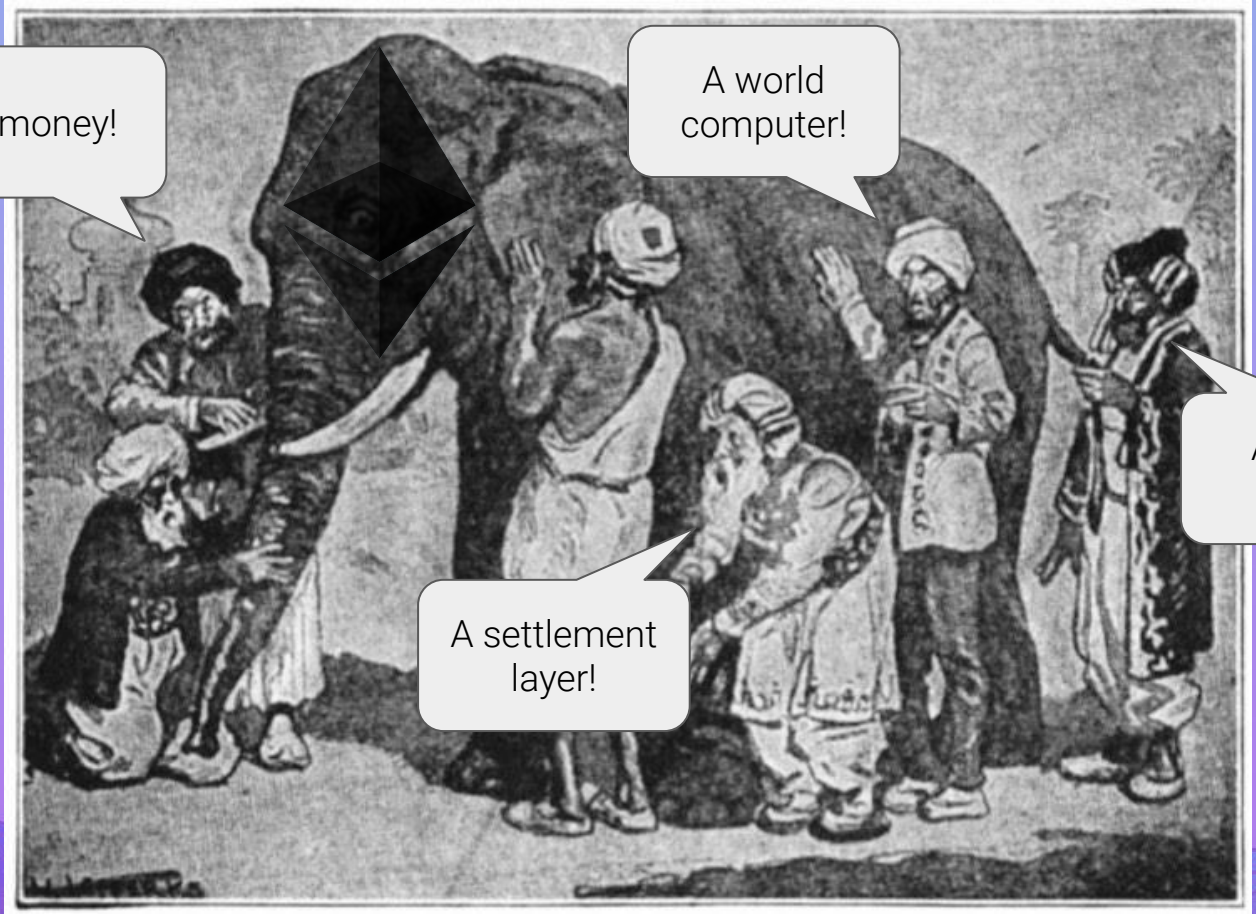
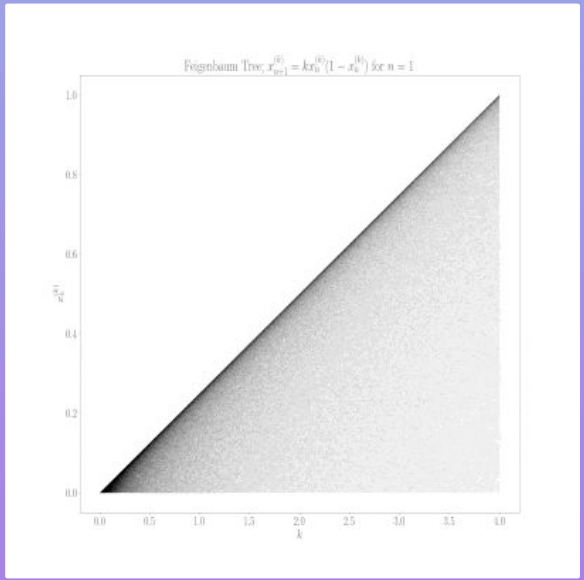
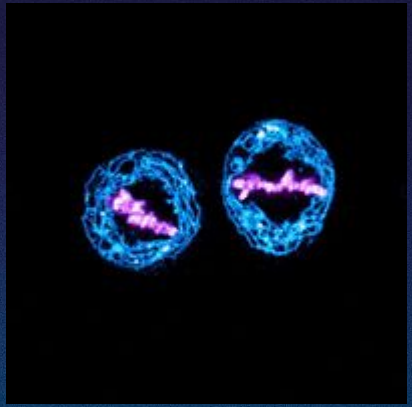
The Shape of Protocols to Come

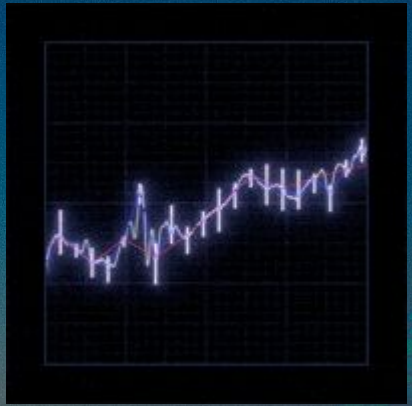
Tim Beiko

Ethereum Foundation


It's money!
A world computer!
A digital nation!
A settlement layer!

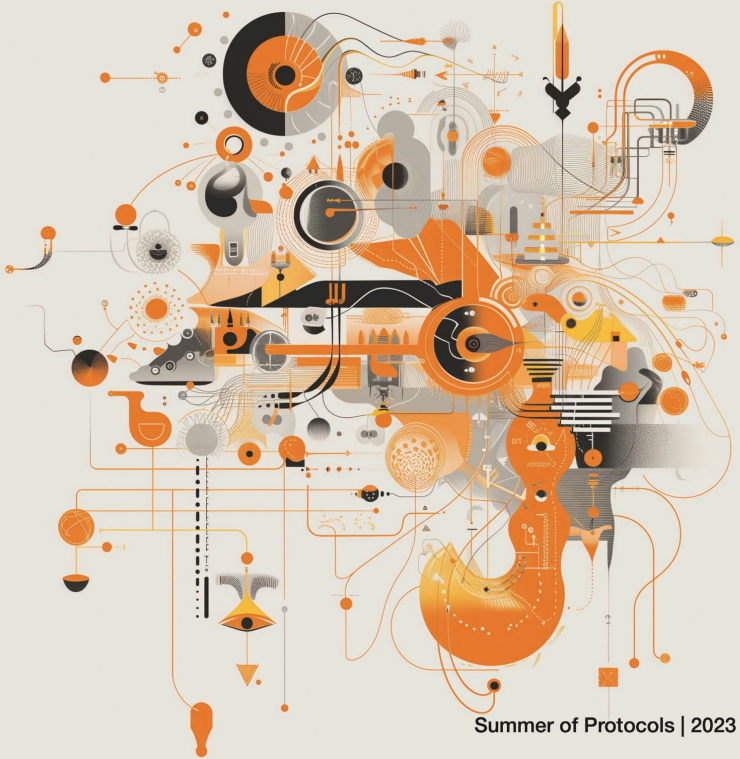

Feigenbaum Tree: $x_{n+1}^{(k)} = kx_n^{(k)}(1 - x_n^{(k)})$ for $n = 1$
1.0
0.8
0.6
0.4
0.2
0.0
$x_n^{(k)}$
0.0
0.5
1.0
1.5
2.0
2.5
3.0
3.5
4.0
k





The Unreasonable Sufficiency of Protocols

Venkatesh Rao, Tim Beiko, Danny Ryan, Josh Stark, Trent Van Epps, and Bastian Aue

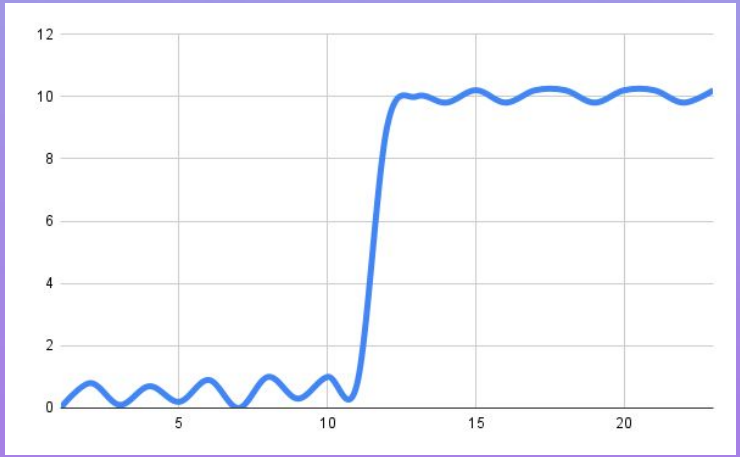


Summer of Protocols | 2023

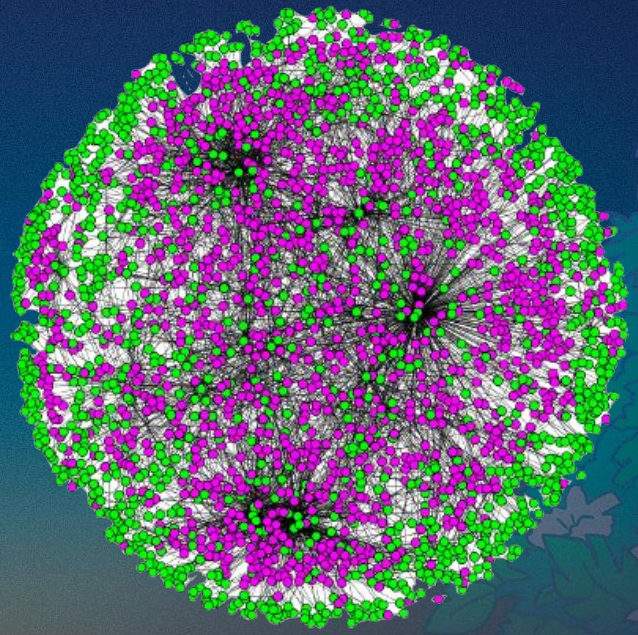
Summer of Protocols

the shape of protocols

Slow Adoption

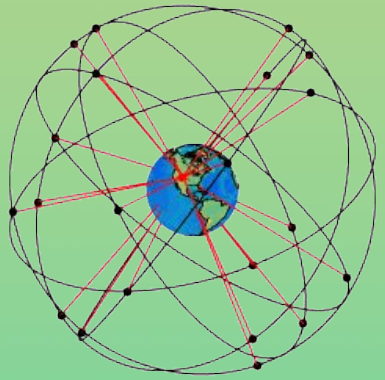


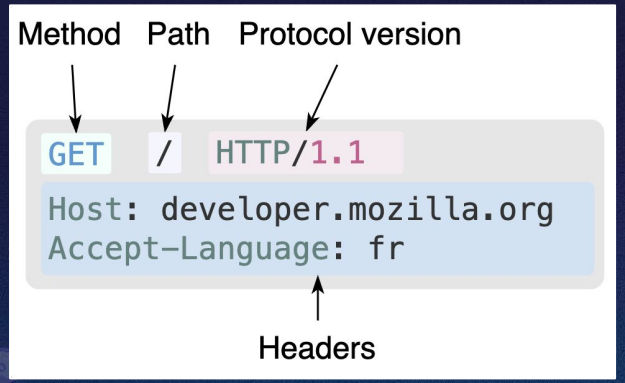
Entrenched Persistence

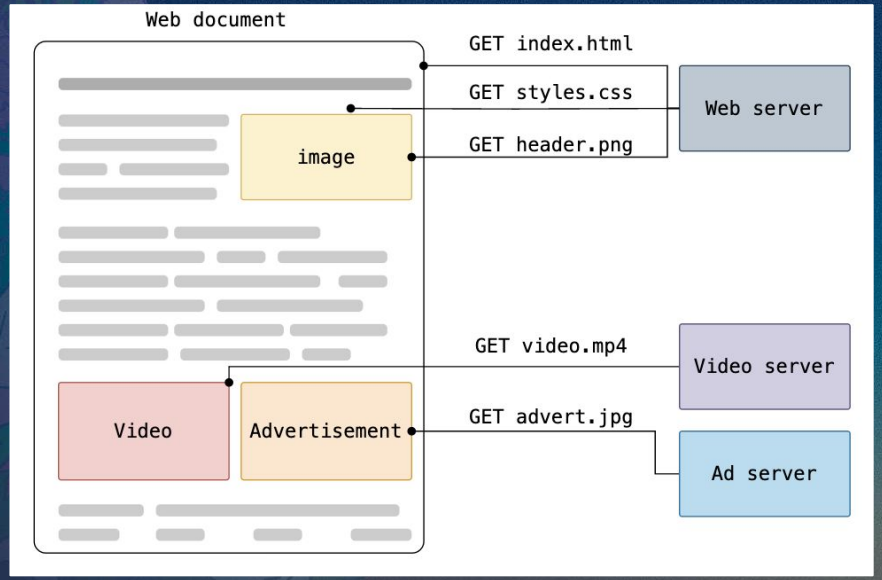


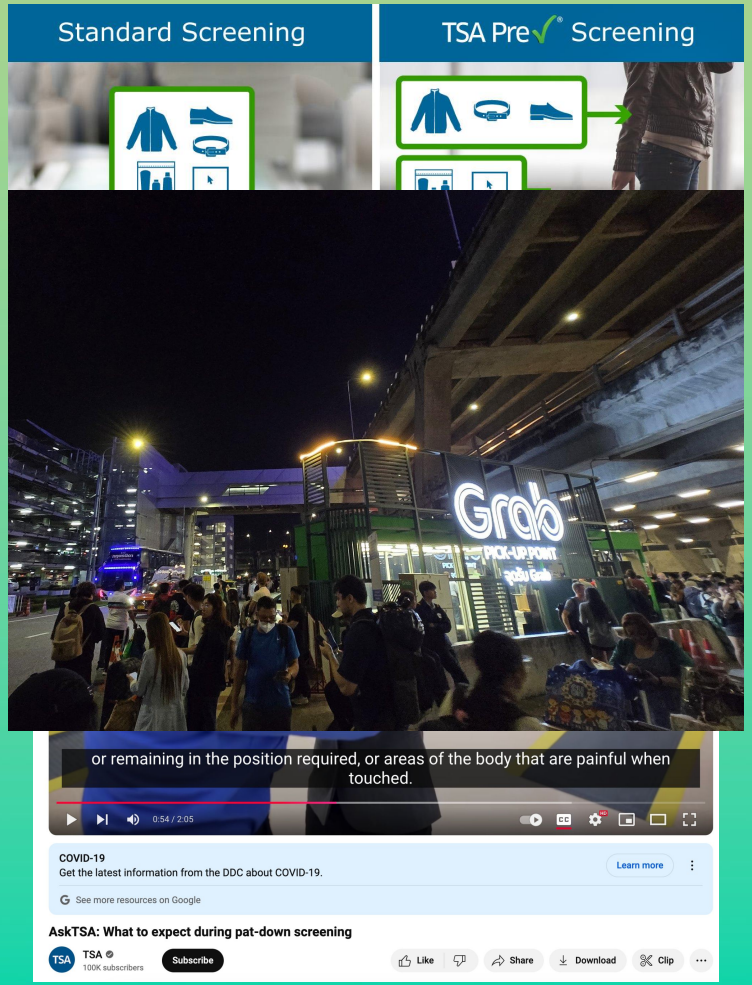
Whitehead Advances

“Civilization advances by extending the number of important operations which we can perform without thinking of them.”




Method
Path
Protocol version
GET / HTTP/1.1
Host: developer.mozilla.org
Accept-Language: fr
Headers


Web document
GET index.html
GET styles.css
GET header.png
Web server
image
GET video.mp4
Video server
Video
Advertisement
GET advert.jpg
Ad server


Standard Screening
TSA Pre✓® Screening
Grab
PICK-UP POINT
or remaining in the position required, or areas of the body that are painful when touched.
0:54 / 2:05
COVID-19
Get the latest information from the DDC about COVID-19.
Learn more
See more resources on Google
AskTSA: What to expect during pat-down screening
TSA
100K subscribers
Subscribe
Like
Share
Download
Clip

Kafka Index

Evaluative criteria for identifying bad protocols

- ☐ **No (or hidden) feedback loop**
  - ☐ Lack of consequences for failed outcomes
  - ☐ Outcomes aren't visible to participants
  - ☐ No evaluative metrics, or wrong metrics prioritized
- ☐ **Too many edge cases addressed at once**
  - ☐ Binary success response; participant required to pass through all use cases sequentially
  - ☐ No branching or forking of use cases
- ☐ **No happy path to follow**
  - ☐ Protocol increases the number of decisions that participant must make
  - ☐ User error is possible (multiple ways to "plug it in")
- ☐ **Success outcomes are randomized or ambiguously defined**
  - ☐ Outcomes succeed or fail inexplicably, even when all inputs appear to be the same
  - ☐ Outcomes can't be debugged or explained retrospectively by participants
- ☐ **Multiple protocols exist that attempt to solve the same problem**
  - ☐ Redundant protocols create conflict and confusion regarding the desired outcome
- ☐ **Recursive, nested protocols**
  - ☐ Protocol's complexity is sprawling, with multiple dead ends
  - ☐ Participants can get trapped in endless loops or "whirlpools" with no resolution
- ☐ **No market or alternatives exist**
  - ☐ High cost to participate, with no other options available
  - ☐ Significant costs incurred if participants defect

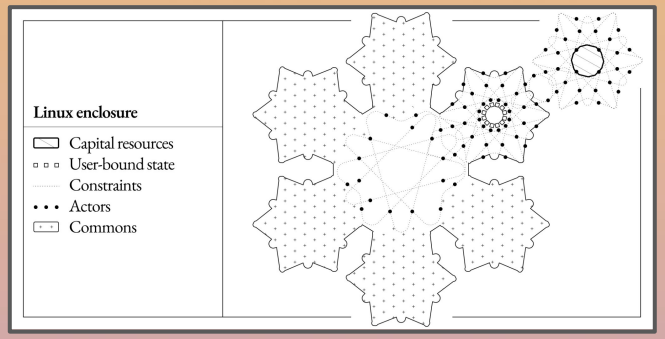
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves 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. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Ethereal Commons

- Collectively held
- Overuse & capture risk
- Need strong stewardship



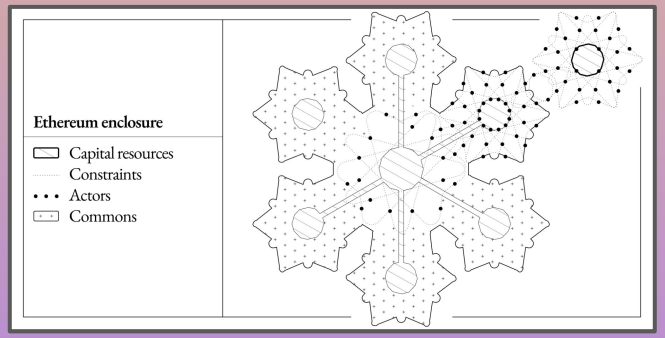
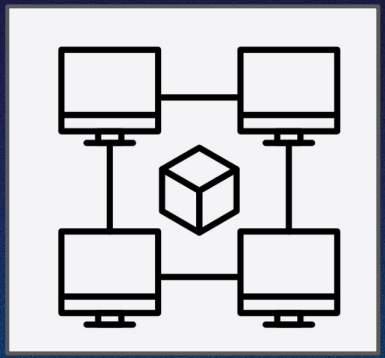


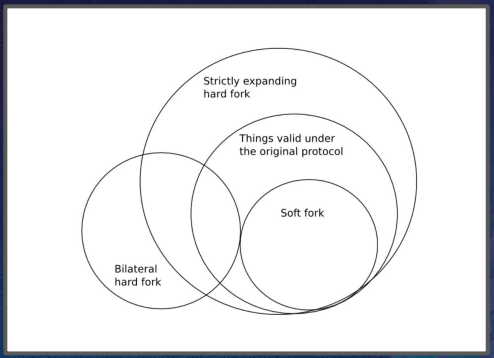
Table 1. Mining Safety Protocols

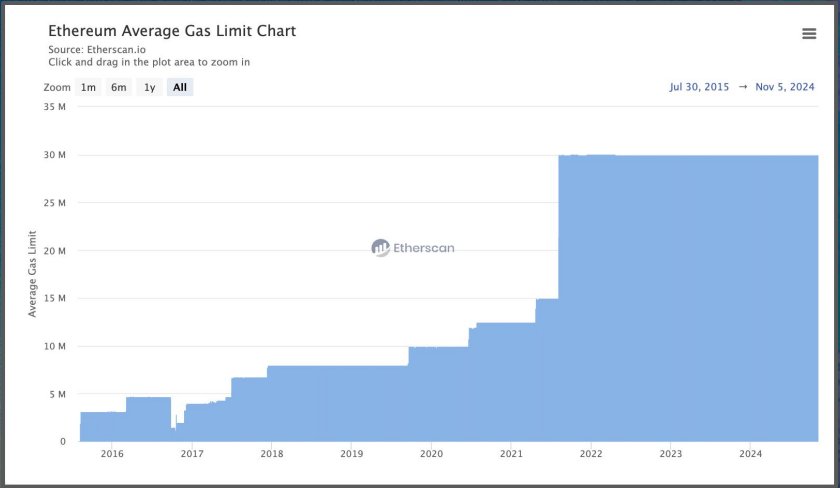
Mining safety protocol	Individual benefit	Emergent group benefit
Group meeting and risk review before entering mines	Increased knowledge of risks and how to avoid them	Reduced chance of one member compromising group safety
Annual Mine Emergency Response Development exercise	Faster and better response to well-known types of mining emergencies	Reduces the total harm in the case of an emergency
Reporting workplace accidents and near misses	Root cause of the incident is fixed	Enhanced ability to allocate investments
Proactively alerting coworkers of your presence by flashing high beams at mine shaft intersections	Many potential accidents (collision, exposure) are averted	Operations are uninterrupted due to lost time
Using signs to indicate the presence of a hazard	Worker can rely less on memory	First-timers know to avoid area
Rotating inspection and monitoring duties	Workers spend less time on cognitively draining tasks	Performance goes up as a result of heightened attentiveness

Conflict

- How do protocols differ from other concepts like grammar, APIs, standards?
- Protocols are designed to mediate conflict, internally and externally







2022 “Protocol” Definition

“a stratum of codified behavior that allows for the construction or emergence of complex coordinated behaviors at adjacent loci”

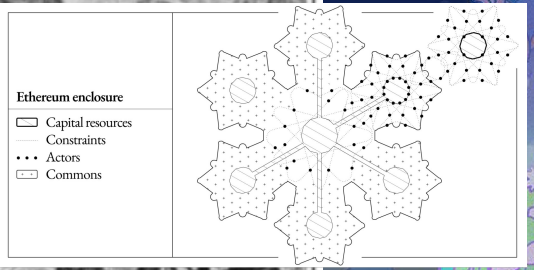
2024 “Protocol” Definition

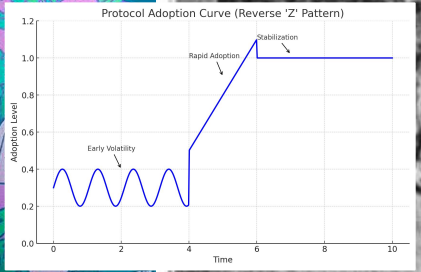
“engineered arguments”

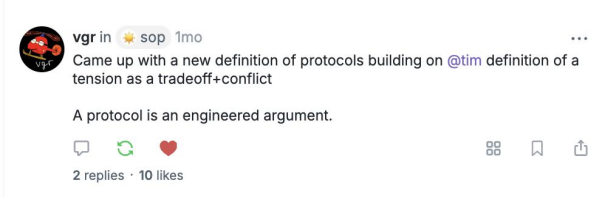
Kafka Index

Evaluative criteria for identifying bad protocols

- ☐ **No (or hidden) feedback loop**
  - ☐ Lack of consequences for failed outcomes
  - ☐ Outcomes aren't visible to participants
  - ☐ No evaluative metrics, or wrong metrics prioritized
- ☐ **Too many edge cases addressed at once**
  - ☐ Binary success response; participant required to pass through all use cases sequentially
  - ☐ No branching or forking of use cases
- ☐ **No happy path to follow**
  - ☐ Protocol increases the number of decisions that participant must make
  - ☐ User error is possible (multiple ways to "plug it in")
- ☐ **Success outcomes are randomized or ambiguously defined**
  - ☐ Outcomes succeed or fail inexplicably, even when all inputs appear to be the same
  - ☐ Outcomes can't be debugged or explained retrospectively by participants
- ☐ **Multiple protocols exist that attempt to solve the same problem**
  - ☐ Redundant protocols create conflict and confusion regarding the desired outcome
- ☐ **Recursive, nested protocols**
  - ☐ Protocol's complexity is sprawling, with multiple dead ends
  - ☐ Participants can get trapped in endless loops or "whirlpools" with no resolution
- ☐ **No market or alternatives exist**
  - ☐ High cost to participate, with no other options available
  - ☐ Significant costs incurred if participants defect







protocols to come

Hardness

- “the capability to make the future more certain.”
- Atoms, Institutions, Blockchains

Ethereum Hardness

- Globally homogeneous
- Independently auditable
- Permissionlessly accessible

hardened foundation

ERC20 LEADERBOARD

Tether USDT	54.91B USD
Lido Staked Ether STETH	25.51B USD
USDC USDC	25.44B USD
Wrapped stETH WSTETH	11.06B USD
Shiba Inu SHIB	10.74B USD
Wrapped Bitcoin WBTC	9.88B USD
WETH WETH	7.85B USD
Chainlink LINK	7.53B USD

NFT LEADERBOARD

CryptoPunks	2.13B USD
Bored Ape Yacht Club	0.68B USD
ENS	0.63B USD
Pudgy Penguins	0.51B USD
Chromie Squiggle by Snowfro	0.26B USD

#	NAME	RISKS	TYPE	STAGE	TOTAL VALUE LOCKED
1	Arbitrum One		Optimistic Rollup	STAGE 1	$15.15B ▲15.5%
2	Base		Optimistic Rollup OP	STAGE 0	$9.02B ▲16.5%
3	OP Mainnet		Optimistic Rollup OP	STAGE 1	$6.43B ▲15.4%
4	Mantle		Optimium OP	N/A	$1.90B ▲26.0%
5	Blast		Optimistic Rollup OP	STAGE 0	$1.53B ▲19.2%
6	Scroll		ZK Rollup	STAGE 0	$1.13B ▲16.9%
7	Linea		ZK Rollup	STAGE 0	$1.02B ▲27.0%
8	ZKsync Era		ZK Rollup	STAGE 0	$961.34M ▲20.8%
9	Starknet		ZK Rollup	STAGE 0	$766.29M ▲26.8%

hardened culture

Why do we need a hard fork?

Since September 18th (UTC) the Ethereum network has been under attack by a person or group resulting in large delays before transactions were processed. The network is currently filled with pending transactions which is causing users delays in processing their transactions. You can think of this as a denial of service (DoS) attack on the Ethereum blockchain.

anyone can kill your contract #6995

Closed ghost opened this issue on Nov 6, 2017 · 17 comments

ghost commented on Nov 6, 2017 • edited by ghost

I accidentally killed it.

https://etherscan.io/address/0x863df6bfa4469f3ead0be8f9f2aae51c91a907b4

75 4 123 64 24 52 3

Research

Ethereum is a Dark Forest

08.28.2020 | By Dan Robinson, Georgios Konstantopoulos

This is a horror story.

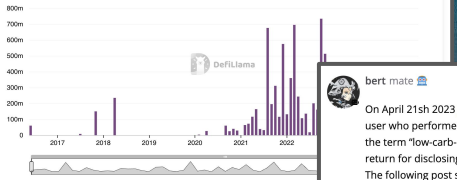
Total Value Hacked (USD)
$9.04b

Total Value Hacked in DeFi (USD)
$6.25b

Total Value Hacked in Bridges (USD)
$2.87b

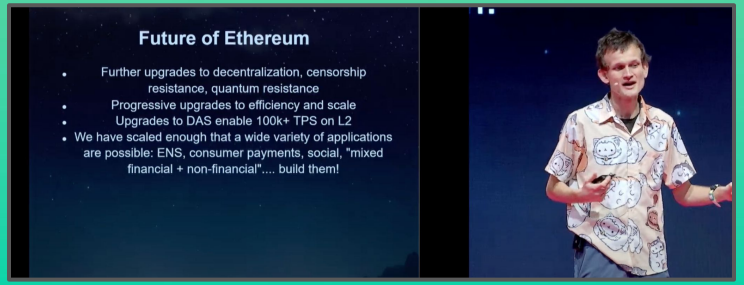
Total Value Hacked

Monthly sum



bert mate 2 Apr 2023

On April 21sh 2023 Justin Drake 34 , samczsun 25 , and myself received a disclosure from the user who performed the unbundling attack on April 3 291 . They requested that they be called the term "low-carb-crusader" instead of "sandwich the ripper" or similar nomenclature in return for disclosing details on a unique block equivocation strategy that should be mitigated. The following post shares a timeline and details of this strategy. **Flashbots relay logs confirm that the strategy was never used in production.**



hardened commons

Growing Our Impact

Launched in 2019, Gitcoin Grants is a quarterly initiative that empowers people and collectives in web
projects and causes they believe in.

While we started small, we've kept growi
goods each year.

In 2022, the amount of funding we ra
3000% higher than when we started in 2

A Flexible Design for Funding Public Goods

Vitalik Buterin
Ethereum Foundation
Zoë Hitzig
Harvard University, zhitzig@g.harvard.edu
E. Glen Weyl
Microsoft Research, glenweyl@microsoft.com

We propose a design for philanthropic or publicly-funded seeding to allow (near) optimal provision of a decentralized, self-organizing ecosystem of public goods. The concept extends ideas from Quadratic Voting to a funding mechanism for endogenous community formation. Citizens make public goods contributions to projects of value to them. The amount received by the project is (proportional to) the square of the sum of the square roots of contributions received. Under the "standard model" this mechanism yields first best public goods provision. Variations can limit the cost, help protect against collusion and aid coordination. We discuss applications to campaign finance, and highlight directions for future analysis and experimentation.

Key words: public goods, free rider problem, mechanism design

Review of Gitcoin Quadratic Funding Re

2019 Oct 24

Special thanks to the Gitcoin team and especially Frank Chen for working wi
numbers

The next round of Gitcoin Grants quadratic funding has just finished, and we the numbers for how much each project has received were just released. Here are the top ten:

Quadratic Voting *

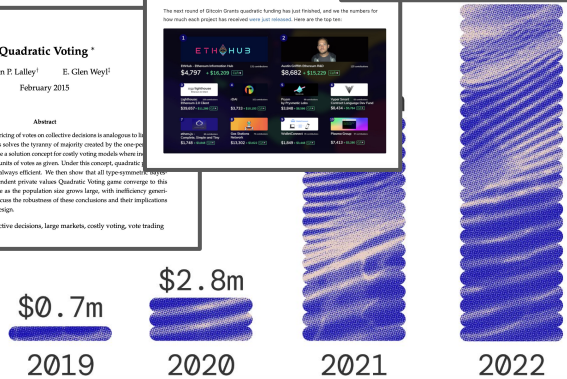
Steven P. Lalley† E. Glen Weyl‡

February 2015

Abstract

We argue that quadratic pricing of votes on collective decisions is analogous to li
ing of private goods and thus solves the tyranny of majority created by the one-pe
vote rule. To do so we propose a solution concept for costly voting models where in
take the price of influence in units of votes as given. Under this concept, quadratic
votes is the only rule that is always efficient. We then show that all type-symmetric mixed
Nash equilibria of an independent private values Quadratic Voting game converge to this efficient price-taking outcome as the population size grows large, with inefficiency generically decaying as $1/n$. We discuss the robustness of these conclusions and their implications for market and mechanism design.

Keywords: social choice, collective decisions, large markets, costly voting, vote trading



From prediction markets to info finance

2024 Nov 09

See all posts

Futarchy: Vote Values, But Bet Beliefs

by Robin Hanson

This short "manifesto" describes a new form of government. In "futarchy," we would vote on values, but bet on beliefs. Elected representatives would formally define and manage an after-the-fact measurement of national welfare, while market speculators would say which policies they expect to raise national welfare.

Democracy seems better than autocracy (i.e., kings and dictators), but it still has problems. There are today vast di
wealth among nations, and we can not attribute most of these differences to either natural resources or human abi
much of the difference seems to be that the poor nations (many of which are democracies) are those that more oft
policies, policies which hurt most everyone in the nation. And even rich nations frequently adopt such policies.

One of the Ethereum applic
me the most are prediction

augur

was an active user
look, mommy, my
ned $58,000
is year, I have been
market.

Kafka Index

Evaluative criteria for identifying bad protocols

- ☐ **No (or hidden) feedback loop**
  - ☐ Lack of consequences for failed outcomes
  - ☐ Outcomes aren't visible to participants
  - ☐ No evaluative metrics, or wrong metrics prioritized
- ☐ **Too many edge cases addressed at once**
  - ☐ Binary success response; participant required to pa through all use cases sequentially
  - ☐ No branching or forking of use cases

ath to follow

increases the number of decisions that par ke

r is possible (multiple ways to "plug it in")

tcomes are randomized or ambiguous!

s succeed or fail inexplicably, even when a pear to be the same

s can't be debugged or explained retrospe ipants

otocols exist that attempt to solve the same problem

nt protocols create conflict and confusion

the desired outcome

nested protocols

s complexity is sprawling, with multiple dead ends

nts can get trapped in endless loops or "whirlpools" esolution

- ☐ **No market or alternatives exist**
  - ☐ High cost to participate, with no other options available
  - ☐ Significant costs incurred if participants defect

#	NAME	RISKS	TYPE	STAGE	TOTAL VALUE LOCKED
1	Arbitrum One		Optimistic Rollup	STAGE 1	$15.15B - 15.5%
2	Base		Optimistic Rollup	STAGE 0	$9.02B - 16.5%
	P Mainnet		Optimistic Rollup	STAGE 1	$6.43B - 15.4%
			Optimium	N/A	$1.90B - 26.0%
			Optimistic Rollup	STAGE 0	$1.53B - 19.2%
			ZK Rollup	STAGE 0	$1.13B - 16.9%
	Linea		ZK Rollup	STAGE 0	$1.02B - 27.0%
	ZKsync Era		ZK Rollup	STAGE 0	$961.34M - 20.8%
			ZK Rollup	STAGE 0	$766.29M - 26.8%

Research

Ethereum is a Dark Forest

08.28.2020 | By Dan Robinson, Georgios Konstantopoulos

This is a horror story.

From prediction markets to info finance

2024 Nov 09 See all posts

Special thanks to Robin Hanson and Alex Tabarrok for feedback and review

One of the Ethereum applications that has always excited me the most are prediction markets. I wrote about futarchy, a model of prediction-based governance conceived by Robin Hanson, in 2014. I was an active user and supporter of Augur back in 2015 (look, mommy, my name is in the Wikipedia article!). I earned $58,000 betting on the election in 2020. And this year, I have been a close supporter and follower of Polymarket.

vgr in sop

Came up with nition of a tension as a t

A protocol is an engineered argument.

2 replies · 10 likes

thank you!