: Aave Collec...	For	30.364909 ($30.49) Aave interes... (aUSDC)
From	Beanstalk Flashlo...	To	Aave: aUSDC Tok...	For	500,450,000 ($500,450,000.00) USD Coin (USDC)
From	Null Address: 0x00...	To	Aave: Aave Collec...	For	89.259866 ($89.97) Aave interes... (aUSDT)
From	Beanstalk Flashlo...	To	Aave: aUSDT Tok...	For	150,135,000 ($150,090,259.77) Tether USD (USDT)
From	Beanstalk Flashlo...	To	Uniswap V2: BEAN 3	For	0.540716100968756904 ($3,977,050.97) Uniswap V2 (UNI-V2)
From	Uniswap V2: BEAN 3	To	Null Address: 0x00...	For	0.540716100968756904 ($3,977,050.97) Uniswap V2 (UNI-V2)
From	Uniswap V2: BEAN 3	To	Beanstalk Flashlo...	For	10,883.105341079068109889 ($17,879,853.76) Wrapped Ethe... (WETH)
From	Uniswap V2: BEAN 3	To	Beanstalk Flashlo...	For	32,511,085.804104 Bean (BEAN)
From	Beanstalk Flashlo...	To	Ukraine Crypto Do...	For	250,000 ($250,000.00) USD Coin (USDC)
From	Uniswap V3: DAI-...	To	Beanstalk Flashlo...	For	15,441,256.987216 ($15,441,256.99) USD Coin (USDC)
From	Beanstalk Flashlo...	To	Uniswap V3: DAI-...	For	15,443,059.846650868575584745 ($15,433,469.71) Dai Stableco... (DAI)
From	Uniswap V3: USD...	To	Beanstalk Flashlo...	For	11,822.158690514861161013 ($19,422,624.51) Wrapped Ethe... (WETH)
From	Beanstalk Flashlo...	To	Uniswap V3: USD...	For	37,228,637.220764 ($37,228,637.22) USD Coin (USDC)
From	Uniswap V3: USDT	To	Beanstalk Flashlo...	For	2,124.852878868396961413 ($3,490,920.79) Wrapped Ethe... (WETH)
From	Beanstalk Flashlo...	To	Uniswap V3: USDT	For	6,597,232.49236 ($6,595,266.52) Tether USD (USDT)

Source: etherscan.io

Cashes out ~25,000 ETH worth ~$75 million at the time

Beanstalk Attack Case Study

April 16th:

- Attacker submits a malicious proposal to the Beanstalk protocol
  - Called "Donate to Ukraine" – code did send $250,000 to Ukraine
  - Code also would send all of Beanstalk's funds to Attacker

April 17th:

- Attacker, in a single block:
  - Gets flash loans worth $1 billion.
  - Buys enough governance tokens to gain >67% voting power.
  - Votes the malicious proposal in and transfers all of Beanstalk's assets to their wallet. These assets were worth $182 million just before the attack.
  - Repays flash loans, sends $250,000 to Ukraine, and cashes out ∼25,000 ETH worth ∼$75 million at the time.
- Cost of Attack:
  - Capital deposit to propose malicious code: 212,858 Beanstalk governance tokens, worth about $200,000 pre-attack.
  - Other transactions costs within the attack include flash loan interest and price-impact costs of converting large amounts of Beanstalk assets to other currencies.

Examples of Crypto Collapses

Name	Type of Business	Date of Collapse	Loss Amount
Three Arrows Capital	Hedge Fund	July 2022	$3 billion
Voyager	Lending Firm	July 2022	$1 billion - $10 billion
Celsius	Lending Firm	July 2022	$4.7 billion
Luna + Terra	Blockchain + Stablecoin	March 2022	$45 billion
Coincheck	Centralized Exchange	January 2018	$530 million
Mt. Gox	Centralized Exchange	February 2014	$480 million

Sources: Bloomberg, WSJ, Coinmarketcap.

Examples of Crypto Collapses

Name	Type of Business	Date of Collapse	Loss Amount
Three Arrows Capital	Hedge Fund	July 2022	$3 billion
Voyager	Lending Firm	July 2022	$1 billion - $10 billion
Celsius	**Lending Firm**	**July 2022**	**$4.7 billion**
Luna + Terra	Blockchain + Stablecoin	March 2022	$45 billion
Coincheck	Centralized Exchange	January 2018	$530 million
Mt. Gox	Centralized Exchange	February 2014	$480 million

Sources: Bloomberg, WSJ, Coinmarketcap.

Celsius Collapse

Summary Balance Sheet | Pictured below is the Balance Sheet for Celsius as of August 13, 2021

Celsius - Operating Balance Sheet

As of August 13, 2021

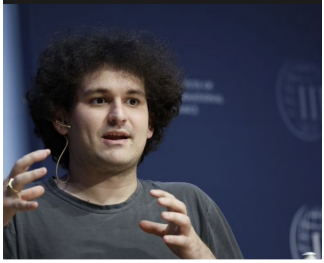
	Assets	Amount ($M)
1	DeFi	$4,483.7
2	Staking	689.6
3	Bank Balances	40.7
4	Undeployed Assets	3,276.2
5	Posted Collateral	2,232.3
6	Institutional Loans	2,241.6
7	CEL Treasury	1,752.6
8	Exchange Balances	2,390.0
9	Mining / Financial Instruments / Other	1,383.6
10	Retail Loans	542.8
11	Undeployable (Prime Trust)	35.9
	Total Assets	**$19,069.0**

	Liabilities & Shareholders' Equity	Amount ($M)
A	Depositor Balances	$12,890.4
B	Depositor Collateral	2,119.7
C	Credit Facility	1,110.4
D	Institutional Collateral	975.8
E	DeFi	785.9
F	Locked CEL	173.6
	Total Liabilities	**$18,055.9**
G	Net Asset Value	$1,013.1
	Total Liabilities and Equity	**$19,069.0**

Source: WSJ, Celsius Investment Memo (September 2021)

FTX Near-Collapse and Rescue (Yesterday!)

Bloomberg



Binance Buys FTX After Bankman-Fried Faces Liquidity Crunch

- Crypto exchange giants joint force after spat between founders
- Token prices tumble amid concern over deal closing, terms

33 mins ago · 4 min read

MARKET OPEN US Stocks Fall as Crypto Upends Risk Sentiment: Markets Wrap

DOW JONES	S&P 500	NASDAQ	N
33.08K	3,795.29	10.56K	8
▲ +0.77%	▼ -0.30%	▼ -0.05%	▼
2:48 PM	2:35 PM	2:51 PM	2-

SBF ✓
@SBF_FTX

1) Hey all: I have a few announcements to make.

Things have come full circle, and FTX.com's first, and last, investors are the same: we have come to an agreement on a strategic transaction with Binance for FTX.com (pending DD etc.).

ftx.com
FTX
Cryptocurrency Derivatives Exchange

10:03 AM · Nov 8, 2022 · Twitter Web App

7,250 Retweets **4,484** Quote Tweets **22.3K** Likes

CZ 🔶 Binance ✓
@cz_binance

This afternoon, FTX asked for our help. There is a significant liquidity crunch. To protect users, we signed a non-binding LOI, intending to fully acquire FTX.com and help cover the liquidity crunch. We will be conducting a full DD in the coming days.

ftx.com
FTX
Cryptocurrency Derivatives Exchange

10:09 AM · Nov 8, 2022 · Twitter Web App

18.9K Retweets **11.7K** Quote Tweets **65K** Likes

Overview of the Talk

A General Introduction:

- What is Nakamoto Blockchain?

The Economic Limits of Bitcoin and Anonymous, Decentralized Trust:

- Nakamoto Blockchain: A Critique in 3 Equations
  - Flow vs. Stock Problem
  - Zero Net Attack Cost Theorem
- Analysis of Double Spending Attacks
- A Way Out: Specialized Capital + Risk of Collapse
  - A Softer Constraint: Stock vs. Stock. Collapse Scenarios.

Open Questions for Future Research:

- **Q1: Permissionless trust beyond Nakamoto**
- **Q2: Economics of permissioned blockchains**
- **Many other open q's related to theory, finance, policy**

Theory Open Question, I

- Open question: is there a different blockchain design that solves the problem raised by my paper?
- Slightly more precisely: *is there a permissionless blockchain protocol that makes all attacks "expensive" (defined below) without reliance on a collapse argument?*

Theory Open Question, I

- Open question: is there a different blockchain design that solves the problem raised by my paper?
- Slightly more precisely: *is there a permissionless blockchain protocol that makes all attacks "expensive" (defined below) without reliance on a collapse argument?*
- We can put some structure to this open question as follows.
- Step 1: Use variation of my model and characterization theorems in Leshno and Strack (2020) and Chen, Papadimitriou and Roughgarden (2019) to obtain a general version of $N^* c = p$

Theory Open Question, I

- Assume
  - Block validation requires capital (ASICs, Stake, etc.).
  - Capital costs C per unit and lasts indefinitely.
  - Permissionless entry/exit with a frictionless capital market pre-attack.

Theory Open Question, I

- Assume
  - Block validation requires capital (ASICs, Stake, etc.).
  - Capital costs C per unit and lasts indefinitely.
  - Permissionless entry/exit with a frictionless capital market pre-attack.
  - Common interest rate of r per unit time. (Could be very small)
  - No variable costs, just the capital. Let $c = rC$.

Theory Open Question, I

- Assume
  - Block validation requires capital (ASICs, Stake, etc.).
  - Capital costs C per unit and lasts indefinitely.
  - Permissionless entry/exit with a frictionless capital market pre-attack.
  - Common interest rate of r per unit time. (Could be very small)
  - No variable costs, just the capital. Let $c = rC$.
  - Large finite set I of potential players, as before. Player i's capital denoted x_i, $N = \sum_{i \in I} x_i$.
  - Compensation for validation: validation occurs in rounds. A round takes one unit of time. Validation is compensated at price p per round.

Theory Open Question, I

- Assume
  - Block validation requires capital (ASICs, Stake, etc.).
  - Capital costs C per unit and lasts indefinitely.
  - Permissionless entry/exit with a frictionless capital market pre-attack.
  - Common interest rate of r per unit time. (Could be very small)
  - No variable costs, just the capital. Let $c = rC$.
  - Large finite set I of potential players, as before. Player i's capital denoted x_i, $N = \sum_{i \in I} x_i$.
  - Compensation for validation: validation occurs in rounds. A round takes one unit of time. Validation is compensated at price p per round.
- Characterization theorems of Leshno and Strack (2020) and Chen, Papdimitriou and Roughgarden (2019):
  - Axioms that relate to strict interpretations of anonymity and decentralization (invariance to name changes, free entry, collusion proof) -> Nakamoto compensation scheme

Theory Open Question, I

- Assume
  - Block validation requires capital (ASICs, Stake, etc.).
  - Capital costs C per unit and lasts indefinitely.
  - Permissionless entry/exit with a frictionless capital market pre-attack.
  - Common interest rate of r per unit time. (Could be very small)
  - No variable costs, just the capital. Let $c = rC$.
  - Large finite set I of potential players, as before. Player i's capital denoted x_i, $N = \sum_{i \in I} x_i$.
  - Compensation for validation: validation occurs in rounds. A round takes one unit of time. Validation is compensated at price p per round.
- Characterization theorems of Leshno and Strack (2020) and Chen, Papdimitriou and Roughgarden (2019):
  - Axioms that relate to strict interpretations of anonymity and decentralization (invariance to name changes, free entry, collusion proof) -> Nakamoto compensation scheme
  - Thus, in this stylized environment, we have a zero-profit condition for honest equilibrium of any permissionless consensus that satisfies the axioms:

$$N^* c = p$$

Theory Open Question, I

- Step 2: Use classic results from CS theory of distributed consensus to get general versions of vulnerability to majority attack.

Theory Open Question, I

- Step 2: Use classic results from CS theory of distributed consensus to get general versions of vulnerability to majority attack.
- BFT-style consensus: 33%. (Dwork, Lynch, Stockmeyer, 1984).
- Nakamoto-style longest-chain consensus: 51%.
- Important note: these results obtain under assumptions about the communications environment. (The "partially synchronous model" of Dwork et al, 1984)
  - If we can assume a perfectly reliable network, with perfect timestamps, then distributed trust becomes a lot simpler. (Dolev and Strong, 1983)

Theory Open Question, I

- Step 3: Use ideas from my paper to define cheap versus expensive attacks.

Theory Open Question, I

- Step 3: Use ideas from my paper to define cheap versus expensive attacks.
- Let's define an attack as cheap if its cost to the attacker is $O(N^* c)$

Theory Open Question, I

- Step 3: Use ideas from my paper to define cheap versus expensive attacks.
- Let's define an attack as cheap if its cost to the attacker is $O(N^* c)$
- Let's define an attack as expensive if its cost to the attacker is $O(N^* C)$

Theory Open Question, I

- Step 3: Use ideas from my paper to define cheap versus expensive attacks.
- Let's define an attack as cheap if its cost to the attacker is $O(N^* c)$
- Let's define an attack as expensive if its cost to the attacker is $O(N^* C)$
- An attack is expensive without reliance on a collapse argument if both
  - The attack is expensive: cost to the attacker is $O(N^* C)$, and
  - Post-attack, all non-attackers can still freely buy/sell capital at price C ("no collapse")

Theory Open Question, I

- Step 3: Use ideas from my paper to define cheap versus expensive attacks.
- Let's define an attack as cheap if its cost to the attacker is $O(N^* c)$
- Let's define an attack as expensive if its cost to the attacker is $O(N^* C)$
- An attack is expensive without reliance on a collapse argument if both
  - The attack is expensive: cost to the attacker is $O(N^* C)$, and
  - Post-attack, all non-attackers can still freely buy/sell capital at price C ("no collapse")
- Question: *is there a blockchain protocol that makes all attacks expensive without reliance on a collapse argument?*

Theory Open Question, I

- Let's first observe that traditional forms of trust solve the problem easily

Theory Open Question, I

- Let's first observe that traditional forms of trust solve the problem easily
- Example: collateral + rule-of-law

Theory Open Question, I

- Let's first observe that traditional forms of trust solve the problem easily
- Example: collateral + rule-of-law
  - Post *NC* of financial collateral. Lose the collateral if you cheat. Enforced by rule-of-law.

Theory Open Question, I

- Let's first observe that traditional forms of trust solve the problem easily
- Example: collateral + rule-of-law
  - Post *NC* of financial collateral. Lose the collateral if you cheat. Enforced by rule-of-law.
  - Opportunity cost of collateral is *rNC* if the collateral is not used productively
  - Opportunity cost of collateral can even be lower if it can be used productively while locked up (e.g., invested in risk-free bonds). ηrNC where $\eta \leq 1$, possibly significantly lower than 1.

Theory Open Question, I

- Let's first observe that traditional forms of trust solve the problem easily
- Example: collateral + rule-of-law
  - Post NC of financial collateral. Lose the collateral if you cheat. Enforced by rule-of-law.
  - Opportunity cost of collateral is rNC if the collateral is not used productively
  - Opportunity cost of collateral can even be lower if it can be used productively while locked up (e.g., invested in risk-free bonds). ηrNC where $\eta \leq 1$, possibly significantly lower than 1.
- So, if rule-of-law works as intended
  - Attack costs attacker their collateral NC. So IC is $NC > V_{attack}$.
  - While cost of securing the trust, if all behave honestly, is only $p = \eta rNC$.
  - So equation (3) is $p \geq \eta rV$.
  - Security is cheap, attacks are expensive.

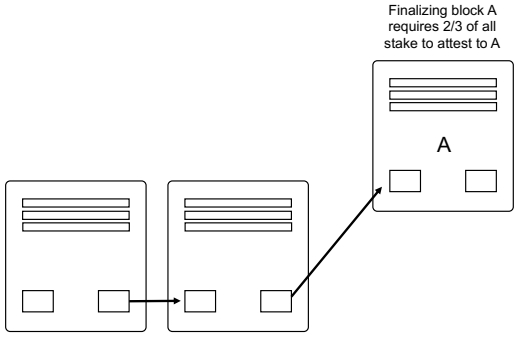
Theory Open Question, I

- Proof of stake and attacks
  - Usual motivation: reduce mining expense and environmental harm
  - Environmental issue is orthogonal to the concerns raised in this paper. Just conceptualize c as per-block opportunity cost of stake
  - But: stakes have *memory*. This creates new possibilities for making attacks expensive.

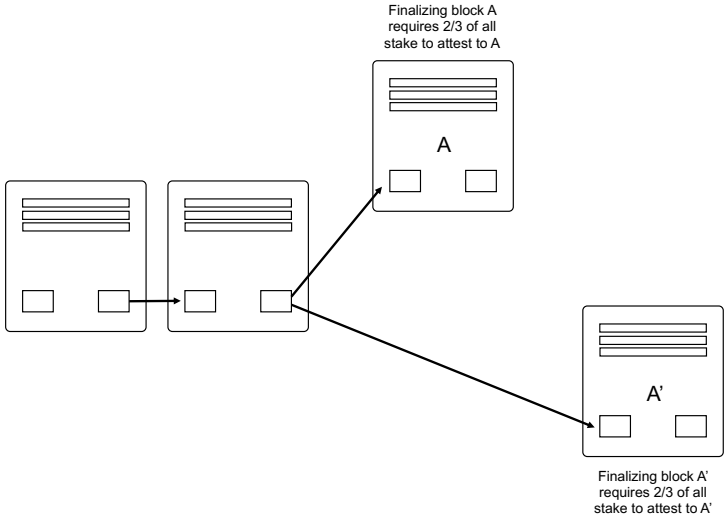
Theory Open Question, I

- Proof of stake and attacks
  - Usual motivation: reduce mining expense and environmental harm
  - Environmental issue is orthogonal to the concerns raised in this paper. Just conceptualize c as per-block opportunity cost of stake
  - But: stakes have *memory*. This creates new possibilities for making attacks expensive.
- Ethereum Proof-of-Stake
  - In event of a double-spending attack ("finality reversion"): confiscate the attacker's stake ("slashing").
    - Takes advantage of observability of attacker signing conflicting transactions.
    - Takes advantage of memory – stakes are locked up for long enough for the confiscation to work.
    - Makes the cost of double-spending attack a stock not a flow: $\frac{1}{2}N^*C$

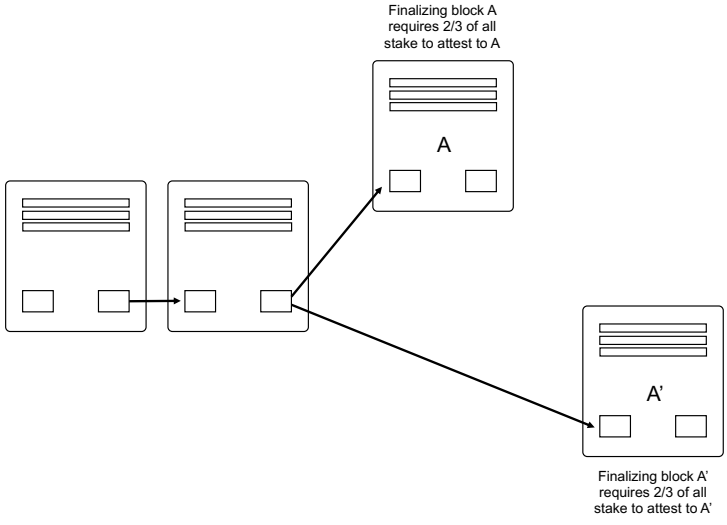
Ethereum PoS: Punishing a Double-Spend Attacker



Ethereum PoS: Punishing a Double-Spend Attacker

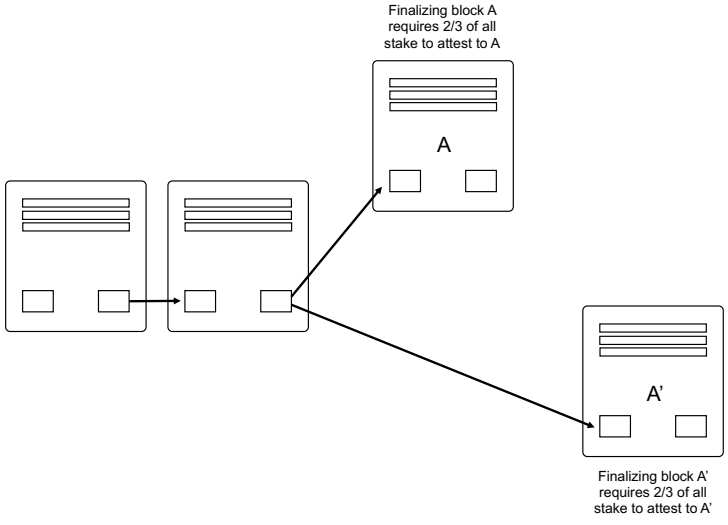


Ethereum PoS: Punishing a Double-Spend Attacker



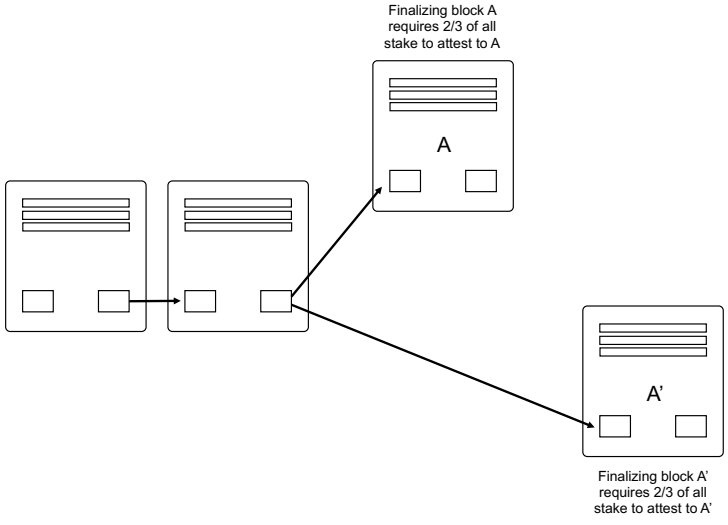
- Therefore, at least 1/3 of all stake signed both A and A'

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

Theory Open Question, I

- Contrast
  - Bitcoin collapse model: "untargeted slashing". All ASICs have to lose their value for the attack to cost $O(N^* C)$.
  - Ethereum PoS model: "targeted slashing". Only confiscate the attacker's stake. Hence don't need implicit assumption of collapse for security.

Theory Open Question, I

- Contrast
  - Bitcoin collapse model: "untargeted slashing". All ASICs have to lose their value for the attack to cost $O(N^*C)$.
  - Ethereum PoS model: "targeted slashing". Only confiscate the attacker's stake. Hence don't need implicit assumption of collapse for security.
- This is great ... but Ethereum PoS raises new issues not faced by Bitcoin:
  - "Liveness" attacks as opposed to "Safety" attacks
  - These only cost a "flow" not a "stock" in Ethereum's new model
  - Attacker could halt the Ethereum blockchain for long periods of time at low cost

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.

Theory Open Question, I

- The reason Ethereum hesitates to slash silent stakes quickly is there could be legitimate/honest network faults (e.g., stake on a computer in Ukraine)
- But this makes it vulnerable to liveness attacks

Theory Open Question, I

- The reason Ethereum hesitates to slash silent stakes quickly is there could be legitimate/honest network faults (e.g., stake on a computer in Ukraine)
- But this makes it vulnerable to liveness attacks
- Intrinsic tension in BFT-style consensus
  - Require a significant fraction to finalize blocks, to reduce vulnerability to double spending ("safety attack").
  - But this in turn leaves vulnerability to liveness attacks.

Theory Open Question, I

- The reason Ethereum hesitates to slash silent stakes quickly is there could be legitimate/honest network faults (e.g., stake on a computer in Ukraine)
- But this makes it vulnerable to liveness attacks
- Intrinsic tension in BFT-style consensus
  - Require a significant fraction to finalize blocks, to reduce vulnerability to double spending ("safety attack").
  - But this in turn leaves vulnerability to liveness attacks.
- The liveness issue leaves me skeptical that Ethereum PoS in its current form could be relied upon for global finance.
- Also leaves me excited about the open question.
- (Brainstorming with Tim Roughgarden. We have some initial conjectures and preliminary results at least.)

Theory Open Question, II

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

Theory Open Question, II

- Computer scientists unimpressed with "permissioned blockchain" / "distributed ledger"
  - "Just a database"
  - Nothing intellectually new from a CS perspective
- Open 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.

Theory Open Question, II

- One initial thought is that the value might come from unlocking small transactional efficiencies in financial markets (early project explorations with Shengwu Li and Adi Sunderam).

Theory Open Question, II

- One initial thought is that the value might come from unlocking small transactional efficiencies in financial markets (early project explorations with Shengwu Li and Adi Sunderam).
- Consider the following stylized game:

	Trust	Cheat	Don't Engage
Trust	+1 +1	+100 -200	0 0
Cheat	-200 +100	0 0	0 0
Don't Engage	0 0	0 0	0 0

Theory Open Question, II

- Some immediate results:

Theory Open Question, II

- Some immediate results:
  1. In a bilateral relationship with sufficient repetition, trust is possible under a standard folk theorem argument. ("Goldman Sachs and JP Morgan, even without rule of law.")

Theory Open Question, II

- Some immediate results:
  1. In a bilateral relationship with sufficient repetition, trust is possible under a standard folk theorem argument. ("Goldman Sachs and JP Morgan, even without rule of law.")
  2. In a larger setting, without specific individual histories and with some bad apples, the Sugaya-Wolitzky (2020) theorem tells us trust is impossible. ("Small banks in different developing jurisdictions.")

Theory Open Question, II

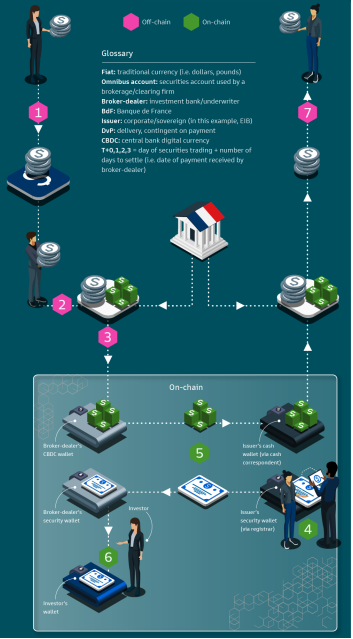
- Some immediate results:
  1. In a bilateral relationship with sufficient repetition, trust is possible under a standard folk theorem argument. ("Goldman Sachs and JP Morgan, even without rule of law.")
  2. In a larger setting, without specific individual histories and with some bad apples, the Sugaya-Wolitzky (2020) theorem tells us trust is impossible. ("Small banks in different developing jurisdictions.")
- If we add to the bad-apples environment a centralized recordkeeper who sees histories and certifies good actors, they can facilitate trust and charge a fee for this service. ("JP Morgan intermediating the small banks.")

Theory Open Question, II

- Some immediate results:
  1. In a bilateral relationship with sufficient repetition, trust is possible under a standard folk theorem argument. ("Goldman Sachs and JP Morgan, even without rule of law.")
  2. In a larger setting, without specific individual histories and with some bad apples, the Sugaya-Wolitzky (2020) theorem tells us trust is impossible. ("Small banks in different developing jurisdictions.")
- If we add to the bad-apples environment a centralized recordkeeper who sees histories and certifies good actors, they can facilitate trust and charge a fee for this service. ("JP Morgan intermediating the small banks.")
- An idealized permissioned blockchain could accomplish the same thing as the centralized recordkeeper, but without the rent extraction (or transactional inefficiencies).
  - Not claiming that such a system exists, rather articulating what the gains of such a system might be.

In April 2021, Goldman Sachs co-led the first public digital issuance on Ethereum public blockchain for the European Investment Bank (EIB), a €100 Million 2-year bond.

Issued under French law, the transaction was selected by Banque de France as part of an experiment with central bank digital currency (CBDC).



1. Investor wired fiat to omnibus account at broker-dealer
2. Broker-dealer wired fiat to central bank escrow account
3. Central-bank created a corresponding amount of CBDC and deposited in broker-dealer's wallet
4. Issuer instructed registrar to create bond token and deposit in issuer's wallet
5. Broker-dealer executed deal book, enabling its conversion into settlement instructions. CBDC was then transferred to Issuer and bond tokens received by broker-dealer (in DvP)
6. Broker-dealer made a "free-of-payment" (vs DvP in traditional settlement process) transfer of bond tokens to respective investor wallets
7. Central bank's digitization mechanism used cash correspondent to convert the Issuer's CBDC into fiat and paid it out to issuer

Why was this important?

First public digital issuance on Ethereum public blockchain

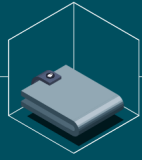
First ever multi-dealer digital issuance

Digitally native tokenization for both securities & cash

T+1 settlement vs a traditional T+3 or longer (with near-term potential to get to T+0)

What are the benefits?

Improved speed and efficiency



Reduction in costs

Increased transparency

Accessible to traditional market participants

More Blockchain Theory Questions

- Are there interesting ways to combine blockchain trust with traditional trust?
  - Idea of "Layer 2" protocols
  - Concede that Bitcoin/Ethereum/etc. are intrinsically very expensive ("Layer 1")
  - Build applications that net to Bitcoin etc. occasionally, but are also partially anchored in traditional trust
- Are there ways to tune the level of blockchain trust — and hence the level of cost — to the nature of the transaction?
- Do models of blockchain trust teach us anything new about traditional trust? (Traditional trust is often multi-layered)

Crypto Data for Finance Research

- There is clearly a lot of cultural, intellectual and financial excitement about Nakamoto's novel form of trust, and decentralization more broadly

Crypto Data for Finance Research

- There is clearly a lot of cultural, intellectual and financial excitement about Nakamoto's novel form of trust, and decentralization more broadly
- Yet, most volume to date appears to be speculative. Moreover, through cryptocurrency exchanges — centralized, trusted, financial intermediaries! (Makarov and Schoar, 2021)
  - Clearly, a distinction between *users* of Nakamoto's novel form of trust and *speculators* about its importance.

Crypto Data for Finance Research

- There is clearly a lot of cultural, intellectual and financial excitement about Nakamoto's novel form of trust, and decentralization more broadly
- Yet, most volume to date appears to be speculative. Moreover, through cryptocurrency exchanges — centralized, trusted, financial intermediaries! (Makarov and Schoar, 2021)
  - Clearly, a distinction between *users* of Nakamoto's novel form of trust and *speculators* about its importance.
- These patterns make me suspect that the most promising paths for future research in finance are not to study crypto finance per se (e.g., asset pricing for crypto assets, DeFi exchange designs), but to use crypto data to study broader issues in behavioral finance and financial market regulation.
  - Blockchain data are especially rich — though, ironically, trading on centralized exchanges may be the exception to this

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 $>>$ NPV of cash flows

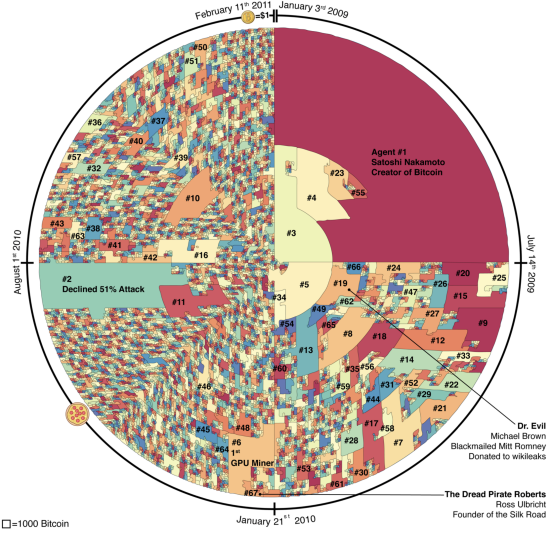
Bubble Formation

- 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 $>>$ NPV of cash flows
- Delong, Shleifer, Summers and Waldman (1990): noise traders follow positive-feedback investment strategies (extended in "Extrapolation and Bubbles", Barberis, Greenwood, Jin and Shleifer, 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

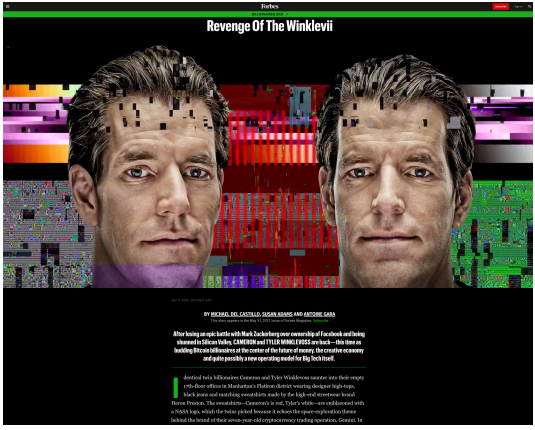
- One specific topic: crypto seems a fascinating laboratory through which to study bubbles
- Key observation here: it's a bubble either way!
  - Whether it persists or collapses!
  - At least in the narrow sense of price $>>$ NPV of cash flows
- Delong, Shleifer, Summers and Waldman (1990): noise traders follow positive-feedback investment strategies (extended in "Extrapolation and Bubbles", Barberis, Greenwood, Jin and Shleifer, 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

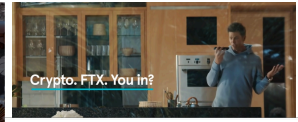


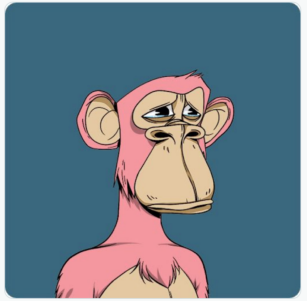
Source: Blackburn et al., 2022, "Cooperation among an anonymous group protected Bitcoin during failures of decentralization"

The Crypto Bros



A Naturally-Occurring Ponzi Process?





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
One word: Doge
3:30 AM · Dec 20, 2020
209.9K Reply Copy link
Read 10.6K replies

Elon Musk @elonmusk · Follow
I will eat a happy meal on tv if @McDonalds accepts Dogecoin
6:30 AM · Jan 25, 2022
408.1K Reply Copy link
Read 29.8K replies

Elon Musk @elonmusk · Follow
Bitcoin is my safe word
2:21 AM · Dec 20, 2020
Read the full conversation on Twitter
223.2K Reply Copy link

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
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
ur welcome

1:57 AM · Feb 4, 2021
937.6K Reply Copy link

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
I will keep supporting Dogecoin
1:19 AM · Jun 19, 2022
388.9K Reply Copy link
Read 37.1K replies

Finance Open Question, II

- 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)

Finance Open Question, II

- 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

Policy / Legal Theory Open Question

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

Policy / Legal Theory Open Question

- 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

Policy / Legal Theory Open Question

- 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

Conclusion: Summary

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

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

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

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

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
- 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")

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
- 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

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
- 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
- Ethereum PoS: solves one problem, creates another. Safety vs. Liveness.

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
- 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
- Ethereum PoS: solves one problem, creates another. Safety vs. Liveness.
- Overall message: there are intrinsic economic limits to how economically important crypto can become. If it gets important enough, it will be attacked. (Unless cost of the system grows even higher)

Conclusion: Summary

- Emphasize: model consistent with earliest uses of Bitcoin and blockchain: hobbyists and black market
  - Black market = willing to pay high implicit fees

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: not skeptical of use of distributed databases more broadly

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: not skeptical of use of distributed databases more broadly
- 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

- 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 ..."

- 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:

- 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?"