Blockchain
Presence

Ethereum
Layer 2

May 2022

Content

Manuel Steger
Market Analytics

David Maurenbrecher
Market Analytics

Design

Kim Stauffer
Digital Marketing

Executive Summary

Ethereum, a blockchain launched in 2015 and developed by a set of brilliant developers, including Vitalik Buterin, has transformed the technology from its main usage as a worldwide, trustless payment system to a global computer, able to run arbitrary computing through its virtual machine, the EVM. Today, Ethereum is the most widely utilized and decentralized blockchain with a total locked value (TVL) of over $148 billion and a valuation of at least $366 billion. Though a great achievement, this increase in use is also Ethereum's biggest challenge as it attempts to keep transactions affordable while limited to 13-15 transactions per second (TPS) and executing 1,250 thousand transactions per day.

The bidding for transaction inclusion in blocks coupled with this limited capacity has led to average transaction fees in excess of $10 for throughout most of 2021 and 2022. Users' transition into lower-cost alternatives has resulted in the rise of Solana, Avalanche, and the Ethereum-Sidechain Polygon. The high Ethereum fees however, have also invigorated the development of innovative protocols seeking to scale the capacity of Ethereum. These platforms build upon and rely on Ethereum, Layer 1 (L1), and are therefore referred to as Layer 2 (L2) solutions. These L2 platforms, the most important of which are analyzed in this report, have seen critical technological development and mass adoption (400% TVL growth YTD). Most of these L2 platforms leverage Ethereum's security by utilizing the mainchain as a settlement layer but have their own execution layer for computing. This approach significantly improves user experience through cheaper transactions and higher throughput while inheriting Ethereum's superior security. As sidechains manage security through their own validators and could, in principle, continue to operate in the absence of Ethereum, they are not considered L2 in the strictest sense and though analyzed, will not be considered as L2 platforms unless explicitly named for the purpose of this report. Combined, the L2 platforms, excluding sidechains, currently have a TVL of over $6.35B.

The L2 landscape and its trajectory can be summarized by two trends and the associated technologies underpinning them.

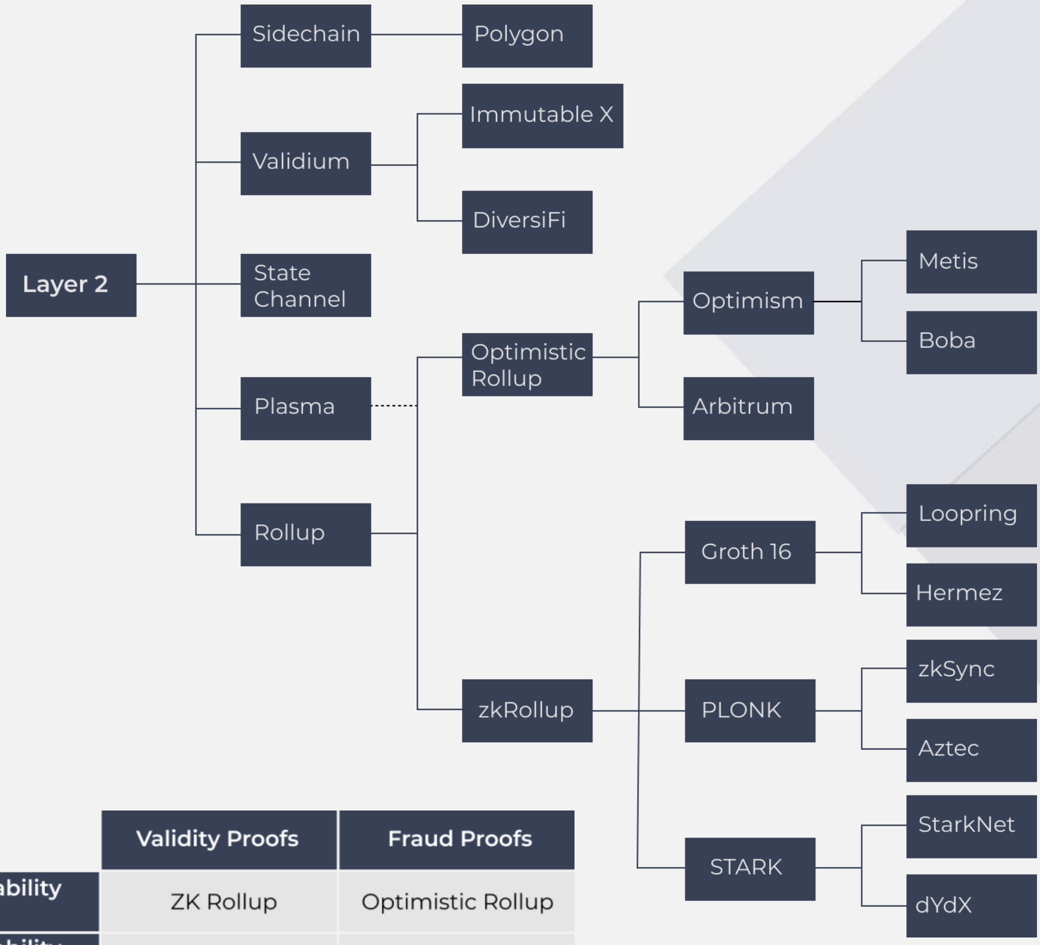
1. Optimistic Rollups dominate the current L2 landscape as they constitute roughly 75% of L2 TVL. These platforms batch transactions off-chain and then submit them to Ethereum assuming the batch producers only included valid transactions, while relying on a fraud-proof. This fraud-proof is essentially a weeklong challenge period for users to dispute the validity of a submitted batch. Given that all transactions are stored on Ethereum, the validity of any transaction can be calculated on-chain. Key to the dominance of Optimistic

Rollups has been their support for Solidity smart contract execution off-chain, available on Optimistic Rollups for over a year, this capability is only now being beta tested on other L2 technology.

2. Zero-Knowledge is the future of L2. While Optimistic Rollups require a fraud-proof, delaying transaction finality, zero-knowledge Rollups, relying purely on mathematic proofs, require neither an honest verifier nor a challenge period. Vitalik Buterin, Ethereum's founder, suggested zkRollups are poised to be the future of all L2 scaling solutions. With the testing of the first zkVM, allowing for all Solidity smart contracts to work out of the box on the zkSync 2.0 Rollup, zkRollups will be able to match any functionality of Optimistic Rollups and do so in a less expensive yet more secure manner. For users seeking near-zero fees, zero-knowledge is also the underlying technology for Validium L2 platforms. Like the zkRollups, a validity proof ensures instant finality and validity of the batches, although the transaction data is stored by an off-chain network. This approach sacrifices some of zkRollups' robust security to further reduce transaction costs.

Although not a true L2 by our definition, one prominent Ethereum alternative is the Polygon PoS sidechain. It is EVM-equivalent, copy-paste solidity SC porting, with transaction fees well below Optimistic and zkRollups. However, as Polygon validators are currently receiving inflationary rewards in orders of magnitudes of the transaction fees collected, current fee levels are not sustainable long term. Additionally, the sidechain is less secure than Rollups that inherit the security from the most decentralized and secure SC Platform, Ethereum. Polygon is most likely aware of the drawbacks of its PoS chain and therefore investing into almost every L2 scaling technology available on the market. The aim is to build a network as an aggregated hub for various scaling solutions while providing a developer-friendly framework to build customizable, EVM-compatible blockchains on it. In addition, along with its data availability blockchain module, Polygon is introducing a new self-sovereign privacy-focused identity solution that brings various new and innovative applications to Ethereum.

Overview



	Validity Proofs	Fraud Proofs
Data Availability on-chain	ZK Rollup	Optimistic Rollup
Data Availability off-chain	Validium	Plasma

The core idea behind Ethereum's first L2 solution, the **State Channel**, originally derived from Bitcoins Lightning Network. It allowed for unlimited off-chain P2P transactions by locking funds in a channel (smart contract), thus minimizing gas costs for normal coin/token transfers. However, even with the innovative approach from Celer or Raiden Network building hubs to connect these channels, vast number of funds needed to be deposited in the channels/hubs resulting in low capital turnover rates. Due to this limitation of the underlying technology, the solution naturally evolved into what we today call Plasma.

Plasma technology resolves the problems its precursor has faced by providing its own structure model, similar to Bitcoins UTXO (Unspent Transaction Output), where all transfers are recorded off-chain and from time to time submitted to a smart contract on the mainnet. This message contains the network's Merkle state, meaning the whole off-chain ledger, to be then challenged on-chain to ensure that all off-chain transactions are executed correctly. Although Plasma solves the state channels' main limitations, it confronts its users with a complex verification mechanism and a week-long exit period while still limiting its application spectrum to transfers.

Optimistic Rollups are addressing two of the main drawbacks the Plasma technology brings, namely the complex data verification as well as its limitation to transfers. By executing arbitrary inputs through their own virtual machine (EVM compatible) and "rolling up" off-chain transactions, Optimistic Rollups allow for cheap smart contract execution while enhancing the data verification process through the submitted raw, compressed transaction data along with both the previous Merkle state and the resulting Merkle state. What remains is the inconveniently long process of verifying state correctness through the fraud-proof protocol.

Zero-Knowledge Rollups solve this problem by leveraging cutting-edge math to enable instant verification (finality) of the submitted batches. Zero-knowledge means that the verifier learns no information beyond the fact that the statement (in our case, the submitted batch) is true. An essential part of this verification process is the creation of a validity proof, which proves that the post-state root is the correct result of executing the batch. No matter the amount of computation, the proof can be very quickly verified on-chain. The validity proof is then submitted to the mainnet along with the compressed transactions (batches). While batches from Optimistic Rollups also need to contain data for verification purposes, batches from zkRollups only consist of data relevant to reconstruct its state. Proofs can be created through various protocols, e.g., Groth16, Plonk, or STARK, which all come with different strengths and weaknesses.

Validium solutions also leverage zk-technology. However, instead of submitting the L2 state to Ethereum along with the validity proof like zkRollups, they only submit the second - thus reducing the gas cost to the bare minimum. As only the proof is needed to be validated on-chain in order to prove state correctness, Validiums make some trade-offs regarding the security of funds as they only publish transaction data via a data availability committee (DAC).

While previously mentioned solutions are, per definition, true L2 (Consensus on Ethereum), **Sidechains** do not conform to this definition as they produce their own blocks and use their own set of validators to validate them, allowing for much cheaper transactions. Most of them submit a Merkle tree of their state on Ethereum, use Ethereum to manage their validator stake, or both, in case of the Polygons PoS Chain.

Comparison

	Validium	Optimistic Rollups	zk Rollup	Sidechains
Security				
Liveness Assumption	No	Bonded	No	Bonded
Quorum of Validators can freeze funds	Yes	No	No	Yes
Quorum of validators can confiscate funds	Yes	No	No	Yes
Vulnerability to hot-wallet key exploits	High	Moderate	Immune	High
Vulnerability to crypto-economic attacks	Moderate	Moderate	Immune	High
Performance / Economics				
Max TPS on ETH 1.0	20,000+	2,000	2,000	40,000+
Max TPS on ETH 2.0	40,000+	20,000+	40,000+	40,000+
Capital-efficient	Yes	Yes	Yes	Yes
Separate on-chain tx to open account	No	No	Sometimes (Loopring)	No
Cost of tx	Very Low	Low	Low	Very Low
Usability				
Withdrawal time	1-10 min	1-2 Weeks	1-10 min	1 confirm.
Time to subjective finality	1-10 min	1 confirm.	1-10 min	N/A (trusted)
Client-side verification of subjective finality	Yes	No	Yes	N/A (trusted)
Instant tx confirmations	Bonded	Bonded	Bonded	Bonded
General Aspects				
Smart Contracts	Flexible	Flexible	Flexible	Flexible
EVM-bytecode portable	Yes	Yes	Yes	Yes
Native privacy options	Full	No	Full	No

Inspired by: Matter Labs

Liveness assumption

Do users need to be monitoring all on-chain (i.e. L1) activity of the scaling solution by themselves or via trusted representatives (bonded)?

Quorum of validators can freeze funds / confiscate funds

Can a quorum of L2 validators make funds inaccessible to users for indefinite periods of time? Can they seize user funds?

Vulnerability to hot-wallet key exploits

Does the safety of funds in this L2 solution depend on the operator’s ability to secure the keys that must be kept on online machines to keep the system operational (i.e. hot-wallet keys)?

Vulnerability to crypto-economic attacks

How vulnerable is the solution to crypto-economic attacks and does it rely on game-theoretic assumptions?

Capital-efficient

How capital efficient is the scaling solution? Does it require a substantial amount of capital to be locked in order to operate?

Time to subjective finality

How quickly can a transaction reach a state where it cannot be reverted on the L1 anymore under the security assumptions of the protocol?

Client-side verification of subjective finality

Can the time to subjective finality (see the previous question) be verified with light clients (browsers/mobile wallets)?

Instant tx confirmations

Can the solution provide full or only bonded (only in the UX, tx can still be reverted for a period until verified on L1) instant transaction confirmations?

Smart Contracts

Does the L2 support arbitrarily programmable smart contracts or only a limited subset that can be implemented using predicates?

EVM-bytecode portable

Can one port the EVM-bytecode of existing Ethereum contracts almost without changes?

Native privacy options

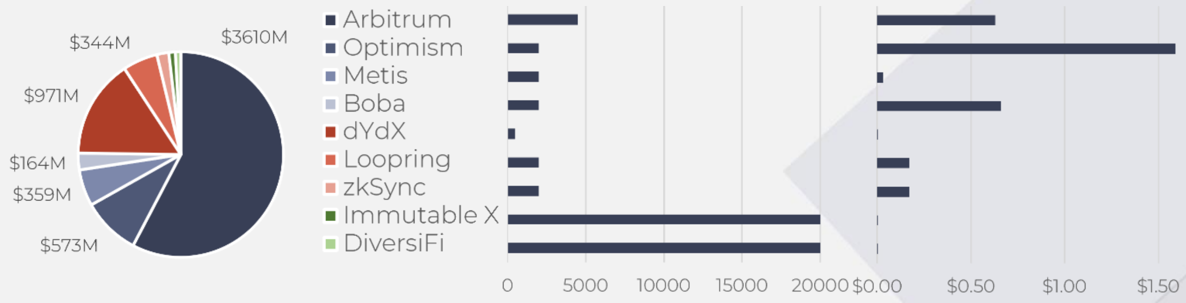
Does the protocol offer native support for privacy?

Dashboard

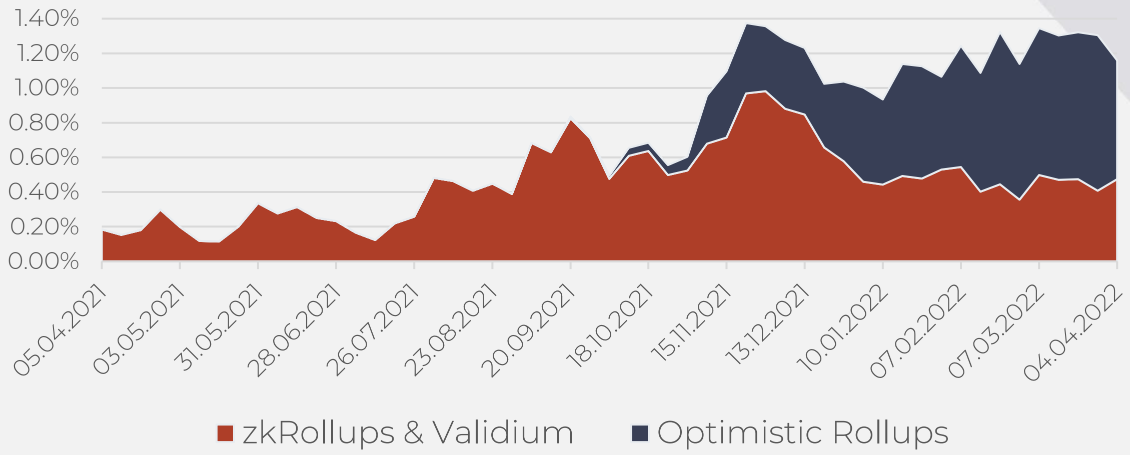
Total Value Locked

Max. Throughput (TPS)

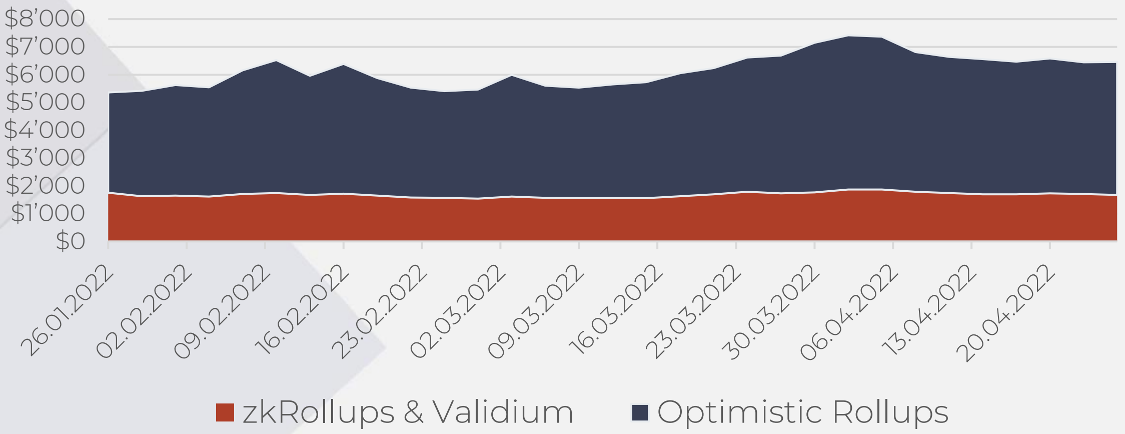
Avg. Tx. Fee



Percentage of Maximum Ethereum Gas Used by L2



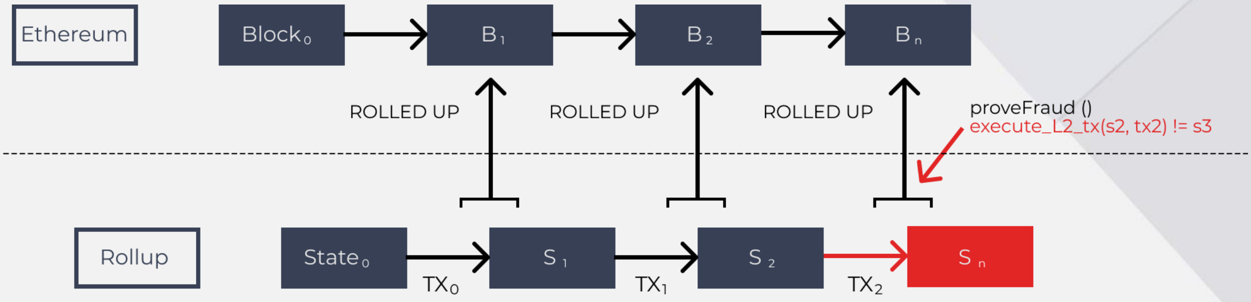
TVL (Millions) total Over 90d



Optimistic Rollups

Optimistic Rollups - Technology

Optimistic Rollups constitute a development from the Plasma L2 approach with the same team that developed plasma going on to develop the first Optimistic Rollup. As with Plasma Optimistic Rollups batch transactions off-chain and stores the off-chain state in the form of a Merkle root on a smart contract on the Ethereum L1. However, in contrast to Plasma all the transactions are stored on Ethereum L1 CALLDATA, making a complete reconstruction of the L2 state possible. This means that even if the Rollup and all its of-chain operators were to go down, users' assets remain safe. The scaling advantage results from the fact that CALLDATA storage on Ethereum is computationally much less intensive than regular L1 storage and hence requires much less gas for the equivalent number of transactions.



The batches (rollups) of transactions posted by the off-chain operators are assumed to be valid (hence optimistic) but can be challenged in a fraud-proof on L1. This fraud-proof, initiated by other operators or users observing the submitted rollups, relies on the immutable CALLDATA stored on L1 to prove fraudulent transactions and revert the L2 to its correct state. This fraud-proof relies only on one honest operator/user to contest a block and staked assets of operators proven to submit fraudulent rollups are slashed. Given that honest users require a certain time to detect wrongdoing the window for fraud-proofs is commonly close to a week. This in turn means that transactions from the L2 to L1 or vice-versa always require significant time for finality (~1 week). For transactions within L2 however there are solutions with instant finality by staking assets as a bond.

Optimistic Rollups greatest improvement on Plasma is that the L1 CALLDATA allows for EVM implementation off-chain. Allowing for Solidity smart contract applications on L2. Though in some cases not EVM equivalent, the EVM compatibility has allowed for the growth of large DApp communities on Optimistic Rollups. Being the first L2 solution to offer this feature may largely explain why Optimistic Rollups constitute approximately 75% of Total Value Locked (TVL) on Ethereum L2.

Arbitrum

Arbitrum is currently the largest Ethereum L2 platform (by TVL) and offers EVM compatibility through their streamlined Arbitrum Virtual Machine. It differs from rival Optimistic Rollups by providing fragmentation challenge, which challenges blocks of transaction piecemeal, lowering the L1 gas use and thus costs for fraud-proofs. Though fully functional, it is still in the mainnet beta phase resulting in transaction throttling, leading to somewhat higher fees. The Arbitrum Nitro upgrade, which is live on the Görli testnet, will remove the throttling, optimize compression efficiency, and increase the overall throughput.

Security Measures: As with all Optimistic Rollups, Arbitrum relies on its fraud-proof to ensure only valid state transitions become final. Though relying on a centralized sequencer that orders transactions for the Rollup, users can force transactions, bypassing censorship, by interacting directly with the L1 Arbitrum smart contract.

Risks: The fraud-proof relies on the assumption that at least one whitelisted validator is honest and will catch a fraudulent state, if not then funds could be stolen. Due to the centralization of the sequencer, producing blocks, a failure of the sequencer would lead to the freezing of funds.

Headquarters

New York, USA

Team

Ed Felten (Co-Founder)
Steven Goldfeder (Co-Founder)
Harry Kalodner (Co-Founder)

Technology

Optimistic Rollup

Applications

Universal (EVM compatibility)

Ecosystem

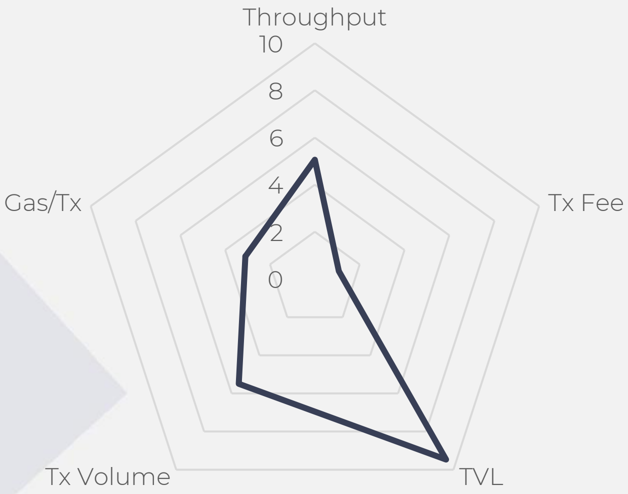
150+ DApps
Bridges to 10+ Chains

Smart Contract language

Solidity

Arbitrum

Price	-
Total Value Locked	$3,660 Mio.
Market Dominance (TVL)	57%
Transaction Fee	$0.63
Throughput	4,500
Gas Consumption (ø7d)	300 Mio.
Inflows/Outflows (7d)	$48 Mio. / $14 Mio.
Transactions per sec. (ø7d)	0.7



Optimism

The first Optimistic Rollup to launch for Ethereum, Optimism was developed by the team behind Ethereum Plasma and is currently the third-largest L2 rollup by TVL. It's Optimism Virtual Machine 2.0 is EVM equivalent allowing for Solidity contract execution off-chain as well as development through tools widely used for Ethereum developers. This full equivalency means no matter the contract complexity, it can be deployed on Optimism without adjustment. Security is assured through a 7-day fraud-proof period, only after which transaction finality is reached.

Security Measures: Optimism will rely on its fraud-proof to ensure only valid state transitions become final. Users can force transactions and bypassing censorship by interacting directly with the L1 smart contract.

Risks: The Optimism fraud-proof is still in development meaning currently users must currently trust block creator. Due to the centralization of the sequencer, producing blocks, a failure of the sequencer would lead to the freezing of funds.

Headquarters

San Francisco, USA

Technology

Vitalik Buterin (CEO, Founder)

Ecosystem

100+ DApps
Bridge to 10+ Chains

Team

Jinglang Wang (Co-Founder)
Kevin Ho (Co-Founder)

Applications

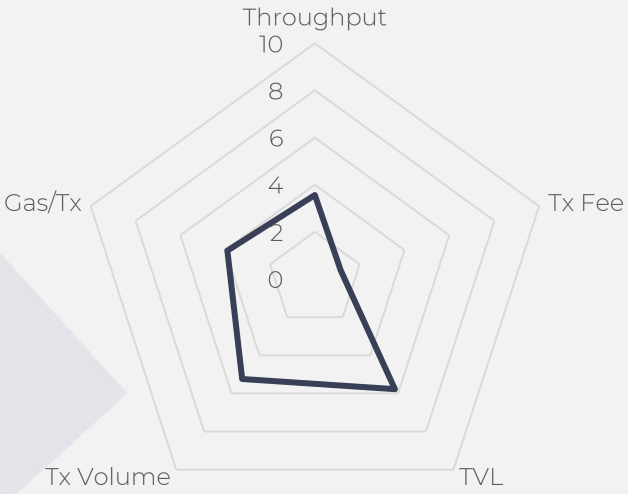
Universal (EVM Equivalence)

Smart Contract language

Solidity

Optimism

Price	-
Total Value Locked	$592 Mio.
Market Dominance (TVL)	15%
Transaction Fee	$0.59
Throughput	2,000
Gas Consumption (ø7d)	160 Mio.
Inflows/Outflows (7d)	$15.7 Mio. / $3.7 Mio.
Transactions per sec. (ø7d)	0.5



Metis

Both Metis and Boba started as forks from Optimism. Metis adds a sharded rollup layout allowing for specialized computational and storage layers in parallel to fit the requirements of its operators (e.g. DAO, DApp) while permitting seamless cross-layer communication and liquidity. It also employs OVM 2.0 for EVM equivalency.

Security Measures and Risks: As a fork from Optimism Metis shares the security measures and risks described for Optimism. Critically its fraud-proof is not fully developed and thus block creators must be trusted to submit valid state transitions to L1.

Headquarters

Singapore

Technology

Optimistic Rollup

Ecosystem

Team

Elena Sinelnikova (Co-Founder)
Kevin Liu (Co-Founder)
Yuan Su (Co-Founder)

Applications

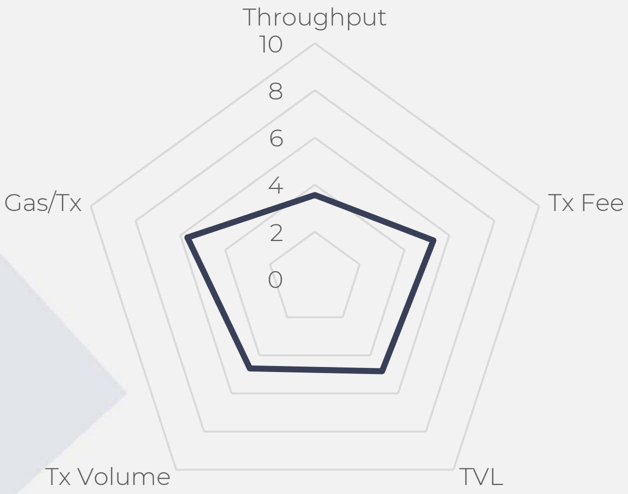
Universal (EVM equivalence)

Smart Contract language

Solidity

Metis

Marketcap	$246 Mio.
Total Value Locked	$376 Mio.
Market Dominance (TVL)	5.7%
Transaction Fee	$0.03
Throughput	2,000
Gas Consumption (ø7d)	40 Mio.
Inflows/Outflows (7d)	$3.7 Mio. / $35 Mio.
Transactions per sec. (ø7d)	0.3



Boba

Boba employs OVM 2.0 as well. However, smart contracts capabilities on Boba are extended by allowing for integration of web-infrastructure (such as AWS) computed off-chain into DApps. Furthermore, Boba has a fast exit option using liquidity pools to move assets of chain within minutes rather than the otherwise 7-day finality time.

Security Measures and Risks: As a fork from Optimism Boba shares the security measures and risks described for Optimism. Critically its fraud-proof is not fully developed and thus block creators must be trusted to submit valid state transitions to L1.

Headquarters

Palo Alto, USA

Technology

Optimistic Rollup

Ecosystem

30+ DApps
Bridges to 10+ Chains

Team

Alan Chiu (Co-Founder)
Jan Liphardt (Co-Founder)

Applications

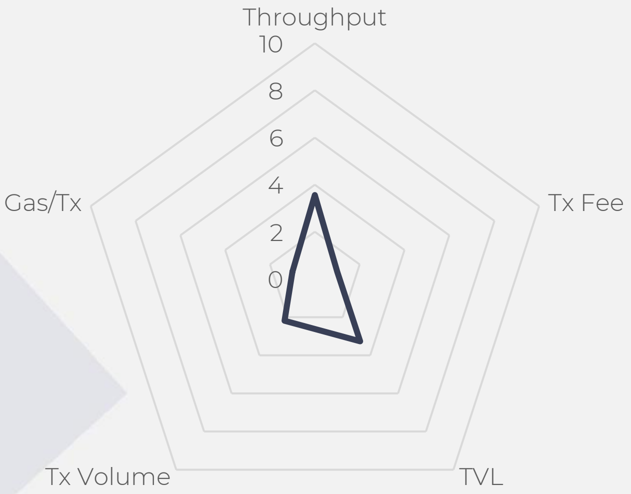
Universal (EVM equivalence)

Smart Contract language

Solidity

Boba

Price	$227 Mio.
Total Value Locked	$174 Mio.
Market Dominance (TVL)	2.6%
Transaction Fee	$0.66
Throughput	2,000
Gas Consumption (ø7d)	40 Mio.
Inflows/Outflows (7d)	$8 Mio. / $3.2 Mio.
Transactions per sec. (ø7d)	0.03



zkRollups

Zero-Knowledge Rollups - Technology

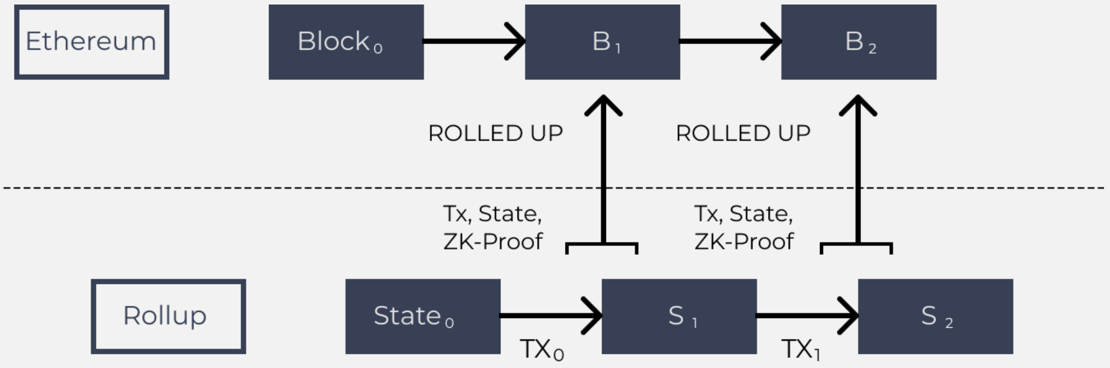
To understand what zkRollups are, we first need to define what properties a zero-knowledge proof must satisfy. We can describe the process with two parties, one called a prover and the other a verifier, where the prover needs to convince the verifier that a statement is true without revealing the statement at all. There are three main properties:

Completeness - If the Prover is honest, then he will eventually convince the Verifier.

Soundness - The Prover can only convince the Verifier if the statement is true.

Zero-Knowledge(ness) - The Verifier learns no information beyond the fact that the statement is true.

These properties are essential to ensure the protocols core function, evaluating on what's true with no way of faking the proof using false information, if any at all. The first two properties are verifiable using simple mathematics, but what makes zero knowledge proofs revolutionary is the ability to verify the last.



Zero Knowledge protocols use complex mathematical calculations to create a validity-proof out of the transactions processed on L2, which is then posted onto the Ethereum mainnet along with the batched and compiled transaction data. This proof only contains the information/statement that all transactions are valid without any additional content, allowing the smart contract on Ethereum to update its state. In this way, transactions cost only a fraction of what they would on L1, as the transaction size can be reduced from 32 bytes to just 4 bytes along with many other compiling possibilities to then be stored as cheap CALLDATA. With zkRollups, batches only need to contain enough information to reconstruct the rollups state, but not as much as it needs to verify each transaction like with Optimistic Rollups. In addition to the smaller batch size, zkRollups allow for instant finality compared to Optimistic Rollups week-long challenge period while also removing the economic vulnerability of its optimistic partner.

Zero-Knowledge Rollups - Comparison

Two of the most used zk-technologies in the market today are SNARKs and STARKs. Both are non-interactive by nature, meaning that the code can be deployed and act autonomously without relying on human interaction. However, their underlying mathematical assumptions differ completely.

Zk-SNARKs at their base depend on elliptic curves for their security. Elliptic curves in cryptography operate under the base assumption that finding the discrete logarithm (DLP) of a random elliptic curve element with respect to a publicly known base point is infeasible. Even though this solution is highly secure today, with the assumption that the secret parameter used to create the keys (prover & verifier) is destroyed, quantum computers would possibly be able to break its cryptography. But due to their efficiency, requiring only 0.1-0.5% the on-chain storage of STARKs and a gas consumption of only ~24% of the latter, SNARKs have been adopted at a faster rate.

STARKs don't rely on elliptic curves but on hash functions. This offers some benefits, such as being quantum resistant without relying on a trusted setup but requires a larger amount of on-chain storage, with higher on-chain computation.

SNORKs (e.g., PLONK, 0.5-1 kB) are SNARKs that can update their trusted setup scheme, changing it from elliptic curves (Groth16 SNARKs) to e.g., FRI (used by STARKs) or DARK (Bulletproofs, another zk-technology).

	SNARK's	STARK's
~size for 1 tx	tx: 200 bytes Key: 50 MB	45 kB
~size for 10000 tx	tx: 200 bytes Key: 500 GB	135 kB
EVM verification gas cost	~600k (Groth16)	~2.5M (no impl.)
Trusted setup Required?	Yes	No
Post-quantum secure	No	Yes
Crypto assumptions	DLP + secure bilinear pairing	Collision resistant hashes
Prover time	~2.3 sec.	~1.6 sec.
Verification time	~10 msec.	~16 msec.

SNARK = **S**uccinct **N**on-interactive **AR**guments of **K**nowledge

SNORK = **S**uccinct **N**on-interactive **O**ecumenical a**R**guments of **K**nowledge

STARK = **S**uccinct (Scalable) **T**ransparent **AR**guments of **K**nowledge

dYdX

DYdX is a decentralized derivatives trading platform. Its off-chain order books combined with on-chain settlement allows for leveraged margin, spot and perpetuals trading with instant execution. The off-chain orders are secured through Starkwares zkRollup technology via STARK-proofs and batched onto the Ethereum mainchain in a specific interval.

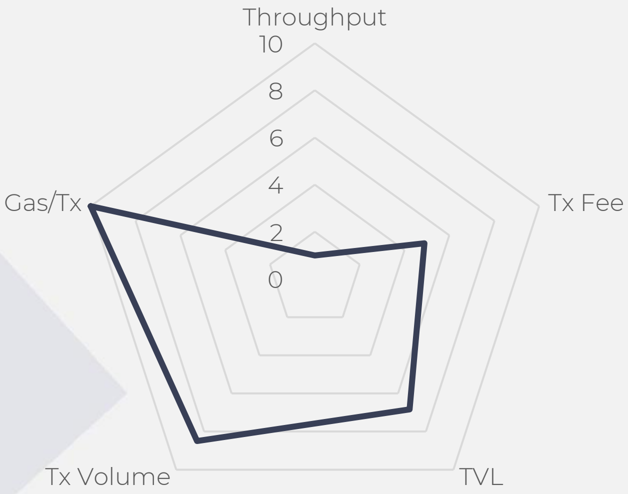
Security Measures: Having the zk-technology implemented removes any reliance on third-parties or on honest participant by solely rely on math. This removes the main attack vector of Optimistic Rollups while still enable for rebuilding the rollup state with the submitted Merkle Tree. Especially with STARK's, no trusted setup is required to verify the zk-proof. If the sequencer of dYdX goes down, users can withdraw their fund through the exit hatch. Even in case of validator failure, funds will not be frozen if the user can submit a Merkle proof of funds.

Risks: Still, if implemented incorrectly, the proofs may not correlate with the underlying data resulting in a loss of funds. Given that the zk-technology is barely battle tested, there is still a considerable risk involved by interacting with such a scaling solution. Another risk of dYdX is the non-existent delay on code upgrades as well as the possibility for MEV to be extracted by the centralized operator.

Headquarters	**Team**
San Francisco, USA	Antonio Juliano (Founder)
Technology	**Applications**
Zk-STARK (STARKEX)	Digital assets trading
Ecosystem	**Smart Contract language**
only dYdX trading application	-

dYdX

Price	$4.64
Total Value Locked	$971 Mio.
Market Dominance (TVL)	15%
Transaction Fee	$0.04
Throughput	500
Gas Consumption (ø7d)	160 Mio.
Inflows/Outflows (7d)	$63.5 Mio. / $56.8 Mio.
Transactions per sec. (ø7d)	10



Loopring

Looprings main feature is the non-custodial exchange that supports both the Automated Market Maker (AMM) and the orderbook exchange model. Combined with the Loopring wallet and their built-in payment protocol, users can exchange various digital assets including ERC-20, ERC-721 and ERC-1155 tokens. The main purpose of Loopring is to provide a platform on which centralized and decentralized exchanges can build on in a cost-efficient manner. A partnership with GameStop for their digital marketplace is already ongoing.

Security Measures: As mentioned in the dYdX chapter, zk-proofs are highly secure pieces of cryptography enabling us to dismiss any third-party involved in the verification process. Users need no honest participants to verify state correctness and can check the validity themselves if they're skilled enough. Loopring also provides the required data on-chain to reconstruct its off-chain state. Similar to dYdX, users can submit a Merkle proof to withdraw funds in case of validator failure.

Risks: However, especially with zk-SNARK's, there are still potential risks of having the proof corrupted. In the process of calculating the prover and the verifier key, a specific "trusted setup" is created where a secret parameter key was used to create both the previously mentioned keys. Knowing this parameter would enable an attacker to create "fake" proofs of something that did not happen, resulting in stolen funds.

Headquarters

Shanghai, China

Team

Daniel Wang (Founder) Adam Browman (Head of growth) Byron Wiebe (Head of community)

Technology

Zk-SNARK (Groth16)

Applications

Scaling solution for Exchanges & Marketplaces, L2 Wallet

Ecosystem

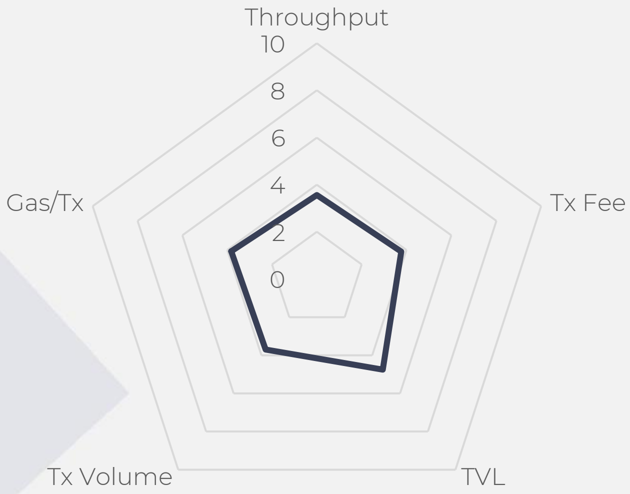
Loopring Exchange & Supports various On-Ramp solutions

Smart Contract language

-

Loopring

Marketcap	$1,183 Mio.
Total Value Locked	$338 Mio.
Market Dominance (TVL)	5%
Transaction Fee	$0.17
Throughput	2,000
Gas Consumption (ø7d)	40 Mio.
Inflows/Outflows (7d)	$3.7 Mio. / $14 Mio.
Transactions per sec. (ø7d)	0.17



zkSync

ZkSync is a zk-Rollup built on top of Ethereum. Its goal is to provide a trustless scaling and privacy solution for Ethereum based on zero-knowledge technology with an emphasis on superb user and developer experiences. At the time of writing, zkSync 2.0 is live on testnet supporting all EVM-compatible Smart Contracts. On the other hand, zkSync 1.1 already allows to transfer various digital assets, burning, minting and swapping tokens (also NFT's) on L2. Being live since June 2020, zkSync advertises itself as the cheapest rollup requiring only 0.5k gas per transaction on average compared to the 1k of STARKs and 3k of alternative SNARKs. Due to its underlying proof mechanism called PLONK, zkSync does not require an app-specific trusted setup.

Security Measures: Similar to other zkRollups, zkSync already has high built-in security by building on zero knowledge technology. Compared to the previous Rollups, it introduces a 21d delay on code upgrades to minimize errors and allows to exit by submitting a zk-proof of funds.

Risks: Funds can be stolen if a malicious code upgrade is received. Although users can be censored by the operator, they can still exit through the previously mentioned proof of funds.

Headquarters

George Town, Cayman Islands

Team

Daniel Wang (Founder) Adam Browman (Head of growth)
Byron Wiebe (Head of community)

Technology

Zk-SNARK (PLONK)

Applications

Scaling solution for Exchanges & Marketplaces, L2 Wallet

Ecosystem

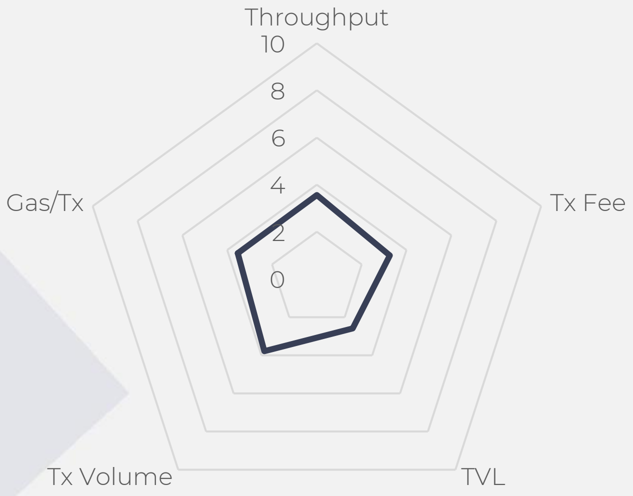
60+ DApps with Walletconnect support, on-ramp, DeFi, Dao's and Bridges

Smart Contract language

Solidity

zkSync

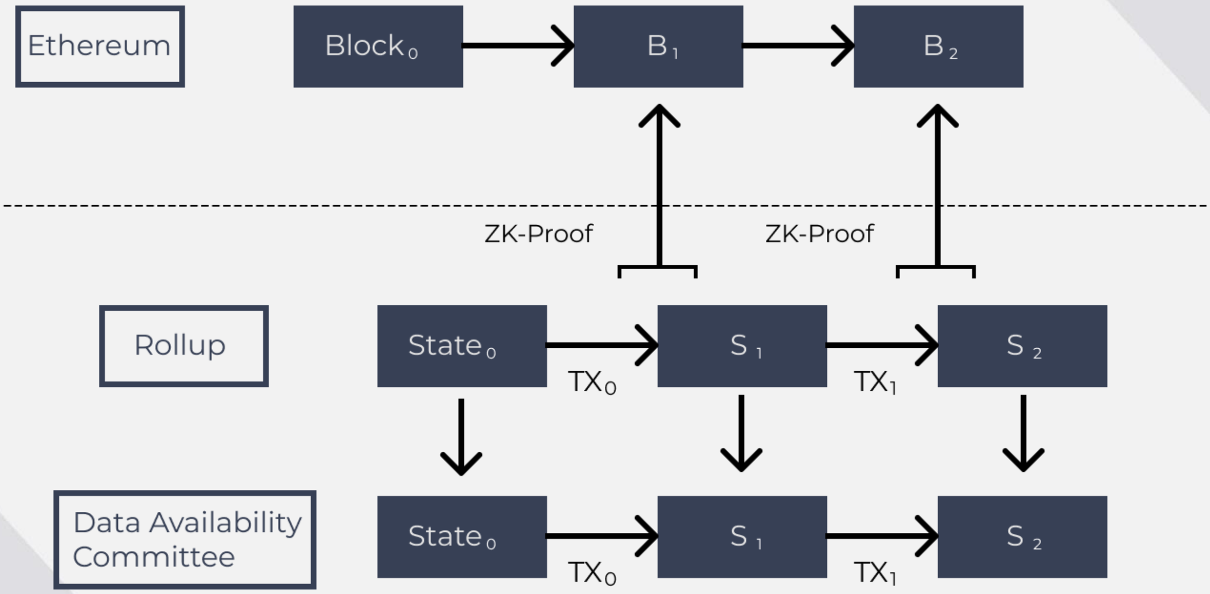
Marketcap	-
Total Value Locked	$112 Mio.
Market Dominance (TVL)	1.7%
Transaction Fee	$0.17
Throughput	2,000
Gas Consumption (ø7d)	50 Mio.
Inflows/Outflows (7d)	$2.31 Mio. / $9.1 Mio.
Transactions per sec. (ø7d)	0.13



Validium & Volition

Validium - Technology

Validium is an L2 scalability solution functioning almost exactly like zk-proofs. Unlike zkRollups, Validium does not submit raw transaction data to the L1 along with its validity proof. This means all the transaction data and history is stored off-chain and managed by staked operators (Data Availability Committee). At the expense of data security, as the state cannot be reconstructed from Ethereum L1, it reduces L1 gas requirements. This massively increases throughput and consequently reduces transaction costs relative to zkRollups. Efforts are being made to try to give the user a choice of the level of data security, by allowing both Validium and zkRollup transactions on the same L2 platform at the same time. Called Volition, this system gives the sender the choice of using the cheaper Validum transaction or the more expensive zkRollup transaction with increased security.



Immutable X

Immutable X is a L2 Volition platform optimized for NFT trading and gaming. It offers free instant trades and token minting. The zk state validity proofs submitted to Ethereum are based on Starkware's zk-protocol and allows for assets transactions either by Validium or zkRollup. The off-chain Validium data is stored by trusted parties of which a quorum must affirm a state change. Governance is provided through the native IMX coin. It can be bought or alternatively obtained as a reward for staking or incentivized actions (trading & gaming). It is also required as 20% of every Immutable X transaction protocol fee.

Security Measures: Zero knowledge transactions feature the mathematical security that zkRollups offer. Validium transactions on the other hand rely on a quorum off-chain operators being honest to confirm on-chain state updates.

Risks: Funds stored through Validium may be lost if the off-chain data becomes unavailable. Further funds become frozen if off-chain operators restrict access to historic transaction data.

Headquarters

Sydney, AU

Team

Yat Siu (Co-Founder)
James Ferguson (Co-Founder)
Alex Connolly (Co-Founder)

Technology

Volition

Applications

Gaming, NFT

Ecosystem

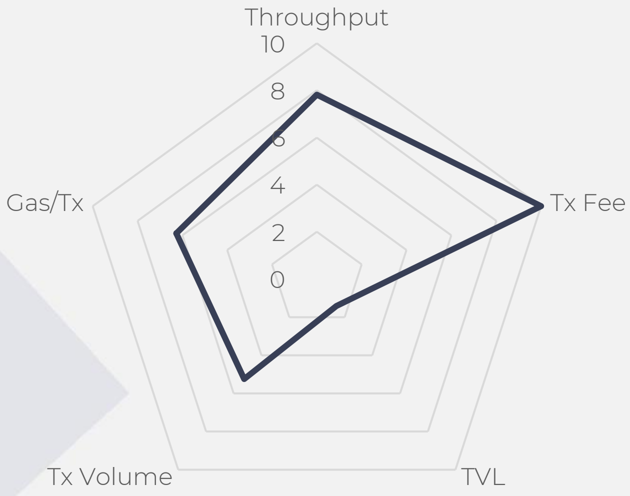
30+ NFT Ccollections & Games

Smart Contract language

-

Immutable X

Marketcap	$418 Mio.
Total Value Locked	$65 Mio.
Market Dominance (TVL)	1%
Transaction Fee	$0.001
Throughput	20,000
Gas Consumption (ø7d)	50 Mio.
Inflows/Outflows (7d)	$11 Mio. / $6.7 Mio.
Transactions per sec. (ø7d)	0.5



DiversiFi

DiversiFi is a decentralized crypto exchange based on Validium. This platform evolved from the Ethfinex DEX in 2019 and uses Starkware zk-proofs while data is stored off-chain and managed by separate operators. The platform offers a simple crypto trading interface for crypto trading with no L1 gas costs.

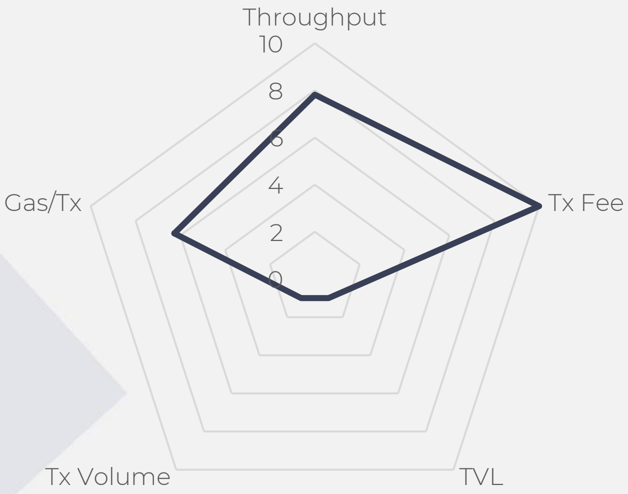
Security Measures: Transactions rely on a quorum of honest off-chain operators to confirm on-chain state updates.

Risks: Funds may be lost if the off-chain data becomes unavailable. Further funds become frozen if off-chain validators restrict access to historic transaction data.

Headquarters	Team
Tel Aviv, Israel	Tzahi Kanza (Co-Founder) Eitan Katz (Co-Founder)
Technology	**Applications**
Validium	Exchange
Ecosystem	**Smart Contract language**
Diversifi DEX	-

DiversiFi

Marketcap	$119 Mio.
Total Value Locked	$53 Mio.
Market Dominance (TVL)	0.8%
Transaction Fee	$0.001
Throughput	20,000
Gas Consumption (7d)	1 Mio.
Inflows/Outflows (7d)	$6.5 Mio. / $23 Mio.
Transactions per sec. (ø7d)	0.03



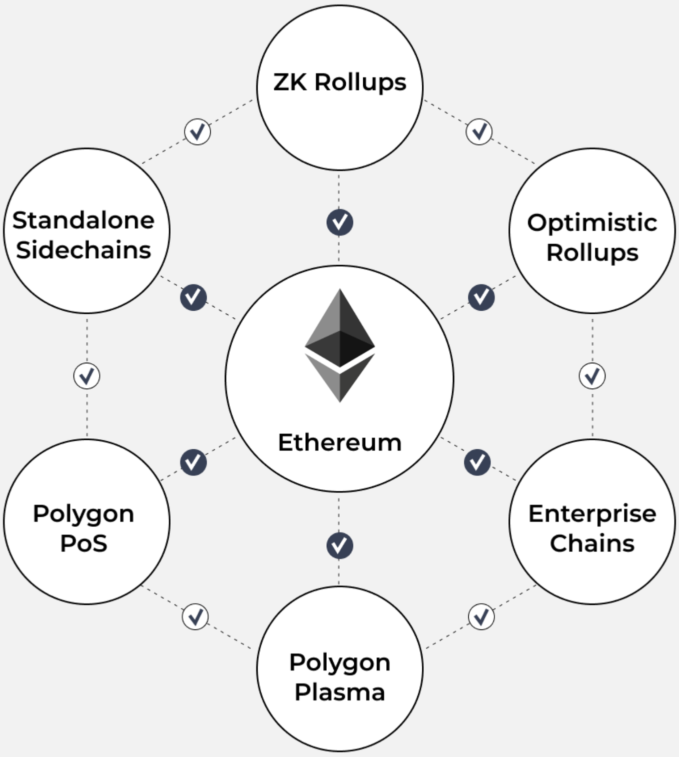
Polygon

Polygon - Technology

Polygon, formerly known as the Matic Network and still using this denomination for its native currency, is a collection of multiple scaling solutions for Ethereum. Each comes with its unique underlying technology, strengths and shortcomings. Visualizing this constellation, Polygon is the construction company of skyscrapers (individual L2/scaling solutions) while Ethereum provides the building area, society, and the governmental institutions. Therefore, even though the building area is a scarce resource, with skyscrapers providing apartments, working space for companies and multi-level libraries a whole nation-state can be built within these walls, where all successfully share the same level of security.

Like its geometric namesake already hypothesizes, each solution has its unique dimensions, shapes and uses to maximize efficiency in every specific use case. With its PoS chain, Polygon made Ethereum's ecosystem of defi and various other decentralized applications available for everybody, especially retail customers who could not afford the high fees of Ethereum itself.

Knowing that the future will belong to true L2 solutions and that current fees paid on the PoS chain are unsustainably high, Polygon is heavily investing in the development of its own zero knowledge and Optimistic Rollups like Maiden (zk-STARK) and Nightfall (Optimistic) while acquiring tech companies to build out the Hermez (Hermez Network, zk-SNARK) and Zero (Mir Protocol, zk-SNARK) solution. Along with these very innovative L2 solutions, Polygon develops a data-focused module called Avail to be used by modular blockchains for data ordering and availability, as well as a zero-knowledge based self-sovereign private identity solution, namely Polgyon ID, to allow for trusted interaction with Web3 native protocols.



Polygon PoS

The Polygon PoS Chain is not a true layer-2 solution by definition as the network does not reach consensus on Ethereum but through its own set of validators. To get onto the Polygon network, users can either choose to go with the Plasma bridging framework, which comes with a higher security guarantee but longer withdrawal time, or by sending their tokens through the PoS bridge, a superior approach to the vulnerable Proof-of-Authority bridges other Sidechains like Ronin are using. The network is split into two underlying chains, one being the Heimdall chain which coordinates validator selection and updates validators on the Ethereum mainnet. Bor, the other chain, is responsible for aggregating transactions into blocks. Heimdall is also responsible for the checkpoint submission via Tendermints weighted round-robin algorithm. Fees are calculated by leveraging EIP-1559 - Ethereum's economic model of limiting demand by setting a base fee for each block and an optional priority fee.

It may seem that the network is highly secure as the staked amount of Matic exceeds $2B, but the PoS/Plasma smart contracts on Ethereum, where the stake is managed, can be upgraded/corrupted using a 5/8 multisig address. In addition, as Polygon validators are currently receive inflationary rewards orders of magnitudes greater than the transaction fees collected, current fee levels are not sustainable long term and slowly reducing incentives to secure the network.

Headquarters

Bengaluru, India

Team

Jaynti Kanani (Co-Founder & CEO)
Sandeep Nailwal (Co-Founder)
Anurag Arjun (Co-Founder & CPO)
Mihalio Bjelic (Co-Founder)

Technology

Layer 1 PoS Chain

Applications

Universal (EVM compatible)

Ecosystem

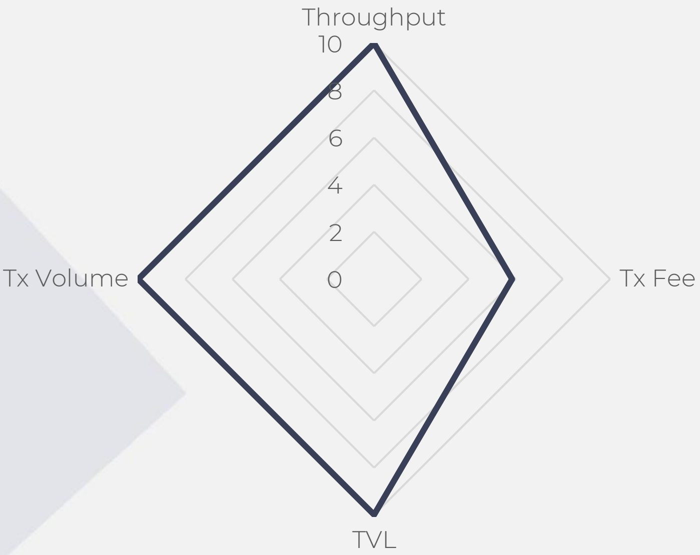
7000+ DApps, 440+ DeFi Applications, 50+ Dao's

Smart Contract language

Solidity

Polygon PoS

Marketcap	$10,726 Mio.
Total Value Locked	$5,490 Mio.
Market Dominance (TVL)	2.09% (vs. other L1's)
Transaction Fee	$0.01
Throughput	65,000
Gas Consumption (ø7d)	-
Inflows/Outflows (7d)	-
Transactions per sec. (ø7d)	34



Avail (Development)

Avail is a scalable data availability focused blockchain. Moving forward, modular blockchains will be an attractive innovation driver as they separate data availability from execution. This will allow Avail to act as the secure data storage for these execution focused layers.

Edge (Live)

Edge is a modular and extensible framework that enables you to run your own blockchain network with customizable features. It is guided by the principles of modular architecture and provides Ethereum compatibility to your network.

Hermez (Live)

Hermez is an open-source zkRollup optimised for secure, low-cost and usable token transfers on the wings of Ethereum. It is the only true decentralized zkRollups as of today, compared to the “still” centralized solutions in the previous chapter. It attains validity through zk-SNARK’s.

Throughput: 2000 TPS Tx Fee: $0.25

Miden (Development)

Polygon Miden is a L2 scaling solution for Ethereum that relies on zero-knowledge technology (zk-STARKs) to “roll-up” thousands of l2 transactions into a single Ethereum transaction. It thus increases throughput and reduces transaction fees. At the heart of Polygon Miden is Miden VM, a Turing-complete STARK-based virtual machine.

Nightfall (Testnet)

Nightfall is a one-of-a-kind privacy-focused rollup that effectively combines the concepts of Optimistic Rollups with Zero-Knowledge (zk) cryptography thus creating a private and scalable solution for transactions.

Zero (Development)

Polygon Zero uses the speed of Plonky2 to enable a more scalable and decentralized ZK L2. It offers both rollup and Validium modes, giving users access to higher throughput and lower fees.

Disclaimer

The information in this report is provided by and is the sole opinion of Blockchain Presence AG’s research team. The information is provided as a general market commentary and should not be the base for investment decisions or be taken as investment advice concerning any digital asset or the issuers thereof. Trading digital assets, in particular smart contracts, involves significant risk. Any person considering trading digital assets should seek independent advice on the suitability of any digital asset. Blockchain Presence AG does not guarantee the accuracy or completeness of the information provided in this report and accepts no liability of any kind arising from the use of any information contained in the report, including without limitation, any loss of profit. Blockchain Presence AG expressly disclaims all warranties of accuracy, completeness, or fitness for a particular purpose concerning the information in this report. Blockchain Presence AG shall not be responsible for any risks associated with accessing third-party websites, including the use of hyperlinks. All market prices, data, and other information are based upon selected public market data, reflect prevailing conditions, and research’s views as of this date, all of which are subject to change without notice. This report has not been prepared by any legal requirements designed to promote the independence of investment research and is not subject to any prohibition on dealing ahead of the dissemination of investment research. Blockchain Presence AG and its affiliates hold positions in digital assets and may now or in the future hold a position in the subject of this research. This report is not directed or intended for distribution to, or use by, any person or entity who is a citizen or resident of or located in a jurisdiction where such distribution or use would be contrary to applicable law or that would subject Blockchain Presence AG and/or its affiliates to any registration or licensing requirement. The digital assets described herein may or may not be eligible for sale in all jurisdictions.

Blockchain Presence AG
Zurich, Switzerland

Contact
info@blockchainpresence.net

Startup
University of
Zurich