Mint Ventures

Polygon (MATIC) Overview: Examining Ethereum Scaling Solution

Snapp Ye Lawrence Lee

01/03/2023

About Mint Ventures

Mint Ventures is a research-driven venture firm that specializes in cryptocurrency and early-stage blockchain start-ups. It is committed to paving the way for blockchain and Web3 revolution by funding promising blockchain companies with positive and sophisticated fundamentals and helping them propel the business forward. Mint Ventures proactively engages in private placements of emerging projects as well as secondary markets.

Contact

@Mint_Ventures

Mint Ventures

info@mintventures.fund

Disclaimer:

This report is for informational purposes only and should not be relied upon as a basis for investment decisions, nor is it offered or intended to be used as legal, investment, financial, or other advice.
You should conduct your own research and consult independent counsel on the matters discussed within this report.
The past performance of any asset is not indicative of future results.

Table of Contents

1. Key Insights

1.1 Core Investment Logic

Polygon provides a very comprehensive plan for the scaling of Ethereum with excellent and all-round performances. Thus, this project is worthy of long-term attention, with the specific logic summarized as follows:

- Ethereum scaling is the number one issue faced by the crypto industry to introduce more users, thus solutions for scaling present a huge market.
- Polygon PoS has developed a good reputation among users and developers, and it maintains a close relationship with the Ethereum community. This good relationship with users, developers and the Ethereum community provide itself with a relatively stable base.
- ZK Rollup (Zero Knowledge Rollup), highly invested by the team, is one of the most promising scaling solutions at present. It is also a promising business growth point for which Polygon has accumulated certain talent advantage and technology first-mover advantage in the ZK field through continuous capital investment and several successful mergers and acquisitions.
- The team shows great strategies and executions, reflected in its great business vision, fast business implementation, excellent marketing and business expansion, with an especially outstanding performance in introducing traditional enterprises and non-Web3 Internet enterprises.
- Compared with other public blockchain projects horizontally, its overall valuation is currently at a relatively low range.

1.2 Main Risks

- Polygon PoS lost its edge in the subsequent public blockchain competition, failing to attract and retain developers and users.
- The scaling of Ethereum has undergone a major technical direction change, making the direction of ZK Rollup no longer recognized by the community and further hitting its related businesses.
- The development progress of Polygon’s ZK Rollup sub-projects have fallen far behind expectations.
- The official cross-chain bridge of Polygon has undergone serious security accidents.

1.3 Valuation

Through horizontal metric comparison, we think the market value of Polygon is underestimated compared with other Layer 1 projects even without considering the value of its ZK Rollup sub-projects; By comparing its own historical data, we think Polygon's valuation is currently at a median level.

For more information, please refer to *Valuation*.

This article is written by the author based on the project information and market background at the time of writing.

Limited by the author's cognition and information limitations, there may be errors in data, facts, analysis and deduction in this article. The idea exchange and correction are welcomed. Please be noted that all content of this article does not constitute any investment suggestion.

2. Project Information

2.1 Business Scope

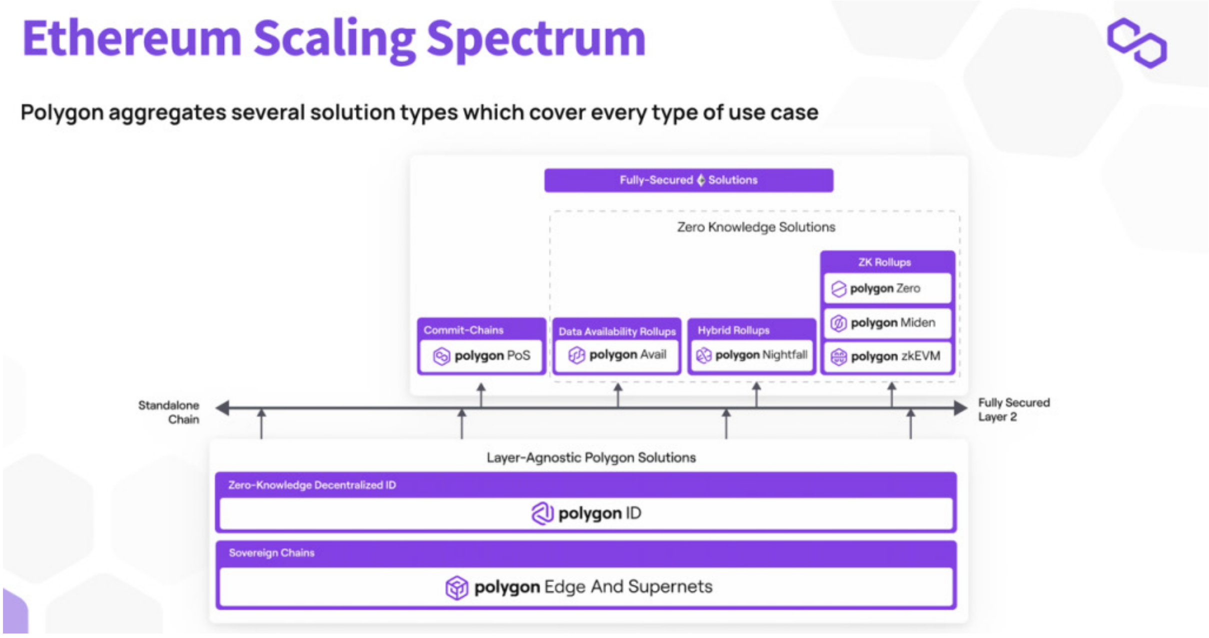
Polygon is committed to solving the scaling problem of Ethereum. It has six scaling solutions including:

• Polygon PoS: an EVM (Ethereum Virtual Machine) compatible sidechain, launched on June 1, 2020, the main business of Polygon at present.
• Polygon Avail: it aims to become the global universal data availability layer of blockchain (various sidechains and Layer2 chains upload complete transaction records to Ethereum mainnet for verification and recording, and ensures that they can be retrieved and used at any time). In Avail's vision, various side chains and Layer2 chains upload all transaction data to Avail, which sorts and records the transaction data, and ensures the accuracy and verifiability of the transaction data by cryptographic means, thus ensuring the data availability.

In this way, for other side chains and Layer2 chains, this part of the cost can be saved. Polygon Avail has launched its test network on June 29, 2022.

- Polygon Nightfall: Nightfall is an Optimistic Rollup for enterprise customers co-built by Polygon and Ernst & Young, which combines some features of zero-knowledge proof. It has been launched on the test net.
- Polygon zkEVM: The original project was called Hermez, which was renamed Polygon zkEVM after Hermez was acquired by Polygon in August 2021. Polygon zkEVM is a ZK Rollup with opcode-level compatibility. According to Vitalik ‘s EVM compatibility classification, Polygon zkEVM is currently ranked as the third level alongside Scroll, surpassing other ZK Rollup, ranking high among current ZK Rollup in terms of EVM compatibility.
- Polygon Zero: In November 2021, Polygon acquired Mir and renamed it as Polygon Zero. Polygon Zero released Plonky2 in January 2022. According to its official website materials, Plonky2 is the fastest recursive zero knowledge prover in the world (which will be elaborated later) and is also a core component of Polygon Zero. Polygon Zero expects its testnet to go alive in 2022 Q4, realizing the pattern of “sharding + ZKEVM”.
- Polygon Miden: In November 2021, Polygon announced plans to develop Ethereum scaling product Polygon Miden. Miden uses ZK-Stark technology to counter quantum computing and emphasizes the ability to validate transactions off chains. Miden expects to launch mainnet in 2023 Q1.

Among these six scaling plans, ZKEVM, Zero and Miden, three projects of ZK Rollup, realized the same security level of Ethernet mainnet, while Polygon PoS is relatively less secure.



Ethereum Scaling Spectrum

Polygon aggregates several solution types which cover every type of use case

Source: Polygon official website

In addition to the above scaling solutions, Polygon also launched its own DID system Polygon ID and developer tools Edge and Supernets.

From the current development of Polygon, Polygon PoS is a fundamental base for Polygon, while its ZK Rollup solution composed of Polygon zkEVM, Polygon Miden, Polygon Zero and Polygon Nightfall areis potential growth points currently recognized by the market. We will focus on these two parts of Polygon business as below.

2.2 History and Roadmap

2017.10	Matic Network was founded
2019.4	Matic received early investment from Mih Ventures and Coinbase Ventures, totaling 615,000 US dollars, accounting for 3.8% of tokens
2019.4	Matic Network conducted IEO in Coinbase and sold 19% of its total token share
2019.4	Release the Alpha mainnet
2020.6	Mainnet was officially launched.
2021.2	Matic Network announced to change name to Polygon and positioned itself as the Ethereum scaling solution provider
2021.6	Set up Polygon Studios to focus on NFT and GameFi
2021.8	Acquired Hermez and renamed it Polygon Hermez to focus on zkEVM research and development
2021.9	Cooperated with Ernst & Young to launch Polygon Nightfall for transactions and privacy protection of enterprises
2021.11	Acquired Mir and renamed it into Polygon Zero, dedicated to building a high-speed and sharded zkEVM
2021.11	Announced the upcoming launch of Polygon Miden, expected to have the quantum-resistant and privacy-reserving zkEVM
2022.6	Announced the launch of Polygon Avail as a data availability layer product
2022.7	Announced Polygon Hermez to implement zkEVM

2.3 Business Details

2.3.1 Polygon PoS

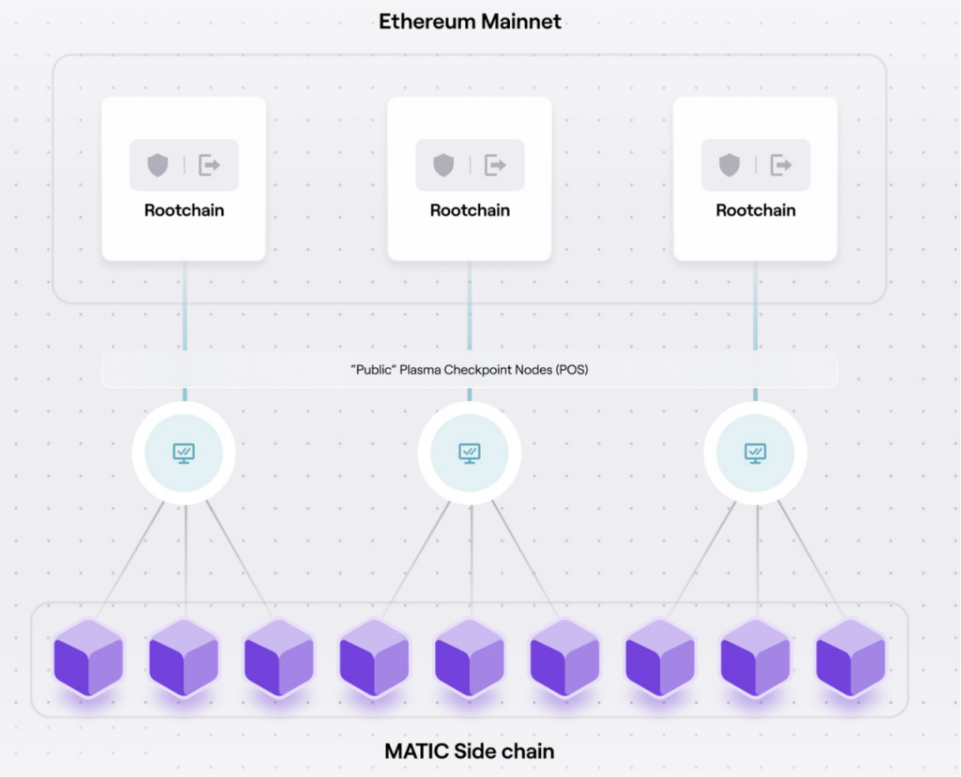
Polygon PoS launched its mainnet on June 1, 2020, which is the main business of Polygon at present.

Technical architecture:

Different from relatively independent blockchains such as BNB Chain and Solana, Polygon PoS is a side chain of Ethereum, so it is necessary for us to have a brief understanding of its architecture first.

Polygon PoS architecture can be divided into three layers as a whole:

1. A series of contracts deployed on the Ethereum chain
2. Checkpoint Node of PoS
3. Matic side chain



Source: Polygon official website

At the core of the architecture are “Checkpoint nodes of PoS”, which generate and validate all blocks on the Matic side chain, and regularly synchronize information between Ethererum and Matic side chain.

Specifically, these PoS nodes transmit the information of Ethereum mainnet to Matic side chain by monitoring events on Ethereum; By regularly aggregating multiple blocks generated by Matic side chain into Merkle tree and publishing them to Ethereum, the information synchronization of Matic side chain to Ethereum mainnet is realized.

From the above process, we can also find the difference between Polygon’s Ethereum side chain architecture and L2 chains such as Rollups and other independent L1 chains:

Compared with independent L1 chains such as Solana, the core work of Polygon verification nodes include synchronizing information between Ethereum main chain and Matic side chain, that is, it cannot exist without its main chain (Ethereum).

Compared with Rollups such as Arbitrum and Optimism, although the Sequencer of Rollups and PoS nodes of Polygon are both responsible for synchronizing the side chain/Rollup information to the mainnet, its Rollup Sequencer needs strict verification when transmitting information to the smart contract of Ethereum mainnet, which enables it to inherit the security of Ethereum.

In Polygon’s architecture, most of the information from Matic side chain to Ethereum mainnet are synchronized rather than validated, so the security of the whole Polygon PoS is actually determined by its PoS nodes. From this point of view, Polygon functions like independent L1 chains such as Solana, to guarantee its security by itself.

- **Progress of the ecosystem**

Polygon PoS has undergone a long-time slow progress since its launch in 2020 until the second quarter of 2021. Sinch then, it has developed rapidly, becoming the third public chain with relatively sound ecological application after Ethereum and BNB Chain.

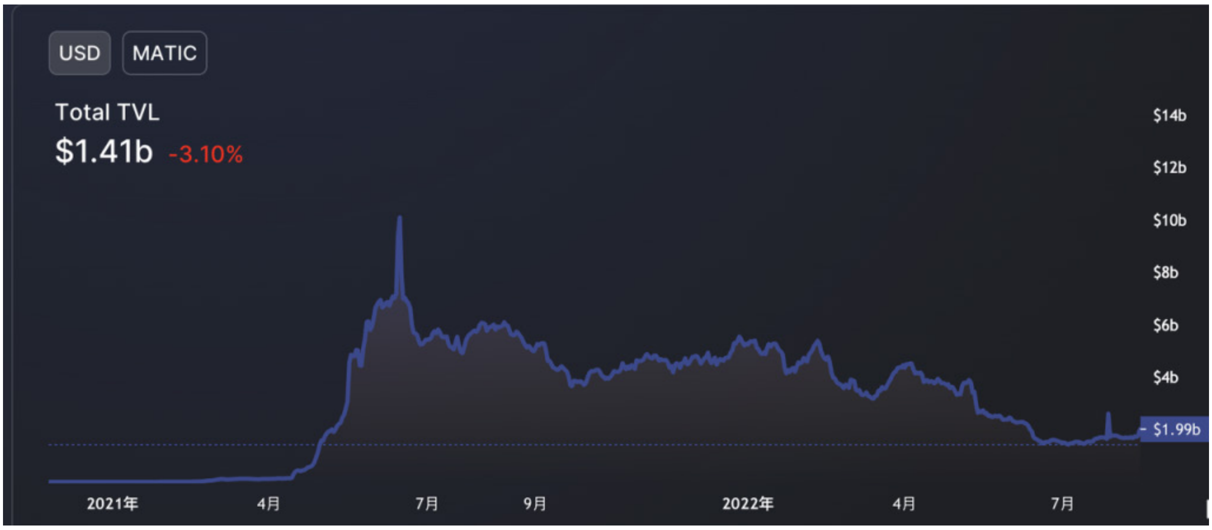
In terms of business development, Polygon is catching up rapidly in DeFi. For a long time in 2021, Polygon’s TVL is second only to Ethereum and BNB Chain.

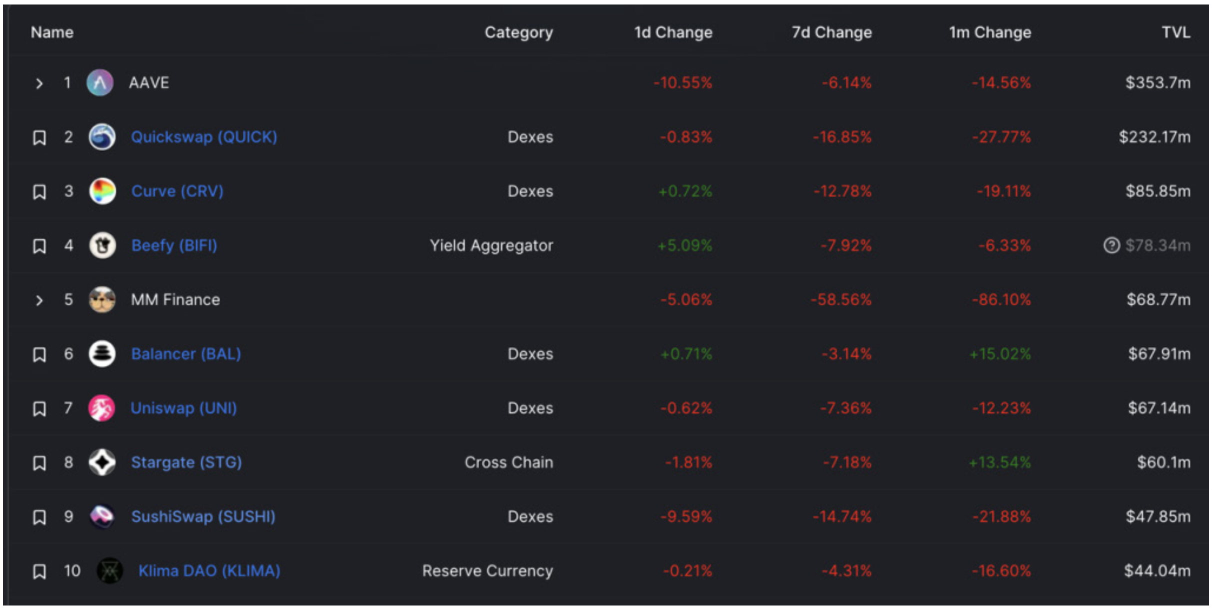
There may be two reasons for this rapid development: First, compared with other public chains that claimng to be “Ethereum killers”, Polygon defined itself as a supplement to Ethereum from the very beginning, and the team also invited members of Ethereum Foundation as consultants. Also its friendly attitude towards Ethereum can also be found in the positioning of its side chain.

This good relationship with Ethereum community, especially with developers makes Polygon the first choice for DeFi blue chips such as Uniswap, Aave and Curve.

Second, at the end of April 2021, Polygon launched a $150 million fund for DeFi adoption, to subsidize users to use Polygon network.

For a long time, liquidity providers can receive the official MATIC token rewards from Polygon when they lend and borrow on Aave(Polygon).





Name	Category	1d Change	7d Change	1m Change	TVL
1 AAVE		-10.55%	-6.14%	-14.56%	$353.7m
2 Quickswap (QUICK)	Dexes	-0.83%	-16.85%	-27.77%	$232.17m
3 Curve (CRV)	Dexes	+0.72%	-12.78%	-19.11%	$85.85m
4 Beefy (BIFI)	Yield Aggregator	+5.09%	-7.92%	-6.33%	$78.34m
5 MM Finance		-5.06%	-58.56%	-86.10%	$68.77m
6 Balancer (BAL)	Dexes	+0.71%	-3.14%	+15.02%	$67.91m
7 Uniswap (UNI)	Dexes	-0.62%	-7.36%	-12.23%	$67.14m
8 Stargate (STG)	Cross Chain	-1.81%	-7.18%	+13.54%	$60.1m
9 SushiSwap (SUSHI)	Dexes	-9.59%	-14.74%	-21.88%	$47.85m
10 Klima DAO (KLIMA)	Reserve Currency	-0.21%	-4.31%	-16.60%	$44.04m

Data source: Defillama

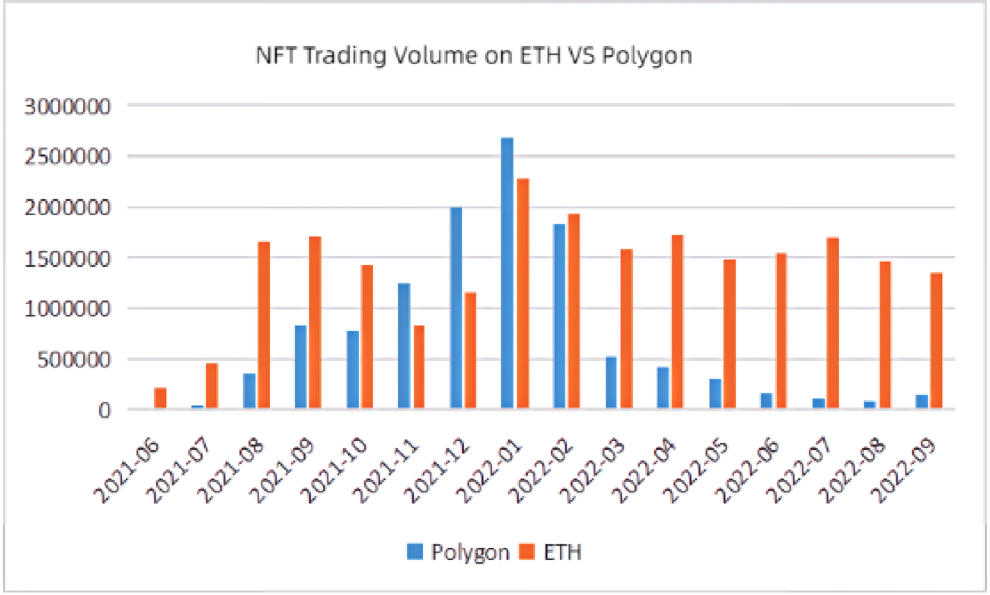
However, perhaps due to the strong brand effect of DeFi leaders, DeFi projects on Polygon chain lack innovation slightly.

For the TVL, among the top 10 projects, only Quickswap and KlimaDAO are Polygon-native projects, and other projects all originate from other chains. Quickswap is the Fork of Uniswap v2, and KlimaDAO may regarded as the fork of Ohm.

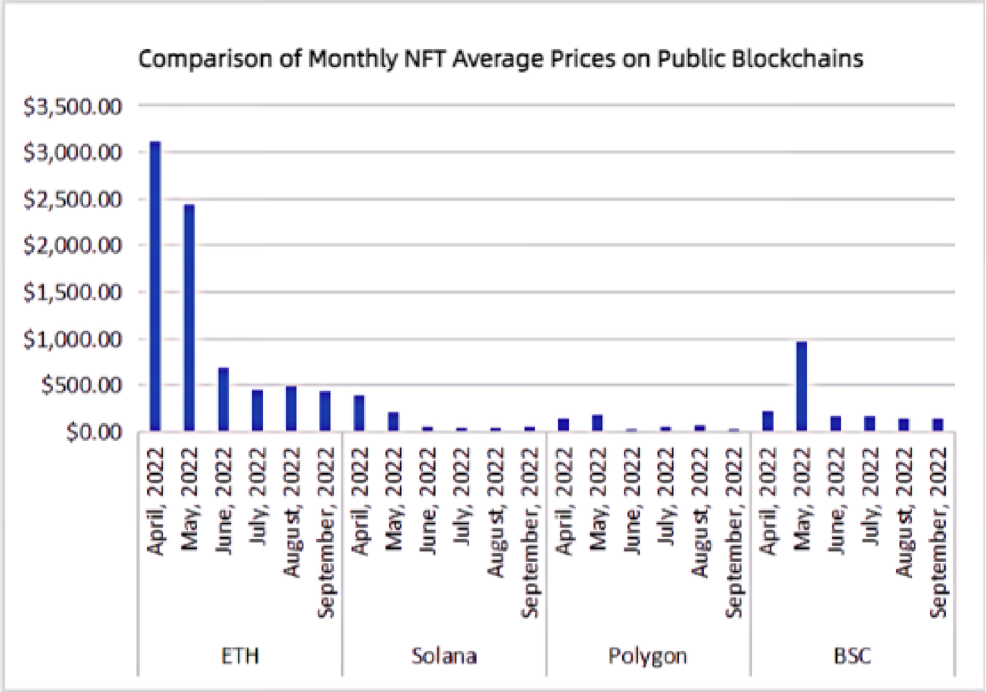
Polygon also has a strategic planning on NFTs. At the end of June 2021, Opensea announced to support Polygon, and this leads to a scenario where Polygon almost take all shares of the low-end NFT market, while Ethereum high-end NFT market.

Since then, benefiting from the cheap and fast trading experience, the NFT trading volume on Polygon once approached or even surpassed Ethereum.

However, the average price of NFT transactions on Polygon chain is extremely low, often less than $100, and its total transaction volume is significantly lower than that of Ethereum. When the NFT bear market comes, Polygon, which focuses on the low-end NFT market, has shown a more obvious downward trend.



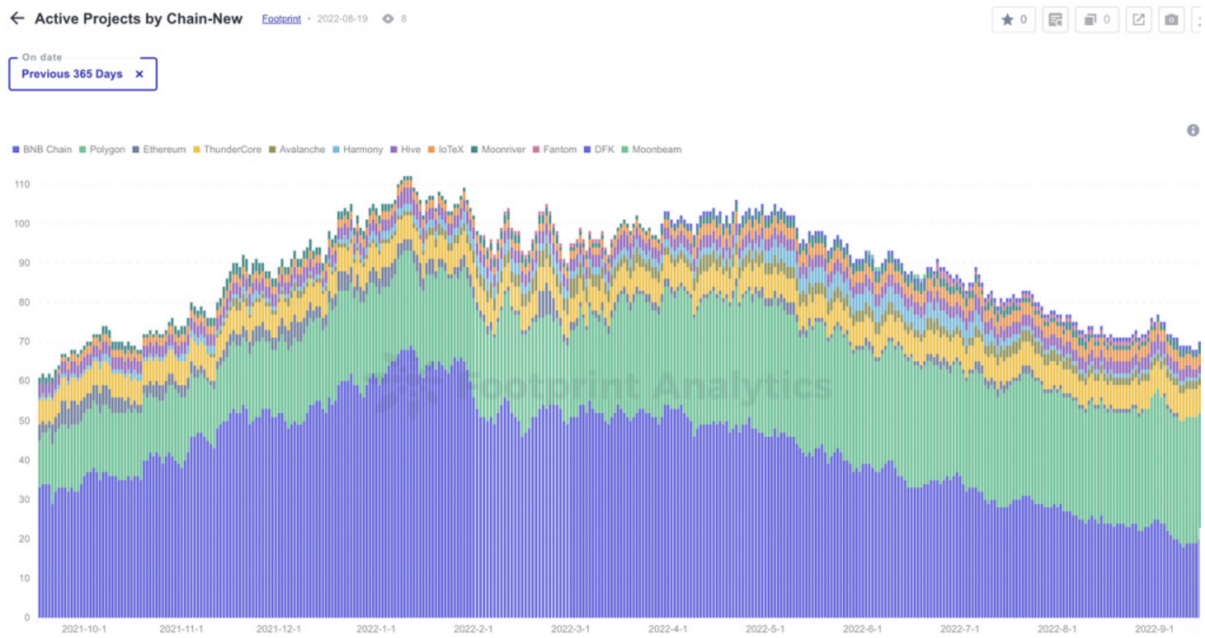
Source: summarized by Opensea and Mint Ventures



Data source: summarized by Crypto Slam and Mint Ventures

In terms of games and metaverse, two leading projects Decentraland and The Sandbox were deployed on Polygon in April and June 2021 respectively.

According to Footprint's statistics, the active game items in Polygon chain are second only to BNB Chain for most of the past year, and in July this year, it surpassed BNB Chain and became the blockchain with the most active game projects.



Active Projects by Chain-New

Footprint · 2022-08-19

On date: Previous 365 Days

Data Source: [*https://www.footprint.network/chart/Active-Projects-by-Chain-New-fp-28725?on_date=past365days~*](https://www.footprint.network/chart/Active-Projects-by-Chain-New-fp-28725?on_date=past365days~)

In July 2021, Polygon announced the establishment of Polygon Studios to focus on investment in NFT, Gaming and Metaverse.

As of today, Messari shows that Polygon Studios has invested in more than 36 projects.

Besides, co-founders Jaynti Kanani and Sandeep Nailwal are also active angel investors, with 25 and 69 projects invested by them respectively.

Almost all of these projects will be deployed on the Polygon chain.

In addition, it is worth mentioning that Lens Protocol, the underlying social protocol of Aave team, also chose to build on Polygon. Toucan Protocol and KlimaDAO, which focus on carbon neutrality, are also deployed on Polygon. They all demonstrate Polygon's support on some scarce directional innovations in Web3 field.

In terms of under-chain scaling, Polygon is one of the best choices for Web2 and traditional enterprises to test the blockchain or Web3 in view of its special position in Ethereum ecosystem, its better environmental friendliness (before ETH Merge) and its low-cost and fast experience compared with Ethereum.

In the past six months alone, Polygon has established partnerships with Web2 and traditional enterprises, including:

- On September 27, Robinhood, a stock and cryptocurrency trading platform, announced the launch of Web3 wallet based on Polygon;
- On September 12, Starbucks announced its cooperation with Polygon to use the blockchain technology provided by Polygon to support its member and partner loyalty platform: Starbucks Odyssey;
- On July 18, Mercedes Benz launched Acentrik, a data market built on Polygon;
- On July 13, Polygon was selected into Disney's accelerator program, which is the only public chain project among the six projects in the same batch;
- On May 23, e-commerce giant eBay released its first NFT series on the Polygon chain, and users can purchase NFT directly on eBay website;
- On May 10, social giant Meta announced that it would cooperate with Polygon to create an NFT platform for Facebook and Instagram;

How to introduce more users is a long-term challenge for the whole Web 3 world.

Traditional enterprises and Web2 giants have tens of millions, even hundreds of millions and billions of users. For better implementation, cooperation with them is a feasible way to introduce more Web3 users.

In this respect, Polygon has made far better progress than other public chains.

Although the above explorations are still in their early stage, we can expect deeper cooperation between Polygon and traditional enterprises and Web2 giants in the future, thus bringing more users to Polygon and even the whole Web3 world.

From above, we may outline some veins of the ecological development of Polygon PoS:

- The core foundation of Polygon PoS development is its low cost and the support of Ethereum community. Although Arbitrum and Optimization also have the support of Ethereum Community, the Gas cost on their chains (tens of cents to several dollars per time) is still too expensive for high-frequency interaction. In the Ethereum ecosystem, Polygon is almost the only choice if you want to make some applications with frequent chain interactions.
- DeFi protocol, represented by transactions and loans, is the infrastructure in the chain, supporting various activities in the chain. Blue-chip DeFi protocols have user-recognized experience and responsible teams, and their reliable performance history also win them user trust. So it is not necessary for Polygon to reinvent the wheel. Therefore, Polygon has adopted a simple strategy of subsidising leading companies, including Aave, Curve, Uniswap and Quickswap, which can already meet the DeFi needs of most users.
- Games and metaverse pay more attention to unique experiences, and the experiences of different projects are quite different. Polygon has adopted the strategy of broad investment + incubation in this field, bringing more high-quality projects to Polygon chain through its investment.

- In the wider world beyond Web3, Polygon actively cooperates with various giants to realize the vision of “bringing the world into Ethereum”.

2.3.2 ZK Rollup

Rollup is currently the most recognized scaling solution of Ethereum executive layer, and its core is to execute transactions outside Ethernet mainnet, and only publish data to Ethereum mainnet, so as to achieve the purpose of scaling.

At present, there are two mainstream Rollup solutions, Optimistic Rollup and ZK Rollup. The main difference between them lies in how the mainnet verifies the transactions uploaded by Rollups.

Optimistic Rollup does not validate these transactions, but “optimistically” assumes that the transactions are all in good faith by default, setting a challenging period of time (7 days) during which anyone who has doubts about these transactions can challenge them by submitting a “fraud-proof”.

ZK Rollup summarizes the calculation results under the chain into a “validity proof”, which is then submitted to the mainnet of Ethereum.

Under the mechanism of zero-knowledge proof, although the contract of Ethereum mainnet does not “know” the actual situation of transactions, it can validate the authenticity of this batch of transactions by validating this “validity proof”, thus ensuring that ZK Rollup can expand its capacity while also inheriting the security of Ethereum mainnet.

ZK Rollup is the business direction where Polygon has been bullish in long run. In August, 21, it announced 1 billion US dollars would be used to support ZK technology. Polygon’s scaling solutions including zkEVM, Miden and Zero are also ZK Rollup solutions (Nightfall also uses some zk technologies).

Compared with Optimistic Rollup, ZK Rollup “will win in all use cases in the medium and long term with the improvement of ZK-SNARK technology” (Vitalik, 2021). However, due to the late development, the overall development progress of ZK Rollup is currently constrained by the lack of EVM compatibility. Polygon is committed to solving this problem, while also facing strong competitors such as Scroll, zksync and Starkware in this sector. For the competition landscape of ZK Rollups, we will explain it in Landscape of ZK Rollup Sector.

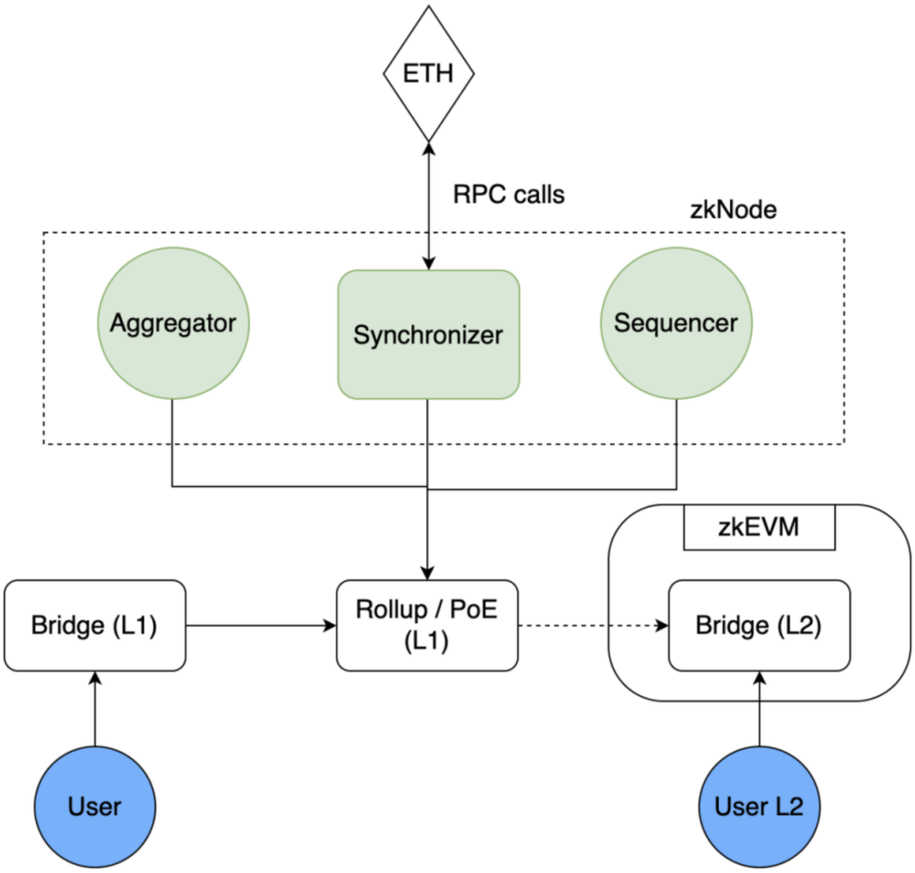
2.3.3 Polygon zkEVM: A ZK Rollup that Emphasizes EVM Compatibility

Polygon zkEVM was originally called Hermez. Hermez once had a version 1.0 product, which was successfully launched in March 2021. This version can support transfer payment scenarios, but not compatible with EVM.

In July 2021, Hermez team announced to develop ZKEVM (Hermez 2.0), which will bring a fully compatible ZKEVM to Ethereum after the development is completed.

Then in August 2021, Polygon acquired Hermez for US $250 million. The original Hermez token HEZ was exchanged at the exchange rate of 1 HEZ = 3.5 MATIC, and the acquisition was completed by tokens. At the same time, 26 members of Hermez team also merged into Polygon team.

The architecture of Polygon zkEVM (Hermez 2.0) is shown in the following figure:

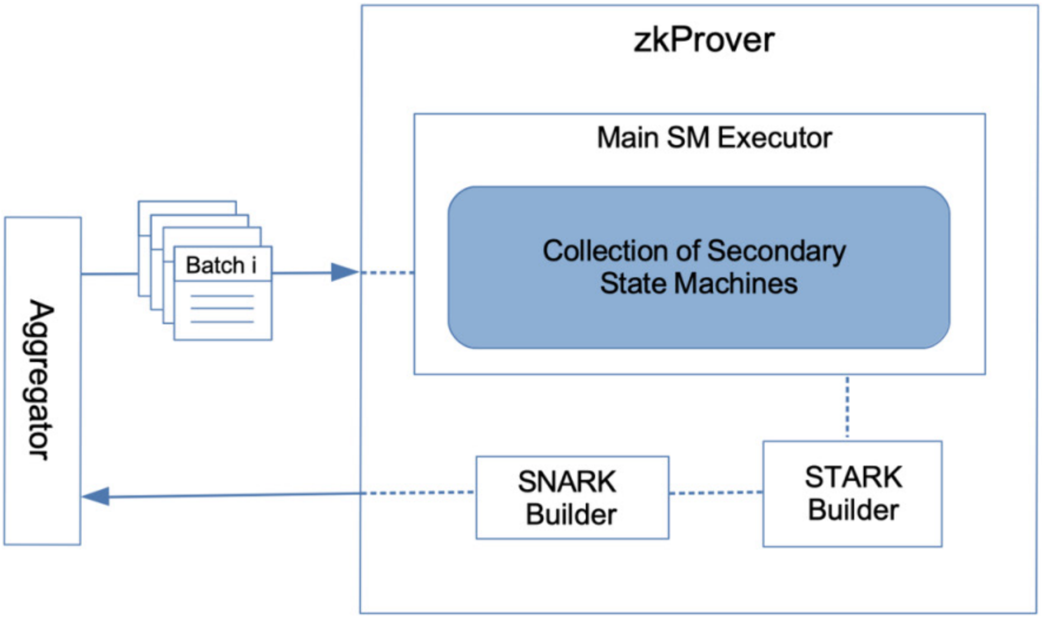


Source: [https://docs.hermez.io/zkEVM/Overview/Overview/# zkevms-architectural-overview](https://docs.hermez.io/zkEVM/Overview/Overview/#zkevms-architectural-overview)

Official documentation and data (https://docs.hermez.io/zkEVM/Overview/Overview/) for a clearer explanation. We will briefly describe the architecture of polygon zkevm here:

zkNode, which includes Sequencer, Aggregator, and Synchronizer

• Sequencer receives transactions from users, preprocesses them as a batch, and then submits the batch as a valid transaction to PoE (Proof of Efficiency) smart contract. Anyone with the software needed to run a zkEVM node can become a Sequencer, and a Sequencer proposing a valid batch can receive an incentive for a fee paid by a transaction requester or a network user.
• Aggregator is tasked with proving the validity of the L2 transaction proposed by Sequencer. In addition to running zkNode, Aggregator uses specialized hardware-zkProver to create zk Proof (zero-knowledge validity proof). Aggregator can charge Sequencer MATIC fees in return for providing this service.
• Synchronizer is responsible for reading events from Ethereum blockchain, including new batches, to keep the state completely synchronized. At the same time Synchronizer provides an external interface to obtain data, including the transaction data issued by Sequencer and the validity proof issued by Aggregator.
• zkProver is the core component of Polygon zkEVM and also the most complex module. The core computation and execution is conducted in zkProver, which means the compatibility of EVM needs to be guaranteed by zkProver. zkProver includes a main state machine executor, a set of auxiliary state machines, the SNARK proof components and the STARK recursion proof component.



zkProver Architecture Source: Official document

- Proof of Efficiency (PoE) consensus algorithm.

In Polygon zkEVM, Sequencer that generates new batches can get the reward for maintaining network consensus. PoE mechanism is mainly used to select Sequencers that can submit batches. PoE algorithm can maintain the normal operation of the whole Rollup network as efficiently and decentrally as possible.

- The bridge between Layer X and Layer Y is responsible for transferring funds from any Layer to other Layers.

On July 20th this year, Polygon shared the code of its zkEVM, and plans to open the unlicensed public test network in Q3 this year, and officially launch the mainnet in early 2023.

2.3.4 Polygon Zero:

Extremely Fast Recursive Proof

Polygon Zero is formerly Mir

Mir, founded in 2019, has been exploring recursive ZK proofs.

Recursive proof is simply “proof of proof”, that is, “a group of transactions” can be validated by validating “a transaction”, thus improving the validation efficiency of proof.

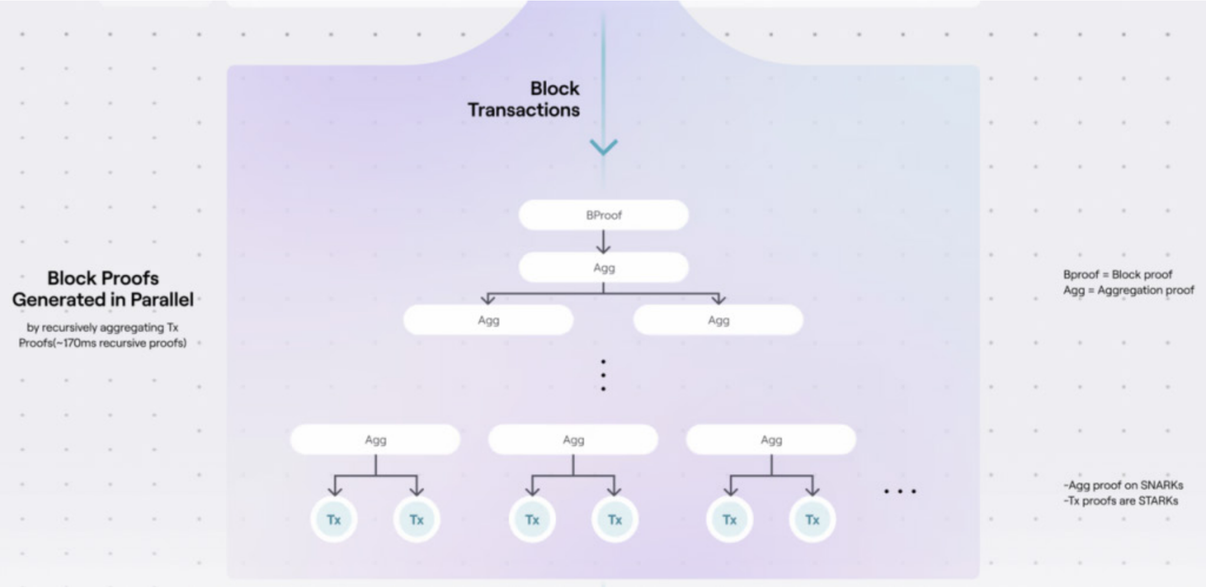
The Mir team released recursive proof Plonky2 proposed in 2020, able to generate recursive proof in 15 seconds.

In December 2021, Polygon acquired Mir for US $400 million (US $100 million +190 million MATIC tokens), and renamed Mir Polygon Zero. This acquisition, like the acquisition of Hermez, also acquired all Mir teams into Polygon teams.

At the same time of acquisition, Zero announced the release of Plonky2, which can generate a recursive proof in only 0.17 seconds on Macbook Pro, 100 times faster than the existing plan. It can also complete any proof (not limited to recursive proof) in 20 seconds. Plonky2 was made open source in January 2022.

Polygon Zero hopes to build zkEVM supported by Plonky2, which, if implemented, will probably be the most efficient and fast ZK proof system.

Zero does not have detailed public documents at present. According to some documents of official website and Mir, the proof process in Polygon Zero’s system is as follows:



Source: Polygon official website

- The system generates an aggregate proof for every two transactions.
- Then, a new aggregated proof is generated from the two aggregated proofs. After rounds of recursions, finally an aggregated single proof for all transactions (up to 3000 transactions) in one block is formed.
- Then a block proof is generated for this single proof.
- Finally, this block proof is uploaded to the Ethereum mainnet.

The fast recursive capability provided by Plonky2 is the key to implementing the above process.

Under this architecture, Zero will have the following significant advantages:

- The characteristic of recursive proof greatly reduces the cost of validating previous transactions for new validators when they join the network.
- The size of recursive proof is only 45kb.
- Because the most underlying proofs are generated in parallel, this gives Zero the ability to “horizontally scale up” its architecture: it only needs to add more machines

to the network to improve the network performance. This means that the throughput of the protocol is not limited by the weakest nodes on the network, but only by the total computation in the network.

In addition, the parallel recursive proof architecture also makes the nodes of Polygon Zero naturally acquire sharding features.

The key of sharding is to distribute the transaction records in a period of time to different groups to process them separately, and then integrate them into a complete block.

For example, the original system processes 100 transactions per second, but now with the system sharded into 10 shards, each shard can process 100 transactions per second. Theoretically, the system will have a parallel processing capacity of 1000 transactions per second.

However, a key problem of sharding is that the person in charge of the whole block must validate the correctness of records in each shard, because each shard is relatively centralized and error-prone. It is assumed that the 51% of nodes are required to modify a record of the mainnet, while the threshold for directly attacking a record of shard is 5.1% of nodes.

Obviously, when validating, we can’t ask a validator to completely recalculate the transactions in the original various shards, which makes sharding meaningless for scaling.

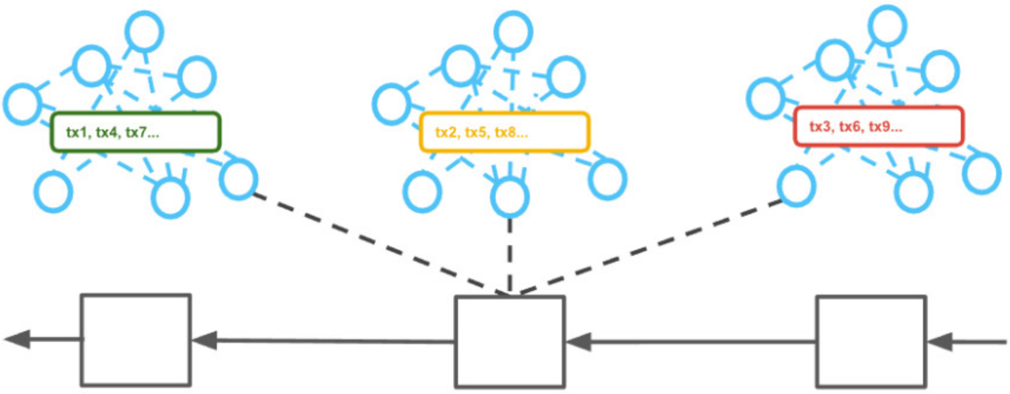
Also in the traditional field, the whole block cannot directly validate a single shard.

Therefore, the following strategies are usually adopted for sharding of public chains such as Ethereum:

1. There must be games within each shard. For example, the packer and the shard producer have to work separately. After packers finish the package, they bid to sell them to shard producers, while the shard producer has to be absolutely random.
2. The overall verification committee also needs division of labor to ensure efficiency, which must be random. Also the members of committee have to be changed frequently, otherwise the verifier can easily delete records by attacking only one verification group.

3. Through Kate-Zaverucha-Goldberg Polynomial Commitment (KZG) and other solutions, validators can validate shards separately to minimize the possibility of data missing.

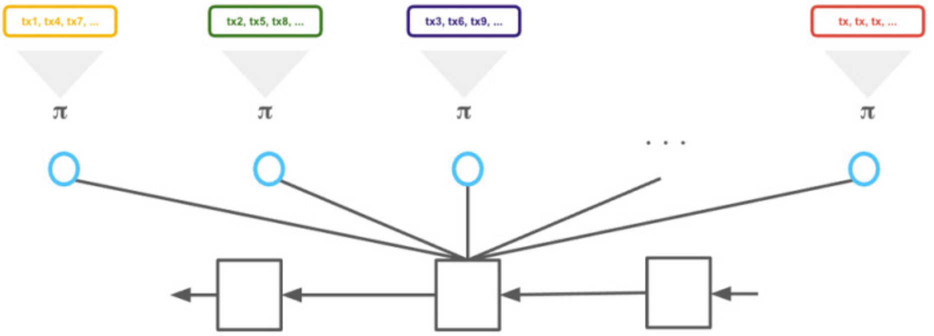
We can see that in the whole process of packaging, block generation, , and verification, several complex mechanisms based on games are needed to ensure security, which is a relatively inefficient parallel processing (sharding) mode.



Source: https://mirprotocol.org/blog/Recursive-proofs-on-Mir

However, in Polygon Zero, due to the characteristic of recursive zero-knowledge proof, the person in charge of the whole block can easily **and directly** read the validity of the transaction from the proof of each shard.

Therefore, the mechanism of Polygon zero sharding (parallel processing) is far simpler and more efficient than the traditional sharding based on the game theory.



Source: https://mirprotocol.org/blog/Recursive-proofs-on-Mir

Of course, ZK Rollup-level shards can only promote the operation efficiency of Layer2 chain itself. To realize the scaling of whole system, the compression rate of the whole ZK Rollup to transactions has to be improved.

2.3.5 Polygon Miden: STARK-based Open-source zkVM

Polygon Miden is a ZK Rollup based on STARK (Scalable Transparent Argument of Knowledge).

At present, most ZK Rollup are based on SNARK (Succinct Non-Interactive Argument of Knowledge), and only Starkware and Polygon Miden are developing ZK Rollup based on STARK.

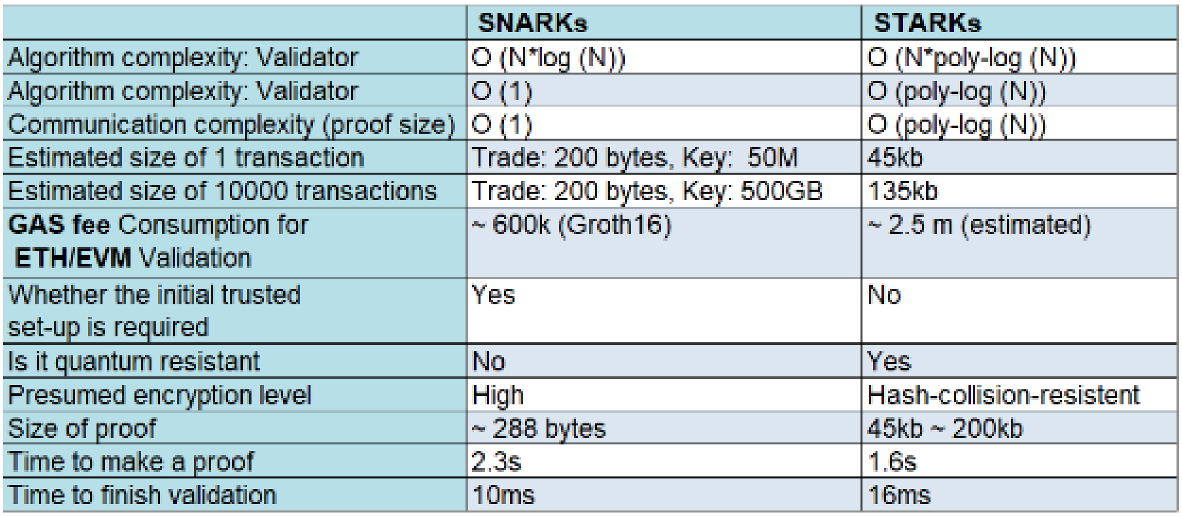
About: STARK and SNARK

ZK-SNARKs proposed in 2012 that there are many related researches and practices (Zcash, Loopring and JP Morgan Chase), which are generally more mature.

It enjoys advantages in metrics of verification time, compression effect, Gas fee consumption.

ZK-STARKs was officially published in an academic paper in 2018, and was proposed by team Starkware. Compared with SNARK, ZK-STARKs is believed to have the advantages not requiring a trusted set-up and enjoying quantum resistance, believed to be ***safer in the long run.***

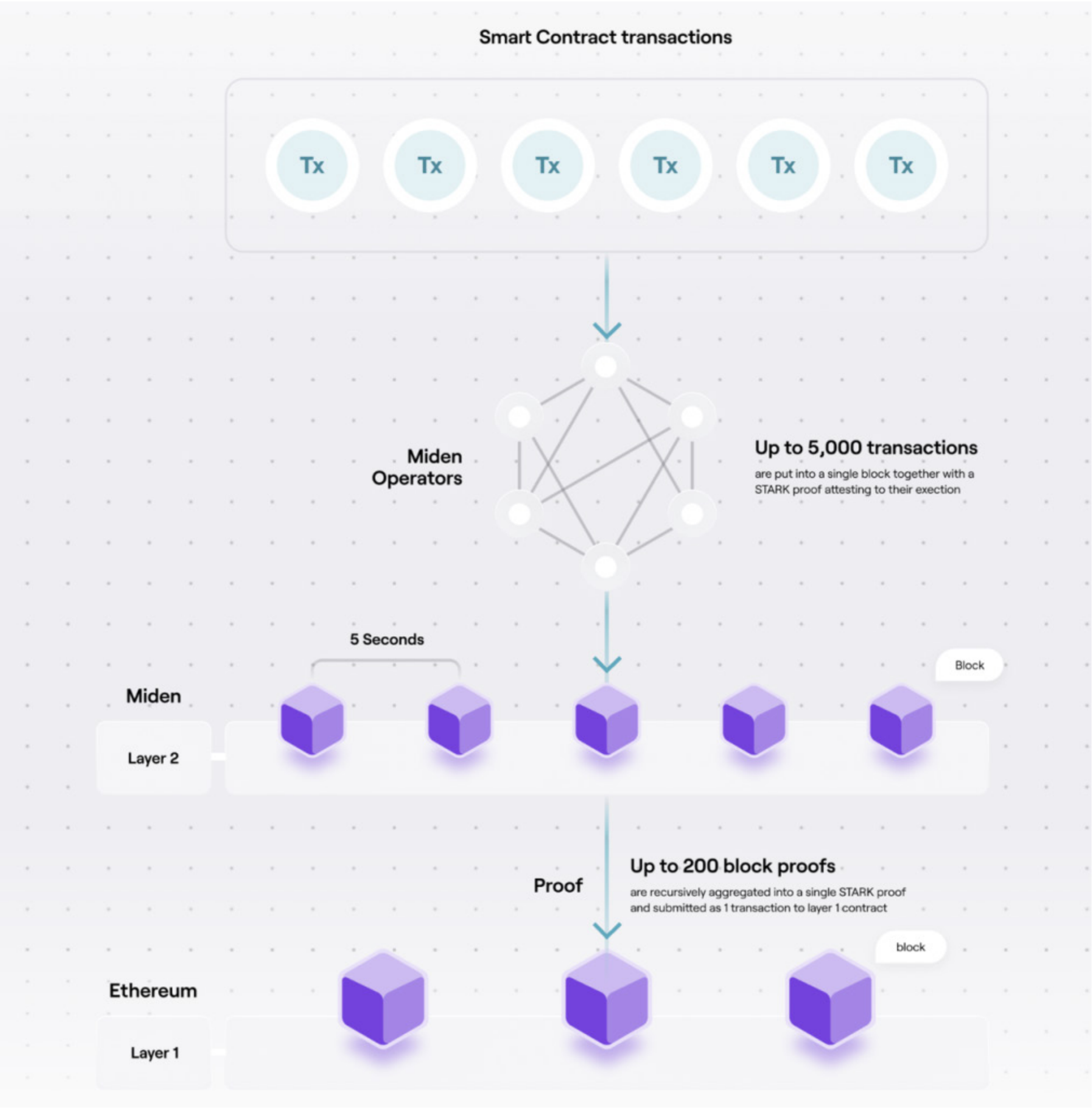
The comparison between the two can be seen in the following table:



	SNARKs	STARKs
Algorithm complexity: Validator	O (N*log (N))	O (N*poly-log (N))
Algorithm complexity: Validator	O (1)	O (poly-log (N))
Communication complexity (proof size)	O (1)	O (poly-log (N))
Estimated size of 1 transaction	Trade: 200 bytes, Key: 50M	45kb
Estimated size of 10000 transactions	Trade: 200 bytes, Key: 500GB	135kb
GAS fee Consumption for **ETH/EVM** Validation	~ 600k (Groth16)	~ 2.5 m (estimated)
Whether the initial trusted set-up is required	Yes	No
Is it quantum resistant	No	Yes
Presumed encryption level	High	Hash-collision-resistent
Size of proof	~ 288 bytes	45kb ~ 200kb
Time to make a proof	2.3s	1.6s
Time to finish validation	10ms	16ms

Source: https://consensys.net/blog/blockchain-explained/zero-knowledge-proofs-stars-vs-snarks/

The architecture of Miden is shown in the following chart:


Smart Contract transactions
Tx
Tx
Tx
Tx
Tx
Tx
Miden Operators
Up to 5,000 transactions
are put into a single block together with a STARK proof attesting to their exection
5 Seconds
Block
Miden
Layer 2
Proof
Up to 200 block proofs
are recursively aggregated into a single STARK proof and submitted as 1 transaction to layer 1 contract
block
Ethereum
Layer 1

Source: Polygon official website

- The transaction is first sent to Miden's execution node;
- The execution node bundles 5000 transactions into the block at a time and generates STARK proofs;
- Miden Layer 2 aggregates 200 blocks and generates a STARK proof to prove that these 200 bundled blocks (each containing 5,000 transactions) are valid;
- Finally, STARK proof will be uploaded to Ethereum to reach a consensus.

The core components of Miden include Miden VM and Winterfall:

The Miden VM was formerly the Distaff VM: the first STARK-based virtual machine.

Distaff has been in development since early 2020 and has gone through multiple development and user testing iterations.

Winterfe is a high-performance STARK validator developed by the Miden founder Bobbin when he was at Facebook.

According to the official introduction, we summarize the main characteristics of Miden as follows:

- Compared with ZK Rollup using SNARK proof, Miden adopts STARK proof which is safer in the long run (although it is more expensive in the short run, it can be processed by recursive proof in the future);
- Miden is completely open source compared to Starkware-related products that also use STARK proof.
- Developer-friendly: Miden's goal is to enable developers to run smart contracts on top of this zkVM without even learning anything about cryptography or zk proof.
- Support for multiple programming languages: In addition to Solidarity, the team is working to increase support for multiple programming languages, including Move.

Miden VM has released its alpha version, and its Turing's complete version 0.2 has just been released on August 22, with its official version planned to be launched in 2023 Q1.

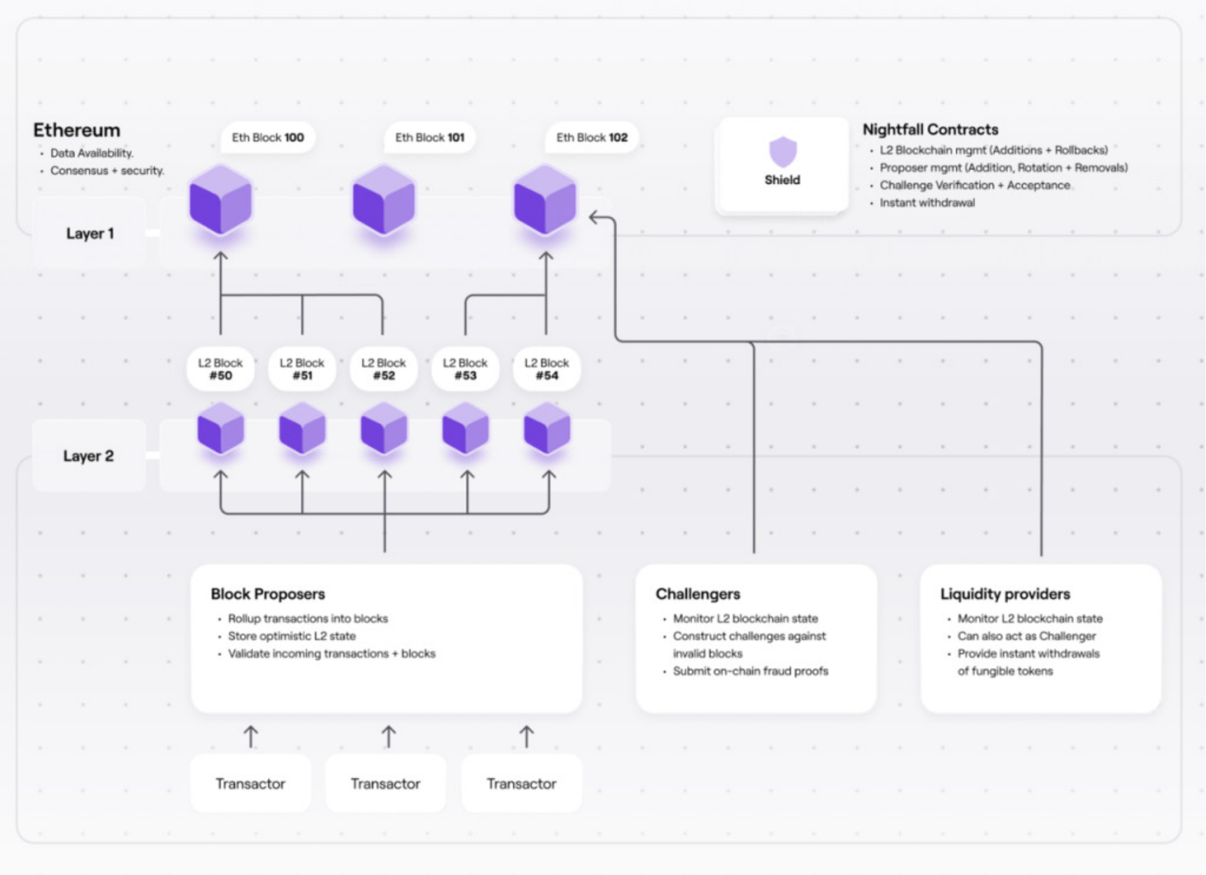
2.3.6 Polygon Nightfall: A Blockchain Solution for Enterprises

Polygon launched Polygon Nightfall in September 2021 after forming a partnership with Ernest & Young, the giant of accounting and business services.

In May 2022, Polygon Nightfall launched its testnet, and plans to launch its mainnet this year.

In fact, Ernst & Young has been working on Nightfall since 2019, and aims to provide blockchain services for enterprises. Therefore, in the related design of Nightfall, the privacy of transactions has always been emphasized, which means users' on-chain transactions are not completely open.

They initially hoped to build on the mainnet of Ethereum, but later found it expensive to save privacy on it. So they turned to L2 chains and chose to work with Polygon.


Ethereum
• Data Availability.
• Consensus + security.
Eth Block 100
Eth Block 101
Eth Block 102
Shield
Nightfall Contracts
• L2 Blockchain mgmt (Additions + Rollbacks)
• Proposer mgmt (Addition, Rotation + Removals)
• Challenge Verification + Acceptance
• Instant withdrawal
Layer 1
L2 Block #50
L2 Block #51
L2 Block #52
L2 Block #53
L2 Block #54
Layer 2
Block Proposers
• Rollup transactions into blocks
• Store optimistic L2 state
• Validate incoming transactions + blocks
Challengers
• Monitor L2 blockchain state
• Construct challenges against invalid blocks
• Submit on-chain fraud proofs
Liquidity providers
• Monitor L2 blockchain state
• Can also act as Challenger
• Provide instant withdrawals of fungible tokens
Transactor
Transactor
Transactor

Architecture of Polygon Nightfall Source: Polygon official website

Polygon Nightfall is essentially an Optimistic Rollup, added with many characteristics of zero-knowledge proof, thus realizing the anonymity of transaction records (after zk technology matures, Polygon Nightfall will adopt a complete ZK Rollup solution in the future).

For enterprises, **the main advantages of Nightfall is its security, privacy, and efficiency:**

- The characteristics of Rollup make Nightfall inherit the security of ETH, which can effectively reduce the cost of trust;
- The application of zk technology makes it unnecessary for enterprises to disclose complete transaction records to the outside world, which is convenient for some businesses to carry out;
- Rollup greatly reduces the cost of the network;

In addition, Polygon Nightfall adopts the fund pool model, where the fund pool provider completes the 7-day fraud proof period for enterprises, thus helping to realize efficient enterprise operation.

According to Polygon official website, Nightfall’s main target use case is the supply chain industry. Compared with the current supply chain industry, Nightfall can provide traceable and unchangeable supply chain data, efficient data check and authenticity validation as well as safe payment, fast settlement and low transaction costs.

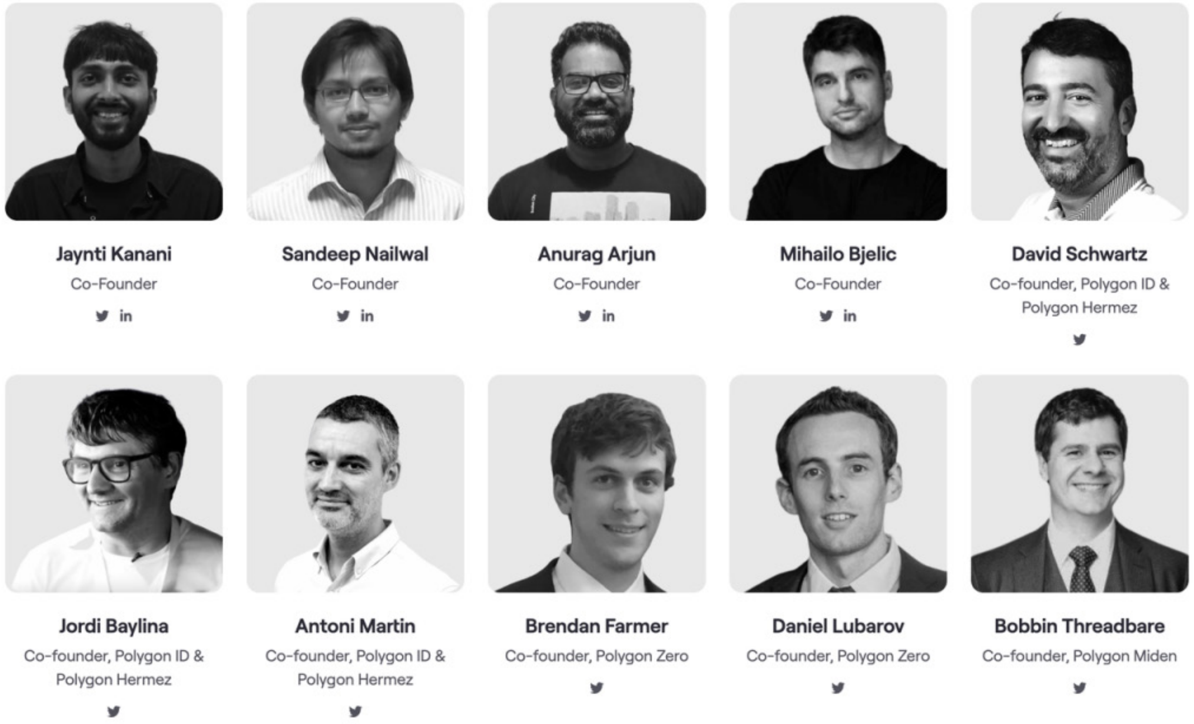
Although the actual business situation needs to be tested after going live, this cooperation with Ernst & Young shows the Polygon team’s good strategy building and implementation ability: it can make promotions with the help of Ernst & Young’s broad channels for enterprise services on a global scale; At the same time, it does not merely depend on technologies, but choose the most practical way of Optimistic Rollup + ZK + fund pool to meet the business needs practically.

2.4 Financing and Team Profile

2.4.1 Financing

- MiH Ventures participated in Polygon seed round investment with an investment amount of 165,000 US dollars.
- On April 24, 2019, the official announced IEO in Binance, raising 5 million US dollars at a price of $0.00263, accounting for 19% of the total tokens.
- On April 30, 2019, the official announced that it had obtained the seed round financing of US $450,000 from Coinbase Ventures, accounting for 1.71% of tokens.
- On December 20, 2020, Polygon announced that it had received an investment of $1 million from angel investor John Lilic.
- On February 7, 2022, Polygon received a financing of US $450 million led by Sequoia Capital (India) (the financing cost was not disclosed). The participating investors included Tiger Global, Softbank, Galaxy Digital, Republic Capital, Makers Fund, Alameda Research, Alan Howard, Alexis Ohanian, Steadview Capital, Elevation Capital, Animoca Brands, Spartan Fund, Dragonfly Capital, Variant Fund and Kevin O’leary and other 37 institutions and individuals.

2.4.2 Team Profile



Jaynti Kanani
Co-Founder

Sandeep Nailwal
Co-Founder

Anurag Arjun
Co-Founder

Mihailo Bjelic
Co-Founder

David Schwartz
Co-founder, Polygon ID & Polygon Hermez

Jordi Baylina
Co-founder, Polygon ID & Polygon Hermez

Antoni Martin
Co-founder, Polygon ID & Polygon Hermez

Brendan Farmer
Co-founder, Polygon Zero

Daniel Lubarov
Co-founder, Polygon Zero

Bobbin Threadbare
Co-founder, Polygon Miden

The Polygon team initially had four co-founders, three of whom were from India:

Jaynti Kanani, co-founder & CEO, graduated from the School of Engineering of Dharmsinh Desai University in India in 2011, and had been engaged in development since then until he co-founded Matic Network in 2017.

Sandeep Nailwal, co-founder & COO, graduated from the National Institute of Industrial Engineering in Mumbai, India, worked as a consultant at Deloitte, and has been engaged in operations since then.

Anurag Arjun, graduated from Polytechnic Institute of Nilma University, India in 2006, and worked as product and project manager in several companies.

Mihailo Bjelic, the co-founder.

He studied information system engineering at Belgrade University.

After a series of mergers and acquisitions, the team has absorbed the following core members:

David Schwartz,was originally the project leader of Hermez. David has more than 20 years of experience in the IT industry and has been working on blockchain since 2018. Besides Hermez, he also founded the DID-oriented project Iden3, which is also one of the underlying protocols of PolygonID.

Jordi Baylina, is the technical lead for Polygon zkEVM.

Jordi is a senior Solidarity developer and co-founder of White Hat Group. He once played an important role in TheDAO and Parity Multisig hacking, and participated in audited projects including MakerDAO and Aragon, enojoying a great influence in the Ethereum developer community.

Antoni Martin is responsible for the cooperation between Polygon and enterprises,with nearly 20 years of experience in the banking system.

Bredan Farmer and Daniel Lubarov, were originally co-founders of Mir. Bredan previously worked on research at Duke University, and Daniel had worked at payment companies Square and Google.

Plonky2 proposed by them can generate recursive proof in 0.17 seconds, which greatly improves the commercial process of recursive proof.

Bobbin Threadbare, is in charge of the Miden business, an STRAK expert with many contributions made in the zk-STARK area.

In addition, **Ryan Wyatt** is responsible for leading Polygon Studios. He was once the head of Google's Global Game Partner Program and head of YouTube Game, and once engaged in e-sports projects as a game commentator, enjoying an undeniable influence in the game field.

Polygon also has a strong advisory team, with its members including Hudson Jameson, the core contributor in Zcash and Ethereum, Ryan Sean Adams, co-founder of Bankless, Pete Kim, wallet engineering director of Coinbase, and billionaire Mark Cuban, etc.

In general, Polygon’s team and consultants for crypto projects are diverse in their background, which also reflects the team’s equal stress on technique and operation.

During Polygon’s development, despite its originally-planned scaling solution Plasma gradually fell behind its competitors, it took several timely adjustments to its business direction. It has demonstrated strong strategic planning and implementation ability, which can be reflected in:

• Before DeFi Summer started in June 20, Polygon launched the side chain of PoS architecture, earlier than BNB Chain launched on September 1. At the same time, after BNB Chain successfully absorbed Ethereum traffic with developer subsidies, The Polygon team also responded quickly, and followed up to launch the subsidy strategy in April 21, and an ecosystem-targeted fund to directly subsidize the user behavior of the leading applications, which quickly improved the TVL application data, thus making Polygon an important participant in the narrative of the public chain war throughout 2021.

• In August 2021, when Optimistic Rollups Arbitrum and Optimism were not launched yet, it announced an investment plan of 1 billion US dollars in the ZK sector. It also quickly bound two excellent ZK teams, Hermez and Mir, into their own ecosystem through merger and acquisition of personnel and projects. These measures greatly improved its technical capabilities in the ZK field, which is also one of the few successful mergers and acquisitions in Crypto field (as faras we can see now). Moreover, this kind of merger and acquisition has produced a good synergy effect in the ZK field, where the business directions of zkEVM, Zero and Miden are diverse and complementary. For example, Polygon zkEVM took Polygon Zero’s advice to choose 64-bit-small-field STARK proof generation.

3. Business Analysis

3.1 Industry Space and Potential

According to Tomasz Tunguz, managing director of Redpoint, there are currently 5 billion Internet users in the world, millions of blockchain users; There are about 27 million Internet developers worldwide, while tens of thousands of Web 3 developers.

If we believe that in the not-too-distant future, Web3 will bring in the vast majority of Web2 users by giving them wider freedom and cheaper trust, then huge space for growth still exist in terms of number of users and developers.

Of course, it is a long-term process for Web2 users to migrate to Web3, and it also requires waiting for further improvement of infrastructure. However, the huge development space presents a huge opportunity for smart contract public blockchains represented by Ethereum.

Ethereum is the pioneer of smart contract public chain and also the most representative smart contract public chain.

In the past seven years, we have seen the great possibilities brought by smart contracts to Ethereum: users can trade, borrow, manage money, play games, create and socialize on the chain. In this cycle, we have seen how Axie Infinity and StepN have deeply changed the lifestyles of millions of people in a period of time.

More importantly, all this happens on the trustless and permissionless blockchains, and all behaviors are bound by the rules made public in advance, with all modifications to the rules open and transparent: codes, not people, govern everything.

The ultimate goal of smart contract public chains is to carry various business activities of billions of people. If it is realized, the counterpart of its final form in Web2 would be a state rather than a company such as Google and Meta.

In 2020-2021, when the on-chain wave of DeFi, NFT and Game came one after another, the high cost and slow reaction of Ethereum seriously affected the user experience and the development of Ethereum itself.

Against such a backdrop, a series of low-cost and high-speed public chains or cross-chain platforms have developed rapidly, which has also created a number of new projects, such as Solana, Polkadot, Cosmos, Polygon and Avalanche, which rank among the top 20 in crypto market value.

In essence, the scaling solution of Ethereum and other L1 public chains all aim to provide scalability, with different implementation paths: depending on Ethereum or replacing Ethereum.

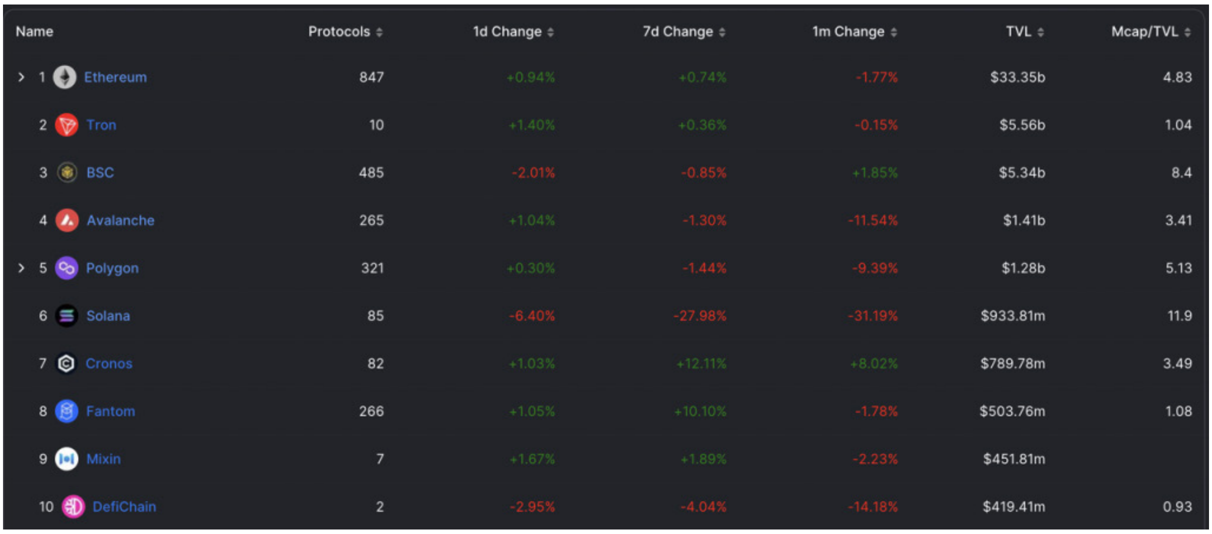
Although it is in a bear market at present, capitals are still actively invested in the new public chain and various Rollup solutions, which also shows capital's recognition of the scaling sector.

It is fair to say the Ethereum scaling sector where Polygon is located presents a vast industry space, and is one of the most attractive narratives in the whole crypto world in the past and in the future.

3.2 Competition Landscape of Polygon PoS

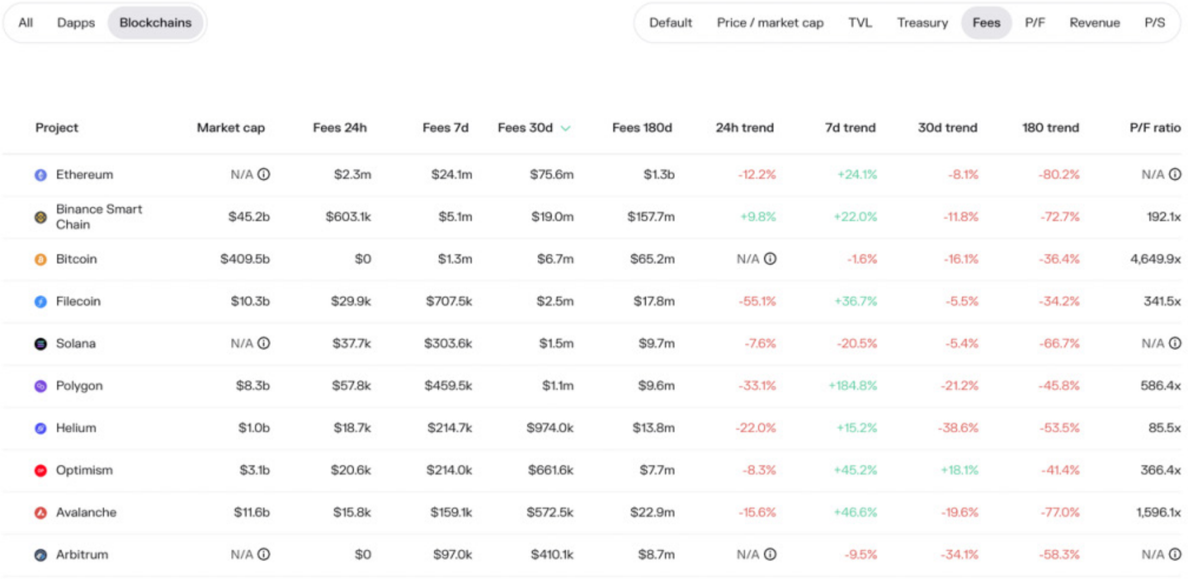
In the current crypto bear market, the competition landscape of smart contract public chains is also constantly changing: Terra crashed tragically, Fantom fell down, Tron quietly climbed to second place in TVL, and the new public chains Aptos and Sui gradually attracted market attention recently, which also concealed Solana's highlight moments.

Traditionally, crypto investors usually use TVL and the fees paid by users as the main metrics to measure the competition between public chains.



Name	Protocols	1d Change	7d Change	1m Change	TVL	Mcap/TVL
1 Ethereum	847	+0.94%	+0.74%	-1.77%	$33.35b	4.83
2 Tron	10	+1.40%	+0.36%	-0.15%	$5.56b	1.04
3 BSC	485	-2.01%	-0.85%	+1.85%	$5.34b	8.4
4 Avalanche	265	+1.04%	-1.30%	-11.54%	$1.41b	3.41
5 Polygon	321	+0.30%	-1.44%	-9.39%	$1.28b	5.13
6 Solana	85	-6.40%	-27.98%	-31.19%	$933.81m	11.9
7 Cronos	82	+1.03%	+12.11%	+8.02%	$789.78m	3.49
8 Fantom	266	+1.05%	+10.10%	-1.78%	$503.76m	1.08
9 Mixin	7	+1.67%	+1.89%	-2.23%	$451.81m	
10 DefiChain	2	-2.95%	-4.04%	-14.18%	$419.41m	0.93

Public chain TVL ranking Data source: Defillama



All Dapps **Blockchains**

Default Price / market cap TVL Treasury **Fees** P/F Revenue P/S

Project	Market cap	Fees 24h	Fees 7d	Fees 30d	Fees 180d	24h trend	7d trend	30d trend	180 trend	P/F ratio
Ethereum	N/A ⓘ	$2.3m	$24.1m	$75.6m	$1.3b	-12.2%	+24.1%	-8.1%	-80.2%	N/A ⓘ
Binance Smart Chain	$45.2b	$603.1k	$5.1m	$19.0m	$157.7m	+9.8%	+22.0%	-11.8%	-72.7%	192.1x
Bitcoin	$409.5b	$0	$1.3m	$6.7m	$65.2m	N/A ⓘ	-1.6%	-16.1%	-36.4%	4,649.9x
Filecoin	$10.3b	$29.9k	$707.5k	$2.5m	$17.8m	-55.1%	+36.7%	-5.5%	-34.2%	341.5x
Solana	N/A ⓘ	$37.7k	$303.6k	$1.5m	$9.7m	-7.6%	-20.5%	-5.4%	-66.7%	N/A ⓘ
Polygon	$8.3b	$57.8k	$459.5k	$1.1m	$9.6m	-33.1%	+184.8%	-21.2%	-45.8%	586.4x
Helium	$1.0b	$18.7k	$214.7k	$974.0k	$13.8m	-22.0%	+15.2%	-38.6%	-53.5%	85.5x
Optimism	$3.1b	$20.6k	$214.0k	$661.6k	$7.7m	-8.3%	+45.2%	+18.1%	-41.4%	366.4x
Avalanche	$11.6b	$15.8k	$159.1k	$572.5k	$22.9m	-15.6%	+46.6%	-19.6%	-77.0%	1,596.1x
Arbitrum	N/A ⓘ	$0	$97.0k	$410.1k	$8.7m	N/A ⓘ	-9.5%	-34.1%	-58.3%	N/A ⓘ

Public chain annualized cost Data source: Tokenterminal

In terms of TVL, Polygon currently has a 1.28 billion TVL, ranking fifth.

In terms of fees paid by users, the fees paid by Polygon users rank sixth among all blockchains (it ranks fourth excluding Bitcoin and Filecoin).

In terms of TVL and public chain data, Polygon's competitors include BNB Chain, Solana, Avalanche, Optimization, Arbitrum, Cosmos and Polkadot.

The characteristics and competitive situation of these public chains are a big topic, which is described in great detail in the article *Finding a home for labs*

Finding a home for labs published by Delphi Digital in early September. So we will just briefly describe the characteristics of current public chains as follows:

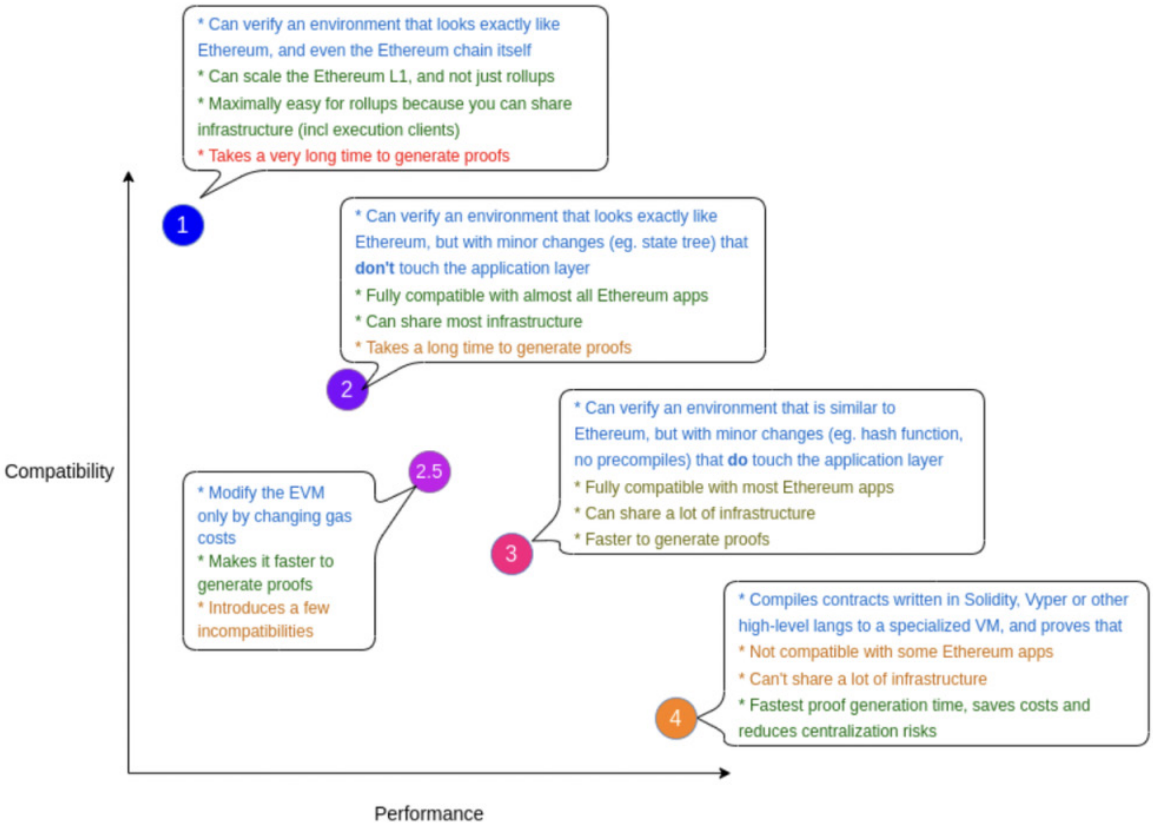
- BNB Chain is a chain under Binance, enjoying the most stable user source in the crypto world, and having carried out continuous subsidy and incentive policies. BNB Chain approaches or even surpasses Ethereum in many aspects of data. However, compared with other public chains, its ecosystem is relatively "closed", and it also has obvious characteristics of "planned economy".
- Solana has achieved the acme of the current crypto world in terms of single-chain scaling, and TPS has reached several thousand orders of magnitude. There are many DeFi applications on chain, and the NFT ecosystem is relatively prosperous, with the appearance with of a million-user hot application such as StepN. However, after a large number of users poured into Solana, its network "downtime" events occurred more frequently, which made people have fundamental concerns about network security.

The two new public chains of Move language with similar technical solutions and investment backgrounds have also made continuous progress: Polygon Avail has launched its test network on June 18, 2022. The rapid development of similar competing products has also had a great impact on Solana.

• Arbitrum and Optimism, two Layer2 solutions adopting Optimistic Rollup, have good EVM compatibility. At the same time, like Polygon, they also attract many blue-chip DeFi projects and corresponding developers in Ethereum, and innovative projects in the chain are emerging one after another. However, constrained by the architecture, although their gas fee is obviously reduced compared with the mainnet of Ethereum, it still registers a level of tens of cents to several dollars, which is still not low enough (although the situation will be improved after EIP-4488), and their TPS is not much higher than that of the mainnet of Ethereum. Also, the decentralization degree of Sequencer, which is responsible for transmitting data to the mainnet of Ethereum, has also been questioned.

• Although Cosmos has experienced the collapse of Terra, the largest chain in the ecosystem, it still attracts more and more developers with its high autonomy and customization (such as using its own token as Gas token, and self-building of its own verifier network, etc.), high interoperability and rich development tools. Recently, dYdX decided to move from StarkEx to Cosmos. At present, the main issue facing Cosmos is still its slow development. At present, the total TVL in the ecosystem is not high, and the non-EVM experience also raises the threshold of some users.
• Polkadot, as another cross-chain giant, has the advantage over Cosmos in that its parallel chain can share the security of relay chains based on heterogeneity, but this is at the huge expense of sacrificing the sovereignty of parallel chains. Recently, Acala, the core parallel chain in the ecosystem, has experienced hacker attacks, while the development of other parallel chains is relatively plain. And there is still a gap between the project activity in its ecosystem and Cosmos.
• Avalanche has a high TVL at present, and they have also launched an application subnet architecture similar to Cosmos, which gives developers higher autonomy. At present, two GameFi projects DefiKingdoms and Crabada have successfully launched Avalanche subnet.

3.2.1 Landscape of ZK Rollup Sector


* Can verify an environment that looks exactly like Ethereum, and even the Ethereum chain itself
* Can scale the Ethereum L1, and not just rollups
* Maximally easy for rollups because you can share infrastructure (incl execution clients)
* Takes a very long time to generate proofs
1
* Can verify an environment that looks exactly like Ethereum, but with minor changes (eg. state tree) that **don't** touch the application layer
* Fully compatible with almost all Ethereum apps
* Can share most infrastructure
* Takes a long time to generate proofs
2
* Can verify an environment that is similar to Ethereum, but with minor changes (eg. hash function, no precompiles) that **do** touch the application layer
* Fully compatible with most Ethereum apps
* Can share a lot of infrastructure
* Faster to generate proofs
Compatibility
2.5
* Modify the EVM only by changing gas costs
* Makes it faster to generate proofs
* Introduces a few incompatibilities
3
* Compiles contracts written in Solidity, Vyper or other high-level langs to a specialized VM, and proves that
* Not compatible with some Ethereum apps
* Can't share a lot of infrastructure
* Fastest proof generation time, saves costs and reduces centralization risks
4
Performance

According to Vitalik's classification of ZK Rollup based on the their trade-offs on performance and compatibility, ZK Rollup is divided into five types of projects (as shown above):

Type 1:

zkEVM that is completely equivalent to Layer 1 chain Ethereum. At present, PSE team of Ethereum Foundation making explorations on this zkEVM.

Type 2:

A zkEVM, completely equivalent to EVM, slightly different from Ethereum. Such as the upcoming Scroll and Polygon zkEVM.

Type 2.5:

A zkEVM Equivalent to EVM, with only difference in gas fees (which may result in subtle compatibility differences). This is the direction where Scroll and Polygon zkEVM are moving to.

Type 3:

A zkEVM almost equivalent to zkEVM. Such as Scroll and Polygon zkEVM at this stage.

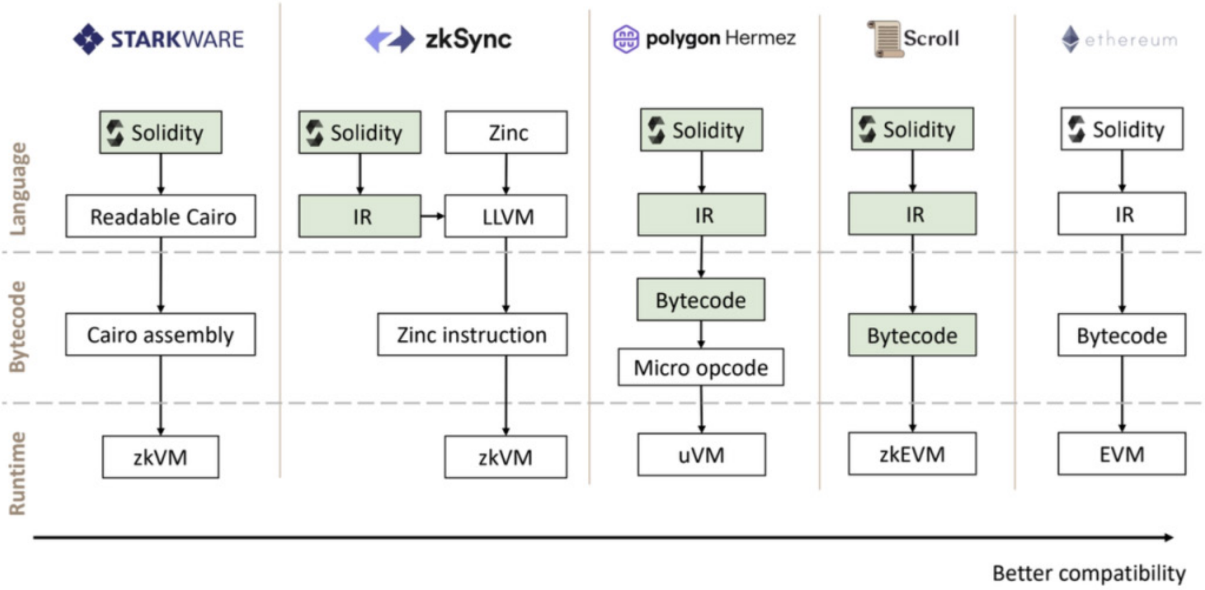
Type 4:

The zkEVM, which is compatible with EVM at the language level. It has different features and developer facilities, and developers cannot write manually EVM Bytecode. The Type4 zkEVM has zkSync and StarkNet with the addition of Solidity to the Cairo compiler.

It is worth pointing out that the aforementioned different types of Rollups are not absolutely superior than another, and their differences lie in their trade-offs made on the performance and adaptability: the larger the serial number, the better its performance, but the lower its compatibility with EVM; The smaller the sequence number, the better the adaptability to EVM, but the performance will be relatively poor.

Polygon’s competitors in ZK Rollups include Scroll, zkSync and Starknet, among which Scroll has the closest level with it.

The following diagram can also show the differences in compatibility between these projects:



Source: Scroll team

The financing background and development progress of Scroll, zkSync and Starknet are as follows:

• In April 2022, Scroll completed the financing of USD 30 million led by Polychain Capital, with the participation of Bain Capital Crypto, Robot Ventures and Geometry DAO. Some angel investors, including Ying Tong and Carlos Aria of Ethereum Foundation, and members of Ethereum Community Anthony Sassal, Ryan Adams and Santiago Santos also joined this round of financing. Scroll released the publicly-tested Pre-alpha version on July 15th. Its roadmap shows that there will be Alpha testing in the future and the complete testnet testing will be started at the end of the year and the mainnet will be launched next year.
• Matter Labs, the development team of zkSync, has completed three rounds of financing, the latest of which was the $50 million financing led by a16z in November 21, with Placeholder, Dragonfly, 1kx and 70 other institutions or individuals participating in the investment. zkSync launched a testnet for its EVM-compliant

product zkSync 2.0 in February 2022, and its mainnet is expected to be launched on October 28.

• Starkware, the development team of Starknet, has completed a total financing of 273 million US dollars, with investors including Paradigm, Sequoia Capital, Pantera Capital and other famous institutions. In the latest round of investment in May 2022, Starkware's valuation reached 8 billion US dollars. Starknet has launched its Alpha version on mainnet since November 2021, with a series of improvements still in progress.

We can roughly see that zkEVM is currently under development. Since the project with better EVM compatibility registers slower development progress, so while Scroll has the best EVM compatibility, its shows slowest development progress.

In Vitalik's view, the future of Ethereum is not a single Rollup controlling everything, but a world where multiple Rollups coexist.

From this point of view, project parties exploring ZK Rollup are not in a complete competitive relationship. At present, the sector is far from the point of a cut-throat competition, and all ZK Rollup may enjoy a bright future.

However, in the short and medium term, teams able to first bring the normal operation of ZK EVM on the mainnet will enjoy a great first-mover advantage in the competition.

From the current situation, Polygon zkEVM is expected to become the first Type 3 ZK Rollup on mainnet.

3.3 Token Model Analysis

3.3.1 Token Function

Polygon's native token is MATIC. At present, its functions mainly include two points:

- Maintain network consensus: Matic side chain uses PoS mechanism to reach a consensus, and users stake MATIC tokens to participate in block generation and obtain income from staking.
- Transaction fees in payment network: The transaction fees on the Matic side chain are paid in MATIC tokens (the transaction fees of a series of sub-projects of ZK Rollup are paid in ETH).

3.3.2 Token Allocation and Unlock

The initial tokens totaled 10 billion, which were officially circulated in April 2019.

Here's how the allocation works:

Private sale tokens account for 3.80% of the total supply, 50% of which were released in TGE (token generation event), and the remaining 50% were released after being locked for 6 months.

Of which:

- **Seed round of Mih Ventures**: raised a total of $165,000 by selling MATIC at $0.00079 per token, with1.71% of the total token supply sold out.
- **Early Supporter (Coinbase Ventures)**: raised a total of $450,000 by selling MATIC at $0.00263 per token, with1.71% of the total token supply sold out.

Binance Launchpad sold tokens, accounting for 19% of overall supply.

It was conducted in April 2019 and raised a total of about $5,000,000 worth of BNB, with each token about $0.00263, accounting for 19% of the total token supply, which is fully circulated at TGE.

Team tokens accounted for 16% of overall supply.

This part of tokens will be locked for one year, and each time 1/5 will be released per six months from April 2020, released out in April 2022.

Consultant tokens accounted for 4% of the total supply.

Each 1/3 of these tokens were released after 6 months, 12 months and 18 months after TGE, and were released out in December 2020.

Network Operation tokens accounted for 12% of overall supply.

1/3 of this token was released in TGE, and the rest was released linearly in 32 months, which was released out in December 2021.

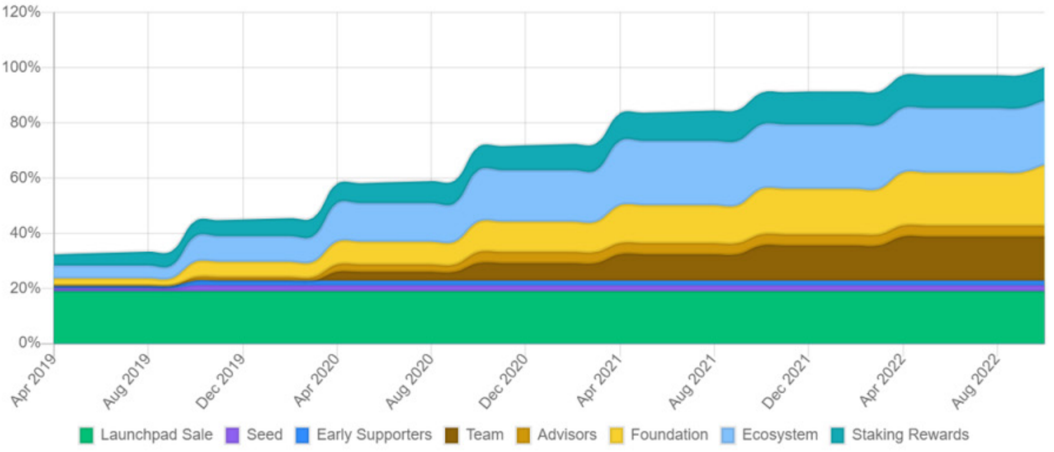
Foundation tokens accounted for 21.86% of the total supply.

1/5 of this token was released in TGE, and the rest was released per half a year, to be released out in April 2021.

Ecosystem tokens accounted for 23.34% of the total supply.

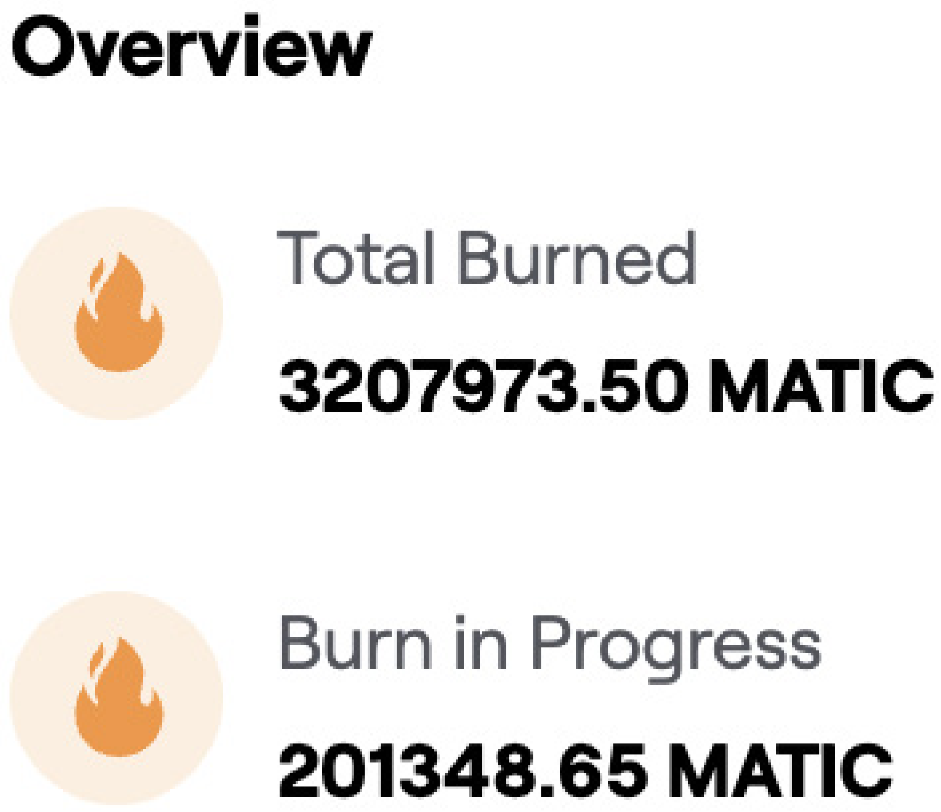
1/8 of these tokens were released in TGE, and 1/8 of the rest was released each time per half a year, to be released out in October 2022.

The token release plan is shown in the figure:



At present, all tokens are theoretically in circulation, but 10% of foundation tokens are still not in circulation, and 2.7% of tokens are still in unlocked contracts. So Binance and other exchanges have adopted 87.3% as the actual circulation rate.

It is also worth mentioning that Polygon launched an update similar to EIP-1559 in January this year, and MATIC will benefit from the prosperity of this network. At present, the total number of burned MATIC is 3.11 million, accounting for 0.03% of the total.



Overview

Total Burned

3207973.50 MATIC

Burn in Progress

201348.65 MATIC

Source: https://burn.Polygon.technology/

3.4 Risk

As far as Polygon’s current development, PoS is its development base, while its several ZK Rollup sub-projects are important potential growth points in the future

Potential risks of the project investment:

- Polygon PoS lost the subsequent public blockchain competition, failing to attract and retain developers and users
- The scaling of Ethereum has undergone a major technical direction change, making the direction of ZK Rollup no longer recognized by the community.
- The development progress of Polygon’s ZK Rollup sub-projects have fallen far behind expectations.
- The official cross-chain bridge of Polygon has undergone serious security accidents.

4. Preliminary Value Assessment

4.1 Five Core Issues

What Business Cycle is the Project In? Is It in Maturity or the Early to Mid Stage?

Polygon is currently in the mid-stage of its development. Polygon, as a side chain, is already an influential public chain, and its on-chain application has been very mature, forming a relatively complete ecosystem; The ZK-Rollup projects proposed by the team will be launched continuously in the next year, with many new growth points worth looking forward to.

Does the Project Have Solid Competitive Advantages? What are the Competitive Advantages?

Polygon has certain competitive advantages in the fierce public chain competition for ecosystems. The author thinks that these competitive advantages are as follows in order of their advantages:

- Accumulation of outstanding talents in ZK field, as well as first-Mover advantage in technology and products
- The growth of users and developers in the public chain ecosystem has formed a positive cycle, especially with its cooperation with non-web3 giants enjoying a large number of users. As a result, the ecological flywheel began to rotate.
- Focus on being the aggregator of the scaling solution for Ethereum ecosystem, and have a good relationship with the Ethereum community, which has the most abundant talents and innovations.
- Despite of many product business lines, good synergy effects in technology and ecosystem can be achieved among them.

These competitive advantages are gradually built up by Polygon's team through their judgments and decisions, behind which is their great industry vision and ecosystem operation ability, all reflecting their sound strategic planning.

However, the war between public chain ecosystems is far from the end. It remains to be seen whether Polygon's judgment on the future is right and whether the resources invested heavily can blossom and bear fruit, thus building a more reliable ecosystem for users.

Is the Medium- to Long-term Investment Logic Clear? Is It in Line With the General Trend of the Industry?

The mid-to-long-term investment logic of the project is clear and consistent with the general trend of the industry.

Compared with Bitcoin's value storage logic, how to introduce more users to participate in the blockchain field, the global settlement layer, is the core narrative of smart contract public chain represented by Ethereum, and it is also the most important investment theme running through this cycle and even the next cycle. For the Ethereum ecosystem, Vitalik clearly pointed out that “Rollups are expected to be a cornerstone of Ethereum scaling in the short and medium-term future”, and “in the medium to long term ZK rollups will win out in all use cases as ZK-SNARK technology improves”.

From the development of Polygon in ZK Rollup, especially in ZK EVM Rollup, it is already one of the most important players in the field.

What are the Main Variable Factors in the Operation of the Project? Are Such Factors Easy to Quantify and Measure?

For Polygon PoS, we can measure the development of Polygon PoS by observing its number of active addresses, TVL, the number of active Dapps and other metrics.

As for ZK Rollup, since several core projects have not been launched yet, the main variable lies in the development and launch progress of each ZK Rollup.

At present, the codes of several core products have been open source, can be tracked by Github code submission (Polygon announced that it would realize EVM-equivalent zkEVM in July, but it did not achieve the expected results; zkEVM was expected to be officially launched in Q3 this year, but the launch time of zkEVM has been updated to 2023).

What is the Management and Governance Approach? How About the DAO?

Project management and governance mainly rely on the core team. From the past history, the core team had great performances.

4.2 Valuation

Polygon’s business is mainly divided into two parts, Polygon PoS chain and a series of sub-projects of ZK Rollup.

4.2.1 Valuation of Polygon PoS

We value Polygon PoS by combining horizontal comparison valuation with vertical comparison valuation.

• Horizontal data comparison

The valuation of smart contract public chain is complex and difficult. The valuation of DeFi protocol can based on its income multiple, while smart contract public chain is more similar to a country, so it may be more appropriate to use a concept similar to "comprehensive national strength" to evaluate the current situation and potential of public chain.

The "comprehensive national strength metric" of the public chain should consider the data such as the number of active dAPPs, the number of active users, TVL, the value of total assets on chain, the number of active developers, the number of transfers on chain, the total value of transfers on chain, etc., and these data should be given different weights. However, such metric is not available.

Therefore, the author selects four metrics: assets, user volume, active business and developers to compare Polygon with its other public chain competitors.

Assets Metric: TVL.

If users are willing to put valuable assets on a certain chain, then that shows users' comprehensive recognition of the safety, availability and investment value of the chain, also the most commonly used data metric for public chain valuation at present.

(In fact, a better asset measurement metric should include on-chain NFT assets which however does not have accurate data.) Therefore, we use TVL of homogeneous assets counted by defillama as an approximate asset measurement metric, and use Market Capitalization/TVL as an asset metric for horizontal comparison.

The smaller the metric value, the more assets on-chain corresponding to its market capitalization unit, and the lower the valuation.

Users Metric: On-chain active addresses.

We choose the average number of daily active users in 30 days as a measure of the active users on this chain, and use the Market Capitalization/number of daily active users as a horizontal comparison user metric.

The smaller the metric value, the more users corresponding to its market capitalization unit, and the lower the valuation.

Activity Metric

The dollar value of gas consumed every day and the total amount of transaction every day.

The activity of transactions on chain is relatively difficult to measure for the public chain. Traditionally, the dollar value of Gas fees consumed every day is usually used for valuation comparison, and its logic is to evaluate the user's real willingness to have activity on-chain more objectively through the user's behavior of paying the cost of Gas fees (for users).

However, the problem of this metric is obvious. High Gas price hinders the development of chain in essence. In other words, reducing the cost of interaction for users on chain is the goal of scaling of Ethereum and its various chain competitors. If this metric is convincing, then we should not strive for scaling and make efforts to improve TPS.

However, the author also fails to find a perfect metric to measure the activity (if you have a better idea, you are welcome to share with us).

Therefore, we combine the dollar value of gas fee consumed every day with the total daily transaction, and convert the dollar value of gas fee consumed in the last 30 days and the transaction number in the last 30 days into an annualized data, thus obtaining two metrics that can be compared horizontally: market value/annualized gas fee consumption amount and market value/annualized transaction number.

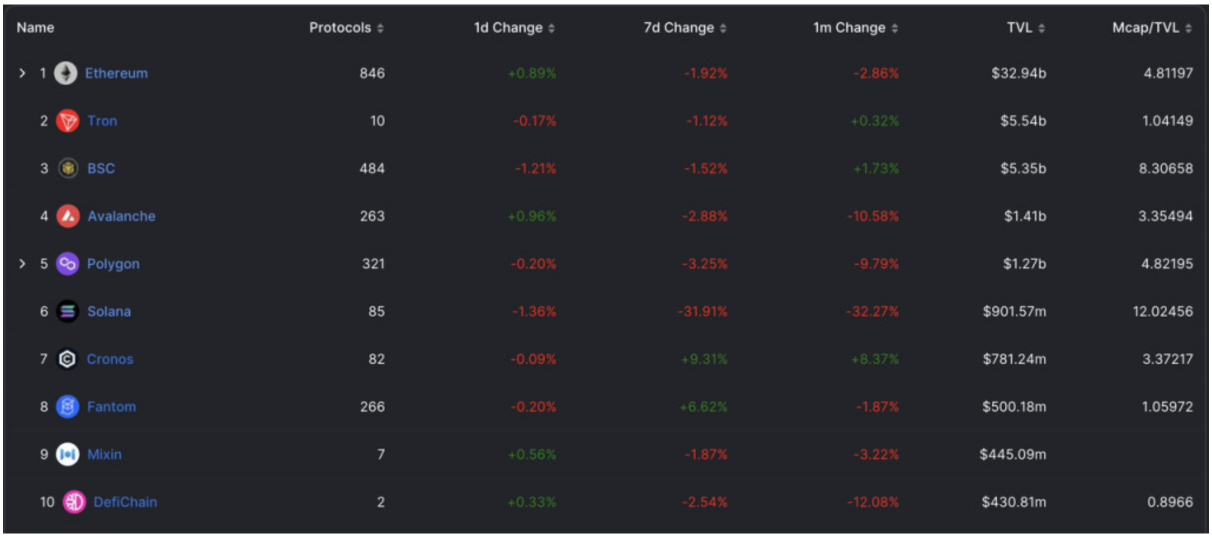
Similarly, the smaller the value of these two metrics, the lower the valuation of the chain.

Developer Metric: Number of validated contracts on the chain.

The number of active dApps is also a good indicator, but there is no reliable data source for this data.

We use the average number of newly validated contracts in the official block browser every day in recent 30 days to measure the developer activity on this chain, and use the Market Capitalization/daily average number of validated contracts as the user metric for horizontal comparison.

The smaller the metric value, the more developers can be carried by its unit circulation market value and the lower its relative valuation (since the value is generally large, we have processed the number digit for the comparison).



Name	Protocols	1d Change	7d Change	1m Change	TVL	Mcap/TVL
> 1 Ethereum	846	+0.89%	-1.92%	-2.86%	$32.94b	4.81197
2 Tron	10	-0.17%	-1.12%	+0.32%	$5.54b	1.04149
3 BSC	484	-1.21%	-1.52%	+1.73%	$5.35b	8.30658
4 Avalanche	263	+0.96%	-2.88%	-10.58%	$1.41b	3.35494
> 5 Polygon	321	-0.20%	-3.25%	-9.79%	$1.27b	4.82195
6 Solana	85	-1.36%	-31.91%	-32.27%	$901.57m	12.02456
7 Cronos	82	-0.09%	+9.31%	+8.37%	$781.24m	3.37217
8 Fantom	266	-0.20%	+6.62%	-1.87%	$500.18m	1.05972
9 Mixin	7	+0.56%	-1.87%	-3.22%	$445.09m	
10 DefiChain	2	+0.33%	-2.54%	-12.08%	$430.81m	0.8966

Top 10 Blockchain with highest TVL *Source: Defillama*

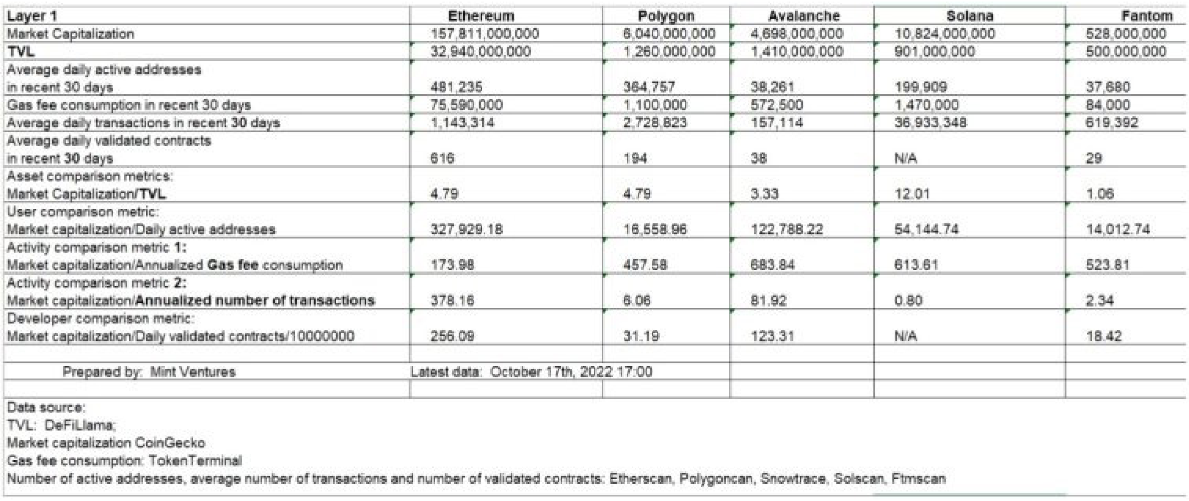
Before comparing, we should also pay attention to the fact that the Layer 1 token use cases of the top 10 blockchains are also quite different.

For example, BNB is both native token of BNB Chain and the platform token for Binance Exchange (CRO is also the same case), and the OP token of L2 chains cannot be used to pay for network gas fees. If these items are directly compared, the results would be less valuable.

We take “the main use case of tokens is to maintain network consensus and pay for on-chain transactions as Gas fees” as the main feature of the smart contract public chains to select comparable objects for Polygon. We finally select Avalanche, Solana and Fantom as horizontal comparable objects for Polygon PoS.

Similarly, we also collect various data of Ethereum as a comparative baseline for readers’ reference.

Horizontal data comparison results as shown as below:



Layer 1	Ethereum	Polygon	Avalanche	Solana	Fantom
Market Capitalization	157,811,000,000	6,040,000,000	4,698,000,000	10,824,000,000	528,000,000
TVL	32,940,000,000	1,260,000,000	1,410,000,000	901,000,000	500,000,000
Average daily active addresses in recent 30 days	481,235	364,757	38,261	199,909	37,680
Gas fee consumption in recent 30 days	75,590,000	1,100,000	572,500	1,470,000	84,000
Average daily transactions in recent **30** days	1,143,314	2,728,823	157,114	36,933,348	619,392
Average daily validated contracts in recent **30** days	616	194	38	N/A	29
Asset comparison metrics: Market Capitalization/**TVL**	4.79	4.79	3.33	12.01	1.06
User comparison metric: Market capitalization/Daily active addresses	327,929.18	16,558.96	122,788.22	54,144.74	14,012.74
Activity comparison metric **1:** Market capitalization/Annualized **Gas fee** consumption	173.98	457.58	683.84	613.61	523.81
Activity comparison metric **2:** Market capitalization/**Annualized number of transactions**	378.16	6.06	81.92	0.80	2.34
Developer comparison metric: Market capitalization/Daily validated contracts/10000000	256.09	31.19	123.31	N/A	18.42
Prepared by: Mint Ventures	Latest data: October 17th, 2022 17:00				

Data source:
TVL: DeFiLlama;
Market capitalization CoinGecko
Gas fee consumption: TokenTerminal
Number of active addresses, average number of transactions and number of validated contracts: Etherscan, Polygoncan, Snowtrace, Solscan, Ftmscan

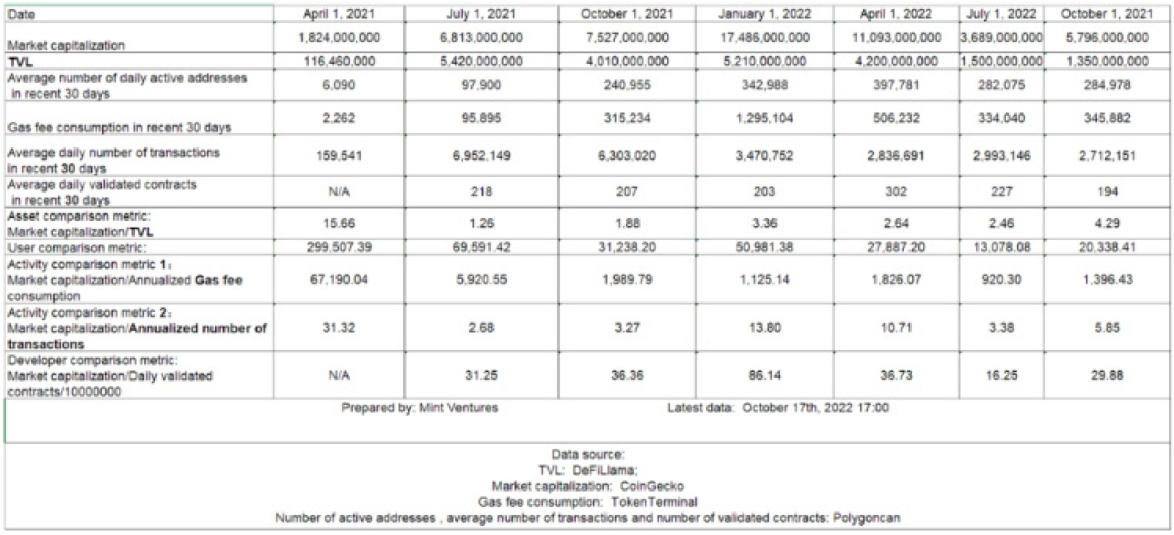
We can clearly see that:

• In terms of metric comparison with Avalanche, Polygon has significant valuation advantages in terms of user, activity and developer comparison metric besides asset metric, especially in terms of number of active users, transaction number and developer data.
• Compared with Solana's metrics, Polygon is also underestimated almost in all aspects except for the daily transaction quantity metric (and the unavailable developer activity metric).
• Compared with Fantom, which fell down after AC left, Polygon has a similar performance with it in user comparison metric, developer comparison metric and daily gas fee consumption metric, but there is a large valuation gap in asset metric from it to Fantom.

In summary, a side-by-side data comparison of Polygon, Avalanche, Solana and Fantom shows that Polygon's overall valuation level is low.

• Horizontal data comparison

We also select the above horizontal comparison metrics to compare the valuation of Polygon PoS vertically on the first day of each quarter, and the results are as follows:



Date	April 1, 2021	July 1, 2021	October 1, 2021	January 1, 2022	April 1, 2022	July 1, 2022	October 1, 2021
Market capitalization	1,824,000,000	6,813,000,000	7,527,000,000	17,486,000,000	11,093,000,000	3,689,000,000	5,796,000,000
TVL	116,460,000	5,420,000,000	4,010,000,000	5,210,000,000	4,200,000,000	1,500,000,000	1,350,000,000
Average number of daily active addresses in recent 30 days	6,090	97,900	240,955	342,988	397,781	282,075	284,978
Gas fee consumption in recent 30 days	2,262	95,895	315,234	1,295,104	506,232	334,040	345,882
Average daily number of transactions in recent **30** days	159,541	6,952,149	6,303,020	3,470,752	2,836,691	2,993,146	2,712,151
Average daily validated contracts in recent **30** days	N/A	218	207	203	302	227	194
Asset comparison metric: Market capitalization/**TVL**	15.66	1.26	1.88	3.36	2.64	2.46	4.29
User comparison metric:	299,507.39	69,591.42	31,238.20	50,981.38	27,887.20	13,078.08	20,338.41
Activity comparison metric **1**: Market capitalization/Annualized **Gas fee** consumption	67,190.04	5,920.55	1,989.79	1,125.14	1,826.07	920.30	1,396.43
Activity comparison metric **2**: Market capitalization/**Annualized number of transactions**	31.32	2.68	3.27	13.80	10.71	3.38	5.85
Developer comparison metric: Market capitalization/Daily validated contracts/10000000	N/A	31.25	36.36	86.14	36.73	16.25	29.88

Prepared by: Mint Ventures Latest data: October 17th, 2022 17:00

Data source:
TVL: DeFiLlama;
Market capitalization: CoinGecko
Gas fee consumption: TokenTerminal
Number of active addresses , average number of transactions and number of validated contracts: Polygoncan

Excluding the business data and the data of the first half of 21 years when the market value rose rapidly, we can see that Polygon's current valuation level is generally at a medium level in history.

To split it up, Polygon's user data, activity data and developer data perform better than its market capitalization; in terms of asset metrics, its valuation shows a rising trend.

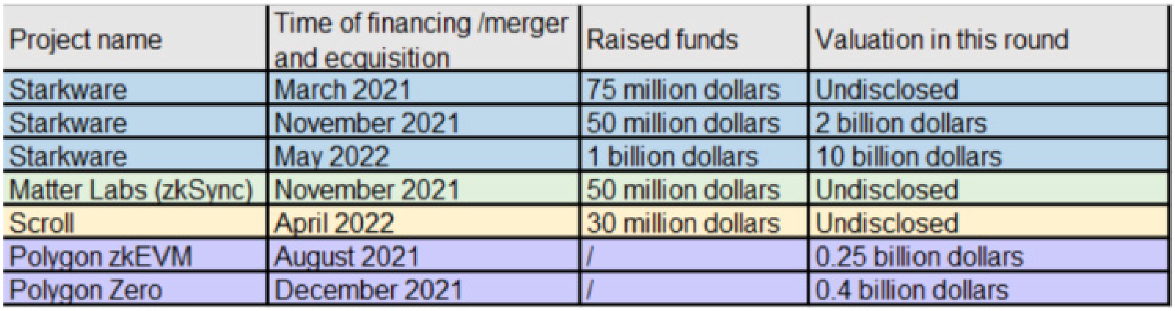
On the other hand, compared with June to July this year, when all valuation data are almost the lowest, the current valuation level has risen in all aspects, showing that this round of rebound is still more driven by valuation improvement.

In addition, Polygon's ZK Rollup sub-project was not included in all the above valuations, and the valuation of ZK project is deliberated in the next chapter.

To sum up, in the comparison between horizontal and other public chain projects, we think Polygon has a low valuation compared with other Layer 1 chains; In the comparison with its historical valuation, Polygon's valuation is at a median level.

4.2.2 Polygon ZK Rollup Sub-project Valuation

For ZK Rollup, since all zkEVM has not been officially launched and there is no business data that can be evaluated and compared, it is impossible to make a more intuitive quantitative valuation comparison. We only list the disclosed financing and valuation of each project.



Project name	Time of financing /merger and ecquisition	Raised funds	Valuation in this round
Starkware	March 2021	75 million dollars	Undisclosed
Starkware	November 2021	50 million dollars	2 billion dollars
Starkware	May 2022	1 billion dollars	10 billion dollars
Matter Labs (zkSync)	November 2021	50 million dollars	Undisclosed
Scroll	April 2022	30 million dollars	Undisclosed
Polygon zkEVM	August 2021	/	0.25 billion dollars
Polygon Zero	December 2021	/	0.4 billion dollars

ZK Financing information of Rollup-related projects from 2021

From the primary market, Starkware's valuation rose from US $2 billion in November 2021 to US $8 billion in May 2022, while Polygon's other two competitors in ZK Rollup, zkSync and Scroll, did not disclose their valuations in the latest round of financing.

Although Starkware has StarkEx business besides Starknet, which focuses on zkEVM, its valuation does not completely correspond to the valuation of their ZK Rollup solution. But we can ignore this impact when comparing the primary market valuation of Starkware vertically.

From the case of Starkware, we can roughly think that the market valuation of a normally developing ZK Rollup project in May 2022 has increased four times compared with that in November 2021.

If we also measure zkEVM and Zero acquired by Polygon in the second half of 2021 with a four-fold increase in valuation, their valuations in May 2022 will be $1 billion and US $1.6 billion respectively.

(Again, this valuation analogy is very rough.)

Looking at the development of Polygon, they have developed their technical solution from Plasma, which was gradually eliminated, to PoS + ZK Rollup, with its market value increasing from 20 million US dollars at Binance Launchpad to more than 8 billion US dollars at present.

Objectively speaking, at the early stage of Polygon's development, its background, resources and even capital reserves of the core team did not show significant advantages compared with its counterpart public chains in the same period. However, it shows its outstanding industry foresight and ecological operation ability to deploy key resources decisively. As a result, its market value moved forward the top 10 and it is expected to continue to maintain its leading position in the future public chain competition.

The next cycle is the key time window for the whole crypto world to develop from its implementation of narratives to large-scale commercialization.

The value of building a decentralized infrastructure that can carry the business activities of hundreds of millions or even billions of people is self-evident.

If it can continue to stand out in the public chain competition in the next round, Polygon will still show huge market value space.

5. References

The Polygon Whitepaper: *https://github.com/maticnetwork/whitepaper*

zkEVM Official documents: *https://docs.hermez.io/zkEVM/Overview/Overview/*

https://blog.Polygon.technology/zk-and-the-future-of-ethereum-scaling/

https://pitch.com/public/caf3ac93-440a-4b69-8136-f1da966f59e2/7de76264-e2ce-443e-981b-fa54dfd17523

Messari: Polygon: A Multi-Sided Approach to ZK Scaling *https://messari.io/report/Polygon-a-multi-sided-approach-to-zk-scaling*

Explanation of polygon full-stack zk scaling solutions: Hermez, Nightfall, Miden, and Zero *https://www.chaincatcher.com/article/2071784*

Learn about the new consensus mechanism PoE developed by the Polygon team for zkEVM *https: //www.chaincatcher.com/article/2070039*

Delphi: Finding a home for labs *https://members.delphidigital.io/reports/finding-a-home-for-labs*

Foresight Ventures: Understand zkEVM Rollup from Polygon zkEVM *https://foresightnews.pro/article/detail/13244*

Pedro: Polygon Miden Deep Dive: A STARK Based zk-Rollup *https://medium.com/@pedronv/Polygon-miden-deep-dive-a-stark-based-zk-rollup-600564264613*

Pedro: Polygon Nightfall Deep Dive: A Private Rollup For Enterprises *https://medium.com/@pedronv/Polygon-nightfall-deep-dive-a-private-rollup-for-enterprises-a01b298721c5*

Pedro: Polygon Zero: The Most Performant zk-Rollup *https://medium.com/@pedronv/Polygon-zero-the-most-performant-zk-rollup-a3c53b786364*

Vitalik: Understanding PLONK *https://vitalik.ca/general/2019/09/22/plonk.html*

Vitalik: The different types of ZK-EVMs *https://vitalik.ca/general/2022/08/04/zkEVM.html*