title: Active areas of Ethereum research description: Explore different areas of open research and learn how to get involved. lang: en

# Active areas of Ethereum research {#active-areas-of-ethereum-research}

One of the primary strengths of Ethereum is that an active research and engineering community are constantly improving it. Many enthusiastic, skilled people worldwide would like to apply themselves to outstanding issues in Ethereum, but it is not always easy to find out what those issues are. This page outlines key active research areas as a rough guide to Ethereum's cutting edge.

## How Ethereum research works {#how-ethereum-research-works}

Ethereum research is open and transparent, embodying principles of Decentralized Science (DeSci). The culture is to make research tools and outputs as open and interactive as possible, for example, through executable notebooks. Ethereum research moves quickly, with new findings posted and discussed in the open on forums such as ethresear.ch rather than reaching the community through traditional publications after rounds of peer review.

## General research resources {#general-research-resources}

Regardless of the specific topic, there is a wealth of information on Ethereum research to be found at ethresear.ch and the Eth R&D Discord channel. These are the primary places where Ethereum researchers discuss the latest ideas and development opportunities.

This report published in May 2022 by DelphiDigital provides a good overview of the Ethereum roadmap.

## Sources of Funding {#sources-of-funding}

You can get involved with Ethereum research and get paid for it! For example, the Ethereum Foundation recently ran an Academic Grants funding round. You can find information on active and upcoming funding opportunities on the Ethereum grants page.

## Protocol research {#protocol-research}

Protocol research is concerned with Ethereum's base layer - the set of rules defining how nodes connect, communicate, exchange and store Ethereum data and come to consensus about the state of the blockchain. Protocol research gets divided into two top-level categories: consensus and execution.

### Consensus {#consensus}

Consensus research is concerned with Ethereum's proof-of-stake mechanism. Some example consensus research topics are:

- identifying and patching vulnerabilities;
- quantifying cryptoeconomic security;
- increasing the security or performance of client implementations;
- and developing light clients.

As well as forward-looking research, some fundamental redesigns of the protocol, such as single slot finality, are being researched to allow for significant improvements to Ethereum. Furthermore, the efficiency, safety, and monitoring of peer-to-peer networking between consensus clients are also important research topics.

#### Background reading {#background-reading}

- Introduction to proof-of-stake
- Casper-FFG paper
- Casper-FFG explainer
- Gasper paper

#### Recent research {#recent-research}

- Ethresear.ch Consensus
- Availability/Finality dilemma
- Single slot finality
- Proposer-builder separation

### Execution {#execution}

The execution layer is concerned with executing transactions, running theEthereum virtual machine (EVM) and generating execution payloads to pass to the consensus layer. There are many active areas of research, including:

- building out light client support;
- researching gas limits;
- and incorporating new data structures (e.g. Verkle Tries).

#### Background reading {#background-reading-1}

- Introduction to the EVM
- Ethresear.ch execution layer

#### Recent research {#recent-research-1}

- Database optimizations
- State expiry
- Paths to state expiry
- Verkel and state expiry proposal
- History management
- Verkle Trees
- Data availability sampling

## Client Development {#client-development}

Ethereum clients are implementations of the Ethereum protocol. Client development makes the outcomes from protocol research into reality by building them into these clients. Client development includes updating the client specifications as well as building specific implementations.

An Ethereum node is required to run two pieces of software:

1. a consensus client to keep track of the head of the blockchain, gossip blocks and handle consensus logic
2. an execution client to support the Ethereum Virtual Machine and execute transactions and smart contracts

See the nodes and clients page for more detail on nodes and clients and for a list of all current client implementations. You can also find a history of all Ethereum upgrades on the history page.

### Execution Clients {#execution-clients}

- Execution client specification
- Execution API spec

### Consensus Clients {#consensus-clients}

- Consensus client specification
- Beacon API specification

## Scaling and performance {#scaling-and-performance}

Scaling Ethereum is a large area of focus for Ethereum researchers. Current approaches include offloading transactions onto rollups and making them as cheap as possible using data blobs. Introductory information on scaling Ethereum is available on our scaling page.

### Layer 2 {#layer-2}

There are now several Layer 2 protocols that scale Ethereum using different techniques for batching transactions and securing them on Ethereum layer 1. This is a very rapidly growing topic with a lot of research and development potential.

#### Background reading {#background-reading-2}

- Introduction to layer 2
- Polynya: Rollups, DA and modular chains

#### Recent research {#recent-research-2}

- Arbitrum's fair-ordering for sequencers
- ethresear.ch Layer 2
- Rollup-centric roadmap
- L2Beat

### Bridges {#bridges}

One particular area of layer 2 that requires more research and development is safe and performant bridges. This includes bridges between various Layer 2s and bridges between Layer 1 and Layer 2. This is a particularly important area of research because bridges are commonly targeted by hackers.

#### Background reading {#background-reading-3}

- Introduction to blockchain bridges
- Vitalik on bridges
- Blockchain bridges article
- Value locked in bridges

#### Recent research {#recent-research-3}

- Validating bridges

### Sharding {#sharding}

Sharding Ethereum's blockchain has long been part of the development roadmap. However, new scaling solutions such as "Danksharding" are currently taking center stage.

#### Background reading {#background-reading-4}

- Proto-Danksharding notes
- Bankless Danksharding video
- Ethereum Sharding Research Compendium
- Danksharding (Polynya)

#### Recent research {#recent-research-4}

- EIP-4844: Proto-Danksharding
- Vitalik on sharding and data availability sampling

### Hardware {#hardware}

Running nodes on modest hardware is fundamental to keeping Ethereum decentralized. Therefore, active research into minimizing the hardware requirements to run nodes is an important area of research.

#### Background reading {#background-reading-5}

- Ethereum on ARM

#### Recent research {#recent-research-5}

- ecdsa on FPGAs

## Security {#security}

Security is a broad topic that might include spam/scam prevention, wallet security, hardware security, crypto-economic security, bug hunting and testing of applications and client software and key-management. Contributing to knowledge in these areas will help stimulate mainstream adoption.

### Cryptography & ZKP {#cryptography--zkp}

Zero-knowledge proofs (ZKP) and cryptography are critical for building privacy and security into Ethereum and its applications. Zero-knowledge is a relatively young but fast-moving space with many open research and development opportunities. Some possibilities include developing more efficient implementations of the Keccak hashing algorithm, finding better polynomial commitments than currently exist or reducing the cost of ecdsa public key generation and signature verification circuits.

#### Background reading {#background-reading-6}

- 0xparc blog
- zkp.science
- Zero Knowledge podcast

#### Recent research {#recent-research-6}

- Recent advance in elliptic curve cryptography
- Ethresear.ch ZK

### Wallets {#wallets}

Ethereum wallets can be browser extensions, desktop and mobile apps or smart contracts on Ethereum. There is active research into social recovery wallets that reduce some of the risk associated with individual-user key management. Associated with development of wallets is research into alternative forms of account abstraction, which is an important area of nascent research.

#### Background reading {#background-reading-7}

- Introduction to wallets
- Introduction to wallet security
- ethresear.ch Security
- EIP-2938 Account Abstraction
- EIP-4337 Account Abstraction

#### Recent research {#recent-research-7}

- Validation focused smart contract wallets
- The future of accounts
- EIP-3074 AUTH and AUTHCALL Opcodes
- Publishing code at an EOA address

## Community, education and outreach {#community-education-and-outreach}

Onboarding new users onto Ethereum requires new educational resources and approaches to outreach. This might include blog posts and articles, books, podcasts, memes, teaching resources events and anything else that builds communities, welcomes new starters and educates people about Ethereum.

### UX/UI {#uxui}

To onboard more people onto Ethereum, the ecosystem must improve the UX/UI. This will require designers and product experts to re-examine the design of wallets and apps.

#### Background reading {#background-reading-8}

- Ethresear.ch UX/UI

#### Recent research {#recent-research-8}

- Web3 Design Discord
- Web3 Design Principles
- Ethereum Magicians UX discussion

### Economics {#economics}

Economics research in Ethereum broadly follows two approaches: validate the security of mechanisms relying on economic incentives ("microeconomics") and analyze the flows of value between protocols, applications and users ("macroeconomics"). There are complex crypto-economic factors relating to Ethereum's native asset (ether) and the tokens built on top of it (for example NFTs and ERC20 tokens).

#### Background reading {#background-reading-9}

- Robust Incentives Group
- ETHconomics workshop at Devconnect

#### Recent research {#recent-research-9}

- Empirical analysis of EIP1559
- Circulating supply equilibrium
- Quantifying MEV: How dark is the forest?

### Blockspace and fee markets {#blockspace-fee-markets}

Blockspace markets govern the inclusion of end-user transactions, either directly on Ethereum (Layer 1) or on bridged networks, e.g., rollups (Layer 2). On Ethereum, transactions are submitted to the fee market deployed in-protocol as EIP-1559, protecting the chain from spam and pricing congestion. On both layers, transactions may produce externalities, known as Maximal Extractable Value (MEV), which induce new market structures to capture or manage these externalities.

#### Background reading {#background-reading-10}

- Transaction Fee Mechanism Design for the Ethereum Blockchain: An Economic Analysis of EIP-1559 (Tim Roughgarden, 2020)

- Simulations of EIP-1559 (Robust Incentives Group)
- Rollup economics from first principles
- Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges

#### Recent research {#recent-research-10}

- Multidimensional EIP-1559 video presentation
- Cross domain MEV
- MEV auctions

### Proof-of-stake incentives {#proof-of-stake-incentives}

Validators use Ethereum's native asset (ether) as collateral against dishonest behavior. The cryptoeconomics of this determines the security of the network. Sophisticated validators may be able to exploit the nuances of the incentive layer to launch explicit attacks.

#### Background reading {#background-reading-11}

- Ethereum economics masterclass and economic model
- Simulations of PoS incentives (Robust Incentives Group)

#### Recent research {#recent-research-11}

- Increasing censorship resistance of transactions under proposer/builder separation (PBS)
- Three Attacks on PoS Ethereum

### Liquid staking and derivatives {#liquid-staking-and-derivatives}

Liquid staking allows users with less than 32 ETH to receive staking yields by swapping ether for a token representing staked ether that can be used in DeFi. However, the incentives and market dynamics associated with liquid staking are still being discovered, as well as its effect on Ethereum's security (e.g. centralization risks).

#### Background reading {#background-reading-12}

- Ethresear.ch liquid staking
- Lido: The road to trustless Ethereum staking
- Rocket Pool: Staking protocol introduction

#### Recent research {#recent-research-12}

- Handling withdrawals from Lido
- Withdrawal credentials
- The risks of Liquid Staking Derivatives

## Testing {#testing}

### Formal verification {#formal-verification}

Formal verification is writing code to verify that Ethereum's consensus specifications are correct and bug-free. There is an executable version of the specification written in Python that requires maintenance and development. Further research can help to improve the Python implementation of the specification and add tools that can more robustly verify correctness and identify issues.

#### Background reading {#background-reading-13}

- Introduction to formal verification

- Formal Verification (Intel)

#### Recent research {#recent-research-13}

- Formal verification of the deposit contract
- Formal verification of the Beacon Chain specification

## Data science and analytics {#data-science-and-analytics}

There is a need for more data analysis tools and dashboards that give detailed information about activity on Ethereum and the health of the network.

### Background reading {#background-reading-14}

- Dune Analytics
- Client diversity dashboard

#### Recent research {#recent-research-14}

- Robust Incentives Group Data Analysis

## Apps and tooling {#apps-and-tooling}

The application layer supports a diverse ecosystem of programs that settle transactions on Ethereum's base layer. Development teams are constantly finding new ways to leverage Ethereum to create composable, permissionless and censorship-resistant versions of important Web2 apps or create completely new Web3-native concepts. At the same time, new tooling is being developed that makes building dapps on Ethereum less complex.

### DeFi {#defi}

Decentralized finance (DeFi) is one of the primary classes of application built on top of Ethereum. DeFi aims to create composable "money legos" that allow users to store, transfer, lend, borrow and invest crypto-assets using smart contracts. DeFi is a fast-moving space that is constantly updating. Research into secure, efficient and accessible protocols is continuously needed.

#### Background reading {#background-reading-15}

- DeFi
- Coinbase: What is DeFi?

#### Recent research {#recent-research-15}

- Decentralized finance, centralized ownership?
- Optimism: The road to sub-dollar transactions

### DAOs {#daos}

An impactful use case for Ethereum is the ability to organize in a decentralized manner through the use of DAOs. There is a lot of active research into how DAOs on Ethereum can be developed and utilized to execute improved forms of governance, as a trust-minimized coordination tool, greatly expanding peoples options beyond traditional corporations and organizations.

#### Background reading {#background-reading-16}

- Introduction to DAOs
- Dao Collective

#### Recent research {#recent-research-16}

- Mapping the DAO ecosystem

## Developer tools {#developer-tools}

Tools for Ethereum developers are rapidly improving. There is lots of active research and development to do in this general area.

### Background reading {#background-reading-17}

- Tooling by programming language
- Developer Frameworks
- Consensus developer tools list
- Token standards
- CryptoDevHub: EVM Tools

### Recent research {#recent-research-17}

- Eth R&D Discord Consensus Tooling channel

## Oracles {#oracles}

Oracles import off-chain data onto the blockchain in a permissionless and decentralized way. Getting this data on-chain enables dapps to be reactive to real-world phenomena such as price fluctuations in real-world assets, events in off-chain apps, or even changes in the weather.

### Background reading {#background-reading-18}

- Introduction to Oracles

### Recent Research {#recent-research-18}

- Survey of blockchain oracles
- Chainlink white paper

## App security {#app-security}

Hacks on Ethereum generally exploit vulnerabilities in individual applications rather than in the protocol itself. Hackers and app developers are locked in an arms race to develop new attacks and defenses. This means there is always important research and development required to keep apps safe from hacks.

### Background reading {#background-reading-19}

- Wormhole exploit report
- List of Ethereum contract hack post-mortems
- Rekt News

### Recent research {#recent-research-19}

- ethresear.ch Applications

## Technology stack {#technology-stack}

Decentralizing the entire Ethereum tech stack is an important research area. Currently, dapps on Ethereum commonly have some points of centralization because they rely on centralized tooling or infrastructure.

### Background reading {#background-reading-20}

- Ethereum stack
- Coinbase: Intro to Web3 Stack
- Introduction to smart contracts
- Introduction to decentralized storage

### Recent research {#recent-research-20}

- Smart contract composability