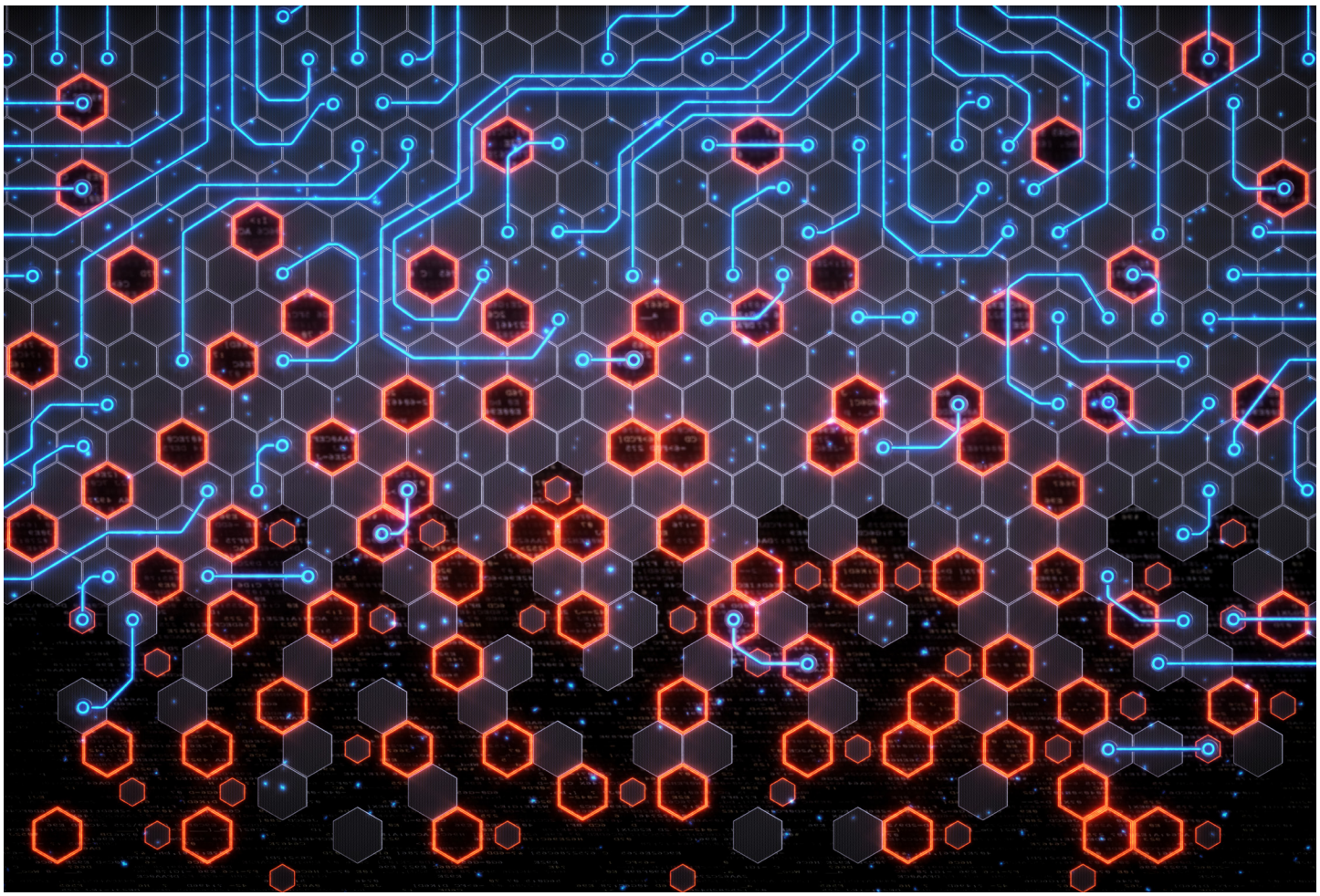
S&P Global

What Can You Trust in a Trustless System

Public Blockchains for Financial Applications

October 2023



This is a thought leadership report issued by S&P Global with contributions from S&P Global Ratings. It neither addresses views about ratings on individual entities nor is a rating action.

Authors

Andrew O'Neill, CFA | Lisa Schroeer | Florent Stiel | Patrick Sun | Matta Uma Maheswara Reddy | Miya Wen, CFA

Contributors

Ellen Jensen | Denise Grazette | Rameez Ali | Joseph William Reyes

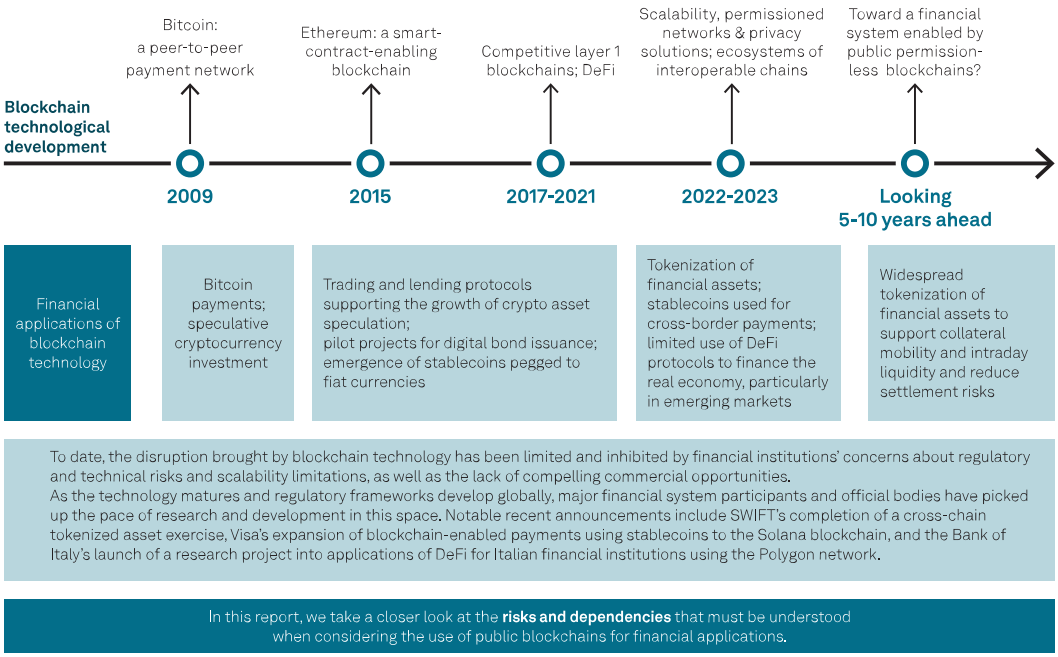
Table of contents

Key Takeaways

- Technological improvements supporting scalability, permissioned networks and privacy may address the main inhibitors to the adoption of public permissionless blockchains by financial institutions, with several regulators and official bodies experimenting with the technology.
- Although decentralization in public permissionless blockchains reduces reliance on intermediaries in the traditional sense, these blockchains still include material trust assumptions and dependencies. Understanding these risks is key to a successful use of the technology.
- In this report, we take a deep dive into three blockchain examples: Ethereum, Polygon and Solana. We look at how they work, what could go wrong and where dependencies lie, how they mitigate risk, how they are governed, and the opportunities they provide and risks they bring due to technological advancements.
- The Ethereum and Polygon networks are developing an ecosystem of scalable blockchains secured by emerging technology, including "zero knowledge" proofs. This has already led to major shifts within decentralized finance markets and may also support the growth of traditional financial use cases.

Introduction

Blockchain technology evolution may support its use in traditional financial systems



DeFi = decentralized finance.
Source: S&P Global Ratings.

This report follows How DeFi's Operational Risks Could Influence Credit Quality, (published June 7, 2023), in which we explored the range of operational risks that can arise in decentralized finance (DeFi) applications. In this report, we take a deep dive into blockchain-specific risks. It is worth noting that operational risks exist in traditional financial infrastructure. (See Operational Resilience Is Key To Global FMIs' Rating Strength, Chart 5, "Outages Are Common For Global FMIs.") What is new in blockchain technology is how these risks can materialize and how they can be remedied or avoided.

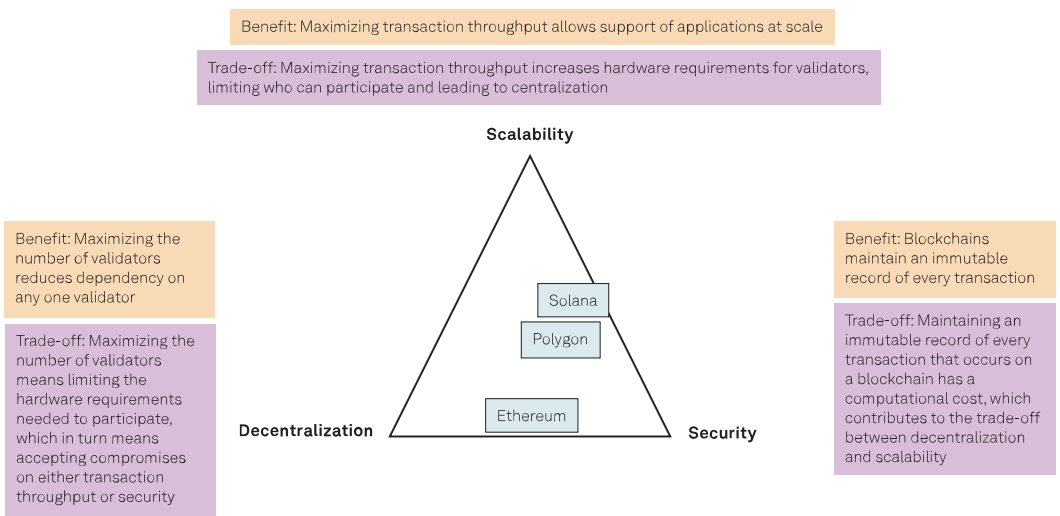
This report focuses on three examples of blockchains that are prominent in DeFi and have supported recent use cases that interact with the traditional financial system: Ethereum, Polygon and Solana. We highlight that although decentralization may reduce the presence of intermediaries, blockchains still include material trust assumptions and dependencies. Currently, blockchain operational risks do not affect ratings, as rated issuers have only started dipping their toes in the water. As use cases for public blockchains begin to expand through the financial system, it is important to understand where dependencies lie, and what can go wrong and how, to effectively mitigate these risks. We also explore the direction of these blockchains, including the impact of zero-knowledge (ZK) proof technology. We include a glossary of technical terms and related research at the end of this report.

The blockchain design trilemma

In this report, we take a deep dive into the following three blockchains:

- **Ethereum** is the blockchain with the largest DeFi ecosystem. Its initial design has prioritized decentralization and security at the cost of scalability. Specifically, decentralization is made possible by minimizing the hardware requirements to participate as a validator in the network, allowing many individuals to participate. However, minimizing hardware requirements involves limiting the number of transactions that can be processed in each block, hindering scalability. Ethereum uses a "proof of stake" (PoS) consensus mechanism (see next section). Its Ethereum virtual machine (EVM) provides the bedrock for a growing ecosystem of scalability-focused blockchain solutions compatible with the main Ethereum chain (Ethereum mainnet).
- **Polygon PoS** is a sidechain to Ethereum, meaning that it is a separate blockchain that is compatible with the EVM and connected to the Ethereum mainnet through a two-way bridge. It aims to increase scalability relative to the Ethereum mainnet while benefiting from some, but not all, of Ethereum's decentralization and security. It uses a PoS mechanism that is similar to but separate from Ethereum's.
- **Solana** is designed to prioritize scalability and security at the expense of some centralization. Specifically, and in contrast with Ethereum, it prioritizes high-transaction throughput, increasing the hardware requirements for validators to a point where currently only professional operators can participate. Whereas Polygon aims to develop within the Ethereum ecosystem, Solana aims to develop a separate ecosystem. Solana uses a "proof of history" mechanism, which is a modified PoS consensus mechanism that allows parallel validation by timestamping transactions and enhances transaction throughput.

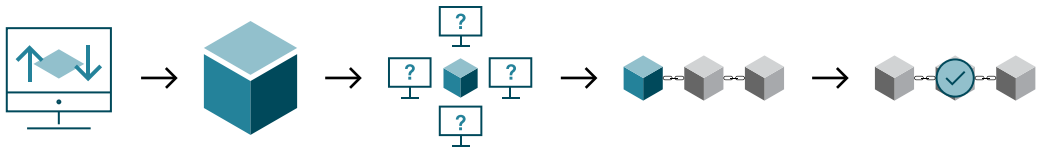
The blockchain design trilemma



Source: S&P Global Ratings.

How blockchains work: Achieving consensus and finality

Simplified blockchain process



An exchange is requested (e.g., general data, digital assets etc.)

The requested exchange is added to a "block", grouping it with other recent requested exchanges

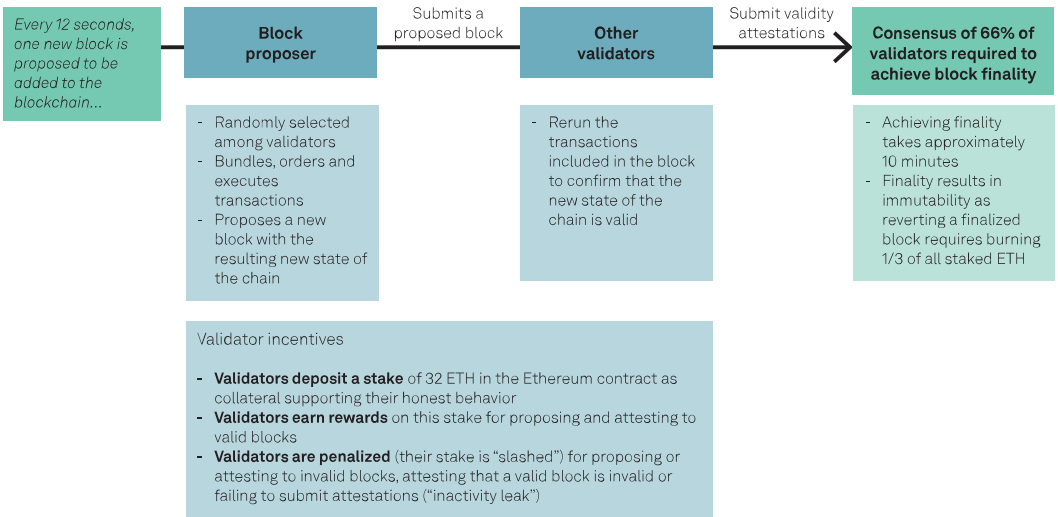
Network nodes validate the block of requested exchanges for a reward

Validated blocks are added to the blockchain

The exchange is complete, with an immutable digital record on the blockchain

Source: S&P Global Ratings.

Proof-of-stake consensus mechanism - Ethereum example



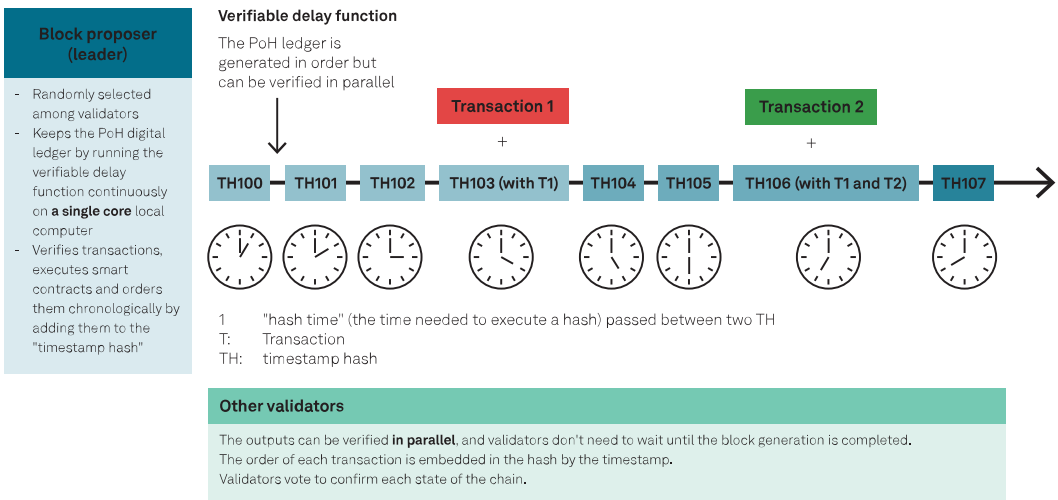
ETH = ether, Ethereum cryptocurrency.
Source: ethereum.org.

Polygon PoS' consensus mechanism is similar to Ethereum's and is connected to the Ethereum mainnet. Like Ethereum, the consensus for finality is two-thirds of the validators. There is a smart contract stored on the Ethereum mainnet to interact with Polygon validators. These smart contracts address the issues of staking management, delegation of validator shares and checkpoints. The PoS layer for Polygon is the validator layer where all blocks since the last checkpoint are validated and then coded to be stored on the Ethereum mainnet. The block-producing layer where individual transactions are aggregated into blocks is all EVM-compatible, allowing for the final blocks to be stored on the Ethereum mainnet. For more information, please see https://wiki.polygon.technology/docs/pos/what-is-polygon-pos/.

Validators stake Polygon's native token, MATIC, to participate in the network. Polygon PoS selects block producers and checkpoint proposers among validators based on their stake ratio, including delegations. Rewards are given to all validators at every checkpoint according to their stake ratio. Validators can leave the network at any time and withdraw their tokens at the end of an unbonding period.

Solana uses a proof-of-history (PoH) mechanism, which is a modified PoS consensus mechanism that allows parallel validation by timestamping transactions and thus enhancing transaction throughput. With PoH, a block proposer uses a verifiable delay function to keep the PoH digital ledger and encrypt timestamps for each transaction, providing a verifiable and permissionless source of time. This technique enhances the platform's throughput by allowing nodes to review blocks without reviewing the entire chain and enabling parallel processing of transactions. The PoH mechanism, combined with other innovative features, allows Solana to achieve scalability with low transaction fees.

Proof-of-history consensus mechanism – Solana example



PoH = Proof of history.
Sources: https://www.youtube.com/watch?v=A5G_FJpzKtk&list=PLWU8l3JVbM63FUgisq9-XtIg1bnGnrNES; https://medium.com/solana-labs/proof-of-history-explained-by-a-water-clock-e682183417b8; https://solana.com/solana-whitepaper.pdf.

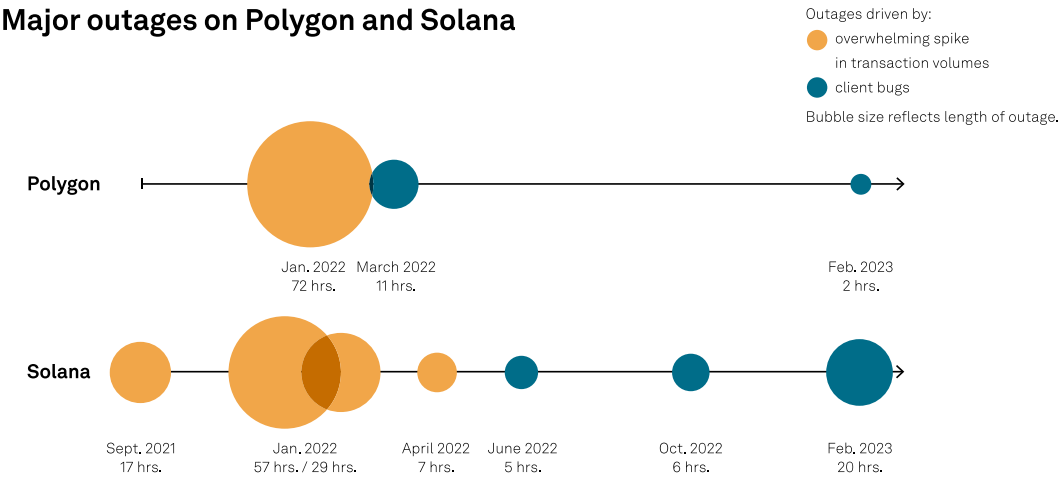
Blockchain security

Liveness versus security bias

A fundamental design choice when building a blockchain is how it will behave in the event of an accidental or malevolent security event. Ethereum has a "liveness biased" design intended to avoid any outage from the user's perspective. Indeed, to date, Ethereum has not experienced such an outage per se: Risks arise, rather, in the form of delayed finality (that is, a delay before new blocks become immutable (see sidebar "Ethereum's delayed finality event in May 2023" in next section). In contrast, Solana and Polygon are "security biased" blockchains: If a bug or attack prevents achieving consensus, these blockchains may experience an outage (that is, users will not be able to transact) while the security risk is addressed.

The timeline below illustrates the major outages on Polygon and Solana. Outages have occurred mainly when high network demand has stretched validator resources or triggered bugs in the client software used to validate the network. In some cases, high network demand has resulted from a distributed denial-of-service cyberattack: Low transaction costs enabled attackers to flood these blockchains with transactions. Both platforms have implemented modifications to their transaction fee structure to reduce vulnerability to such attacks. Solana has also increased its number of validators, whereas Polygon aims to achieve this as part of its "Polygon 2.0" proposal (described later in this report).

Major outages on Polygon and Solana



Data compiled September 2023.
Source: Public reports.

Blockchain cyberrisks — Ethereum example

Public blockchains mitigate cyberrisk through decentralization: In the absence of a centralized node operator, it is very difficult for an attacker to control or shut down the network (see Cyber Brief: Reviewing the Credit Aspects of Blockchain, published May 5, 2022). In the chart below, we illustrate the example of Ethereum and how its proof-of-stake consensus mechanism addresses cyberrisk. An attacker's ability to influence the network is directly related to the share of validator nodes that it controls and, therefore, to the volume of ETH the attacker has staked. The key defense mechanisms inhibiting any attack include:

- The cost of accumulating a stake large enough to launch an attack, against the near certainty that substantially all of this stake will be lost if the attack is successful.
- Slashing mechanisms to reduce the stake of validators that are behaving dishonestly.
- "Social" defense mechanisms: Honest validators can withhold consensus attestations on the chain and create a minority fork, to which all economic activity can migrate (see the chart "Governance and social layer" in the next section).

– In addition to the cost, it is difficult to accumulate such a proportion of control because there is a waiting time to activate new validators, and any stake accumulation is highly visible on-chain, making it difficult to reenter following an initial attack.

– The impossibility of creating invalid states of the chain: Even with control over a large share of validator nodes, there are limits to what an attacker can actually gain through "rewriting history" on the chain.

– The mitigation of "long-range reorg attacks" through regular validator checkpoints through time. This type of attack involves a validator that participated in the genesis of the chain, maintaining a separate chain until at some later point it attempts to have this separate chain accepted by validators as the legitimate chain. Simply put, validator checkpoints mitigate this risk because the consensus mechanism cannot be used to accept an alternative chain prior to the latest checkpoint. The risk of attack is, therefore, limited to "short range" and focused on the most recent blocks.

Risk of cyberattack on Ethereum

Less risk → More risk

Attacker's stake	What an attacker can do with this stake	Cost to the attacker to accumulate this stake*	Probability of successful attack given this stake	Potential impact of a successful attack on the chain
Low	**Denial-of-service attack on the next proposer:** The attacker may prevent the selected node from proposing a block in that slot (possible as the next proposer is determined based on a public function).	Low cost > high risk	Low	Low
Over 33%	**Delayed finality:** The attacker may prevent reaching 66% validator consensus by withholding attestations. Its stake would gradually be slashed, and the attack would end once it fell back below 33% and remaining honest validators could reach consensus.	$14.7 billion	High	Depends on the length of delay
	Double finality: The attacker could attest to two competing blocks in the same slot, resulting in a split of the chain into two forks. A successful attack would require sophistication and luck. The attacker would see its full stake slashed on one of the chains, which would then likely be agreed as the main chain by remaining honest validators.		Low	High
Over 50%	**Control over non-finalized blocks only:** The attacker could reorder blocks or transactions within these blocks to extract economic rent. The attacker could also censor transactions.	$22.0 billion	High	High
Over 66%	**Finality reversion:** The attacker could reorder blocks or transactions and censor transactions on finalized blocks as well. It would control the network going forward. In this scenario, it is likely that economic activity on the Ethereum blockchain would largely cease, the value of ETH (and therefore of the attacker's stake) would fall toward zero, and centralized exchanges would not support the attacker off-ramping from the Ethereum blockchain to fiat.	$29.4 billion	Very high	Very high

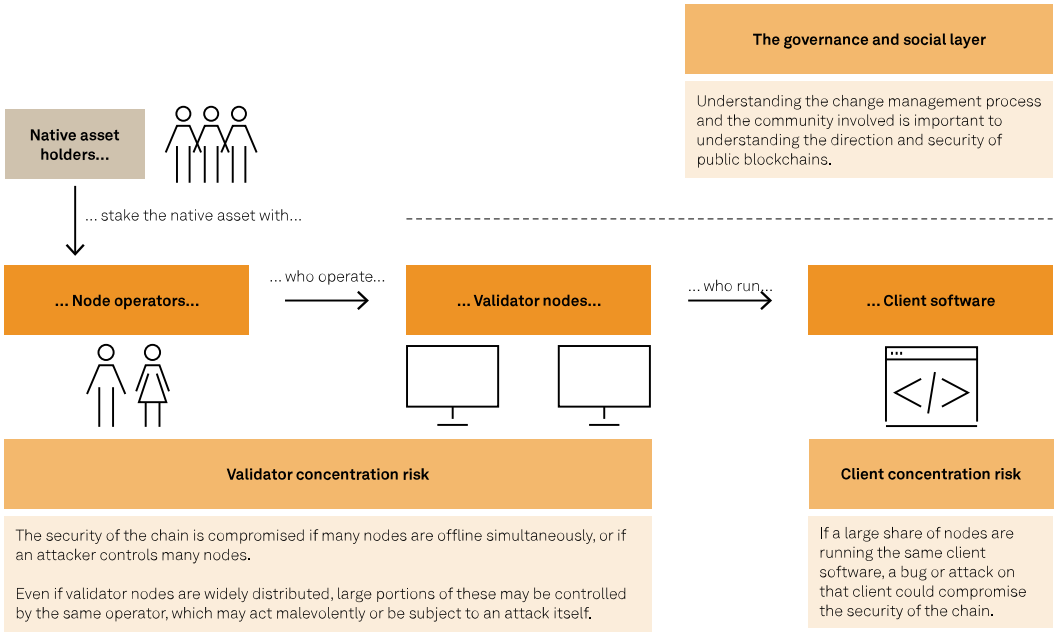
As of Oct. 9, 2023.
* Based on the price of ETH and volume staked.
Sources: Ethereum proof-of-stake attack and defense; ethereum.org; Dune (@hildobby).

Ethereum's defense mechanisms have prevented any significantly impactful cyberattack on the network to date. It is important to note, however, that the risk of a "zero-day" event can never be entirely excluded.

Blockchain risk dependencies

Although decentralization may reduce the presence of intermediaries, blockchains still include material trust assumptions and dependencies. As highlighted in the previous section, the consensus mechanism that underpins a blockchain's security requires the continuous participation of a sufficient number of honest validators. It can also be halted or delayed, in particular by bugs in client software. Here we take a look at various forms of concentration risk within the validator network for these blockchains, and also at dependencies within their governance structure.

Understanding a PoS/PoH blockchain's risk ecosystem

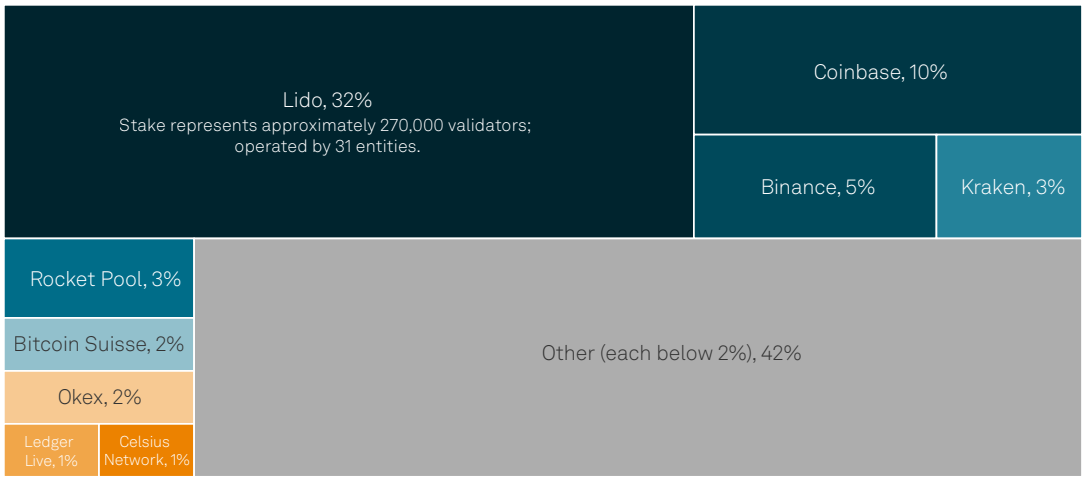


PoS = proof of state; PoH = proof of history.
Source: S&P Global Ratings.

Validator concentration risk

Validator nodes control a blockchain's consensus mechanism. As discussed in the prior section, dishonest or inactive validator nodes can compromise the security of a blockchain; therefore, concentration of validator nodes represents a security risk. Of the three examples considered in this report, Ethereum's design is the most focused on decentralization, with more than 800,000 validators. In contrast, Solana has approximately 2,000 validators, and Polygon's maximum validator count is set at 100. Even if validator nodes are widely distributed, multiple validator nodes may be operated by the same entity: The chart below illustrates how even Ethereum can, therefore, be exposed to concentration risk. A node operator could act malevolently or in a way that is detrimental to the network's interests. Further, it may itself be subject to technological risks or attacks. Concentration at the node operator level can, therefore, create risks to the consensus mechanism even in a highly decentralized network.

Ethereum: Share of validator nodes



Data compiled Oct. 9, 2023.
Source: Rated (www.rated.network).

Is Ethereum's Lido concentration a concern?

An attacker's ability to affect Ethereum's consensus mechanism grows in proportion to the share of validator nodes it controls, and the first material threshold is 33% of nodes (see the chart "Risk of cyberattack on Ethereum"). Lido is approaching this threshold (see the chart "Ethereum — share of validator nodes"). It is, therefore, important to understand the risk this could represent to Ethereum:

- Lido is a decentralized staking protocol, allowing ETH holders to stake, and earn staking yield, through the protocol without the operational burden of running a node themselves, or the need to have the 32 ETH required to stake to run a node. Lido's share, therefore, represents the stake of approximately 270,000 that are able to withdraw from the protocol (thereby reducing Lido's share) if there is a concern with the direction of the protocol.
- The nodes controlled by the Lido protocol are operated by 31 entities, reducing rogue operator risk, with a distribution of consensus clients (see next section) that is consistent with that of the network overall. The protocol governance mechanism selects the node operators and can dismiss them if a concern emerges. The operators can also leave the protocol; however, the stake belongs to the protocol, so this would not reduce Lido's share.
- Viewing Lido as a single point of failure risk is, therefore, an oversimplification. Nonetheless, the concentration risk remains relevant because decisions taken by the Lido protocol governance (which is controlled by holders of the native token, LDO) could plausibly have an impact on Ethereum. Lido's share of validators is on a continuous upward trend, so understanding evolutions in its governance is important to understanding risks on Ethereum.

Client concentration risk

"Clients" are the software packages that each validator node is running to execute transactions, validate the proposed block and send attestations of its validity. A bug in or an attack on this client software could take validators offline and compromise the consensus mechanism: If there are insufficient validators to provide consensus, new blocks cannot be finalized and, therefore, do not achieve immutability. This occurred on Ethereum in May 2023 (see sidebar "When client risk materializes: Ethereum's delayed finality event in May 2023). Client diversification is a stated aim of the blockchains addressed in this report: Different software packages are built by different companies, to the same specification, but using different coding languages and structures. This builds some redundancy into a blockchain's consensus mechanism because a bug affecting one client would only affect the validators using that client software. The risk that such a bug could delay block finality is a function of client concentration risk: If there is sufficient diversification of clients, a client issue will not in itself affect sufficient validators to prevent finality.

Client diversification is generally improving over time as new clients emerge; however, material concentrations remain. All three blockchains discussed in this report are exposed to client concentrations that exceed the 33% threshold that can lead to finality issues (see the chart "Risk of cyberattack on Ethereum"). Having launched more recently, Solana and Polygon both have higher client concentration than Ethereum; therefore, if a client bug arises, it is more likely to disrupt these blockchains (see the chart "Major outages on Polygon and Solana"). Currently, there are two available clients for use on the Solana blockchain, although the development of new clients is underway.

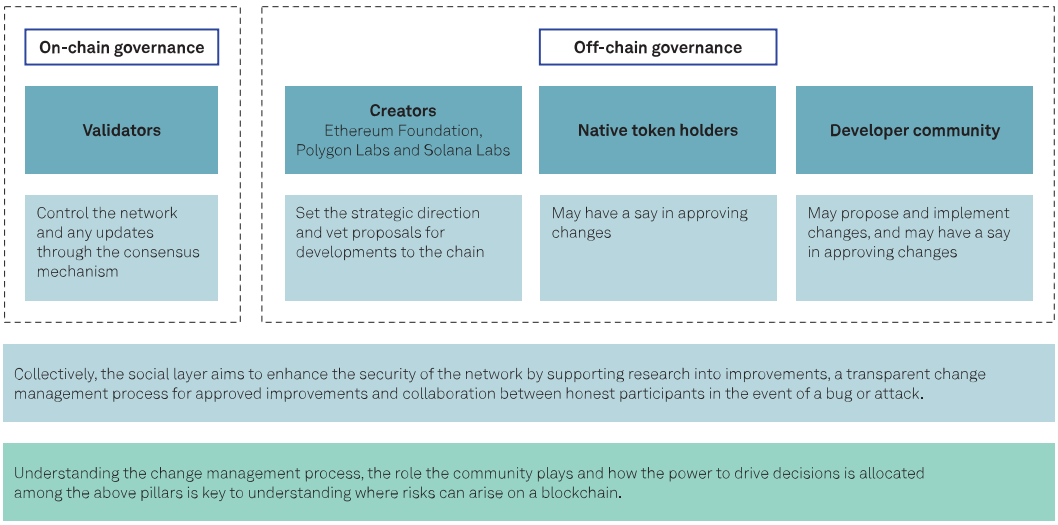
When client risk materializes: Ethereum's delayed finality event in May 2023

In May 2023, a bug affected some of Ethereum's consensus clients, representing more than 33% of validator nodes. Validators running these clients were unable to validate blocks; therefore, Ethereum could not achieve finality. This was the first such delay since Ethereum moved to a proof-of-stake consensus mechanism in October 2022. Client development teams addressed the bug quickly, and finality was resumed in a matter of hours, with no other significant consequence. A longer delay would impede the settlement of financial transactions, so understanding these concentration risks and considering how to mitigate such a scenario are important in designing on-chain financial applications. The design of the blockchain itself includes some mitigation because inactive validators' stakes are slashed gradually, meaning that eventually they would represent less than 33% of staked ETH; therefore, the remaining active validators would be sufficient to achieve finality.

Governance and social layer

The validator consensus mechanisms described above form a blockchain's on-chain governance. It is also important to understand which aspects of a blockchain may change over time, as well as the process, timeline and visibility for future changes, and who the decision-makers are. This governance happens off-chain through information sharing (a social layer), change management (governance structure) and a core developer team that often drives the creation, major changes and funding of innovation for a blockchain. While many participants in these types of governance are also participants on-chain, understanding their off-chain roles, responsibilities and interactions is important to understanding how a blockchain may evolve. On-chain features and risks are baked into a blockchain's coding language, smart contracts and structure. If the participants or the community want to address these risks or create different opportunities, they must rely on the other off-chain factors of governance (see the chart "Governance and social layer").

Governance and social layer



Source: S&P Global Ratings.

These layers of governance work together to address any changes for the blockchain. Changes can be small and compatible with previous blocks. More significant changes can cause a "hard fork" of the chain. If the community does not achieve consensus on such changes, different participants may choose the new path or stay on the existing one, effectively creating two blockchains and letting market forces determine which one is used.

This level of interaction and responsibility enables community coordination that can help protect the network from bad actors and resolve any technical vulnerability that may arise. During an attack or bug event, information can be shared quickly through various communication boards, and core developers can coordinate with client team developers to test and implement fixes. This has been a major factor in limiting the impact of outages and finality delays, which to date have generally been resolved within hours.

Ethereum, Polygon and Solana follow a broadly similar blockchain change management process, which engages the broader community of developers and stakeholders. There are some nuances in how a proposed change is reviewed and implemented, how long it takes to implement and who can approve. There are also potential trade-offs to manage between decentralization (involving the broader community in a decision) and the need to make rapid changes in a crisis.

Chain-specific change management process

Source: S&P Global Ratings.

None of the three blockchains discussed in this report currently include a formal token holder voting mechanism to implement changes, although recent discussions within the Solana community are exploring this. Where such a mechanism exists, key considerations in assessing governance risk include:

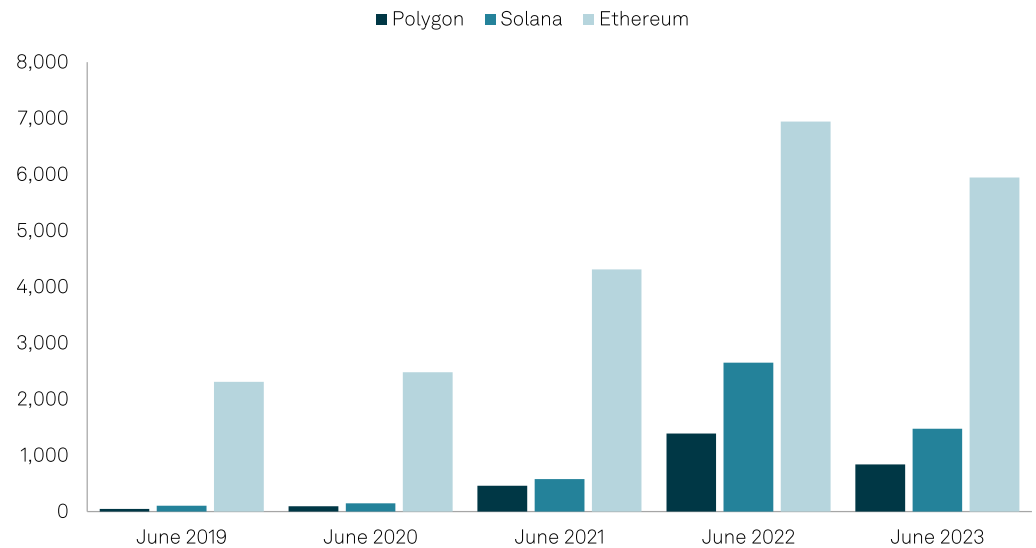
- The role that a governance token may play in approving certain decisions, where applicable.
- Any large concentration among the holders of such governance tokens.
- Whether the benefits accruing to these holders incentivize the safeguarding of the protocol.

The social layer: Led by the masses

A blockchain's social layer is made up of its developers (core developers, client developers and application developers) and users more broadly and serves several important roles. When reviewing the on-chain improvement process, it is the members of this community that often propose improvements and discuss as a group their views on the proposed changes. These open-forum discussions aim to identify potential pitfalls and desirability prior to implementation and allow coordination between development teams. Looking at the number of active developers for each blockchain is one indicator of the level of community engagement.

Based on data from Electric Capital's developer report, the number of active developers has grown for all three chains over the past five years, and very rapidly for Solana and Polygon. As the oldest of the three blockchains, Ethereum's growth is slower; however, it maintains by far the largest active developer community.

Active developers*



Data compiled September 2023.
* Code authors.
Source: Electric Capital.

Does creators' continued involvement in blockchain governance constitute a risk?

The Ethereum Foundation, Polygon Labs and Solana Labs are entities set up by the creators of these respective blockchains. These entities (non-profit organizations or firms) can help fund innovation and drive new ideas within the broader community. As such, they play an important role in governance discussions. In considering a long-term financial use of these blockchains, potential users must, therefore, understand these entities' visions for developments to their blockchain. However, it is also important to understand that each blockchain could continue to operate without these entities. Given the open-source nature of a public permissionless blockchain, the remaining social layer could continue to use and support the chain's existence.

How blockchains scale

The initial design of Solana prioritized security and scalability over decentralization. By maximizing transaction throughput potential, Solana required advanced hardware to be a validator. This effectively limited validators initially to professional operators, with the expectation that over time, hardware improvements would allow decentralization to a broader network of validators. In contrast, the design of Ethereum initially prioritized decentralization, with relatively low validator hardware requirements but accepting the resulting limits on transaction throughput, with the expectation that developments to Ethereum itself would improve scalability. Ethereum's roadmap to improve scalability over time features a "modular" blockchain architecture, where further blockchains ("layer 2 roll-ups") that are optimized for scalability can be built on top of the main Ethereum network. This contrasts with Solana's "monolithic" design where scalability is achieved within one blockchain.

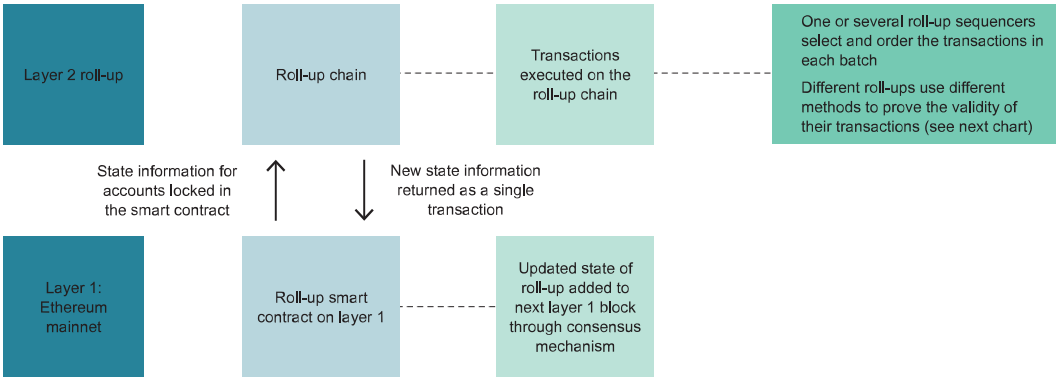
How do Ethereum's layer 2 roll-ups work?

Roll-ups work by grouping transactions, executing them on a separate blockchain (the "roll-up chain"), and then posting the new state information resulting from these transactions back to the Ethereum blockchain ("layer 1") as a single transaction. Executing transactions on layer 2 significantly reduces the computation load on layer 1, as well as the transaction costs paid by users because the single transaction cost on layer 1 is socialized across all users who have submitted a transaction on layer 2. Posting data back to layer 1 ensures that layer 2 benefits from the same security guarantees as layer 1 in terms of immutability and data availability across all nodes on the chain (see the chart "Addressing Ethereum scalability through layer 2 roll-ups").

A key consideration in layer 2 roll-ups is how to ascertain the validity of the updated state that is posted back to layer 1 when transactions have been executed. There are currently two models:

Optimistic roll-ups assume all the transactions are valid unless proven otherwise and rely on the active participation of users to identify and prevent invalid transactions. If a user identifies an invalid transaction, it is up to that user to challenge that transaction within a set challenge period (usually seven days) by providing a "fraud proof." The roll-up smart contract on layer 1 verifies this fraud proof, and if a transaction is confirmed as invalid, the roll-up chain is rolled back to the state prior to the invalid transaction. Users cannot withdraw funds from a roll-up smart contract immediately because the withdrawal transaction can only complete once the applicable challenge period has terminated.

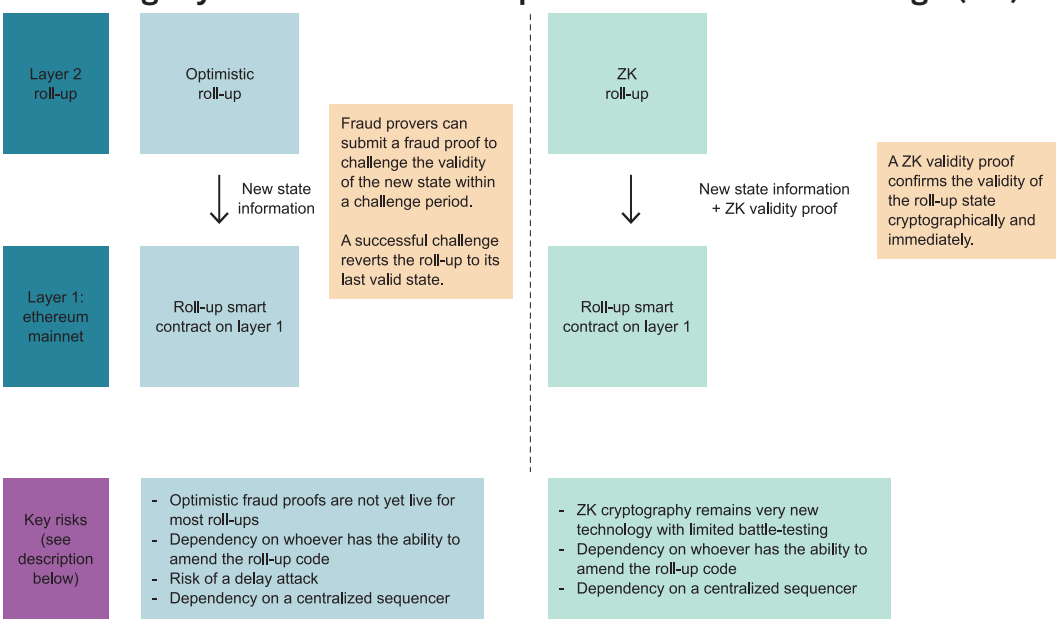
Addressing Ethereum scalability through layer 2 roll-ups



Source: S&P Global Ratings.

Zero-knowledge roll-ups provide validity proofs along with the new state information using ZK proof systems, a cryptographic solution that verifies the truth of a given statement without conveying any information about the truth. This means that the validity of transactions is confirmed instantaneously without the need for user intervention or any subsequent challenge period. The transmission of ZK proofs has a low computational cost and, therefore, boosts scalability; however, the computation of the proofs is more intensive and can lead to latency issues. Beyond scalability, ZK research is also focused on enabling privacy in blockchain applications, potentially supporting regulatory compliance for financial institutions and overcoming a major roadblock for institutional adoption. ZK proofs allow for verification of the truth of a specific statement (for example, the exclusion of a user from a set of sanctioned individuals) without transmitting all data about that user and their transaction history. For more information. (See Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium by Vitalik Buterin, Jacob Illum, Matthias Nadler, Fabian Schär and Ameen Soleimani.)

Validating layer 2 transactions: optimism or zero-knowledge (ZK)



Source: S&P Global Ratings.

Key risks of layer 2 roll-ups

Roll-ups are more complex than the Ethereum mainnet because they aim to add functionality and speed. This makes them more susceptible to outage risk. They are also relatively recent technological developments that will be battle-tested as they scale, which may identify vulnerabilities that need to be addressed. This is particularly true for ZK roll-ups, where the "unknown unknowns" represent a risk. Beyond the broad risks associated with complexity and technological innovation, roll-ups include specific risks and dependencies that must be understood when considering their use for a financial application.

The following risks apply to both optimistic and ZK roll-ups:

- ***Upgradability:*** The smart contracts underpinning both types of roll-ups are upgradable, introducing a dependency on whoever can amend the code. Currently, the development team behind each roll-up can change the code in the smart contract, generally subject to multi-signature approval, where any nine out of 12 keys in a multi-signature wallet must approve the change (and the bulk of these keys are held by the development team). In some cases, decentralized autonomous organization (DAO) governance is in place, and DAO approval is needed for any change, although DAOs themselves can carry their own voter concentration risks. On one hand, this can mitigate the risk associated with the novelty of the technology because a vulnerability that is identified can be addressed quickly. On the other hand, it introduces a trust assumption that users need to be aware of.
- ***Reliance on a central sequencer:*** The sequencer orders transactions in the batch to create the new state to return to layer 1. Although most roll-up developers claim that eventually this role will be decentralized, currently, roll-ups rely on a central sequencer, creating an operational dependency. From a user's perspective, the actual risk exposure to the sequencer is not critical because there are limits to what a sequencer can do: It cannot withdraw funds for itself, amend or directly censor transactions.

The following risks apply to optimistic roll-ups only:

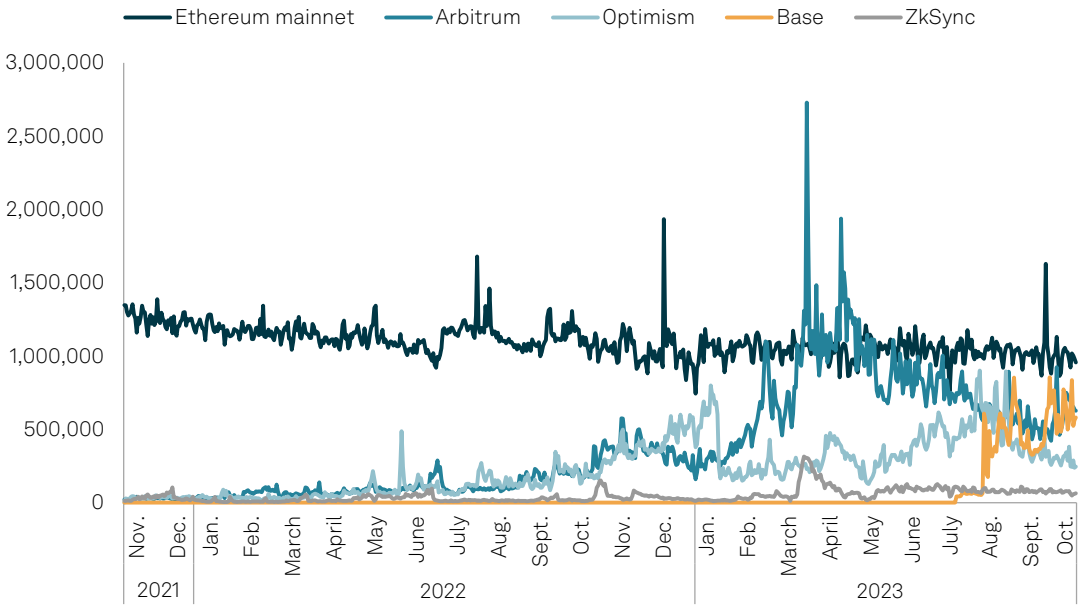
- ***Optimistic fraud proofs:*** At their core, optimistic roll-ups rely on the assumption that someone will challenge an invalid state if one occurs. One way for a user to get comfortable with this assumption is to act as a fraud prover themselves, which is possible where permissionless fraud proofs are enabled. At the time of writing, however, fraud proofs were live on Arbitrum One but not on other major optimistic roll-ups such as Optimism or Base (according to L2Beats, a blockchain analytics company).
- ***Risk of a delay attack on an optimistic roll-up:*** Any user can challenge the validity of a given transaction on an optimistic roll-up by providing a fraud proof during the challenge period (typically seven days after a transaction is executed.) If a fraud proof is submitted, this starts a resolution period (typically, a further seven days). During the resolution period, transactions cannot be confirmed, and users cannot withdraw funds from the roll-up. If a further fraud proof is provided during the resolution period, a new resolution period is initiated. Therefore, an attacker could plausibly submit repeated fraud proofs on valid transactions to prevent the layer 2 from operating.

Layer 2 adoption

Layer 2's lower transaction costs and fast throughput have supported relatively rapid adoption since the first optimistic roll-ups went live in 2021 (see the chart "Daily transactions on Ethereum mainnet and selected layer 2 roll-ups"). ZKsync was the first

ZK roll-up to go live on top of the Ethereum mainnet in March 2023, and the novelty of the technology has contributed to limiting adoption so far. Base is the latest optimistic roll-up, launched by Coinbase, a leading crypto exchange, in August 2023 (see the sidebar "'Base': Coinbase's optimistic roll-up"). It has quickly matched Optimism and Arbitrum in terms of daily transaction count, boosted by Coinbase's customer base and brand recognition.

Daily transactions on Ethereum mainnet and selected layer 2 roll-ups



Data compiled Oct. 5, 2023.
Source: Dune (@blockworks_research, @tk_research, @dashagubaha).

"Base": Coinbase's optimistic roll-up

On Aug. 9, 2023, Coinbase, a major global crypto exchange, launched Base, an optimistic roll-up. Base is built on Optimism Lab's OP Stack and is, therefore, similar to Optimism and other existing optimistic roll-ups, and not a technological innovation in itself. On Sept. 5, Base experienced its first major outage that lasted approximately 45 minutes, before Coinbase developers addressed the issue. This highlighted both the operational risk in using these tools at scale and the prompt reactivity of the developers involved in the roll-up.

Ethereum's scaling developments continue

The next step in the Ethereum scaling roadmap is "Proto-Danksharding." This will be implemented as part of the next major update to the Ethereum blockchain (referred to as the "Cancun" update), which the Ethereum community expects will take place in late 2023 or early 2024. Currently, roll-ups store transaction data permanently on the Ethereum layer 1 chain, such that anyone can download and verify historical data. The idea behind Proto-Danksharding is that it is not necessary to store this data perpetually to guarantee the security of the chain. Instead, roll-up data will be stored temporarily on "blobs" linked to each block on the layer 1 chain, and the blob data would be deleted periodically. Participants would still be able to download data before it is

deleted to keep an off-chain record if desired. Validators will no longer need to store the full record of all historical roll-up transactions to participate in the network. This supports decentralization by improving the economics of data storage and reducing the computational load on validator nodes. It addresses the risk that otherwise, the volume of data on the blockchain would balloon over time, increasing the hardware requirement to act as a validator and thereby leading to centralization.

Polygon 2.0 proposal: Toward an ecosystem of interoperable ZK roll-ups

Polygon 2.0 is a further example of continuous development in the blockchain landscape. It is a proposed upgrade to the Polygon network that aims to further improve scalability. Rather than a single blockchain, the proposal would create a network of interoperable and EVM-compatible ZK roll-ups connected to the Ethereum mainnet. Potential users could build their own ZK roll-up within this ecosystem to suit their needs — for example, in terms of privacy and permissioning, or relative to the trade-offs highlighted in the chart "The blockchain design trilemma." They could also choose between storing all data on the Ethereum mainnet or only the ZK proofs, with transaction data then stored off-chain by a trusted party. The interoperability between roll-ups within this new ecosystem would limit any risk of fragmentation of liquidity that could arise from different users using different chains.

In terms of governance, one proposal would include a 12-member ecosystem council with representatives from different members of the social layer, which is similar to the governance of existing individual roll-ups. Another proposed change is to give more voting power to those that lock up their tokens for longer periods. It is important that builders of potential financial applications understand how this can influence decision-making and changes to the ecosystem.

Looking forward: Disruption could come gradually — then suddenly

Although blockchains have been around for nearly 15 years, these technologies are evolving continuously. The latest developments described in this report may overcome some of the hurdles that have so far constrained the adoption of public blockchains within the traditional financial system, particularly by rated issuers. These developments attempt to address issues with scalability while preserving the benefits of security and decentralization, as well as potentially enabling privacy and identity verification solutions. The emergence of ecosystems of interoperable blockchains may also allow users to build to their own "sweet spot" in terms of the trade-offs between scalability, security and decentralization, and enable permissioned networks without fragmenting markets.

As regulatory frameworks emerge and market participants execute on current research and pilot projects, we expect that real use cases will emerge that demonstrate benefits in areas such as collateral mobility, intraday liquidity and reduced settlement risks. If successful test cases are accompanied with further developments supporting interoperability, network effects may then lead to the rapid adoption of tokenization of financial assets. That said, these are nascent technologies that will need to be battle-tested to identify unforeseen vulnerabilities, and currently present identifiable risks and dependencies. Understanding and addressing these risks will be critical to developing robust market infrastructure and financial applications around public blockchains.

Glossary

Block finality. The completion of the consensus mechanism. A block becomes immutable upon finality.

Consensus mechanism. The mechanism through which participants in a blockchain network confirm the validity of a proposed block.

Client software. The software packages that each validator node is running to execute transactions, validate the proposed block and send attestations of its validity. Different software packages are built by different companies, to the same specification, but using different coding languages and structures.

Layer 1 blockchain. A base-layer blockchain network.

Layer 2 roll-up. A blockchain network built on top of a layer 1 blockchain that aims to add functionality and speed.

Node. One of several dedicated computational engines, stores of memory and broadcasting sites on a distributed ledger technology network.

Reorg attack. An attack on a blockchain network that seeks to modify the content or ordering of previous blocks. Such attacks are described as "short range" if they target recent blocks or "long-range" if they target blocks much earlier in the chain.

Slashing mechanism. A feature of a proof-of-stake consensus mechanism that penalizes validators by reducing ("slashing") the value of their stake if they are inactive or behave badly, for example by attesting to the validity of invalid blocks.

Staking. The process of committing digital assets to a protocol on a distributed ledger technology network to either actively or passively participate in return for rewards.

Validator. A node in a blockchain network that executes transactions, validates the proposed block and sends attestations of its validity.

Zero-day event. An attack on a blockchain or protocol that exploits a previously unknown vulnerability.

Zero-knowledge proof. A cryptographic technique that verifies a statement is true without revealing the statement's contents. In a blockchain context, this has applications in enhancing scalability as well as privacy and regulatory compliance.

Related research

- Operational Resilience Is Key To Global FMIs' Rating Strength, Oct. 4, 2023
- How DeFi's Operational Risks Could Influence Credit Quality, June 7, 2023
- Cyber Brief: Reviewing The Credit Aspects Of Blockchain, May 5, 2022

Acknowledgements

The open-source ethos of public permissionless blockchains means that there is a wealth of publicly available information that has informed our analysis. The authors would like to acknowledge in particular the work published by the Ethereum Foundation, Polygon Labs, Solana Labs, the Bankless podcast and research (www.bankless.com) and L2Beat (www.l2beat.com).

CONTACTS

www.spglobal.com
www.spglobal.com/en/enterprise/about/contact-us.html