Ethereum Protocol 101

(Pre)History, design
overview and development

Protocol Development

Philosophy, fundamentals and ideas

Prehistory

Genesis of...

Unix philosophy

FOSS

Cryptography and Cypherpunks

Ethereum design

The UNIX System: Making Computers More Productive https://yewtu.be/watch?v=tc4ROCJYbm0

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

https://yewtu.be/watch?v=Ag1AKIl_2GM

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

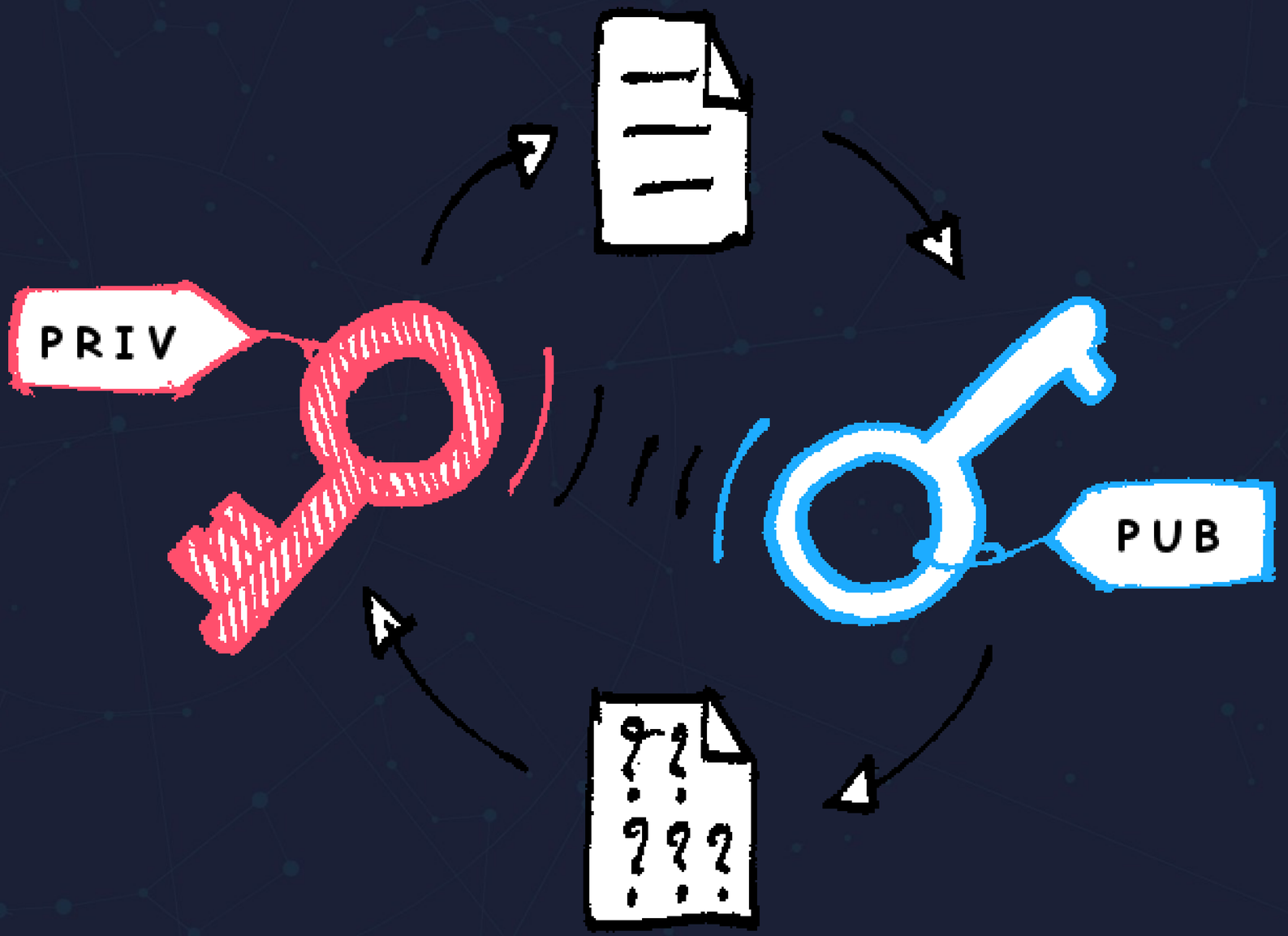
***Abstract*—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This 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.**

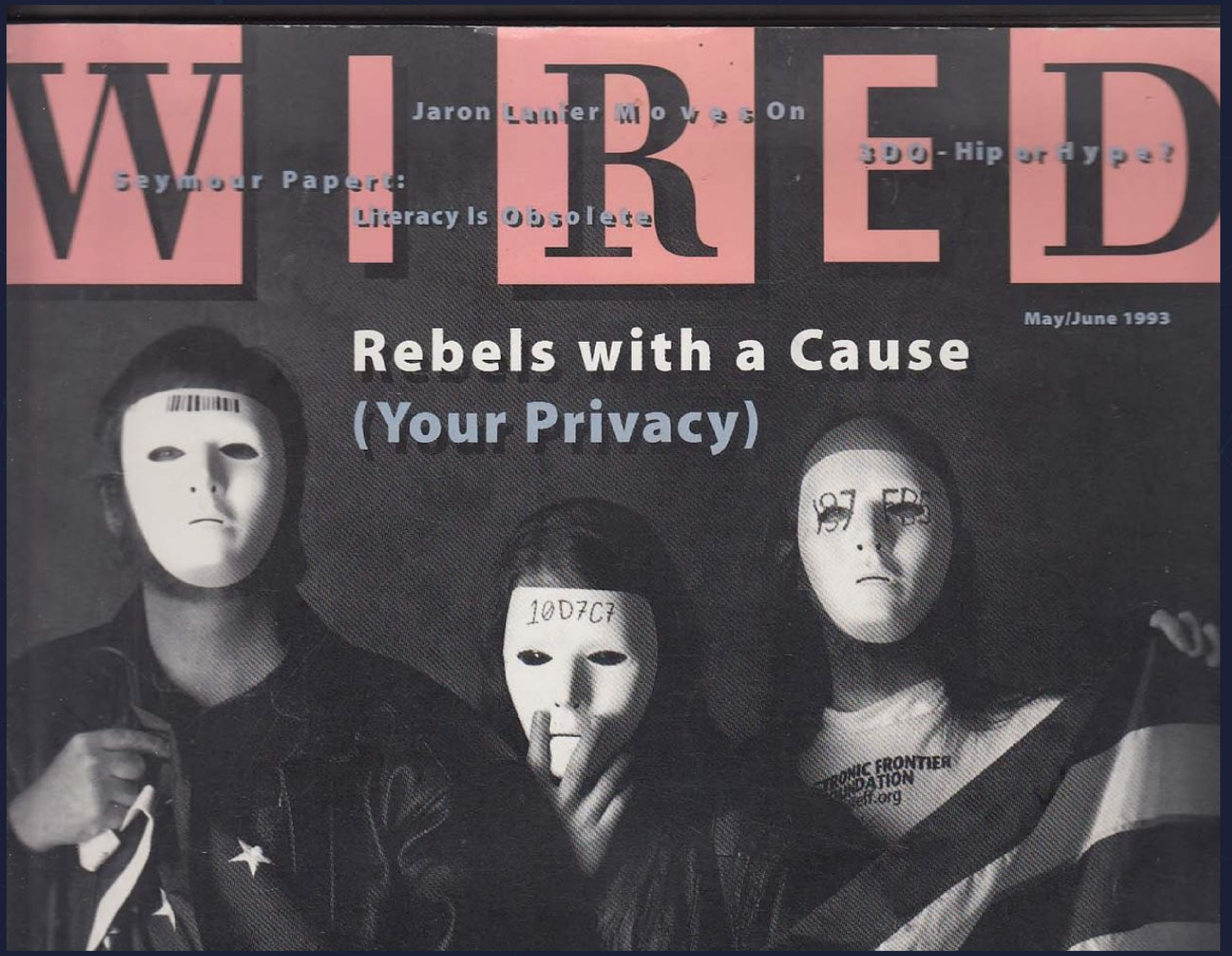
I. Introduction

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

https://www-ee.stanford.edu/~hellman/publications/24.pdf


PRIV
PUB
??
???

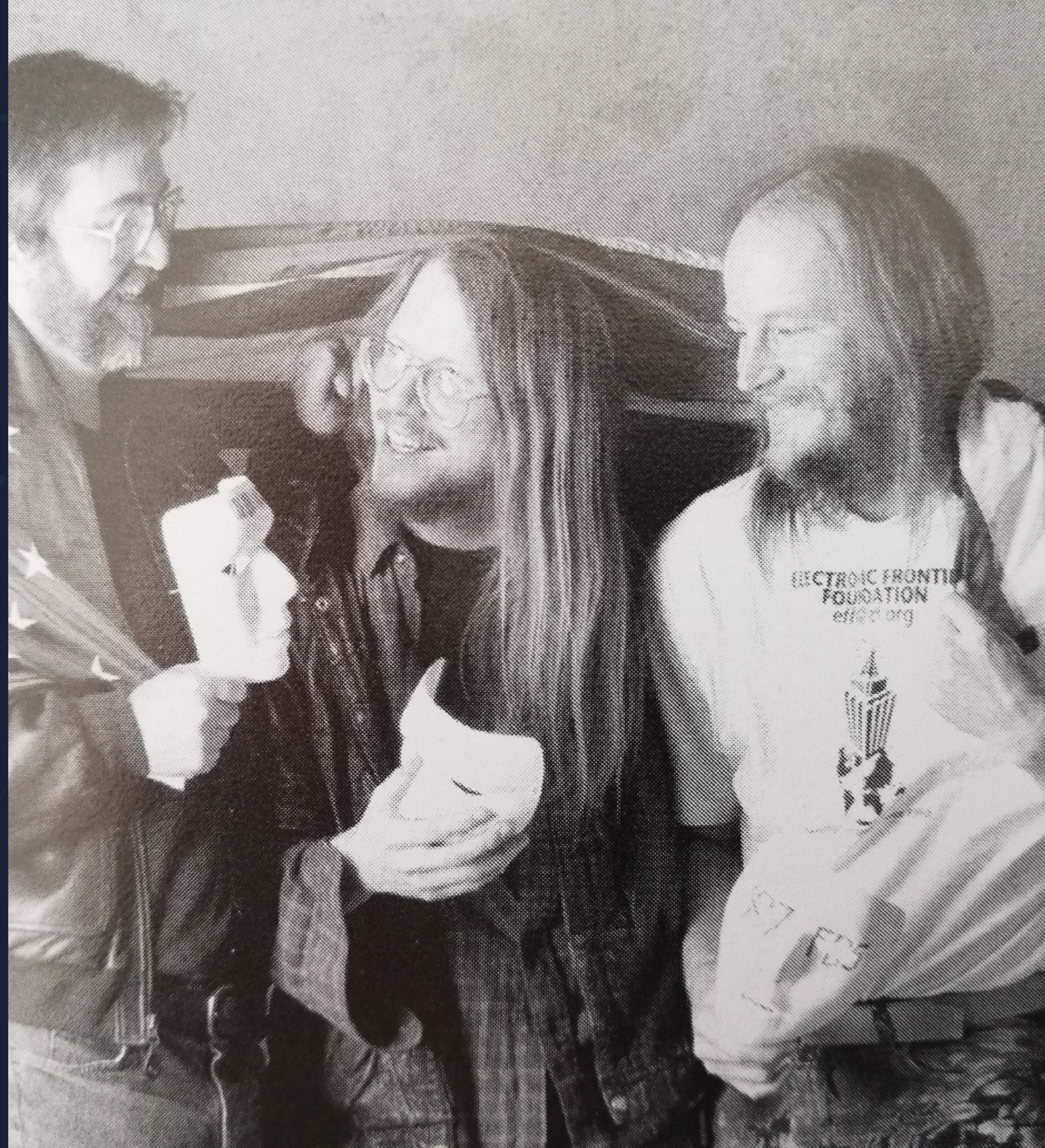

WIRED
Jaron Lanier Moves On
3DO - Hip or Hype?
Seymour Papert:
Literacy Is Obsolete
May/June 1993
Rebels with a Cause
(Your Privacy)
10D7C7
FRONTIER
FOUNDATION
eff.org

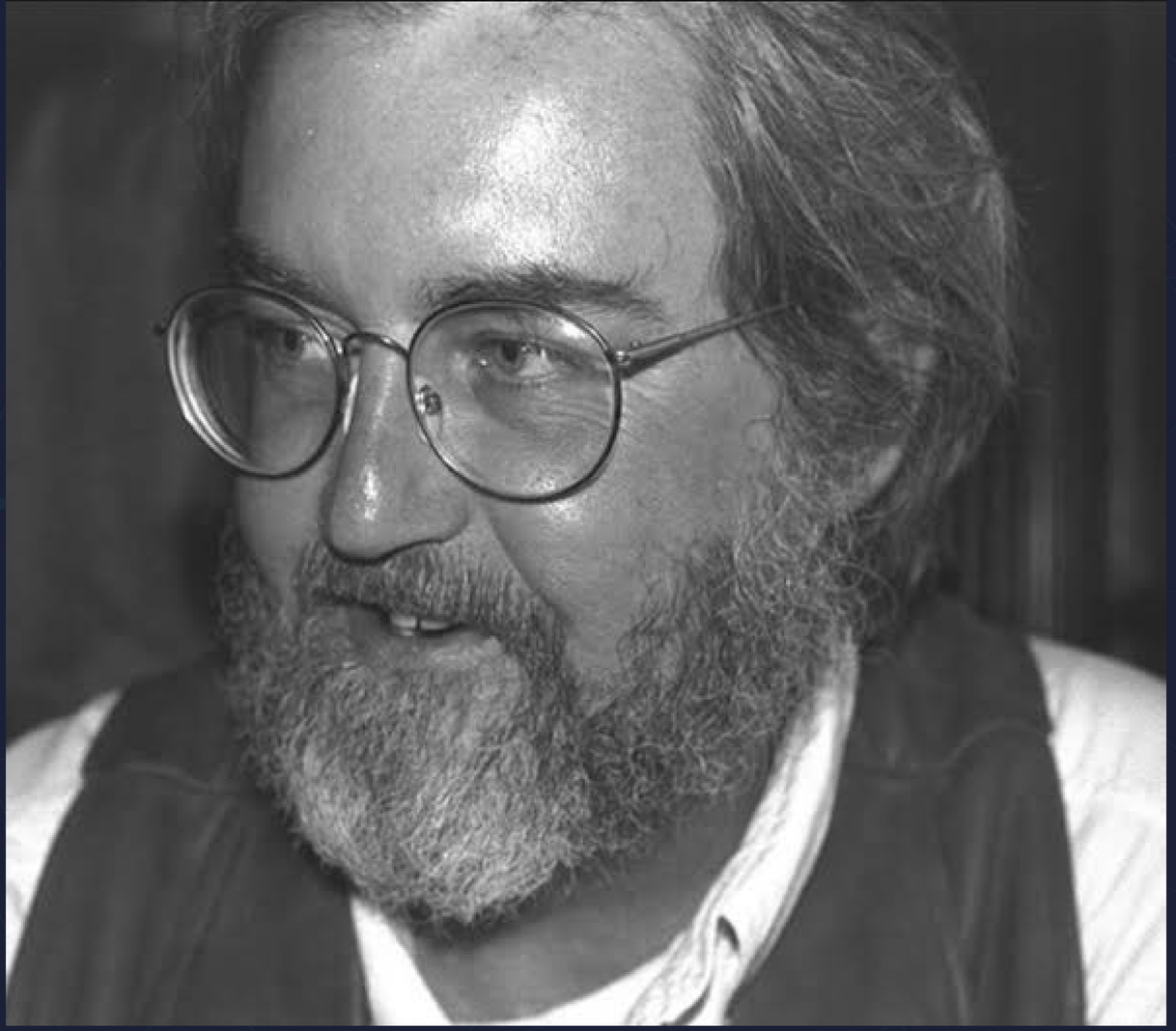
Cypherpunks

“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	Crypto Anarchy: encryption, digital money,
tcmay@netcom.com	anonymous networks, digital pseudonyms, zero
408-688-5409	knowledge, reputations, information markets,
W.A.S.T.E.: Aptos, CA	black markets, collapse of governments.
Higher Power: 2^756839	PGP Public Key: by arrangement.

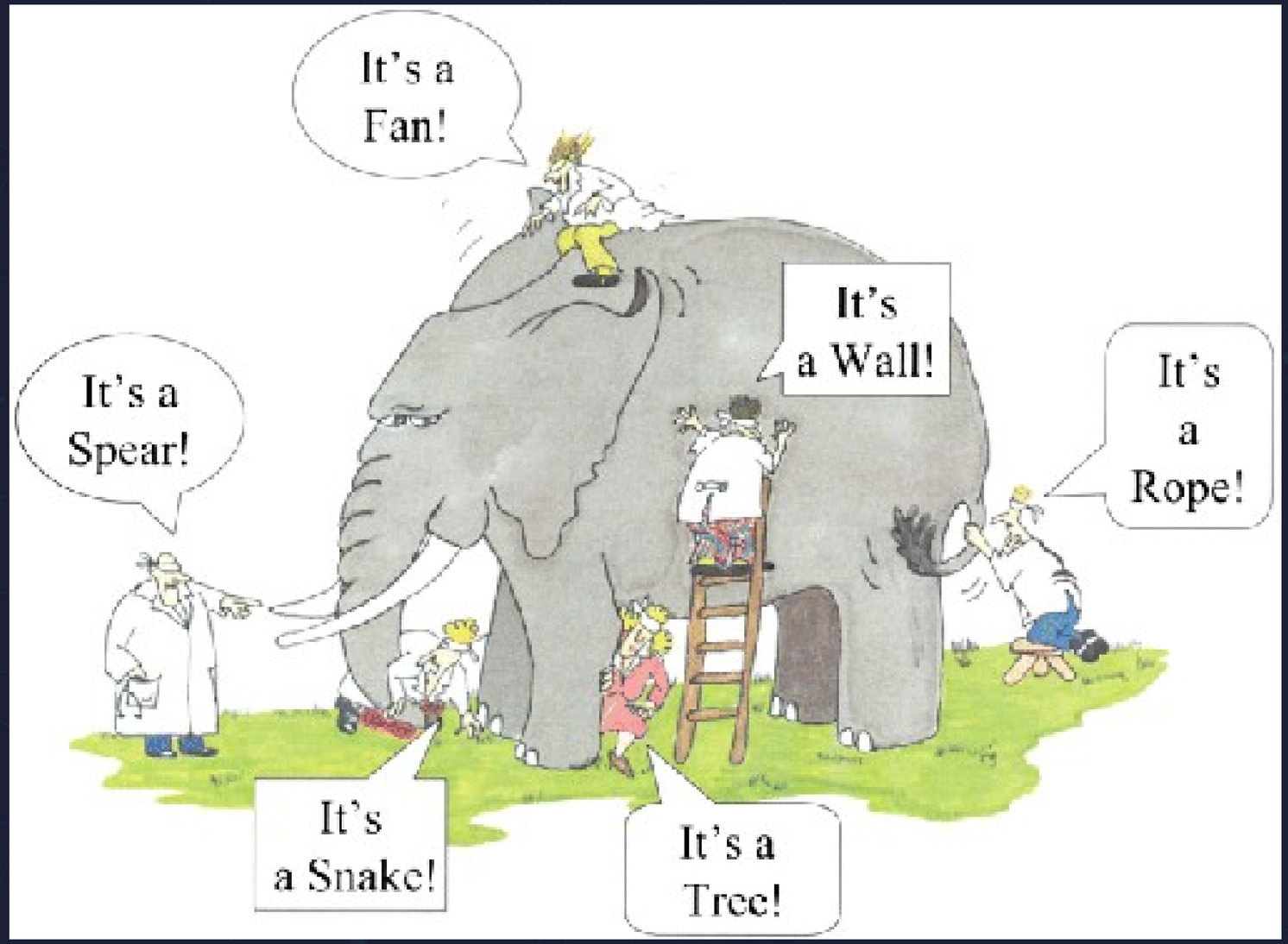
Cryptoanarchy

“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?


It's a Fan!
It's a Spear!
It's a Wall!
It's a Rope!
It's a Snake!
It's a Tree!

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

Ethereum

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

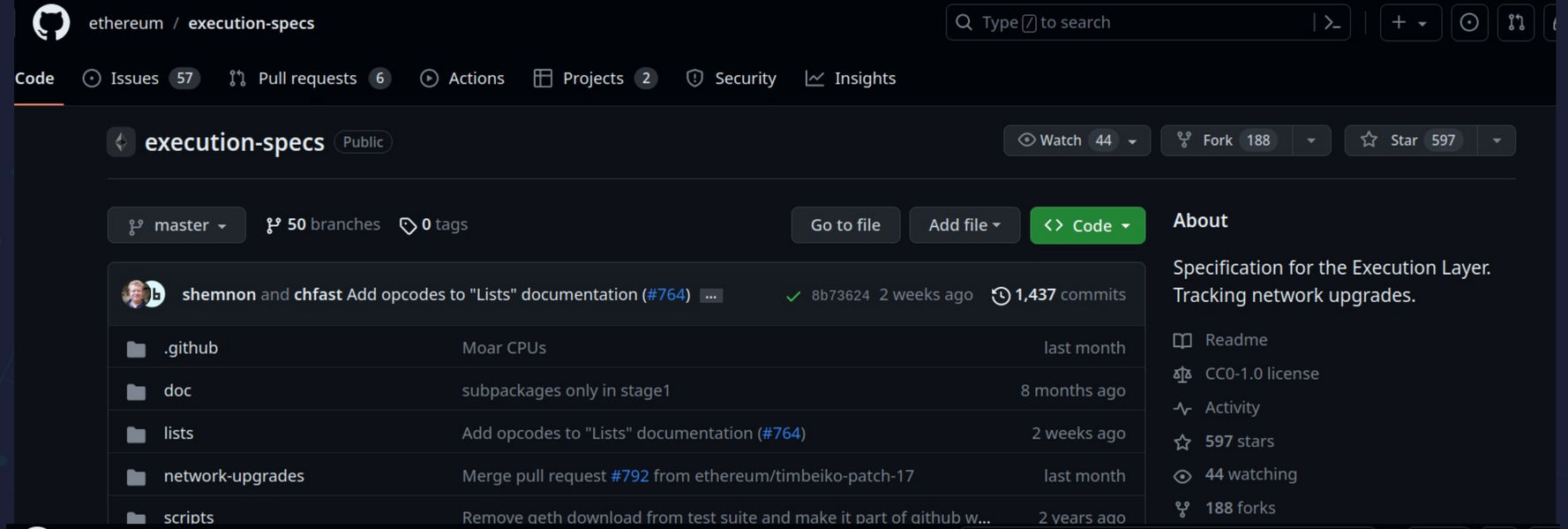
Ethereum Cat Herders 2076 members | Eth R&D 11413 members | Ethereum Wallets 616 members | rss Everything | rss Last Calls | rss All except ERC

email alerts

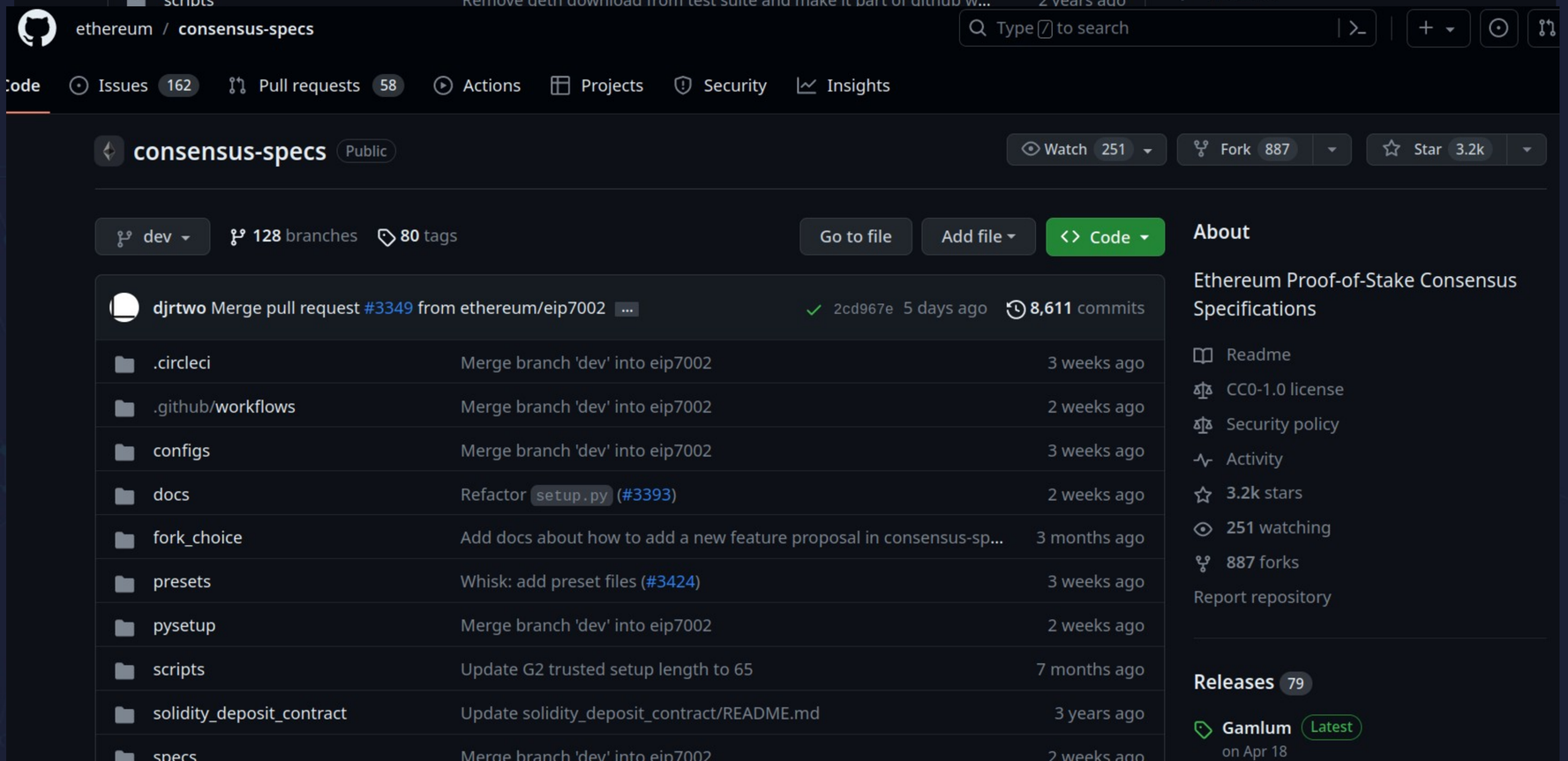
Ethereum Improvement Proposals (EIPs) describe standards for the Ethereum platform, including core protocol specifications, client APIs, and contract standards. Network upgrades are discussed separately in the Ethereum Project Management repository.

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.



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



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

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

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

https://eth2book.info/capella

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

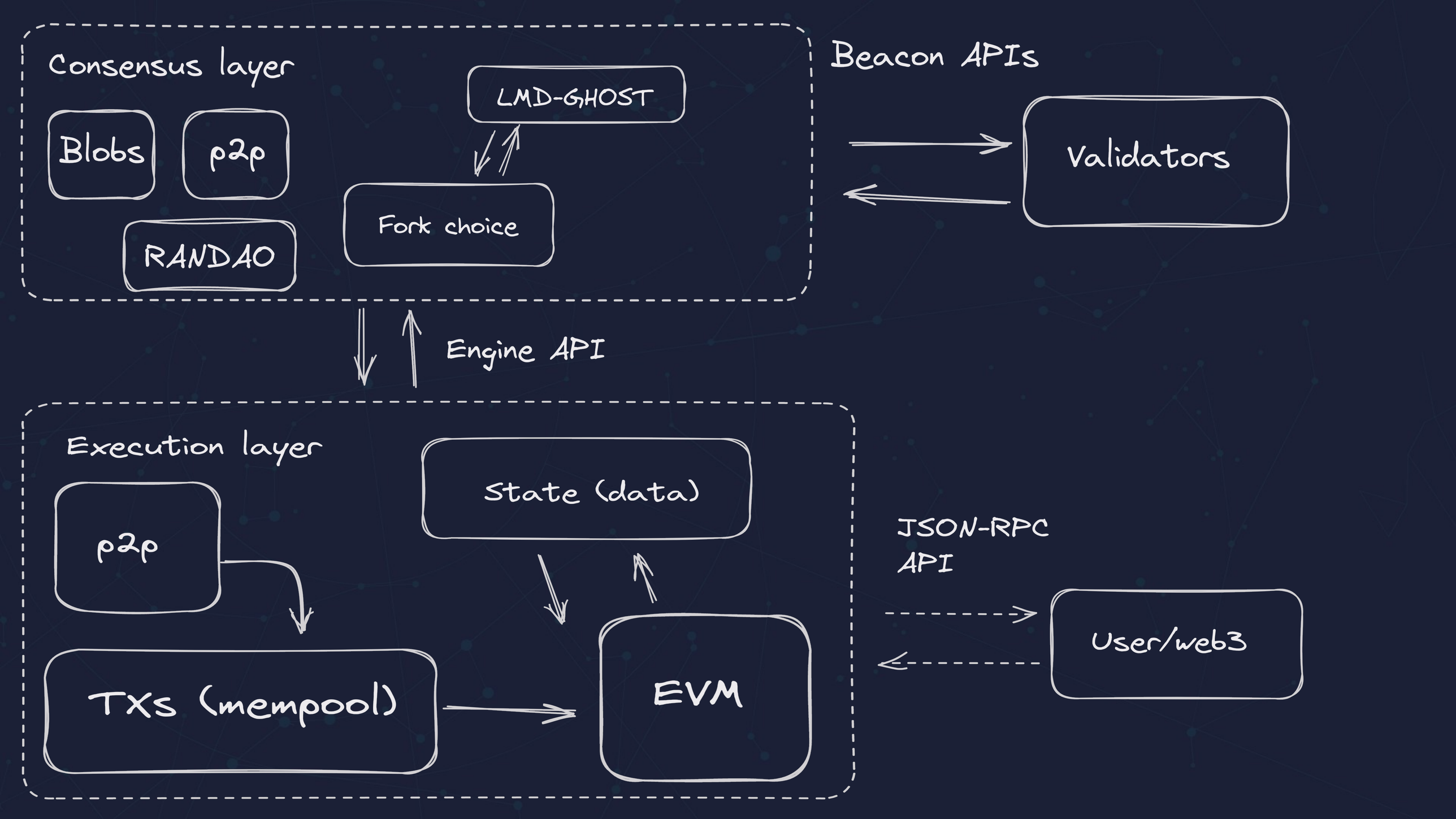
Sandwich/encapsulated complexity

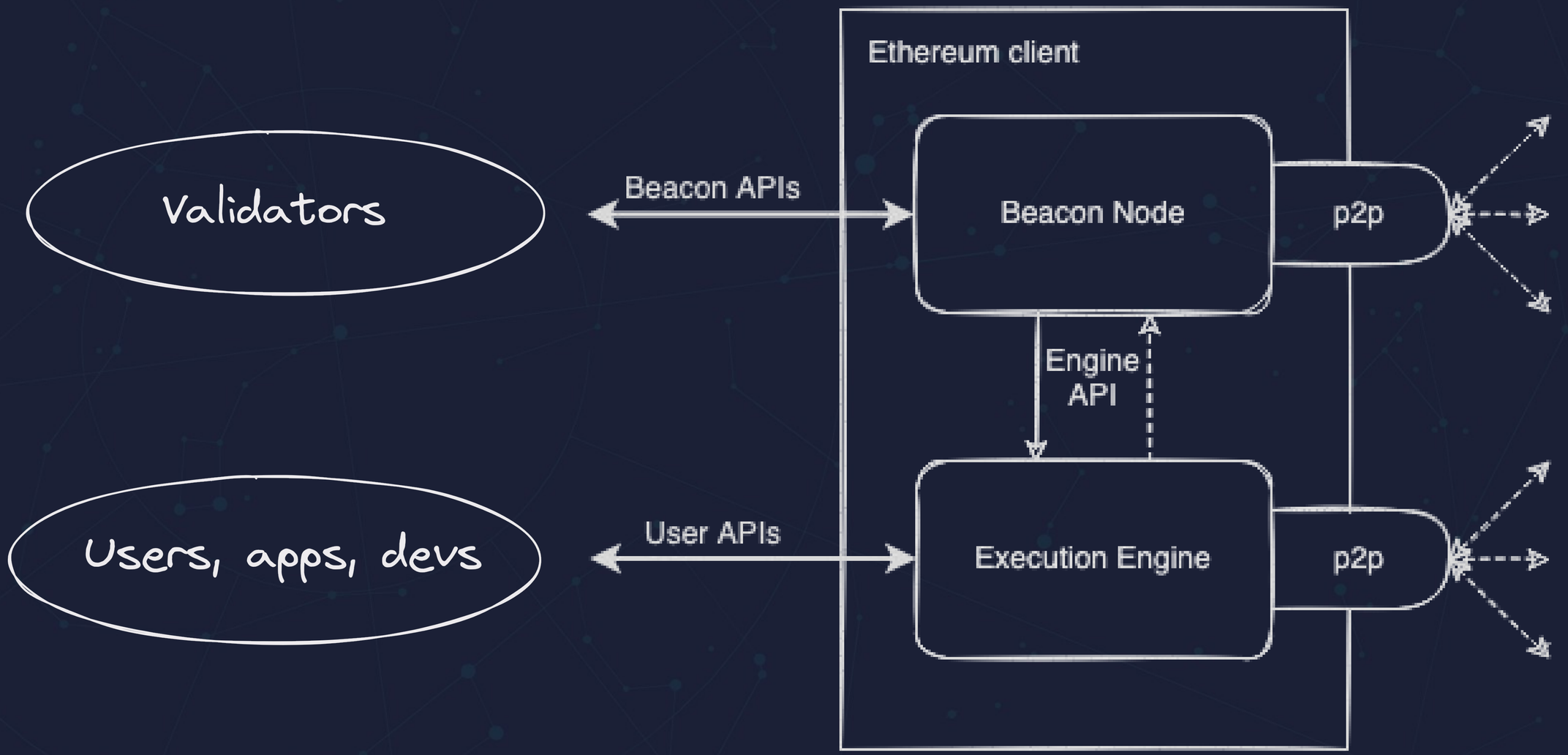
Freedom, neutrality

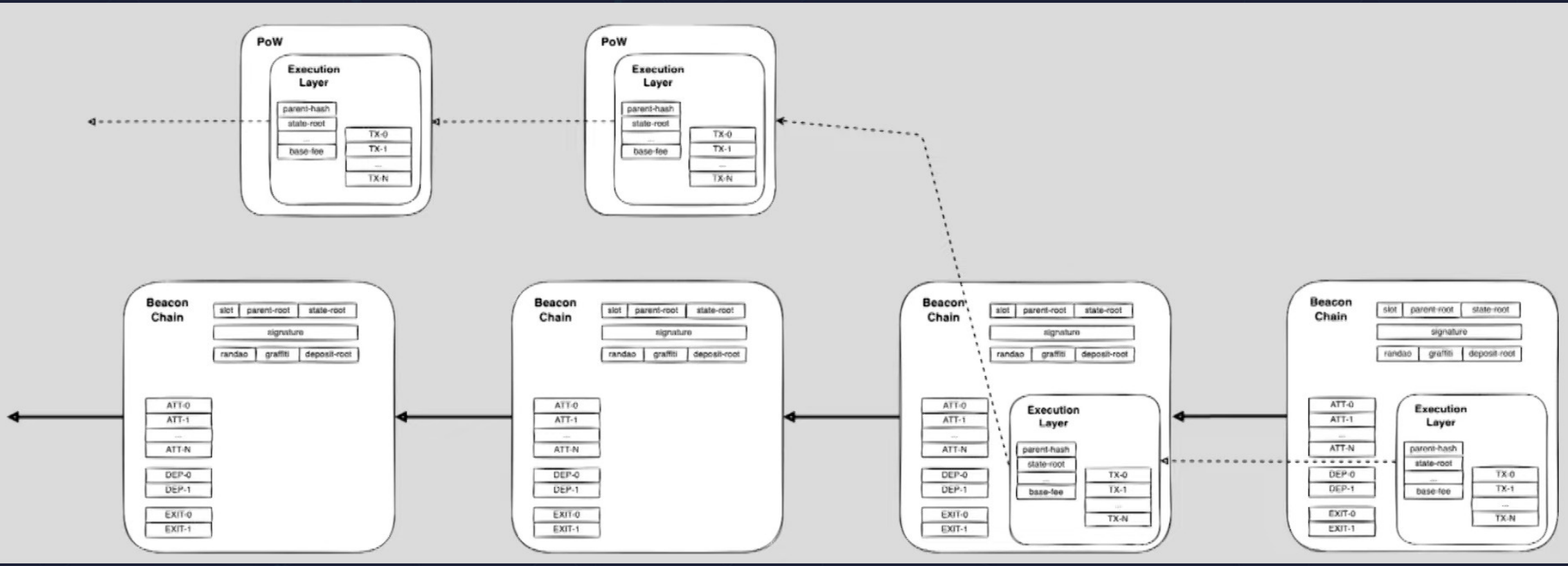
Generalization, No features

Non-risk aversion

https://web.archive.org/web/20211121044757/https://ethereumbuilders.gitbooks.io/guide/content/en/design_rationale.html


Consensus layer
Blobs
p2p
RANDAO
LMD-GHOST
Fork choice
Beacon APIs
Validators
Engine API
Execution layer
p2p
State (data)
TXs (mempool)
EVM
JSON-RPC API
User/web3


Validators
Users, apps, devs
Beacon APIs
User APIs
Ethereum client
Beacon Node
Engine API
Execution Engine
p2p
p2p


PoW
Execution Layer
parent-hash
state-root
...
base-fee
TX-0
TX-1
...
TX-N
PoW
Execution Layer
parent-hash
state-root
...
base-fee
TX-0
TX-1
...
TX-N
Beacon Chain
slot
parent-root
state-root
signature
randao
graffiti
deposit-root
ATT-0
ATT-1
...
ATT-N
DEP-0
DEP-1
EXIT-0
EXIT-1
Beacon Chain
slot
parent-root
state-root
signature
randao
graffiti
deposit-root
ATT-0
ATT-1
...
ATT-N
DEP-0
DEP-1
EXIT-0
EXIT-1
Beacon Chain
slot
parent-root
state-root
signature
randao
graffiti
deposit-root
ATT-0
ATT-1
...
ATT-N
DEP-0
DEP-1
EXIT-0
EXIT-1
Execution Layer
parent-hash
state-root
...
base-fee
TX-0
TX-1
...
TX-N
Beacon Chain
slot
parent-root
state-root
signature
randao
graffiti
deposit-root
ATT-0
ATT-1
...
ATT-N
DEP-0
DEP-1
EXIT-0
EXIT-1
Execution Layer
parent-hash
state-root
...
base-fee
TX-0
TX-1
...
TX-N

Implementations - EL

geth/go

nethermind/C#

besu/java

erigon/go

reth/rust

silkwarm/c++

ethereumjs/TS

Implementations - CL

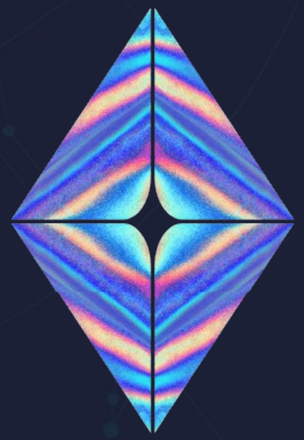
prysm/go

lighthouse/rust

teku/java

nimbus/nim

lodestar/TS

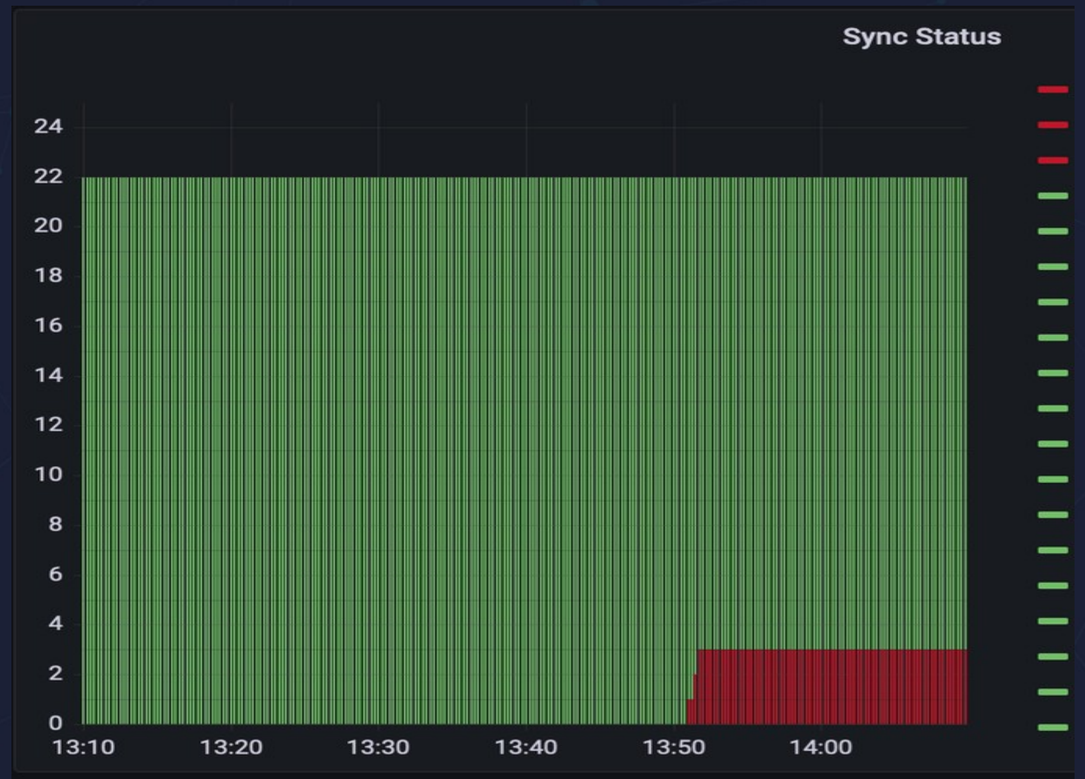


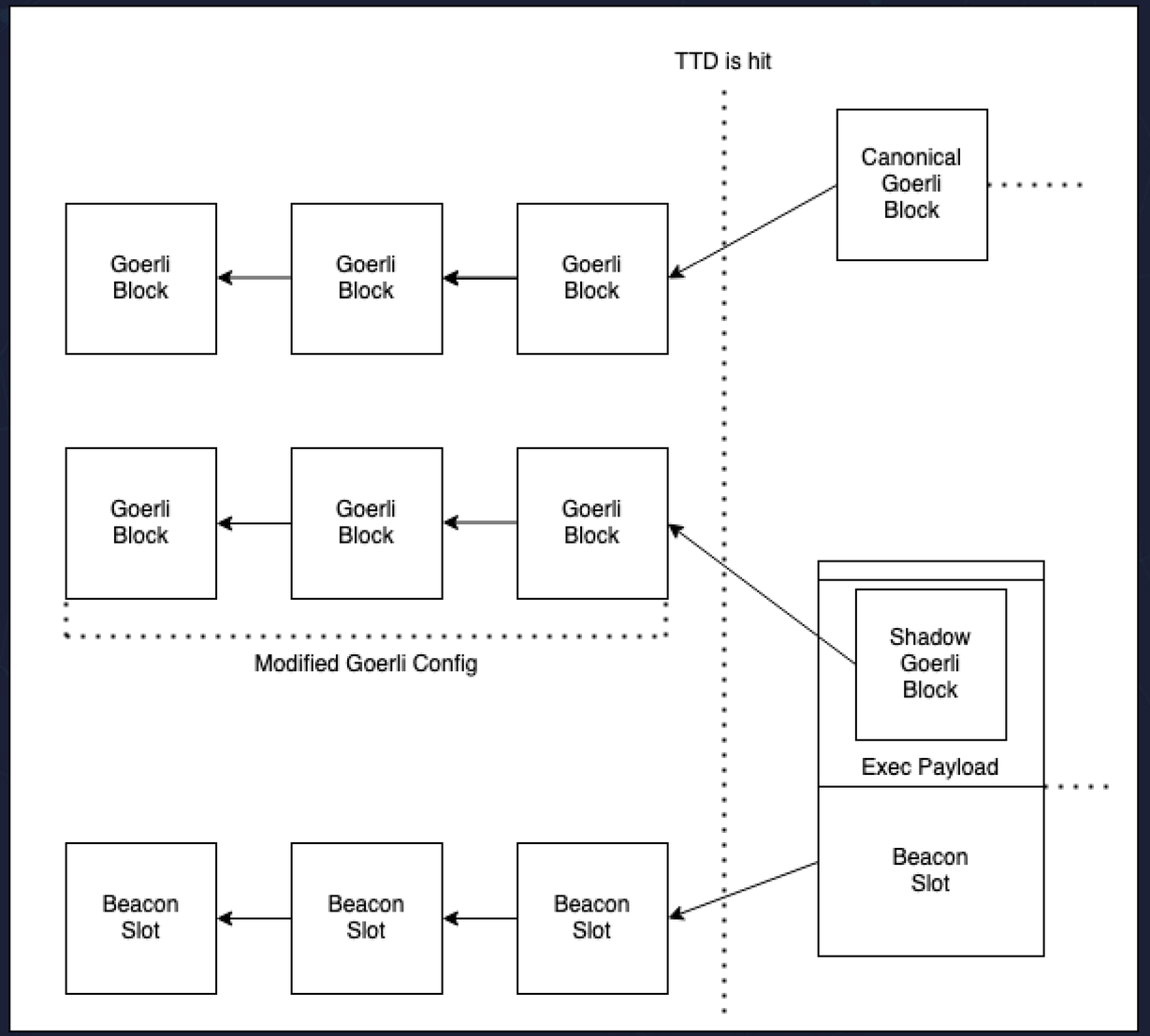
Testing

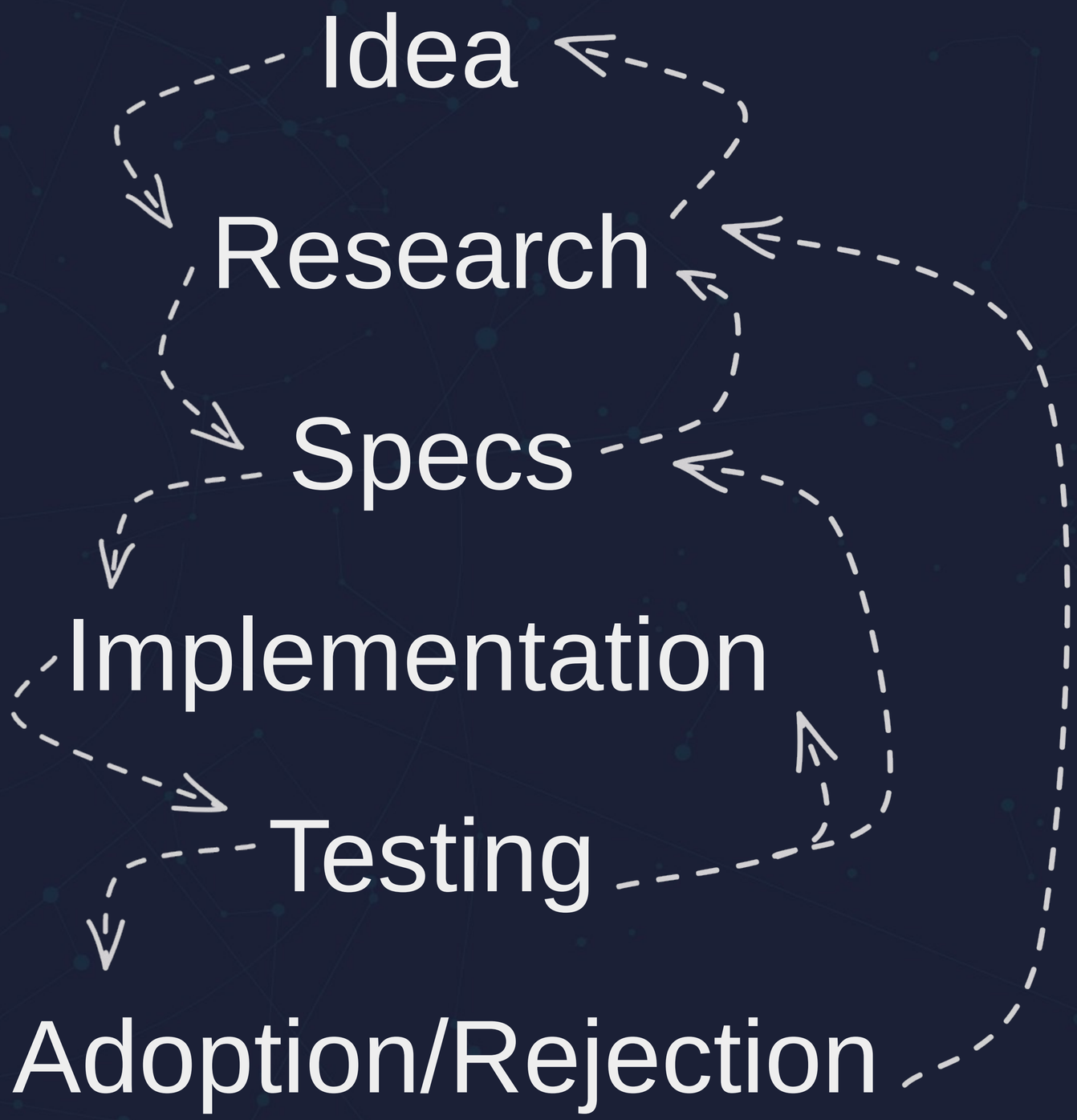
https://github.com/ethereum/tests
https://github.com/ethereum/retesteth
https://github.cosm/ethereum/execution-spec-tests
https://github.com/lightclient/rpctestgen
https://github.com/ethereum/hive
https://github.com/kurtosis-tech/kurtosis
https://github.com/MariusVanDerWijden/FuzzyVM
https://github.com/MariusVanDerWijden/tx-fuzz

Other tests

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






Idea
Research
Specs
Implementation
Testing
Adoption/Rejection

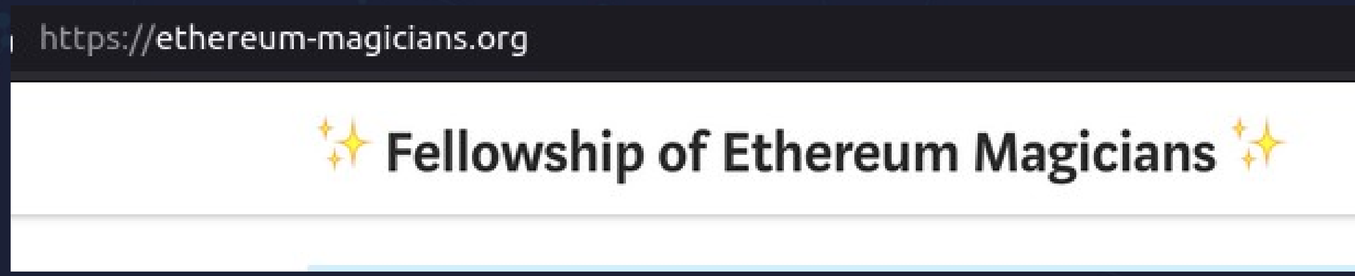
Coordination

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

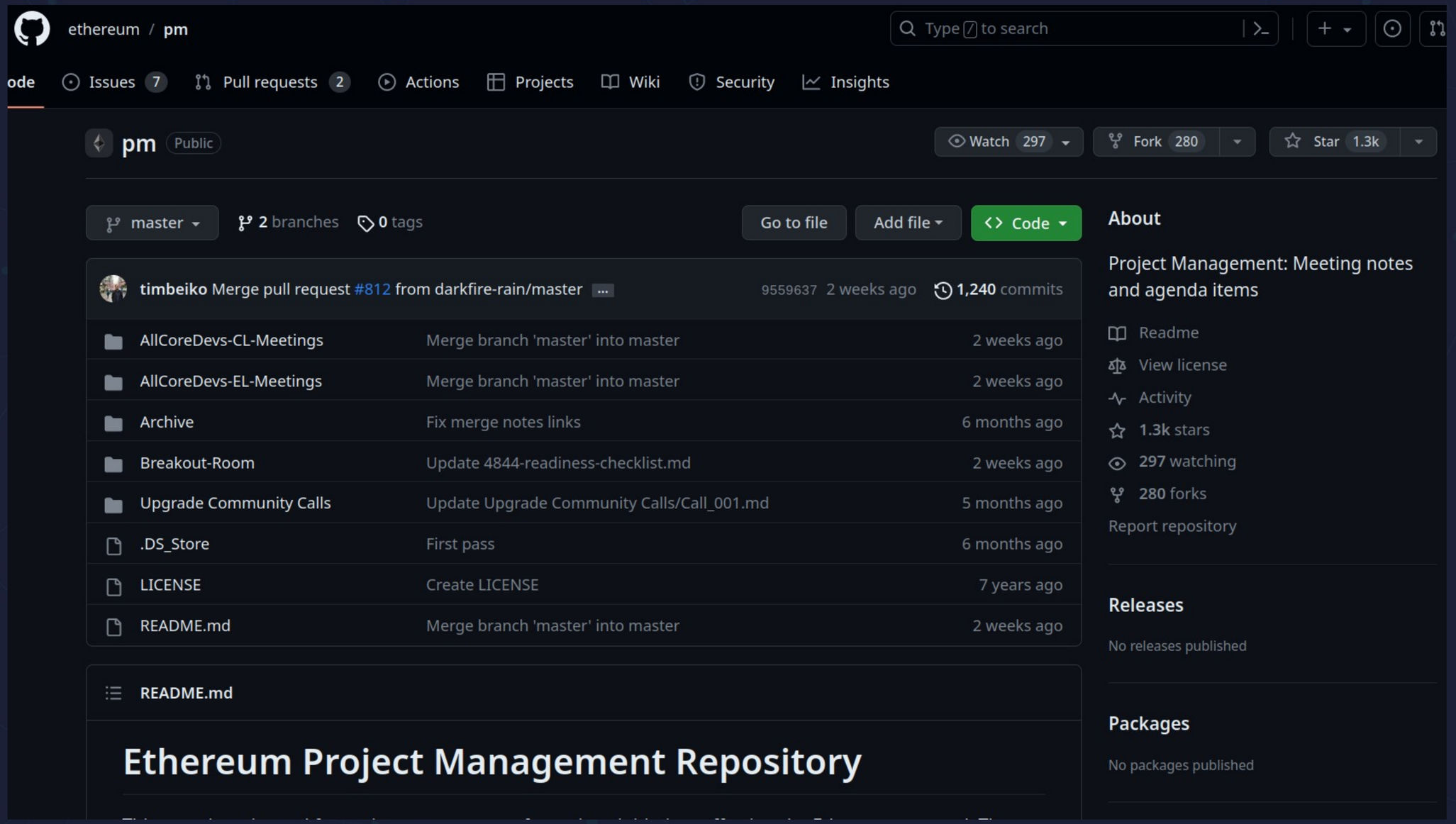
EIPs – Eth Magicians, EIPIP, Cat herders

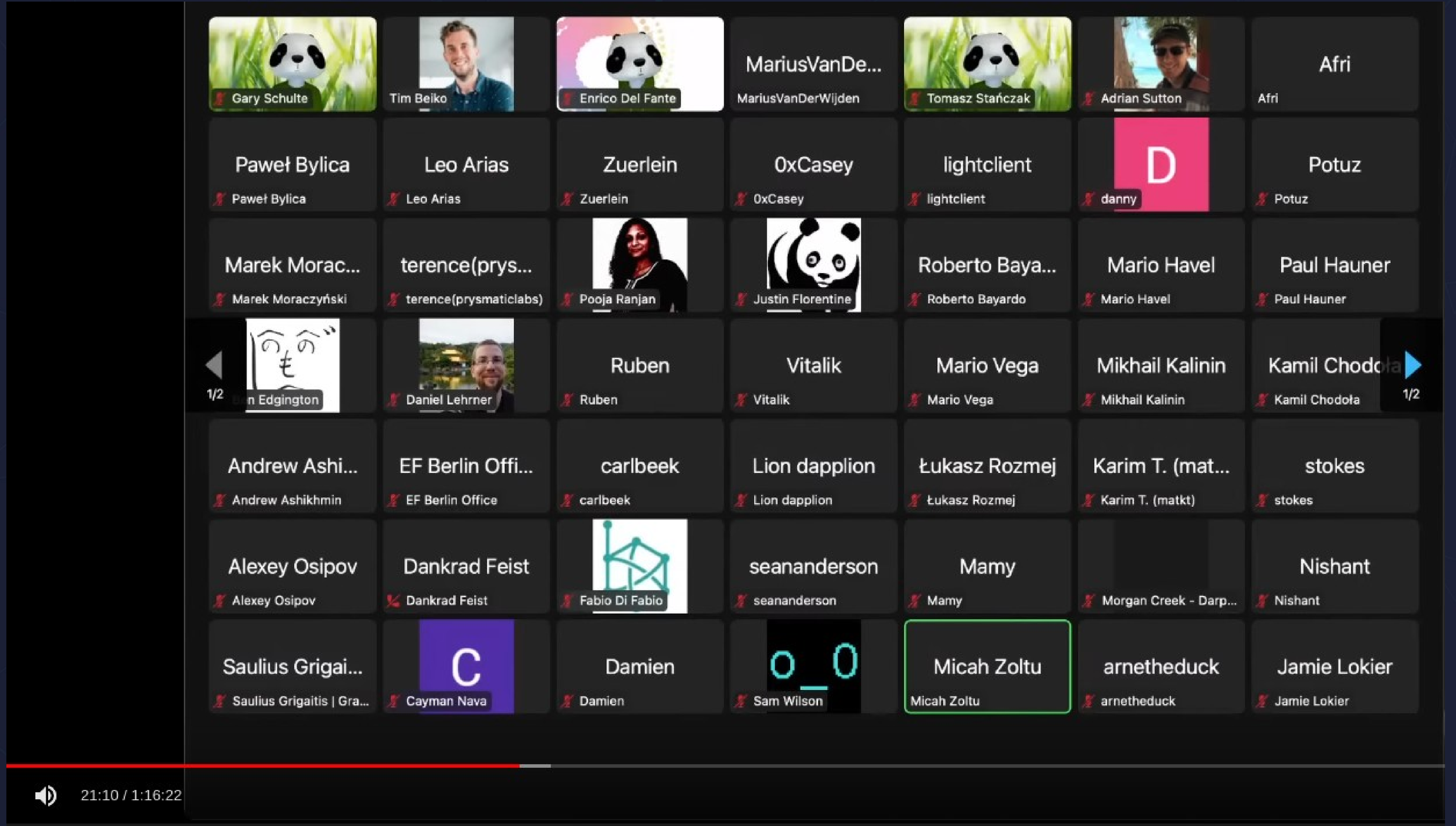
R&D Discord

Ethresear.ch



Coordination





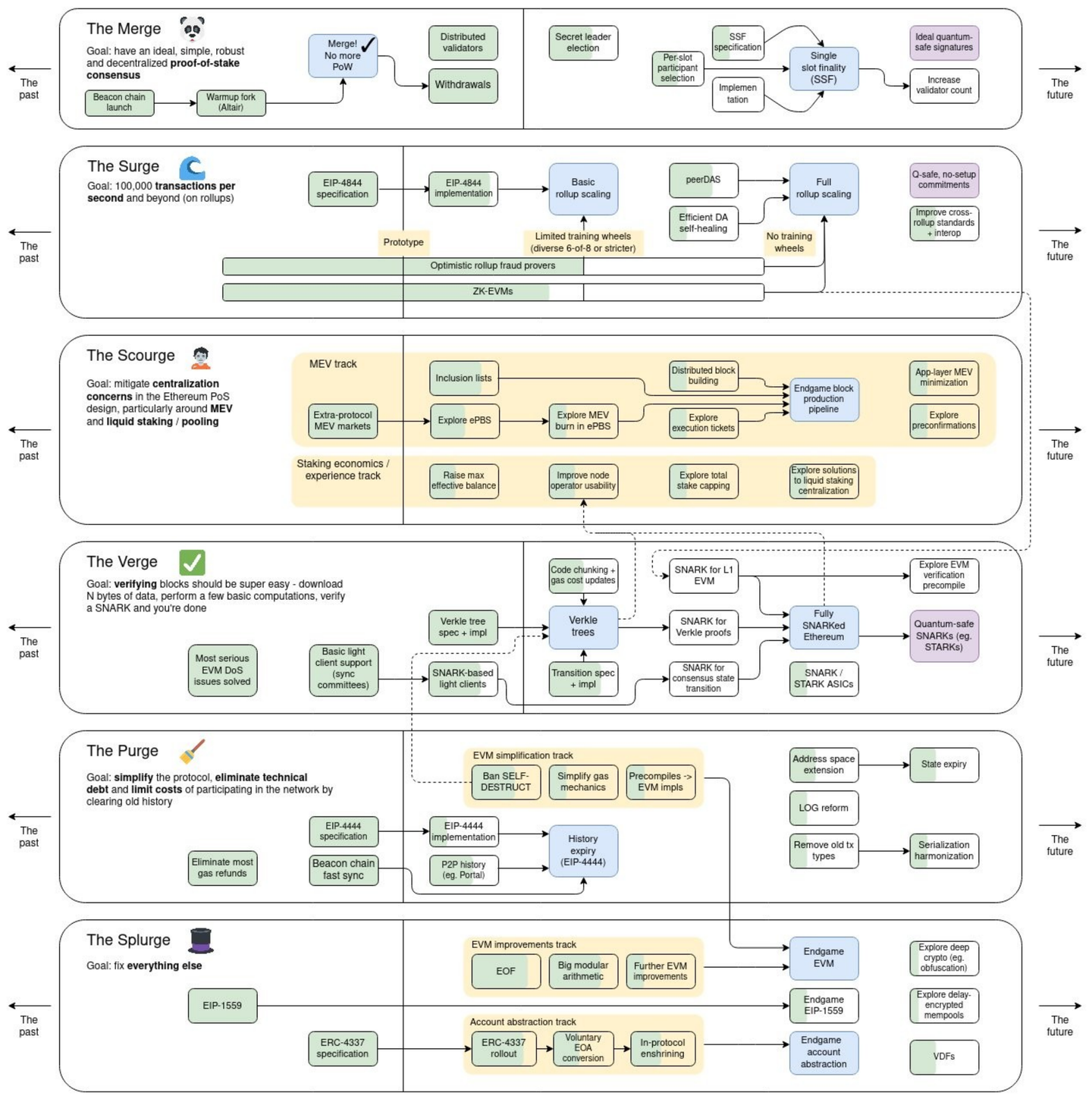
21:10 / 1:16:22

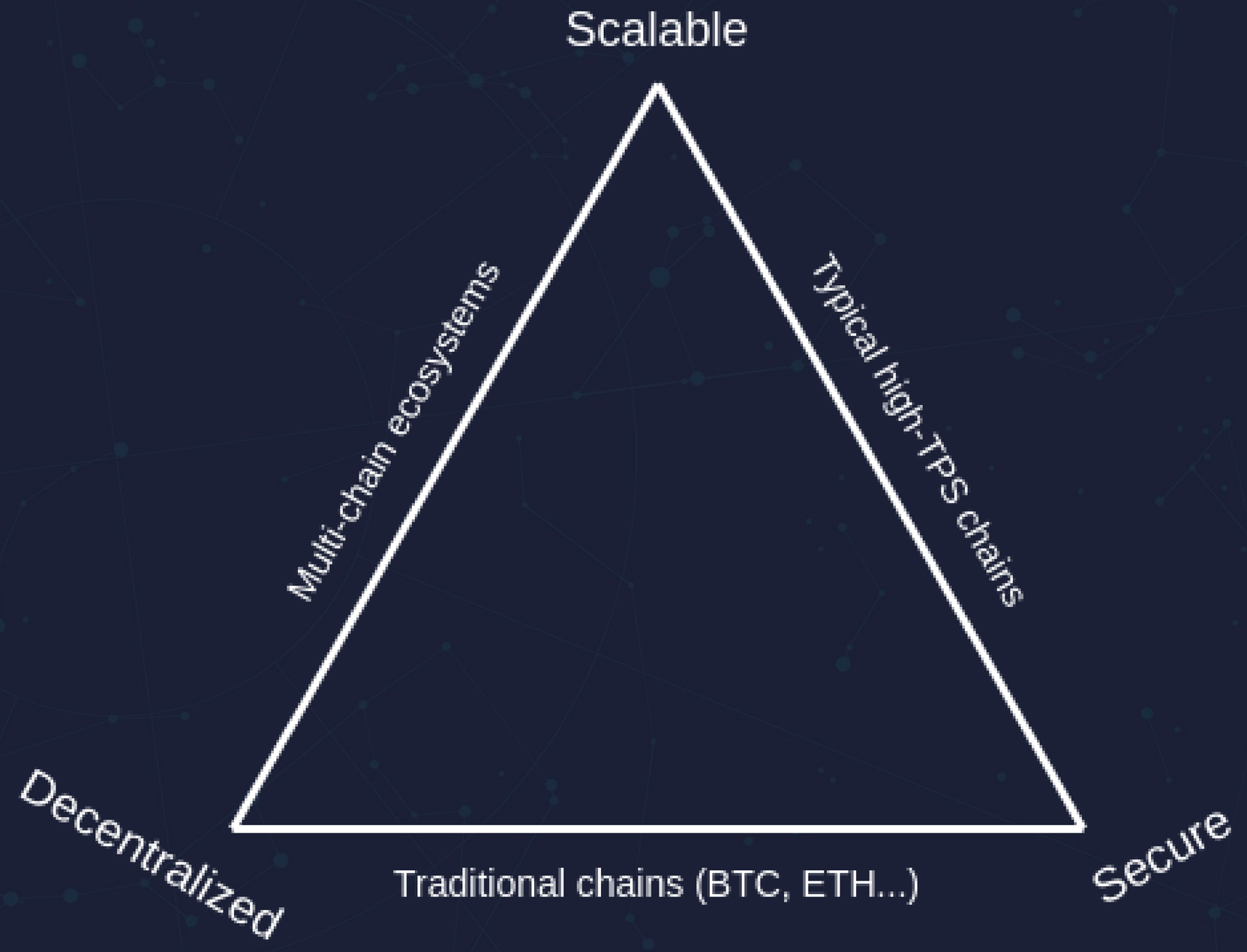
Ethereum Core Devs Meeting #145 [2022-8-18]

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

200 Dislike Share Clip Save

Research and roadmap


The Merge
Goal: have an ideal, simple, robust and decentralized proof-of-stake consensus
Beacon chain launch
Warmup fork (Altair)
Merge! No more PoW
Distributed validators
Withdrawals
Secret leader election
Per-slot participant selection
SSF specification
Implemen tation
Single slot finality (SSF)
Ideal quantum-safe signatures
Increase validator count
The past
The future
The Surge
Goal: 100,000 transactions per second and beyond (on rollups)
EIP-4844 specification
EIP-4844 implementation
Basic rollup scaling
peerDAS
Efficient DA self-healing
Full rollup scaling
Q-safe, no-setup commitments
Improve cross-rollup standards + interop
Prototype
Limited training wheels (diverse 6-of-8 or stricter)
No training wheels
Optimistic rollup fraud provers
ZK-EVMs
The Scourge
Goal: mitigate centralization concerns in the Ethereum PoS design, particularly around MEV and liquid staking / pooling
MEV track
Inclusion lists
Distributed block building
Endgame block production pipeline
App-layer MEV minimization
Extra-protocol MEV markets
Explore ePBS
Explore MEV burn in ePBS
Explore execution tickets
Explore preconfirmations
Staking economics / experience track
Raise max effective balance
Improve node operator usability
Explore total stake capping
Explore solutions to liquid staking centralization
The Verge
Goal: verifying blocks should be super easy - download N bytes of data, perform a few basic computations, verify a SNARK and you're done
Code chunking + gas cost updates
SNARK for L1 EVM
Explore EVM verification precompile
Verkle tree spec + impl
Verkle trees
SNARK for Verkle proofs
Fully SNARKed Ethereum
Quantum-safe SNARKs (eg. STARKs)
Most serious EVM DoS issues solved
Basic light client support (sync committees)
SNARK-based light clients
Transition spec + impl
SNARK for consensus state transition
SNARK / STARK ASICs
The Purge
Goal: simplify the protocol, eliminate technical debt and limit costs of participating in the network by clearing old history
EVM simplification track
Ban SELF-DESTRUCT
Simplify gas mechanics
Precompiles -> EVM impls
Address space extension
State expiry
LOG reform
EIP-4444 specification
EIP-4444 implementation
History expiry (EIP-4444)
Remove old tx types
Serialization harmonization
Eliminate most gas refunds
Beacon chain fast sync
P2P history (eg. Portal)
The Splurge
Goal: fix everything else
EVM improvements track
EOF
Big modular arithmetic
Further EVM improvements
Endgame EVM
Explore deep crypto (eg. obfuscation)
EIP-1559
Endgame EIP-1559
Explore delay-encrypted mempools
Account abstraction track
ERC-4337 specification
ERC-4337 rollout
Voluntary EOA conversion
In-protocol enshrining
Endgame account abstraction
VDFs


Scalable
Multi-chain ecosystems
Typical high-TPS chains
Decentralized
Traditional chains (BTC, ETH...)
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?!

Check out resources

Find more and share

Find your niche and contribute

Checkout EPF projects

EPF cohorts history

https://github.com/eth-protocol-fellows/cohort-four/

https://github.com/eth-protocol-fellows/cohort-three/


That's all Folks!