CONSENSYS

Besu Product Update

Matt Nelson
PM - Besu & Web3Signer Consensys

Agenda

1	*Roadmap Review*
2	*Besu & Public / Hybrid Networks*
3	*Besu & Layer 2s*
4	*Modular Besu & Post-Merge Architecture*
5	*Steering & Contributing to Besu & Core Dev*

Roadmap Review

Why Change Besu? Refining our Mission

Consensus Engine

Besu

Key part of PoS validator stack and execution + consensus combo. Besu roadmap will follow the Ethereum spec and maintain compatibility with mainnet.

Ethereum network participation requires this stack, private networks remain unchanged

Feature development: Prioritize an enterprise shift to public networks by prioritizing institutional features and security on mainnet and by simplifying staking

Post Merge: Focus on performance, modularization, and resolving tech debt

Network Participation

Besu enables **network participation** for institutions. It supports **Ethereum** post-Merge, **private networks**, **mining networks** (Ethereum Classic). We aim to evolve for the **multi-chain world** (EVM-compatible, rollups, hybrid, more)

Besu provides a **familiar license**, a **familiar programming language**, and institutional-grade features for running low-overhead nodes, **staking** Ether, and interacting with blockchain networks

Besu aims to be the **best and most flexible infrastructure** for institutions looking to participate in **blockchain networks**

Hyperledger Besu Roadmap 2023
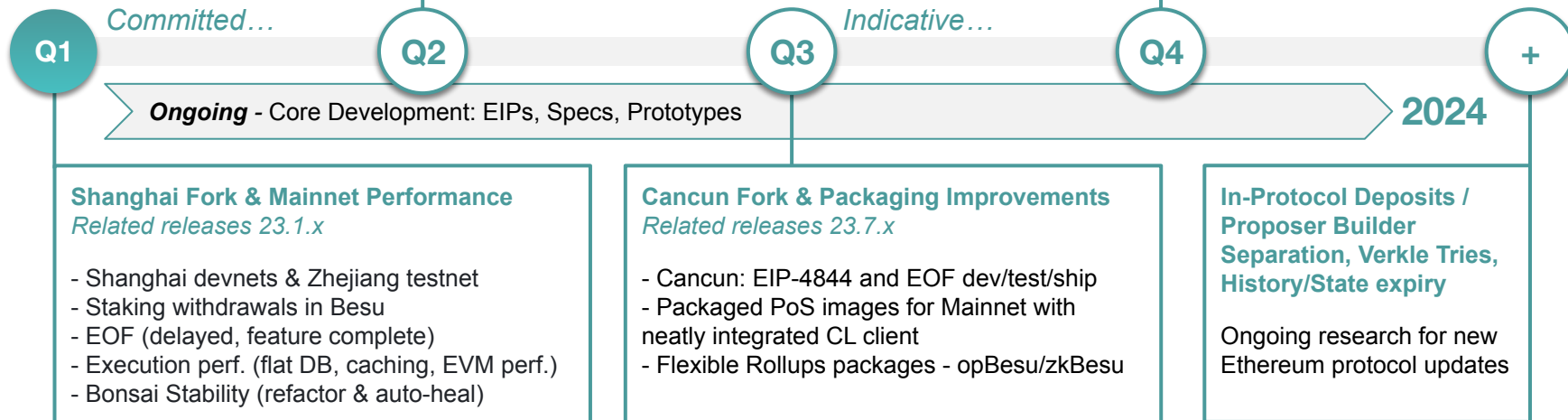
HYPERLEDGER BESU

Rollups & Staking Experience
Related releases 23.4.x

- Ship Shanghai, wrap up staking UX improvements
- Besu as a rollups engine (plugable crypto, RPC, rollup-compatible state management)
- Prepare for Cancun

Multi-Chain Besu, Flexible Infrastructure
Related releases 23.10.x

- Codebase tailored for multi-use case support (Mainnet, private nets, EVM-compatible L1/L2s)
- Tooling & features for infrastructure providers
- Besu as an Ethereum reference client in Java, bringing enterprise to public nets

Committed…   *Indicative…*

Q1 **Q2** **Q3** **Q4** **+**

Ongoing - Core Development: EIPs, Specs, Prototypes   **2024**

Shanghai Fork & Mainnet Performance
Related releases 23.1.x

- Shanghai devnets & Zhejiang testnet
- Staking withdrawals in Besu
- EOF (delayed, feature complete)
- Execution perf. (flat DB, caching, EVM perf.)
- Bonsai Stability (refactor & auto-heal)

Cancun Fork & Packaging Improvements
Related releases 23.7.x

- Cancun: EIP-4844 and EOF dev/test/ship
- Packaged PoS images for Mainnet with neatly integrated CL client
- Flexible Rollups packages - opBesu/zkBesu

In-Protocol Deposits / Proposer Builder Separation, Verkle Tries, History/State expiry

Ongoing research for new Ethereum protocol updates

HYPERLEDGER BESU

Besu & Public / Hybrid Networks

Public & Hybrid Networks in the news…

[JPMorgan Executes Its First DeFi Trade Using Public Blockchain](#)

[Visa Proposal Would Bring Ethereum Users One Step Closer To Being Their Own Bank](#)

['Big Four' Australian Bank Issues Stablecoin On Ethereum](#)

['Deposit Tokens' Could Trade On DeFi Like Stablecoins: JPMorgan](#)
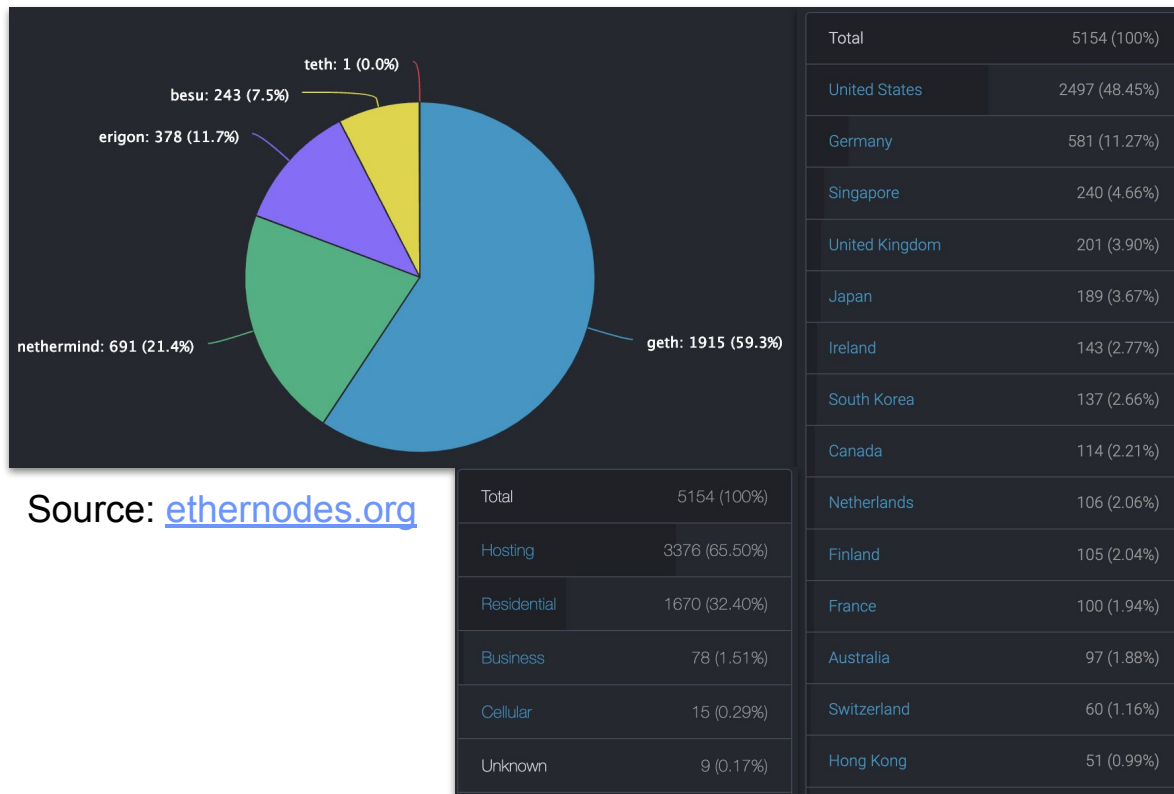
[Brazil's Largest Digital Bank Nubank to Launch Native Crypto on Polygon Blockchain](#)

[Goldman Sachs, Hamilton Lane and Siemens are among institutions choosing to represent real-world assets as digital tokens on a blockchain](#)

[Brazil's central bank unveils pilot digital real CBDC on Besu](#)

HYPERLEDGER
BESU

Besu is a Complete Mainnet Client

- 4 Main Clients make up the Execution Layer and have prominent voices among Ethereum Core Developers

- Besu participates in and steers network upgrades on Ethereum Mainnet

- Besu has historically been used for private networks, but has climbed from ~1% network share pre-Merge
  - Differentiated by Bonsai

- No other client has been built with the same enterprise features used in private networks and infrastructure

Source: ethernodes.org

Total	5154 (100%)
United States	2497 (48.45%)
Germany	581 (11.27%)
Singapore	240 (4.66%)
United Kingdom	201 (3.90%)
Japan	189 (3.67%)
Ireland	143 (2.77%)
South Korea	137 (2.66%)
Canada	114 (2.21%)
Netherlands	106 (2.06%)
Finland	105 (2.04%)
France	100 (1.94%)
Australia	97 (1.88%)
Switzerland	60 (1.16%)
Hong Kong	51 (0.99%)

Total	5154 (100%)
Hosting	3376 (65.50%)
Residential	1670 (32.40%)
Business	78 (1.51%)
Cellular	15 (0.29%)
Unknown	9 (0.17%)

Pie chart:
- geth: 1915 (59.3%)
- nethermind: 691 (21.4%)
- erigon: 378 (11.7%)
- besu: 243 (7.5%)
- teth: 1 (0.0%)

Besu is built on standards to support Hybrid Networks

palm.network

"The Palm network uses IBFT 2.0 Proof of Authority (PoA) consensus, with network validators being run by key stakeholders. The network offers a fast transaction speed and super low minting costs… An automated bridge relay service connects payment tokens, like DAI, and NFTs on Ethereum and the Palm network, with bridging contracts deployed on both networks to manage the connection."

Hybrid infrastructure customizes and scales "off-chain" while taking advantage of the security and network effects of Ethereum Mainnet and its standards.

Evolution of Besu networks:

- Private net → Hybrid → Public infrastructure (L2, L3)
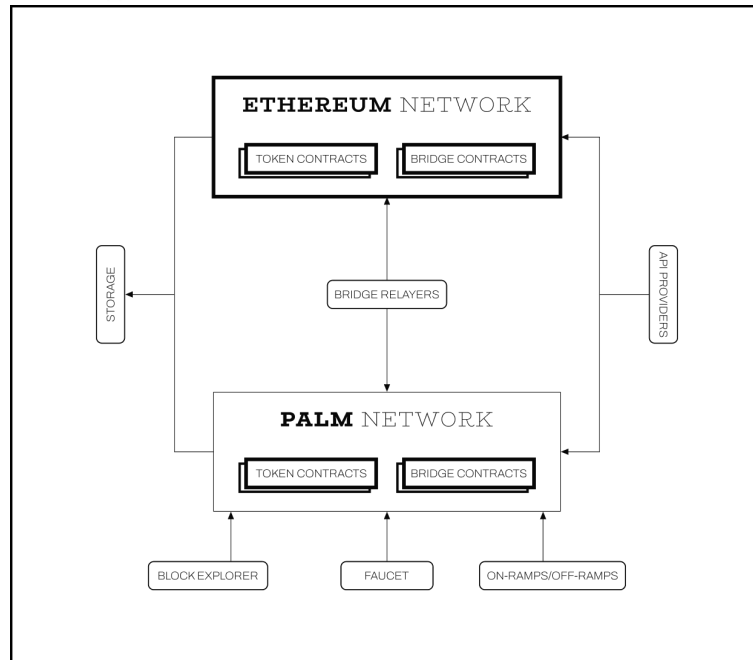
What does Ethereum Participation mean for Enterprise?

Public network participation is **rewarding**...
- Learn to operate node infrastructure, help with network security via staking ETH, and engage a new community of developers and users
- Staking rewards network participation with ~12% returns on an initial stake after the Merge (lower rewards prior)

Public network participation is a **new opportunity**…
- Proof of Stake Ethereum is sustainable, scalable, and open for business
- Public networks provide new ways of interacting with financial and cryptographic primitives, launching distributed apps, doing business with self-sovereign users, and accessing liquidity and services with DeFi

Enterprises can feel safe and secure participating in public networks…
- We are working to provide education around staking, business and apps on public Ethereum, and more for enterprise and institutions
- Regulators are waiting for experts to create opinions and standards to get everyone talking

HYPERLEDGER
BESU

Besu & Layer 2s

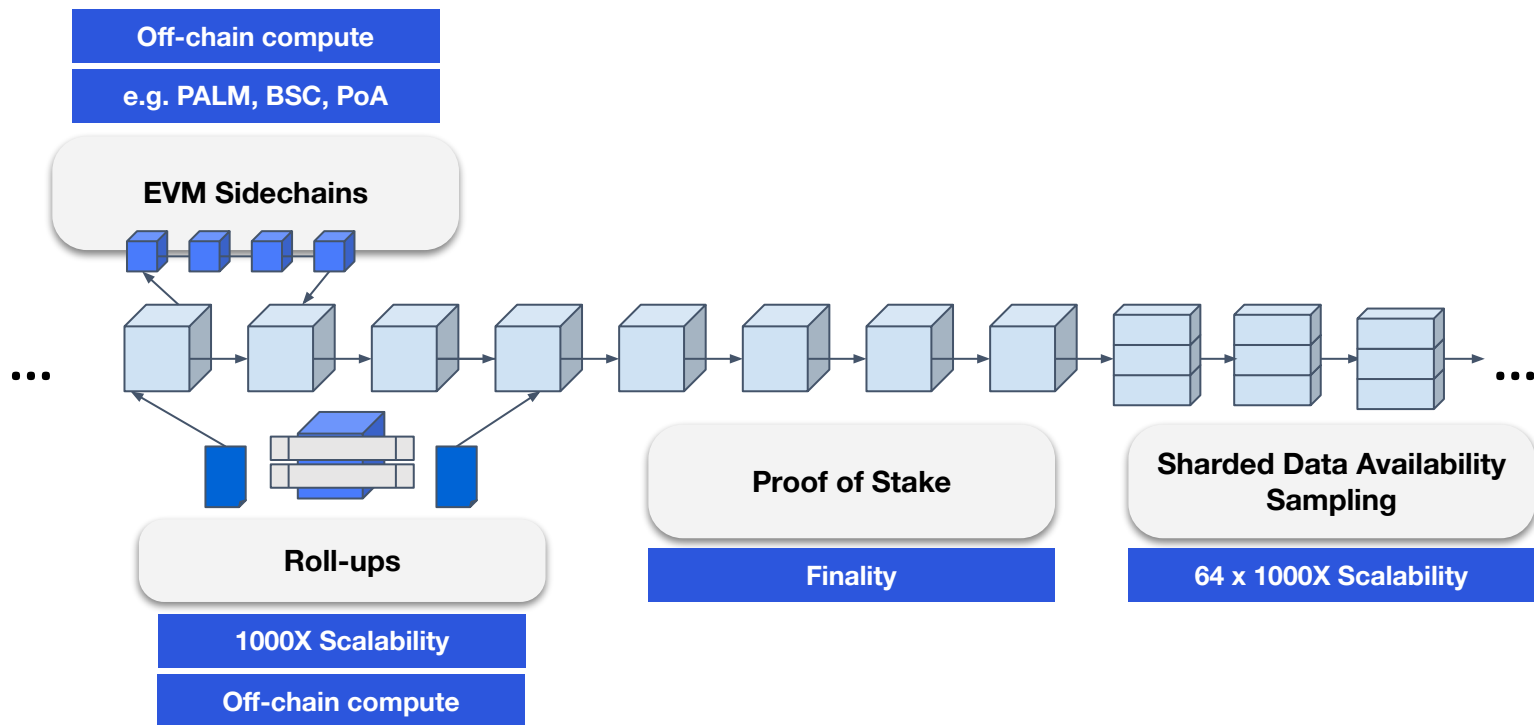# Institutions & DeFi Need More than Layer 1

- **Throughput** on mainnet Ethereum is becoming a bottleneck as institutions and users struggle with queues, fees, and long finality times

- While auditability is key to Ethereum's security and success, institutions and users require transaction **privacy** for certain use-cases on-chain

- Utility tokens and stablecoins require privacy and scalability to power revolutionary use-cases for CeFi like CBDCs or high throughput use-cases like micro-transactions

- Compatibility with Layer 1 smart contracts and composable platforms are key to ecosystem success but have key technical challenges for adoption by businesses and new users

- Layer 1 token transfers are too expensive and non-private (and lack compatibility with ecosystem)

Scalability Increasing

Layer 1 & 2 Scalability Solutions Increasing Throughput by x10,000

Off-chain compute

e.g. PALM, BSC, PoA

EVM Sidechains

Roll-ups

1000X Scalability

Off-chain compute

Proof of Stake

Finality

Sharded Data Availability Sampling

64 x 1000X Scalability

Layer 2 Solutions are Scaling Ethereum

**Technology enhancements are taking place at two levels...**

Layer 2 (L2):
Multiple faster networks, with smaller # of nodes, leveraging Layer 1 for anchoring, interoperability, and security.

L2 **bridges & frameworks** interoperate assets, sidechains, & separate L1 blockchains

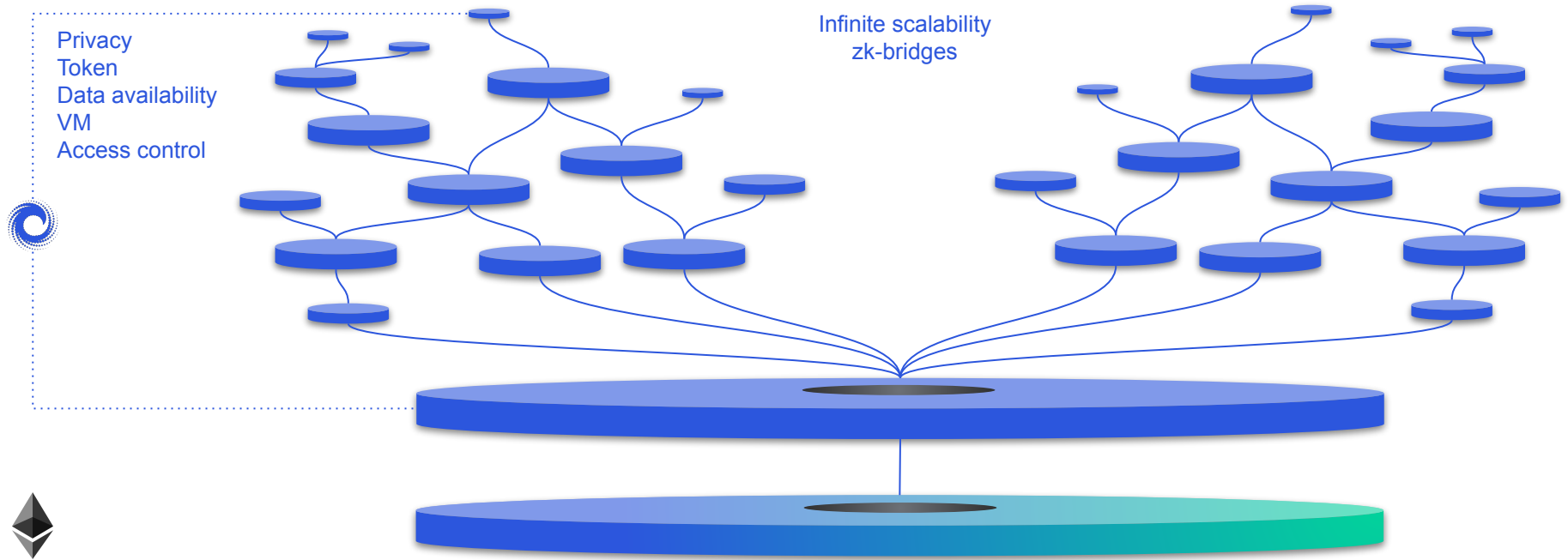**Rollups** batch and execute transactions off-chain

Layer 1 (L1):
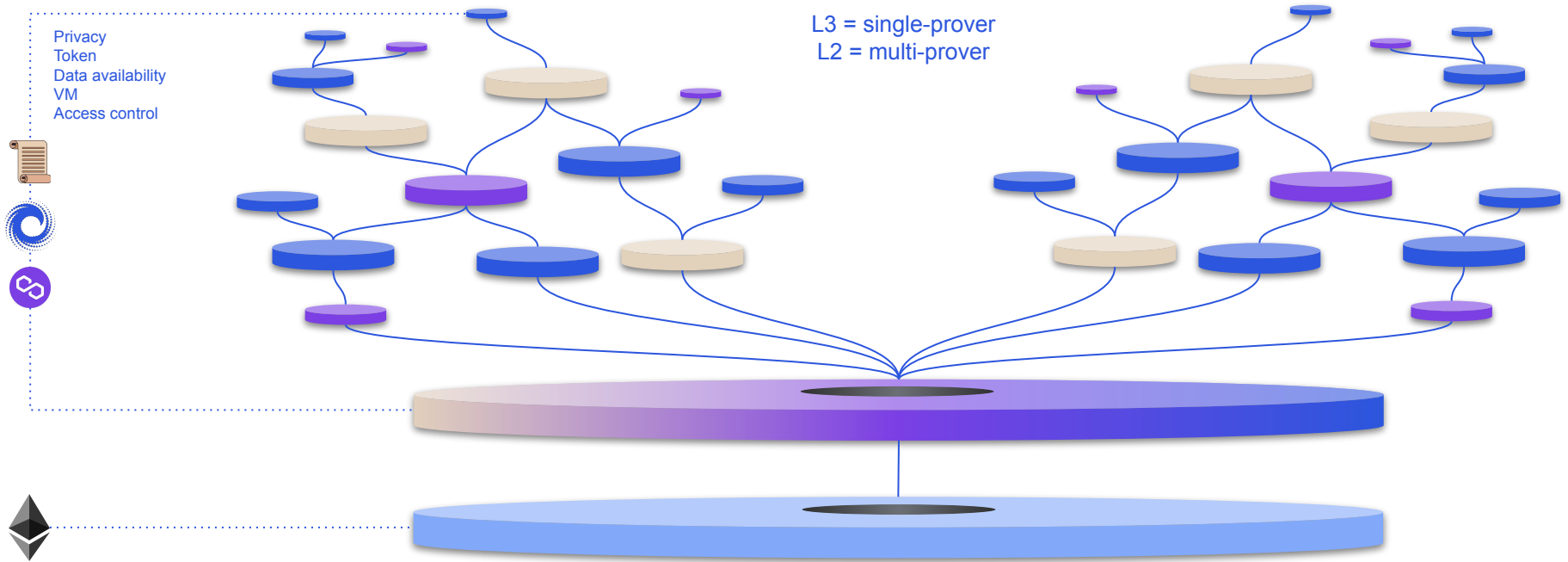Base settlement layer, most decentralized and resilient network with the largest # of nodes.
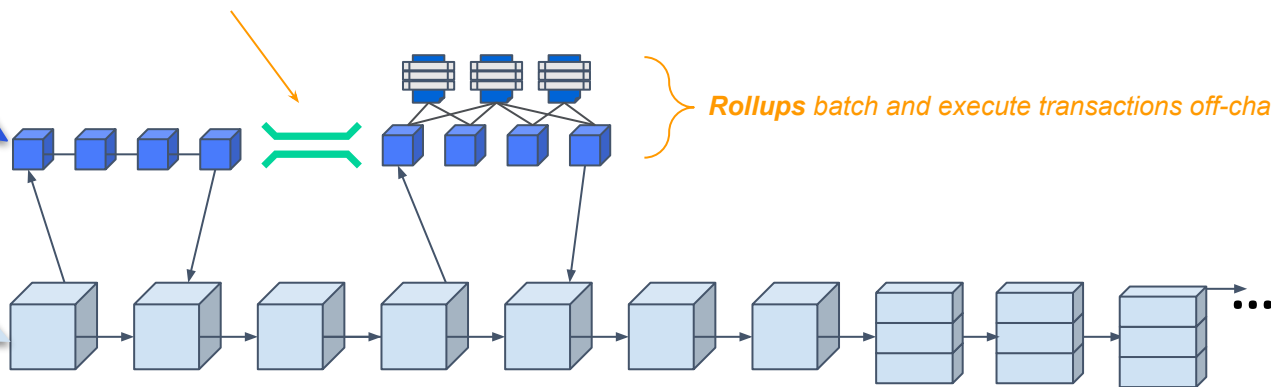
Note: Layer 1 may include "shards" in 2022, which are interconnected sub-networks that are still considered to be part of Layer 1.
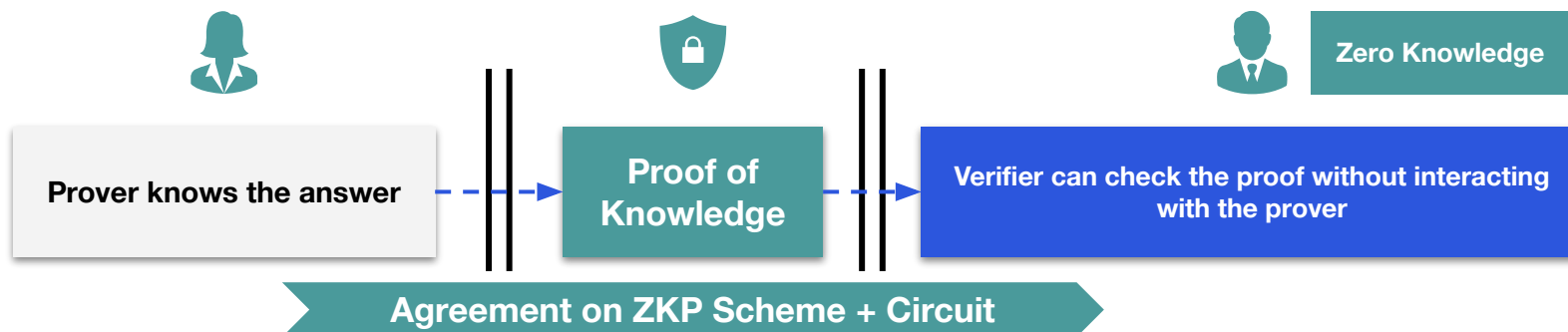
L3 brings Web2 to Web3

Privacy
Token
Data availability
VM
Access control

Infinite scalability
zk-bridges

L3 brings Web2 to Web3

Privacy
Token
Data availability
VM
Access control

L3 = single-prover
L2 = multi-prover

Proving knowledge without revealing it and without interactions

Prover knows the answer

Proof of Knowledge

Verifier can check the proof without interacting with the prover

Zero Knowledge

Agreement on ZKP Scheme + Circuit

ZKP Scheme

Different schemes with
different properties
Ex: Groth16, Plonk, Stark
gnark library

Circuit

Public Inputs
Private Inputs
Statements

Privacy Comparison: Private transaction vs zk-SNARKs privacy

Private transactions

Concept
Send and execute transactions only to/by a subset of participants. There is 1 public state and N private state for each privacy group/set of participants.
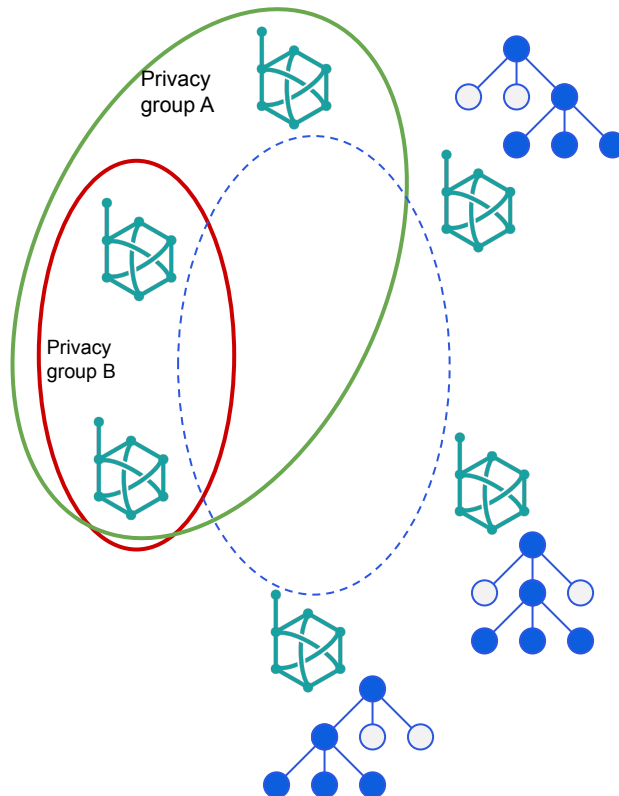
Pro
- EVM compatible
- Fully private

Cons
- Vulnerable to DDoS
- Siloed private state/no unified state → many use-cases (incl. assets) are impossible

Use-cases
Point to point private communication between participants, contract negotiation.

zk-SNARKs privacy (L3)

Concept
Account state is split across actors, transactions and state are hashed in a merkle tree, zk-SNARKs are generated to ensure correctness of the protocol and prevent double spend.

Pros
- Unified state - can perform token transfers at scale, fully private
- Higher throughput
- zk-EVMs make code compatible

Cons
- zk-EVMs are nascent
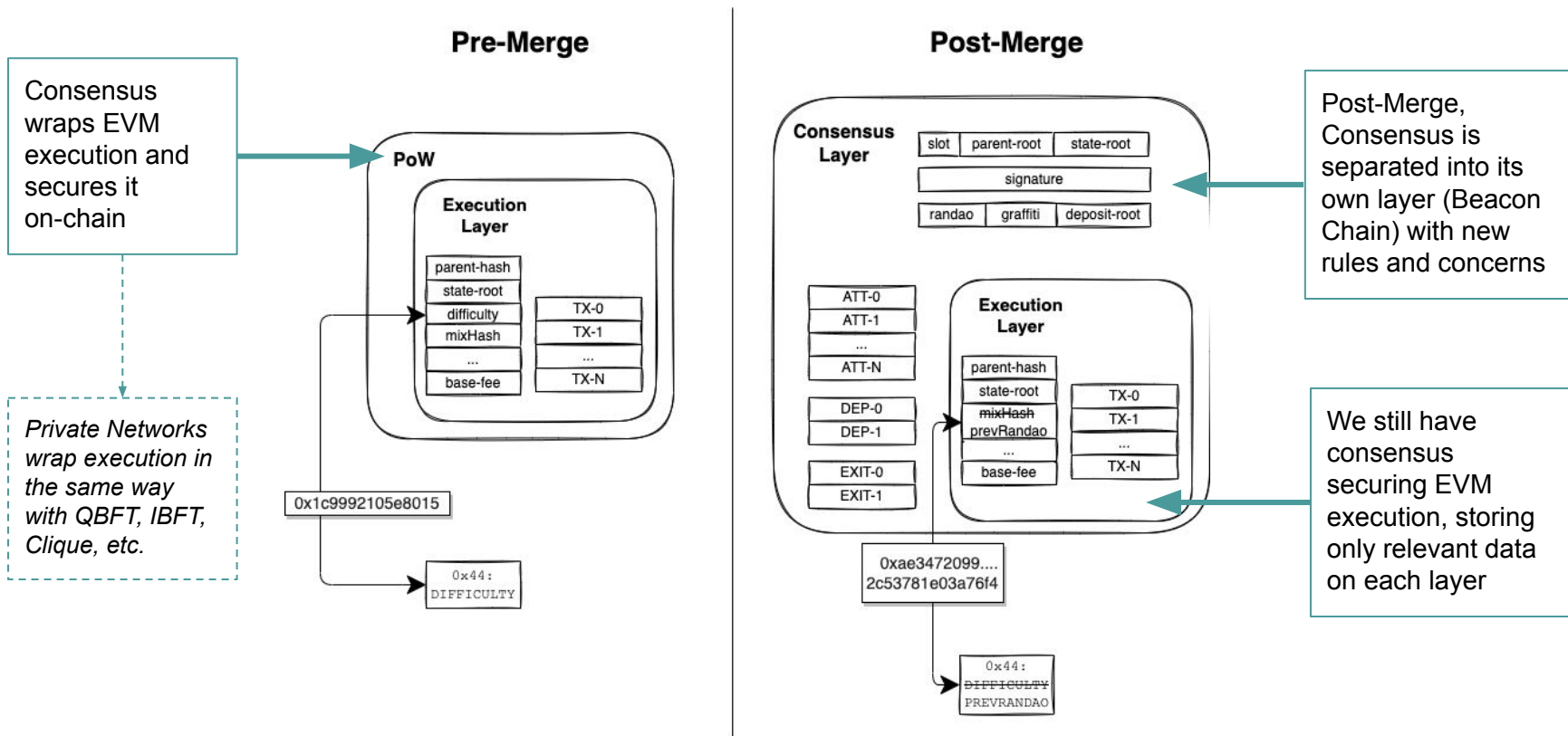- Require heavy machines to operate (but the technology is progressing at a high speed)

Use-cases
Assets trading & transfers, payment, otc, secondary markets, exchange, etc.

Privacy group A

Privacy group B

HYPERLEDGER
BESU

Modular Besu & Post-Merge Architecture

Merge Recap

Pre-Merge

Post-Merge

Consensus wraps EVM execution and secures it on-chain

Private Networks wrap execution in the same way with QBFT, IBFT, Clique, etc.

Post-Merge, Consensus is separated into its own layer (Beacon Chain) with new rules and concerns

We still have consensus securing EVM execution, storing only relevant data on each layer

Besu as an Execution Client

From our documentation:

Execution clients, such as Besu, manage the execution layer, including executing transactions and updating the world state. Execution clients serve JSON-RPC API requests and communicate with each other in a peer-to-peer network.
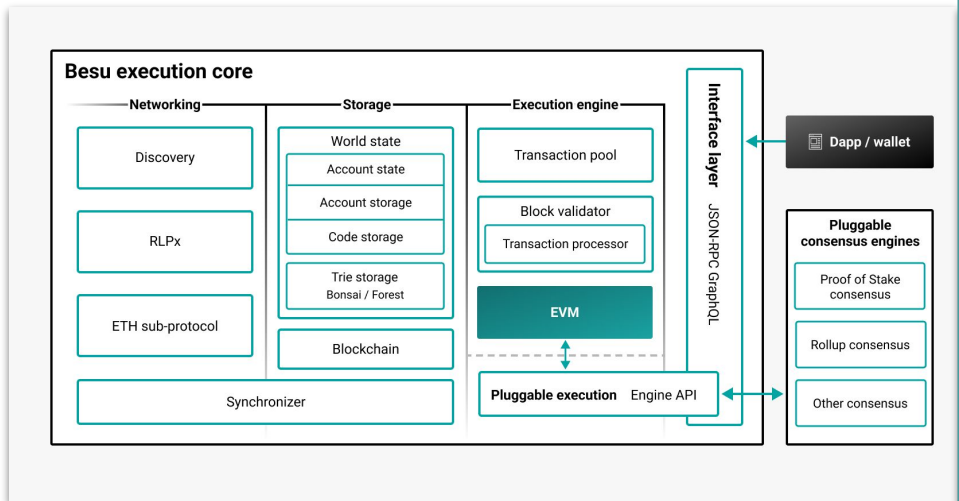
Engine API:

Novel set of APIs to enable maximum re-use of technology for proof of stake and to keep consensus operations quick (via a lightweight consensus client) as Ethereum scales
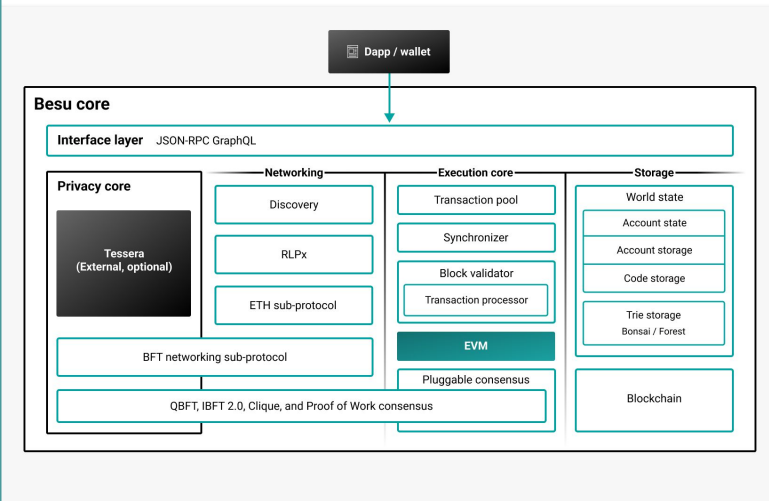

Ethereum Mainnet node

Consensus client

p2p

Engine API

REST-API

User

JSON-RPC API

Execution client

p2p
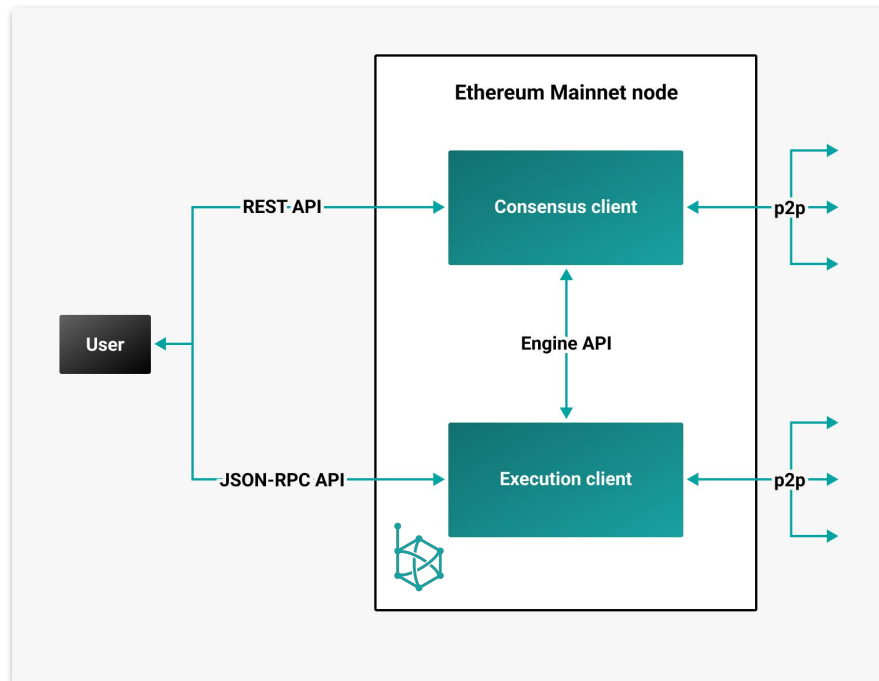
Two Client Abstractions

Public Network Architecture

Private Network Architecture

…over time we want to decouple these abstractions
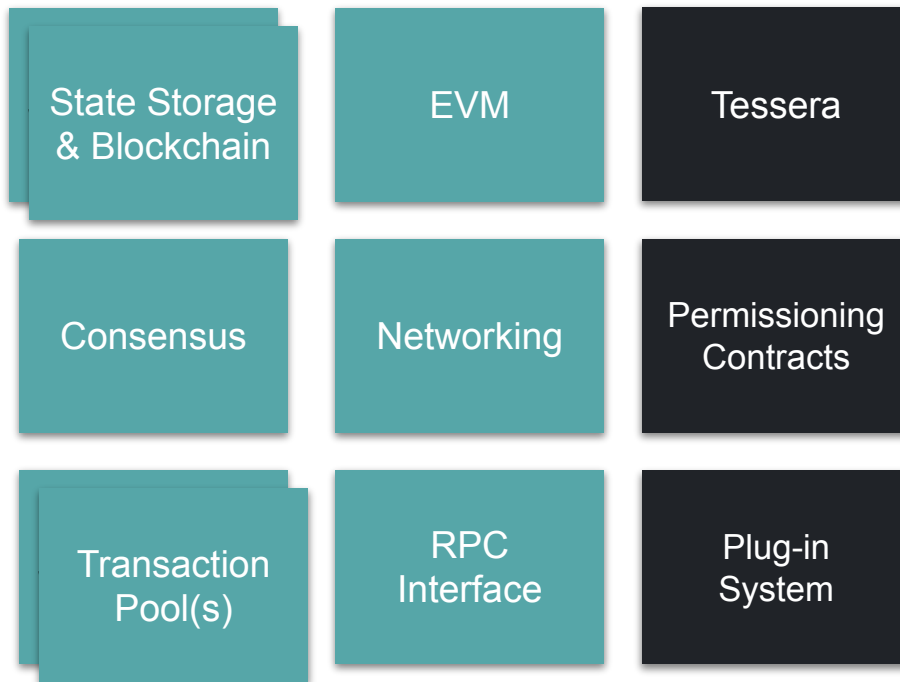
Componentization

Execution Engine

State Storage & Blockchain

EVM

Transaction Pool

Consensus

Networking

RPC Interface
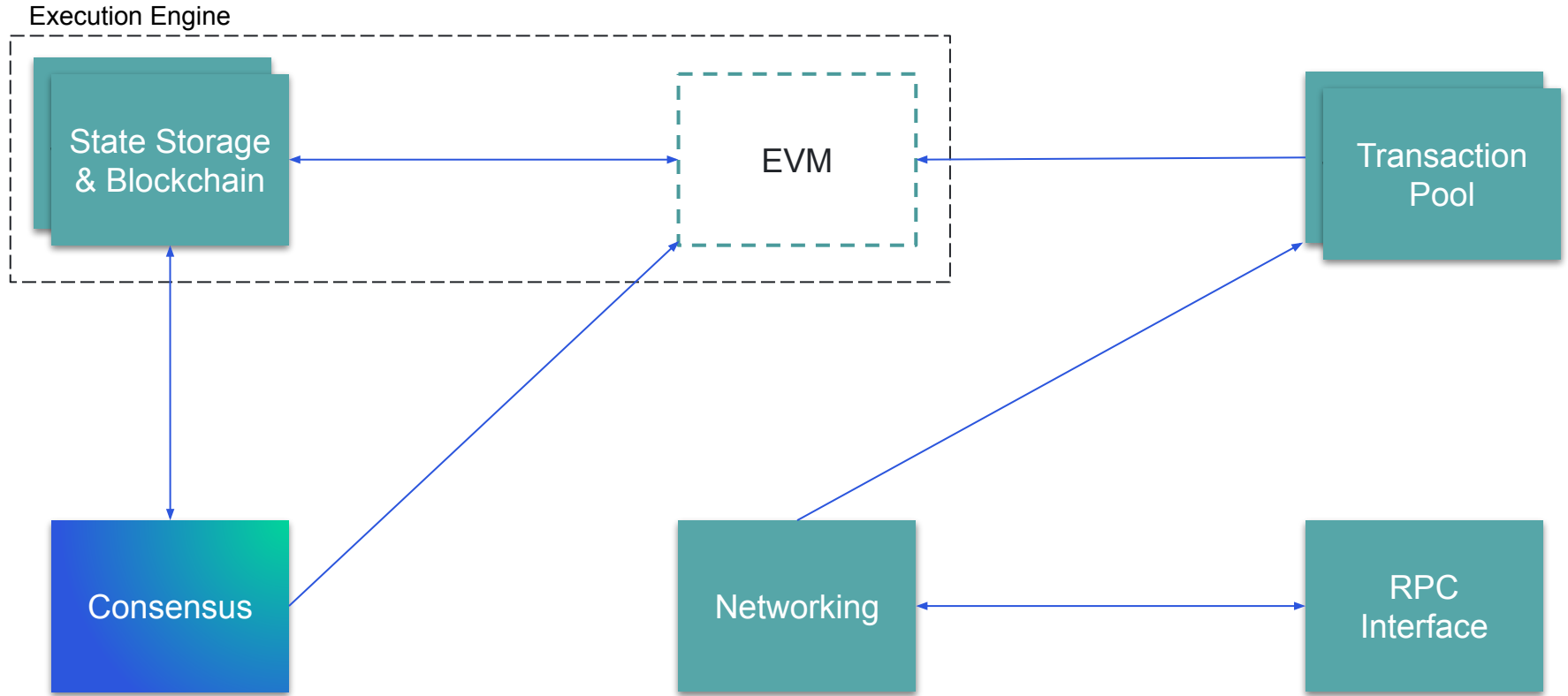
Reusable Building Blocks

Mainnet & PoS Chains

State Storage & Blockchain	EVM
Consensus	Networking
Transaction Pool	RPC Interface

Private Net

State Storage & Blockchain	EVM	Tessera
Consensus	Networking	Permissioning Contracts
Transaction Pool(s)	RPC Interface	Plug-in System
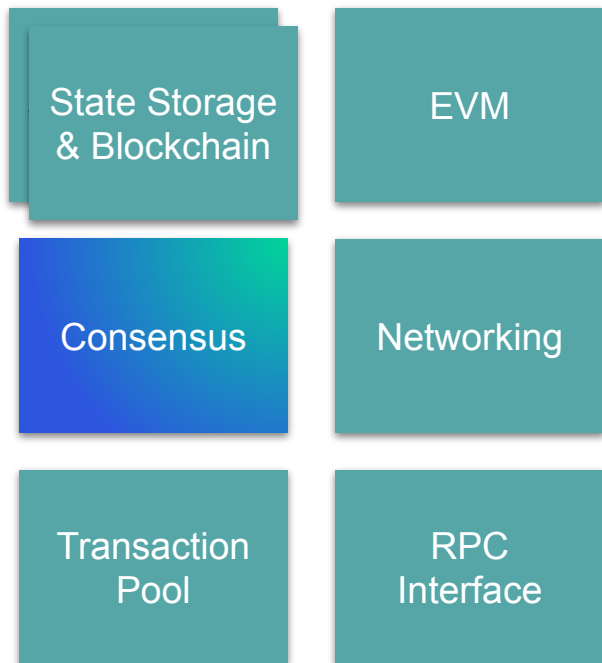
Reusable Building Blocks

Rollup

State Storage & Rollup State	EVM
Sequencer	Networking
Transaction Pool	RPC Interface

Hybrid Net

State Storage & Blockchain	EVM	Bridge Contracts
Consensus	Networking	Relayer
Transaction Pool(s)	RPC Interface	

HYPERLEDGER BESU
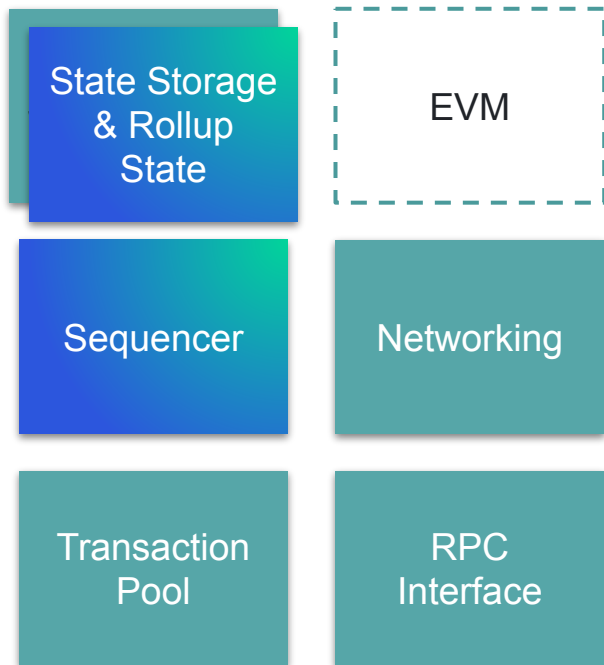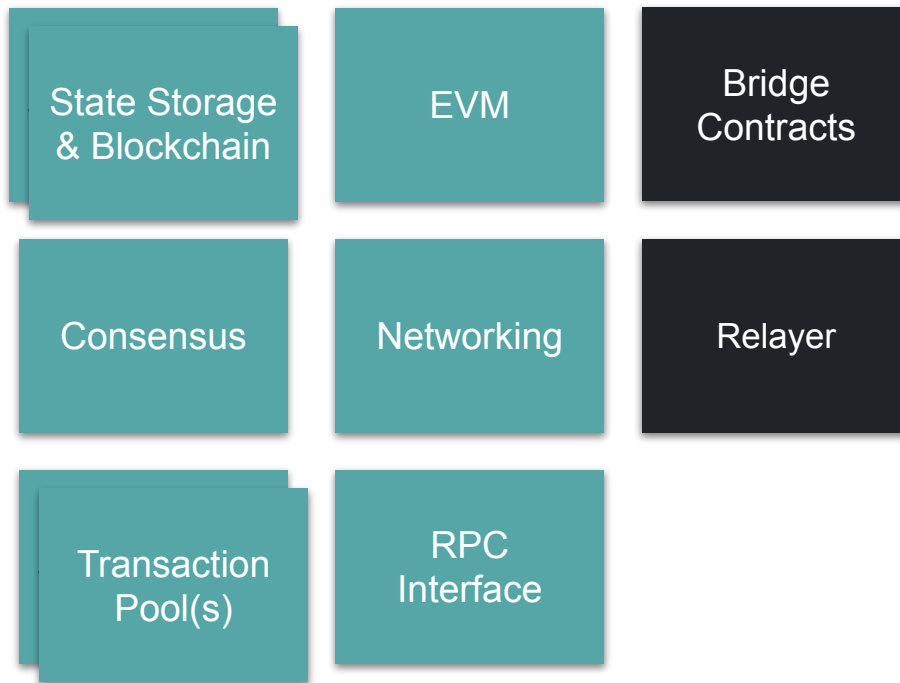
One Node Software, Many Configurations…

Public Network Architecture

Besu execution core

Networking
- Discovery
- RLPx
- ETH sub-protocol
- Synchronizer

Storage
- World state
  - Account state
  - Account storage
  - Code storage
- Trie storage
  Bonsai / Forest
- Blockchain

Execution engine
- Transaction pool
- Block validator
  - Transaction processor
- **EVM**
- **Pluggable execution**   Engine API

Interface layer   JSON-RPC GraphQL

Dapp / wallet

Pluggable consensus engines
- Proof of Stake consensus
- Rollup consensus
- Other consensus

HYPERLEDGER
BESU

Steering & Contributing to Besu & Core Development

Existing Process

Besu is primarily maintained by contributors from Consensys, Swirlds Labs, ETC Co-op, and Splunk
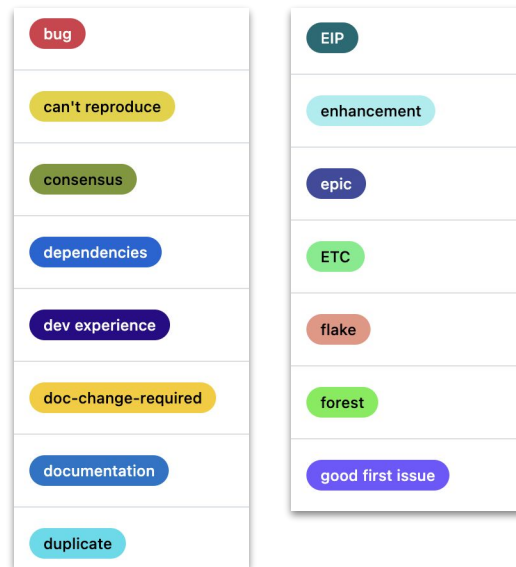
- These contributors are primarily focused on Public networks
- Web3Labs contributors focusing on private network feature maintenance, bug fixes, etc.

Contributing to Besu has existing guidelines

- Bi-weekly Contributor Calls - Open Forum, multiple Time-zones
- Roadmap routinely updated here
- Public Zenhub board to see issues, epics, and priorities of contributors (mainly Consensys)

Code Contributions…

- Labels
- Contributor calls
- More

bug
can't reproduce
consensus
dependencies
dev experience
doc-change-required
documentation
duplicate

EIP
enhancement
epic
ETC
flake
forest
good first issue

Some relevant labels…

HYPERLEDGER
BESU

What's Possible…

Open-governance…

- Any of the existing process can be changed with consensus among contributors
- Maintainer status is for pull requests into the Main repo, but non-maintainers can propose project changes
- Discord → #besu-contributors for governance discussions (discord.gg/hyperledger)

Some New Proposals…

- Quarterly or Bi-annual Roadmap Review, open to the public
  - Steer-co?
- Quarterly or Bi-annual Core Development Review to align on Ethereum Improvement Proposals and standards
  - I host existing Core Devs reviews and can make these public if there is appetite
- Public Issue Triage calls

HYPERLEDGER
BESU

Why does Core Development matter?

- Getting involved in Core Development reduces platform risk as more activity moves onto public networks

- More voices in Core Development deepens collaboration and opens the door for progressive decentralization

- Brings an understanding of business and regulatory requirements back to Core Devs

- Web2 → Web3 migration requires collaboration

- Core Development and protocol updates are constantly in the news…

Bloomberg — US Edition

● Live Now   Markets   Economics   Industries   **Technology**   Politics   Wealth   Pursuits   Opinion   Business

Technology

Ethereum's Shanghai Upgrade to Enable Withdrawals Set for April

- Software upgrade will let users 'withdraw staked' Ether
- Ether stakers may have to wait in line to withdraw tokens

GARETH JENKINSON   MAR 10, 2023

Next stop Shanghai — Ethereum's latest milestone approaches

The Ethereum ecosystem is edging closer to its latest milestone as the Shanghai upgrade draws near.

30576 Total views   32 Total shares   Listen to article   ▶ 8:01

Own this piece of history   Collect this article as an NFT →

Forbes

Why Ethereum's Post-Post-Merge Will Be Better Than The Merge

Kenneth Rapoza Senior Contributor ⊙
I write about global business and investing in emerging markets.

Follow

□ 0   Nov 3, 2022, 08:00am EDT

▶ Listen to article 7 minutes

Decision making: All Core Devs

The "All Core Devs Execution" call is the decision-making forum for Ethereum protocol upgrades.

It is split in two to coordinate each layer of the protocol, ACDE and ACDC.

The All Core Devs Execution call (ACDE)

- Fortnightly on Thursdays at 14:00 UTC. Live-streamed.
- Not a closed or appointed group. Anyone who is able to help "move the ball forward" can participate. Mainly clients devs, R&D people, some other interested parties (e.g. Layer 2s).
- Chaired by Tim Beiko.
- Follows an ill-defined "rough consensus" process.

The All Core Devs Consensus call (ACDC) happens on the alternate Thursdays, also at 14:00 UTC.

- Also live-streamed.
- Open participation. Mostly consensus client devs, but increasingly others (e.g. Flashbots).
- Chaired by Danny Ryan.
- Also seeks rough consensus.

HYPERLEDGER
BESU

Types of EIPs

- **Standards Track EIP** describes any change that affects most or all Ethereum implementations,
  - **Core**: improvements requiring a consensus fork, as well as changes that are not necessarily consensus critical but may be relevant to "core dev" discussions
  - **Networking**: includes improvements around devp2p (EIP-8) and Light Ethereum Subprotocol, as well as proposed improvements to network protocol specifications of whisper and swarm.
  - **Interface**: includes improvements around client API/RPC specifications and standards, and also certain language-level standards like method names (EIP-6) and contract ABIs.
  - **ERC**: application-level standards and conventions, including contract standards such as token standards (EIP-20), name registries (EIP-137), URI schemes, library/package formats, and wallet formats.

- A **Meta EIP** describes a process surrounding Ethereum or proposes a change to (or an event in) a process. Process EIPs are like Standards Track EIPs but apply to areas other than the Ethereum protocol itself. Examples include procedures, guidelines, changes to the decision-making process, and changes to the tools or environment used in Ethereum development.

- An **Informational EIP** describes an Ethereum design issue, or provides general guidelines or information to the Ethereum community, but does not propose a new feature. Informational EIPs *do not necessarily represent Ethereum community consensus or a recommendation*, so users and implementers are free to ignore Informational EIPs or follow their advice.

HYPERLEDGER
BESU

Questions & Discussion

HYPERLEDGER
BESU