Ethereum Basics for Governments and Institutions

ethereum foundation
GPS

Disclaimer

This paper is provided by the Ethereum Foundation for general educational and informational purposes only. It does not constitute legal, regulatory, financial, investment, or other professional advice, and should not be relied upon as such.

The Ethereum Foundation is one participant in the broader Ethereum ecosystem. It does not operate or control Ethereum, or determine whether protocol changes are adopted.

The information in this paper may include estimates, third-party data, and publicly available information believed to be reliable as of the dates indicated, but it may change over time.

A Note on Data and Sources

This report quotes several figures from OpenZeppelin's Technical Risk Assessment,[1] which provides a structured, side-by-side risk assessment of six blockchain networks. Key metrics in this report were anchored in the OpenZeppelin report in order to provide readers with an objective, auditable, and static baseline from a credible and independent source.

Some of the blockchain metrics included in the OpenZeppelin report fluctuate frequently. Fortunately, a defining property of public blockchain infrastructure is that the underlying data is verifiable by anyone, at any time, without relying on any single report or publication. We encourage readers to consult these sources directly. This may help with both verifying the figures cited in this report and tracking how the ecosystem continues to develop.

The structural conclusions of this report, however, rest on architectural and governance properties that are durable across the market cycles of the last decade.

Contents

Executive Summary

Modern societies increasingly rely on digital systems to move value and coordinate at scale. Yet the core systems for finance, data, and institutional coordination remain fragmented, opaque, and controlled by a small number of intermediaries. This concentrates authority, enabling these intermediaries to **remove access** at will or upon being pressured, **creates single points of failure**, and **limits user sovereignty**.

As governments and institutions confront mounting pressures across geopolitics, financial infrastructure, digital identity, data integrity, and AI governance, **the need for shared, neutral digital public infrastructure, not controlled by a centralized entity or single state has become increasingly evident.**

Ethereum was built to address precisely these pressures. This paper is a comprehensive, non-technical primer on Ethereum specifically and on blockchain infrastructure more broadly. We drafted it such that you can read all the way through or just jump to the questions most relevant to you.

This paper was prepared for government officials, central bankers, regulators, multilateral institutions, and enterprise leaders faced with evaluating digital infrastructure. These evaluations may be conducted from the perspective of both procurement and deployment decisions, as well as regulatory and policy choices.

Our objective is to equip readers with **clear, balanced, evidence-based materials to support these evaluations.**

Ethereum is a decentralized ecosystem that functions through the activity of a large, diverse, and global group of stakeholders. That breadth of participation is one of the things that makes Ethereum so secure; which in turn is what **makes it the top choice for institutions, enterprises, and the public sector.**

Ethereum is not controlled by any organization, individual, or state. Like the internet's core protocols, Ethereum is open, programmable, and globally accessible.

System-level indicators underscore Ethereum's role as digital public infrastructure compared to other layer 1 blockchains (statistics taken as of March, 2026 from OpenZeppelin's Technical Risk Assessment,[2] except where stated otherwise):

- **Most reliable:** Ethereum has maintained **uninterrupted uptime** ever since its launch over a decade ago.[3]

Contrast this to other large layer 1 blockchains like Solana, Ripple, BNB Smart Chain, Canton, TRON — which have each had between one and seven[4] instances during which their networks could not process transactions, one such network failure lasted for about 19 hours on Solana[5].

Network outages since launch

Ethereum Launched in 2015- 0 network outages	**NONE** Uninterrupted since launch
Solana Launched in 2020 - At least 7 outages	**~19 Hours** in 2023
BNB Smart Chain Launched in 2020 - At least 1 outage	**~5 Hours** in 2022
XRP Ledger Launched in 2012- At least 1 outage	**~1 Hour** in 2025

- **Most economically secure:** Attacking Ethereum is prohibitively expensive by design. It would cost an attacker **~$50.7 billion**[6] to unilaterally influence consensus and finalize a fraudulent transaction on the Ethereum network, which is secured by **~$76 billion.**[7] in staked ETH. In addition to the cost of buying ~$50.7 billion in ETH, the attacker would also lose billions of dollars worth of ETH as penalty to automatic on-chain slashing resulting from their malicious activity.

  Contrast that to Solana, BNB Smart Chain, and TRON where the cost of an attack to finalize a fraudulent transaction is ~$23.3 billion, ~$11.3 billion, ~$18.7 billion,[8] respectively.

  Notably, Solana and TRON lack[9] the added deterrence of automatic on-chain slashing for this kind of an attack.

Ethereum is the most economically secure blockchain

$76B

Total Value Staked

Ethereum is more secure than the next three chains combined

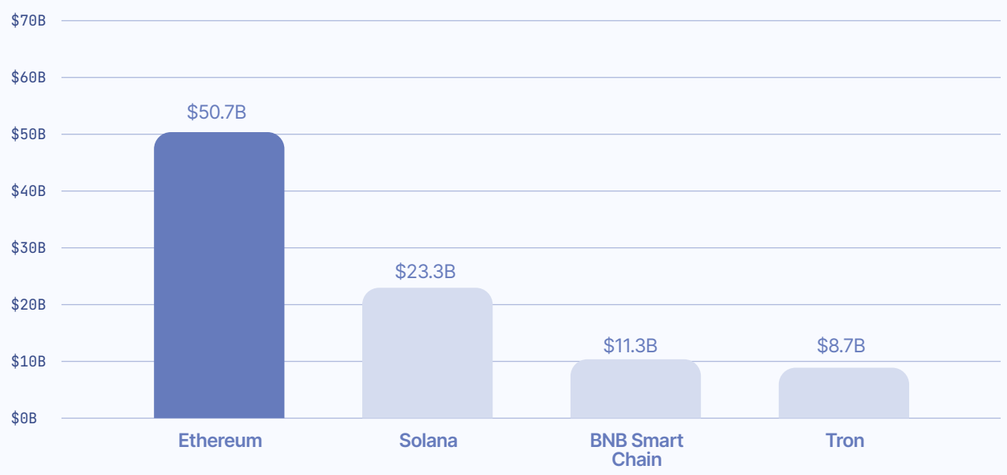
$76B vs **$65B**

Solana + BNB Smart Chain + Tron

Cost to finalize a fraudulent transaction

Ethereum sets the highest barrier to attack

Capital required to finalize a fraudulent transaction, in USD billions



- **Most trusted by institutions:** As of March, 2026, Ethereum hosted **$159 billion**[10] **in stablecoin value,** whereas Solana hosted about $15 billion,[11] and BNB Smart Chain hosted about $14 billion[12]. Ethereum also hosted over **$15.2 billion**[13] in tokenized real-world assets, **3X more than the combined** value hosted on BNB Smart Chain ($3 billion)[14] and Solana ($2.1 billion)[15].

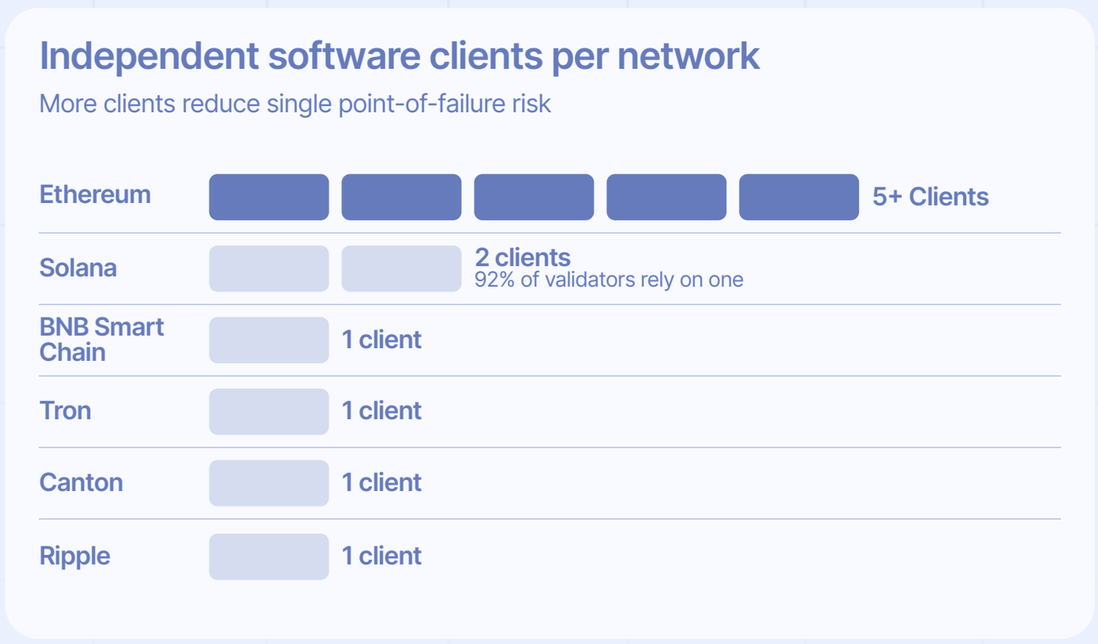
  Some of the large institutions building, deploying, or transacting on Ethereum include: European Investment Bank, Franklin Templeton, BlackRock, JPMorgan, ChinaAMC, Amundi, EY, Deutsche Bank, Fidelity, Société Générale-Forge, Visa, PayPal, UBS, SWIFT, DTCC, Robinhood, Ant Group, and many more.

- **Most trusted by governments and multilateral bodies:** Ethereum and its standards are trusted by governments and international development institutions globally, across a wide range of use cases serving real citizens and public mandates.

  Some examples include national identity systems in Bhutan and Buenos Aires; land registries in India; and humanitarian cash disbursements via UNICEF and UNHCR.

- **Most robust software:** Ethereum maintains **5+**[16] **independent software clients**, providing meaningful redundancy against implementation-specific bugs or vulnerabilities.

By contrast, 92 percent of Solana validators rely on a **single client** (Agave as of June 2025)[17] and BNB Smart Chain, TRON, Canton, and Ripple[18] have no client diversity at all.

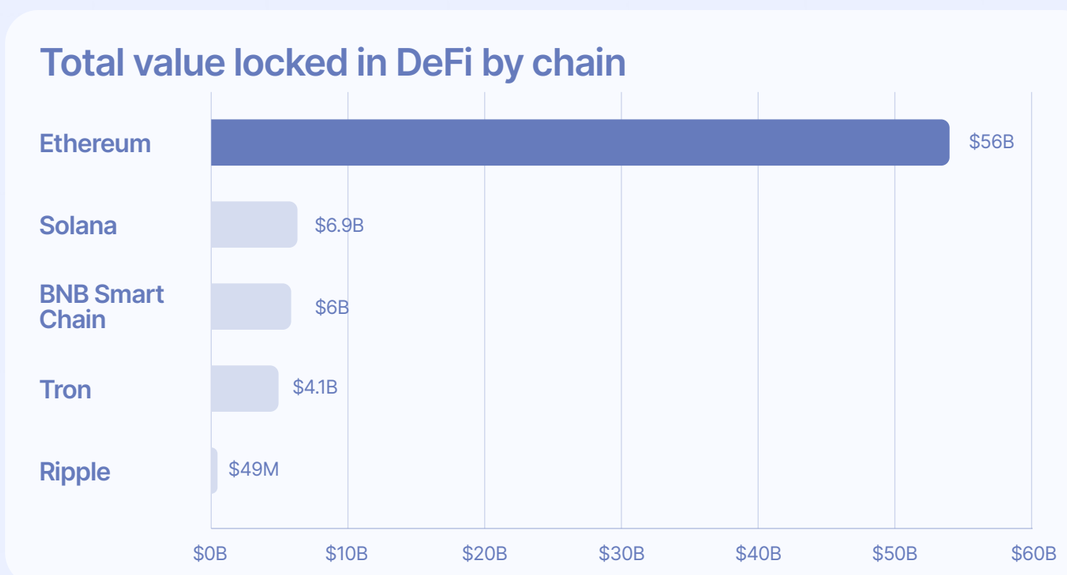


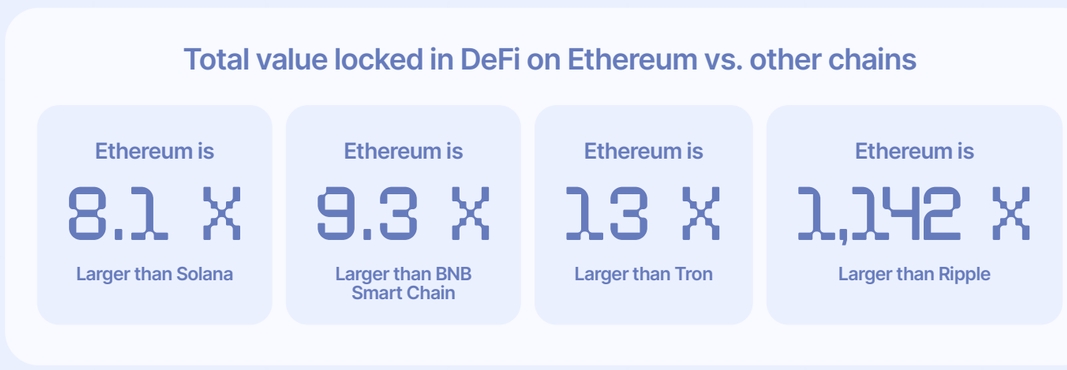
- **Largest developer network:** As of May, 2026, the EVM stack is supported by nearly **11,000 total developers**[19] reflecting long-term technical investment and testing over a decade.

  Contrast this with Solana (~2,600 devs[20]), BNB Smart Chain (837 devs[21]), TRON (~359 devs[22]), and Ripple (~272 devs[23]).

- **Largest DeFi ecosystem:** As of March, 2026, Ethereum had over **$56 billion**[24] in total value locked in DeFi.

  Contrast this with Solana ($6.9 billion)[25], BNB Smart Chain ($6 billion)[26], TRON ($4.11 billion)[27], and Ripple ($49 million)[28].





- **Most interoperable:** Interoperability is increasingly recognized as critical for state capacity and institutional coordination across jurisdictions. Ethereum is the only public blockchain that meets this standard at scale. **ERC-20 has become the de facto standard** for tokenized assets and **the Ethereum Virtual Machine (EVM) is the most widely adopted execution environment**. Building on Ethereum enables moving across compatible networks with minimal modification. By contrast, networks that use proprietary languages or non-EVM runtimes such as Solana, require bespoke bridges and full rewrites to interoperate with the broader ecosystem, creating structural barriers and risks to coordination.

- **Environmentally friendly:** Ethereum's shift to proof-of-stake reduced its electricity consumption by 99.98[29] percent and its carbon footprint by approximately 99.99[30] percent, making it roughly 53,000[31] times more energy-efficient than the Bitcoin network and roughly 100 times[32] more efficient than PayPal

- **Most futureproof:** Ethereum is leading layer 1 networks on post-quantum security and is actively building a post-quantum security roadmap into its core protocol, not as a bolt-on. This includes a dedicated research team, a $2M cryptographic prize fund[33], and a phased path designed to transition the network without downtime or loss of user funds.

By examining Ethereum's architecture, governance model, security design, and real-world adoption, this paper provides institutional leaders with a framework to evaluate Ethereum against alternatives and against their objectives such as inclusive participation, market integrity, accountable governance, privacy and human rights, sustainability, interoperability, and systemic stability.

System Overview and Foundational Concepts

What is a blockchain?

1

A blockchain is a distributed digital ledger produced when a network of participants executes a shared protocol. The protocol defines how transactions are validated, how blocks are formed, and how agreement is reached on the order of transactions. The network consists of participants who run this protocol software and process transactions according to its rules.

The blockchain is the resulting record: a chain of cryptographically linked blocks containing validated transactions. One defining characteristic of a “public” blockchain is that **no single institution holds exclusive control** over the transaction record. Instead, the integrity of the ledger is maintained through cryptographic verification and the economic incentives of network participants.

Modern economic and civic systems depend on coordination between independent actors who do not fully trust one another. This coordination is achieved through trusted intermediaries such as banks, land registries, clearinghouses, and licensed institutions, whose authority substitutes for direct trust between parties. In this model, the integrity of the record is inseparable from the integrity of the institution that maintains it.

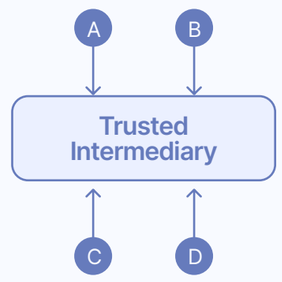
A sufficiently decentralized blockchain offers a more reliable solution to this same coordination need. Agreement is reached **not through institutional authority**, but through **transparent protocol rules and cryptographic verification**, with transactions validated by a distributed network of independent participants. This represents a distinct **model of distributed trust**.

Two models of trust

How independent actors coordinate without fully trusting one another.

Traditional model

Trust through institutions

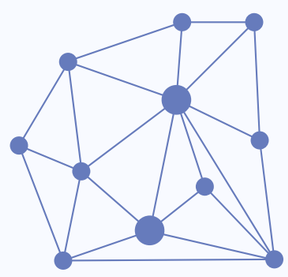


Coordination between parties achieved by trusted intermediary

- Relies on a trusted intermediary
- Integrity depends on the institution that maintains the record

Blockchain model

Trust through distributed verification



Independent participants run the shared protocol, no trusted intermediary involved

- No trusted intermediary or institutional authority
- Trust through cryptographic verification and transparent protocol rules

Public blockchains are collectively maintained by communities of developers and other key participants through established processes for proposing and implementing upgrades. While the protocol governs routine transaction validation, the system’s long-term adaptability and resilience depend on social coordination around its evolution. **Trust is therefore reinforced at two levels: through verifiable technical rules in protocol operations, and through collective governance when change is required.**

How does Ethereum work?

2

Ethereum works as a shared digital record maintained by a global network of independent computers. It is the foundation for building apps and organizations in a **decentralized** and **permissionless** way. The absence of a single owner renders Ethereum **censorship resistant**. This means that no one has the power to unilaterally remove access, block transactions, shut down the network, or deny service to certain participants.

A useful **analogy is the internet**. The internet allows anyone to publish information and build services without needing approval from a central operator. Email, websites, and online platforms all run on top of shared technical standards. No single entity owns the internet itself.

Structural Parallel: The Internet and Ethereum

	THE INTERNET	ETHEREUM
FUNCTION	Public infrastructure for information	Public infrastructure for transactions and programmable commitments
WHAT IS BUILT ON TOP	Email, websites, platforms, cloud services	Financial services, digital identity, tokenized assets
ACCESS	Anyone can publish or build without central approval	Anyone can deploy or transact without central approval
OWNERSHIP	No single owner; maintained by distributed and diversified stakeholders	No single owner; maintained by distributed and diversified stakeholders
RESILIENCE	No single point of failure	No single point of failure; 10+ years continuous uptime

OPEN — Internet + Ethereum

PERMISSIONLESS — Internet + Ethereum

NO SINGLE OWNER — Internet + Ethereum

Ethereum plays a similar role for value and digital agreements. If the internet is a public infrastructure for information, **Ethereum is public infrastructure for transactions and programmable commitments.**

At its core, Ethereum is a collection of thousands of independent computers called nodes. These nodes are run by people all over the world. They work together to store data, run programs, and record every transaction on an open, public ledger. As of June 1, 2026, there are over 11,000[1] active nodes on the Ethereum network.

The Ethereum Virtual Machine (EVM) is the execution engine that processes transactions and runs programs deterministically across all Ethereum nodes. Every full node that participates in the Ethereum network maintains a copy of Ethereum's state, which is the canonical record of all account balances, contract storage, and code. When a user broadcasts a transaction, nodes independently execute it through their local EVM instance. The EVM takes the current state and the transaction as inputs, and produces a new state as output. Nodes then verify that they arrive at the same resulting state. This validated state transition is committed and propagated throughout the network via the consensus protocol.

When someone sends a transaction on Ethereum, such as transferring digital assets or interacting with an application, the request is broadcast to the network. Independent participants known as validators check that the transaction follows established rules. Valid transactions are grouped into blocks and added to a permanent record. Each new block links to the previous one, forming a continuous chain. Users pay transaction fees to compensate validators and prevent overuse. Fees compensate for the computing resources consumed by each transaction.

Block production and finality are economically secured by validators staking ETH as collateral. New blocks are typically added to Ethereum **every 12 seconds**. To **finalize a block, at least two-thirds of the total active staked ETH must attest to it** during a two "epoch" (approximately 13 minute) period.

If two conflicting finalized histories were created, this would mean an attempt to propagate something different from the canonical block. For this to occur, at least one-third of total stake would have had to sign both versions. Signing both versions would constitute **punishable behavior and the offending validators would be automatically penalized.** They would **lose their staked ETH through a process called slashing (and would be forcibly ejected from the validator set)**. Because penalties scale with the number of validators involved, large-scale coordinated attacks would result in substantial losses, making such behavior economically self-destructive.

The cost of network attack fluctuates with the price of ETH. By way of example, in March 2026 the number of ETH staked amounted to about $76 billion[2]. Controlling the two-thirds majority required to execute an attack by unilaterally finalizing a fraudulent transaction would require commanding upwards of $50.7 billion[3] in ETH. It is **prohibitively expensive to execute such attacks.**

Ethereum also offers users the functionality of running programs on the blockchain. These programs, called **"smart contracts," are a collection of code and data that resides at a specific address on the Ethereum blockchain**. User accounts can interact with smart contracts by submitting transactions that execute a function defined on these smart contracts. Smart contracts can define rules, like a regular contract, but with the added benefit of automatically enforcing those rules via code. Any developer can create a smart contract and make it public to the network, using the blockchain as its data layer. This functionality enables developers to build and deploy user-facing apps and services such as marketplaces, stablecoins, games, etc.

In practical terms, Ethereum functions like a shared global settlement layer—similar to how the internet serves as a shared communications layer. It enables people and organizations to transact and deploy automated agreements without relying on a central intermediary.

Stakeholder parallels across the stack

Both systems are sustained by independent participants at every layer

	INTERNET STAKEHOLDERS	ETHEREUM STAKEHOLDERS
LAYER 4: APPLICATIONS & USERS Economic Activity & Policy	✶ **Businesses** (social media, marketplaces) ✶ **Governments** (community services) ✶ **End users**	✶ **Businesses** (stablecoin issuers, tokenization) ✶ **Governments** (Identity, cross-border settlement, land registry etc.) ✶ **End users**
LAYER 3: SERVICE PROVIDERS Access And Network Interfaces	✶ **ISPs** ✶ **Cloud providers** ✶ **Browsers & platforms**	✶ **Wallet providers** ✶ **Custodians** ✶ **RPC providers** ✶ **Layer 2 network operators**
LAYER 2: CORE PROTOCOLS Shared Protocol Rules And Upgrade Coordination	✶ **Open protocol maintainers and contributors** (TCP/IP, HTTP) ✶ **Standards bodies** (IETF, WSC)	✶ **Ethereum core contributors** ✶ **Open-source client teams**
LAYER 1: BASE INFRASTRUCTURE Consensus, Security, Settlement	✶ **Networks operators** (ISPs) ✶ **Data centers operators** ✶ **Infrastructure operators**	✶ **Validators** ✶ **Node operators** ✶ **Cryptographic infrastructure operators**

What gap in today's internet does Ethereum fill?

3

The analogy of Ethereum being akin to the internet requires an important caveat. The internet was conceived as an open, permissionless public utility, a shared protocol layer that anyone can build on without seeking approval. The earliest standards, such as TCP/IP to HTTP and SMTP, were deliberately designed to be neutral, interoperable, and free for any participant to implement. No single entity could dictate who connected, what was published, or how information was exchanged. This architectural neutrality is what allowed the internet to become the foundation of the modern global economy.

Contrasting user experience on the internet and on Ethereum

	INTERNET USER EXPERIENCE	ETHEREUM USER EXPERIENCE
TRUST	✗ Trust the tech company	✓ Trust the protocol
OWNERSHIP	✗ Owned by a corporation	✓ Owned by thousands of stakeholders
CUSTODY	✗ Assets held by intermediaries	✓ Held by the users themselves
ACCESS	✗ Permissioned by gatekeepers	✓ Open to anyone
INTEROPERABILITY	✗ Walled gardens, locked APIs	✓ Open, composable building blocks
CONTINUITY	✗ Subject to platform decisions	✓ Continuous, no central operator
CENSORSHIP	✗ Tech companies can deplatform	✓ Resistant by design
AUDITABILITY	✗ Opaque internal records	✓ Public, independently verifiable

While the neutrality and openness of the internet itself has not changed, the layer at which most users actually interact with it bears little structural resemblance to that original design. Over the course of roughly three decades, **corporations have built proprietary platforms on top of the open protocols, and those platforms have become the practical entry point through which the majority of digital activity now flows.** Commerce, communication, identity, payments, and content distribution are **intermediated by a handful of operators** whose terms of service, opaque policies, and commercial incentives effectively determine what users experience. Further, the **intermediaries that shape what users see are not always visible**. Beyond the large platforms, smaller operators sitting between users and the open protocols, such as filters, reputation systems, and access providers, can also determine what content reaches whom. The user often has no visibility into who made which decision, or why a message, transaction, or piece of content did not arrive.

The protocols beneath remain open, but the experience layer above them has consolidated into private channels. User data is captured and monetized by the platforms that host it. Access to application programming interfaces, audiences, and payment rails can be revoked unilaterally. The result is an internet whose foundations are still public, but whose day-to-day surface

has come to resemble a collection of private fiefdoms operating on shared pipes.

This analysis also extends to AI capabilities. Frontier AI models are also controlled by a small number of companies which creates single points of pressure. A jurisdiction with authority over a central operator can require the suspension of AI capabilities for millions of users.

This is the gap Ethereum is designed to fill. Rather than replacing the open protocols of the internet, Ethereum extends them upward, into the layer where openness has thinned. It provides a neutral, auditable, programmable settlement layer for applications that sits at the same level as the commercial platforms but operates on the same principles as the underlying internet itself. **Where today's experience layer requires users to trust the platform, Ethereum allows them to transact and coordinate by trusting the protocol.** Assets and data are held by their owners rather than by intermediaries. Applications are composable rather than walled off, which means innovation can build directly on prior innovation without requiring permission from a gatekeeper.

The network operates continuously, with no central operator who can take it offline, deplatform a participant, or alter the rules retroactively. It is inspectable by design. The rules, the state, and the operations that determine what happens on Ethereum are visible to any participant, minimizing the scope for opaque intermediation to take hold. In this sense, **Ethereum is not an alternative to the internet. It is an extension of the internet's open architecture into a layer the original protocols did not address.**

The distinction matters for policy and institutional decision-making. The questions that increasingly define modern digital policy, including **data sovereignty, market concentration, financial inclusion, systemic resilience, and censorship resistance, are not failures of the internet's foundational protocols. They are properties of how the experience layer has been commercialized.**

Regulatory intervention can constrain the behavior of dominant platforms, but it cannot, on its own, recreate at the experience layer the structural neutrality that the protocol layer possesses by design. Achieving that requires a foundation at the experience layer that shares the same properties as the protocols beneath it.

Ethereum offers precisely such a foundation. It is **credibly neutral**, in the sense that its rules apply uniformly to all participants and cannot be changed by any single party, including its own developers. It is **auditable**, because every transaction and contract is recorded on a public ledger that any party may independently verify. It is **interoperable** by default, because applications built on it share a common settlement layer rather than competing data silos. Interoperability of this kind is no longer a technical convenience.

As recent years have shown, the ability of allied institutions to coordinate across jurisdictions, exchange value, and share data without negotiating bespoke standards is increasingly a determinant of state capacity itself. Ethereum's interoperability extends this capability into the layer of digital infrastructure where coordination has historically been hardest. Further, Ethereum is **resistant to capture**, because the economic and cryptographic mechanisms that secure it are distributed across thousands of independent participants worldwide.

In this respect, Ethereum is best understood as a **continuation of the internet's founding architectural principles, applied at a layer of the stack where, until now, those principles have not been available**.

What is ETH and what role does it play?

4

Ether (ETH) is the native asset of the Ethereum protocol. ETH is the **mechanism through which computation is priced, consensus is secured, and economic incentives are aligned** across a decentralized network.

At the most basic level, ETH is required to **pay for computation.** Ethereum operates as a shared global system in which transactions and smart contracts update a common state. Each update consumes computational resources, which are measured in units known as gas. Users pay for gas using ETH at a rate that adjusts dynamically based on network demand. This pricing mechanism serves multiple purposes: it allocates scarce blockspace through market demand, prevents spam transactions from flooding the network, deters infinite execution, and removes the need for a central authority to approve or ration network usage.

ETH also plays a **central role in network security**. Ethereum uses a proof-of-stake consensus mechanism in which validators must stake ETH as economic collateral in order to participate. Validators are selected to propose and verify blocks and are rewarded for correct participation. If a validator attempts to disrupt the network or violate protocol rules, a portion of their staked ETH can be destroyed, known as slashing. **Security therefore emerges from aligned economic incentives rather than reliance on a trusted intermediary.**

Finally, ETH **coordinates incentives across users and validators** through protocol-defined supply mechanics. New ETH is issued to compensate validators for securing the network, while a portion of transaction fees is automatically burned. This burn mechanism is algorithmic and usage-driven: it reflects demand for blockspace rather than discretionary monetary policy. When network usage increases, more ETH is removed from circulation; when usage declines, less is burned. During periods of sustained high demand, the burn rate can exceed new issuance, resulting in a net reduction in total ETH supply.[4]

By requiring both users and validators to rely on the same asset for execution and security, ETH aligns participants around the integrity and availability of a shared public infrastructure. **Its role is therefore best understood as that of a protocol resource.** ETH enables Ethereum to function as neutral, decentralized infrastructure whose operation does not depend on the ongoing efforts or discretion of any single organization.

What is staking and how does it work?

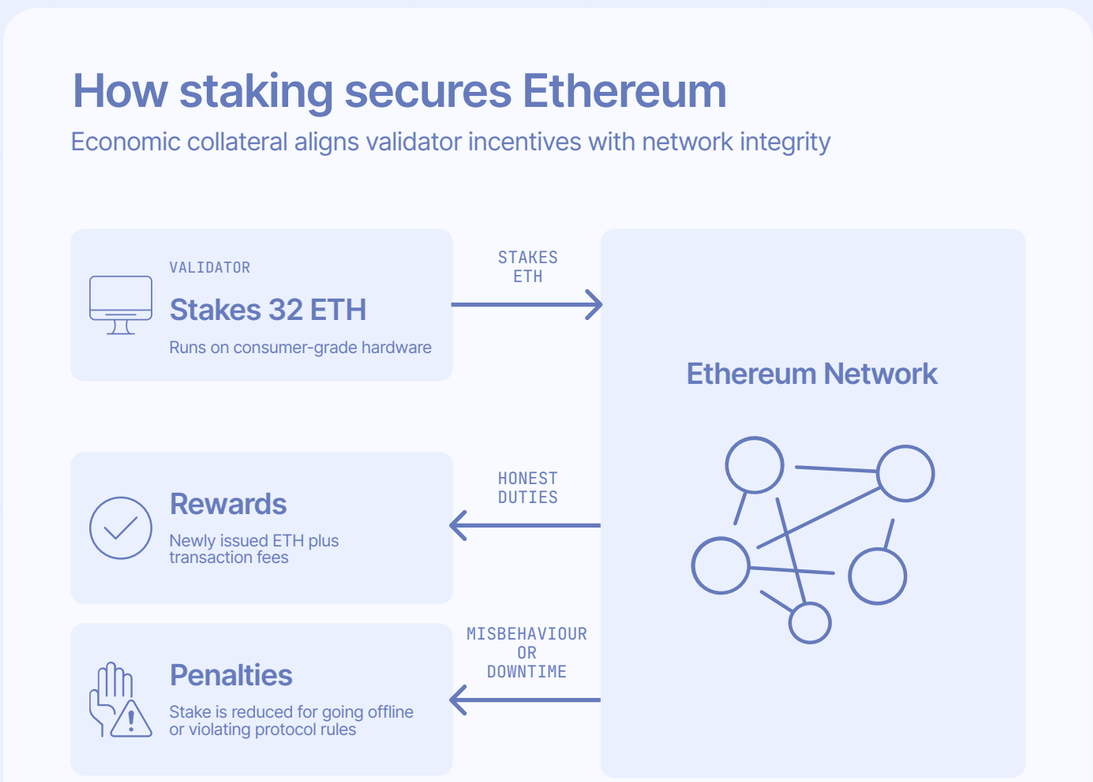
5

Staking is the mechanism used to secure the Ethereum network under the **proof-of-stake (PoS)** consensus model. It replaced the energy-intensive "mining" used in proof-of-work (like Bitcoin) with economic collateral.

- **Validator Participation:** To participate in the consensus process, a user must lock (stake) a specific amount of ETH (currently a minimum of 32 ETH) into the staking deposit smart contract. This deposit activates a validator node. Participation is open to anyone who meets the staking requirements and runs the validator software. Validators are operated by a diverse set of participants globally, contributing to the network's resilience and distributed security model.

- **Economic Incentives:** Validators are chosen pseudo-randomly to propose new blocks and all active validators periodically attest to the validity of blocks proposed by others. They are rewarded with transaction fees and newly issued ETH for performing these duties correctly.

- **Security via Slashing:** Staking aligns the incentives of validators with the health of the network. If a validator acts maliciously (e.g., by validating conflicting histories), a portion or all of their staked ETH is destroyed. This penalty is known as **slashing.** For unintentional failures that threaten **system stability**, such as mass downtime preventing the network from finalizing transactions, an emergency protocol called the **"inactivity leak"** [4] causes the staked assets of inactive participants to gradually diminish.



- **Energy efficiency and participation models:** Ethereum's transition to proof-of-stake reduced its electricity consumption by 99.98[5] percent and its carbon footprint was decreased by approximately 99.99[6] percent.

How does Ethereum achieve settlement and finality?

6

Ethereum distinguishes between **settlement,** when a transaction is executed and reflected in the system state, and **finality**, when that result becomes irreversible under the protocol.

Settlement occurs continuously, with transactions typically included in a block within 12 seconds. Transactions are included in blocks that update balances and smart contract state. Once included, these transactions are executed and reflected in the canonical chain.

Finality occurs periodically, approximately every 13 minutes under normal network conditions. Ethereum's consensus mechanism designates certain blocks as finalized at regular intervals. When a super majority of validators agrees on a checkpoint, that checkpoint and all prior blocks are treated as final by the protocol. Block production and finality are economically secured by validators staking ETH as collateral.

As of March 2026, over $76 billion[7] in ETH was locked in the protocol. To finalize a block, at least two-thirds of the total stake must attest within that approximately 13-minute window. By contrast, proof-of-work networks like Bitcoin do not have the notion of "finality" — once you own 51 percent of the hash-rate you could infinitely revert history.

If two conflicting finalized histories were created, this would mean an attempt to propagate something different from the canonical block. For this to occur, at least one-third of total stake would have had to sign both versions. Signing both versions would constitute **punishable behavior and the offending validators would be automatically penalized.** They would **lose their staked ETH through a process called slashing (and would be forcibly ejected from the validator set)**. Because penalties scale with the number of validators involved, large-scale coordinated attacks would result in substantial losses, making such behavior economically self-destructive.

Therefore, once finalized, reversing these blocks would require coordinated control of a large share of staked ETH and would trigger substantial penalties, **making reversal economically impractical and prohibitively expensive.**

In practical terms, Ethereum combines fast transaction execution with a clear, protocol-defined notion of irreversible settlement.

How do self-custodial wallets work and why are they critical?

Self-custodial wallets are software tools that allow users to interact with the blockchain while maintaining full control over their private keys. Unlike a bank account where a third party manages funds, a self-custodial wallet gives the user exclusive authority to sign transactions.

- **Private Key:** The wallet does not "store" assets; assets exist as records on the blockchain. The wallet stores the private key, which is the cryptographic proof of ownership required to authorize transfers. Losing the key means losing access to the assets, unless the wallet employs a recovery mechanism.

- **Criticality:** Self-custody is critical because it eliminates counterparty risk. In the event of a centralized exchange failure (e.g., FTX), users with self-custodial wallets are unaffected because they do not rely on the exchange's solvency. It creates a "certificateless" ownership model where individuals own digital assets directly, similar to holding physical cash or gold.

- **Programmable Capabilities:** Multisignature (multisig) configurations are a coordination mechanism in which a predefined number of approvals is required before a transaction can be executed, distributing control across individuals, communities, institutions, or other stakeholders to reduce single points of failure and enable transparent, auditable management of shared assets.

- **Social Recovery Mechanisms:** These enable users to designate trusted guardians who can collectively restore account access if credentials are lost, reducing reliance on seed phrase storage and aligning security with existing social trust relationships. While both rely on threshold-based coordination, multisignature governs transaction execution, whereas social recovery is generally limited to restoring access and does not grant ongoing control over funds.

Promoting Stability and Self-Sovereignty

This shift toward self-custodial and programmable account models introduces new ways of managing assets, identity, and transaction validation that have direct implications for financial stability, consumer protection, and market access.

- **Elimination of Counterparty Risk:** These mechanisms enable individuals and institutions to hold digital assets directly, reducing exposure to the failure or insolvency of centralized intermediaries.

- **Data Self-Sovereignty:** By placing control with end-users rather than centralized platforms, self-custodial wallets allow individuals to directly manage their data and identity, reducing dependence on intermediary-controlled systems.

- **Financial Inclusion:** Permissionless access enables anyone with an internet connection to participate in global financial systems without requiring approval from a central gatekeeper.

- **Integrity by Design:** Because transaction rules are defined in open-source code and verified by a distributed network, the system remains transparent, auditable, and consistently executed.

- **Built-in Interoperability:** Because users hold their assets and identity in a single, open standard, the same wallet can interact seamlessly with any application on the network without bespoke integrations, accounts, or onboarding for each one.

What is a layer 2?

8

Layer 2 networks are **independent execution environments that benefit from the security of their layer 1 blockchain.** Layer 2 networks on Ethereum use the base layer for security anchoring and final settlement, though the degree of security inheritance varies by the design decisions of each layer 2 network.

In the Ethereum ecosystem, the role of layer 2s has evolved significantly as the ecosystem has matured. Originally, layer 2s functioned as scaling solutions due to high transaction costs on the base layer. However, as the Ethereum base layer efficiency improves, the continued relevance of layer 2s is **less about raw throughput and more about differentiated functionality, custom execution environments, integrated data layers, and specialized application design.**

Rather than serving purely as scaling extensions, layer 2s are increasingly evolving toward modular, specialized environments. This includes:

- Privacy-preserving execution environments.
- High-throughput systems for gaming or social applications.
- Application-specific networks with tailored performance characteristics.

Under this model, layer 2s exist along a spectrum of integration with the mainnet, with differing assumptions around security, trust, function, and decentralization.

Which core technologies are used to preserve privacy on Ethereum?

9

Privacy is not only essential for personal safety, it is a key guarantor of decentralization. Avoiding centralized control over information, enabling self-sovereignty so end-users can choose what data they share, and building a privacy-first Ethereum are key priorities of the Ethereum ecosystem. The Ethereum community currently deploys a range of cryptographic technologies to further privacy on the network.

- **Zero-knowledge proofs** (ZKPs) are cryptographic techniques that allow someone to prove that a statement is true **without revealing the data used to prove it.** In practice, they make it possible to verify facts without unnecessary disclosure. ZKPs can be understood through the example of an identity check.

Many services need to confirm specific attributes about a person, such as whether they are over a certain age, have passed sanctions screening, or are resident in a particular jurisdiction. Today, this often requires sharing a full identity document, even though only **a single attribute, such as age eligibility,** is being verified. Using a zero-knowledge proof, the user can instead provide cryptographic confirmation that they meet the age requirement, without disclosing their name, date of birth, or other personal data. Various decentralized identity (DID) protocols built on top of Ethereum allow zero-knowledge proofs to be generated from verifiable credentials in order to achieve privacy-preserving KYC.

- **Multi-Party Computation (MPC):** Multi-Party Computation (MPC) is a cryptographic method that allows multiple parties to jointly compute a result without revealing their individual inputs. In practice, MPC is commonly used in institutional digital asset custody. Instead of storing a private key in a single location, key control is distributed across multiple parties. A transaction can only be authorized when a defined threshold of participants cooperates, aligning digital asset control with governance models such as quorum approval and segregation of duties. Ethereum itself does not require MPC to function. Rather, MPC operates at the wallet or custody layer above the protocol.

Ethereum provides a decentralized settlement environment onto which MPC-secured accounts can transact. For policymakers, MPC illustrates how cryptography can replicate familiar institutional control structures within a decentralized infrastructure context.

- **Fully Homomorphic Encryption (FHE):** FHE is a cryptographic technique that allows computations to be performed on encrypted data without decrypting it. FHE enables data to remain encrypted[8] throughout processing, with only the final result decrypted. Although still computationally intensive and not widely deployed at scale, FHE is an active area of research. In the context of public blockchains, it could eventually support confidential analytics or financial logic without exposing sensitive data on-chain. At present, Ethereum-based privacy solutions more commonly rely on zero-knowledge proofs rather than FHE. Nonetheless, FHE demonstrates that privacy and transparency are not mutually exclusive. Advanced cryptographic tools increasingly allow selective disclosure and verifiable computation, expanding the policy design space between full opacity and full public visibility.

Governance, Control, and Responsibility

Who operates Ethereum?

10

Ethereum is **not operated or governed by a single person, company, or organization.** There is no CEO, board, or central authority. The network is a decentralized ecosystem that is maintained by thousands of diverse contributors. Some types of Ethereum's key stakeholders include:

- **Core developers and researchers:** A global community of developers and researchers contribute to Ethereum's code and design. These contributors propose, discuss, and implement improvements through an open, public process[1]. Decisions are made by a group rather than by any single person. This structure is similar to the decision-making process at the Internet Engineering Task Force.

- **Node operators and validators:** Ethereum's network is maintained by independent node operators who run software that verifies blocks, transactions, and the current state of the chain. A subset of these operators act as validators by staking ETH, which allows them to propose new blocks and attest to the validity of blocks proposed by others. Full nodes independently verify all transactions and blocks, ensuring no participant must trust others for chain state. Validators are node operators who additionally stake ETH to participate in consensus, proposing and attesting to blocks. This mechanism secures the network through economic incentives and penalties, rewarding honest participation while discouraging malicious behavior. Because thousands of validators and nodes operate across different jurisdictions, organizations, and infrastructures, control over the network remains broadly distributed and resilient against attempted interference.

- **EIP Authors:** One important process used in Ethereum governance is Ethereum Improvement Proposals (EIPs). EIPs are standards specifying potential new features or processes for Ethereum. Anyone can create an EIP and be an EIP author. There is a formal, open and transparent process[2] for introducing EIPs and it is entirely consensus based.

- **Client Developers:** A client is an implementation of Ethereum that verifies data against the protocol rules and keeps the network secure. A node has to run two clients to participate on Ethereum: a consensus client and an execution client. Both of these clients exist in a variety of programming languages developed by different teams, known as client developers.

The Ethereum ecosystem is open to anyone. Anyone with a **consumer-grade computer, an internet connection, and Ethereum client software can run a node**, making participation comparatively accessible and less resource-intensive. This stands in deliberate contrast to networks such as Solana, where the hardware requirements to validate transactions are effectively data-center grade. Ordinary participants hence cannot realistically run their own node and must instead rely on a smaller set of professional infrastructure providers to interact with and verify the chain. That dependency introduces a counterparty risk by design. Users of those networks are not self-sovereign participants, but clients of an intermediary layer they cannot opt out of. On Ethereum, the ability to independently verify the chain is accessible to any individual with modest hardware, preserving the principle that **participation in the network does not require trusting anyone else**.

Anyone can participate in Ethereum, at any level

No gatekeeper, no application process, no central authority. Only open standards.

Use the network	Hold ETH, transact, interact with applications	REQUIRES: Internet connection
Run a node and validate	Verify transactions; stake ETH to help secure consensus	REQUIRES: Consumer-grade equipment
Build the network	Deploy smart contracts, applications, or alternative client software	REQUIRES: Open-source tools
Shape the protocol	Author improvement proposals (EIPs); research and review changes	REQUIRES: A written proposal

Responsibility within Ethereum emerges through functional roles that develop through participation and real-world use. Different actors maintain different layers of the system, coordinating through shared technical rules, community norms, and open governance processes rather than centralized management.

This structure mirrors the operation of other digital infrastructures that form the core plumbing of our civilization. The internet itself has no single owner; it functions through open standards, independently operated infrastructure, and distributed responsibility among network participants. Core protocols such as TCP/IP, Domain Name System, and Simple Mail Transfer Protocol are developed through open standards bodies such as the Internet Engineering Task Force and maintained by independent operators and developers.

As a result, both the internet's core protocols and Ethereum's **evolve through open processes, voluntary adoption, and the cumulative work of thousands of contributors rather than a centralized authority.** This open-source model allows Ethereum to function as neutral, shared infrastructure, much like the protocols that underpin email and the internet itself.

What is the role of the Ethereum Foundation (EF)?

The Ethereum Foundation (EF)[3] is a **non-profit organization** that is **one of many stakeholders** in the Ethereum ecosystem. Much like the Internet Engineering Task Force (IETF) in internet governance, the EF facilitates consensus-building around protocol development within a globally distributed, open-source community.

At the EF, our **mandate is two-fold:** (1) ensuring Ethereum stays a decentralized and resilient tool for self-sovereignty, empowering end-users with the final say over their identities, assets, actions, and agents, and (2) scaling the guaranteed availability of self-sovereignty to users. We strive to **help steward an Ethereum that upholds properties of censorship resistance, open-source, privacy, and security.** The Ethereum protocol and core application layers must be sustainable such that they would continue to reliably function and evolve even if the EF and today's core developers disappeared.

We focus on tasks that are least likely to be effectively undertaken by other ecosystem actors. This includes long-horizon research, neutral multi-client specs and tests, public-good security work, crisis coordination, preventing chokepoints, and core dev tooling and documentation where no sustainable owner exists. As soon as a function or role can be successfully managed by an aligned community actor, we facilitate that transition, so capability and responsibility diffuse through the ecosystem rather than concentrate in one place. **We do not operate the network, enforce protocol changes, or control participation.**

This **separation between stewardship and operational control is intentional, and is designed to preserve Ethereum's core design principles of neutrality and decentralization** while allowing the protocol to evolve through distributed coordination rather than centralized authority.

The EF's governance neutrality is further reinforced by its limited economic footprint in the Ethereum ecosystem. Based on the EF's most recent public disclosures[4], the EF's ETH holdings represent approximately 0.26 percent of total ETH supply, far below any level that would enable influence over network validation or protocol outcomes.

How are decisions made and upgrades managed on Ethereum?

12

To ensure the longevity and resilience of the Ethereum network, the protocol upgrades over time. Upgrades are achieved through a **well-defined, governance process rooted in open discussion, technical review, and voluntary adoption.**

Decisions regarding the evolution of the Ethereum protocol are managed through a transparent, open process called Ethereum Improvement Proposals (EIPs). An EIP is a technical specification for a proposed change, which is debated publicly by the community.

The Ethereum ecosystem **does not have a central authority** that decides on upgrades. The upgrade process follows an open, multi-stakeholder model, where protocol changes are debated, implemented, and adopted through broad participation rather than centralized decision-making. The process generally involves three stages:

1. **Proposal and Debate:** Technical discussions occur in public forums like the "AllCoreDevs" calls, which anyone can join and have been live-streamed for years. Anyone is able to propose changes.
2. **Client Implementation:** Once a specification is agreed upon, the independent client teams implement the changes in their respective software clients (e.g., Geth, Besu, Lighthouse, Prysm), releasing new versions of the client software that contain the new protocol rules.
3. **Network Adoption:** Upgrades are activated only when the network reaches a consensus. Node operators and validators must actively download and install new versions of client software, signaling their agreement to use it. When the agreed-upon timestamp hits, the upgraded software automatically flips the switch and begins enforcing the new rules.

If participants do not agree on a proposed change, they are not required to adopt it.

A widely cited **example of a successful protocol transition is The Merge**[5], executed in September 2022. The Merge was an upgrade that transitioned Ethereum's consensus mechanism from proof-of-work to proof-of-stake. The canonical Ethereum blockchain continued under proof-of-stake. Critically, the upgrade preserved existing transaction history, applications, and user balances, while reducing Ethereum's electricity consumption by 99.98[6] percent and its carbon footprint was decreased by approximately 99.99[7] percent, making it roughly 53,000 times[8] more energy-efficient than the Bitcoin network and roughly 100 times[9] more efficient than PayPal. The transition required coordinated adoption across multiple stakeholder groups, including software developers who implemented the upgrade, node operators and validators who adopted the new consensus rules, and users and application providers who chose to continue transacting on the upgraded network.

Can Ethereum be shut down or controlled by a single entity?

13

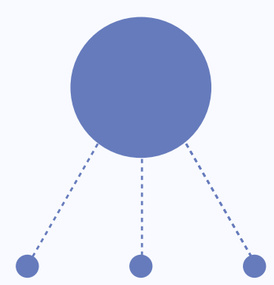
Ethereum is the most secure, resilient, and decentralized blockchain network in operation today. It is designed to be structurally **immune to single points of failure and unilateral influence**. Unlike conventional digital systems, including centralized banking platforms, cloud-hosted services, and traditional payment networks, **Ethereum cannot be unilaterally shut down or controlled by any individual, corporation, state, or institution.** Its resilience also extends to physical disruptions such as natural disasters.

Conventional digital systems are typically operated by a single organization or a small consortium. Outages, regulatory orders, cyberattacks, and insolvency events affecting these operators have repeatedly produced service disruptions of national or international scale. Even physical disruption, such as the April 2025 power blackout across Spain and Portugal, can take entire regions of digital infrastructure offline at once.

Ethereum, by contrast, has maintained **continuous operation since its launch in 2015**[10] through periods of extreme market volatility, attempted attacks, major protocol upgrades, physical disruptions, and significant shifts in the global regulatory environment. Its uptime record, sustained by distributed and economically incentivized participation rather than by any single operator's diligence, offers a model of resilience that is structurally difficult to replicate in centralized architectures.

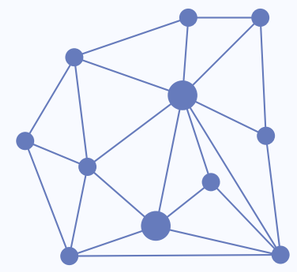
No single entity can shut Ethereum down

Centralized platforms can be shut down by a single entity. Ethereum's structure makes that impossible.



Centralized platforms

Run by a single operator



Ethereum

Run by thousands of independent operators

Single point of failure

The organization behind the centralized platform can suspend or terminate service at will, or be compelled to do so by external pressures.

No single point of failure

No party or localized physical disruption can switch off the network. It continues operating as long as nodes run it.

These properties are not incidental but derive from deliberate architectural, economic, and governance choices that **distinguish Ethereum from both centralized systems and other layer 1s.**

Critically, they are not merely passive safeguards. Ethereum's design ensures that the network does not simply lack a kill switch, but actively resists capture even when subjected to determined adversarial pressure.

Protocol governance

Protocol governance design provides the most direct framework for assessing whether a blockchain can be controlled or shut down. In any layer 1 system, governance determines where authority sits, that is, whether decisions are made by a network operator, a designated committee, or through a distributed staking and voting mechanism.

Different layer 1 designs involve materially different trade-offs. **Networks optimized for transaction speed often concentrate validators** to achieve performance, which increases coordination and capture risk. **Permissioned or consortium chains retain familiar governance models but reintroduce legal and administrative control points** that can be subjected to regulatory or judicial intervention. **Newer layer 1 networks typically combine limited operational history with concentrated token ownership**, producing elevated governance uncertainty.

Ethereum's governance and consensus model is grounded in **stake-weighted validator participation** rather than operator or committee control, and has been continuously battle-tested in public operation for over a decade. This concept does not exist in traditional digital systems, and the contrast with comparable layer 1 networks is especially structurally significant. Most other popular[11] protocols have critical single-entity development dependencies.

For instance, XRPL depends on Ripple for core development, TRON on the TRON Foundation, BNB Smart Chain on Binance and the BNB Smart Chain Foundation, and Canton on Digital Asset. During the 2022 bridge exploit, the CEO of Binance publicly directed a chain halt, demonstrating[12] that a single individual could influence the suspension of transaction processing on BNB Smart Chain, with the network deliberately halted for ~8 hours following a bridge exploit affecting over $500 million. No comparable intervention is available on **Ethereum, where, by design, no single authority may direct such action.**

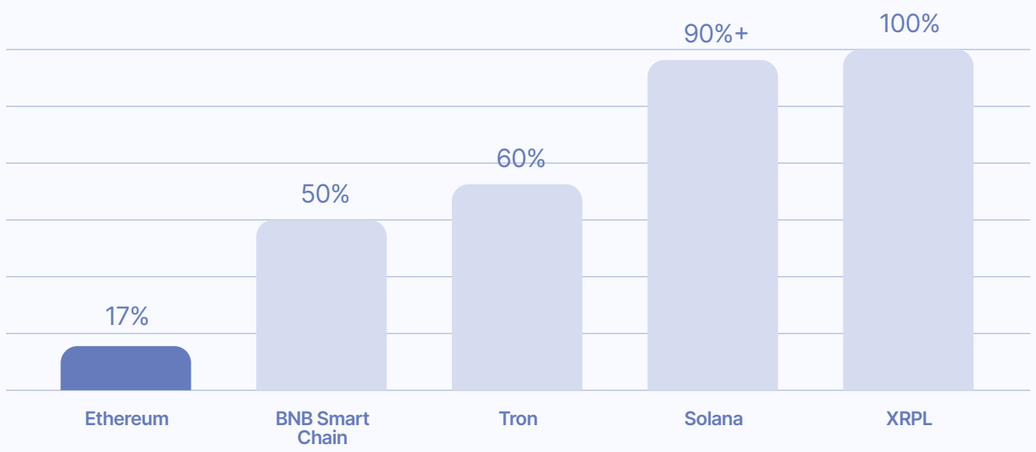
Decisions are instead taken based on **consensus among client teams**.

This structural difference reflects Ethereum's broader governance architecture, in which protocol changes require multi-team consensus across independent organizations. This assures that **no single team is able to unilaterally push changes, ensuring that no individual, executive, or coalition can alter the network's rules or suspend its operation without broad and observable consent.**

Token concentration at genesis is another critical factor that shapes long-term governance dynamics[13] , since in Ethereum, BNB Smart Chain, TRON, and Solana, token holdings translate directly into influence over protocol decisions. Ethereum allocated ~17 percent to insiders. BNB Smart Chain reserved 50 percent for the founding team and angel investors, with the remainder offered through public sale. Solana reportedly allocated more than 90 percent to insiders. TRON directed 60 percent to the founding team and angel investors. XRPL allocated its entire initial supply to the company and founders.

Insider allocation at genesis

Ethereum's launch was the most broadly distributed



Token holdings translate directly into long-term governance influence. Lower insider concentration means more distributed protocol authority.

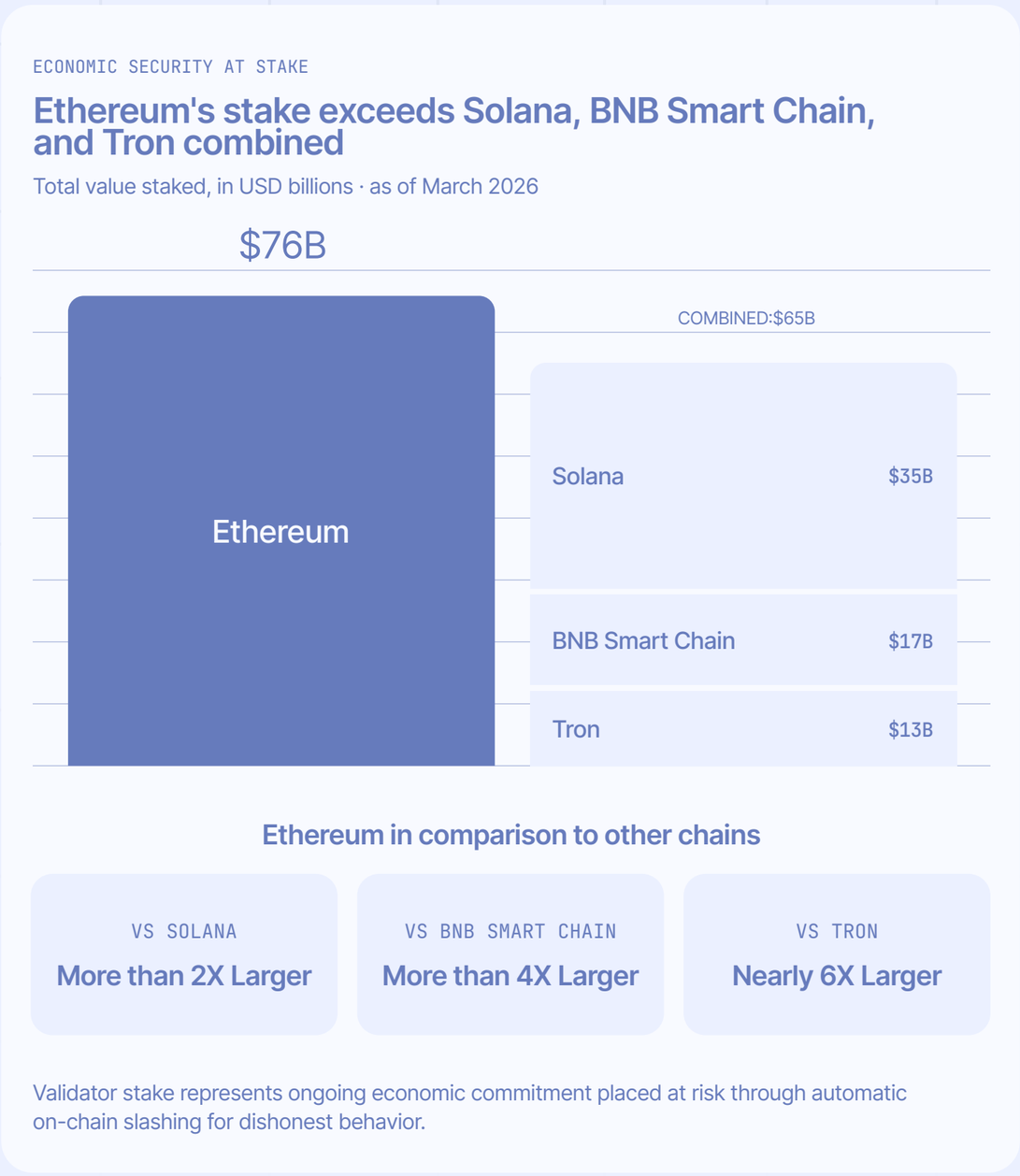
Further, as of March 2026, Ethereum was **supported by more than 900,000 validators**[14] that verify protocol rules and maintain copies of the ledger. Consensus decisions on block validity and finality are made through stake-weighted validator voting. Participation is publicly observable, economically constrained, and distributed across a wide and diverse set of participants, while software adoption remains voluntary across the ecosystem. This **validator population is the largest among**

other popular networks[15] **, by orders of magnitude**. Solana[16] has more than 800 validators. BNB Smart Chain, XRPL, and TRON[17] each maintain sets of validators ranging from dozens to ~100. One of the fundamental reasons for the large number of validators on Ethereum is the **low barrier to entry which essentially enables anyone with consumer-grade hardware to meaningfully engage with the network.** This is materially different from other popular networks. Solana, for instance, requires enterprise-grade infrastructure far beyond the reach of average participants. Censorship resistance therefore derives from the distribution of validator voting power, rather than from node count alone.

Voting power and consensus

Ethereum's proof-of-stake consensus mechanism distributes voting power through a stake-weighted system with built-in economic accountability. Validators are responsible for proposing and attesting to blocks, and participation requires staking a minimum of 32 ETH as economic collateral. Voting power is proportional to the amount of ETH staked, and network finality requires agreement from a supermajority of at least two-thirds of active staked ETH. This threshold follows established Byzantine fault tolerance principles, under which the network continues to operate correctly even if up to one-third of participating stake is offline, compromised, or behaving maliciously.

Collectively, validators staked approximately $76 billion in ETH[18] , as of March 2026, representing a substantial and ongoing economic commitment to Ethereum's security. This capital is explicitly at risk. **Validators that fail to perform their duties incur small but continuous penalties, while validators that attempt to manipulate consensus are subject to slashing, that is, the automatic destruction of part or all of their staked ETH.**



These penalties are enforced automatically by protocol rules, producing accountability that operates consistently across jurisdictions and without recourse to any administrative authority. Most other popular protocols,[19] including Solana, do not have this penalty mechanism, which is critical for security. Their economic stake is also substantially lower[20] than Ethereum's. Solana, TRON, and BNB Smart Chain are secured by $35 billion, $13 billion, and $17 billion respectively.[21]

A distinctive property of Ethereum's design is the **inactivity leak, which is a penalty mechanism that gradually drains the stakes of validators who go offline.** This shifts voting power to the remaining active validators, ensuring the network can keep finalizing transactions even if a large portion of participants disappear. The practical significance of this mechanism is **reflected in Ethereum's operational record. Ethereum has never stopped operating since its launch in 2015.** This track record is unparalleled across both centralized platforms and other popular layer 1 networks.[22]

There have been several **recent examples where centralized systems** such as AWS,

Crowdstrike, Cloudflare, and Microsoft Azure that underpin much of today's digital and financial infrastructure have faced debilitating outages. In the same vein, **other layer 1 blockchains have also faced significant disruptions**. For instance, Solana has experienced the most network failures[23] , with at least seven outages including one lasting ~19 hours. BNB Smart Chain was deliberately halted for ~8 hours following a bridge exploit affecting over $500 million. XRPL halted twice (longest ~64 minutes), and TRON halted once (~2 hours).

Ethereum's consensus mechanism operates through two coordinated software layers: the execution layer, which processes transactions and maintains state, and the consensus layer, which coordinates validators and achieves finality. Once data is added to the blockchain, it is cryptographically linked to previous blocks.

Distributed network operation

Ethereum's operational resilience is reinforced by the geographic, jurisdictional, and organizational distribution of validators. The network relies on thousands of independent entities to perform consensus functions, distributed across continents, legal jurisdictions, energy systems, cloud providers, and client development teams. Approximately 35 percent of validators[24] are hosted on cloud infrastructure, across multiple providers to avoid a single point of failure. There is no centralized registry that concentrates control or attribution in any single entity or jurisdiction.

Even in the event that a major nation-state were to prohibit Ethereum participation within its borders, the network would continue to operate without interruption through validators in other jurisdictions. This redundancy is a structural property of the system, not a discretionary policy that can be revoked.

The principal indicators by which the distribution of voting power may be assessed are summarized in the table below, together with their significance for network resilience. On each of these measures, Ethereum compares favorably both to alternative layer 1 networks and to the centralized digital infrastructure on which most institutions currently depend.

Indicators of Voting Power Distribution	Significance for Network Resilience
GEOGRAPHIC DISTRIBUTION	Validator participation distributed across multiple jurisdictions reduces exposure to any single legal regime, regulatory action, or political contingency. Ethereum validators operate across continents and dozens of jurisdictions.
CLIENT DIVERSITY	The use of multiple independent software implementations reduces the systemic risk that a defect or compromise in any one codebase could cause network-wide failure. Ethereum supports five or more independent clients in production at both the execution and consensus layers, a property unmatched among comparable layer 1 networks.
OPERATOR DIVERSITY	The presence of validators with differing legal obligations, risk tolerances, commercial incentives, and political contexts diversifies the network's response to external shocks and renders sustained collusion impractical. Ethereum's validator population spans solo operators, institutions, regulated custodians, staking services, exchanges, and decentralized staking pools, with no single entity approaching either threshold.
INFRASTRUCTURE DIVERSITY	Diversity of cloud providers, hosting arrangements, and physical infrastructure prevents any single provider's outage, policy change, or coercion from disrupting the network. Approximately 35 percent of Ethereum validators are hosted on cloud infrastructure, distributed across multiple providers, with the remainder operating on independent or bare-metal infrastructure.
STAKE CONCENTRATION	Measures whether a small number of entities could compromise. Higher concentration increases coordination risk. Ethereum's stake is distributed across solo operators, institutional custodians, staking services, exchanges, and decentralized staking pools, with no single entity approaching either threshold.

Credible neutrality

A further dimension of Ethereum's resilience lies in what is often termed its credible neutrality. The **protocol applies the same rules to every participant** regardless of identity, nationality, or political affiliation. There is no administrative interface[25] through which a privileged party may freeze accounts, reverse transactions, or deny service. Ethereum does not have a single actor who can unilaterally override or censor

transactions through a privileged protocol-level mechanism. **There are no[26] built-in admin keys, emergency kill switches, or protocol-level override functions**. Neutrality also requires that operations themselves remain visible. Ethereum's protocol, state, and operational behaviour are inspectable by any participant, which means that any attempt to introduce opaque rules or policies cannot be hidden.

Where Ethereum differs materially from other layer 1s is in the practical, as opposed to merely formal, distribution of authority. On networks where a small number of validators[27] or a single foundation effectively controls protocol evolution, the absence of formal kill switches is of limited practical consequence. On Ethereum, the absence of such mechanisms is reinforced by the genuine distribution of authority across thousands of independent stakeholders.

Software upgrades to the Ethereum protocol take effect only when validators and node operators voluntarily run new client software. Any proposed change that lacks broad community support will simply not activate, as the network will continue to operate under the previous rules. This consensus-based governance is materially different from the unilateral control structures characteristic of centralized platforms, where a single corporate or governmental decision can change the terms of service for all users overnight.

For institutional users and governments, this property has significant implications. **Settlements, contractual obligations, and recorded states on Ethereum are not subject to discretionary intervention by an operator.** For applications such as cross-border settlement, registry services, identity attestation, and the tokenization of financial instruments, this **provides a degree of finality and predictability that legacy systems cannot match.**

Attack vectors and why they fail on Ethereum

A report by a leading blockchain cybersecurity firm, OpenZeppelin, identifies the following three attack vectors that typically apply across blockchain networks.[28] Each is examined below in the context of Ethereum's specific defenses.

- **Acquiring sufficient economic stake:** As of March 2026 Ethereum's security derived from $76 billion[29] in staked assets, with automatic slashing (penalties) that destroys attacker's collateral. For an external entity to unilaterally influence consensus by finalizing a fraudulent transaction where the attacker would need to convince the network to acknowledge and mark as irreversible a transaction that was invalid, or never even happened, they would require commanding upwards of $50.7 billion[30] in ETH (as of March 2026). This figure is the highest among[31] other popular networks. Solana, TRON, and BNB Smart Chain are secured by $35 billion[32] (cost of finalizing a fraudulent transaction $23.3 billion[33]), $13 billion[34] (cost of finalizing a fraudulent transaction $8.7 billion[35]), and $17 billion[36] (cost of finalizing a fraudulent transaction $11.3 billion[37]) respectively.

  Acquiring a stake of this magnitude would itself be observable in public markets and would drive the price of ETH sharply upward during accumulation, further increasing the cost of attack.

Cost to finalize a fraudulent transaction

Ethereum sets the highest barrier to attack

Ethereum	Solana	BNB Smart Chain	Tron
$50.7B	$23.3B	$11.3B	$8.7B
Highest barrier to attack	More than 2X cheaper to attack	More than 4X cheaper to attack	Nearly 6X cheaper to attack

Once deployed in an attack, the attacker's stake would be subject to automatic on-chain slashing. **The economic deterrent is materially more stringent on Ethereum[38] than on comparable networks.** Ethereum automatically penalizes up to all of the attacker's staked collateral. This too is unique among its competitors[39] as Solana has no automatic penalty mechanism in place and TRON imposes no economic penalties at all.

The economic security model of Ethereum thus converts attempted attacks into immediate and irrecoverable financial losses, with the cost of attack scaling alongside the value of the network itself.

- **Executing a supply chain attack on validator client software:** Supply chain risk is most acute where a single codebase dominates network operation. Ethereum employs unmatched client diversity[40] at both the execution and consensus layers. At least five or more independent teams[41] maintain these open-source clients across both the execution layer and the consensus layer each.

  Solana[42] has two independent implementations, though one dominates. BNB Smart Chain and TRON[43] rely on a single codebase where a critical vulnerability in any of them would affect 100 percent of validators simultaneously. The cloud providers and physical server infrastructure utilized by Ethereum nodes and validators are similarly diversified.[44] Unlike most other layer 1 blockchains, Ethereum's operation does not depend on any single client software implementation, materially reducing the likelihood that a defect or compromise in any one codebase could cause systemic disruption.

- **Colluding with a sufficient number of validators:** Coordinated collusion at the scale required to compromise consensus would necessitate[45] the cooperation of validators controlling at least one-third of staked ETH (to halt finality) or two-thirds (to manipulate it and finalize a fraudulent transaction). Validators on Ethereum include solo operators, institutional custodians, staking services, exchanges, and decentralized staking pools, distributed across continents, legal jurisdictions, energy systems, cloud providers, and client teams. Differences in legal obligations, risk tolerances, commercial incentives, and political contexts make sustained collusion at this scale extraordinarily difficult to organize and conceal. Any detectable collusion attempt would also trigger the same slashing penalties described above, exposing colluding parties to catastrophic and automatic financial loss. By contrast, for networks with small validator sets, like BNB Smart Chain and TRON, collusion is a structurally more accessible vector[46] than on networks with larger, more distributed sets.

Comparative Analysis of Different Blockchains

What are the key differences between permissioned and permissionless blockchains?

14

Permissioned and permissionless blockchains are often understood as binaries of one another. That is an oversimplification. **They are better understood as two ends of a spectrum. Every blockchain sits somewhere between those extremes, depending on its particular features.**

Blockchains close to the permissionless end of the spectrum are open by default. Anyone can read the data. Anyone can send transactions. Anyone can become a validator or node operator without asking a company, government, or committee for approval. There is no central list of who is allowed in. The system runs because many independent participants are incentivized to follow shared rules and face automatic penalties for misbehaving, not because a central authority grants access.

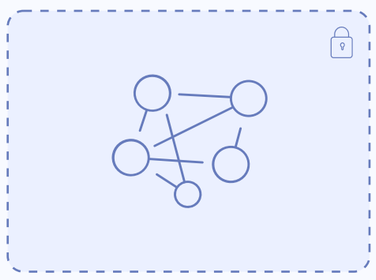
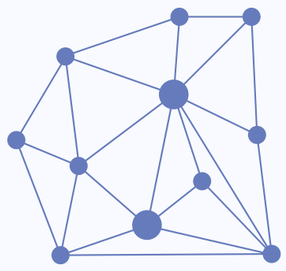
Blockchains close to the permissioned end of the spectrum are restricted by design. Only approved participants can validate transactions. Access may require identity verification or membership in a specific organization. Governance decisions are made by a defined group. Because control is concentrated among known actors, transaction filtering or rule changes can be coordinated more easily.

A useful analogy is the **internet versus an intranet.**

The internet is open. Anyone can connect to it, publish content, or build applications without asking for central approval. That is similar to a permissionless blockchain.
An intranet is private. It is limited to employees or approved members of an organization. Access is controlled, and administrators can decide who participates. That resembles a permissioned blockchain.

Permissioned and permissionless blockchains

The same structural distinction that separates intranets from the open internet.

	PERMISSIONED BLOCKCHAIN Like an intranet	PERMISSIONLESS BLOCKCHAIN Like the open internet
		
ACCESS	Requires approval	Open to anyone
OPERATORS	Defined group	Anyone can run a node
FINALITY AND TRUST	Trust in the operator group	Cryptographic and economic
SINGLE POINT OF FAILURE	Yes, the operator group	No
CENSORSHIP RESISTANCE	Limited, set by the operators	Strong, no party can block use

FEATURE	HIGHLY PERMISSIONED (e.g., consortium blockchains)	HIGHLY PERMISSIONLESS (e.g., Ethereum)
RESILIENCE	**Vulnerable** Prone to single points of failure; if the group or consortium is compromised, the network stops	**Anti-fragile** Designed to survive state-level attacks and localized internet outages via a global node set
ACCESS CONTROL	**Restricted** Users must be vetted or whitelisted by a central authority to join	**Open** Anyone with an internet connection can transact or deploy code
VALIDATION	**Centralized** Only known entities can run nodes or verify blocks	**Decentralized** Thousands of anonymous, globally distributed validators secure the network
CENSORSHIP RESISTANCE	**Low** A central admin can freeze accounts, reverse transactions, or soft-censor users	**High** Protocol ensures no single actor can block a valid transaction
INNOVATION	**Closed** Development is restricted to insider groups; requires permission to build apps	**Permissionless** Anyone can build and compose new financial tools (DeFi, stablecoins) instantly or participate in the development of the blockchain
FINALITY & TRUST	**Legal/Contractual** Trust is placed in the legal standing of the operators	**Cryptoeconomic** Trust is mathematically enforced by slashing capital for dishonest behavior

The spectrum from highly permissioned to highly permissionless is broad. Just like the internet represents the open, globally accessible base layer for the world's custom digital applications, Ethereum serves as neutral, censorship-resistant base infrastructure for applications tailored to specific mandates.

When governments and institutions evaluate blockchains for adoption, **the question of where a given chain sits on this spectrum should be assessed against the specific objectives of the deployment**, not treated as an abstract property. Different goals demand scrutiny of different factors.

For instance, if a primary **objective is to eliminate a single point of failure**, it is imperative to evaluate **how many independent validators** secure the network, the **distribution of stake** between them, and if they are **geographically and jurisdictionally distributed**. It is also worth assessing whether any **single entity, company, government, or consortium, can shut down or pause the network unilaterally**. It is worth determining if the **client software is diversified**, so that a bug in one implementation does not take down the whole system. A permissioned blockchain, by design, concentrates validation among a known and restricted group of operators. If that group is compromised, coerced, or simply ceases to operate, the network fails.

This structure mirrors how other digital infrastructures that currently form the core plumbing of the world operate. The internet itself has no single owner; it functions through open standards, independently operated infrastructure, and distributed responsibility among network participants. Core protocols such as TCP/IP, Domain Name System, and Simple Mail Transfer Protocol are developed through open standards bodies such as the Internet Engineering Task Force and maintained by independent operators and developers.

As a result, both the internet's core protocols and Ethereum's evolve through open processes, voluntary adoption, and the cumulative work of thousands of contributors rather than centralized authority. This open-source model allows Ethereum to function as neutral, shared infrastructure, much like the protocols that underpin email and the internet itself.

How is the Ethereum blockchain different from the Bitcoin blockchain?

15

Bitcoin and Ethereum are **both decentralized blockchain networks**, but they were **designed for different purposes**. Bitcoin was created as a system for the peer-to-peer transfer of value and is widely understood today as a digital monetary asset or store of value. Its design prioritizes simplicity, stability, and resistance to change.

Ethereum, by contrast, was designed as a general-purpose digital public infrastructure for programmable applications, analogous to how the internet provides a shared foundation for information exchange.

While Bitcoin supports limited scripting, **Ethereum was designed from the outset for general-purpose programmability.** Its Turing-complete virtual machine allows arbitrary rules and logic to be embedded directly into financial and non-financial arrangements. Ethereum can thus support programmable transactions and applications such as stablecoins, payment systems, social protocols, attestations, and identity solutions. This enables Ethereum to function as a shared platform rather than a single-purpose system for value exchange.

Key differences include

- **Functionality:** Bitcoin focuses on transferring digital value between participants. Ethereum supports programmable transactions, allowing rules and logic to be embedded directly into financial and non-financial arrangements.
- **System design:** Bitcoin uses an Unspent Transaction Output (UTXO) model, which tracks discrete units of value as they move between users. Ethereum uses an account-based model that maintains balances and application state, making it better suited for complex programmable logic.
- **Energy and security model:** Bitcoin secures the network through proof-of-work, which requires continuous expenditure of computational energy. Ethereum has transitioned to proof-of-stake, which secures the network through locked economic collateral rather than ongoing energy consumption. Transitioning to proof-of-stake reduced Ethereum's electricity consumption by 99.98[1] percent and its carbon footprint was decreased by approximately 99.99[2] percent, while maintaining network security.

How does Ethereum compare with other public blockchains?

16

Ethereum is widely used as digital public infrastructure because **it prioritizes security, neutrality, and long-term reliability.** This neutrality is made credible by **decentralization at every layer**: validator participation, protocol governance, open-source development, and client diversity. No single company, consortium, or state controls transaction ordering, system upgrades, or access to the network.

This **diversity is a direct source of resilience**. Ethereum's validator set is secured by multiple independent client implementations, effectively meaning that **a bug, vulnerability, or failure in any single implementation does not propagate across the entire network**. Where a network built on a single client codebase faces the risk of a single defect causing widespread outage, Ethereum's multi-client architecture means that the failure of one implementation, if any, is contained while the rest of the network continues to operate normally.

By contrast, layer 1s including Canton, BNB Smart Chain, TRON, and Ripple only have a single client[3]. As per its 2025 report[4], there are two primary validator client implementations for the Solana network, with 92 percent of the network's validators running on Agave representing substantial centralization. This concentration poses critical risks.

The same principle extends across the stack: because no single entity controls infrastructure, governance, or development, there is no single point of pressure, compromise, or failure that can bring the network down or redirect it. Resilience on Ethereum is not a property of any one component but an emergent quality of the whole system's diversity.

Network outages since launch

Ethereum Launched in 2015 - 0 network outages	**NONE** Uninterrupted since launch
Solana Launched in 2020 - At least 7 outages	**~19 Hours** in 2023
BNB Smart Chain Launched in 2020 - At least 1 outage	**~5 Hours** in 2022
XRP Ledger Launched in 2012 - At least 1 outage	**~1 Hour** in 2025

Unparalleled resilience

Ethereum has maintained **continuous operation and uninterrupted uptime**[5] since its launch in 2015. **No other**[6] smart contract platform can match that record. For instance, **Solana**, another popular blockchain, has witnessed at least **7 major outages**[7] since its launch in 2020. The longest reported outage of the Solana network lasted about **19 hours**[8] and the last major outage spanning nearly 5 hours was reported in February 2024.[9] **BNB Smart Chain**, also launched in 2020, was "paused"[10] for at least 5 hours in 2022. **XRP** Ledger, a chain launched in 2012 has also witnessed similar incidents, including a stoppage for over an hour[11] in 2025.

Decentralization of validators by design

Validator operations on Ethereum are **geographically distributed**[12] **across continents and legal jurisdictions**. This diversity is partially attributable to the relatively low barrier to participation. Anyone with average consumer-grade computers, Ethereum's client software, and 32 ETH to stake can become a validator. These **participation requirements are relatively accessible and substantially less onerous than those of many other blockchains.**

By contrast, **Solana and BNB Smart Chain**[13] **validator operations demand enterprise-grade infrastructure far beyond the reach of average participants.** Beyond hardware, operators must maintain deep Linux administration expertise, manage cryptographic identity keys, and sustain near-perfect uptime to avoid penalties. These steep requirements concentrate Solana and BNB Smart Chain validation among well-capitalized enterprise operators which is a stark contrast to Ethereum's relatively open validator landscape. These accessible requirements have resulted in **unparalleled diversity in Ethereum's validator set**, which in turn reduces reliance on any single provider, rendering the system more decentralized, secure, and neutral.

Unmatched infrastructure and client diversity

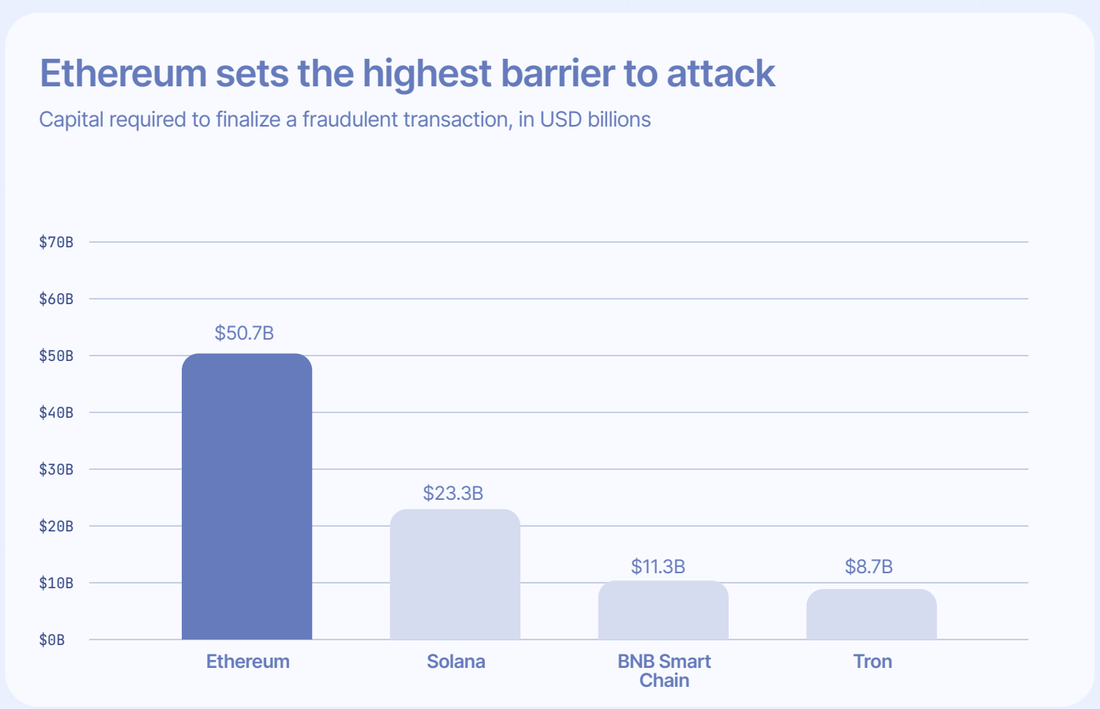
The **cloud providers**[14] **and physical server infrastructure utilized by nodes and validators on Ethereum are also diversified**. The Ethereum community further **maintains several open-source clients**[15] **developed by at least 5+ teams using different programming languages.** These efforts materially reduce the likelihood of a single point of failure. By contrast, the infrastructure and client ecosystems of other popular layer 1s exhibit meaningful points of centralization across both dimensions. **Solana**, for instance, has limited client diversity. As per its 2025 report,[16] there are two primary validator client implementations for the Solana network, with 92 percent of the network's validators running on Agave representing substantial centralization. Many other chains, including **BNB smart chain, TRON, and XRP Ledger** have no client diversity[17] and rely on a single client, creating a material risk.

Economic security at scale

Beyond the logistical hurdle of compromising so many independent and diverse nodes on Ethereum, **executing an attack would require acquiring, and risk the destruction of, tens of billions of dollars in capital, rendering it prohibitively expensive.** The system is designed to destroy staked ETH if validators behave dishonestly through the process called slashing.

As of March 2026, $76 billion[18] in ETH was staked on the Ethereum network. **Controlling the two-thirds majority required to finalize a fraudulent transaction would require commanding upwards of $50.7 billion**[19] **in ETH**.

If two conflicting finalized histories were created, this would mean an attempt to propagate something different from the canonical block. For this to occur, at least one-third of total stake would have had to sign both versions. Signing both versions would constitute **punishable behavior and the offending validators would be automatically penalized.** They would **lose their staked ETH through a process called slashing (and would be forcibly ejected from the validator set)**. Because penalties scale with the number of validators involved, large-scale coordinated attacks would result in substantial losses, making such behavior economically self-destructive. Subsequently, coordinated attacks at scale are prohibitively expensive.



The economic security models of other popular layer 1s differ from Ethereum's in two important structural ways. First, the dollar value of capital at risk is substantially lower, and second, the mechanisms for punishing dishonest behavior are either materially weaker or, in some cases, absent altogether.

For instance, as of March 2026, Solana, TRON, and BNB Smart Chain were secured by $35 billion[20] (cost of finalizing a fraudulent transaction $23.3 billion[21]), $13 billion[22] (cost of finalizing a fraudulent transaction $8.7 billion[23]), and $17 billion[24] (cost of finalizing a fraudulent transaction $11.3 billion[25]) respectively. This is **materially lower than the value** securing Ethereum.

Further, unlike Ethereum, Solana, XRP Ledger, and TRON do not employ an automatic slashing mechanism.[26] This means that on Solana for instance, a validator that behaves dishonestly does not face automatic, immediate destruction of their staked capital and enforcement depends on social coordination and a network restart, which renders the deterrent a lot less effective. **BNB Smart Chain** security is also structurally narrow. The network relies on a small number of active validators.[27] The economic cost of capturing consensus is therefore not a function of thousands of independent validators, like it is in **Ethereum. Ethereum's combination of $76 billion in staked ETH, automatic slashing enforced algorithmically on-chain, and penalties that scale with the size of a coordinated attack creates a deterrent architecture that none of these alternatives can match.**

No incremental counterparty risk

For policymakers and institutions, Ethereum's unparalleled **decentralization, neutrality, and security** matters, as building on the network does not introduce counterparty risk. There is no operator that could change rules, restrict access, alter monetary policy, reprioritize the network for commercial advantage, or unilaterally turn it off. The integrity of the system does not depend on the continued solvency, goodwill, or strategic interests of any one entity. Instead, it rests on a globally distributed validator set and transparent, open governance processes.

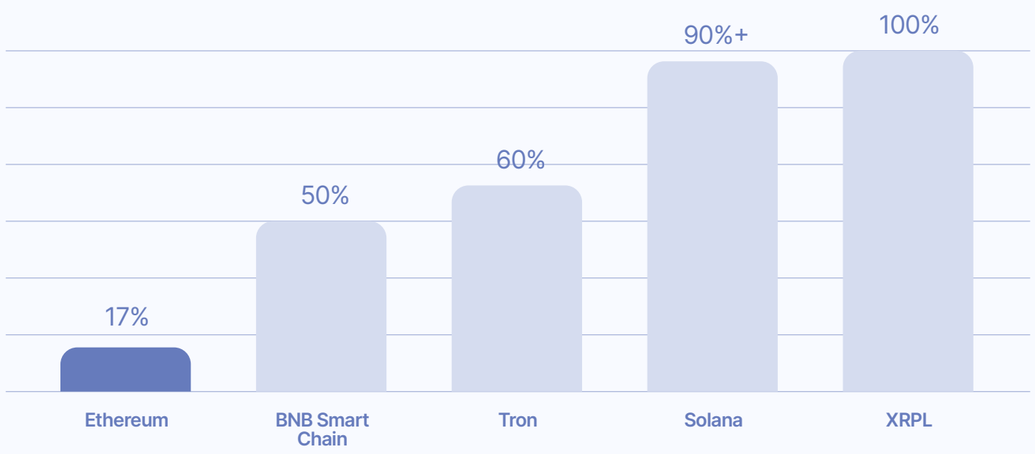
This is structurally different from many other layer 1s. **Solana's structure, for instance, concentrates significant influence in the Solana Foundation**, which directly shapes the

validator ecosystem through avenues such as its delegation program.[28] The program helps contributors within the Solana ecosystem become network validators by covering several aspects of the involved cost through mechanisms like stake matching and vote cost coverage. This places the Solana Foundation as a critical counterparty in this ecosystem. In the same vein, Binance has often been criticized[29] for the material control it exercises over the **BNB Smart Chain**. Similarly, Ripple controls approximately 42 percent[30] of **XRP's** total supply, with this control extending to validator selection and node lists, raising concerns about governance risks.

Token concentration at genesis[31] further shapes long-term governance dynamics, since in Ethereum, BNB Smart Chain, TRON, and Solana, token holdings translate directly into influence over protocol decisions. Ethereum allocated ~17 percent to insiders. BNB Smart Chain reserved 50 percent for the founding team and angel investors, with the remainder offered through public sale. Solana reportedly allocated more than 90 percent to insiders. TRON directed 60 percent to the founding team and angel investors. XRPL allocated its entire initial supply to the company and founders.

Ethereum's launch was the most broadly distributed

Insider allocation at genesis



Token holdings translate directly into long-term governance influence. Lower insider concentration means more distributed protocol authority.

While many public blockchains optimize for other elements at the cost of decentralization, Ethereum has deliberately evolved as a neutral global settlement layer. Its design choices prioritize long-term resilience and credible independence, enabling sovereign, institutional, and cross-border use cases.

Compounding network effects

Beyond security and decentralization, Ethereum benefits from a **self-reinforcing network effect that no other layer 1 has yet replicated**. It is, by a wide margin, the **most mature blockchain ecosystem**. It is the most **thoroughly documented** and **widely-tooled** public blockchain in existence. **ERC-20** Ethereum assets are the most **commonly supported token standards, which makes integration easier across** these platforms and service providers, but still allows for whitelisting, configuration, and compliance enablement on a case-by-case basis. The same applies to other ERC-based token standards. **Native composability throughout Ethereum-based finance increases utility while reducing payment rail fragmentation**. Notably, these standards can be implementable by any developer, custodian, or institution without permission or license fee.

Building on Ethereum therefore means building on a standard that thousands of institutions already use, rather than negotiating bespoke connections with every counterparty from scratch. Ethereum hosts the world's **largest global developer community** and the most diverse application layer of any public blockchain. As of May 2026, live data from open-source code deployments indicate that the EVM stack is supported by ~11,000[32] developers, significantly exceeding all other blockchain ecosystems. Contrast this with **Solana** which has ~2,600[33] developers, **BNB Smart Chain** with ~837[34] developers, **TRON** with ~359[35] developers, and **Ripple** with ~272[36] developers.

This scale of Ethereum developers translates directly into a depth of open-source tooling, audited libraries, security research, and documentation that competing chains cannot match. **The practical implication is that an engineering team integrating with Ethereum finds well-maintained standards, abundant reference implementations, and a global talent pool already familiar with Ethereum Virtual Machine (EVM) development.**

The EVM is a computation engine, not hugely dissimilar to the virtual machines of Microsoft's .NET Framework, or interpreters of other bytecode-compiled programming languages such as Java. EVM has become a de facto industry standard for smart contract execution across several chains.

For governments and institutions, this is not merely a developer convenience. Interoperability of this kind is increasingly recognized as a determinant of operational capability. Coordination across jurisdictions, whether for cross-border settlement or identity attestation depends on shared standards that no single party controls. Building on Ethereum gives institutions access to the most widely adopted shared standards in the blockchain ecosystem, with long-term portability across multiple compatible networks.

Leading institutional adoption across the global financial system

Ethereum's ecosystem maturity has translated into **sustained adoption by regulated institutions across banking, asset management, custody, payments, and market infrastructure.** This adoption is no longer limited to isolated pilots. It spans live products, regulated funds, settlement infrastructure, and multi-year institutional programs built on Ethereum or Ethereum-anchored layer 2 networks.

Institutions actively building or operating on Ethereum include:

- **Global banks** such as JPMorgan,[37] Société Générale,[38] UBS,[39] Deutsche Bank,[40] and Standard Chartered,[41] using Ethereum-based infrastructure for tokenized bonds, deposits, funds, and regulated settlement pilots.
- **Global asset managers** including BlackRock,[42] Fidelity,[43] Franklin Templeton,[44] and Amundi,[45] issuing tokenized money market funds, government securities, and investment products directly on Ethereum.
- **Custody and market infrastructure providers** such as BNY Mellon[46] and SWIFT,[47] supporting Ethereum-native assets and exploring interoperability between traditional financial infrastructure and public blockchain settlement.
- **Global payment networks and processors**, including Visa,[48] Mastercard,[49] and PayPal,[50] operating stablecoin settlement, credentialing, and programmable payment infrastructure on Ethereum.
- **Regulated trading and fintech platforms** such as Robinhood and Coinbase[51] building Ethereum-based layer 2 networks optimized for tokenized real-world assets, stablecoins, and on-chain capital markets access.

Taken together, these deployments reflect a structural shift. Ethereum is no longer perceived by institutions as an emerging experiment, but as a neutral, public digital infrastructure that can support financial and socioeconomic activity at scale while remaining interoperable across jurisdictions and market participants.

Leading settlement layer for stablecoins and tokenized assets

Ethereum's leadership in economic security and network reliability makes Ethereum the primary settlement layer for stablecoin transactions, far exceeding alternative layer 1s in real economic usage.

As of March 2026, Ethereum hosted **$159 billion**[52] **in stablecoin value,** whereas Solana hosted about $15 billion,[53] and BNB Smart

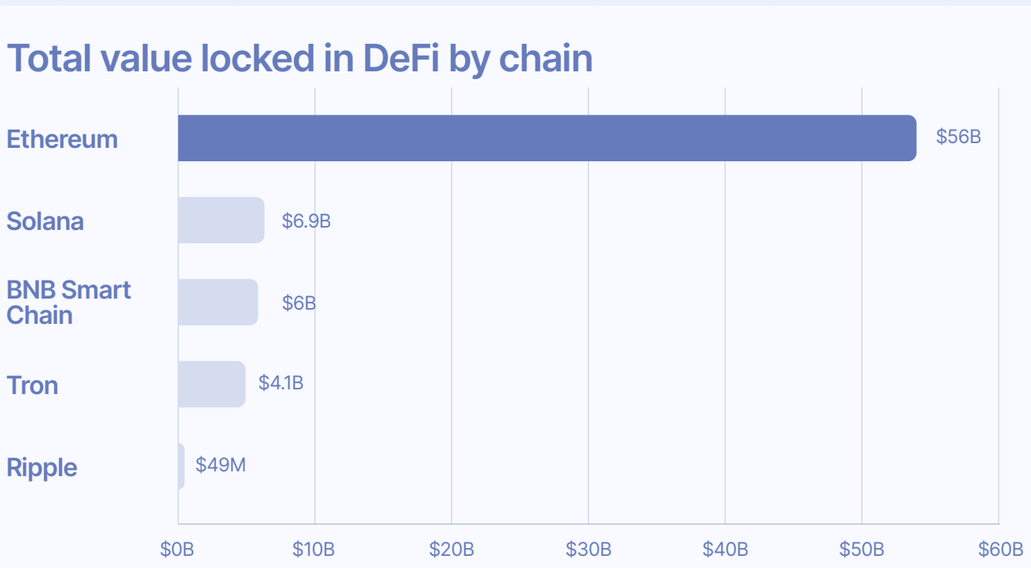
Chain hosted about $14 billion[54] . Ethereum also hosted over **$15.2 billion**[55] in tokenized real-world assets, **3X more than the combined** value hosted on BNB Smart Chain ($3 billion[56]) and Solana ($2.1 billion[57]).

Ethereum has over **$56 billion**[58] in total value locked in DeFi. Contrast this with Solana ($6.9 billion[59]), BNB Smart Chain ($6 billion[60]), TRON ($4.11 billion[61]), and Ripple ($49 million[62]).

Total value locked in DeFi on Ethereum vs. other chains

Ethereum is	Ethereum is	Ethereum is	Ethereum is
8.1 X	9.3 X	13 X	1,142 X
Larger than Solana	Larger than BNB Smart Chain	Larger than Tron	Larger than Ripple

Total value locked in DeFi on Ethereum vs. other chains



Sustainability aligned with public sector mandates

Following its transition to proof-of-stake in 2022, Ethereum reduced its electricity consumption by 99.98[63] percent and its carbon footprint was decreased by approximately 99.99[64] percent, addressing environmental concerns that continue to affect proof-of-work networks. This shift has materially changed how Ethereum is assessed by public institutions evaluating environmental impact alongside financial innovation.

How does Ethereum compare with permissioned blockchains?

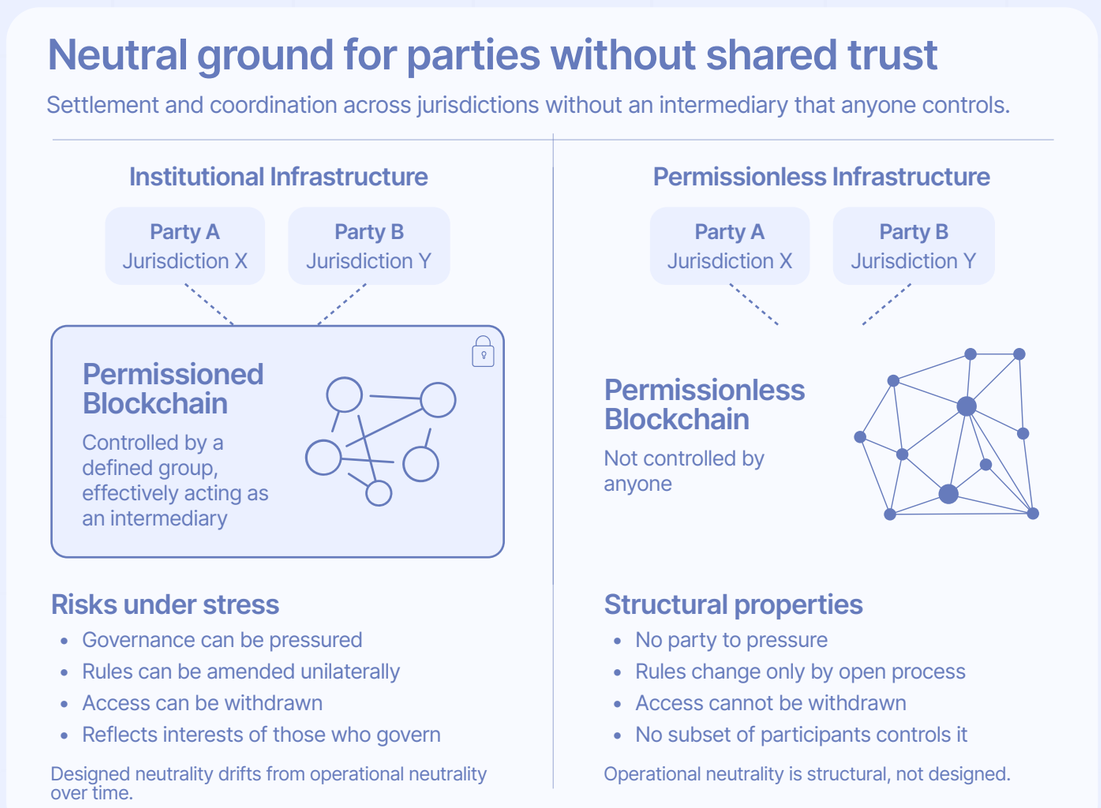
17

The primary argument for permissionless public blockchain infrastructure like Ethereum is the novel functionality it offers as compared to legacy alternatives. They are the **only solution to enable multiple parties to transact without relying on a system that one of them, or a third party, controls**.

Cross-border trade and settlement have always required some form of shared infrastructure. Historically, that infrastructure has been provided by institutions: correspondent banks, clearing houses, messaging networks, custodians, etc. These systems work when participants share a common legal framework, broadly trust the institutions involved, and operate within a stable set of relationships, agreeing upon certain standards. However, they become unreliable when those conditions do not hold.

Global trade entered 2026 under mounting pressure from shifting supply chains, tighter national regulations, and a more complex and fragmented international environment. Parties that previously relied on shared institutions for settlement are increasingly asking whether those institutions can serve as genuinely neutral ground for all participants.

In recent times, it has become abundantly clear that **any system with a defined governance structure will reflect, to some degree, the interests and constraints of those who govern it**. This is an inherent property of controlled infrastructure, and it is a genuine concern.



A counterparty's willingness to rely on shared settlement infrastructure depends on its confidence that the rules of that infrastructure will apply consistently, that access will not be withdrawn for reasons unrelated to the transaction itself, and that no participant in the governance structure can unilaterally alter the terms on which others operate.

These requirements are difficult to satisfy through institutional design alone. The history of institutional infrastructure shows that the gap between designed neutrality and operational neutrality tends to widen as the stakes rise and the range of participants grows. Risks that **governance bodies can be pressured, rules can be amended, and access can be unilaterally denied are not theoretical in nature anymore.** This is the problem that permissionless public blockchain infrastructure is structurally

designed to solve. Ethereum does not have a governance body that can be pressured, its rules change only through a decentralized process in which no single participant holds decisive control, and access cannot be withdrawn by any operator because there is no operator. The result is a settlement and coordination layer that can serve parties who share no prior relationship, operate under different legal frameworks, and have no basis for extending institutional trust to one another or to a common intermediary.

By contrast, permissioned and consortium blockchains offer control and restricted access, but they do so by sacrificing properties that are critical for competitiveness, including neutral governance, cross-network interoperability, and continuity of operations across participants and jurisdictions over time. **There are no examples of permissioned blockchains that have achieved anywhere near the success of public alternatives.**

For government and institutional audiences, this matters. **Where shared infrastructure is needed across a diverse or distributed set of participants, the durability and credibility of that infrastructure depends on the degree to which its operation is insulated from the interests of any subset of those participants. Ethereum offers that insulation more completely than any permissioned alternative.** This mirrors the architecture of the public internet, on which banks, regulators, and sovereigns operate while relying on a shared, ownerless substrate that no single actor controls.

Permissioned blockchains do not constitute neutral infrastructure

Permissioned blockchains operate as permissioned systems, where governance, validation, and rule changes are controlled by a limited set of participants. This structure resembles an intranet.

Permissioned blockchains do not resolve the coordination problem discussed above. They replicate it by concentrating governance in a defined set of participants, every permissioned system creates a new class of gatekeeper, and a new class of parties who are excluded from, or dependent on, that gatekeeper's goodwill.

Canton, for example, is one of the most widely discussed permissioned platforms to date, backed by some large institutions. Its stated goal[65] is to create a 'network of networks', allowing previously siloed systems in financial markets to interoperate with the appropriate governance, privacy, permissioning, and controls required for highly regulated industries.

Despite this goal, **Canton is not decentralized or neutral. A small group of stakeholders control access and set its rules.** The Canton Foundation is co-chaired[66] by the Depository Trust & Clearing Corporation (DTCC) and Euroclear. Protocol changes[67] require voting with a 2/3 Super Validator majority. Joining the network as a validator currently requires sponsorship[68]. This is **consortium governance, not decentralized governance**. If those entities are pressured, they can change the network's rules.

In the same vein, **Tempo**, incubated by Stripe and Paradigm, has the stated purpose[69] of enabling high-throughput, low-cost global transactions for any use case, including machine payments. However, the management of the active validator set on Tempo is currently permissioned by the Tempo team[70]. This effectively means that at least for now, **a party transacting on Tempo is trusting Stripe and Paradigm, not cryptographic guarantees**.

Similarly, another popular permissioned chain, **Google Cloud Universal Ledger (GCUL)** was launched with the stated[71] objective of creating innovative payments services and financial markets products. It aims[72] to simplify the management of commercial bank money accounts and facilitates transfers via a

distributed ledger, empowering financial institutions and intermediaries to meet the demands of their most discerning clients and compete effectively. GCUL too operates as a permissioned system[73], leveraging Google's technology. **Adoption of GCUL means, in practice, that a single commercial entity controls the foundational infrastructure underpinning financial settlement**, which poses an existential governance risk, similar to the current state of play.

Ethereum, on the other hand, functions more like the public internet: no single operator controls access, rule-setting, or participation. It can be used as the foundational trust layer that further projects can build on top of. These projects can then inherit Ethereum's decentralization, reduce their security costs, and enhance performance interoperability, while building their own custom environments.

Permissioned blockchains require trust in the consortium

In permissioned ledgers, users ultimately need to trust the consortium operator to maintain records honestly, resolve disputes, and enforce rules. **Ethereum replaces institutional trust with cryptographic verification and decentralized consensus, reducing reliance on intermediaries and lowering single points of failure**. Ethereum's credible neutrality and open access for auditing is particularly relevant for cross-border use cases, where authority, supervision, or enforcement is distributed across jurisdictions.

Canton takes a delegated trust approach. The network relies on trusted synchronization domain operators to sequence and confirm transactions. However, the whitepaper acknowledges[74] that where highly trusted operators exist, the sync domain can be implemented in a centralized way. Participants in the network are effectively trusting that the consortium of Super Validators will act honestly. This is institutional trust, not the cryptographic trust minimization that defines Ethereum's security model.

Tempo compounds this problem. As noted previously, the management of the active validator set on Tempo is currently permissioned by the Tempo team[75], which retains significant control. Participants hence trust them to act in good faith.

GCUL suffers from the same issue of institutional trust. Users must rely on Google Cloud to operate effectively, efficiently and in a fair manner.

These permissioned blockchains risk rebuilding the old system with new players in charge and elevating tech giants to an even greater position of dominance.[76]

Permissioned blockchains do not support material interoperability and composability

Interoperability is no longer treated as a technical convenience. Across use cases including finance and identity, the ability of allied institutions to coordinate without bespoke integration has become a first-order strategic concern. For shared infrastructure to be useful at scale, it must allow parties operating under different legal frameworks and without prior trust to transact on common terms. **Ethereum enables applications to interoperate by default.**

Permissioned blockchains require institutional trust

What each system asks participants to take on faith.

Assets, identities, and contracts issued on Ethereum can be used across wallets, platforms, and jurisdictions without bespoke integrations. Permissioned blockchains tend to become isolated systems that require bilateral agreements and custom bridges to interact with external networks, increasing operational complexity and fragmentation.

Canton's stated value proposition is enabling transactions across sovereign, independently governed subnetworks. However, **applications interoperate within the bounds set by their respective permissioned models**. An institution can thus, in practice, restrict who accesses or composes with their application.

Tempo operates similarly. In addition to the mainnet infrastructure, the company also released[77] its Machine Payments Protocol (MPP), an open standard for agentic payments. MPP claims to be payment-agnostic and is said to work with stablecoins, cards, Affirm, Klarna, and other payment methods. However, this interoperability is at least partially through leveraging partnerships[78] with private companies.

In essence, the interoperability and composability offered by the network is because these corporations got together and agreed on standards, which is fairly similar to the status quo. This further underscores the system's reliance on parties agreeing to work together and trust one another, as opposed to everyone operating on neutral infrastructure.

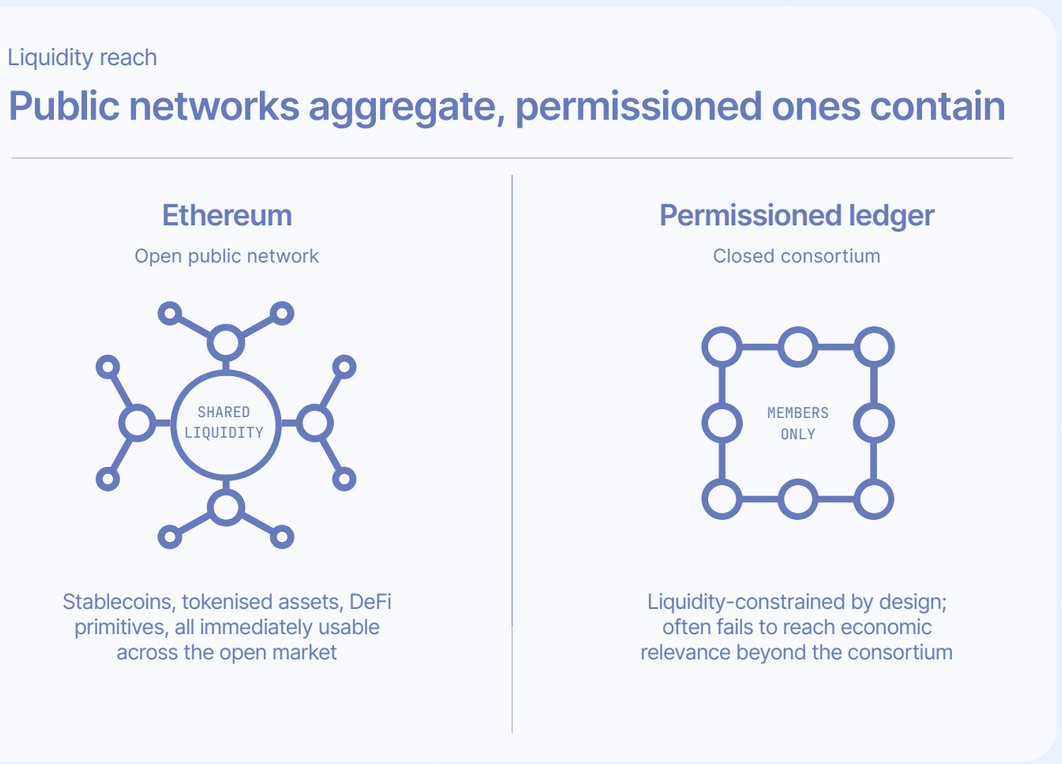
Notably, buy-in from a defined set of large institutions also implies the exclusion of those outside it: any payment network, financial institution, or market participant that has not been invited into the partnership structure must seek permission to participate, **replicating the very gatekeeping dynamic that permissionless infrastructure is designed to eliminate.**

The same critique holds true for **GCUL**. Its deep integration with Google's analytics and AI stack is a feature for Google Cloud customers, but it also means that **composability outside that environment depends on Google-controlled interfaces.** Institutions building on GCUL are composing within a walled garden, not within the open, global ecosystem that Ethereum provides.

Unlike Ethereum's open ecosystem, where seamless composability is central to its success, permissioned chains offer a highly restricted form of composability, if any at all.

Permissioned blockchains limit access to global liquidity

Public blockchains aggregate global liquidity. **Stablecoins, tokenized securities, and financial primitives on Ethereum are immediately usable across a broad market of participants**. Permissioned ledgers remain liquidity-constrained by design. Even when technically functional, they often fail to achieve economic relevance beyond the initiating consortium.



Canton enables cross domain transactions, but **liquidity is concentrated among a set of known, vetted counterparties** within a permissioned ecosystem. Liquidity hence tends to be fragmented rather than compound across separate deployments given the ecosystem isolation.

Tempo's liquidity is similarly constrained by its curated partner base. A stablecoin issued on Tempo is not immediately usable across the full global ecosystem of wallets, DeFi protocols, and institutional platforms the way an Ethereum-native asset is. As a permissioned ledger, **GCUL** is also likely to face the same issues.

Institutional and public sector readiness

Taken together, neutrality, trust minimization, interoperability, and access to global participation are widely recognized as critical characteristics of systems designed to function as shared infrastructure across institutions and jurisdictions over long time horizons. These characteristics distinguish open, durable infrastructure from closed or bespoke systems that rely on continuous coordination among trusted parties.

In practice, institutional and public-sector adoption patterns reflect these architectural considerations. **Governments and regulated institutions have increasingly selected Ethereum-based architectures in contexts where durability, auditability, and cross-institutional coordination are required.** Rather than replacing existing legal or operational frameworks, Ethereum is typically used as a neutral settlement or coordination layer, with policy, compliance, and access controls applied at higher layers. These deployments illustrate how infrastructure-level properties translate into real-world institutional use, which is examined in more detail below.

Canton, Tempo, and GCUL may be well-suited to connect institutions that already share legal frameworks and agreed standards. This by definition excludes the vast majority of the world's economic participants. Ethereum, by contrast, operates as a shared, ownerless space, where parties who share no prior trust, institutional membership, or agreed standards can transact on equal terms.

This matters acutely today, in a world of accelerating geopolitical fragmentation. **Neutral digital infrastructure that cannot be controlled by a centralized gatekeeper or consortium is no longer a theoretical concept, it is an urgent necessity**

Permissionless infrastructure like Ethereum provides a foundation for cross-border coordination that does not depend on pre-existing legal agreements or shared institutional membership, expanding access to participants who would otherwise be excluded from closed systems.

Technological portability and exit costs

Public blockchain infrastructure is built on open technical standards, which reduces the cost and complexity of migrating applications or assets across compatible environments. This lowers long-term exit costs and supports procurement flexibility.

By contrast, systems built on proprietary stacks, such as **Canton, Tempo, and GCUL,** or non-interoperable standards can require significant redevelopment effort to migrate, creating structural barriers to exit over time. For instance, **Canton** requires Daml — Digital Asset's smart contract language. The use of a unique language that does not run on public EVM chains, materially restricts portability and increases exit costs. Migration away from Canton would require a full rewrite, not a port, creating switching costs at every level, including tooling, talent, and institutional knowledge.

Economic and Financial System Implications

How should a central bank evaluate stablecoin issuance and settlement on Ethereum vs alternative networks?

18

When evaluating stablecoin issuance and settlement infrastructure, discussions commonly surface questions on monetary stability, legal settlement finality, systemic resilience, and cross-border interoperability. These considerations reflect long-standing central bank concerns around private money, payment system design, and financial infrastructure governance.

A structured evaluation across these dimensions **points strongly toward Ethereum as the most appropriate settlement layer** for systemically relevant stablecoins today.

Market adoption and revealed issuer preference

The liquidity on Ethereum is substantially higher when compared to other layer 1s, demonstrating market preference.

As of March 2026, **Ethereum hosted over $159 billion**[1] in stablecoin value. By contrast, Tron, Solana, and BNB Smart Chain host $89.1 billion[2], $15 billion[3], and $14 billion[4], respectively. **Ethereum also hosts over $15.2 billion**[5] **in tokenized real-world assets**, whereas Solana and BNB Smart Chain host $2.1 billion[6] and $3 billion[7] respectively.

Further, **Ethereum hosts over $56 billion**[8] in total value locked in DeFi, compared to Solana, with $6.9 billion[9], BNB Smart Chain with $6 billion[10], TRON with $4.1 billion[11], and Ripple with $49 million[12].

For a central bank, this **distribution is not merely a market statistic**. It reflects the collective risk assessment of issuers operating under regulatory, legal, and reputational constraints. **Ethereum is the most battle-tested, liquid, and neutral settlement layer for institutional digital asset operations** with over 10.5 years of uninterrupted uptime, $76 billion+ in staked ETH, and the leading market share in tokenized assets.

Large stablecoin issuers and users have selected Ethereum because it offers the deepest liquidity, the most robust security, the highest confidence in operational stability, the most robust tooling, a large developer base, programmability, neutrality minimizing counterparty risk, and the most end users. In other words, issuers that are already subject to supervisory scrutiny have effectively conducted cross-platform due diligence and converged on Ethereum where it best satisfies their operational, legal, and reputational constraints at scale.

Settlement Layer Design

Ethereum's settlement layer is secured by the largest pool of economically staked capital of any smart-contract platform, with over

$76 billion staked[13] as of March 2026. The chain's validator pool is also diversified, owing in part to the relatively low technical and financial barriers to entry. As a result, nodes participate from all over the world.[14] **The network also does not rely solely on cloud providers, and enables running nodes on local hardware, ensuring that there is no dependency on a single service provider**.[15]

Client diversity[16] is also a key feature of the network as there are several production-level Ethereum clients, each one developed and maintained in different languages by separate teams. These design features reduce reliance on any single party, enhancing resilience in crisis scenarios, and limiting the scope for unilateral intervention or disruption. The network's resilience is further demonstrated by the fact that it has been running uninterrupted for over 10 years, since its genesis in 2015.

From a central bank and systemic risk perspective, distributed validation functions as a mechanism to mitigate operational risk at the settlement layer. Infrastructure that depends on a narrow set of validators, operators, or legal regimes may perform efficiently under normal conditions, but can introduce governance and intervention vulnerabilities during periods of market stress or geopolitical tension.

There have been several recent examples where tech outages stemming from major service providers such as AWS, Crowdstrike, Cloudflare, Microsoft Azure, etc. have affected critical infrastructure. By contrast, Ethereum's structure diffuses operational and political dependencies, supporting continuity of settlement even under adverse conditions.

Ethereum's architecture further mitigates operational risk by separating settlement verification from operational and access control. The base layer is neutral, transparent, and auditable, while higher layers and applications can implement access restrictions, compliance requirements, and jurisdiction-specific controls without centralizing settlement authority in a single entity. Central banks evaluate settlement finality as a legal and economic concept, not merely a technical attribute. Ethereum provides economic finality under its proof-of-stake consensus mechanism. As of March 2026, the network was economically secured by about $76 billion[17] in staked ETH. Controlling the two-thirds majority required to finalize a fraudulent transaction[18] would require commanding upwards of $50.7 billion[19] in ETH. To finalize a block, at least two-thirds of the total active staked ETH must attest to it during a two "epoch" (approximately 13-minute) period.

If two conflicting finalized histories were created, this would mean an attempt to propagate something different from the canonical block. For this to occur, at least one-third of total stake would have had to sign both versions. Signing both versions would constitute **punishable behavior and the offending validators would be automatically penalized.** They would **lose their staked ETH through a process called slashing (and would be forcibly ejected from the validator set)**. Because penalties scale with the number of validators involved, large-scale coordinated attacks would result in substantial losses, making such behavior economically self-destructive. This all means that there are material economic disincentives and a coordinated attack or other dishonest behavior would be very costly for the attacker. **Economic finality on Ethereum is thus analogous to existing payment systems**, where reversibility is theoretically possible but practically excluded due to governance, cost, and reputational constraints.

Interoperability and composability

Stablecoins are most effective when they function as **general-purpose settlement assets, not siloed instruments**.

Ethereum hosts the largest and most mature blockchain ecosystem. ERC-20/Ethereum

assets are the most commonly supported token standards, which makes integration easier across these platforms and service providers, but they are still subject to whitelisting, configuration, and compliance enablement on a case-by-case basis.

The same applies to other ERC-based token standards. **Native composability throughout Ethereum-based finance increases utility while reducing payment rail fragmentation.** Notably, these standards can be implemented by any developer, custodian, or institution without permission or license fee. **Building on Ethereum therefore means building on standards that thousands of institutions already use**, rather than negotiating bespoke connections with every counterparty from scratch.

- **Wallets:** MetaMask alone has 143 million[20] total accounts created and approximately 30 million[21] monthly active users, with nearly every DeFi, NFT, or DAO project integrating with it by default. Institutional-grade smart contract wallets such as Safe secure over $100 billion[22] in assets across corporate treasuries and funds, while hardware providers Ledger and Trezor both natively support Ethereum and ERC-20 tokens as a baseline standard.

- **Custodians:** Providers like Coinbase Custody, BitGo, Fidelity Digital Assets, and Copper all offer regulated, insured Ethereum custody built around the same address format and token standards. An asset issued as an ERC-20 token slots immediately into all of them; conversely, an asset issued on a newer or proprietary chain requires a bespoke integration at each provider, if one is available at all.

- **Auditors and Security Infrastructure:** OpenZeppelin's open-source contract library which is the industry-standard collection of audited, reusable smart contract components, underpins the majority of token deployments on Ethereum. Further, specialist audit firms including Trail of Bits, Consensys Diligence, and Certik have collectively reviewed thousands of Ethereum contracts, developing tooling and institutional knowledge specific to the EVM.

  This depth of security infrastructure, built over a decade, materially de-risks any new deployment on Ethereum relative to alternatives.

Permissioned or consortium ledgers may offer greater local control but limit interoperability and increase concentration risk, potentially recreating fragmented settlement systems rather than a unified digital monetary layer. For stablecoins, especially in cross-border trade amid geopolitical uncertainty, networks that can be unilaterally restricted undermine this functionality. Ethereum's neutrality, open standards, security, and decentralization instead provide shared infrastructure with minimal protocol-level gatekeeping, analogous to the role of the internet in the digital economy.

Is Ethereum interoperable with the existing infrastructure of financial institutions?

19

Ethereum's design embodies a clean "separation of concerns" that mirrors established financial market infrastructure: a neutral, public settlement layer provides immutable finality and verifiability, while compliance, access control, data privacy, and eligibility checks are enforced at higher (application, intermediary, or layer 2) layers.

Ethereum is increasingly interoperable with traditional financial infrastructure through institutional connectivity layers, such as regulated intermediaries, custody solutions, and compliance-aligned integration platforms. Institutions retain compliance, operational control, and data protection while accessing Ethereum's settlement, liquidity, and programmability.

Real World Asset (RWA) tokenization: Bridging traditional finance and Ethereum

Financial institutions already connect existing balance sheets and securities infrastructure to Ethereum through tokenization, the process of representing real-world assets such as bonds, funds, deposits, or collateral as digital assets on Ethereum.

Tokenization enables real-world assets to be:

- Settled with near-real-time finality.
- Transferred across borders without correspondent banking friction, and at lower cost.
- Programmed with embedded rules for lifecycle events, compliance, and cash flows.

Rather than replacing existing systems, Ethereum functions as a **shared settlement and coordination layer** that sits alongside (and can enhance) traditional record-keeping and custody frameworks.

Layered integration models for regulated institutions

Regulated institutions sometimes engage with Ethereum through **modular integration models** that enable compliance, disclosure, and operational controls to be applied at the appropriate layer, while anchoring settlement to Ethereum's public base layer.

These models include layer 2 networks, permissioned execution environments, and hybrid architectures that connect to Ethereum without fragmenting settlement or liquidity, while also:

- Enforcing rules at the application or access layer.
- Providing built-in privacy while still enabling compliance and auditability.
- Limiting data visibility while still anchoring transactions to a public, auditable settlement layer.
- Achieving scalability and cost efficiency without fragmenting liquidity.

Ethereum's design explicitly supports this separation between open settlement and controlled participation, which aligns with how regulated finance already operates.

Interoperability through service providers and financial market infrastructure

A growing ecosystem of custodians, banks, middleware providers, and market infrastructure firms bridge Ethereum with existing core banking, treasury, and post-trade systems. These intermediaries abstract private key management, reporting, and reconciliation while allowing institutions to interact with Ethereum-based assets and protocols.

From an institutional perspective, Ethereum integration increasingly resembles:

- A new settlement rail rather than a retail crypto system
- An extension of existing infrastructure rather than a wholesale replacement

This resemblance mirrors how the internet integrated with financial services through APIs, messaging layers, and standardized protocols rather than direct exposure to underlying networks.

Strategic implication for institutions and regulators

Institutions generally do not integrate with Ethereum to mimic legacy systems, but to reduce concentration risk in cross-border settlement, liquidity movement, and coordination, particularly under conditions of geopolitical stress.

Ethereum can be understood as **neutral settlement infrastructure**, analogous to how the internet functions as neutral communications infrastructure. Just as the internet did not replace banks, governments, or regulated service providers but instead provided a shared, non-sovereign layer for information exchange, Ethereum provides a shared, open layer for value settlement and coordination.

In this framing, Ethereum does not displace sovereign money, regulated intermediaries, or supervisory authority. Rather, it enables institutions and regulators to rely on a **common, public settlement layer** that reduces dependence on any single operator, jurisdiction, or proprietary network, while enabling policy, compliance, and risk controls to remain anchored at the institutional and application layers.

What is DeFi and how is it different from centralized equivalents?

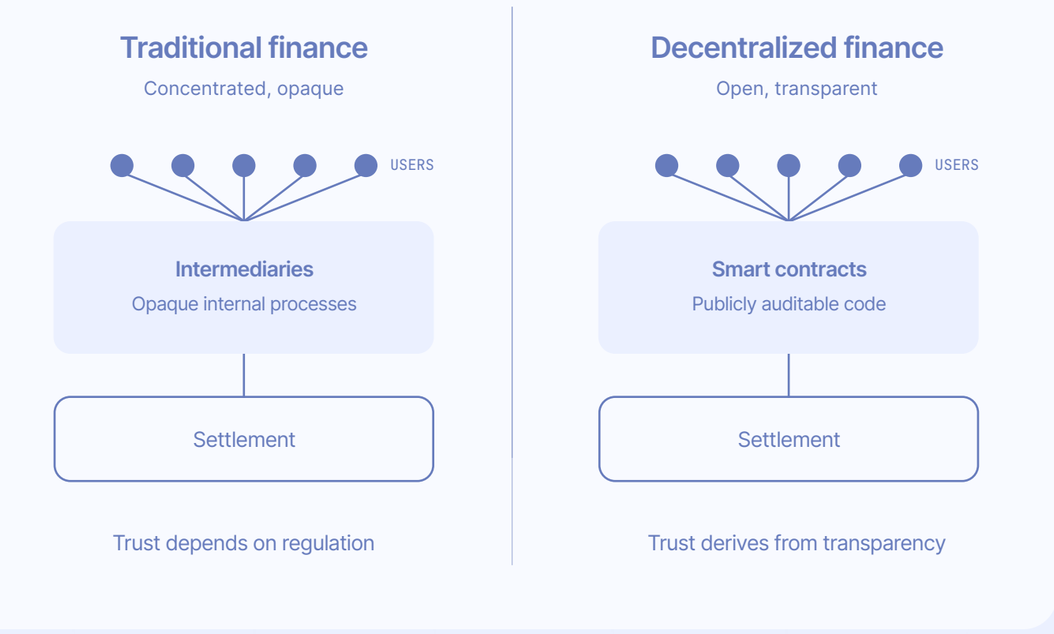
20

Traditional finance relies on institutions to guarantee transactions, concentrating power over money flows in a small set of intermediaries. Because transactions, risk exposure, and internal processes are largely opaque, trust depends on regulation, consumer protections, and legacy security frameworks rather than transparency. This concentration creates systemic fragility: failures at single institutions can cascade through the financial system, as seen in events such as the Lehman Brothers fraud (2008) and the collapse of FTX (2022). Centralized gatekeeping also leaves large segments of the global population excluded from basic financial services.

Decentralized Finance (DeFi) replaces intermediaries with smart contracts: self-executing programs deployed on blockchains. These contracts run as written and are publicly accessible, allowing anyone to inspect, audit, and verify them.

As a result, DeFi markets operate continuously without centralized authorities that can block payments or restrict participation. **Users retain direct control over their assets and can access global financial services with only an internet connection.** Processes that were previously slow, opaque, and prone to human error become automated and transparent through open, verifiable code. One example of a DeFi protocol putting these principles into practice is Morpho, a decentralized lending and borrowing platform built on Ethereum.

Two structures for financial coordination



Morpho is designed around a philosophy of modularity and simplicity. It leverages a minimal, immutable smart contract that provides the foundational layer for lending markets. Instead of bundling risk management, collateral decisions, and interest rate logic into a single opaque system, Morpho separates these concerns. This allows users to permissionlessly create an isolated lending market for any asset, with any collateral and risk parameters they choose. This architectural approach dramatically reduces the attack surface of the core protocol while giving sophisticated participants the flexibility to build on top of it.

The scale at which Morpho operates demonstrates the growing appetite for this kind of open financial infrastructure. As of March 15, 2026, the protocol stood at over $7.3 billion[23] in total value locked.

What are some compelling examples of how institutions and governments use Ethereum?

21

Ethereum is already used by major financial institutions and public-sector actors as settlement and coordination infrastructure, particularly where cross-border and cross-entity interoperability, neutrality, and programmability are required. Adoption has concentrated around several identifiable categories.

Ethereum hosts over $15.2 billion[24] in tokenized real-world assets (March 2026)

Several globally significant institutions have issued or settled tokenized assets on Ethereum or Ethereum-anchored networks.

Institutional Ecosystem

LEADING GLOBAL FINANCIAL INSTITUTIONS ACTIVELY BUILDING, DEPLOYING, AND TRANSACTING ON ETHEREUM

Asset Managers	BlackRock	Fidelity Investments	VanEck	WisdomTree	Franklin Templeton
Banks & Capital Markets	J.P.Morgan	Morgan Stanley	UBS	standard chartered	Societe Generale
Infrastructure & Payments	Mastercard	VISA	Swift	DTCC	PayPal
Platforms & Exchanges	coinbase	Robinhood	eToro	SECURITIZE	CIRCLE
Technology & Consulting	EY Shape the future with confidence	SONY	ANT GROUP	consensys	aave

LOGOS REPRESENT INSTITUTIONS WITH ETHEREUM-BASED DEPLOYMENTS, PILOTS, OR INTEGRATIONS AS OF Q1 2026. NOT EXHAUSTIVE.

- **Franklin Templeton**[25] operates tokenized money market funds where share ownership is recorded on Ethereum, integrating blockchain settlement with regulated fund administration.

- **BlackRock**[26] launched the BUIDL tokenized fund on Ethereum, explicitly citing liquidity, interoperability, and institutional infrastructure readiness.

- **JPMorgan**[27] launched its first ever on-chain money market fund on Ethereum, which currently holds over $100 million in assets under management.

- **Amundi**[28] **,** Europe's largest asset manager, launched a tokenized share class of its euro money market fund on Ethereum mainnet.

- The **Commodity Futures Trading Commission (CFTC)**[29] also announced the launch of a digital assets pilot program for certain digital assets, including ETH to be used as collateral in derivatives markets.

In these cases, **Ethereum is not mimicking legacy capital markets infrastructure. It functions as a shared settlement and record-keeping layer that multiple intermediaries can rely on simultaneously**.

Stablecoins on Ethereum as global payment infrastructure

As of March 2026, Ethereum hosted over **$159 billion**[30] in stablecoin value, which is **over 10X more than** Solana ($15 billion[31]) and BNB Smart Chain ($14 billion[32]).

- **Circle**[33] issues USDC on Ethereum, which is used by financial institutions, payment providers, and governments for treasury operations and cross-border transfers.

- **Fidelity**[34] launched its stablecoin on Ethereum.

- **Société Générale-Forge**[35], a major European bank to support a stablecoin, launched its stablecoin CoinVertible on Ethereum.

- **Visa**[36] started supporting settlement through stablecoin transactions for issuers and acquirers on Ethereum.

- **PayPal**[37] issues its stablecoin on Ethereum.

Banks using Ethereum alongside internal and permissioned systems

Large banks increasingly use Ethereum as an external settlement anchor while operating proprietary or permissioned ledgers internally. This hybrid architecture uses Ethereum as a neutral reference layer, reducing the need for bilateral infrastructure coordination and reconciliation.

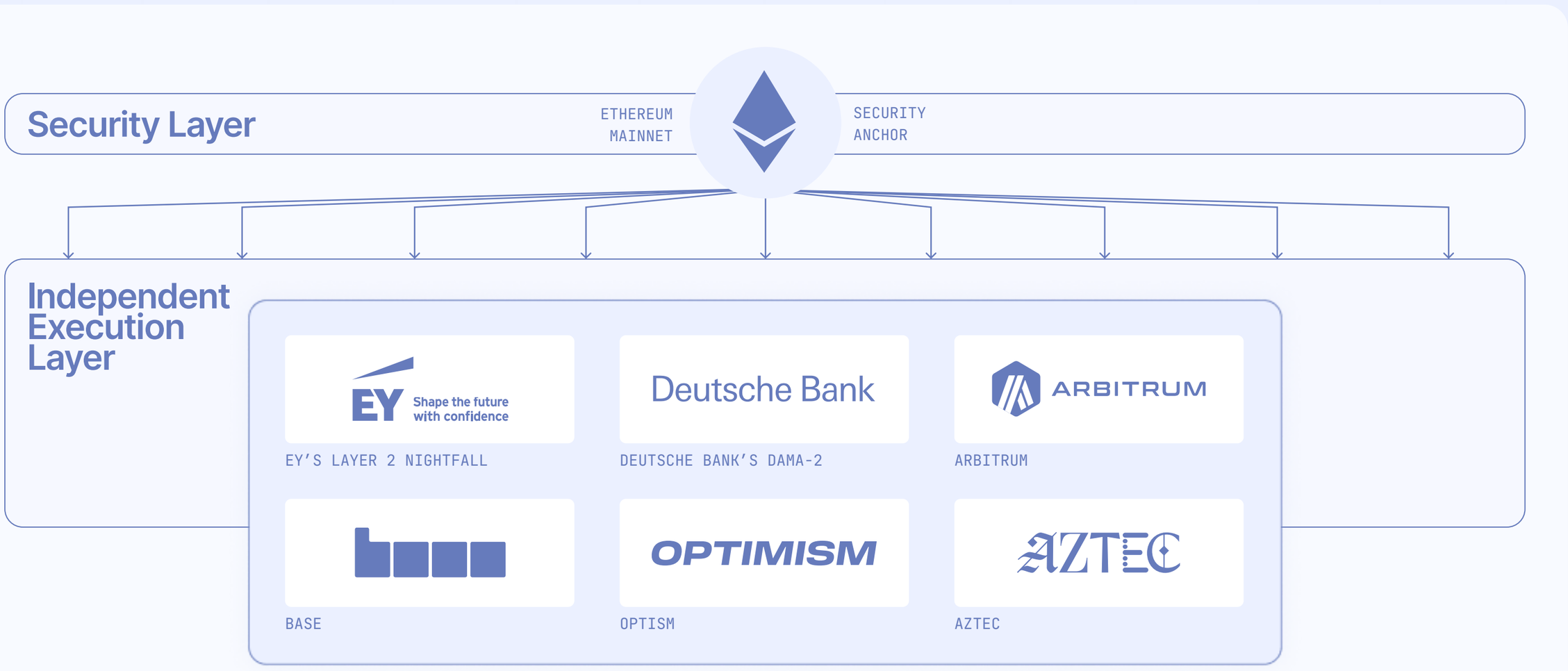
- **JPMorgan Chase**[38], through its Kinexys platform, has explicitly explored interoperability between internal tokenized systems and public blockchains, including Ethereum.

- **BNY Mellon**[39] **,** provides digital asset custody services that support Ethereum-native assets, enabling institutional clients to hold and settle Ethereum-based instruments within regulated frameworks.

Layer 2 networks used by institutions

Layer 2s are secondary protocols built on top of Ethereum. They are ideal for implementing unique value propositions and differentiated functionalities by offering custom execution environments, integrated data layers, or specialized application design. Several major institutions have built specialized layer 2 networks on Ethereum including EY's layer40 2[40] Nightfall and Deutsche Bank's DAMA-2 [41].

Some other proven layer 2 networks that exist in the Ethereum ecosystem include Arbitrum, Aztec, ZKsync, Optimism, Base, Ink, Scroll, Unichain, and Linea.



Key Benefits

Custom execution: Unique computing environments

Integrated data layers: Built-in data infrastructure

Specialized app design: Tailored for specific use cases

Public-sector and government-aligned use cases

Governments engage with the Ethereum ecosystem through project-based initiatives that include using Ethereum as digital public infrastructure, sometimes via regulated intermediaries and service providers.

These projects are designed so that sensitive data remains off-chain, while Ethereum provides verifiable settlement or audit references. Some examples include:

- **India (Land Records)**[42]**:** The Indian government has utilized Ethereum-based rails for managing land records and caste certificates, combating fraud and ensuring the immutability of public records.

- **Bhutan's National Digital Identity**[43]**:** Bhutan has anchored its National Digital Identity (NDI) system on Ethereum. This allows for a decentralized identity model where citizens control their credentials without relying on a central database that could be breached.

- **Buenos Aires' Digital Identity**[44]**:** The Government of the City of Buenos Aires launched a decentralized digital identity system designed to reshape how citizens manage and access their personal information. It enables users to own their identity and choose the data they want to share.

- **European Investment Bank – Digital Bond Issuance**[45]**:** The European Investment Bank has issued multiple digital bonds using Ethereum as a settlement and record-keeping layer. These issuances were conducted with traditional legal documentation and regulated intermediaries, with Ethereum used to coordinate issuance and settlement rather than to replace existing capital-markets law.

- **UNICEF CryptoFund**[46]**:** UNICEF's CryptoFund accepts, holds, and disburses funds using Ethereum and Ethereum-based assets. The program is designed to improve transparency and auditability of grant funding while keeping beneficiary data off-chain.

Environmental and Societal Considerations

How much energy does Ethereum consume?

22

Following Ethereum's transition to a Proof-of-Stake (PoS) consensus mechanism in September 2022 (known as "The Merge"), the network's **electricity consumption reduced by 99.98 percent**[1] and its **carbon footprint was decreased by approximately 99.99 percent**[2]**.**

Current Energy Profile

Ethereum's global network is estimated to consume approximately **0.0026 terawatt-hours (TWh) per year** (around 2,600 megawatt-hours)[3]

- **Annual electricity consumption:** ~2,601 MWh[4]
- **Estimated carbon footprint:** ~870 tonnes[5] of CO_2e annually

Impact of the Transition ("The Merge")

Prior to The Merge, Ethereum operated under a Proof-of-Work (PoW) model and consumed approximately **21 TWh per year**[6]**.** As noted previously, the transition to PoS reduced annualized electricity consumption by **more than 99.98 percent.** This shift reflects a structural change in how the network is secured: from computational energy expenditure to **economic security via staked capital (ETH).**

This comparative scale contextualizes Ethereum's current energy footprint:

- **Global data centers:** ~190 TWh (≈73,000× higher)[7]
- **Bitcoin network:** ~149 TWh (≈53,000× higher)[8]
- **Google:** ~19 TWh (≈7,300× higher)[9]
- **Netflix:** ~0.457 TWh (≈176× higher)[10]
- **PayPal:** ~0.26 TWh (≈100× higher)[11]
- **Airbnb:** ~0.02 TWh (≈8× higher)[12]

These comparisons illustrate that Ethereum's energy consumption is **orders of magnitude lower than both traditional digital infrastructure and Proof-of-Work systems.**

How can Ethereum help with issues presented by AI?

23

As artificial intelligence systems advance, three foundational governance challanges have emerged. First, frontier AI infrastructure today **reflects the same concentration dynamic as the rest of the internet**. It is controlled by a small number of operators, each setting their own rules, and subject to the pressure in their home jurisdictions. Millions' access to these AI capabilities can thus be switched off overnight, with no prior warning. Second, institutions must **determine how to verify identity** in a world where AI agents can generate realistic media and act independently. Third, policymakers must consider **how to verify the authenticity and integrity of digital content and machine-generated outputs**. Ethereum can serve as a neutral verification layer that supports identity assurance, provenance tracking, and accountability across all three challenges.

- **Coordination Infrastructure for AI:** As AI agents take on increasingly complex tasks, they require infrastructure for discovery, payment, and trust that operates without a central gatekeeper. Today, an AI agent acting autonomously has no standardized way to identify itself, demonstrate its track record, pay for services, or have its outputs independently verified by parties that have no prior relationship with it. Ethereum addresses this gap through open standards that **any developer or institution can implement without permission or license fee.**

ERC-8004 provides AI agents with portable, censorship-resistant identifiers, a standard interface for reputation, and hooks for independent validation of outputs. x402 provides a payment standard for machine-to-machine commerce. Because both standards are anchored on Ethereum, they inherit its core properties. This means that no single operator controls them, access cannot be withdrawn, and the rules governing them can be verified and audited by anyone.

- **Identity Verification:** The proliferation of AI-generated content (deepfakes) and agents creates a need to distinguish between human and machine actors. Ethereum provides a robust substrate for anchoring digital identity and content provenance, leveraging open standards developed outside the blockchain ecosystem. The World Wide Web Consortium's Verifiable Credentials (VCs) and Decentralized Identifiers (DIDs) offer a framework for making and verifying identity claims. Ethereum's role is to serve as a public, censorship-resistant registry for these identifiers and the credentials they issue, as demonstrated by implementations like the did:ethr method.

For example, projects like the National Digital Identity in Bhutan are anchoring identity systems on Ethereum-based rails to provide secure, verifiable proof of identity.

- **Content Authenticity:** By cryptographically signing and timestamping content on an immutable ledger, creators can prove the origin and integrity of media. This creates a "truth layer" where the provenance of information can be audited, helping to combat misinformation and AI-generated forgery. Ethereum can anchor a cryptographic hash of digital content at a specific point in time. If the content is later altered, the hash will no longer match, making tampering detectable. This creates an auditable integrity record without storing the content itself on-chain.

- **Governance for AI Agents:** As AI agents begin to transact and perform economically meaningful tasks, they require a corresponding governance framework. ERC-800413 proposes a standardized framework for agent identity, reputation, and validation on Ethereum. The proposal introduces registries for globally unique agent identifiers, portable reputation signals, and independent validation of higher-risk outputs. By settling these registries on Ethereum, they inherit the network's credible neutrality and proof-of-stake economic security. Beyond these, Ethereum can be an important addition to the AI stack, with protocols that are built to enhance privacy and security in AI systems, for example by using ZKPs to help users keep their data or identity private, or using smart contract commitments to enforce compliance policies.

While AI operates as a powerful computational tool, Ethereum provides the **verification layer:** a neutral, tamper-proof substrate to register identities and certify the authenticity of digital assets and information in an AI-enabled digital economy.

What is post-quantum security, and how is Ethereum addressing it?

24

Post-quantum security refers to cryptographic systems designed to remain secure even if large-scale quantum computers become capable of breaking current public-key cryptography. Most modern digital systems, including public blockchains, online banking platforms, and secure internet communications, **rely on cryptographic schemes that could theoretically be weakened by sufficiently advanced quantum computers**. While such machines do not yet exist at the scale required to compromise widely used standards, the risk is recognized as a long-term infrastructure consideration.

Importantly, **quantum resilience is not unique to blockchain systems**. It is a **cross-sector digital infrastructure issue**. Where many institutions have deferred on the problem until it becomes urgent, the **Ethereum community takes the view that critical infrastructure should be hardened well before the threat materializes, not after.**

Despite its decentralization, Ethereum's open governance model allows for adaptability, enabling cryptographic primitives to evolve through the Ethereum Improvement Proposal (EIP) process. If quantum-resistant signature schemes become necessary, they can be introduced through coordinated protocol upgrades and adopted by network participants.

How does quantum computing pose a risk to blockchains?

The **potential quantum risk to blockchains concerns digital signature security**. If sufficiently advanced quantum computers become operational, they could undermine the elliptic curve cryptography currently used to authenticate user transactions and validator attestations.

Ethereum's mitigation approach is through future-proofing upgrades to the protocol[14] **and its post-quantum Ethereum initiative**.[15] By separating signature verification logic from settlement rules, the network can transition to quantum-resistant cryptographic standards in a phased manner as those standards mature.

At present, practical quantum systems capable of breaking contemporary elliptic curve cryptography at scale do not exist. The risk is therefore prospective, but the Ethereum community's willingness to plan and build for it now, rather than wait for a crisis, reflects its forward-looking commitment to long-term infrastructure resilience.

Endnotes

Executive Summary

1. OpenZeppelin, Technical Risk Assessment on Blockchain Networks, op. cit.
2. OpenZeppelin, Technical Risk Assessment on Blockchain Networks, OpenZeppelin, March 2026, openzeppelin.com.
3. *Ibid.*
4. *Ibid.*
5. *Ibid.*
6. *Ibid.*
7. *Ibid.*
8. *Ibid.*
9. *Ibid.*
10. *Ibid.*
11. *Ibid.*
12. *Ibid.*
13. RWA.xyz, 'Tokenized Real-World Assets by Network', app.rwa.xyz/networks, accessed June 2026..
14. *Ibid.*
15. *Ibid.*
16. Client Diversity', *Client Diversity, Ethereum*, https://clientdiversity.org, accessed June 2026.
17. Solana Foundation, Network Health Report (Solana Foundation, June 2025), https://solana.com/news/network-health-report-june-2025.
18. OpenZeppelin, Technical Risk Assessment on Blockchain Networks, op. cit.
19. Electric Capital, *Developer Report 2026* (Electric Capital, 2026), https://www.developerreport.com.
20. *Ibid.*
21. *Ibid.*
22. *Ibid.*
23. *Ibid.*
24. OpenZeppelin, Technical Risk Assessment on Blockchain Networks, op. cit.
25. *Ibid.*
26. *Ibid.*
27. *Ibid.*
28. *Ibid.*
29. Ethereum Foundation, 'Ethereum Energy Consumption', *Ethereum.org*, ethereum.org/energy-consumption, accessed June 2026.
30. *Ibid.*
31. *Ibid.*
32. *Ibid.*
33. Ethereum Foundation, 'Future-Proofing Ethereum', *Ethereum.org*, https://ethereum.org/roadmap/future-proofing, accessed June 2026.

System Overview and Foundational Concepts

1. Etherscan, 'Ethereum Node Tracker', Etherscan, https://etherscan.io/nodetracker, accessed June 2026.
2. OpenZeppelin, Technical Risk Assessment on Blockchain Networks, op. cit.
3. *Ibid.*
4. Ethereum Foundation, 'Proof-of-Stake Rewards and Penalties', Ethereum.org, https://ethereum.org/developers/docs/consensus-mechanisms/pos/rewards-and-penalties, accessed June 2026.
5. Ethereum Foundation, 'Ethereum Energy Consumption', Ethereum.org, ethereum.org/energy-consumption, accessed June 2026.
6. *Ibid.*
7. OpenZeppelin, Technical Risk Assessment on Blockchain Networks, op. Cit.
8. IBM, 'What Is Homomorphic Encryption?', IBM Topics, https://www.ibm.com/topics/homomorphic-encryption, accessed June 2026.

Governance, Control, and Responsibility

1. Ethereum Foundation, 'Ethereum Governance', Ethereum.org, https://ethereum.org/governance, accessed June 2026.
2. Ethereum Foundation, 'Ethereum Improvement Proposals (EIPs)', Ethereum.org, https://ethereum.org/eips, accessed June 2026.
3. *Ibid.*
4. Ethereum Foundation, Annual Report 2024, Ethereum Foundation, 2024, ethereum.foundation/report-2024.pdf.
5. Ethereum Foundation, 'The Merge', Ethereum.org, ethereum.org/roadmap/merge, accessed June 2026.
6. Ethereum Foundation, 'Ethereum Energy Consumption', Ethereum.org, ethereum.org/energy-consumption, accessed June 2026.
7. *Ibid.*
8. *Ibid.*
9. *Ibid.*
10. OpenZeppelin, Technical Risk Assessment on Blockchain Networks, op. Cit.
11. *Ibid.*
12. *Ibid.*
13. *Ibid.*
14. *Ibid.*
15. *Ibid.*
16. *Ibid.*
17. *Ibid.*
18. *Ibid.*
19. *Ibid.*
20. *Ibid.*
21. *Ibid.*
22. *Ibid.*
23. *Ibid.*
24. *Ibid.*
25. *Ibid.*
26. *Ibid.*
27. *Ibid.*
28. *Ibid.*
29. *Ibid.*
30. *Ibid.*
31. *Ibid.*
32. *Ibid.*
33. *Ibid.*
34. *Ibid.*
35. *Ibid.*
36. *Ibid.*
37. *Ibid.*
38. *Ibid.*
39. *Ibid.*
40. *Ibid.*
41. 'Client Diversity, Ethereum', Client Diversity, https://clientdiversity.org, accessed June 2026.
42. OpenZeppelin, Technical Risk Assessment on Blockchain Networks, op. Cit.
43. *Ibid.*
44. *Ibid.*
45. *Ibid.*
46. *Ibid.*

Comparative Analysis of Different Blockchains

1. Ethereum Foundation, 'Ethereum Energy Consumption', Ethereum.org, ethereum.org/energy-consumption, accessed June 2026.
2. *Ibid.*
3. OpenZeppelin, Technical Risk Assessment on Blockchain Networks, op. Cit.
4. *Ibid.*
5. *Ibid.*
6. *Ibid.*
7. *Ibid.*
8. *Ibid.*
9. Solana Status, 'Uptime History, Page 9', status.solana.com, accessed June 2026.
10. BNB Chain, 'BNB Chain: A Decentralised Response', BNB Chain Blog, bnbchain.org, accessed June 2026.
11. KuCoin News, 'XRP Ledger Suffers Hour-Long Network Halt Before Recovery', KuCoin, kucoin.com, accessed June 2026.

12. Probelab, 'Ethereum Topology, Countries Map', probelab.io, accessed June 2026.
13. OpenZeppelin, Technical Risk Assessment on Blockchain Networks, op. Cit.
14. Probelab, 'Ethereum Topology, Cloud Provider Distribution', probelab.io, accessed June 2026.
15. 'Client Diversity, Ethereum', Client Diversity, https://clientdiversity.org, accessed June 2026.
16. Solana Foundation, *Network Health Report* (Solana Foundation, June 2025), https://solana.com/news/network-health-report-june-2025.
17. OpenZeppelin, Technical Risk Assessment on Blockchain Networks, op. Cit.
18. *Ibid.*
19. *Ibid.*
20. *Ibid.*
21. *Ibid.*
22. *Ibid.*
23. *Ibid.*
24. *Ibid.*
25. *Ibid.*
26. *Ibid.*
27. *Ibid.*
28. Solana Foundation, 'Delegation Program', Solana.org, https://solana.org/delegation-program, accessed June 2026.
29. Panda Academy, 'BSC's 45 Validator Nodes Exposed: Who's Pulling the Strings?', Medium, 7 June 2025, https://pandaacademy.medium.com/bscs-45-validator-nodes-exposed-who-s-pulling-the-strings-143c3dc3c5c3, accessed June 2026.
30. Who Owns the Most XRP? Ripple Ownership Details', Capital.com, https://capital.com/en-int/analysis/ripple-who-owns-most-xrp, accessed June 2026.
31. OpenZeppelin, Technical Risk Assessment on Blockchain Networks, op. Cit.
32. Electric Capital, *Developer Report 2026* (Electric Capital, 2026), https://www.developerreport.com.
33. *Ibid.*
34. *Ibid.*
35. *Ibid.*
36. *Ibid.*
37. JPMorgan Asset Management, 'JPMorgan Asset Management Launches Its First Tokenized Money Market Fund', press release, https://am.jpmorgan.com/us/en/asset-management/adv/about-us/media/press-releases/jp-morgan-asset-management-launches-its-first-tokenized-money-market-fund, accessed June 2026.
38. Société Générale–Forge, https://www.sgforge.com, accessed June 2026.
39. UBS, 'First Tokenized Investment Fund', UBS Media, 1 November 2024, https://www.ubs.com/global/en/media/display-page-ndp/en-20241101-first-tokenized-investment-fund.html.
40. Galaxy Digital, 'Big Companies Building on Ethereum', *Galaxy Research*, https://www.galaxy.com/insights/research/big-companies-building-on-ethereum, accessed June 2026.
41. The Block, 'Standard Chartered Says 2026 Will Be the Year of Ethereum', *The Block*, https://www.theblock.co/post/385097/standard-chartered-says-2026-will-be-the-year-of-ethereum, accessed June 2026.
42. Securitize, 'BlackRock Launches First Tokenized Fund BUIDL on the Ethereum Network', https://securitize.io/learn/press/blackrock-launches-first-tokenized-fund-buidl-on-the-ethereum-network, accessed June 2026.
43. Ondo Finance, 'Fidelity Unveils Onchain Money Market Fund Anchored by Ondo Finance', https://ondo.finance/blog/fidelity-unveils-onchain-money-market-fund-anchored-by-ondo-finance, accessed June 2026.
44. Franklin Templeton Digital Assets, Benji, https://digitalassets.franklintempleton.com/benji, accessed June 2026.
45. Amundi, 'Amundi Launches First Tokenised Share: Amundi Funds Cash EUR', https://www.amundi.com/institutional/article/amundi-launches-first-tokenised-share-amundi-funds-cash-eur-caceis, accessed June 2026.

46. PRNewswire, 'DigiFT Introduces First Actively Managed Tokenized Equity Fund with BNY', https://www.prnewswire.com/news-releases/digift-introduces-first-actively-managed-tokenized-equity-fund-with-bny-as-investment-management-services-provider-302669662.html, accessed June 2026.
47. SWIFT, 'Swift's Blockchain-Based Shared Ledger Progresses to MVP Implementation', SWIFT.com, 30 March 2026, https://www.swift.com/news-events/news/swifts-blockchain-based-shared-ledger-progresses-mvp-implementation, accessed June 2026.
48. Visa, 'Visa Accelerates Stablecoin Momentum: Adding Five Blockchains for Settlement', Press release, 2026, https://investor.visa.com/news/news-details/2026/Visa-Accelerates-Stablecoin-Momentum-Adding-Five-Blockchains-for-Settlement/default.aspx, accessed June 2026.
49. Mastercard, 'Mastercard Expands Settlement Capabilities to Include Stablecoin', press release, June 2026, https://www.mastercard.com/global/en/news-and-trends/press/2026/june/mastercard-expands-settlement-capabilities-to-include-stablecoin.html, accessed June 2026.
50. PayPal, 'PayPal Launches U.S. Dollar Stablecoin', press release, 7 August 2023, https://newsroom.paypal-corp.com/2023-08-07-PayPal-Launches-U-S-Dollar-Stablecoin.
51. Robinhood, 'Robinhood Launches Stock Tokens, Reveals Layer 2 Blockchain', press release, https://robinhood.com/newsroom/robinhood-launches-stock-tokens-reveals-layer-2-blockchain-and-expands-crypto-suite-in-eu-and-us-with-perpetual-futures-and-staking, accessed June 2026.
52. Coinbase, 'Introducing Base', Coinbase Blog, https://www.coinbase.com/blog/introducing-base, accessed June 2026.
53. OpenZeppelin, Technical Risk Assessment on Blockchain Networks, op. Cit.
54. *Ibid.*
55. *Ibid.*
56. *Ibid.*
57. *Ibid.*
58. *Ibid.*
59. *Ibid.*
60. *Ibid.*
61. *Ibid.*
62. *Ibid.*
63. Ethereum Foundation, 'Ethereum Energy Consumption', *Ethereum.org*, ethereum.org/energy-consumption, accessed June 2026.
64. *Ibid.*
65. Canton Network, 'Canton Network Press Release', canton.network, accessed June 2026.
66. Canton Network and DTCC, 'DTCC and Digital Asset Partner to Tokenize DTC-Custodied U.S. Treasury Securities on the Canton Network', canton.network, accessed June 2026.
67. Canton Network, 'Global Synchronizer', canton.network/global-synchronizer, accessed June 2026.
68. Canton Network, 'FAQ', canton.network/faq, accessed June 2026.
69. Tempo, tempo.xyz, accessed June 2026.
70. Tempo, 'Validator Documentation', Tempo Docs, docs.tempo.xyz, accessed June 2026.
71. Google Cloud, 'Beyond Stablecoins', cloud.google.com, accessed June 2026.
72. *Ibid.*
73. *Ibid.*
74. Canton Network, 'Global Synchronizer', canton.network/global-synchronizer, accessed June 2026.
75. Tempo, tempo.xyz, accessed June 2026.
76. CoinDesk, 'Stripe's Tempo Blockchain Is a Referendum on the Ghost of Libra, Says Libra Co-Creator', CoinDesk, 7 September 2025, coindesk.com.
77. Finovate, 'Tempo's Payments Infrastructure and Protocol Goes Live', Finovate, finovate.com, accessed June 2026.
78. *Ibid.*

Economic and Financial System Implications

1. OpenZeppelin, Technical Risk Assessment on Blockchain Networks, op. Cit.
2. *Ibid.*
3. *Ibid.*
4. *Ibid.*
5. RWA.xyz, 'Tokenized Real-World Assets by Network', app.rwa.xyz/networks, accessed June 2026.
6. *Ibid.*
7. *Ibid.*
8. OpenZeppelin, Technical Risk Assessment on Blockchain Networks, op. Cit.
9. *Ibid.*
10. *Ibid.*
11. *Ibid.*
12. *Ibid.*
13. *Ibid.*
14. Probelab, 'Ethereum Topology, Countries Map', probelab.io, accessed June 2026.
15. *Ibid.*
16. 'Client Diversity, Ethereum', Client Diversity, https://clientdiversity.org, accessed June 2026.
17. OpenZeppelin, Technical Risk Assessment on Blockchain Networks, op. Cit.
18. *Ibid.*
19. *Ibid.*
20. Bitcoin Magazine, 'MetaMask Launches Native Bitcoin Integration for 30 Million Active Users', *Bitcoin Magazine*, 16 December 2025, https://bitcoinmagazine.com/business/metamask-launches-native-bitcoin-integration-for-30-million-active-users, accessed June 2026.
21. *Ibid.*
22. Safe, 'Crypto Treasury Management Solutions', *Safe.global*, https://safe.global/teams, accessed June 2026.
23. DeFiLlama, 'Morpho Protocol', defillama.com/protocol/morpho, accessed June 2026.
24. RWA.xyz, 'Tokenized Real-World Assets by Network', app.rwa.xyz/networks, accessed June 2026.
25. Franklin Templeton Digital Assets, *Benji*, https://digitalassets.franklintempleton.com/benji, accessed June 2026.
26. Securitize, 'BlackRock Launches First Tokenized Fund BUIDL on the Ethereum Network', https://securitize.io/learn/press/blackrock-launches-first-tokenized-fund-buidl-on-the-ethereum-network, accessed June 2026.
27. JPMorgan Asset Management, 'JPMorgan Asset Management Launches Its First Tokenized Money Market Fund', press release, https://am.jpmorgan.com/us/en/asset-management/adv/about-us/media/press-releases/jp-morgan-asset-management-launches-its-first-tokenized-money-market-fund, accessed June 2026.
28. Amundi, 'Amundi Launches First Tokenised Share: Amundi Funds Cash EUR', https://www.amundi.com/institutional/article/amundi-launches-first-tokenised-share-amundi-funds-cash-eur-caceis, accessed June 2026.
29. Commodity Futures Trading Commission, 'Acting Chairman Pham Announces Launch of Digital Assets Pilot Program for Tokenized Collateral in Derivatives Markets', CFTC Press Release No. 9146-25, 8 December 2025, https://www.cftc.gov/PressRoom/PressReleases/9146-25, accessed June 2026.
30. OpenZeppelin, Technical Risk Assessment on Blockchain Networks, op. Cit.
31. *Ibid.*
32. *Ibid.*
33. 'What Is USDC?', USDC.com, https://www.usdc.com/learn/what-is-usdc, accessed June 2026.
34. Ondo Finance, 'Fidelity Unveils Onchain Money Market Fund Anchored by Ondo Finance', https://ondo.finance/blog/fidelity-unveils-onchain-money-market-fund-anchored-by-ondo-finance, accessed June 2026.

35. Société Générale–Forge, https://www.sgforge.com, accessed June 2026.
36. Visa, 'Visa Expands Stablecoin Settlement Capabilities to Merchant Acquirers', press release, 5 September 2023, https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.19881.html, accessed June 2026.
37. PayPal, 'PayPal Launches U.S. Dollar Stablecoin', press release, 7 August 2023, https://newsroom.paypal-corp.com/2023-08-07-PayPal-Launches-U-S-Dollar-Stablecoin, accessed June 2026.
38. JPMorgan Asset Management, 'JPMorgan Asset Management Launches Its First Tokenized Money Market Fund', press release, https://am.jpmorgan.com/us/en/asset-management/adv/about-us/media/press-releases/jp-morgan-asset-management-launches-its-first-tokenized-money-market-fund, accessed June 2026.
39. BNY, 'BNY Expands Digital Asset Platform with Launch of Innovative On-Chain Offering', press release, 3 April 2025, https://www.bny.com/corporate/global/en/about-us/newsroom/press-release/bny-expands-digital-asset-platform-with-launch-of-innovative-on-chain-offering.html, accessed June 2026.
40. EY, 'EY Upgrades Nightfall, a Zero-Knowledge Roll-Up Enabling Private Transactions on the Ethereum Blockchain', press release, 3 April 2025, https://www.ey.com/en_gl/newsroom/2025/04/ey-upgrades-nightfall-a-zero-knowledge-roll-up-enabling-private-transactions-on-the-ethereum-blockchain, accessed June 2026.
41. Deutsche Bank, 'DAMA 2 Litepaper: Institutional Blueprint for Asset Tokenisation and Servicing on Ethereum Layer 2', DB.com, 18 June 2025, https://www.db.com/news/detail/20250618-dama-2-litepaper-institutional-blueprint-for-asset-tokenisation-and-servicing-on-ethereum-layer-2, accessed June 2026.
42. Cointelegraph, 'Indian State Gov't Uses Polygon to Issue Verifiable Caste Certificates', Cointelegraph, 29 March 2022, https://cointelegraph.com/news/indian-state-gov-t-uses-polygon-to-issue-verifiable-caste-certificates, accessed June 2026.
43. The Block, 'Bhutan Migrates National Digital ID System to Ethereum', The Block, 14 October 2025, https://www.theblock.co/post/374480/bhutan-migrates-national-digital-id-system-ethereum, accessed June 2026.
44. Cointelegraph, 'Buenos Aires to Issue Blockchain-Based Digital ID', Cointelegraph, 2 October 2023, https://cointelegraph.com/news/buenos-aires-blockchain-based-digital-identity, accessed June 2026.
45. European Investment Bank, 'EIB Issues Its First Ever Digital Bond on a Public Blockchain', press release, 28 April 2021, https://www.eib.org/en/press/all/2021-141-european-investment-bank-eib-issues-its-first-ever-digital-bond-on-a-public-blockchain, accessed June 2026.
46. UNICEF, 'UNICEF Launches Cryptocurrency Fund', press release, 9 October 2019, https://www.unicef.org/press-releases/unicef-launches-cryptocurrency-fund, accessed June 2026.

Environmental and Societal Considerations

1. Ethereum Foundation, 'Ethereum Energy Consumption', Ethereum.org, ethereum.org/energy-consumption, accessed June 2026.
2. *Ibid.*
3. *Ibid.*
4. *Ibid.*
5. *Ibid.*
6. *Ibid.*
7. *Ibid.*
8. *Ibid.*

9. *Ibid.*
10. *Ibid.*
11. *Ibid.*
12 *Ibid.*
13. 'ERC-8004: Trustless Agents', Ethereum Improvement Proposals, https://eips.ethereum.org/EIPS/eip-8004, accessed June 2026.
14. Ethereum Foundation, 'Future-Proofing Ethereum and Crypto Quantum Security', Ethereum.org, https://ethereum.org/roadmap/future-proofing, accessed June 2026.
15. Ethereum Foundation Post-Quantum Team, Post-Quantum Ethereum, https://pq.ethereum.org, accessed June 2026.

Ethereum Basics for Governments and Institutions

ethereum foundation
GPS