

Ethereum Protocol 101

(Pre)History, design
overview and devel

Protocol Development

Philosophy, fundamentals and ideas

Prehistory

Genesis of...
Unix philosophy
FOSS
Cryptography and Cypherpunks
Ethereum design



AT&T Archives: The UNIX Operating System

Watch on YouTube (Embed)



Play next by default:

The UNIX System: Making Computers More Productive

<https://yewtu.be/watch?v=tc4ROCJYbm0>



Free software, free society: Richard Stallman at TEDxGeneva 2014

Watch on YouTube (Embed)



Switch Invidious Instance

Play next by default: ■

<https://www.gnu.org/philosophy/free-sw.html>

https://yewtu.be/watch?v=Ag1AKII_2GM

New Directions in Cryptography

Invited Paper

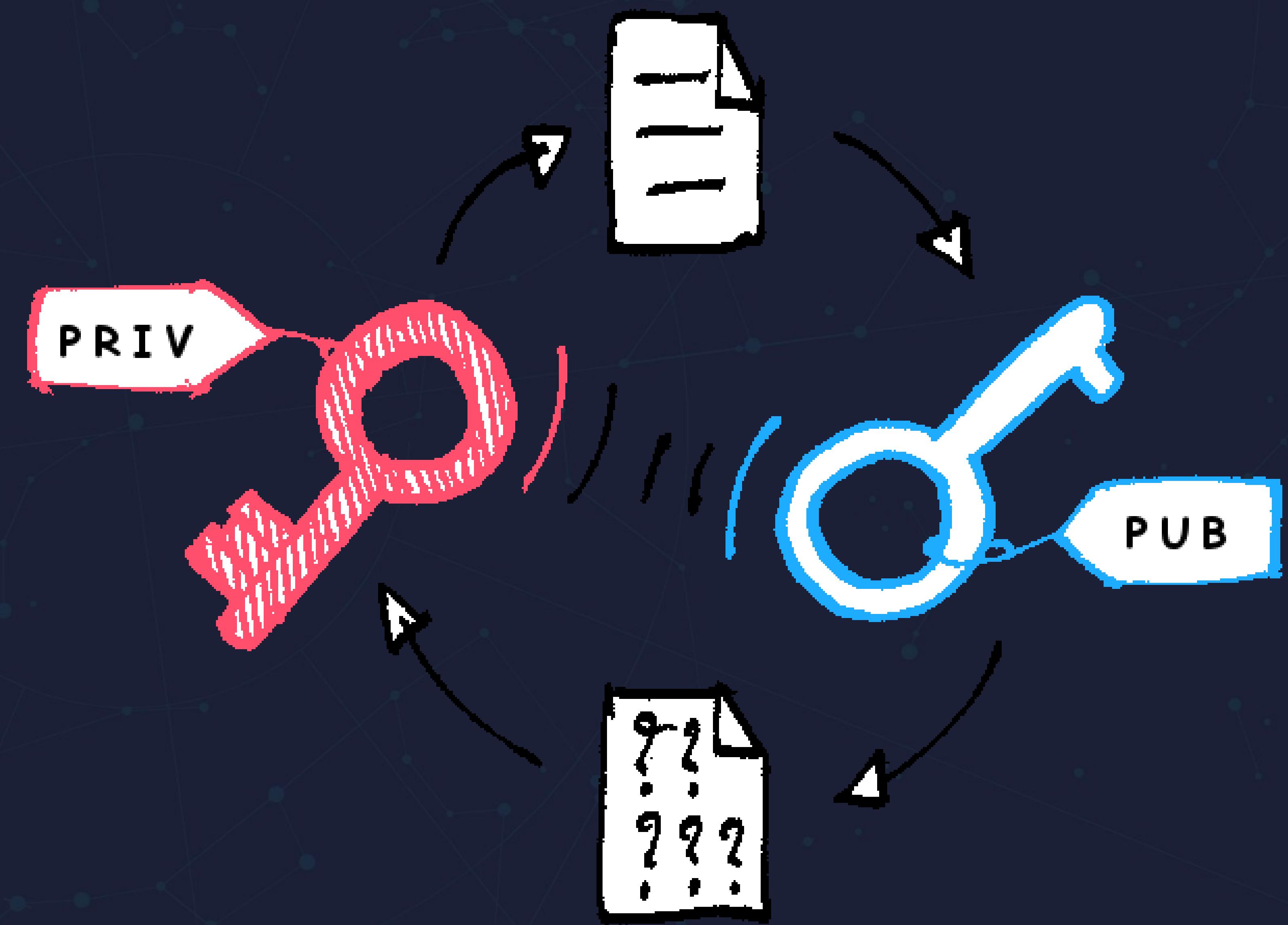
WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

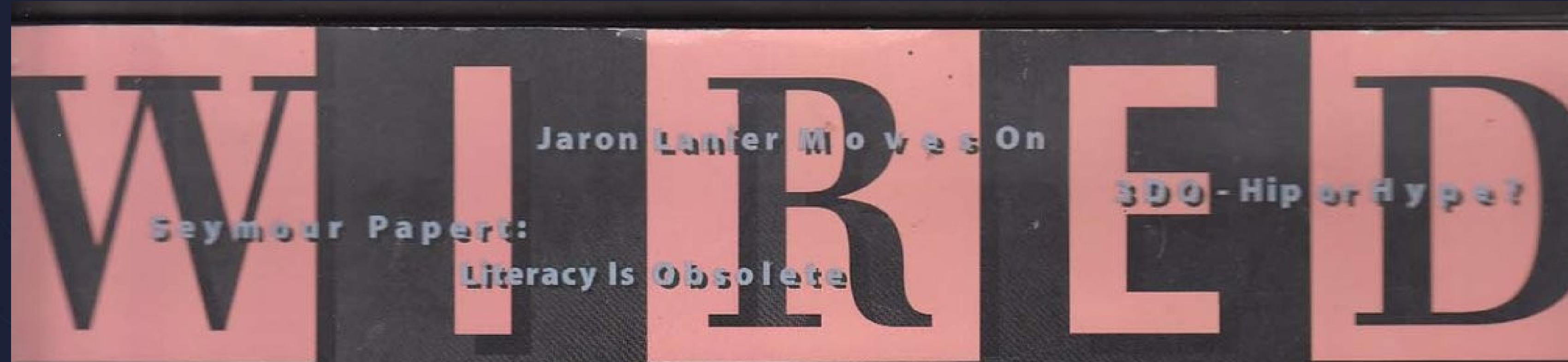
Abstract—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

I. INTRODUCTION

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of me-

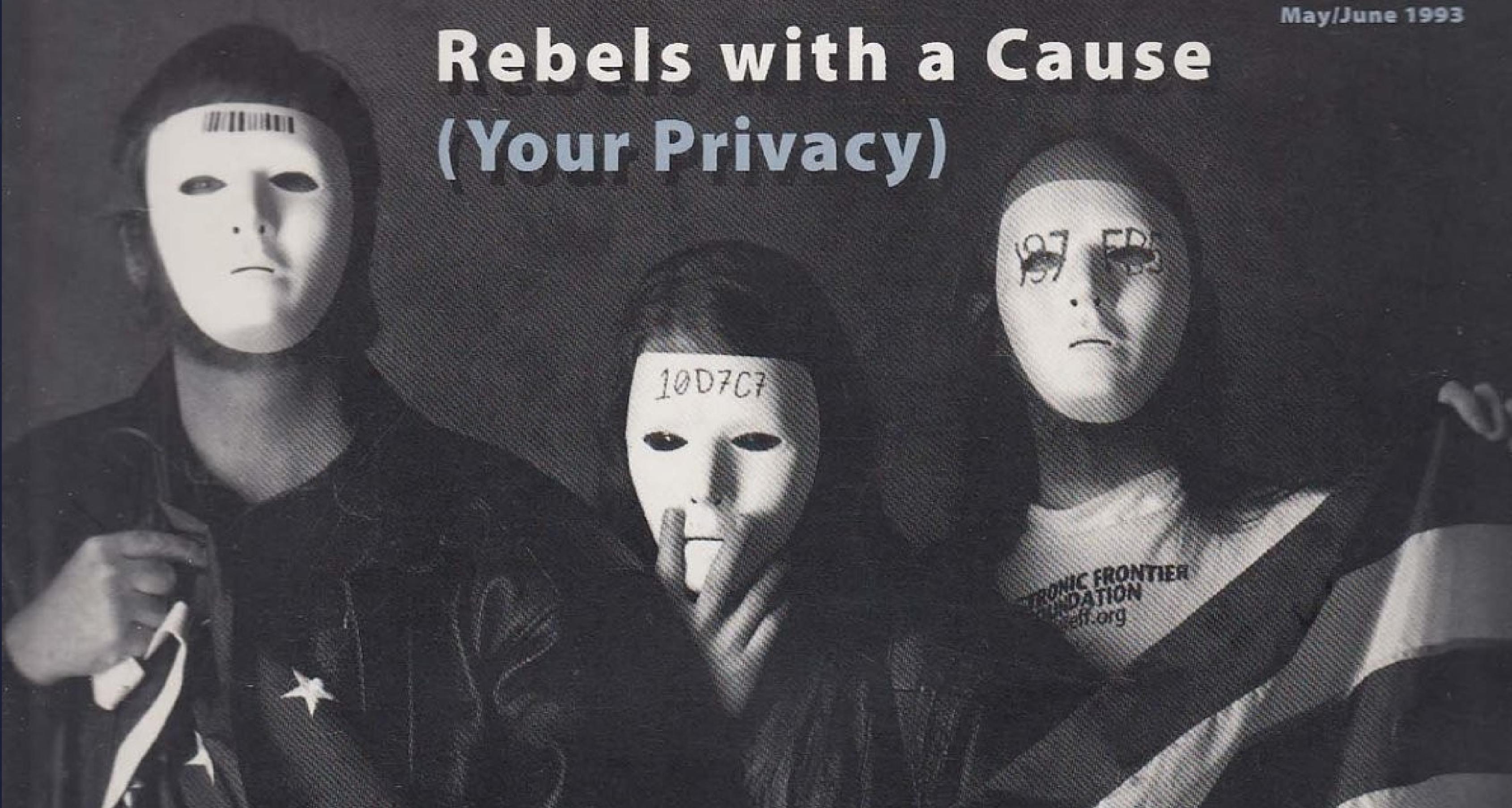
The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.





May/June 1993

Rebels with a Cause (Your Privacy)



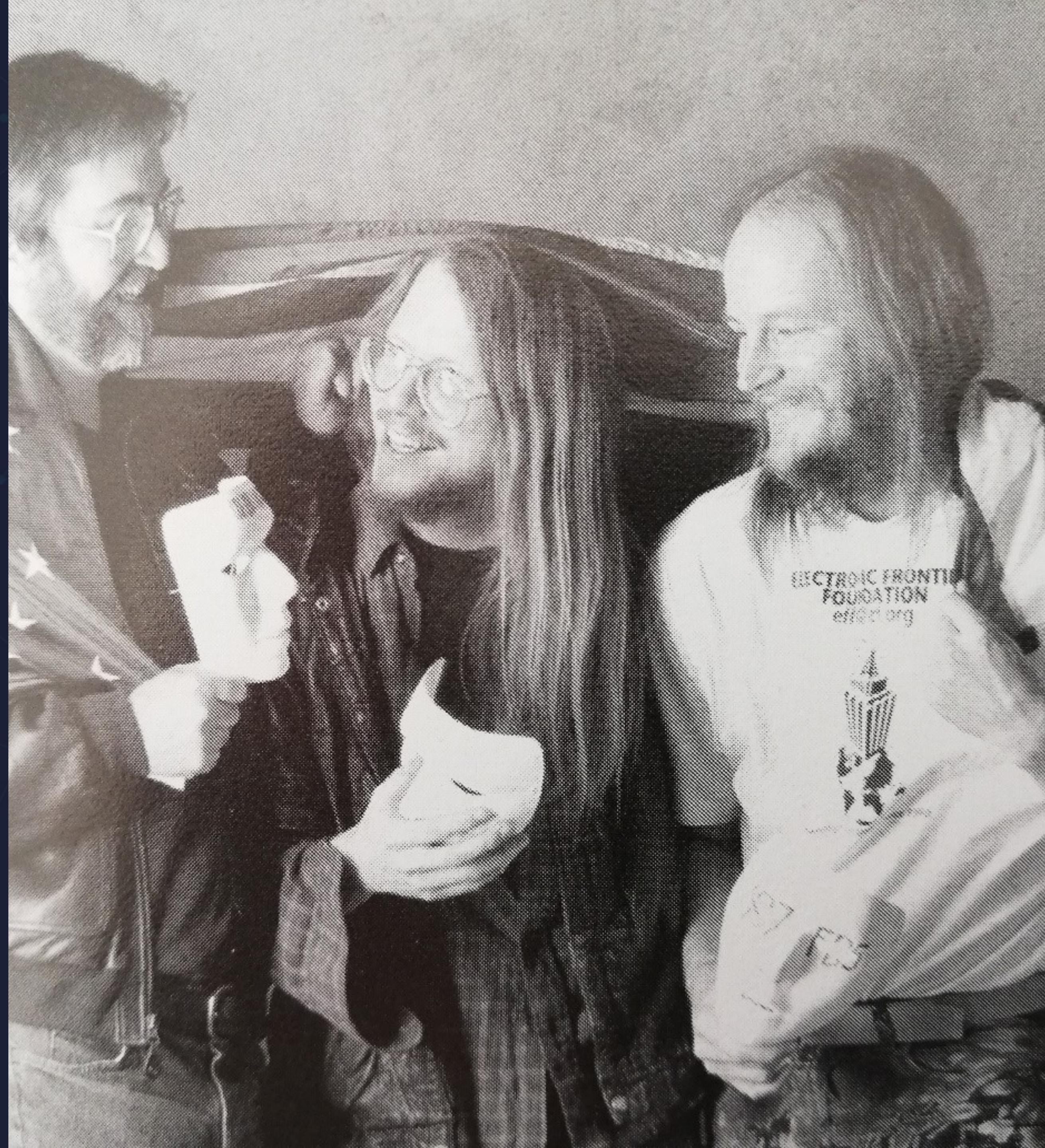
TRONIC FRONTIER
eff.org

Cypherpunks

“Cypherpunks write code... Our code is free for all to use, worldwide. We don't much care if you don't approve of the software we write. We know that software can't be destroyed and that a widely dispersed system can't be shut down.”

- Eric Hughes, Cypherpunk Manifesto, 1993

<https://activism.net/cypherpunk/manifesto.html>





Arise, you have nothing to lose but your barbed wire fences!

..

.....
Timothy C. May
tcmay@netcom.com
408-688-5409
W.A.S.T.E.: Aptos, CA
Higher Power: 2^756839

| Crypto Anarchy: encryption, digital money,
| anonymous networks, digital pseudonyms, zero
| knowledge, reputations, information markets,
| black markets, collapse of governments.
| PGP Public Key: by arrangement.

Cryptoanarchy

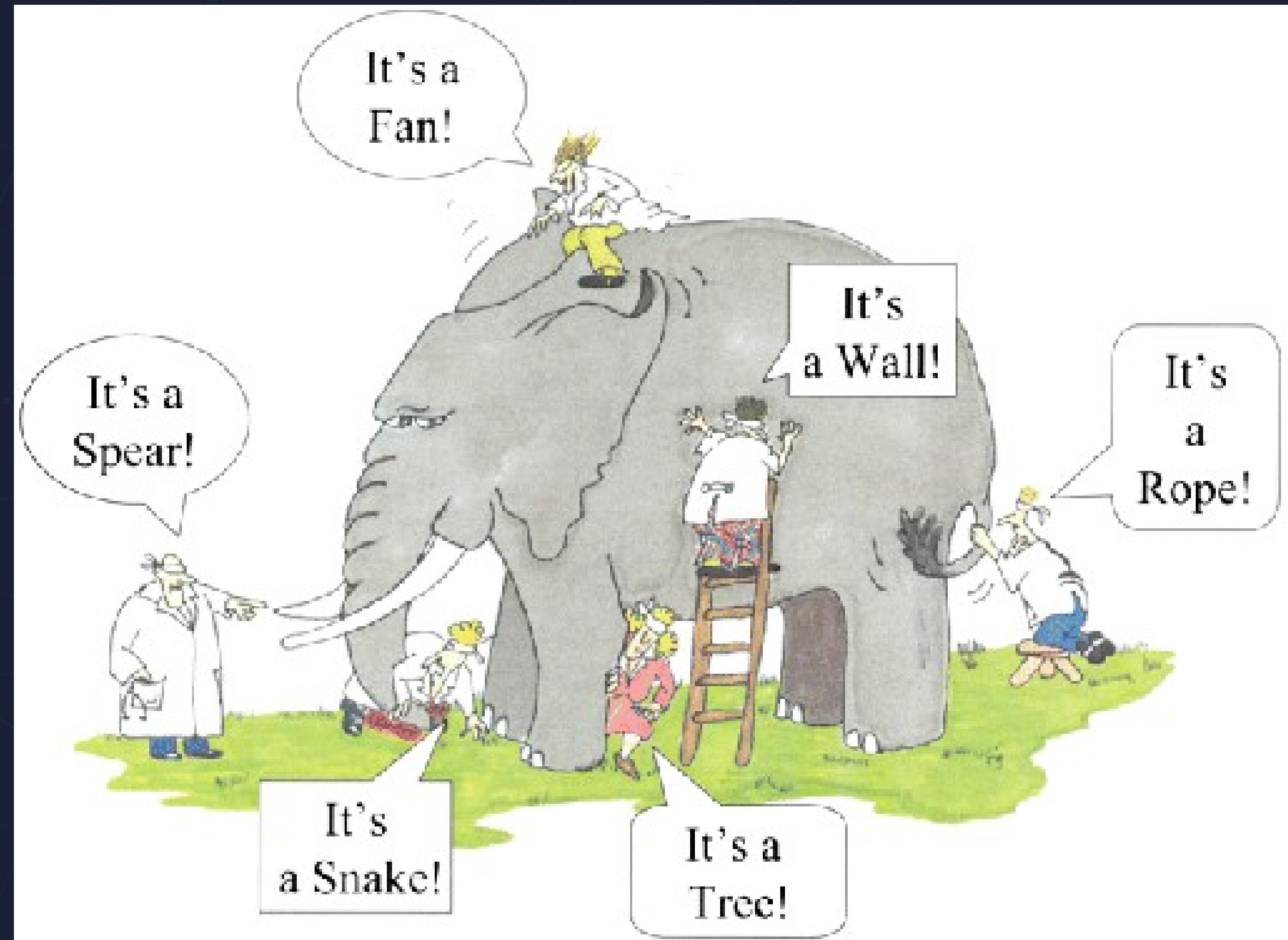
“Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures.”

- *Timothy C. May, Cryptoanarchy Manifesto, 1988*

<https://activism.net/cypherpunk/crypto-anarchy.html>



What is ethereum?





Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. By Vitalik Buterin (2014).

When Satoshi Nakamoto first set the Bitcoin blockchain into motion in January 2009, he was simultaneously introducing two radical and untested concepts. The first is the "bitcoin", a decentralized peer-to-peer online currency that maintains a value without any backing, intrinsic value or central issuer. So



Vitalik Buterin reveals Ethereum at Bitcoin Miami 2014

[Watch on YouTube \(Embed\)](#)



[Switch Invidious Instance](#)

Play next by default:

ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER

BERLIN VERSION 934279c – 2022-04-07

DR. GAVIN WOOD
FOUNDER, ETHEREUM & PARITY
GAVIN@PARITY.IO

ABSTRACT. The blockchain paradigm when coupled with cryptographically-secured transactions has demonstrated its utility through a number of projects, with Bitcoin being one of the most notable ones. Each such project can be seen as a simple application on a decentralised, but singleton, compute resource. We can call this paradigm a transactional singleton machine with shared-state.

Ethereum implements this paradigm in a generalised manner. Furthermore it provides a plurality of such resources, each with a distinct state and operating code but able to interact through a message-passing framework with others. We discuss its design, implementation issues, the opportunities it provides and the future hurdles we envisage.

1. INTRODUCTION

With ubiquitous internet connections in most places of the world, global information transmission has become incredibly cheap. Technology-rooted movements like Bitcoin have demonstrated through the power of the default, consensus mechanisms, and voluntary respect of the social contract, that it is possible to use the internet to make

is often lacking, and plain old prejudices are difficult to shake.

Overall, we wish to provide a system such that users can be guaranteed that no matter with which other individuals, systems or organisations they interact, they can do so with absolute confidence in the possible outcomes and how those outcomes might come about.

Ethereum Improvement Proposals

All Core Networking Interface ERC Meta Informational

EIPs

 Ethereum Cat Herders 2076 members

 Eth R&D 11413 members

 Ethereum Wallets 616 members

 Everything

 Last Calls

 All except ERC

email alerts

Ethereum Improvement Proposals (EIPs) describe standards for the Ethereum platform, including core protocol specifications, client APIs, and contract standards. Network upgrades are discussed separately in the [Ethereum Project Management repository](#).

Contributing

First review EIP-1. Then clone the repository and add your EIP to it. There is a [template EIP here](#). Then submit a Pull Request to Ethereum's EIPs repository.

 ethereum / execution-specs

Type ⌘ to search | >_ | + ▾ | ○ | ⓘ | ⌂

Code Issues 57 Pull requests 6 Actions Projects 2 Security Insights

[execution-specs](#) Public

Watch 44 Fork 188 Star 597

master 50 branches 0 tags Go to file Add file ▾ Code ▾

shemnon and chfast Add opcodes to "Lists" documentation (#764) ... ✓ 8b73624 2 weeks ago 1,437 commits

.github Moar CPUs last month

doc subpackages only in stage1 8 months ago

lists Add opcodes to "Lists" documentation (#764) 2 weeks ago

network-upgrades Merge pull request #792 from ethereum/timbeiko-patch-17 last month

scripts Remove aeth download from test suite and make it part of aithub w... 2 years ago

About Specification for the Execution Layer. Tracking network upgrades.

Readme CC0-1.0 license Activity 597 stars 44 watching 188 forks

 ethereum / consensus-specs

Type ⌘ to search | >_ | + ▾ | ○ | ⓘ | ⌂

Code Issues 162 Pull requests 58 Actions Projects Security Insights

[consensus-specs](#) Public

Watch 251 Fork 887 Star 3.2k

dev 128 branches 80 tags Go to file Add file ▾ Code ▾

djrtwo Merge pull request #3349 from ethereum/eip7002 ... ✓ 2cd967e 5 days ago 8,611 commits

.circleci Merge branch 'dev' into eip7002 3 weeks ago

.github/workflows Merge branch 'dev' into eip7002 2 weeks ago

configs Merge branch 'dev' into eip7002 3 weeks ago

docs Refactor (setup.py) (#3393) 2 weeks ago

fork_choice Add docs about how to add a new feature proposal in consensus-sp... 3 months ago

presets Whisk: add preset files (#3424) 3 weeks ago

pysetup Merge branch 'dev' into eip7002 2 weeks ago

scripts Update G2 trusted setup length to 65 7 months ago

solidity_deposit_contract Update solidity_deposit_contract/README.md 3 years ago

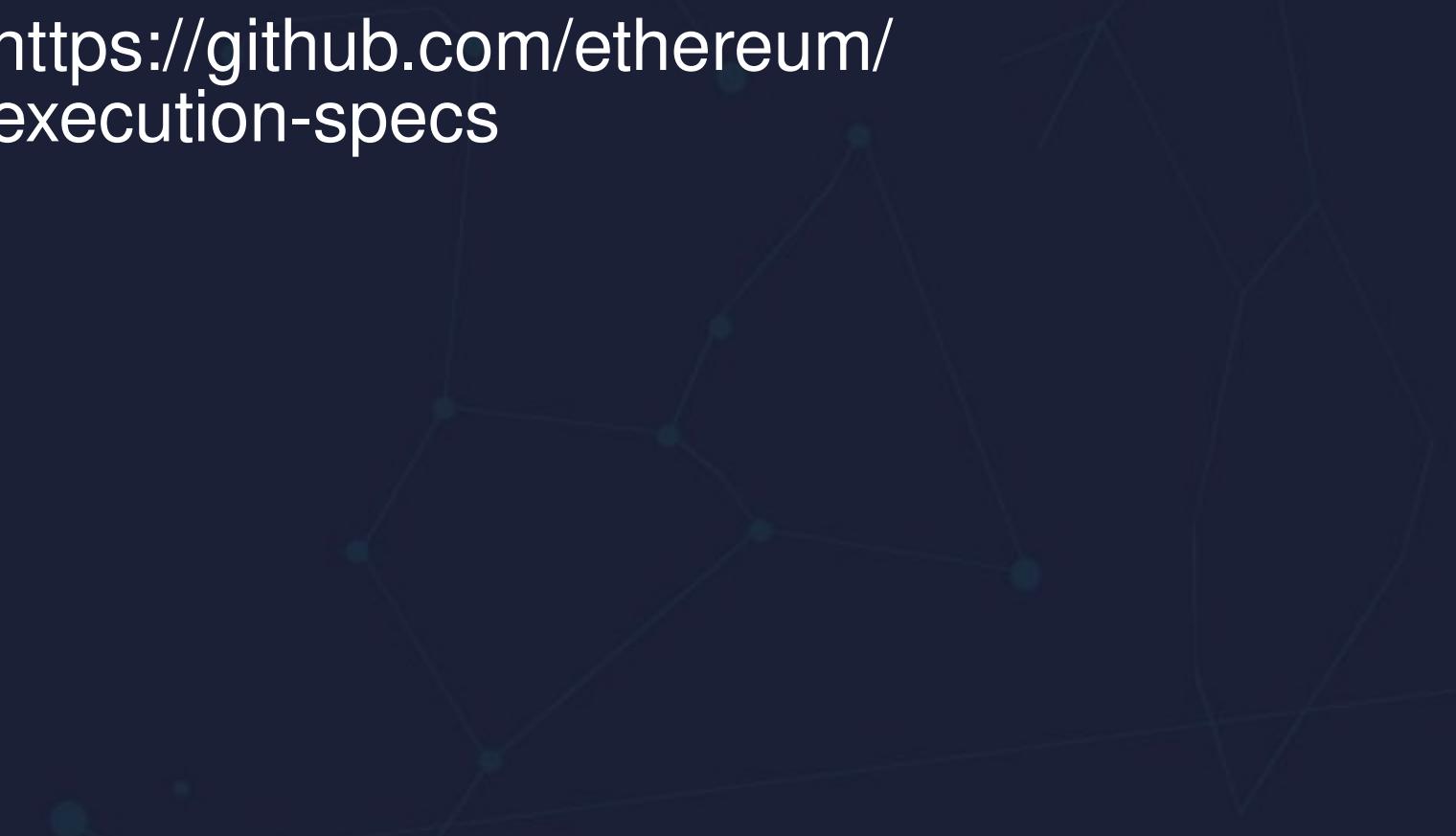
specs Merge branch 'dev' into eip7002 2 weeks ago

About Ethereum Proof-of-Stake Consensus Specifications

Readme CC0-1.0 license Security policy Activity 3.2k stars 251 watching 887 forks Report repository

Releases 79

Gamlum Latest on Apr 18



<https://github.com/ethereum/execution-specs>

<https://github.com/ethereum/consensus-specs>

<https://github.com/ethereum/execution-apis>

<https://github.com/ethereum/beacon-apis>

Ethereum

je
iew

Slot
Epoch

drawals

F
S

ification

Presets, and

https://eth2book.info/capella

Upgrading Ethereum

A technical handbook on Ethereum's
move to proof of stake and beyond

Edition 0.3: Capella [WIP]

by Ben Edgington



Contents

The history of Ethereum

<https://ethereum.org/en/history/>

A timeline of all the major milestones, forks, and updates to the Ethereum blockchain.

What are forks?

More

Changes to the rules of the Ethereum protocol which often include planned technical upgrades.

Skip straight to information about some of the particularly important past upgrades: [The Beacon Chain](#); [The Merge](#); and [EIP-1559](#)

Looking for future protocol upgrades? [Learn about upcoming upgrades on the Ethereum roadmap.](#)

2023

Shanghai

 Apr 12, 2023, 10:27:35 PM +UTC

Design principles

Simplicity, Universality, Modularity, Non-discrimination, Agility

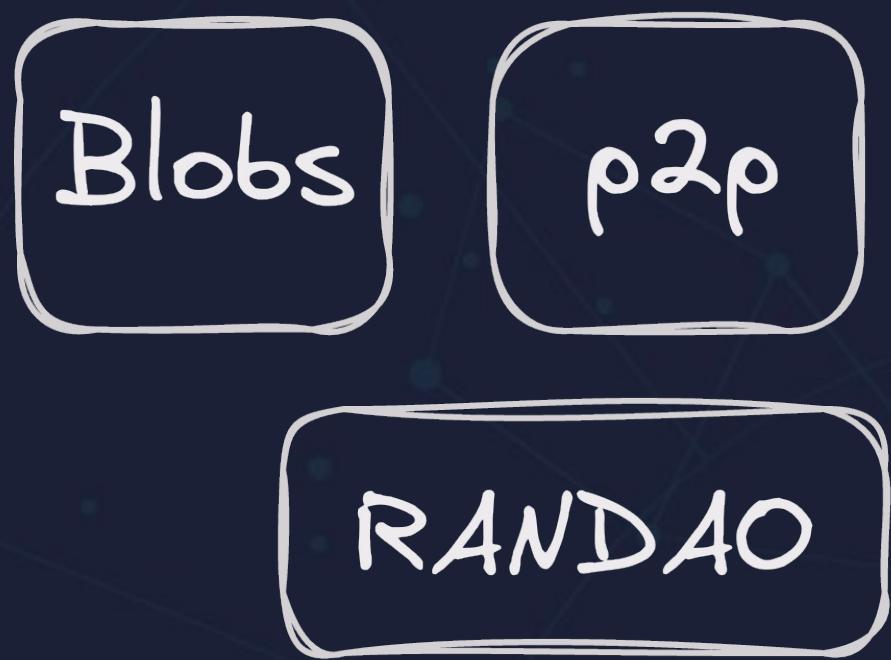
Sandwich/encapsulated complexity

Freedom, neutrality

Generalization, No features

Non-risk aversion

Consensus layer



LMD-GHOST

Fork choice

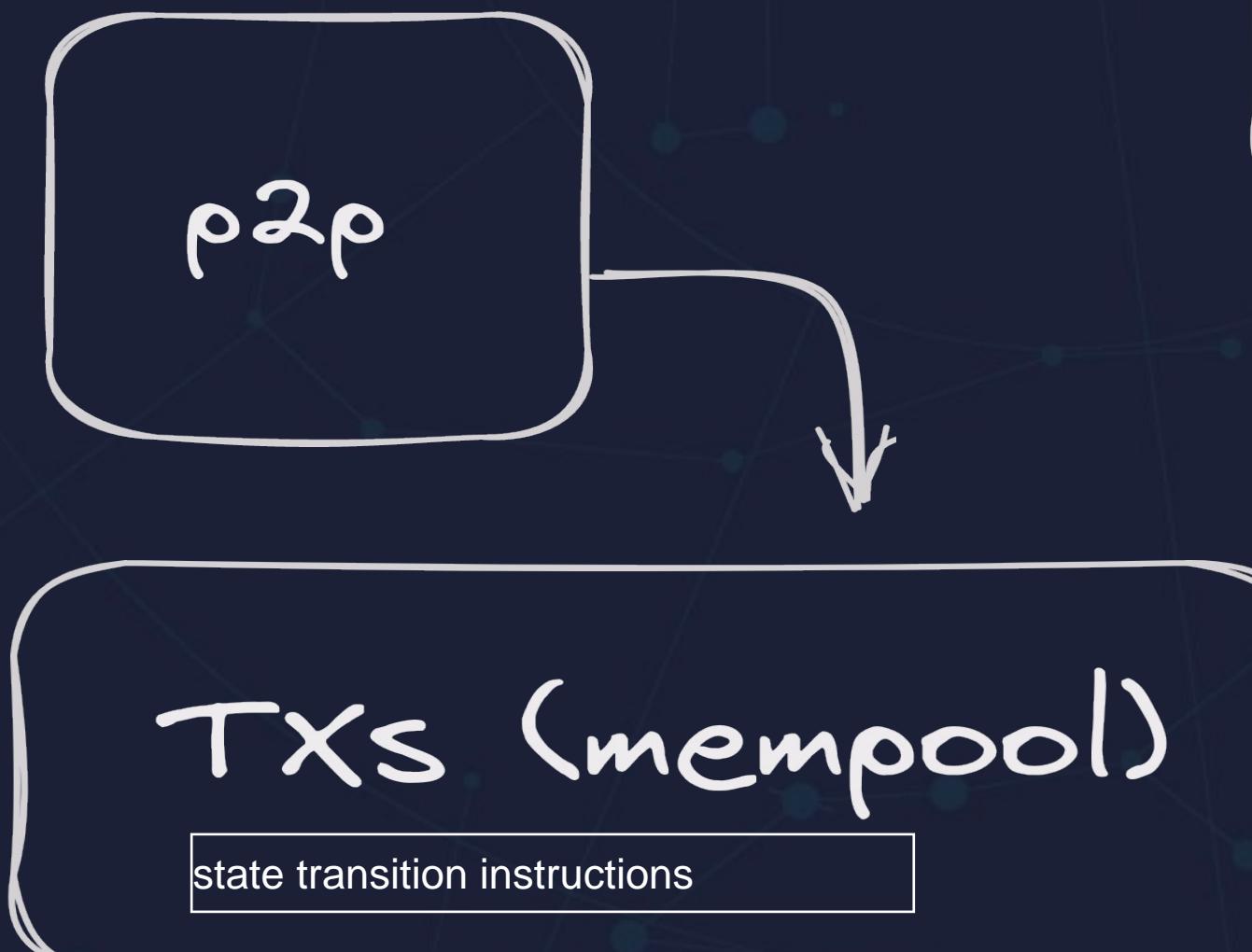
RANDAO

Beacon APIs

Validators

Engine API

Execution layer



State (data)

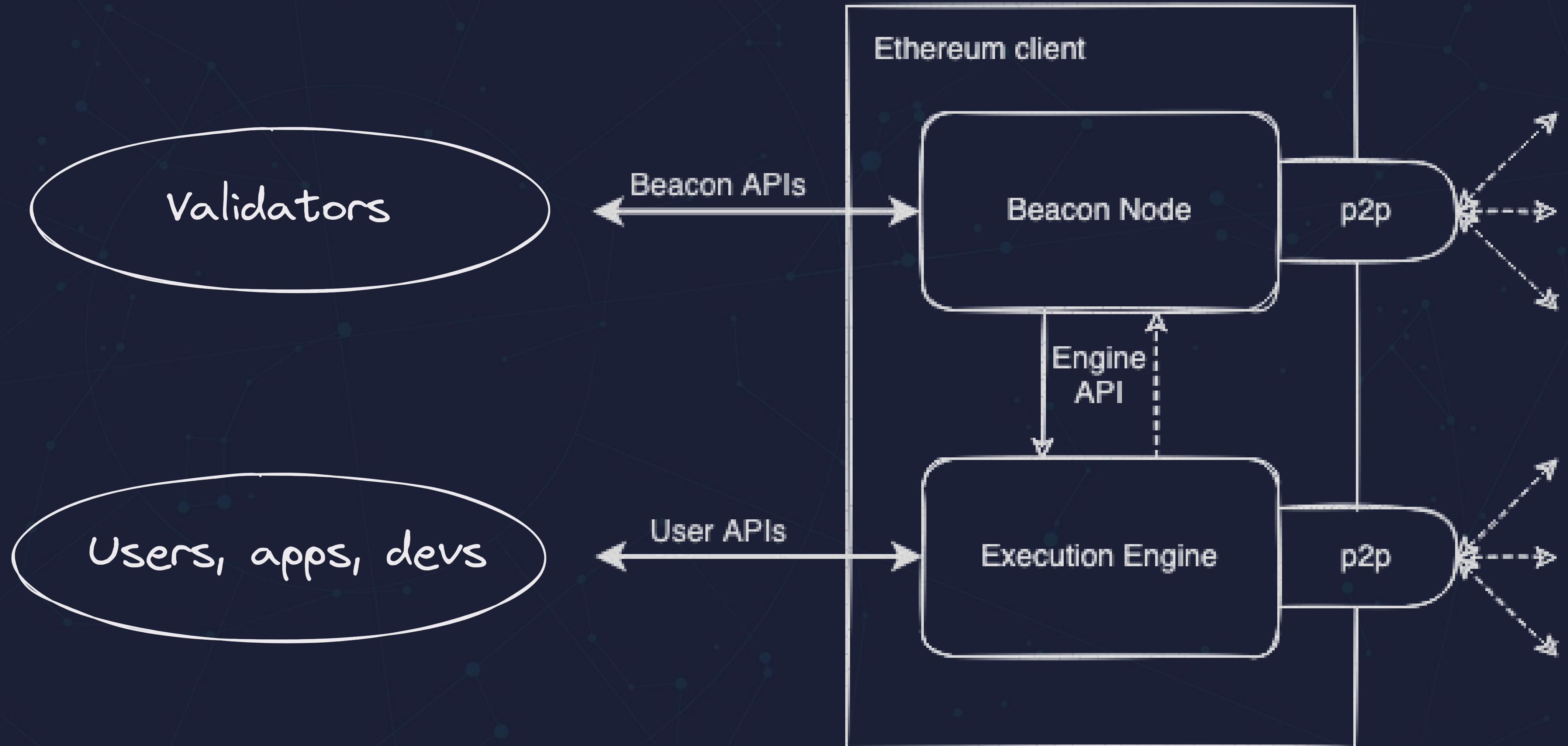
TXs (mempool)
state transition instructions

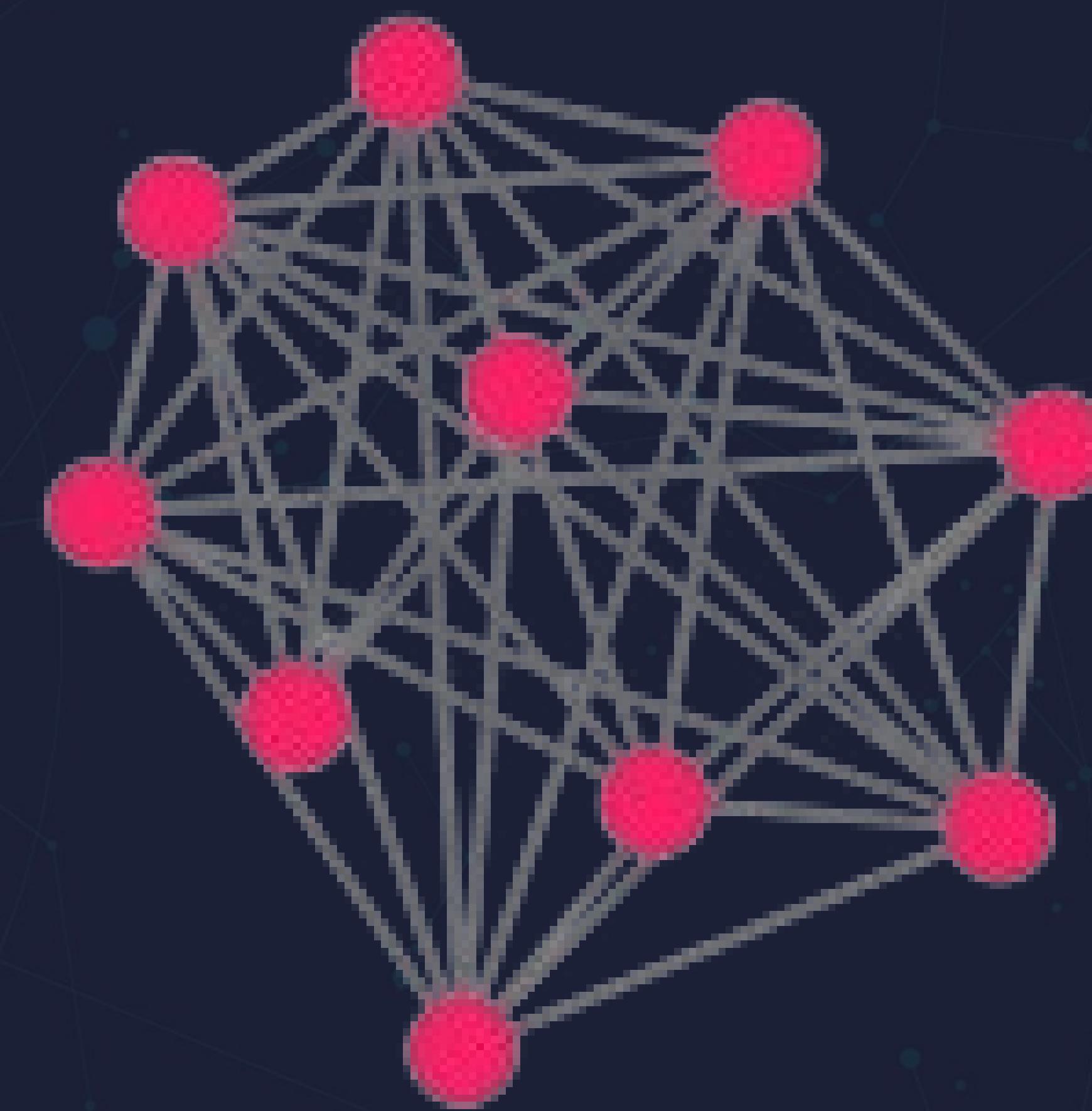
EVM

ensures a code on the blockchain

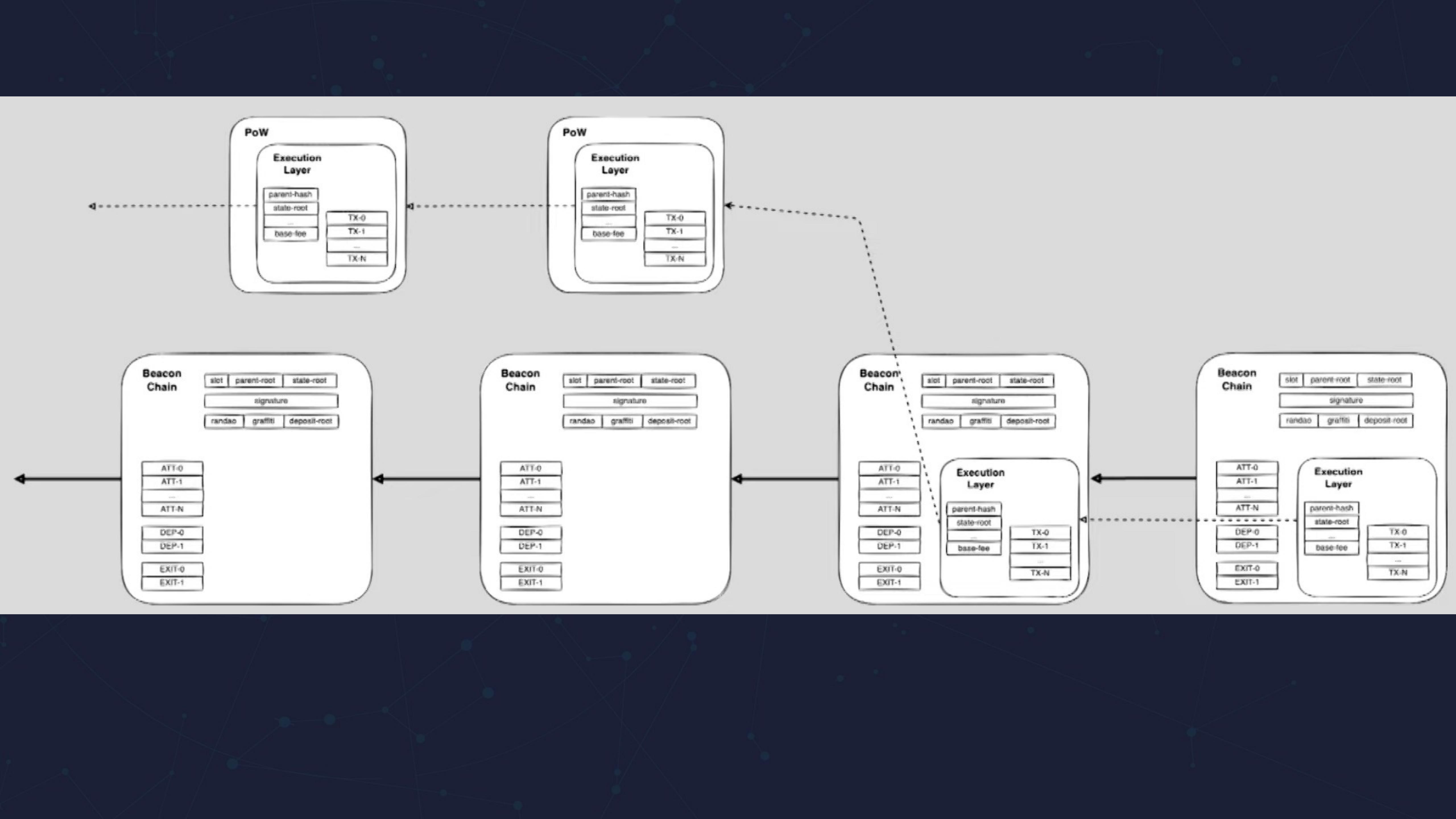
JSON-RPC
API

User/web3





Nodes in decentralized topology



Implementations - EL

geth/go



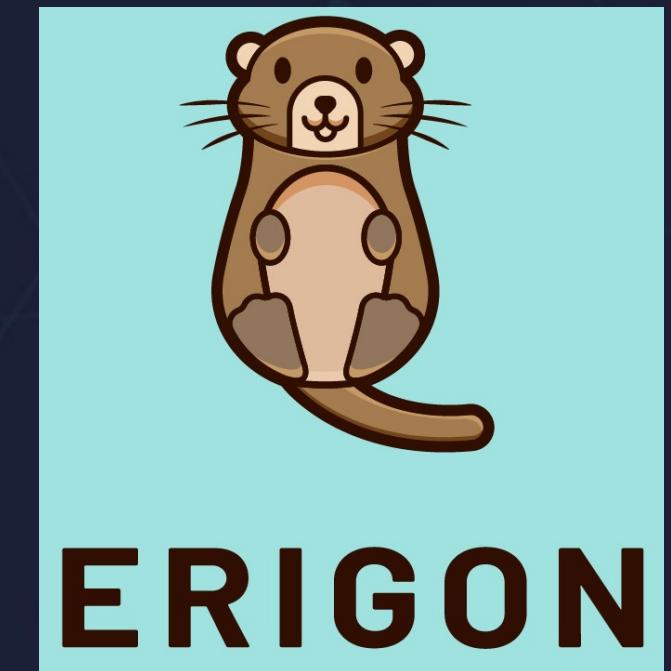
nethermind/C#



besu/java



erigon/go



reth/rust



silkwarm/c++



ethereumjs/TS



Implementations - CL

prysm/go



lighthouse/rust



teku/java



nimbus/nim



lodestar/TS



Testing

<https://github.com/ethereum/tests>

<https://github.com/ethereum/retesteth>

<https://github.com/cosm/ethereum/execution-spec-tests>

<https://github.com/lightclient/rpctestgen>

<https://github.com/ethereum/hive>

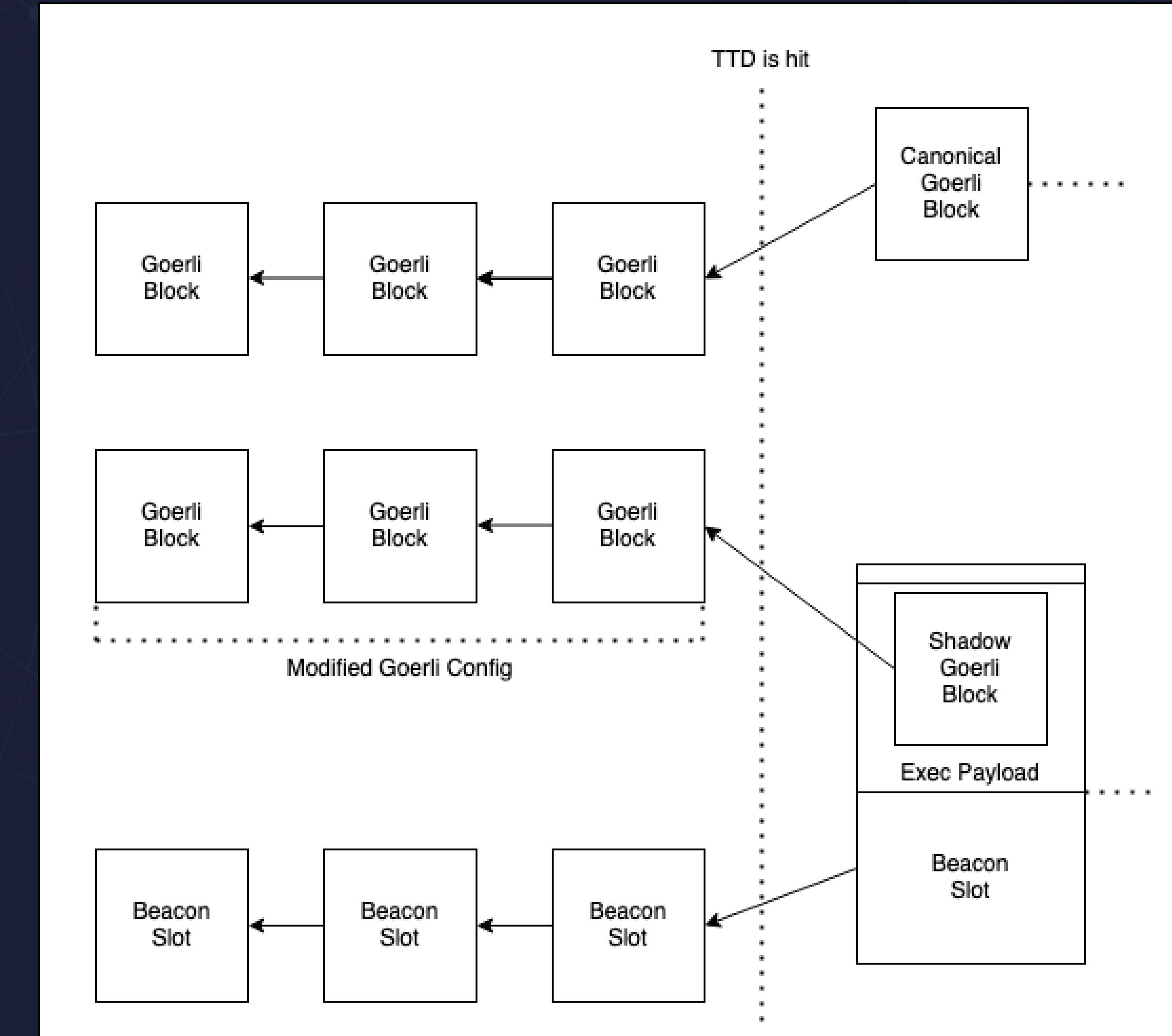
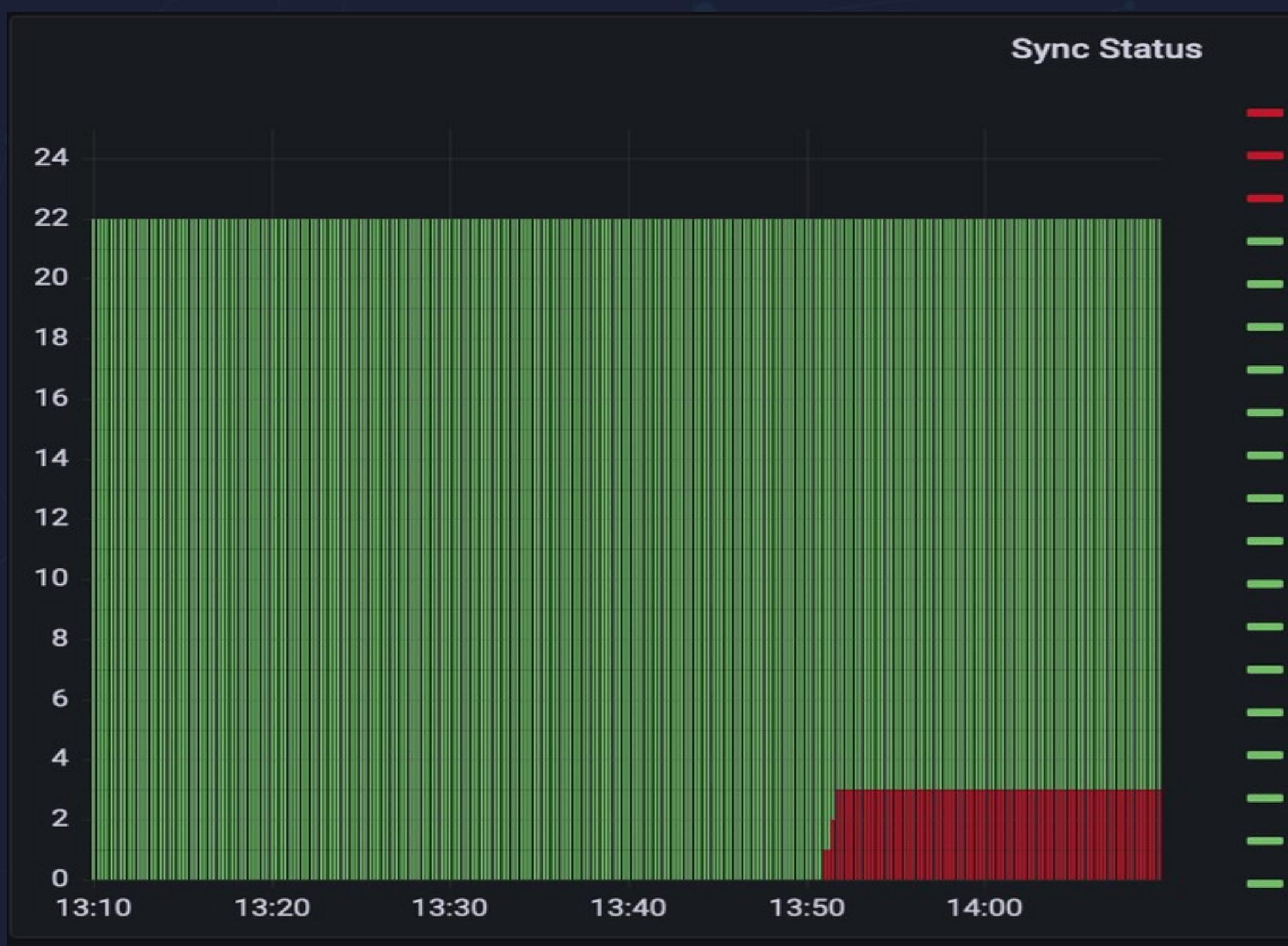
<https://github.com/kurtosis-tech/kurtosis>

<https://github.com/MariusVanDerWijden/FuzzyVM>

<https://github.com/MariusVanDerWijden/tx-fuzz>

Other tests

Benchmarking, Stress
Shadow forks - live transition
Client tests, unit testing
CI/CD





Coordination

Dev calls (EL, CL, 4844, tesnets, EOF...)

EIPs – Eth Magicians, EIPIP, Cat herders

R&D Discord

Ethresear.ch

<https://ethresear.ch>



research

<https://ethereum-magicians.org>

✨ Fellowship of Ethereum Magicians ✨

Coordination

The screenshot shows a GitHub repository page for the Ethereum Project Management repository. The repository name is `ethereum / pm`. The main navigation bar includes links for Code, Issues (7), Pull requests (2), Actions, Projects, Wiki, Security, and Insights. The repository is public and has 297 watchers, 280 forks, and 1.3k stars.

The repository contains 2 branches and 0 tags. The `master` branch is selected. The activity feed shows the following commits:

Author	Commit Message	Date
timbeiko	Merge pull request #812 from darkfire-rain/master	9559637 2 weeks ago
	Merge branch 'master' into master	2 weeks ago
	Merge branch 'master' into master	2 weeks ago
	Fix merge notes links	6 months ago
	Update 4844-readiness-checklist.md	2 weeks ago
	Update Upgrade Community Calls/Call_001.md	5 months ago
	First pass	6 months ago
	Create LICENSE	7 years ago
	Merge branch 'master' into master	2 weeks ago

The repository also contains files like `README.md`, `LICENSE`, and `README.md`.

About

Project Management: Meeting notes and agenda items

- Readme
- View license
- Activity
- 1.3k stars
- 297 watching
- 280 forks
- Report repository

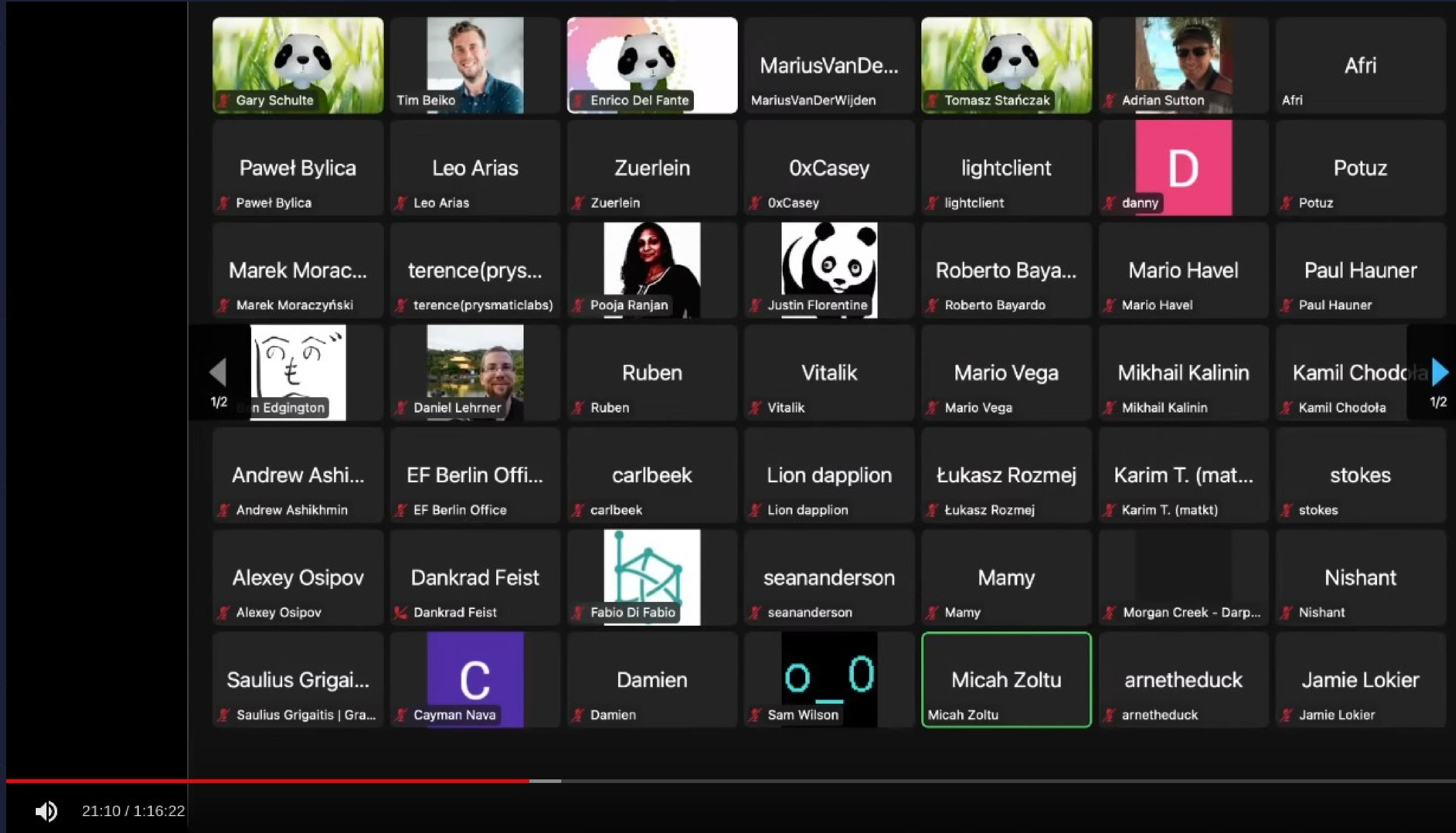
Releases

No releases published

Packages

No packages published

Ethereum Project Management Repository



Ethereum Core Devs Meeting #145 [2022-8-18]

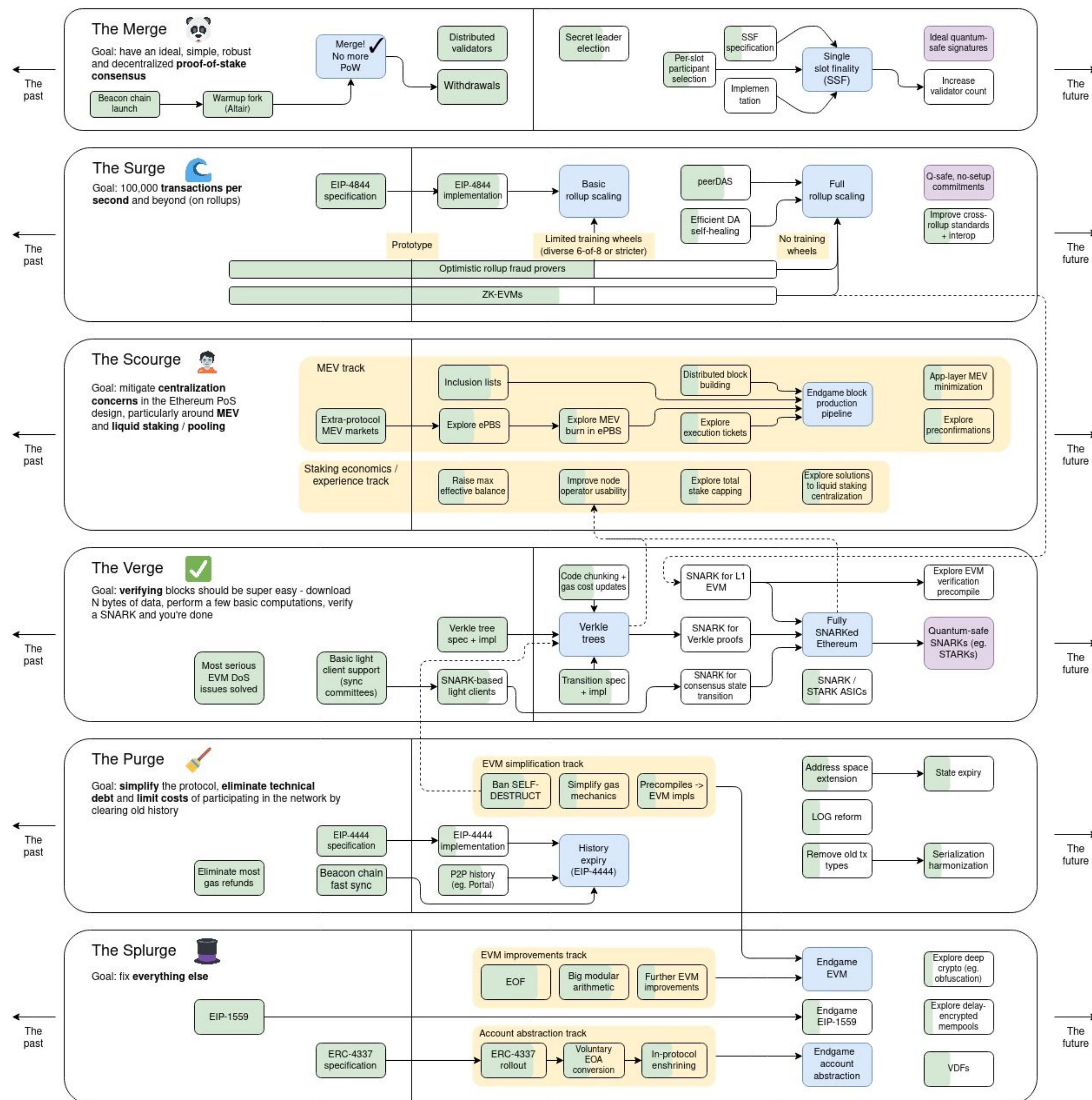
7,165 views Streamed live on Aug 18, 2022 <https://github.com/ethereum/pm/issues...> ...more

200 Dislike Share Clip Save





Research and roadmap



Scalable

Multi-chain ecosystems

Decentralized

Traditional chains (BTC, ETH...)

typical high-TPS chains

Secure

Nurturing the Infinite Garden

"A finite game is played for the purpose of winning. An infinite game for the purpose of continuing the play." ~ James P. Carse

Infinite garden of
Development, research, testing...

Ossification?

Can you imagine world with Eth2 Ethereum done?





Vitalik

Welcome to EPF Study Group!

What now?!

Dive into resources

Find more and share

Find your niche and contribute

Check out EPF projects

EPF cohorts history

[https://github.com/eth-protocol-fellows/
cohort-four/](https://github.com/eth-protocol-fellows/cohort-four/)

[https://github.com/eth-protocol-fellows/
cohort-three/](https://github.com/eth-protocol-fellows/cohort-three/)



SUPERB[®]
wallpapers