OpenZeppelin

Technical Risk Assessment on Blockchain Networks

Apr 30, 2026

Table of Contents

Executive Summary

Purpose and Audience

This report provides a structured, side-by-side risk assessment of six blockchain networks: Ethereum, BNB Smart Chain (BSC), XRP Ledger (XRPL), TRON, Solana, and the Canton Network. It is written for policymakers, supervisory authorities, and institutional decision-makers who need to understand the operational characteristics and risk profiles of these networks, without requiring deep technical expertise.

The report does not recommend or endorse any network. The goal is to equip readers with a factual basis for evaluating the risks associated with blockchain infrastructure, particularly as these networks increasingly underpin financial products and services that fall within regulatory perimeters.

Scope and Methodology

The assessment examines each network across six dimensions, chosen for their direct relevance to regulatory and institutional risk concerns. This report is limited to base-layer (Layer 1) networks. Layer 2 scaling solutions and other application-layer risks are outside the scope of this assessment. The dimensions assessed are:

1. **Maturity and Operational Track Record**: Network history, stress performance, and incident response.
2. **Finality**: Transaction irreversibility and underlying guarantees.
3. **Technical Resilience and Supply Concentration**: Single points of failure and attack paths.
4. **Control, Governance, and Concentration of Authority**: Concentration of authority and collusion risk.
5. **Continuity and Institutional Sustainability**: Network's ability to survive key sponsor failure.
6. **Network Activity and Adoption**: Current usage scale and supported activity types.

These dimensions were selected because they map onto the core concerns that regulators typically evaluate: operational resilience, settlement assurance, systemic concentration risk, governance accountability, and business continuity.

Data was gathered from public sources including official documentation, foundation reports, on-chain analytics, post-incident analyses, and academic or industry research. Where data was unavailable or unverifiable, it was explicitly noted. All findings reflect conditions as of early March 2026.

Comparability

The six networks in this report are not alike in design, purpose, or trust model. Thus, readers should resist the temptation to rank them on a single scale. These networks differ from one another in fundamental ways, not just in performance or architecture, but in the problems they were built to solve, who they were built for, and what assumptions they make about trust.

Ethereum and Solana prioritize general-purpose programmability but make very different trade-offs between decentralization and throughput. XRP Ledger, BNB Smart Chain, and TRON all prioritize high volume and low cost over decentralization, achieving this through a smaller set of validators rather than a broadly distributed trust base. The Canton Network is a blockchain built specifically for financial institutions, where transaction privacy is a default rather than an add-on. Participation is currently invite-only, with plans to transition to permissionless access.

These architectural differences mean that the same metric can carry very different implications depending on the network. A small validator set may represent a centralization risk on one chain and a deliberate design choice on another. Fast finality may signal efficiency or may reflect a narrower trust base. As such, readers are encouraged to interpret each network's characteristics within the context of its design goals and intended use instead of treating any single metric as universally good or bad.

A glossary of technical terms is provided at the end of the report for reference.

Foundational Concepts

A blockchain is a shared record of transactions (ledger) maintained by a network of computers (validators) that collectively agree on its contents. No single party controls the ledger; instead, validators follow a set of rules (the consensus mechanism) to agree on which transactions are valid and in what order they occurred.

For regulators and institutional decision-makers, three properties are particularly relevant. First, finality - the point at which a transaction can be considered irreversible and settled. Second, resilience - the network's ability to continue operating under stress, whether from technical failures, malicious actors, or the exit of key participants. Third, governance - who has the practical authority to change the rules of the network, and how quickly they can do so.

These properties sit in tension with one another. Networks that prioritise speed and low cost typically achieve this through a smaller group of validators and more concentrated decision-making. Networks that prioritise decentralisation and censorship resistance typically sacrifice throughput and governance agility in return. Understanding these trade-offs is essential context for the assessments that follow.

Key High-Level Observations

- **The barriers to controlling a network differ fundamentally in nature, not just in cost:** Three attack vectors apply across these networks: acquiring sufficient economic stake, executing a supply chain attack on the validator client (in other words, validator software implementation), or colluding with a sufficient number of validators. For stake-based networks, the minimum value of controlled stake for an external entity to unilaterally influence consensus (i.e. finalizing a fraudulent transaction - the attacker convinces the network to acknowledge and mark as irreversible a transaction that was invalid, or never even happened) ranges from approximately $8.7bn(Tron), $11.3bn (BSC), $23.3bn (Solana), to $50.7bn (Ethereum). The economic deterrence also varies significantly: Ethereum automatically penalises up to all of the attacker’s staked collateral (all of which must be the validator's own), while BSC only penalises the stake that the validator itself put up - not the stake that third parties entrusted to it. Solana has no automatic penalty mechanism in place, Tron imposes no economic penalties at all,

and XRPL and Canton rely entirely on institutional trust rather than financial collateral, with no penalties of any kind for misbehaviour. Supply chain risk is most acute where a single codebase dominates; every network except Ethereum runs a single validator client in production, and on Solana, while two clients exist, one runs on approximately 90% of validators. For networks with small validator sets, like BSC, XRPL, Tron, and Canton, collusion is a structurally more accessible vector than on networks with larger, more distributed sets.

- **Chain maturity varies widely:** XRPL (2012) and Ethereum (2015) have over a decade of operational history, providing the longest track record to assess. TRON, Solana, and BSC sit at 5–7 years. Canton (2024) has just over one year of production history. Maturity correlates broadly, though imperfectly, with operational resilience.

- **Every network except Ethereum has experienced a full halt in transaction processing.** Solana has the most disrupted record, with seven outages including one lasting ~19 hours. BSC was deliberately halted for ~8 hours following a bridge exploit affecting over $500 million. XRPL halted twice (longest ~64 minutes), TRON once (~2 hours). Canton pauses during scheduled upgrades. Ethereum has never fully stopped operating, though it has experienced temporary finality delays, and a chain split due to an application vulnerability.

- **Finality models differ fundamentally.** XRPL, Canton, and Solana provide deterministic finality - confirmed transactions are irreversible by protocol design. Ethereum and BSC provide economic finality - reverting a transaction is theoretically possible but would require an attacker to forfeit collateral. The cost is substantially higher on Ethereum, where all staked collateral is at risk, than on BSC, where only a validator's own stake is subject to penalties. TRON only provides probabilistic finality - confidence in irreversibility grows with each block, but the protocol never formally declares a transaction final. Finality times range from seconds to minutes. Faster finality typically comes at the cost of a smaller or more concentrated validator set.

- **Governance models vary widely in the distribution of decision-making authority and the speed at which protocol changes can be enacted:** Ethereum requires multi-team consensus across independent organizations, with no single team able to unilaterally push changes; meaning that non-emergency upgrades can take

months to coordinate. Solana has multiple contributing teams but a narrower governance base. BSC, XRPL, and TRON each depend primarily on a single core team that proposes, implements, and coordinates changes, which enables faster no-emergency upgrades but concentrates influence over the protocol's direction. Canton's governance is heavily influenced by the Canton Foundation and the primary developer, Digital Asset.

- **Client diversity is the exception, not the norm.** Ethereum has numerous independent execution and consensus software clients. Solana has two independent implementations, though one dominates. BSC, XRPL, TRON, and Canton each rely on a single codebase - a critical vulnerability in any of them would affect 100% of validators simultaneously.

- **Validator set sizes vary by orders of magnitude across networks.** A larger validator set distributes trust across more independent parties, making the network more resistant to collusion or coordinated failure. However, raw validator counts can be misleading - a single operator may run many validators, and large staking service providers can aggregate substantial stake under unified control. Ethereum has the largest set of active validators, over 900,000. Solana has more than 800 validators. BSC, XRPL, and TRON each maintain sets of validators ranging from dozens to ~100. Canton uses a model where validators only participate in transactions they are a party to, while the super validators only do transaction ordering and routing. Smaller sets enable faster coordination but concentrate trust in fewer hands.

- **The cost to compromise consensus varies dramatically.** Ethereum's security derives from $76bn in staked assets, with automatic slashing (penalties) that destroys attacker collateral. Solana secures its network with $35bn in staked SOL, but has no automatic slashing. TRON and BSC have significantly less staked assets $13bn and $17bn respectively - TRON imposes no automatic penalty for misbehavior, while BSC only penalizes that particular validator’s own stake. XRPL's security is not stake-based, and it depends on the integrity of a curated set of validators with no economic consequences for acting maliciously. Canton uses a "proof-of-stakeholder" model where only parties to a transaction validate it, with no staking requirement or penalties of any kind. Its security relies on institutional trust and consensus of Super Validators rather than at-risk economic collateral.

These differences have direct implications for how much confidence should be placed in each network's resistance to manipulation.

- **Most networks have critical single-entity development dependencies.** XRPL depends on Ripple for core development, TRON on the TRON Foundation, BSC on Binance and the BNB Chain Foundation, and Canton on Digital Asset. Ethereum and, to a lesser extent, Solana have multiple independent organisations capable of sustaining core protocol development without a single sponsor.

- **No network has implemented quantum-resistant cryptography.** Ethereum has the most active research programme on this topic. XRPL and Solana have nascent projects in early development. BSC, as an EVM-chain, can inherit any post-quantum protections from Ethereum. However, just like TRON and Canton, it has no publicly documented plans. While the threat is not imminent, migrating live financial infrastructure requires preparation timelines measured in years.

- **Token concentration at genesis varies significantly**. Token concentration at genesis shapes long-term governance dynamics, since in Ethereum, BSC, TRON, and Solana, token holdings translate directly into influence over protocol decisions. Ethereum allocated ~17% to insiders. BNB reserved 50% for the founding team and angel investors, with the remainder offered through public sale. Solana reportedly allocated more than 90% to insiders. TRON directed 60% to the founding team and angel investors. XRPL allocated its entire initial supply to the company and founders. Canton launched with no pre-mined supply, with all tokens earned through network participation. It is worth noting that native token holdings in XRPL and Canton do not directly constitute governance or consensus power.

- **Security audit practices differ considerably.** Ethereum benefits from regular audits across multiple client implementations by independent firms. Solana's major upgrades are generally audited. BSC's client is derived from Ethereum’s primary client, and thus, inherits some upstream audit coverage. XRPL's upgrades are open-source, but no public reports document routine formal audits; formal reviews appear limited to major new features like smart contract primitives. TRON had its first and only known third-party security assessment of its core client in 2024. Canton had an audit of the smart contracts implementing the Canton Coin in 2025. No other audit evidence was found for Canton. The absence of routine

independent audits is notable for networks processing billions in daily transaction value.

- **No network has a single actor who can unilaterally override or censor transactions through a privileged protocol-level mechanism.** None of the six networks have built-in admin keys, emergency kill switches, or protocol-level override functions. The practical ability to exert control varies considerably for each chain.

- **Ecosystem maturity and developer activity are concentrated in Ethereum.** It has the most diverse application ecosystem, deepest liquidity, and longest track record of sustained development. BSC and Solana have active ecosystems with growing developer communities, though narrower in scope. TRON has meaningful usage but a less diverse application landscape. XRPL has built-in financial primitives and nascent general smart contract applications. Canton is the newest entrant, with early adoption focused on regulated financial applications rather than permissionless DeFi.

Risk manifests differently across chains and no single metric captures the full picture. Thus, meaningful assessment requires examining multiple dimensions.

Detailed Assessment

The following sections examine each network across the six risk dimensions introduced above, presented in tabular form for direct comparison. Narrative risk assessments for each network follow the tables, providing interpretive context where the data warrants further explanation.

Maturity and Operational Track Record						
	BSC	**Canton**	**Ethereum**	**Solana**	**Tron**	**XRPL**
When did the network launch?	September 2020, 5+ years ago	June 2024, 1+ year ago	July 2015, 10+ years ago	March 2020, 6+ years ago	May 2018, 7+ years ago	June 2012, 13+ years ago
What significant incidents have occurred? How has the network recovered from these incidents?	Core bridge exploit in 2022 resulted in deliberate chain halt. Recovery required core team coordination. Ethereum client software bugs affected BSC as well.	None	Two brief instances in 2020 and 2021, where client software bugs caused a subset of validators to produce conflicting records, and two instances of finality delays, in 2023. Recovery required client team coordination for software patches, finality was recovered autonomously via inactivity leak.	7 full-outage incidents since launch. Recovery required software patches and validators to reach off-chain consensus on a safe restart slot.	Smart contract attack that stopped transaction processing in 2020. It required a software patch and coordination with Super Representatives to upgrade quickly.	Transaction processing had stopped in 2025. The network self-recovered with minimal manual intervention.
What was the most severe incident in the network's history?	Core bridge vulnerability, >$500m of funds affected, resulting in deliberate chain halt lasting for ~8 hours.	No recorded incident	<1 hour finality delays, blocks continued to be produced at a reduced rate, liveness maintained.	~ 17-hour complete halt without processing transactions, in 2021.	~2 hours without processing transactions.	~64 minutes without processing transactions.

Maturity and Operational Track Record						
	BSC	**Canton**	**Ethereum**	**Solana**	**Tron**	**XRPL**
Has the network ever been fully unable to process transactions? What was the longest halt?	Yes, 1 incident lasting ~8 hours (chain deliberately halted in October 2022).	Yes, transaction processing has stopped during multiple scheduled upgrades (last one was in December 2025). Longest instance unknown.	No	Yes, 7 times. The longest was ~19 hours long (February 2023) in which it did not process any user-created transactions.	Yes, 1 incident which lasted ~2 hours without producing transactions (November 2020).	Yes, 2 incidents. The longest lasted ~64 minutes (February 2025).
Have detailed post-incident analyses been published? Who published them?	Yes, through a brief incident response by the core team, and independent analysis.	Not applicable	Yes, by client teams, the foundation, and independent researchers.	Yes, by the Solana Foundation and independent teams.	No public post-incident analysis was found.	Yes, by the XRPLF on the xrpl.org/blog website.
How had users been notified during and after the incidents?	Through X accounts controlled or affiliated with Binance and the BNB Chain Foundation. Independent analyses posted on Reddit.	Not applicable	Multiple client teams' official channels, individual developer accounts, and independent sources.	Multiple client teams' official channels, individual developer accounts, the incident status page, and independent sources.	Through a post by the Tron Founder on X.	Through the public incident status page, posts on X from the Engineering Team Leadership, as well as a dedicated mailing list.
Have similar incidents recurred?	No	Not applicable	Yes, finality delay incidents repeated on two consecutive days in May 2023.	Yes, but the frequency of full-outage incidents has dropped.	No	No

Maturity and Operational Track Record						
	BSC	**Canton**	**Ethereum**	**Solana**	**Tron**	**XRPL**
Does the network maintain a bug-bounty program?	Yes, by the BNB Chain Foundation, up to $100k.	No public bug bounty program.	Yes, by the Ethereum Foundation, up to $1 million.	Yes, the Solana Foundation offers up to 25,000 SOL for the Agave client. The Firedancer and the Jito-Solana (Agave fork) teams offer up to $500k and $250k for their respective clients.	Yes, by the TRON Foundation. Mostly inactive in recent years.	Yes, by Ripple and through bug bounty platforms.
Who decides what to do during a crisis?	Influenced by the BNB Chain Foundation, which holds primary responsibility for situation assessment, patching the sole validator client, and coordinating rollout across the network.	Influenced by Digital Asset, the Canton Foundation, and the Super Validators.	No single authority, decisions taken based on consensus among client teams.	Validator operators coordinate publicly alongside client engineering teams.	Influenced by the Tron Foundation, which holds primary responsibility for situation assessment, patching the sole validator client, and coordinating rollout across the network.	Influenced by the XRPL Foundation, which holds primary responsibility for situation assessment, patching the sole validator client, and coordinating rollout across the network.
Is there a test network that reflects the production environment?	1 public test network.	1 test network and 1 dev network, but they both currently require allowlisting.	2 public test networks; multiple earlier test networks have been deprecated.	1 public test network and 1 public dev network.	2 public test networks.	1 public test network and 1 public dev network.

Finality						
	BSC	**Canton**	**Ethereum**	**Solana**	**Tron**	**XRPL**
What type of consensus mechanism does the network use?	Proof-of-Staked-Authority (Delegated Proof-of-Stake and Proof-ofAuthority)	A two-tier consensus mechanism	Proof-of-Stake (Gasper)	Proof of Stake (augmented with Proof of History)	Delegated Proof-of-Stake	XRPL Consensus Protocol
What constitutes decision power in this network?	Staked BNB. 45 validators with the most stake are elected daily. Of these, 18 of the 21 with the highest stake (called Cabinets) + 3 others (called Candidates) are selected each epoch to propose and attest to blocks (active validators). Transactions are finalized only if >⅔ of the 21 elected validators are in agreement.	Validators only validate transactions they are a party to. Super Validators manage the ordering and confirmation of transactions and provide a publicly verifiable view of the Canton Coin ledger.	Staked ETH. Validators are selected to propose and attest to blocks in proportion to their stake. Transactions are finalized only if validators representing >⅔ of total staked ETH agree on two consecutive checkpoints.	Staked SOL. Validators are selected to produce blocks and vote on consensus in proportion to their stake. Transactions are finalized only if validators representing >⅔ of total staked SOL are in agreement and 31 blocks have been built on top of it.	TRX is locked and used to vote every 6 hours. The 27 most voted validators are elected as Super Representatives (SRs). The elected SRs perform consensus and process transactions. Transactions are processed only if >⅔ of SRs are in agreement.	Meaningfully participating in consensus requires being included on the Recommended Validator Lists, constructed and published by Ripple and the XRPL Foundation. Transactions are processed only if >⅘ of the validators are in agreement.
How long until a transaction is	~1-2 seconds	Can be near instant	~13 minutes	~12.8 seconds	~1 minute	~4-6 seconds

Finality						
	BSC	**Canton**	**Ethereum**	**Solana**	**Tron**	**XRPL**
considered irreversible?						
What would it take to maliciously reverse a finalized transaction?	Controlling >⅔ of the 21 block producers.	Processed transactions cannot be reversed.	Controlling >⅔ of the total staked ETH.	Controlling >⅔ of total staked SOL.	Controlling >⅔ of the SRs, or enough TRX to select your own SRs.	Controlling >⅘ of the validators involved in consensus.
What is the total value of native tokens currently staked to secure the network?	~$17b	Not applicable as network security is not based on economic stake.	~$76b	~$35B	~$13B	Not applicable as network security is not based on economic stake.
What is the economic threshold for compromising the network's ability to finalize transactions, based on current staked amounts? *For networks using BFT-style consensus, controlling >⅓ of the currently staked tokens is sufficient to create two conflicting chains or prevent the supermajority needed to confirm blocks as irreversible. New blocks cannot be finalized, and already existing blocks cannot be re-written.*	<$5.7bn, based on the heuristic that in the most expensive scenario, the attacker needs ⅓ of total stake to control >⅓ of the 21 validators.	Not applicable, as participation in consensus is not based on stake.	~$25.3bn	~$11.7bn	<$4.3bn, based on the heuristic that in the most expensive scenario, the attacker needs ⅓ of total stake to control >⅓ of the 27 SRs.	Not applicable, as participation in XRPL consensus is not based on stake.

Finality						
	BSC	**Canton**	**Ethereum**	**Solana**	**Tron**	**XRPL**
What is the economic threshold for finalizing a fraudulent transaction on the network, based on current staked amounts? Finalizing a fraudulent transaction requires forging a supermajority attestation for an invalid block. *For networks using BFT-style consensus, this requires controlling >⅔ of the currently staked tokens.* New blocks can be finalized, and already existing blocks can be re-written.	<$11.3bn, based on the heuristic that in the most expensive scenario, the attacker needs ⅔ of total stake to control >⅔ of the 21 validators.	Not applicable, as participation in consensus is not based on stake.	~$50.7bn	~$23.3bn	<$8.7bn, based on the heuristic that in the most expensive scenario, the attacker needs ⅔ of total stake to control >⅔ of the 27 SRs.	Not applicable, as participation in XRPL consensus is not based on stake.
What is the amount a bad actor would lose if they attempted to compromise finality by creating two conflicting chains?	Only self-bonded stake is subject to slashing, up to 200 BNB (~$120,000) per validator, which would amount to at least ~$800k, and at most ~$2.5mn.	Not applicable.	All the attacker's stake is subject to slashing, which would amount to at least ~$25.3bn.	No in-protocol automatic slashing has been implemented yet. Validators can be slashed if they cause a network halt, through a manual, governance-driven mechanism when the network restarts.	No economic penalties. The validator would lose the stakers' trust and no longer be elected as a SR.	No economic penalties. The validator would no longer be trusted by fellow validators on the network, leading to no further influence on consensus.

Finality						
	BSC	**Canton**	**Ethereum**	**Solana**	**Tron**	**XRPL**
Is finality probabilistic or deterministic? Is it guaranteed by economic incentives?	Probabilistic until finalization, then protected by economic incentives.	Deterministic	Probabilistic until finalization, then protected by economic incentives.	Optimistic until finalization, then protected by exponential vote lockouts.	Probabilistic	Deterministic
Under what conditions could finality be delayed?	>⅓ of 21 producers not voting on new blocks, resulting in consistently slower finality.	There is no separate concept of finality in Canton. All processed transactions are final. Any situation that affects transaction processing would also affect finality, for example, more than one-third of Super Validators being offline for a transaction routed through the Global Synchronizer, or a transaction party being offline.	>⅓ of staked ETH not voting on new blocks, self-healed via inactivity leak.	>⅓ of staked SOL not voting on new blocks, resulting in delayed or halted finalization.	>⅓ of the SRs not voting on new blocks, resulting in delays or halted transaction processing.	>⅕ of the recommended validators not voting on new blocks, resulting in halted transaction processing.

Technical Resilience and Concentration						
	BSC	**Canton**	**Ethereum**	**Solana**	**Tron**	**XRPL**
How many independently developed software implementations run the network?	There is only one, derived from an Ethereum client, developed and maintained by Binance-affiliated teams. Another client is under development.	There is only one client, called Splice, developed and maintained by Digital Asset.	Multiple. 5+ production execution clients and 5+ production consensus clients.	Two: Agave and Firedancer.	There is only one client called java-tron, developed and maintained by the Tron Foundation.	There is only one client, called rippled, developed and maintained by the XRPL Foundation.
What share of validators run the dominant software client?	100%	100%	~50% run the Lighthouse consensus client. ~40% run the Geth execution client.	90% run Agave or Agave forks.	100%	100%
What percentage of the initial token supply was distributed to insiders? *Insiders include founders, team members, the foundation and private investors. Tokens subject to vesting are included.*	~50%: 100 million BNB were allocated to insiders. Estimated 100 million BNB in public offering (2017).	Canton coin supply was zero at genesis.	~17%: 12 million ETH retained for insiders 60 million ETH in public offering (2014).	Reportedly > 90%, however this could not be independently validated. 500 million SOL were minted at genesis. 8 million SOL was offered through a	~60%: 100 billion TRX were minted at genesis: ~15 billion sold in private sale, 40 billion sold in the public ICO (2017), the remainder given to the TRON Foundation and	100%: 100 billion XRP minted at genesis: 80 billion to Ripple, the remaining 20 billion to the founders.

Technical Resilience and Concentration						
	BSC	**Canton**	**Ethereum**	**Solana**	**Tron**	**XRPL**
				public auction and the rest reportedly went to insiders.	team.	
What are the thresholds for censorship, and transaction rewriting?	For censorship and transaction rewriting, one should control >⅔ of 21 active validators. Only the self-delegated BNB slashed.	For censorship and transaction manipulation of transactions synced through the Global Synchronizer, one should control > ⅔ of Super Validators.	For censorship and transaction rewriting, one should control >⅔ of total staked ETH. Attacking validators are penalised.	For censorship and transaction rewriting, one should control >⅔ of all staked SOL.	For censorship and transaction rewriting, one should control >⅔ of Super Representatives.	The thresholds are not economic in nature, but rather operational. For censorship and transaction rewriting, attacking more than ⅘ of the validators is necessary.
What percentage of validators is hosted on cloud providers? Has a hosting provider outage or policy change ever disrupted the network?	Precise infrastructure distribution data cannot reliably be derived.	Precise infrastructure distribution data cannot reliably be derived.	Estimates show that ~35% of validators are hosted on cloud infrastructure, across multiple providers. No data on individual providers.	33% of total stake is hosted on the single largest cloud provider, TeraSwitch. In November 2022, Hetzner blocked all Solana validators, taking over 1,000 offline and making 20% of stake delinquent but the network remained operational during the transition.	Precise infrastructure and country distribution data cannot reliably be derived.	Precise infrastructure distribution data cannot reliably be derived.

Technical Resilience and Concentration						
	BSC	**Canton**	**Ethereum**	**Solana**	**Tron**	**XRPL**
What percentage of validators are located in the top three countries?	Precise country distribution data cannot reliably be derived.	~ 90% of active Super Validator entities are from the USA, UK, and Switzerland.	~52-60% estimated to be hosted in the USA, Germany and France.	~ 65% estimated to be hosted in the USA, Germany and Netherlands.	Precise country distribution data cannot reliably be derived.	Precise country distribution data cannot reliably be derived.
What is the network's observed transaction throughput capacity?	~44-164 observed TPS.	TPS is domain- and party-specific instead of being global.	~13-28 Observed TPS. Layer 2 solutions enable orders of magnitude larger throughput.	~2800-4700 observed TPS (including vote transactions).	~93-164 observed TPS.	>1600 observed TPS.

Control, Governance, and Concentration of Authority						
	BSC	**Canton**	**Ethereum**	**Solana**	**Tron**	**XRPL**
How many validators participate in consensus? *This figure reflects the number of active validator nodes, not the number of independent entities operating them.*	BSC maintains 45 active validators, elected daily based on stake. For each epoch, 21 validators produce blocks.	Each validator only receives a copy of the parts of a transaction that specifically apply to them. The active super validator set (13 currently) orders	~950,000 validators	~800 validators	27 Super Representatives, chosen every 6 hours based on most votes from stakers. The SRs take turns producing blocks.	130+ validators exist on mainnet. In practice, it is likely that only 35 of them meaningfully influence consensus.

Control, Governance, and Concentration of Authority						
	BSC	**Canton**	**Ethereum**	**Solana**	**Tron**	**XRPL**
		and routes the transactions to the validators.				
What are the main accumulation points of power within the network?	The BNB Chain Foundation and Binance, which maintain the sole validator client, lead protocol development, and are associated with a significant share of active validators.	The Super Validators exercise outsized influence over the network.	Liquid staking providers (notably Lido), centralized exchanges (Coinbase, Binance), and a small number of specialized block builders.	The top 20 validators form a superminority (33% staked) and can affect chain liveness. A sizable amount of SOL is staked through liquid staking protocols/entities.	The top 10 TRX stakers account for 45% of the overall votes. Some of the addresses are likely to belong to the same entity. Some of the related entities are the JustLend DAO, HTX and Binance.	The XRPLF and Ripple, which decide who is included within the Recommended Validator Lists.

Control, Governance, and Concentration of Authority						
	BSC	**Canton**	**Ethereum**	**Solana**	**Tron**	**XRPL**
How accessible is participation in validation?	Permissionless, 2000 BNB required. Practically much higher to be active (only top 45 by stake). High hardware requirements.	Currently invite only with plans to become permissionless.	Permissionless, 32 ETH required. Low hardware requirements. Liquid staking solutions available as applications.	Permissionless but moderately difficult due to high hardware requirements. Liquid staking solutions available as applications.	Permissionless in theory, but high practical barriers. In practice, unachievable for a participant without massive capital backing or exchange partnerships. The least voted SR required at least ~280 million USD worth of votes.	Permissionless in theory, but high practical barriers. Influencing consensus likely requires addition to the default UNLs, decided by the XRPL Foundation or Ripple, which demands proven identity, operational track record, and vetting.
What is the mechanism that rotates the decision makers in transaction validation and consensus?	The active set of 45 validators is re-elected daily by staking power (top 21 become Cabinet, next 24 become Candidates). Each epoch, 18 are randomly selected from the 21 Cabinet and 3 from the 24 Candidates. These 21 take turns producing blocks in	Existing Super Validators vote to admit or remove members, requiring a ⅔ supermajority, meaning the incumbents control who joins and who leaves.	Pseudorandom, stake-weighted selection to propose a block in each slot (~12 seconds). The committee of validators attesting to the blocks is re-assigned every epoch (~6.4 minutes).	A stake-weighted, pseudorandom leader schedule is computed at the start of each epoch to assign slots to validators, and validators continuously cast stake-weighted, on-chain votes over these slots.	Every 6 hours, Super Representatives are elected through votes from all TRX stakers. Due to concentrated voting power and self-voting, the elected SR list is rigid, with its composition rarely changing.	The Recommended Validator Lists significantly have tremendous impact in which validators participate in consensus. These lists are rigid, with few validators changing over the years.

Control, Governance, and Concentration of Authority						
	BSC	**Canton**	**Ethereum**	**Solana**	**Tron**	**XRPL**
	a fixed order.					
Who has the practical authority to change the protocol?	Protocol changes are usually proposed by the BNB Chain Foundation core team, and must be accepted on-chain by a simple majority of staking power.	Digital Asset develops proposals and code upgrades, and must be accepted by >⅔ of the super validators.	No single entity. The proposal process requires multi-team consensus, which takes place off-chain.	Core teams (Anza, Firedancer) create proposals; significant economic changes require stake-weighted validator governance votes needing a ⅔ supermajority to pass.	Protocol changes are usually proposed by the Tron Foundation, and must be accepted on-chain by >⅔ of the validators.	Protocol changes are usually proposed by the XRPLF, and must be accepted on-chain by >⅘ of the validators.
How often is the protocol upgraded?	4+ upgrades per year. Fast cadence enabled by single-team development.	~2-3 major upgrades a year.	1–2 major upgrades per year. Conservative cadence; changes are bundled together and deployed through months of multi-team coordination.	Multiple small and big upgrades per year.	Multiple smaller upgrades every year.	Multiple smaller upgrades every year.

Control, Governance, and Concentration of Authority						
	BSC	**Canton**	**Ethereum**	**Solana**	**Tron**	**XRPL**
Can validators reject an upgrade and continue operating?	Theoretically yes, but a validator that does not upgrade would fork onto an incompatible chain. No precedent of upgrade rejection.	No	Yes, with historical precedent. In 2016, a portion of validators rejected a protocol change, resulting in two separate live chains: Ethereum and Ethereum Classic.	Yes, but can lead to exclusion from consensus (due to software version mismatch) if the upgrade was accepted by the ⅔ majority.	Yes, but can lead to exclusion from consensus (due to software version mismatch) if the upgrade was accepted by the ⅔ majority.	Yes, but will lead to exclusion from consensus (due to hardcoded rules) if the upgrade was accepted by the ⅘ majority.
Is there a documented emergency upgrade procedure?	No formal procedure. The foundation team will implement a software patch and coordinate the validators.	No formal procedure.	No single formal procedure. Coordination among independent client teams required.	Yes	No formal procedure. The foundation team will implement a software patch and coordinate the SRs.	No formal procedure. The foundation team will implement a software patch and coordinate the validators.
Has the network undergone independent third-party security audits? Are upgrades tested on public testnets before deployment?	Upgrades are open-source and can be reviewed by the community. Most upgrades do not undergo formal audits. Upgrades are deployed on public testnets.	Upgrades are deployed on public testnets. One audit has been performed in 2025 over the smart contracts implementing Canton Coin. No other audit evidence was found.	Yes, upgrades are deployed on public testnets and independently audited for major client upgrades.	Upgrades are open-source and can be reviewed by the community and are also reviewed by third party auditors. Upgrades are deployed on public testnets.	Upgrades are open-source and can be reviewed by the community. One security assessment has been performed in 2024 over the java-tron client. No other audit evidence was found. Upgrades are	Upgrades are open-source and can be reviewed by the community. Most upgrades do not undergo formal audits; there have been formal reviews of major functionalities such as native smart

Control, Governance, and Concentration of Authority						
	BSC	**Canton**	**Ethereum**	**Solana**	**Tron**	**XRPL**
					deployed on public testnets.	contract primitives (i.e. lending or exchange-type applications). Upgrades are deployed on public testnets.
What are some theoretical ways for a single actor to take over the chain?	1. A supply chain attack that compromises the BSC client, impacting all validators. 2. Colluding with or compromising a majority of the 21 block-producing validators selected for a given epoch.	1. A supply chain attack that compromises the Splice client, impacting all validators and Super Validators. 2. Colluding with or compromising ⅔ of the Super Validators.	Requires compromising staking providers, client teams and governance processes.	1. A supply chain attack that compromises the majority client, impacting > ⅔ staked SOL. 2. Colluding with or compromising a superminority of validators.	1. A supply chain attack that compromises the java-tron client, impacting all validators. 2. Amassing sufficient TRX tokens, through either acquisition or collusion, in order to control at least 18 SRs.	1. A supply chain attack that compromises the rippled client, impacting all validators. 2. Compromising the XRPL Foundation or Ripple, as they control the Recommended Validator Lists and hence have significant influence over the network.

Continuity and Institutional Sustainability						
	BSC	**Canton**	**Ethereum**	**Solana**	**Tron**	**XRPL**
Do the primary governing or funding entities publish audited financial reports?	No public information.	No public information.	Partially. The foundation publishes annual reports and treasury policies.	No public information.	No public information.	No public information.
Do independent organizations contribute to core protocol development?	Concentrated in Binance-affiliated core team.	Concentrated in the Digital Asset-affiliated core team.	Multiple independent teams contribute to the clients. A public proposal process allows anyone to suggest protocol changes for community review.	Multiple independent teams contribute to the clients. A public proposal process allows anyone to suggest protocol changes for community review.	Outside contributions are rare, from independent developers.	Outside contributions are concentrated in XRPL-affiliated organizations.
Is there meaningful preparation for quantum computing risks?	No official public information. Although the chain can inherit the post-quantum upgrade of Ethereum.	Acknowledged as a concern.	Acknowledged as priority, actively researched, but no production features yet.	Exploring solutions, post quantum signatures deployed on a Solana Testnet.	No post-quantum migration plan or quantum-resistant features are currently in place.	No post-quantum migration plan or quantum-resistant features are currently in place. A project called AlphaNet, reportedly combining smart contracts with quantum-secure design, is in development, though public

Continuity and Institutional Sustainability						
	BSC	**Canton**	**Ethereum**	**Solana**	**Tron**	**XRPL**
						documentation remains limited.

Network Activity and Adoption						
	BSC	**Canton**	**Ethereum**	**Solana**	**Tron**	**XRPL**
Does the network support programmable smart contracts?	Yes	Yes	Yes	Yes	Yes	Limited general smart contract functionality and application adoption; several native primitives built into the rippled client.
What is the total value of assets deposited in the network's decentralized financial applications? *This measures assets actively deployed in lending, trading, and other on-chain financial protocols. It does not include stablecoins or tokens simply held in wallets.*	$6b	Not discernable due to the private nature of the chain.	$56b	$6.9B	$4.11b	$49m

Network Activity and Adoption						
	BSC	**Canton**	**Ethereum**	**Solana**	**Tron**	**XRPL**
What is the total value of stablecoins in the network?	~$14b	Not discernable due to the private nature of the chain.	~$159b	$15B	$86.1b	$413m
How many unique active addresses interact with the network on a monthly basis?	~53M	No publicly available data available	~13M	~ 50M	~14.2M	~490k
What is the total market capitalization of the network's native token?	~$89b	~$6B	~$257b	~$52B	~$27B	~$86B
What is the total current supply of the network's native token?	~136 million	~38 billion	~121 million	~622 million	~95 billion	~100 billion
What percentage of the native token supply is locked in securing the network?	~19%	Not applicable as network security is not based on economic stake.	~30%	~68%	~45%	Not applicable as network security is not based on economic stake.
Is transaction data public, private, or configurable?	Public, with privacy options through applications.	Private	Public, with privacy options through applications.	Public, with privacy options through applications.	Public, with privacy options in development. Companies can deploy their own private version (Tron Private Chain).	Public, with privacy options in development.
What types of applications or use cases dominate the	DeFi (primarily decentralized	Repo trading, digital bond issuance,	DeFi (lending, decentralized	DeFi (lending, decentralized	Stablecoin Transfers, DeFi,	Cross-border Payments,

Network Activity and Adoption						
	BSC	**Canton**	**Ethereum**	**Solana**	**Tron**	**XRPL**
network's activity?	exchanges and yield farming), stablecoin transfers, and meme token trading.	collateral management, tokenized real-world assets (bonds, money market funds, private equity), and stablecoin payments.	exchanges, liquid staking), stablecoins, and tokenized real-world assets	exchanges, liquid staking), stablecoins, memecoins, and tokenized real-world assets	Gaming and NFTs	Tokenized Real-World Assets and some DeFi, through native primitives.

Posture & Principal Risks

Ethereum

Ethereum has the longest uninterrupted operational track record among general-purpose smart-contract platforms, the highest estimated cost of attack through slashing-backed economic finality, meaningful client diversity in production, and transparent, distributed governance practices. It hosts the most mature ecosystem of decentralised finance and regulated institutional activity, with the broadest base of independent protocol development teams. The principal risk is not overt control of the network, but rather the possibility that subtler forms of concentration could erode the decentralisation that underpins its security model. This concern manifests across multiple layers simultaneously.

At the consensus layer, staking concentration is notable, but difficult to quantify. The staking landscape comprises liquid staking protocols, staking pools, centralised exchanges, and node operators with overlapping and often opaque relationships. These entities vary in governance structure, custody arrangements, and the degree of operational independence they afford to the underlying validators. As a result, the headline validator count may materially overstate the number of truly independent decision-makers.

At the block production layer, a separate and equally important concentration exists. The majority of blocks are assembled by a small number of specialised builders and routed through a handful of relays. Even with a distributed validator set, the practical control over which transactions are included in blocks, and in what order, is concentrated among a few entities. This has direct implications for censorship resistance and transaction fairness.

Additional considerations include the Foundation's ETH-denominated treasury, which introduces correlated funding risk, and increasing share of Ethereum's transaction activity has migrated to Layer 2 networks, which carry their own trust assumptions and are outside the scope of this assessment.

BSC (Binance Smart Chain)

BSC is an Ethereum-compatible smart contract platform, that offers fast finality and high throughput through a compact validator set and centralised development model. It hosts a sizable DeFi ecosystem and stablecoin supply, and its Ethereum compatibility has enabled broad application-layer adoption. The central risk characteristic of BSC is the concentration of influence within Binance and its affiliated entities across multiple dimensions of the network.

At the consensus layer, the validator set is structurally narrow: only 21 validators produce blocks in a given period, and disrupting liveness requires compromising just 8 of them. Of the 45 active validators, the top 21 by stake form the "Cabinet" forming a largely stable validator set over time, meaning a persistent group of validators exercises outsized influence over block production. Binance-affiliated teams maintain the sole production validator client, lead core protocol development, and the exchange operates or is closely associated with a significant share of the active validator set. Only self-bonded stake is subject to slashing, delegated stake faces no automatic penalty, which reduces the economic cost of a misbehaving validator. During the 2022 bridge exploit, the CEO of Binance publicly directed a chain halt, demonstrating that a single individual could influence the suspension of transaction processing.

At the block production layer, BSC has adopted a builder separation model in which a small number of specialised builders assemble the majority of blocks. The network's short block time imposes stringent latency requirements that raise the barrier to entry for competing builders, reinforcing this concentration structurally rather than as a transitional market condition.

BSC operates a single validator client, a fork of Ethereum's Geth client. A critical vulnerability in this codebase would affect the entire validator set simultaneously. No independent core protocol development ecosystem exists outside of Binance-affiliated teams. Post-incident disclosure has been partial, and no publicly audited financial reports are available for the foundation or its governing entities. The network's upgrade cadence is fast enabled by the single-team development model. While this allows rapid feature delivery and incident response, it also means protocol changes undergo shorter periods of public review and independent scrutiny.

Additional considerations include the network's continuity risk: if Binance or the BNB Chain Foundation ceased operations, the network's ability to continue functioning and evolving is uncertain, given the absence of independent teams capable of maintaining and upgrading the core protocol.

XRP Ledger

The XRP Ledger is one of the most established blockchain networks, with a relatively stable operational track record and deterministic finality that does not rely on economic stake, meaning consensus cannot be influenced through token acquisition. It hosts built-in financial primitives for cross-border payments and tokenised real-world assets. Although reportedly implemented through a 2025 launch of an EVM sidechain, general-purpose smart contract support is nascent and significantly less adopted than other chains. The principal risk is the concentration of governance and security around two entities, Ripple and the XRP Ledger Foundation, whose influence spans across validator inclusion, protocol development and ecosystem direction.

At the consensus layer, the network's security model depends on the Recommended Validator Lists published by Ripple and the XRPLF, which suggest which validators are trusted to participate in the network. This creates a structural dependency: a compromise, regulatory action, or cessation of either entity could materially impair the network's operation. Unlike stake-based networks, there are no economic penalties for validator misbehaviour - safety relies entirely on the social trust assumptions embedded in the validator selection process.

At the development and infrastructure layer, the network runs a single software client, meaning a single software vulnerability would affect every participant. No independent core protocol development ecosystem exists outside of XRPL-affiliated organisations.

Additional considerations include the lack of economic penalties for validator misbehaviour, and the concentration of the initial token supply. It is worth noting that the network has a nascent post-quantum security roadmap consisting of an experimental network called Alphanet.

Tron

Tron is an Ethereum-compatible smart-contract platform, with a relatively stable operational track record. Its dominant use case is stablecoin settlement, and general-purpose smart contract support enables straightforward application migration from other EVM-based networks. The principal risk is the concentration of governance, development, and validator coordination within the TRON Foundation, which has historically exercised significant influence across all dimensions of the network's operation.

At the consensus layer, 27 Super Representatives are elected through votes from TRX holders, but voting power is heavily concentrated - the top 10 stakers account for a substantial share of all votes, and some addresses are likely controlled by the same entity. In practice, the Super Representative set rarely changes composition. The network imposes no economic penalties for validator misbehaviour; the only consequence is potential loss of staker trust and subsequent non-election.

At the development and infrastructure layer, the network runs a single software client with no independently developed alternative in production. A critical vulnerability would affect every validator simultaneously. No independent core protocol development ecosystem exists outside of the TRON Foundation and affiliated entities. The network's first and only known third-party security assessment of its core client was conducted in 2024.

Additional considerations include the continuity risk: a cessation or regulatory action against the TRON Foundation could materially impair the network's operation, given the absence of independent teams capable of maintaining the core protocol. No post-quantum security roadmap has been identified.

Solana

Solana delivers high base-layer throughput and fast finality. It ranks second only to Ethereum by estimated cost of attack. Institutional adoption is broad, with several major financial institutions actively building on the network. The principal risks centre on operational reliability, concentration, and incomplete economic security.

At the consensus layer, in-protocol automatic slashing has historically been absent and is only now being introduced. The top 20 validators control a superminority of stake

sufficient to affect chain liveness, and the validator set has contracted significantly as foundation subsidies have wound down. Geographic concentration is notable, with the majority of validators hosted in three countries.

At the development and infrastructure layer, two client implementations exist, but the dominant client runs on approximately 90% of validators, leaving the network exposed to single-codebase risk in practice. Solana has the most troubled outage record of the six networks, with multiple full halts requiring manual off-chain coordination to recover. While the frequency of incidents has decreased, the historical pattern remains a concern for operational resilience.

Additional considerations include the absence of a post-quantum plan in production, and the Foundation does not publish audited financial reports.

Canton

Canton occupies a distinct position as the only permissioned (currently) and privacy-first blockchain in this assessment, purpose-built for regulated financial institutions. Its deterministic finality and transaction-level privacy align it closely with institutional financial use cases including repo trading, bond issuance, and collateral management. The principal risk is the concentration of the protocol development, and client maintenance, within a single entity, Digital Asset.

At the consensus layer, the Super Validator set is small, geographically concentrated, and self-governing - incumbents control who joins or leaves through a supermajority vote. Canton's security model relies on institutional trust rather than economic collateral: there is no staking, no slashing, and no financial penalty for misbehaviour.

At the development and infrastructure layer, the network runs a single software client. A supply-chain compromise could affect 100% of validators simultaneously. No independent development ecosystem exists, and the network's continuity is directly tied to Digital Asset's continued operation. Digital Asset authors all protocol upgrades, which are accepted by the Super Validators on recommendation of the Canton Foundation.

Additional considerations include the network's limited track record, with no public security audits for the client implementation, no bug bounty programme, and limited transparency into on-chain activity. Meaningful assessment of Canton's resilience and

governance maturity will require a longer operational history and greater disclosure than is available today.

Appendix

Glossary

- **Block Builders** - Firms or operators that run specialised software to assemble the contents of a block, selecting which transactions to include and in what order, and submit the completed block to validators for proposal. Distinct from validators, who sign and propose blocks but may not determine their contents.
- **Block Producers** - Nodes responsible for creating new blocks and adding them to the chain. May be called validators, miners, or Super Representatives depending on the network.
- **BNB** - The native token of BNB Smart Chain, used to pay transaction fees and participate in staking.
- **BNB Chain Foundation** - The organization responsible for the development and governance of BNB Smart Chain.
- **Canton Coin (CC) -** The native utility token of the Canton Network's Global Synchronizer, earned by validators and app providers for contributing to the network, with no pre-sale or pre-mine.
- **Canton Foundation** - An independent, non-profit body under the Linux Foundation that governs the Canton Network's Global Synchronizer.
- **Client (Execution / Consensus)** - Software that allows a node to participate in a blockchain. Some networks split this into an *execution client* (processes transactions) and a *consensus client* (handles finalization). Multiple independent client implementations reduce the risk of a single bug affecting the whole network.
- **Consensus Mechanisms** - The set of rules by which a blockchain network agrees on which transactions are valid, in what order, and when that record becomes final.
    - **Canton's two-tier consensus mechanism** - The Canton Network employs a two-tier consensus mechanism: a 2/3 majority Byzantine Fault Tolerant (BFT) consensus protocol run by Super Validators on the Global

Synchronizer for message ordering and confirmation, combined with a "proof-of-stakeholder" model where only the validators involved in a given transaction are responsible for validating it.

- **Delegated Proof-of-Stake (DPoS)** - A consensus mechanism where token holders elect a fixed number of representatives to produce blocks on their behalf. Enables high throughput but concentrates validation among a small elected group.
- **Proof-of-Stake (Gasper)** - A consensus mechanism where validators deposit 32 ETH as collateral and are selected to propose and confirm blocks. Finality requires ≥⅔ of staked ETH to agree on two consecutive checkpoints (~13 minutes). Misbehaving validators lose their stake ("slashing").
  - **Inactivity Leak** - A penalty mechanism in Ethereum 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.
- **Proof of Stake (augmented with Proof of History)** - A consensus mechanism in which proof-of-stake validators secure the network and finalize blocks, while Proof of History, a chain of sequential SHA-256 hashes, acts as a cryptographic clock that timestamps transactions and establishes their order without requiring validators to communicate back and forth, enabling high throughput.
- **Proof-of-Staked-Authority** - A consensus mechanism combining staking with authority-based validation. The top 45 validators by staked BNB are elected daily; the top 21 take turns producing blocks. Finality within 1–2 seconds. Only validators' self-delegated BNB is subject to slashing.
- **XRPL Consensus Protocol** - XRP Ledger's consensus mechanism. Validators iteratively exchange and compare proposed transaction sets until a supermajority (≥80%) agree. No mining or staking involved.

- **DAO (Decentralized Autonomous Organization)** - An organization governed by smart contracts rather than a central authority. Members vote on decisions using governance tokens.
- **Deterministic Finality** - Transactions are irreversible once a defined agreement threshold is reached. If validators cannot agree, the network halts rather than produce conflicting records.
- **Digital Asset -** The technology company that developed the Daml smart contract language and the Canton protocol, backed by investors including Citadel Securities, DTCC, and DRW.
- **Economic Finality** - A protocol-defined point after which reversal requires destroying a quantifiable amount of staked value. The protocol enforces penalties (slashing) on any validator that attempts to finalize conflicting records.
- **Epoch** - A fixed time window used to organize blockchain operations such as validator rotations or reward distribution. Often composed of multiple slots.
- **ETH (Ether)** - The native token of the Ethereum blockchain, used to pay transaction fees, participate in staking, and secure the network.
- **Ethereum Foundation** - A non-profit organization that supports the research, development, and long-term sustainability of the Ethereum protocol.
- **EVM (Ethereum Virtual Machine)** - The standardised execution environment that processes smart contracts on Ethereum. Other blockchains have adopted EVM compatibility, meaning they can run the same smart contract code as Ethereum and, in principle, inherit technical upgrades developed for Ethereum, including future cryptographic improvements.
- **Global Synchronizer** - The decentralized, permissionless synchronization domain of the Canton Network, operated by Super Validators using BFT consensus, that sequences and coordinates transactions across otherwise independent sync domains.

- **ICO (Initial Coin Offering)** - A fundraising method where a project sells new tokens to early investors before launch. Widespread in 2017–2018 but drew heavy regulatory scrutiny for often involving unregistered securities.
- **Liquid Staking** - Staking tokens while receiving a tradeable receipt token in return. Solves the illiquidity of traditional staking by allowing staked assets to still be used in DeFi.
- **Liveness** - A network's ability to continue processing new transactions without interruption. A network that has stopped producing blocks has lost liveness.
- **Maximal Extractable Value (MEV)** - The additional profit that can be earned by controlling the order, inclusion, or exclusion of transactions within a block. MEV is a key driver of block builder concentration, as builders compete to assemble the most profitable blocks.
- **Post-Quantum / Quantum Computing Risk** - Future quantum computers may be powerful enough to break the cryptographic techniques that currently secure blockchain transactions. Post-quantum readiness refers to whether a network has begun adapting its security foundations in anticipation of this risk. It is a longer-term rather than immediate concern, but nevertheless critical.
- **Probabilistic Finality** - No protocol-defined point of finality. Transactions become increasingly difficult to reverse as more blocks are built on top, but the protocol never declares them irreversible.
- **Proposer-Builder Separation (PBS)** - An architecture that splits block production into two roles: builders assemble block contents, and proposers (validators) select and sign the most profitable block offered. Designed to prevent validators from needing to engage in transaction ordering strategies themselves.
- **Recommended Validator Lists** - Lists of trusted validators published by Ripple and the XRP Ledger Foundation that most network participants use by default.
- **RWA (Real-World Asset)** - A traditional asset (real estate, bonds, commodities) tokenized and represented on a blockchain, bridging traditional finance and DeFi.

- **Self-Bonded / Self-Delegation / Delegation** - *Self-bonding* is a validator locking their own tokens as collateral. *Delegation* is token holders assigning their stake to a validator without running a node themselves.
- **Slashing** - The concept of automatic financial penalties for misbehaviour.
- **Slot** - The smallest unit of scheduled time in which one designated validator is expected to produce a block. Missed slots are skipped. Slots are typically grouped into epochs.
- **Solana Foundation -** The non-profit organization that supports the development, decentralization, and adoption of the Solana blockchain network.
- **SOL -** The native token of the Solana blockchain, used to pay transaction fees, participate in staking, and secure the network through its proof-of-stake consensus mechanism.
- **Super Validator -** An enhanced Canton Network node that combines validator functionality with a Global Synchronizer node, responsible for validating Canton Coin transfers and providing core network services like transaction ordering.
- **Supply Chain Attack** - Rather than attacking a network directly, an attacker compromises the software that participants rely on - in this context, the validator client. If malicious code were introduced into this software, every validator running it could be affected simultaneously. Networks that rely on a single software client are particularly exposed, as there is no diversity of implementations to contain the impact.
- **TRON Foundation** - The organization responsible for the development, maintenance, and coordination of the TRON blockchain.
- **Tron SuperRepresentative (SR)** - One of 27 elected nodes in TRON responsible for block production and governance. Elected by TRX holders and rotated in round-robin order.
- **Total Value Secured (TVS)** - The total value of assets a network protects through its consensus mechanism. Higher TVS implies a greater economic cost for an attacker to compromise the network.

- **TRX (Tronix)** - The native token of the TRON blockchain, used to pay for network resources, vote for Super Representatives, and participate in DeFi.
- **UNL (Unique Node List)** - An XRP Ledger concept. Each validator maintains a personal list of trusted validators whose votes it considers for consensus. Overlap between different nodes' UNLs is critical to network-wide consistency.
- **Validators / Validator Set** - Nodes that verify transactions and vote on new blocks. The *validator set* is the full group of active validators at any given time.
- **Vote Transactions** - Vote transactions are consensus messages that validators submit to confirm they agree on the current state of the blockchain, and because they typically account for a large portion (historically around 50-70%) of Solana's total transaction count, the "true TPS" of actual user transactions is significantly lower than the headline TPS figure that Solana reports.
- **XRP** - The native token of the XRP Ledger, used to pay transaction fees and as a bridge currency for cross-border payments. XRP holdings do not confer voting rights or influence over consensus.
- **XRPLF (XRP Ledger Foundation)** - An independent non-profit supporting XRP Ledger development and adoption.

Data Sources & References

DefiLlama: metrics on Total Value Locked, Stablecoins and Native Token Market Capitalization

CoinmarketCap: metrics on Token Price, Supply and Market Capitalization.

Ethereum

- Etherscan: Genesis Block, Accounts, Node Tracker

- Ethereum.org: Ethereum.org: Consensus Mechanisms, Ethereum Forks, Bug Bounty
- Ethereum Blog: EF Treasury Policy, Geth Security Release
- Ethereum.foundation: 2024 Report
- ClientDiversity.org
- BeaconCha.in
- EtherNodes.org
- EthStaker.org
- Dune Dashboard ETH Staking
- CryptoQuant Staking Metrics
- Go-ethereum Repository: Post Mortem, Audits
- Reth Repository
- Nethermind Repository
- Besu Repository
- Erigon Repository
- Lighthouse Repository
- Lodestar Repository
- Offchain Labs Post Mortem Medium Article
- EthResear.ch Incident Analysis
- ProbeLab Dashboard
- Who Wins Ethereum Block Building Auctions and Why?
- TokenTerminal: Monthly Active Addresses, Transactions per Second

BSC (Binance Smart Chain)

- Bscscan: Block 21962149, Block 21962150
- BnbChain.org: Overview, Staking Overview, BNB Staking, Governance Overview, Tech Roadmap 2026, Ecosystem Update, Running Validators, Blog on keeping Validators Active, Reth Client Development, Block-Proposer-Separation, Chain Governance Upgrades, Slash Rules
- BSC Client Repository: Contributors, Releases
- BNB ICO: [1] [2]
- X posts: BnbChain Status, CZ posts [1] [2]
- Reddit posts: Incident Analysis
- Nansen Vulnerability Analysis
- PurpleSec Breach Report
- BSC Validators
- MEV in Binance Builder
- TokenTerminal: Monthly Active Addresses, Transactions per Second

XRP Ledger

- XRPL Developer Documentation: Test and Dev Networks, Recommended Validator Lists, Consensus Protocol, Finality of Results,
- Longest Lasting Incident and Resolution
- XRPL Blog for Vulnerability Disclosures.
- Self-hosted Bug Bounty, Ripple Attackathon
- Mention of Alphanet Test Network

- Validator Client and Contributors, List of rippled Releases
- Monthly Active Addresses
- Transactions per Second Metrics in the Last Month

Tron

- Tron Developer Documentation: Test Networks, Consensus Protocol and Programming Language Capabilities
- Announcement by TRON Founder of Network Halt Due to Smart Contract Attack
- Tron DAO Bug Bounty Program
- Tronscan Voting, Top Stakers and Current Super Representatives
- Validator Client and Contributors
- Monthly Active Addresses

Solana

- Solana Liquid Staking Yields Ranked
- Solana Compass
- Solana Staking Overview
- Orb Markets
- Helius Blog: Alpenglow, Complete History of Solana Outages, Solana Governance, Bringing Slashing to Solana
- Solana Validators Overview
- Solana Beach

- Solana Status
- Anza Blog: SIMD-0204: The First Step to Slashing on Solana, SIMD-0212: Slashing on Solana
- Solana Improvement Documents (SIMDs)
- Firedancer Validator Client Repository
- Jump Crypto
- Hetzner Blocks Access for Solana Validators (November 2022)
- Token Terminal
- Validators App
- Solana Foundation on Post Quantum Signatures on Testnet
- FireDancer Bug Bounty
- JitoSolana Bug Bounty
- Solana Tokenomics Deep Dive
- History of Solana Medium Article
- December 2020 Mainnet Beta Stall
- September 2021 Network Outage Initial Overview
- April 2022 Mainnet Beta Outage Report and Mitigation
- June 2022 Mainnet Beta Outage Report
- September 2022 Mainnet Beta Outage Report
- February 2023 Mainnet Beta Outage Report
- Solana Outage Caused by a Previously Identified Bug (Blockworks)
-

Canton Network

- Canton Network White Paper
- A Technical Primer to the Canton network
- Canton Foundation
- Validation Application Form
- Digital Asset Trust Center
- Global Synchronizer Documentation
- The TIE's Canton Network Series (Part 2 of 5)
- Canton Coin: A Responsible Approach to Digital Tokens
- Canton Scan Super Validators
- Canton Data Analytics Dashboard
- Digital Asset Platform Documentation
- Daml SDK Documentation
- Global Synchronizer Architecture
- Splice Disaster Recovery Documentation
- Splice GitHub
- Canton Foundation CIPs (Canton Improvement Proposals)
- Daml SDK Documentation

Legal

This report and any related materials are provided solely for general informational and educational purposes. This report reflects our analysis, opinions, and judgments as of the date of publication, based on the information, data, assumptions, methodologies, and evaluation criteria described in this report or otherwise applied by us in preparing the relevant materials. The analysis, opinions, and judgments in this report may involve qualitative and quantitative assessments, methodological choices, assumptions, estimates, and weighting decisions. Different inputs, assumptions, methodologies, or evaluative frameworks may produce different results, comparisons, rankings, or conclusions.

We may rely on public information, third-party information, data sets, software tools, testing environments, and other source materials that we believe to be reliable, but we do not represent or warrant that any such information or materials are accurate, complete, current, independently verified, or fit for any particular purpose. We have not independently verified all facts, statements, code, metrics, network conditions, governance arrangements, security properties, performance data, or other third-party materials referenced, tested, summarized, or relied on in this report or any related materials.

No content (including analyses within the report, data, formulas, code, software or other information) or any part thereof may be modified, reverse engineered, reproduced or distributed in any form by any means, without the prior written permission of Zeppelin Group Ltd or its affiliates.

This report and any related materials do not constitute legal, regulatory, compliance, financial, investment, tax, accounting, technical, cybersecurity, commercial, or other professional advice. This report and any related materials do not constitute, and should not be construed as, a recommendation, solicitation, endorsement, certification, guarantee, insurance, audit opinion, fairness opinion, legal opinion, or approval of any blockchain, protocol, network, digital asset, validator set, governance framework, software implementation, product, service, person, or entity. No statement in this report or any related materials should be interpreted as a conclusion that any blockchain,

protocol, network, or related participant satisfies any legal, regulatory, supervisory, enforcement, listing, fiduciary, disclosure, compliance, risk management, or duty-of-care standard.

Any discussion of risk characteristics, resilience, decentralization, security, performance, reliability, governance, fault tolerance, economic design, or similar attributes is inherently judgment-based, context-dependent, and subject to change. Blockchain networks and related ecosystems are dynamic. Code bases, governance processes, validator or operator composition, network usage, incentives, market structure, security assumptions, third-party dependencies, legal treatment, and regulatory expectations may change materially over time, including after publication. As a result, any findings, comparisons, rankings, or conclusions in this report or any related materials may become outdated, incomplete, or inaccurate. We undertake no duty or obligation to update, revise, correct, monitor, or supplement this report or any related materials for any subsequent event, change in facts, change in methodology, change in law or regulation, technological development, market development, security incident, or other changed circumstance.

This report and any related materials are not intended to serve as the basis for any decision of any kind, including any legal, regulatory, enforcement, supervisory, compliance, policy, commercial, investment, technical, governance, or operational decision. No person or entity, including any regulator, governmental authority, court, legislative body, self-regulatory organization, exchange, market participant, media organization, investor, user, or other third party, may rely on this report or any related materials for any purpose. Any use of, reference to, or reliance on this report or any related materials is solely at the user's own risk.

A report or related materials may be commissioned, funded, or sponsored by a client or other third party. Any such engagement, funding, or sponsorship does not by itself imply that any governmental authority, regulator, or other third party should treat the report or related materials as neutral, independent, verified, or free from client-selected scope, assumptions, or objectives. Unless expressly stated otherwise, any conclusions expressed are ours alone as of the publication date.

References to third-party names, marks, protocols, products, services, publications, or statements are for identification and discussion purposes only. Those references do not imply affiliation with, endorsement by, or endorsement of any third party unless expressly stated otherwise in writing.

To the fullest extent permitted by law, we disclaim any and all liability, responsibility, and duty of care arising out of or in connection with this report and any related materials, including any use of, reference to, publication of, distribution of, or reliance on this report or any related materials by any person or entity. All information contained herein is provided “AS IS” without warranty of any kind, express or implied, including those related to accuracy, timeliness, completeness, merchantability or fitness for any particular purpose.

For purposes of this disclaimer, “related materials” includes any presentation, slide deck, summary, abstract, excerpt, interview, testimony, white paper, blog post, article, marketing material, social media post, dataset, model output, visualization, oral statement, or other content derived from, based on, summarizing, or referring to this report.