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

Eric Budish
University of Chicago, Booth School of Business

April 18th, 2023
Booth All-Faculty Seminar

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, at least in principle, 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 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 serves as both
  1. an explanation for why cryptocurrencies and blockchains have not been very economically useful to date, and
  2. a reason to be skeptical that Bitcoin and the Nakamoto blockchain will play a major role in the global economy and financial system in the future.

The Paper's Argument

- The paper argues that Bitcoin and Nakamoto's novel form of trust — while undeniably ingenious — have serious economic limitations
- Analysis serves as both
  1. an explanation for why cryptocurrencies and blockchains have not been very economically useful to date, and
  2. a reason to be skeptical that Bitcoin and the Nakamoto blockchain will play a major role in the global economy and financial system in the future.
- The paper also provides a framework for thinking about the problem future blockchains would have to solve to overcome these economic limitations.
  - Remains an open question whether such a solution exists

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)

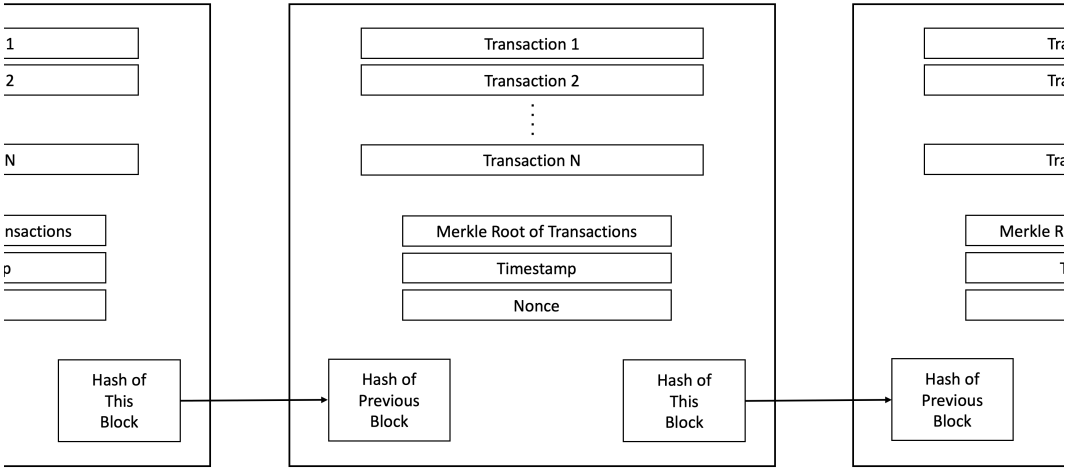
Nakamoto (2008) Blockchain Innovation

- **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)

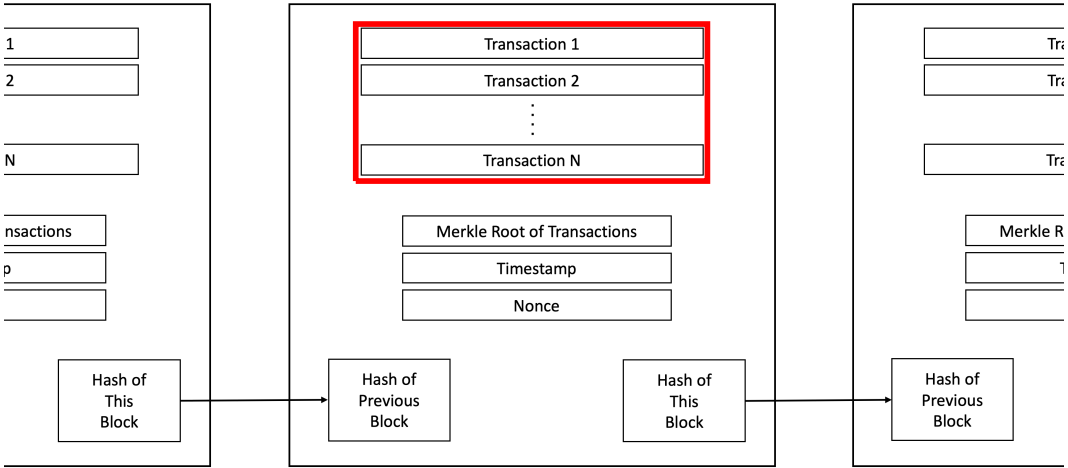
Nakamoto (2008) Blockchain Innovation

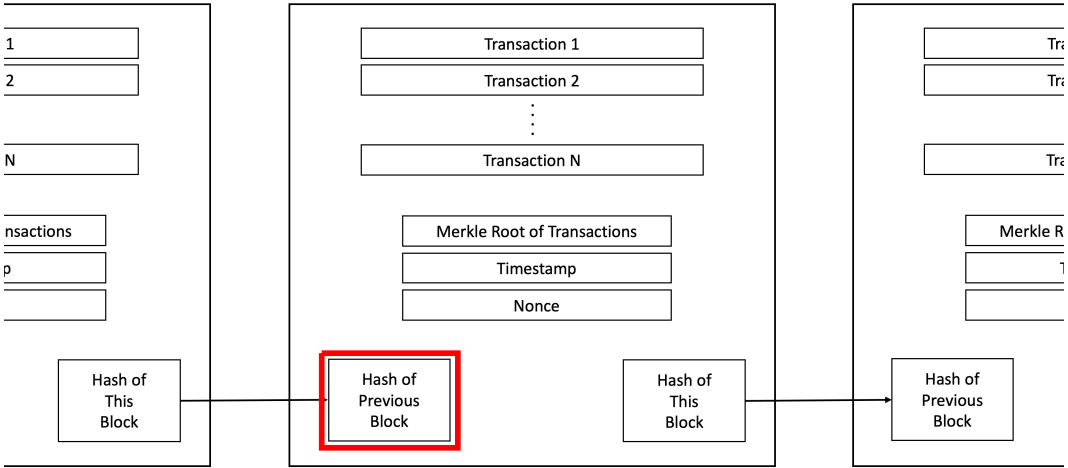
- **I: Pending Transactions List**
  - Users submit transactions to a pending transactions list, called mempool
  - Like a google spreadsheet — not considered official yet
- **II: Valid Blocks**
  - Any computer around the world can compete for the right to add transactions from the mempool to a data 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 350 million TH/s (3.5×10^{20})

SHA-256 Hash Function: Example

Name	SHA256 Hash	Name	SHA256 Hash
Rodrigo Adao	c43f52b74a1f5424c73f9db2dc9283c6bc5998514c1dfc74dedfed0ddc6daa0f	Harry L. Davis	16bec3fe78ccf3157c0473f5e629d313e363952e9b0589c7eedcd0313e4e522f
Dan Adelman	dd5e6e598a330b24c284a5453b6c39dffd4d1c7618fc69393d8e519f74de2e48	Joshua Dean	b01080cb0aa1ff7a2655e0a3baf5f21beda1016e0223574959e316bf06802584
Milena Almagro	27218fcbf01de5787270d1140e63474b034989c9806d9c05c1dda098f2f1a0b1	Levi DeValve	5b46b4f7eb3fb483484e245d01e24144a02b11c264519c2e909547ffeca98c1d
Bryon Aragam	f96deeb5ee3414f9e1354a5c1dc0bd77a29e05d75d269c80d03309372db34b98	Sanjay K. Dhar	f803ff56de7c667b3a99e7fd9fd548e9ce2b5d925d83aced5e9d8253e272d7ae
Baris Ata	a401e2336dac12710c2c19915cb6032562e625cd69f8f39dae9ad0e7e438f62e	Douglas W. Diamond	1a7c4d7ea76219745f5d209be0fe70edfa476ca26ea601b3bbf6cc0a076641fb2
Daniel Bartels	d07474851a924a1a12150812e70f73e47fa92ce4904990b1b5e4f3e31cbdcc81	Berkeley J. Dietvorst	2572dca946080e2c36bc7e9ec037b8ae4f2fb9e6ad2a3cdb275e9dd3f070f328
Francesca Bastianello	bc9fccdcce45e25e40900abaeeb0d4421a1fd0553736fb60c980eee0a220fd6c	Jonathan Dingel	96ca023943b6bf8108d0f520de753625004bed001d4806d976a5a188c97154e9
Philip G. Berger	4b74717d0ac307f003c24129caeafdbfb4a69f226be766fb85219ff9b7cd5381	Rebecca Dizon-Ross	5b22bec6d7ca026cb3fccffdee04f4b8494dece486e67331c540228fe85f5962
Marianne Bertrand	0053bc398f704ecd857f6edaac5a8e2ade8c600852dab0e88a85ebf86c78776e	Kristin Donnelly	e3dbe9e581ca5cb81bd48991d5b5562ec74b2bc09d9cdf6f85efdd8c3c286610
John R. Birge	83b8262a785844d002d4d7d9a858572d95a30589f92b624ddf64128ff280c6da	Wenxin Du	12af62eea44ad482450d42f44364d3e5f79a15fca63e1ca9be380e99324e4c4c4
Jonathan Bonham	534c78d299c0f6244b342807d921cd92aded43fb6093d78d1c13ab378ccab3ec	Jean-Pierre Dubé	65dfa660ab6c36b88c16e4224a7b0f2cc1dae9454e4d5143c7326fe74039b98f
Eric Budish	222667cd0f3bb9c5baf1be47ed5f416f6cd2b413c0721a45ad6bae5977867c16	Donald D. Eisenstein	71d8f349834e9c33ce9a0ce9d8f85d9c6330344c1667a444f505b39d08fe5b86
Ronald S. Burt	079b2671eaa8a167902bc60c57089a0a3887c9abd3ba1ed8c912a0807adb6fc2	Nicholas Epley	b7ba97d0003d1194af87f9c6fbc8e542fc634da88df8beb43528b3b2947e0b7414
Rene Caldentey	7739ba7a4b39070c733c2d4098ad2e708be374f1b59d634d79417121cbc543aa	Merle Erickson	9c781b5004164efc297418ee78548ac0f5a86efbd99641b5e734ffd81fad058c
Christopher Campos	0027d8c4c07cafa45e651340a3537d8ce144b7a986c6d556b9051d5e0f738ada	Eugene F. Fama	dfa8a902d7d1c46988702d8a82a6a0ab61e665e2ca9d54bafbc236c6a4931185
Ozan Candogan	757600d2582a6ece044e2fb11535ead6ce8d19b44d614ba5ba1839fcd1893dc7	Max Farrell	3e04b657a892d717979f816f589a6182a914954134a7e6f93b22af282a0ce6264
Shereen Chaudhry	d3e486436f351c444240f290f05b451d29958330128297c56e80c02fadfe7376	Ayelet Fishbach	371ca020472baa0cd9e474fda944c1a5eedaaaef101ef507ad8c7add109a6b00
Pradeep K. Chintagunta	2a4fa47da0ff905370af0400f5bd1aa922d423eb952b4305d13d029bbdbbbb7e	Alexander P. Frankel	ada5fe2a27b40e5a6d17571b35d1d7723f8a762b9565a3fb36c5b1047a6220c5
Hans B. Christensen	c4b4312f1e29b693c75c4d76f6c00bbb188ec3a23bccb97d77eedc1411ab4cf7	Robert H. Gertner	159e8ac6f68530fc786d6fb6b18e58a4264b4589e37b9c3b300829b5b9d3094d
Emanuele Colonnelli	c7705b0346c15f414e10f0ac38d6dc60d63065881b4387158334945dc9bc9251	Austan D. Goolsbee	8a41b670e79dfbfb787165c19c0052952db44d59b1e7a3e96a3bf4e003950d46
Giovanni Compiani	e8a764369840f37996a3a6ce8521f563be18b44287ef087eaf3600db016bc661	Niels Gormsen	e322ccd5f3095142ace4388412b4cc2247303b023ef1634c1adfa289b72fb39a
George M. Constantinides	f442c6314f9abbfb5856b621f0f8c814fc8eff33ddc02d90f03ed60f7193cb21	Joao Granja	4b01bccb1909399c6edff0b89c8854ae67c008ec6690f7c2e3b01ae987557ed
Anna Costello	637fc29b19e98f6a27747e919bd5ad04f374f96194e73b4e7873a16ee8598f04	Veronica Guerrieri	aea43bc44f75d217fd4cbd9c6d0840976f403d62bec01adc789216561615b11f
Thomas Covert	b33f79d2ef516c1c0cfe1d0a6e1ad1b9b4ad9fc6195c78fce9196855388cd4b2	Varun Gupta	06a075106b1a472f4db2fab338bf69007772bbe6190192778a49c9ed4a3f7b50f
Steven J. Davis	1174d6553b7499383bd3ab7f527cdfac630c229ee75b90e036fff6f6016db0a	Lars Hansen	9ee2fdf49fce186e157ee9cddee2e2ad28edab2bba1b86edca2d66648e3f9930

SHA-256 Hash Function: Example

Name	SHA256 Hash	Name	SHA256 Hash
Christian B. Hansen	2a49485b0a9b2099ecd20f71178aa8a9e1e6f07a00bcf8678d834722cdc2da65	Emma Levine	3ca0e858b48366b023be9b49a677cf365cd8cea623fa40508ccdab66f91c9f0d
Reid Hastie	c3d438e49107aa2c1bd699938dd58f758c967631ffafac0a6dbb901308943886	Tengyuan Liang	d9cc3d02bb5147ea30c775a620d73c9b9478150f973e4cb0d1b7a3b3cb5a87c6
Zhiguo He	dc5fa66163b4118cbdd609a6b6fcf42b36ffd7f3b1bbbe91e3be21cbdff84d14	Guido Lorenzoni	01a1daa8d66b986d91d92e850bf618805477fb2fb958dd05ef71a590d9ec0d73
John C. Heaton	e4478dbd0a0b4b0343e51f80e56ee424ce9981a1947e1d098990e4095c17fe63	Haihao Lu	9a65806f07d87dc0751e455e695df9db32eb323dbf46c8326f617abf1f5be3a95
Guenter J. Hitsch	3d3e4a61ac1cb25e061cd0b386acfd77bc0df9483927957d2761f7e7a4d7b721	Yueran Ma	5c20e4b958d34fac31de52df393ed752cbfbb47bbdb5cafa243348c34a26119a
Richard Hornbeck	a6570aa5b588a2ed2975818e724ab393f1b9659735314099c4c7be41ad3e18bb	Andrew McClellan	7e86c6118564a227030a2fce835150391487892f5c7b48d50b03bcdc5fe8eb96
Christopher K. Hsee	1c2adb25b786b4d5e38de866260f79c63b22debd8fb654facc0ea330e41a89164	Charles McClure	a3844aefadd4da94a0513db096e42b0defce29c06abb48bae11aa3cf44ecc22a
Chang-Tai Hsieh	a6597c76423e5e060079b918e2cab5c0b59c2ceded7d6202f1083de2fccde235	Ann L. McGill	0ac9bc8de1ee0d3d09663ac1f131cf9d7bfa2872870617934ebcbbd26cd92c6c
Kilian Huber	3113b3a80ec1740b2fe5ac572b006d1737f55168e9c419597e6f907c52ce87f6	Michael Minnis	44bb3c49cc50b3961158469d1939c42744cec5123a8ddfb65687cd8de0529e38
John Huizinga	87f1b2432708814484e18d3b9594bcdc90867441c36d4bf73442df2d12c6d9c5	Sanjog Misra	b745fd4aa844392b760ee68f1a2b1fa8bf479fb07ac0ed0caed096f4fbb02da7
Anders Humlum	b6215e59a470a07e1f4750ea3d8e1396d229dc1a32e965cab200f59f517e44a5	Jack Mountjoy	2b8075d3b7a49327bee8b11e9a2794c39a5ed3421c21bf6e592b647f60447bae
Erik Hurst	0dd6c2741c9a46939d6468474ec50f680dbbc27f12b745b3bc2789619ec5995d	Maximilian Muhn	05511ed68be79b068f1a49f26452e4e22ec4720329fe44ed8e299264b81583c4
Alex Imas	fbc33f0929307b6487cd0bce159c903859c9f0b48eecebf4d892e85698763dbb	Sendhil Mullainathan	ab3e83fff24881ecc778afbe48b545b2979c0ca8a90a3e048c5453438c460a0e
Tetsuya Kaji	a2bfe35f2642fcd1c42ecda963dfdbbdaaf658d9a2b5e8aa00867394a694c6	Kevin M. Murphy	08dde39f398faf53c8571908726c9a5c23ceaa77469562547bb39f25344613e6
Emir Kamenica	7be350947ea8e80e9560aa6443fa5021ff1cc0ac658307567647d4cf00a4b6382	Stefan Nagel	141f5f85e38585aefdf6ee68c9f9677c5327d69357d5a930aad0ef2a53aeb542
Steven Neil Kaplan	e5714f1357b694d485994e9a4c3554df5ecea2befa8b2d23bebc6e023f36503a	Brent Neiman	179b03572b2468ceaf2dbc9fab5a044c65e250a3c3f15928c2c7e81363088eb9
Anil Kashyap	c062962df257479541f39d9e2845e8f616c613d2ce816d5c334aded601c19782	Scott Nelson	c17e65672df8b7bcb5127344bb77ee80239762544cd51fa8615272dbb61bdaa1
Rohan Kekre	18ed88e4c679aa7dbab99711dd7c8fb29c5ffb4068676e65ddc6d1a4b5f392d7	Rad Niazadeh	4d4a1b18ee32c56920bc87d57358f029d6d7d493f5ec0122aa2022c39c5dab4c
Erika Kirgios	2dac9e181f61015d1299e073ebf6dded4e5f74356b2ef143bc1246f390a76847	Valeri Nikolaev	3663ee9a50f4f2b0bfb39df8dc1d66c236ccaee352eb9d0e5e700819882f25c3
Alex Koch	4e1faecde2d5c5ae3a64f0d96f4b6ca5058100681c9f7c2b73ba4b75629a200f	Pascal Noel	78403447a78b73679bc326ba9aac99ab7797250790d6bdedc3963f5db1c64631
Ralph S.J. Koijen	24357fd3472fe4ea8cc32ea6cbf1aa624c152d33c536a43b6d72629a446afc4a	Matthew Notowidigdo	9512927c05cc857784eaa65dc399cf67e7020d397c79ca10325253f1901c4def
Mladen Kolar	cb447f4d06161e0afdb491e0fb30b56069db77305aae272460141e53b6322d91	Ed O'Brien	fe3e0fa35111917b7b449880a3c3c0b6410cee86e7c25761c2ca35b91f64871d
Randall S. Kroszner	ba22176cccbf63740cbcd3f19f11602faa5abb20fef2ba3b180cdd8effca8b4c	Lubos Pastor	3b5254b8e44ece8e9979d0fdb84757980031b6505455a3bdff4317cad696f947d
Jacob Leshno	92a55a161f82983fb33e1131fc625dda89cdca891f325e1805cd8a50fecb8388	Christina Patterson	a40599e64a417a8fb05761f93a4fec319456d1f3702c117f284de8a869c6dfe9
Christian Leuz	32ba3f7ca8fedb7bdb4652894c6cbb1e9f961e4c2621601c696024f900b5c14e	Nicholas Polson	70e3502dbfc59e2d57c05776e6a2ffc10456db52e61fe5e7335cdfa69855d88e

SHA-256 Hash Function: Example

Name	SHA256 Hash	Name	SHA256 Hash
Devin G. Pope	1d0c04e6c602132dc38a1ba3f9451d32459f42e94c4d5566be8916521aafc360	Thomas Talhelm	0d68437684ec8f590186b63229377bf7a0c5811b071fcdc1338a12bb813ef767
Canice Prendergast	4682d9ce384e21d37ec1132c3ce9f11daeac7c7d2dc58a7785500aae34fd166c	Richard H. Thaler	8cc701bb6debb569f02803e93f4699eecd77f37546a6d075449ac03c995be10a
Madhav Rajan	be8c84ab21bfe5376c929b4ed8bd86f5776f859d2dee5d5c70c3e36953defe5	Alexander Todorov	e1198087b547a03fc29e99746afcae2fc2f3e0170b8088a5969638cef2b1b09c
Raghuram G. Rajan	3215ab7fe46cd118055237451674 28e30772960995ed4a89e16cd7ff36f5638b	Rimmy Tomy	994fef38e6aad2fbed6524b3991b3b1c7cf0a62c0773c4cd55b9223255bacc46
Daniel Rappoport	8bbc726ad0b7e31336e5b5ba2b2c91f6ff21d2debdbcd6f981fe0ed5f7d69b6a	Robert H. Topel	be0ad2c204fbcc0335025a1d4d4bc3fdd246f4b57fb3c50e1ac98e31ccca7819
Thomas Rauter	881b459c6348657f61ed79d17094fc6cc2544fc098a8f09a056d8f28bee287a6	Panagiotis Toulis (Panos)	2396bf43a342c4c29eafe71b769d27495404c2e9abb86ab662e5779bdf091919
Amoray Riggs-Cragun	ca3f0389c01babf6442b24dc7e6a7b94285c81e466321c6a315e187609f93fc5	Oleg Urminsky	ecc6679a0d783370a997e28f1e8024d231443d4994e0f79db44e89cfd0051544
Jane L. Risen	d6a9429b7131d0cc3f772f1eb2d2a59f98bfb65fdade89b1c4ec7faf57adf52b	Quentin Vandeweyer	81ab2d635ad8ec882950c90646d2b213630762b636e246a55b21920cd7a78aac
Veronika Rockova	4530be6d1eccff6df39d5675f9776c28af487c508790aa4000d5742a85611a30	Joseph Vavra	b802f5e833286758665457c0836e2fcd6d43f3ee4536822b71fd01b86e83db60
Elisa Rubbo	7604e439432fad14195ec50bb731f84bc19ba2333bd1931607913b905af6644d	Pietro Veronesi	1c860307de95ac2e1114516ea305aaa6e64f123b81503bbc68066dcd224acc19
Jeffrey R. Russell	eae75416d345a4b4cf9e2370b3819687d0542041b2b195abf0034b610f8e8c97	Robert W. Vishny	832788bd5e8b868057ddf71027e1107098beb014aa3de316ed91b25d8f21ecc9
Delphine Samuels	95cb541213d91335c3b1b68b2c90bd243a853d9f4d643a5360dd61091e32ff4e	Amy Ward	6e554aeac710de4b381cc1a0d23510aaccec534d518912c24064ea27f11ca73e
Haresh Sapra	176880f76742237887a6c640f5d0681ff2c2be79bd8fb126806a29c046f30299	Michael Weber	1ea3d035edcf80c6dfa04c76ed4bfa6cbdef4465a2e40e65e3829a0bb55f7dc6
Anuj Shah	27e0bc5bc74ceb30f014a3d5e497fac87dfc778470dd1cff13598f8cf1362e28	Bernd Wittenbrink	4121ed4211ab78b807f1c7ba072668783c3f654f8e819a9c9a78121c78a8aea3
Bradley Shapiro	afa4e64101ed0575ccd8b3c3ef648e265c7589b8e0ef0e0e9237718b03be99a4	Thomas Wollmann	8e705da8122f9088fdf1a9d2d0ab6847fb10162dc3f9f758b6e54386375423ab
Douglas J. Skinner	057e51a2f4e2b135e8bfa0810d25d24baf40c6c0ff1a51cebb69a4a32f9ffea5	George Wu	943a7756112b21d5cdc18f52447946550cfd60a4e2b6534ac6b6387287d4dcda
Ekaterina Smetanina	060850166d050e0d3fab92b79f9acd4ea00c4007425cacc27d813568357fa29a	Linwei Xin	2845083efb9e5c00faf7678628b1cac36bd9644ce41f0dcdee349831e94d73d8
Stephanie Smith	c274d0af13eb96511b4afe6af3cdb416b3187f042ca4a9f25783496748 7d6720	Dacheng Xiu	17d4e7b30454900c0429884ec4593601bd0b5862acc5e25f1a21761fd95e241b
Abbie J. Smith	2462fb627c7e6df5910b4db75d14daae9ad552b810f8fe424a15be2d575a8a9c	Constantine Yannelis	7df95c23c32d4189f70ea1e05beb8955d81eda9d44422ce1565896b9392c047c
Christopher Stewart	4b945e862fd01b2a1ed5274dba5a5a3b7804070015e5fcea8997332a89b76afb	Anastasia A Zakolyukina	ed35ee9affbb0858ec569e11127f6070e2906fbb31f84344a561ee9d00cbaa55
Lars Stole	99dfd38f1a508635f6cb294332f1a17ed1c80f2b08ca5ca673355ed538fd78dd	Anthony Lee Zhang	d3e81d35f317b9e2d2e798b4b30a8ea48b1beb5cfe159f6f7acdaf654214188d
Avner Strulov-Shlain	e3f611b01875eb8b2ec9465fd3eaca7d9651abd1db95f73e5c919e8383ec0458	Yuan Zhong	a2466184c88a1d970fb725e4bcdd71754b8d90118018fb557c6c1bb118efca68
Amir Sufi	0576270b04346cd30db3ef94eefcdfff8267fa0076672ccdc8ff4ef239b0d6e2	Luigi Zingales	d3b5a511e9b479c09ce92f797b88f583d172cf88d157bae4f86728d6af2b3aa9
Abigail Sussman	a190fb8d752b18e6fca0be3f6ad149a1f4af35d03cd2222d4058951106ee968c	Eric Zwick	3e46cf6cddb60beaddee5ee47f8c2b42da597d4afd8d90ec7cf53812e7a2d841
Chad Syverson	7f3fde70eb98bf8ad3458882f23847c99341a5f9210a427d8cc4d2ab5a05a02d		

SHA-256 Hash Function: Example

Name	SHA256 Hash	Name	SHA256 Hash
Rodrigo Adao	c43f52b74a1f5424c73f9db2dc9283c6bc5998514c1dfc74dedfed0ddc6daa0f	Harry L. Davis	16bec3fe78ccf3157c0473f5e629d313e363952e9b0589c7eedcd0313e4e522f
Dan Adelman	dd5e6e598aa330b24c284a5453b6c39dffd4d1c7618fc69393d8e519f74de2e48	Joshua Dean	b01080cb0aa1ff7a2655e0a3baf5f21beda1016e022357a959e316bf06802584
Milena Almagro	27218fcbf01de5787270d1140e63474b034989c9806d9c05c1dda098f2f1a0b1	Levi DeValve	5b46b4f7eb3fb483484e245d01e24144a0b11c264519c2e909547ffeca98c0d1
Bryon Aragam	f96deeb5ee3414f9e1354a5c1dc0bd77a29e05d75d269c80d03309372db34b98	Sanjay K. Dhar	f803ff56de7c667b3a99e7fd9fd548e9ce2b5d925d83aced5e9d8253e272d7ae
Baris Ata	a401e2336dac12710c2c19915cb6032562e625cd69f8f39dae9ad0e7e438f62e	Douglas W. Diamond	1a7c4d7ea76219745d5209be0fe70edfa476ca26ea601b3bbf6cc0a076641fb2
Daniel Bartels	d07474851a924a1a12150812e70f73e47fa92ce4904990b1b5e4f3e31cbdcc81	Berkeley J. Dietvorst	2572dca946080e2c36bc7e9ec037b8ae4f2fb9e6ad2a3cdb275e9dd3f070f328
Francesca Bastianello	bc9fccdcce45e25e40900abaeeb0d4421a1fd0553736fb60c980eee0a220fd6c	Jonathan Dingel	96ca023943b6bf8108e0f520de753625004bed001d4806d976a5a188c97154e9
Philip G. Berger	4b74717d0ac307f003c24129caeafdbfb4a69f226be766fb85217ff9b7cd5381	Rebecca Dizon-Ross	5b22bec6d7ca026cb3fccffdee04f4b8494daece486e67331c540228fe85f5962
* Marianne Bertrand	0053bc398f704ecd857f6edaac5a8e2ade8c600852dab0e88a85ebf86c78776e *	Kristin Donnelly	e3dbe9e581ca5cb81bd48991d5b5562ec74b2bc09d9cdf6f85efdd83c8c286610
John R. Birge	83b8262a785844d002d4d7d9a858572d95a30589f92b624ddf64128ff280c6da	Wenxin Du	12af62eea44ad482450d42f44364d3e5f79a15fca63e1ca9be380e99324e4c4c4
Jonathan Bonham	534c78d299c0f6244b342807d921cd92aded4f3b6093d78d1c13ab378ccab3ec	Jean-Pierre Dubé	65dfa660ab6c36b88c16e4224a7b0f2cc1dae9454e4d5143c7326fe74039b98f
Eric Budish	222667cd0f3bb9c5baf1be47ed5f416f6cd2b413c0721a45ad6bae5977867c16	Donald D. Eisenstein	71d8f349834e9c33ce9a0ce9d8f85d9c6330344c1667a444f505b39d08fe5b86
Ronald S. Burt	079b2671eaa8a167902bc60c57089a0a3887c9abd3ba1ed8c912a0807adb6fc2	Nicholas Epley	b7ba97d0003d1194af87f9c6fbc8e542fc634da88df8beb43528b3b2947e0b7414
Rene Caldentey	7739ba7a4b39070c733c2d4098ed2e708be374f1b59d634d79417121cbc543aa	Merle Erickson	9c781b50044164efc297418ee78548ac0f5a86efbd99641b5e734ffd81fad026
** Christopher Campos	0027d8c4c07cafa45e651340a3537d8ce144b7a986c6d556b9051d5e0f738ada **	Eugene F. Fama	dfa8a902d7d1c46989702d8a82a6a0ab61e665e2ca9d54bafbc236c6a4931185
Ozan Candogan	757600d2582a6ece044e2fb11535ead6ce8d19b44d614ba5ba1839fcd1893dc7	Max Farrell	3e04b657a892d717797f816f589a6182a914954134a7e6f93b22af282a0ce6264
Shereen Chaudhry	d3e486436f351c444240f290f05b451d29958330128297c56e80c02fadfe7376	Ayelet Fishbach	371ca020472baa0cd9e474fda944c1a5eedaaaef101ef507ad8c7add109a6b00
Pradeep K. Chintagunta	2a4fa47da0ff905370af0400f5bd1aa922d423eb952b4305d13d029bbdbbbb7e	Alexander P. Frankel	ada5fe2a27b40e5a6d17571b35d1d7723f8a762b9565a3fb36c5b1047a6220c5
Hans B. Christensen	c4b4312f1e29b693c75c4d76f6c00bbb188ec3a23bccb97d77eedc1411ab4cf7	Robert H. Gertner	159e8ac6f68530fc786d6fb6b18e58a4264b4589e37b9c3b300829b5b9d3094d
Emanuele Colonnelli	c7705b0346c15f414e10f0ac38d6dc60d63065881b4387158334945dc9bc9251	Austan D. Goolsbee	8a41b670e79dfbfb787165c19c0052952db44d59b1e7a3e96a3bf4e003950d46
Giovanni Compiani	e8a764369840f37996a3a6ce8521f563be18b44287ef087eaf3600db016bc661	Niels Gormsen	e322ccd5f3095142ace4388412b4cc2247303b023ef1634c1adfa289b72fb39a
George M. Constantinides	f442c6314f9abbfb5856b621f0f8c814fc8eff33ddc02d90f03ed60f7193b221	Joao Granja	4b01bccb1909399c6edff0b89c8854ae67c008ec6690f7c2e3b01ae987557ded
Anna Costello	637fc29b19e98f6a27747e919bd5ad04f374f96194e73b4e7873a16ee8598f04	Veronica Guerrieri	aea43bc44f75d217fd4cbd9c6d0840976f403d62bec01adc789216561615b11f
Thomas Covert	b33f79d2ef516c1c0cfe1d0a6e1ad1b9b4ad9fc6195c78fce9196855388cd4b2	Varun Gupta	06a075106b1a472f4db2fab33bf69007772bbe6190192778a49c9ed4a3f7b50f
Steven J. Davis	1174d6553b7499383bd3ab7f527cdfac630c229ee75b90e036fff6f6016db0a	Lars Hansen	9ee2fdf49fce186e157ee9cddee2e2ad28edab2bba1b86edca2d66648e3f9930

SHA-256 Hash Function: Example

Name	SHA256 Hash	Name	SHA256 Hash
Christian B. Hansen	2a49485b0a9b2099ecd20f71178aa8a9e1e6f07a00bcf8678d834722cdc2da65	Emma Levine	3ca0e858b48366b023be9b49a677cf365cd8cea623fa40508ccdab66f91c9f0d
Reid Hastie	c3d438e49107aa2c1bd699938dd58f758c967631ffafac0a6dbb901308943886	Tengyuan Liang	d9cc3d02bb5147ea30c775a620d73c9b9478150f973e4cb0d1b7a3b3cb5a87c6
Zhiguo He	dc5fa66163b4118cbdd609a6b6fcf42b36ffd7f3b1bbbe91e3be21cbdff84d14	Guido Lorenzoni	01a1daa8d66b986d91d92e850bf618805477fb2fb958dd05ef715a90d9ec0d73
John C. Heaton	e4478dbd0a0b4b0343e51f80e56ee424ce9981a1947e1d098990e4095c17fe63	Haihao Lu	9a65806f07d87dc0751e455e695df9db32eb323dbf46c8326f617abf1f5be3a95
Guenter J. Hitsch	3d3e4a61ac1cb25e061cd0b386acfd77bc0df9483927957d2761f7e7a4d7b721	Yueran Ma	5c20e4b958d34fac31de52df393ed752cbfbb47bbdb5cafa243348c34a26119a
Richard Hornbeck	a6570aa5b588a2ed2975818e724ab393f1b9659735314099c4c7be41ad3e18bb	Andrew McClellan	7e86c6118564a227030a2fce835150391487892f5c7b48d50b03bcdc5fe8eb96
Christopher K. Hsee	1c2adb25b786b4d5e38de866260f79c63b22debd8fb654fac0ea330e41a89164	Charles McClure	a3844aefadd4da94a0513db096e42b0defce29c06abb48bae11aa3cf44ecc22a
Chang-Tai Hsieh	a6597c76423e5e060079b918e2cab5c0b59c2ceded7d6202f1083de2fccde235	Ann L. McGill	0ac9bc8de1ee0d3d09663ac1f131cf9d7bfa2872870617934ebcbbd26cd92c6c
Kilian Huber	3113b3a80ec1740b2fe5ac572b006d1737f55168e9c419597e6f907c52ce87f6	Michael Minnis	44bb3c49cc50b3961158469d1939c42744cec5123a8ddfb65687cd8de0529e38
John Huizinga	87f1b2432708814484e18d3b9594bcdc90867441c36d4bf73442df2d12c6d9c5	Sanjog Misra	b745fd4aa844392b760ee68f1a2b1fa8bf479fb07ac0ed0caed096f4fbb02da7
Anders Humlum	b6215e59a470a07e1f4750ea3d8e1396d229dc1a32e965cab200f59f517e44a5	Jack Mountjoy	2b8075d3b7a49327bee8b11e9a2794c39a5ed3421c21bf6e592b647f60447bae
Erik Hurst	0dd6c2741c9a46939d6468474ec50f680dbbc27f12b745b3bc2789619ec5995d	Maximilian Muhn	05511ed68be79b068f1a49f26452e4e22ec4720329fe44ed8e299264b81583c4
Alex Imas	fbc33f0929307b6487cd0bce159c903859c9f0b48eecebf4d892e85698763dbb	Sendhil Mullainathan	ab3e83fff24881ecc778afbe48b545b2979c0ca8a90a3e048c5453438c460a0e
Tetsuya Kaji	a2bfe35f2424cd24c1c42ecda963dfdbbdaaf658d9a2b5e8aa00867394a694c6	Kevin M. Murphy	08dde39f398faf53c8571908726c9a5c23ceaa77469562547bb39f25344613e6
Emir Kamenica	7be350947ea8e80e9560aa6443fa5021ff1cc0ac658307567474cf00a4b6382	Stefan Nagel	141f5f85e38585aefdf6ee68c9f9677c5327d69357d5a930aad0ef2a53aeb542
Steven Neil Kaplan	e5714f1357b694d485994e9a4c3554df5ecea2befa8b2d23bebc6e023f36503a	Brent Neiman	179b03572b2468ceaf2dbc9fab5a044c65e250a3c3f15928c2c7e81363088eb9
Anil Kashyap	c062962df257479541f39d9e2845e8f616c613d2ce816d5c334aded601c19782	Scott Nelson	c17e65672df8b7bcb5127344bb77ee80239762544cd51fa8615272dbb61bdaa1
Rohan Kekre	18ed88e4c679aa7dbab99711dd7c8fb29c5ffb4068676e65ddc6d1a4b5f392d7	Rad Niazadeh	4d4a1b18ee32c56920bc87d57358f029d6d7d493f5ec0122aa2022c39c5dab4c
Erika Kirgios	2dac9e181f61015d1299e073ebf6dded4e5f74356b2ef143bc1246f390a76847	Valeri Nikolaev	3663ee9a50f4f2b0bfb39df8dc1d66c236ccaee352eb9d0e5e700819882f25c3
Alex Koch	4e1faecde2d5c5ae3a64f0d96f4b6ca5058100681c9f7c2b73ba4b75629a200f	Pascal Noel	78403447a78b73679bc326ba9aac99ab7797250790d6bdedc3963f5db1c64631
Ralph S.J. Koijen	24357fd3472fe4ea8cc32ea6cbf1aa624c152d33c536a43b6d72629a446afc4a	Matthew Notowidigdo	9512927c05cc857784eaa65dc399cf67e7020d397c79ca10325253f1901c4def
Mladen Kolar	cb447f4d06161e0afdb491e0fb30b56069db77305aae272460141e53b6322d91	Ed O'Brien	fe3e0fa35111917b7b449880a3c3c0b6410cee86e7c25761c2ca35b91f64871d
Randall S. Kroszner	ba22176cccbf63740cbcd3f19f11602faa5abb20fef2ba3b180cdd8effca8b4c	Lubos Pastor	3b5254b8e44ece8e9979d0fdb84757980031b6505455a3bdff4317cad696f947d
Jacob Leshno	92a55a161f82983fb33e1131fc625dda89cdca891f325e1805cd8a50fecb8388	Christina Patterson	a40599e64a417a8fb05761f93a4fec319456d1f3702c117f284de8a869c6dfe9
Christian Leuz	32ba3f7ca8fedb7bdb4652894c6cbb1e9f961e4c2621601c696024f900b5c14e	Nicholas Polson	70e3502dbfc59e2d57c05776e6a2ffc10456db52e61fe5e7335cdfa69855d88e

SHA-256 Hash Function: Example

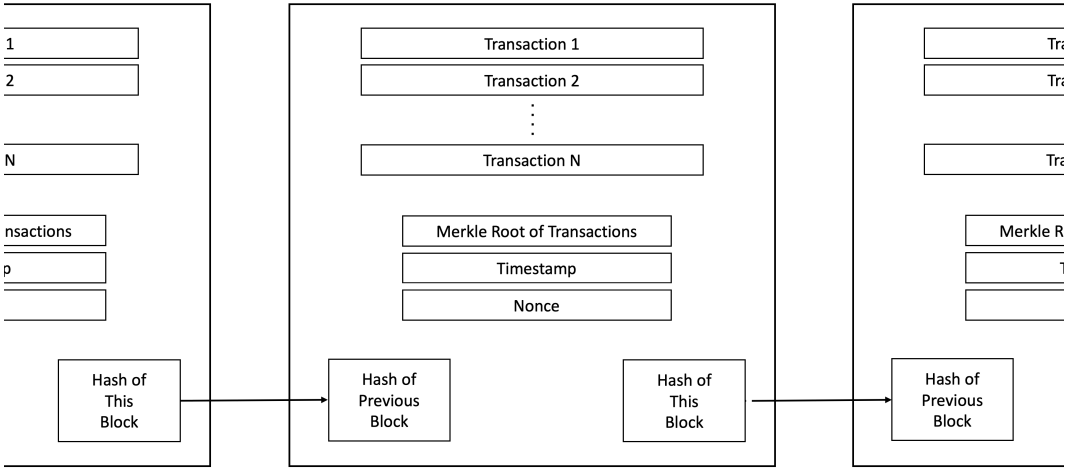
Name	SHA256 Hash	Name	SHA256 Hash
Devin G. Pope	1d0c04e6c602132dc38a1ba3f9451d32459f42e94c4d5566be89165 21aafc360	Thomas Talhelm	0d68437684ec8f590186b63229377bf7a0c5811b071fcdc1338a12bb813ef767
Canice Prendergast	4682d9ce384e21d37ec1132c3ce9f11daeac7c7d2dc58a7785500aae34fd166c	Richard H. Thaler	8cc701bb6debb569f02803e93f4699eecd77f37546a6d075449ac03c995be10a
Madhav Rajan	be8c84ab21bfe5376c929b4ed8bd86f5776f859d2dee5d5c70c3e36953defe5	Alexander Todorov	e1198087b547a03fc29e99746afcae2fc2f3e0170b8088a5969638cef2b1b09c
Raghuram G. Rajan	3215ab7fe46cd118055237 45f67428e307729609 95ed4a89e16cd7ff36f5638b	Rimmy Tomy	994fef38e6aad2fbed6524b3991b3b1c7cf0a62c0773c4cd55b9223255bacc46
Daniel Rappoport	8bbc726ad0b7e31336e5b5ba2b2c91f6ff21d2debdbcd6f981fe0ed5f7d69b6a	Robert H. Topel	be0ad2c204fbcc0335025a1d4d4bc3fdd246f4b57fb3c50e1ac98e31ccca7819
Thomas Rauter	881b459c6348657f61ed79d17094fc6cc2544fc098a8f09a056d8f28bee287a6	Panagiotis Toulis (Panos)	2396bf43a342c4c29eafe71b769d27495404c2e9abb86ab662e5779bdf091919
Amoray Riggs-Cragun	ca3f0389c01babf6442b24dc7e6a7b94285c81e466321c6a315e187609f93fc5	Oleg Urminsky	ecc6679a0d783370a997e28f1e8024d231443d4994e0f79db44e89cfd0051544
Jane L. Risen	d6a9429b7131d0cc3f772f1eb2d2a59f98bfb65fdade89b1c4ec7faf57adf52b	Quentin Vandeweyer	81ab2d635ad8ec882950c90646d2b21363076 2b636e246a55b21920cd7a78aac
Veronika Rockova	4530be6d1eccff6df39d5675f9776c28af487c508790aa4000d5742a85611a30	Joseph Vavra	b802f5e833286758665457c0836e2fcd6d43f3ee4536822b71fd01b86e83db60
Elisa Rubbo	7604e439432fad14195ec50bb731f84bc19ba2333bd1931607913b905af6644d	Pietro Veronesi	1c860307de95ac2e1114516ea305aaa6e64f123b81503bbc68066dcd224acc19
Jeffrey R. Russell	eae75416d345a4b4cf9e2370b3819687d0542041b2b195abf0034b610f8e8c97	Robert W. Vishny	832788bd5e8b868057ddf71027e1107098beb014aa3de316ed91b25d8f21ecc9
Delphine Samuels	95cb541213d91335c3b1b68b2c90bd243a853d9f4d643a5360dd61091e32ff4e	Amy Ward	6e554aeac710de4b381cc1a0d23510aaccec534d518912c24064ea27f11ca73e
Haresh Sapra	176880f76742237887a6c640f5d0681ff2c2be79bd8fb126806a29c046f30299	Michael Weber	1ea3d035edcf80c6dfa04c76ed4bfa6cbdef4465a2e40e65e3829a0bb55f7dc6
Anuj Shah	27e0bc5bc74ceb30f014a3d5e497fac87dfc778470dd1cff13598f8cf1362e28	Bernd Wittenbrink	4121ed4211ab7b8f38b807f1c7ba072668783c3f654f8e819a9c9a78121c78a8aea3
Bradley Shapiro	afa4e64101ed0575ccd8b3c3ef648e265c7589b8e0ef0e0e9237718b03be99a4	Thomas Wollmann	8e705da8122f9088fdf1a9d2d0ab6847fb10162dc3f9f758b6e54386375423ab
Douglas J. Skinner	057e51a2f4e2b135e8bfa0810d25d24baf40c6c0ff1a51cebb69a4a32f9ffea5	George Wu	943a7756112b21d5cdc18f52447946550cfd60a4e2b6534ac6b6387287d4dcda
Ekaterina Smetanina	060850166d050e0d3fab92b79f9acd4ea00c4007425cacc27d813568357fa29a	Linwei Xin	2845083efb9e5c00faf7678628b1cac36bd9644ce41f0dcdee349831e94d73d8
Stephanie Smith	c274d0af13eb96511b4afe6af3cdb416b3187f042ca4a9f257834967487d6720	Dacheng Xiu	17d4e7b30454900c0429884ec4593601bd0b5862acc5e25f1a21761fd95e241b
Abbie J. Smith	2462fb627c7e6df5910b4db75d14daae9ad552b810f8fe424a15be2d575a8a9c	Constantine Yannelis	7df95c23c32d4189f70ea1e05beb8955d81eda9d44422ce1565896b9392c047c
Christopher Stewart	4b945e862fd01b2a1ed5274dba5a3a3b7804070015e5fcea8997332a89b76afb	Anastasia A Zakolyukina	ed35ee9affbb0858ec569e11127f6070e2906fbb31f84344a561ee9d00cbaa55
Lars Stole	99dfd38f1a508635f6cb294332f1a17ed1c80f2b08ca5ca673355ed538fd78dd	Anthony Lee Zhang	d3e81d35f317b9e2d2e798b4b30a8ea48b1beb5cfe159f6f7acdaf654214188d
Avner Strulov-Shlain	e3f611b01875eb8b2ec9465fd3eaca7d9651abd1db95f73e5c919e8383ec0458	Yuan Zhong	a2466184c88a1d970fb725e4bcdd71754b8d90118018fb557c6c1bb118efca68
Amir Sufi	0576270b04346cd30db3ef94eefcdfff8267fa0076672ccdc8ff4ef239b0d6e2	Luigi Zingales	d3b5a511e9b479c09ce92f797b88f583d172cf88d157bae4f86728d6af2b3aa9
Abigail Sussman	a190fb8d752b18e6fca0be3f6ad149a1f4af35d03cd2222d4058951106ee968c	Eric Zwick	3e46cf6cddb60beaddee5ee47f8c2b42da597d4afd8d90ec7cf53812e7a2d841
Chad Syverson	7f3fde70eb98bf8ad3458882f23847c99341a5f9210a427d8cc4d2ab5a05a02d		

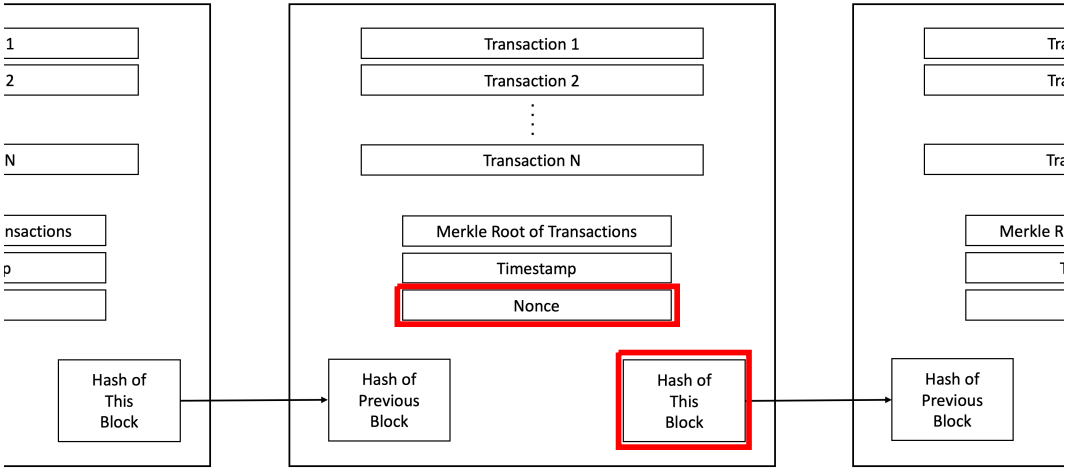
What is Nakamoto Blockchain (3/4)

- **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.
    - Currently small as a fraction of total compensation. I will ignore for the purpose of this talk.
    - See Huberman, Leshno and Moallemi (2021) on the economics.
- Tournament difficulty adjusts every two weeks, calibrated to take about 10 minutes


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 are not memory-less*:* they are locked up on chain (like collateral) and observably persist over time (like reputation). This opens up the possibility of punishing attackers by confiscating their stakes, 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. Necessary condition for no player to have a profitable attack: $p \geq \frac{V_{attack}}{1+\frac{1}{l}}$ (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. Necessary condition for no player to have a profitable attack: $p \geq \frac{V_{attack}}{1+\frac{1}{I}}$ (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 and use Lemma: $V_{attack} \leq p + \frac{x_i^*}{N^*} p$
  - Using smallest x_i^*: $V_{attack} \leq p(1 + \frac{1}{I})$. 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. Necessary condition for no player to have a profitable attack: $p \geq \frac{V_{attack}}{1+\frac{1}{I}}$ (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 and use 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

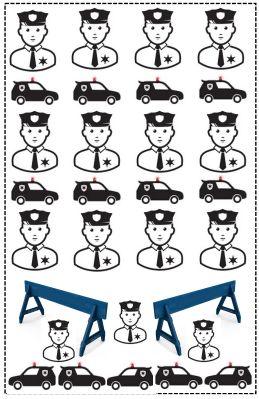
Traditional Security Model:

Traditional Security Model

Traditional Security Model:

- Security Guards

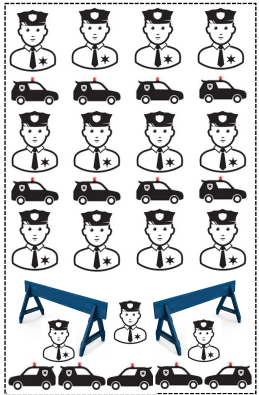
Traditional Security Model

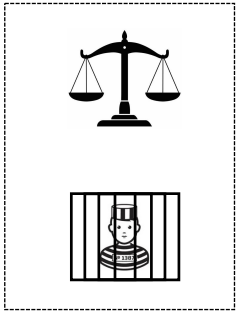


Traditional Security Model:

- 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:

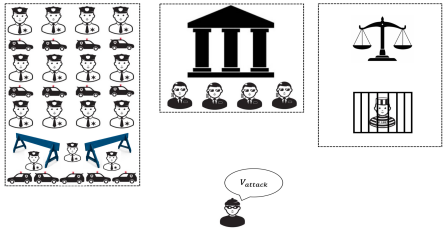
- Large amount of Security Guards
- But no additional layers (Police, Rule of Law)

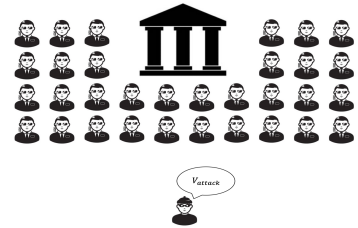
Bank Security Model

Bitcoin Security Model:

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

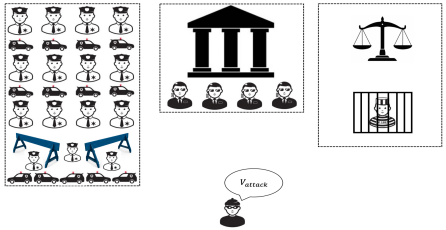
Comparison of Security Models

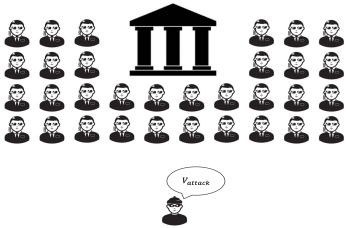




Traditional Security	Bitcoin Security
cost of overcoming guards + cost of overcoming police reinforcements + risk × punishment if caught $> V_{attack}$	cost of overcoming guards $> V_{attack}$

Comparison of Security Models



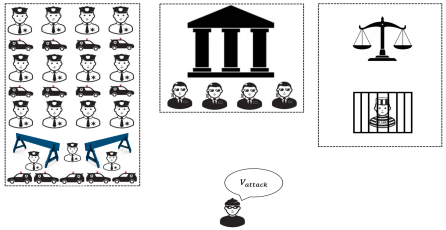


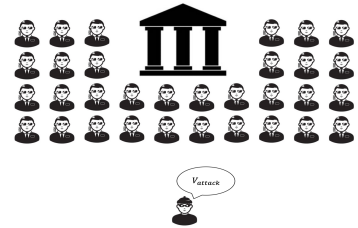
Traditional Security	Bitcoin Security
cost of overcoming guards + cost of overcoming police reinforcements + risk × punishment if caught $> V_{attack}$	cost of overcoming guards $> V_{attack}$

Key contrast:

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

Comparison of Security Models



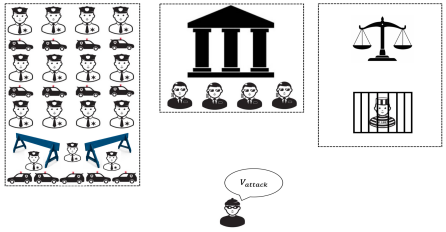


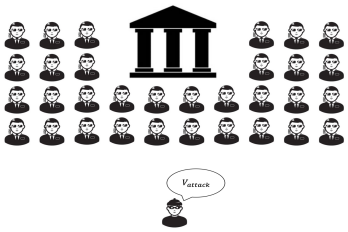
Traditional Security	Bitcoin Security
cost of overcoming guards + cost of overcoming police reinforcements + risk × punishment if caught $> V_{attack}$	cost of overcoming guards $> V_{attack}$

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

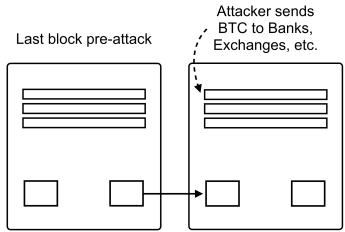


Illustration of Double Spending

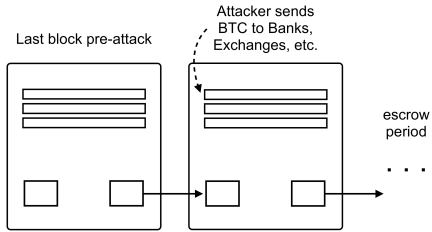


Illustration of Double Spending

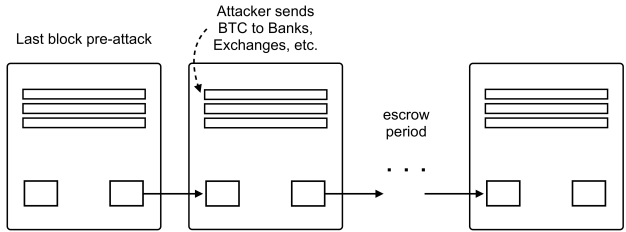


Illustration of Double Spending

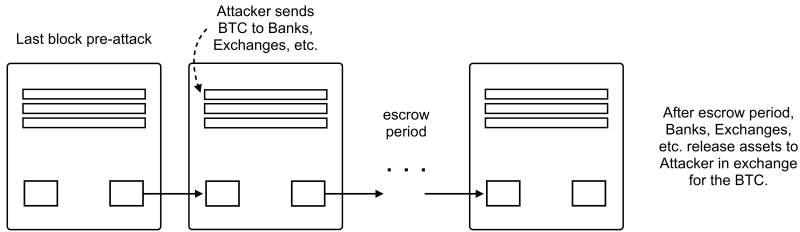


Illustration of Double Spending

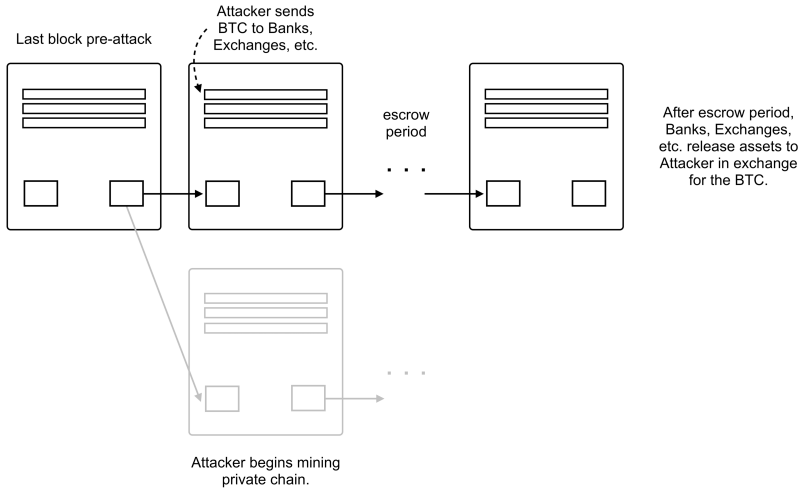


Illustration of Double Spending

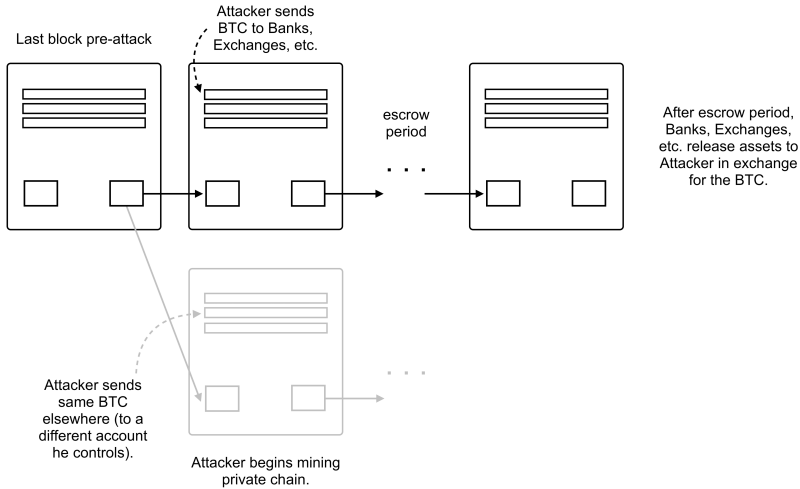


Illustration of Double Spending

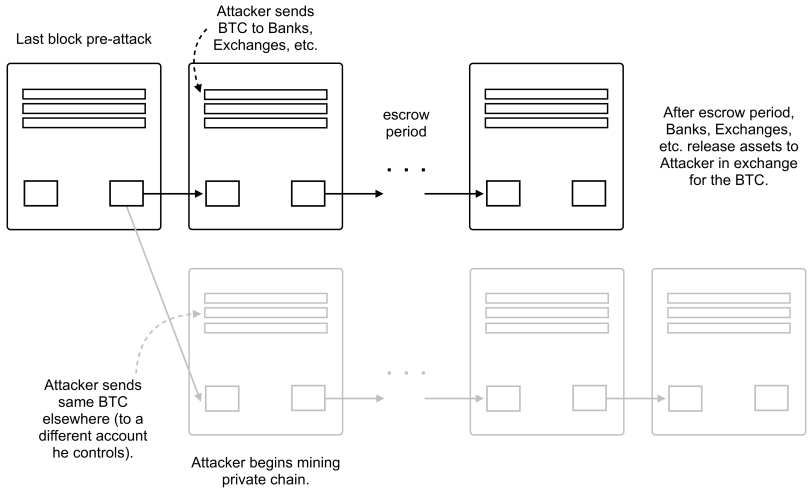
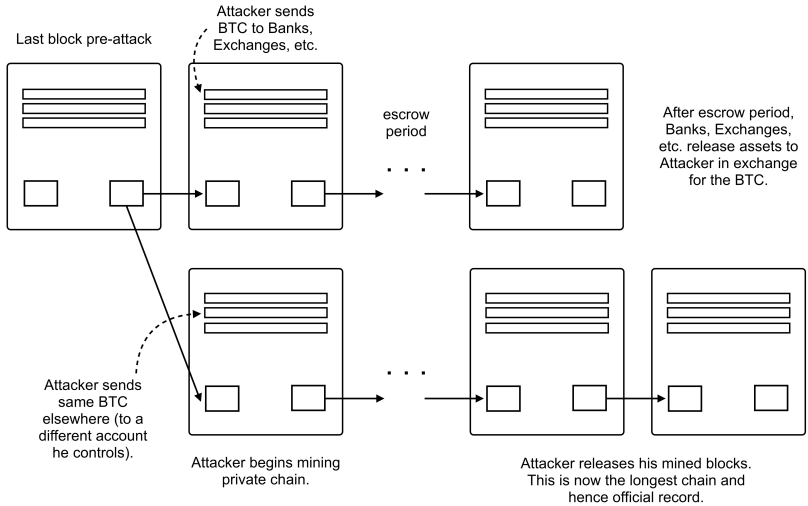


Illustration of Double Spending



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. Then will consider a range informed by the computations.

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 will consider a range informed by the computations.
- Then ask: how big need p_{block} be for a given desired amount to secure, V_{attack}

Double Spending: Attack Duration in Closed Form

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

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

Double Spending: Attack Duration in Closed Form

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

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

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

Double Spending Attack: Simulation Details I

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

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

Double Spending Attack: Simulation Details I

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

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

Double Spending Attack: Simulation Details II

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

	$e = 0$	$e = 1$	$e = 6$	$e = 10$	$e = 100$	$e = 1000$
$A = 1.05$	26.78	31.26	47.31	57.17	190.38	1,121.22
$A = 1.1$	14.32	16.96	26.92	33.39	138.39	1,104.45
$A = 1.2$	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: 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

For analysis I will consider:

- **Base case**: $At = 16$. Corresponds to gross costs under current escrow period and modest attacker majority. Net costs if $\kappa = 1$ and $\Delta_{attack} = 0$.
- **Expensive attack case**: $At = 150$. Corresponds to one full day of block-compute-costs.
- **Very expensive attack case**: $At = 1000$. Corresponds to 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. (Security is not 0-1, but more like a % tax).

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

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

Examples of 51% Attacks

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

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

Attacks of Crypto Financial Entities

Name	Type of Business	Date of Attack	Amount Stolen	Attack Vector
Euler Finance	Decentralized Lending Firm	January 2023	$197	Flashloan Attack + Flawed Code
Mango Market	Decentralized Exchange	October 2022	$100 million	Price Manipulation
BNB Chain	DeFi Bridge	October 2022	$568 million	Flawed Code
Wintermute	DeFi Market Maker	September 2022	$160 million	Compromised Wallet Generator
Nomad	DeFi Bridge	August 2022	$200 million	Flawed Code
Horizon Bridge	DeFi Bridge	July 2022	$100	Compromised Private Keys + Governance Control
Beanstalk Farms	DeFi Stablecoin	April 2022	$182 million	Flashloan Attack + Governance Control
Ronin Network	DeFi Bridge	March 2022	$625 million	Compromised Private Keys + Governance Control
Wormhole	DeFi Bridge	February 2022	$320 million	Flawed Code
Qubit Finance	Lending Firm	January 2022	$80	Flawed Code
BitMart	Centralized Exchange	December 2021	$150 million	Compromised Private Keys
C.r.e.a.m. Finance	DeFi Lending Protocol	October 2021	$130 million	Flashloan Attack + Price Manipulation
PolyNetwork	DeFi Bridge	August 2021	$600 million	Flawed Code
KuCoin	Centralized Exchange	September 2020	$281 million	Compromised Private Keys
BitGrail	Centralized Exchange	February 2018	$170 million	Unknown
Coincheck	Centralized Exchange	January 2018	$530 million	Unknown
The DAO	Decentralized Venture Capital	Juny 2016	$55 million	Flawed Code
Mt. Gox	Centralized Exchange	February 2014	$480 million	Compromised Private Keys

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

Attacks of Crypto Financial Entities

Name	Type of Business	Date of Attack	Amount Stolen	Attack Vector
Euler Finance	Decentralized Lending Firm	January 2023	$197	Flashloan Attack + Flawed Code
Mango Market	Decentralized Exchange	October 2022	$100 million	Price Manipulation
BNB Chain	DeFi Bridge	October 2022	$568 million	Flawed Code
Wintermute	DeFi Market Maker	September 2022	$160 million	Compromised Wallet Generator
Nomad	DeFi Bridge	August 2022	$200 million	Flawed Code
Horizon Bridge	DeFi Bridge	July 2022	$100	Compromised Private Keys + Governance Control
Beanstalk Farms	**DeFi Stablecoin**	**April 2022**	**$182 million**	**Flashloan Attack + Governance Control**
Ronin Network	DeFi Bridge	March 2022	$625 million	Compromised Private Keys + Governance Control
Wormhole	DeFi Bridge	February 2022	$320 million	Flawed Code
Qubit Finance	Lending Firm	January 2022	$80	Flawed Code
BitMart	Centralized Exchange	December 2021	$150 million	Compromised Private Keys
C.r.e.a.m. Finance	DeFi Lending Protocol	October 2021	$130 million	Flashloan Attack + Price Manipulation
PolyNetwork	DeFi Bridge	August 2021	$600 million	Flawed Code
KuCoin	Centralized Exchange	September 2020	$281 million	Compromised Private Keys
BitGrail	Centralized Exchange	February 2018	$170 million	Unknown
Coincheck	Centralized Exchange	January 2018	$530 million	Unknown
The DAO	Decentralized Venture Capital	Juny 2016	$55 million	Flawed Code
Mt. Gox	Centralized Exchange	February 2014	$480 million	Compromised Private Keys

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

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

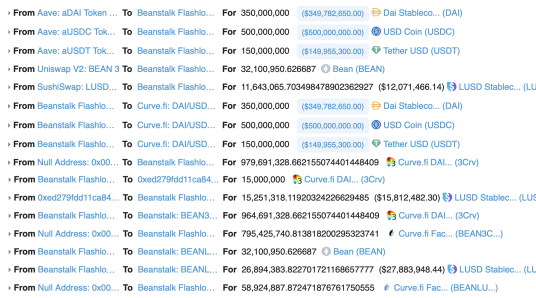
April 16th:

- 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.

Collapses of Crypto Financial Entities

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

Sources: Bloomberg, WSJ, Coinmarketcap.

Collapses of Crypto Financial Entities

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

Sources: Bloomberg, WSJ, Coinmarketcap.

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

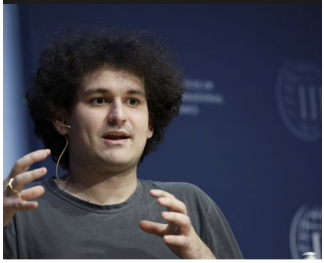
	Assets	Amount ($M)
1	DeFi	$4,483.7
2	Staking	689.6
3	Bank Balances	40.7
4	Undeployed Assets	3,276.2
5	Posted Collateral	2,232.3
6	Institutional Loans	2,241.6
7	CEL Treasury	1,752.6
8	Exchange Balances	2,390.0
9	Mining / Financial Instruments / Other	1,383.6
10	Retail Loans	542.8
11	Undeployable (Prime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

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 (at interface of Econ and CS): 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 (at interface of Econ and CS): 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?*
- (Work in progress with Andrew Lewis-Pye and Tim Roughgarden)

Theory Open Question, I

- Step 1: Define a more general economic environment that allows for proof-of-work, proof-of-stake, and potentially other consensus protocols, in which we can state the same zero-profit condition as before: $N^* c = p$
- 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

- Step 1: Define a more general economic environment that allows for proof-of-work, proof-of-stake, and potentially other consensus protocols, in which we can state the same zero-profit condition as before: $N^* c = p$
- 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

- Step 1: Define a more general economic environment that allows for proof-of-work, proof-of-stake, and potentially other consensus protocols, in which we can state the same zero-profit condition as before: $N^* c = p$
- 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

- Zero-profit condition, as before

$$N^* c = p$$

- Fixed cost of capital in zero-profit equilibrium, as before

$$N^* C$$

- Note: characterization theorems of Leshno and Strack (2020) and Chen, Papadimitriou and Roughgarden (2019) tell us that axioms that relate to strict interpretations of anonymity and decentralization imply this zero-profit condition (and hence capital stock) in this environment.
- We will also allow for protocols that don't satisfy these axioms (ex: many proof-of-stake implementations violate these papers' axioms)

Theory Open Question, I

- Step 2: All known permissionless consensus protocols are vulnerable to majority attack. We can use ideas from my paper to distinguish whether the attacks are cheap or expensive.

Theory Open Question, I

- Step 2: All known permissionless consensus protocols are vulnerable to majority attack. We can use ideas from my paper to distinguish whether the attacks are cheap or expensive.
- 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' capital is still worth C per unit ("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).

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).
- 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 $p = rNC$.
  - So equation (3) is $p \geq rV$.
  - Security is cheap, attacks are expensive.

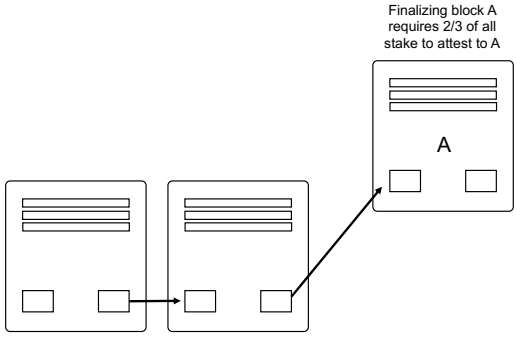
Theory Open Question, I

- Proof of stake and attacks
  - In its simplest form, proof-of-stake is vulnerable to the exact same critique as proof-of-work. Just conceptualize c as per-block opportunity cost of stake
  - But:
    - (i) stakes are locked on chain, like collateral, and
    - (ii) a stake's behavior over time is observable (i.e., non memory-less)
  - This creates possibilities for punishment that don't exist in Nakamoto proof-of-work: can confiscate stake (called "slashing")
  - Hence, proof-of-stake can make attacks more expensive

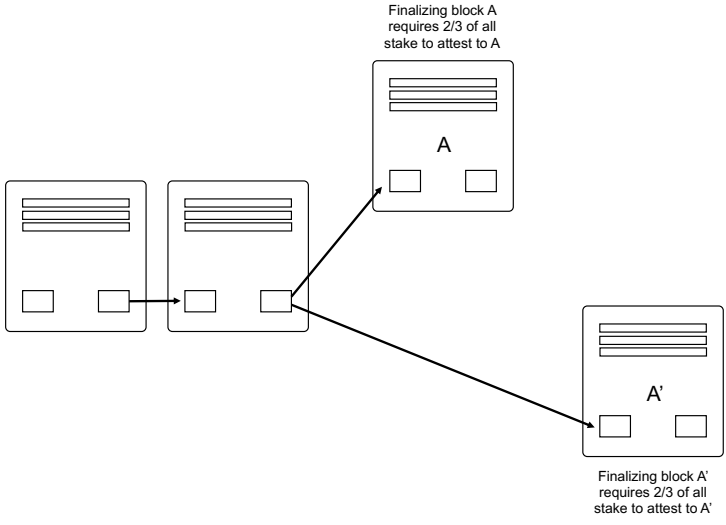
Theory Open Question, I

- Proof of stake and attacks
  - In its simplest form, proof-of-stake is vulnerable to the exact same critique as proof-of-work. Just conceptualize c as per-block opportunity cost of stake
  - But:
    - (i) stakes are locked on chain, like collateral, and
    - (ii) a stake's behavior over time is observable (i.e., non memory-less)
  - This creates possibilities for punishment that don't exist in Nakamoto proof-of-work: can confiscate stake (called "slashing")
  - Hence, proof-of-stake can make attacks more expensive
- Ethereum Proof-of-Stake + Slashing
  - 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: $\frac{1}{2}N^*C$

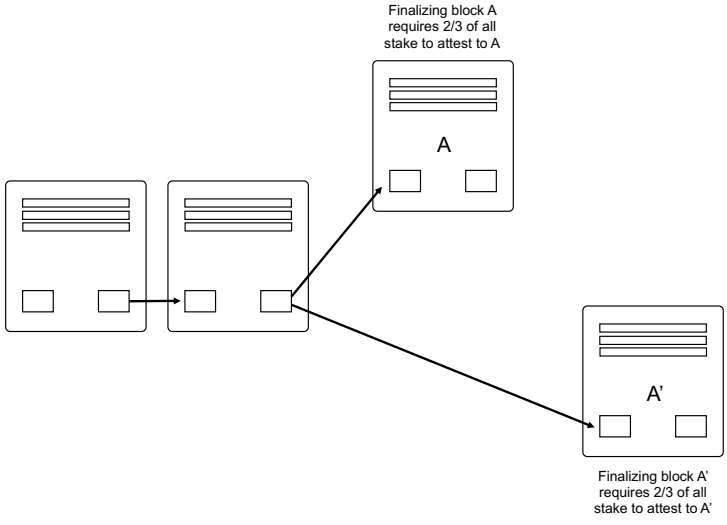
Ethereum PoS: Punishing a Double-Spend Attacker



Ethereum PoS: Punishing a Double-Spend Attacker

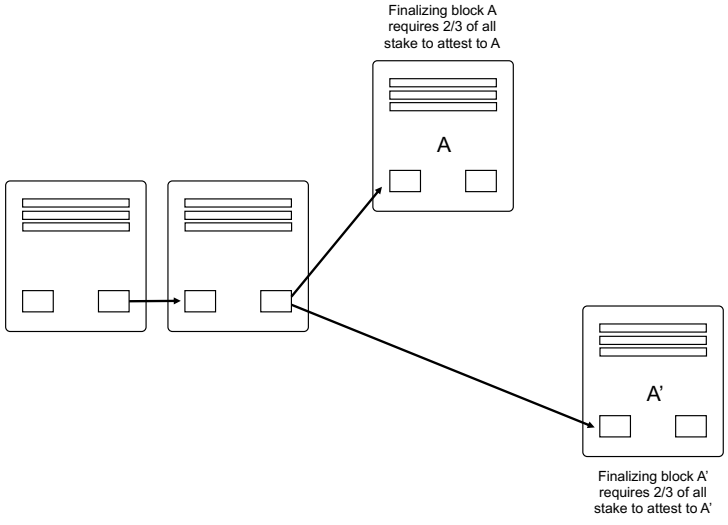


Ethereum PoS: Punishing a Double-Spend Attacker



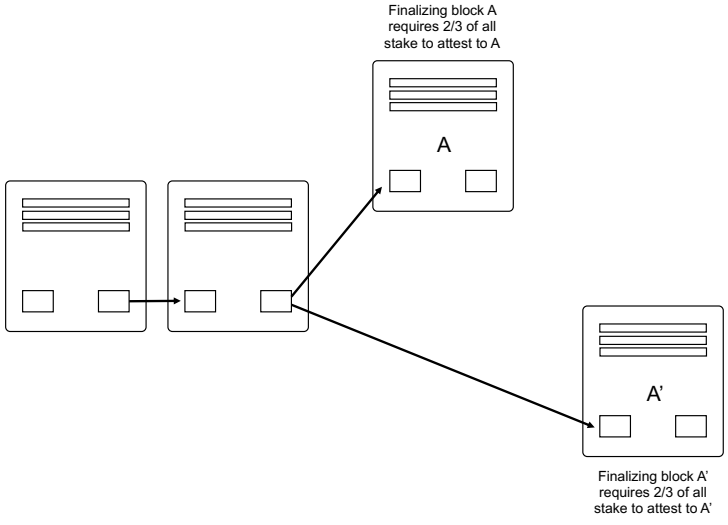
- Therefore, at least 1/3 of all stake signed both A and A'

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

- Note the key contrast
  - Bitcoin collapse model: All ASICs have to lose their value for the attack to cost $O(N^* C)$. Hence, attack is expensive only with collapse. (Lewis-Pye, Roughgarden and Budish prove that this negative result holds for a class of protocols that includes Bitcoin's, called "dynamically available protocols")
  - Ethereum PoS model: Confiscate just the attacker's stake. Hence don't need implicit assumption of collapse for security.

Theory Open Question, I

- Note the key contrast
  - Bitcoin collapse model: All ASICs have to lose their value for the attack to cost $O(N^*C)$. Hence, attack is expensive only with collapse. (Lewis-Pye, Roughgarden and Budish prove that this negative result holds for a class of protocols that includes Bitcoin's, called "dynamically available protocols")
  - Ethereum PoS model: Confiscate just the attacker's stake. Hence don't need implicit assumption of collapse for security.
- This is great ... Ethereum PoS successfully makes double-spending attacks "expensive"
- Problem: creates a new issue not faced by Nakamoto consensus: "liveness attacks"
  - Since need $\frac{2}{3}$ of all stake to sign any transaction
  - Attacker can ground Ethereum to a halt for a long period of time
- Do you confiscate this attacker too?
  - Issue: how do you distinguish between "liveness attack" and an honest network outage
  - Hence, Ethereum hesitant to punish silent stake quickly

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.
- Additional tension:
  - If slash silent stakes fast, then honest participants will need backup systems to be robust to systems outages
  - But using backup systems raises risk of accidentally signing conflicting transactions ... and getting slashed for that!
  - (Slashing is controversial, this discussion gives sense of why)

How Ethereum Proof-of-Stake Tries to Solve the Problem

	Bitcoin Proof-of-Work	Ethereum Proof-of-Stake
Capital	Computer hardware off chain (i.e., in the physical world)	Crypto coins locked on chain ("stake")
Consensus Mechanism	Longest-Chain Proof-of-Work. Single explicit validator per block. (Whoever solves the computational puzzle builds/signs the block. Others signal their implicit consent by moving on to next block.)	BFT-Style Consensus, Proof-of-Stake. All stake explicitly votes on all blocks. (Proposer is random. 2/3 majority of stake must explicitly sign to confirm a block.)
On-Chain Punishment System	No.	Yes. Double-Spend Attacks: ▶ If stake signs conflicting transactions → algorithmically confiscated. Liveness-Denial Attacks: ▶ If stake does not sign any transactions → algorithmically confiscated.
Network Reliability Assumption	None.	Assumes high network reliability: ▶ Need 2/3 of stake to sign all blocks → else, vulnerable to double spends. ▶ Need to be able to punish silent actors → else, vulnerable to liveness-denial attacks.
Risk of Punishment of Honest Actors	N/A	Software bug: confiscate capital of an accidental conflicting signature. Network outage: confiscate capital of stake with a network outage. (Note: these are related. Network robustness requires backup systems which can create conflicts.)

Theory Open Question, II

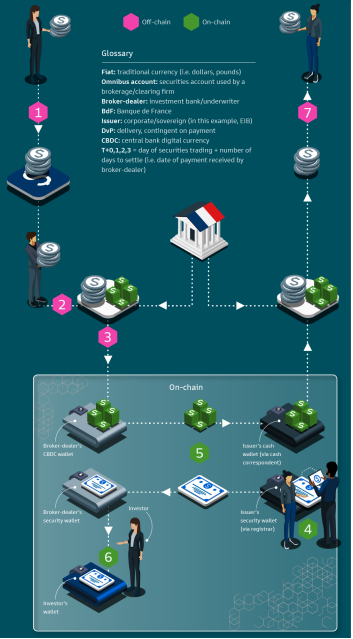
- Computer scientists unimpressed with “permissioned blockchain” / “distributed ledger”
  - “Just a database”
  - Nothing intellectually new from a CS perspective

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.

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

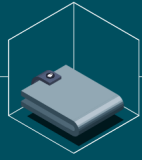
First ever multi-dealer digital issuance

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 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 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

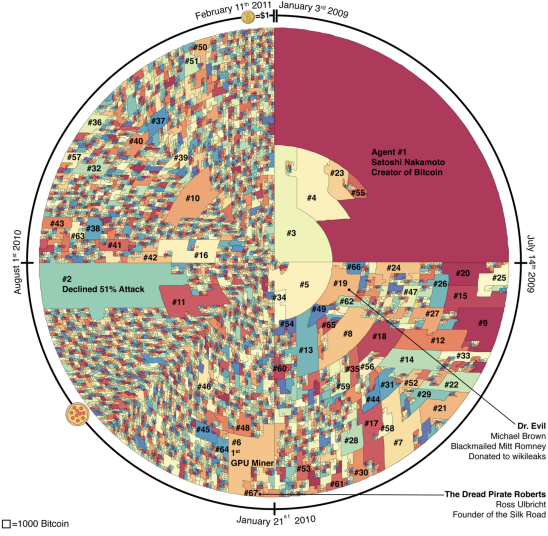
Bubble Formation

- 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
- Conceptual approaches to bubble formation
  - Delong, Shleifer, Summers and Waldman (1990): bubbles can arise if noise traders follow positive-feedback investment strategies (extended in 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

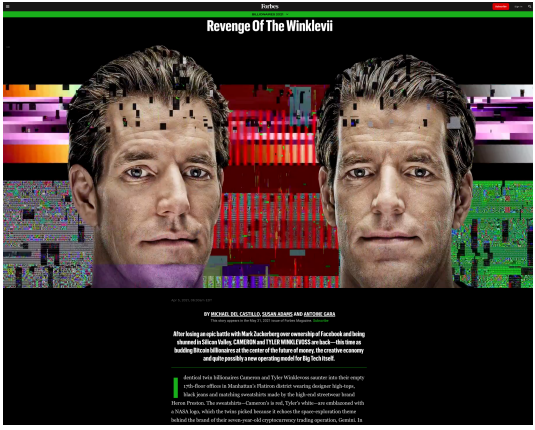
- One specific topic: crypto seems a fascinating laboratory through which to study bubbles
- Key observation here: it's a bubble either way!
  - Whether it persists or collapses!
  - At least in the narrow sense of price $>>$ NPV of cash flows
- Conceptual approaches to bubble formation
  - Delong, Shleifer,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

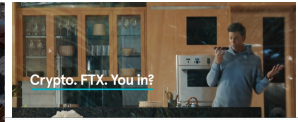


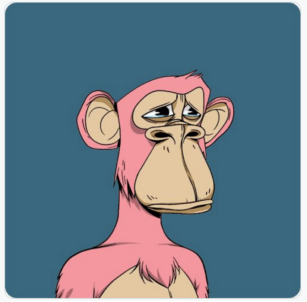
Source: Blackburn et al., 2022, "Cooperation among an anonymous group protected Bitcoin during failures of decentralization"

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.
- Overall message: there are intrinsic economic limits to how economically important crypto can become. (Unless there is a further breakthrough)

The Friendly Colleague

Alex Imas
@alexolmas

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

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

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

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

The Economic Limits of Bitcoin and the Blockchain*†

Eric Budish‡

June 5, 2018

Abstract

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

10:58 AM · May 14, 2022

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

The Friendly Colleague

Alex Imas
@alexolmas

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

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

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

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

The Economic Limits of Bitcoin and the Blockchain*†

Eric Budish‡

June 5, 2018

Abstract

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

10:58 AM · May 14, 2022

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

The Bitcoin Community

Pedro 🚀
@pedromvpg

Replying to @alexoimas

Have fun staying poor

4:51 PM · May 15, 2022

Pomp 🌪️
@APompliano

Replying to @alexoimas

Sir, too much school is bad for thinking skills

5:29 PM · May 14, 2022

Dr Tufty Sylvestris
@tuftythecat

Replying to @alexoimas

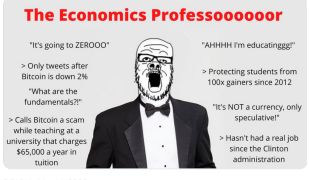
TL;DR: Bitcoin incentives work in the real world, but don't work in Budish's theoretical world, therefore the real world must be wrong. QED.

12:02 PM · May 16, 2022

Cantillionaire Disrespecter
@ToxicBitcoiner

Replying to @alexoimas

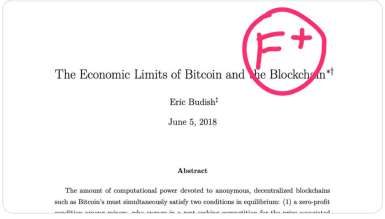
Fucking morons



8:51 PM · May 14, 2022

Peter McCormack
@PeterMcCormack

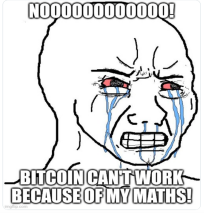
Replying to @alexoimas



7:40 PM · May 14, 2022

J. Gett, BTC Psychopath
@jgetttctc

Replying to @alexoimas



13% Monetary Mulligan
@MichaelPasture

Replying to @alexoimas

1:46 AM · May 15, 2022

Bitcoin Bergkamp
@BergkampBitcoin

Replying to @alexoimas

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

6:47 PM · May 14, 2022

Shayne in the Blockchayne
@ShayneOnChayne

Replying to @alexoimas

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

6:35 PM · May 14, 2022

Ari Paul
@AriDavidPaul

Replying to @alexoimas

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

6:27 AM · May 15, 2022

Darin Feinstein
@DarinFeinstein

Replying to @DarinFeinstein and @alexoimas

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

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

6:23 PM · May 14, 2022

The Wise Son

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

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

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

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

The Wise Son

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

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

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

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

- Nathan Budish, June 2022:

The Wise Son

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

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

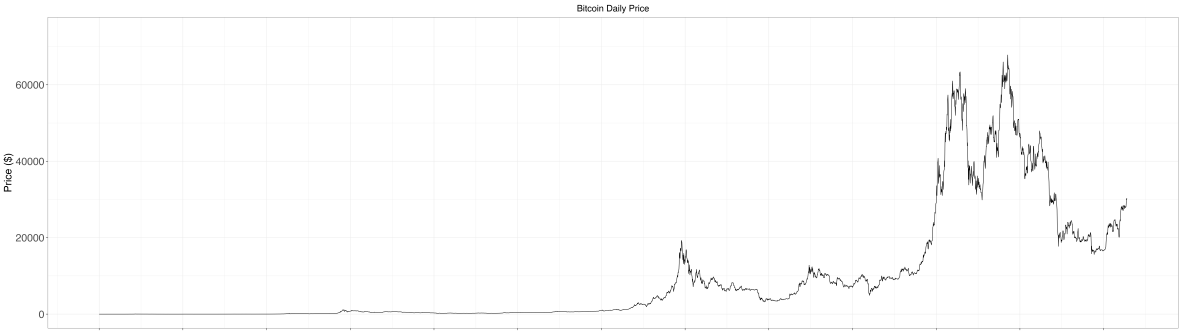
- U.S. SEC Chair, Gary Gensler, in Aug. 2021:

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

- Nathan Budish, June 2022:

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

Backup: Bitcoin Price



Backup: Bitcoin Price