Polygon: Multifaceted Offense

I. Executive Summary

We believe that Polygon is currently undervalued and should be worth at least as much as Solana's ~$12 billion circulating market cap. Under our base case, MATIC is worth $1.37 per token, giving us an upside of 50% from the current price. We believe the re-pricing will happen in Q1 2023 as Polygon zkEVM gets launched on mainnet, improving market condition, and the market waking up to new and extended use cases of MATIC.

Key takeaways that support our thesis:

- Polygon PoS has had an annualized transaction volume of 976.37 million in the last 30 days. For context, it is much bigger than most chains and yet its market cap is much smaller. Compared to Ethereum specifically, Polygon's transaction volume is 2.4x Ethereum's, and yet its market cap is 1/60th of Ethereum's.
- Most investors know Polygon for its PoS Chain and that it has several other solutions that are not dissimilar. After delving into the projects, we learned that each project is different yet complementary. When taken together, these projects are bigger than the sum of their parts and form the building blocks of the one-stop platform for anyone who wants to build on Web3. The table below summarizes various projects under Polygon.

Project	Summary	Status	Role of MATIC
Polygon PoS Chain	PoS sidechain that uses Plasma bridging framework	Live	Gas, Staking
Polygon Edge	Framework for building EVM-compatible blockchains	Live	-
Polygon Hermez 1.0	ZKR for scaling payments and transfers of ERC-20 tokens	Live	-
Polygon zkEVM (Hermez 2.0)	ZKR with EVM-equivalent at the bytecode level	Public Testnet	Gas, Staking
Polygon Zero	Recursive SNARK* proof that is 100x faster than alternatives and compatible with Ethereum	In development	-
Polygon Miden	ZKR with STARK* proof system	In development	Gas, Staking **
Polygon Nightfall	Privacy-focused optimistic rollup targeted at Enterprise	Mainnet Beta	-
Polygon Avail	A blockchain that records transactions data for other blockchains so they do not have to	In development	Gas, Staking **

- Polygon is working on all these projects in parallel. They have been able to do so through aggressive fundraising and acquisition of top talents and projects. Taking into consideration a $450 million VC round in February and the $530 million balance in the Foundation's wallet, Polygon has enough financing to build these projects through the crypto winter and even an appetite to acquire even more solutions. This gives us confidence that they would be able to deliver these projects on time.
- As the four L2 projects go live over the next 6-18 months, Polygon will be worth significantly more. We believe that Polygon's Hermez 2.0 zkEVM solution will be at least as competitive as Optimism and Arbitrum, and we believe Hermez 2.0 alone can add an additional $2+ billion to Polygon's market cap. Success by Nightfall, Miden, and Avail will only increase this value accretion.
- With multiple projects under Polygon, we think that MATIC will inevitably also expand its use cases. The company has not revealed its redesign of MATIC, but from the breadcrumbs, we expect that MATIC's use cases will be expanded from gas and staking for PoS Chain to gas, staking, and governance tokens across multiple projects. The expansion of use cases means more demand for MATIC and bullish for the token price. In fact, as soon as 3-6 months from now, we expect Hermez 2.0 to hit the mainnet, increasing the demand for MATIC.

II. Table of Contents

III. Preface

Polygon has always been in the business of scaling Ethereum since the launch of Matic Network in 2017. This network has been re-branded the Polygon proof-of-stake (PoS) sidechain (Polygon PoS), with MATIC as its native token. Based on what we are seeing unfolding, Polygon's ambition is bigger than operating the largest scaling solution currently for Ethereum— it wants to offer a comprehensive suite of solutions for every conceivable Web3 use case.

This month, Polygon launched its zkEVM onto the testnet, making Polygon a frontrunner to become the first generalized zk rollup (ZKR) Layer-2 (L2) scaling solution in the market. The rollout of a fully functional generalized ZKR is seen as a watershed moment for Ethereum, so we think that Polygon is a must-have on your watchlist.

A quick search on Google and Twitter reveals that the knowledge of how Polygon zkEVM works has yet reached the mainstream media. As a technical researcher, I was able to understand the technical documentation and access the zkEVM testnet to try it out, and this report contains some of my early findings, simplified for you.

If this is the first time you heard about ZKR or L2s, you can read our L2 report for an in-depth introduction to various L2 solutions. Otherwise, simply put, L2s are blockchains that increase Ethereum's ability to execute transactions faster and more cheaply, while leveraging Ethereum's decentralization for more robust security. L2s help solves Ethereum's high latency and transaction costs, which have been hampering its progress toward adoption, technological efficiency, and user experience.

By the end of this report, you will understand Polygon's various scaling solutions and how they fit together in Polygon's game plan, how they are getting there, and what all these mean for its token MATIC.

V. Polygon - Today

Polygon was launched as the Matic Network by co-founders Jaynti Kanani, Sandeep Nailwal, and Anurag Arjun. It had two products: a plasma chain and a PoS sidechain that helps Ethereum handle the growing user demand. But Matic Network did not stop at PoS Chain.

We provide below a summary of the networks and solutions Polygon currently offers, as well as technologies that will likely launch in the next 6-18 months.

Project	Summary	Status	Role of MATIC
Polygon PoS Chain	PoS sidechain that uses Plasma bridging framework	Live	Gas, Staking
Polygon Edge	Framework for building EVM-compatible blockchains	Live	-
Polygon Hermez 1.0	ZKR for scaling payments and transfers of ERC-20 tokens	Live	-
Polygon zkEVM (Hermez 2.0)	ZKR with EVM-equivalent at the bytecode level	Public Testnet	Gas, Staking
Polygon Zero	Recursive SNARK* proof that is 100x faster than alternatives and compatible with Ethereum	In development	-
Polygon Miden	ZKR with STARK* proof system	In development	Gas, Staking **
Polygon Nightfall	Privacy-focused optimistic rollup targeted at Enterprise	Mainnet Beta	-
Polygon Avail	A blockchain that records transactions data for other blockchains so they do not have to	In development	Gas, Staking **

Exhibit 1 Summary of Solutions under Polygon

**) SNARK stands for Succinct Non-Interactive Argument of Knowledge while STARK stands for Scalable Transparent Argument of Knowledge. Both are ZK prover systems where STARK has the advantage of being more scalable, i.e. fast proof, and transparent, i.e. does not require trusted setup, but it does inevitably result in bigger proofs that incur higher gas fees*

***) Our best guess on the role of MATIC in the pre-launched project*

We will look at each of the technology in turn in this section and the next.

PoS Chain

The PoS Chain is one of the most successful Blockchain projects. As of writing, the PoS chain is home to **53k dApps** including Aave, Uniswap V3, and OpenSea; **174.9m unique user addresses** and **$5b in TVL**. It has processed **2.1b+** transactions thus far, making it the top Ethereum scaling solution in the market right now.

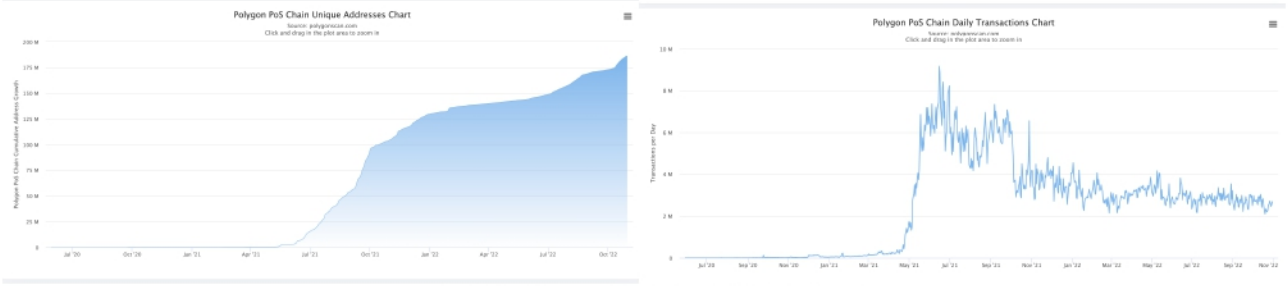

Exhibit 2 Polygon PoS Chain's Activity Charts

Polygon PoS achieved very strong traction as the go-to Ethereum-compatible scaling solution during the 2021 NFT and DeFi booms and was rewarded with a peak circulating market cap of nearly US$18 billion. The MATIC token's outperformance during the 2022 market downturn (current circulating market cap of US$8

billion) reflects Polygon's success in pivoting towards supporting multiple L2 infrastructures, diversifying away from a concentration in NFTs.

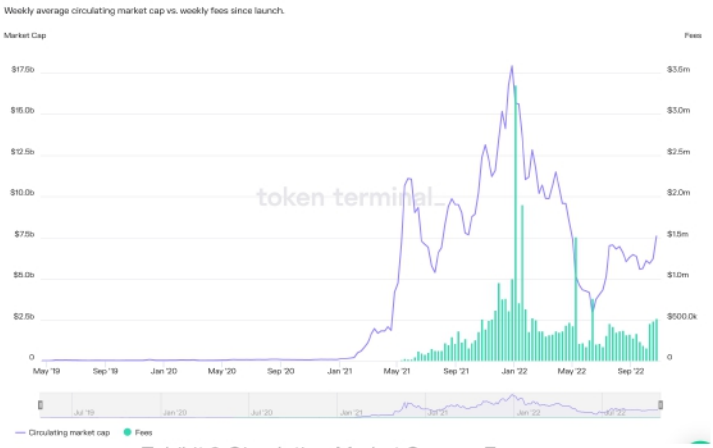

Exhibit 3 Circulating Market Cap vs. Fees

Key specs of PoS Chain	
Prover system	Fraud proof*
EVM-compatible	Yes
Throughput	7000 TPS
Transaction fee	~$0.002 per txn
Status	Live

**) Fraud proof relies on network participants to catch fraudulent transactions*

To further attract mainstream adoption, PoS Chain has secured partnerships with brands and institutions that are close to our daily lives, including:

- Starbucks uses Polygon to accept payments in crypto and launch an NFT-based rewards program called Starbucks Odyssey, in which the holder can earn benefits such as a trip to Starbucks' coffee farms in Costa Rica
- Using Polygon, Mercedes Benz has launched Acentrik, a decentralized data-sharing marketplace for businesses to purchase and sell data. To save gas, data is not stored directly on the blockchain but is stored off-chain and is attached as metadata on a non-fungible token (NFT) that represents each dataset
- Police in India launched a portal on Polygon that allows victims of crimes to register complaints against local police officers. It leverages the immutability of blockchain to ensure that the complaints cannot be dismissed or manipulated by potentially corrupt officers

Polygon did not stop at PoS Chain. As the need for Layer-2 solutions emerges, Matic Network rebranded itself as Polygon in February 2021 to work towards building a solution to connect the different Ethereum scaling solutions.

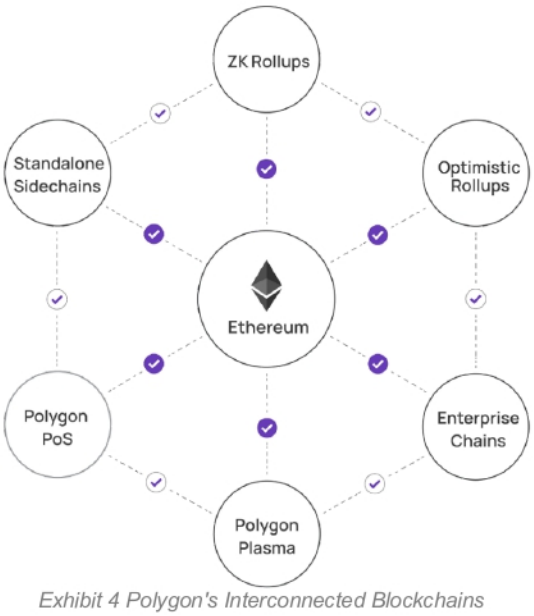

Exhibit 4 Polygon's Interconnected Blockchains

Polygon Edge

At the core of this L2 connective tissue is the Polygon Edge (previously Polygon SDK), which will serve as a modular, flexible software framework for launching new chains based on any Ethereum scaling technology. It currently supports building stand-alone chains (e.g. Dogechain), but Polygon Edge will support building and connecting to L2 solutions. Building on Polygon Edge has allowed Dogechain to quickly spin up a sovereign blockchain that offers Dogecoin users access to DeFi and Web3. Dogechain currently has a TVL of $5.4m.

Polygon Hermez 1.0

As part of the effort of offering a selection of L2 solutions on its platform, Polygon acquired networks such as Hermez Network—a payment-focused ZKR solution—in August 2021. Hermez 1.0 delivers up to 2,000 transactions per second while keeping costs under 300,000 gas.

However, Hermez Network (Hermez 1.0) was not as well received as the PoS Chain. It has been live since March last year but has not gained meaningful adoption. The TVL as of writing is $309k, which is 0.01% of the L2 market. We think this is because Hermez 1.0 is a payments-only ZKR; it can only be used for transferring funds between exchanges or paying for products in centralized ecosystems that support L2. They cannot be directly used with DeFi, as it would require users to withdraw and redeposit funds each time, partially defeating the purpose of the rollup.

This may however change as Polygon rolls out Hermez 2.0, the general-purpose ZKR, which we will discuss in the next section.

VI. Polygon - Future Roadmap

The next building block for Polygon to become the Amazon Web Services (AWS) of Web 3 is a comprehensive set of L2 solutions built on top of Ethereum.

L1 blockchains have at least three layers:

- Execution, which computes the new state based on incoming transactions
- Data availability (DA), which stores the transactions
- Consensus, which provides security and the agreement of the transaction ordering

The thesis behind most L2 is to take over the execution layer while continuing to utilize Ethereum's consensus layer and DA layer. Polygon, however, is building solutions to offload the DA layer in addition to the execution layer.

For offloading the execution layer, Polygon is betting on ZK technologies and has committed $1 billion to develop ZK-based scaling solutions. In the second half of 2021, Polygon announced four projects that they are currently developing:

- Nightfall – an Optimistic Rollup (OR) L2 that uses zero-knowledge proof for privacy
- 3 separate ZKR L2s: Hermez 2.0, Miden, and Zero.

For offloading the DA layer, Polygon is working on Polygon Avail. By letting Avail take care of storing their transactions data, both standalone chains and L2 such as rollups can lower their transaction costs by 80-95%.

As a reminder, rollups are L2 blockchains that execute transactions on behalf of Ethereum and send a summary of the transactions to Ethereum. Rollups come in two flavors depending on the verification method. Optimistic Rollups assume that all transactions are valid and give the network participants a window of opportunity to challenge otherwise, whereas Zero-Knowledge Rollups (ZKR) send along proof that the transactions are valid on submission to Ethereum. For more explanation of rollups, you can read our L2 report.

Polygon Nightfall: Optimistic Rollups for Enterprise

Polygon Nightfall is a privacy-focused optimistic rollup that, in addition to increasing throughput and lowering transaction fees, uses zero-knowledge proof to anonymize transactions and hide wallet balances.

Key specs of Nightfall	
Prover system	Fraud proof
EVM-compatible	Yes
Throughput	100 TPS
Transaction fee	12k gas per txn
Status	Mainnet Beta

Prior to Nightfall, most enterprises resorted mostly to permissioned, centralized blockchains because public blockchains like Ethereum lack privacy and are expensive. With Nightfall, businesses can use Ethereum for its decentralization and security, while keeping their transactions private from third parties.

Polygon identified the following use cases for Nightfall:

- Supply chain management, where assets and goods can be tokenized, exchanged, paid, and tracked across the globe. In fact, EY is already using Nightfall for its clients.
- Private NFT marketplaces where businesses can tokenize physical assets such as inventory and exchange them for NFTs
- Blockchain mixers: a service to increase the anonymity of certain crypto transactions

Polygon's ZKR initiatives

Polygon Hermez 2.0, Polygon Zero, and Polygon Miden are the three ZKR-focused initiatives that coexist under the Polygon umbrella. Each of them is solving a different problem and/or taking a different approach toward building a generalized ZKR.

One major difference is the proof architecture they adopted:

- Miden uses STARKs, which is scalable, has fast proof generation, and requires no "trusted setup"—a common point of failure in cryptography, but does inevitably result in bigger proofs that incur higher gas fees

- Hermez was initially using SNARKs, which supports recursion, and has fast verification but requires a trusted setup, but switched to Zero's Plonky2, which combines the best of STARKs and SNARKs

The diversity in their approaches paid off when the three teams collaborate on delivering Polygon zkEVM. Essentially, zkEVM is a virtual machine that can generate zk-proofs for any possible Ethereum Virtual Machine (EVM) opcodes, which are the low-level programming commands that EVM executes when we call an Ethereum smart contract. **With zkEVM, dApps can execute transactions on ZKR L2 just like on Ethereum. EVM is critical to an L2's adoption—the easy onboarding of popular dApps that crypto users are already familiar with on Ethereum will help accelerate the development of an ecosystem native to the L2.**

We will now look at each of the projects in turn.

Polygon Zero: Generating Validity Proofs in Parallel

Key specs of Zero	
Prover system	Plonky2 (Recursive SNARK)
Status	Plonky2 is used in Polygon zkEVM

Polygon Zero is working on reducing the computational cost of generating validity proofs. Instead of generating proofs for one transaction at a time, Zero generates proofs simultaneously for every transaction in the batch. As a result, Zero can generate a recursive proof in 0.17 seconds, making it arguably the fastest ZK proof-generation scheme today. Zero achieves this by leveraging Plonky2, a recursive SNARK developed by the team behind Mir Protocol that Polygon acquired.

Polygon Zero is an eight-member team of cryptographers and engineers, coming from a variety of backgrounds and skill sets, from engineering at Google to Ph.D. research in pure math, and degrees from top crypto research institutions like Berkeley and EPFL.

Polygon Zero's prover system, Plonky2, is also a key component in Hermez 2.0.

Hermez 2.0: Polygon zkEVM

Key specs of Hermez 2.0	
Prover system	Plonky2 (by Polygon Zero)
EVM-compatible	Yes (Bytecode level)
Throughput	2000 TPS
Transaction fee	N/A
Status	Public Testnet

As mentioned in the previous section, Hermez started out as a payments-only ZKR—it can be only used for transferring any registered ERC-20 token from one Hermez account to another via a simple web or mobile interface. The team, after the acquisition by Polygon, focused its development efforts on creating a zkEVM solution, codenamed Hermez 2.0.

Hermez 2.0 is secured by network participants running zkNodes (and in some cases, as explained below, zkProvers) under the novel **Proof-of-Efficiency (PoE)** consensus mechanism. PoE has two participants, **Sequencers** and **Aggregators**, each with a different incentive:

- **Sequencers** collect transactions into batches and add them to the **PoE Smart Contract** deployed on Ethereum. They collect transaction fees from users of the network and in turn, pay both Aggregators for generating proofs in MATIC, and L1 gas fees required for sending the transaction batch to the PoE Smart Contract.
- **Aggregators** check the validity of the transaction batches proposed by Sequencers and provide validity proofs to L1. To create validity proofs, Aggregators need to run a **zkProver** node, which requires specialized hardware like GPUs. While zkProver technically can be run on commodity hardware, it would be pointless to do so because, for any given batch, an Aggregator that submits a validity proof first earns the MATIC fee. Aggregators would have to bear the server cost and L1 gas fees to submit the proofs to the PoE Smart Contract.

One potential concern for PoE is that its hardware requirements may lead to less decentralization. The bar of becoming Aggregators is relatively high: they need specialized hardware like GPUs which have become expensive in recent years; and then they need to have enough computation power to be the first to generate the proof so they get paid the block reward. That said, Bitcoin mining has similar constraints and while the network is not as decentralized as we would like it to be, it works.

The Hermez team currently has 33 people led by Jordi Baylina. Jordi's involvement in Ethereum started when he helped rescue TheDAO hack funds, and ever since then he has been actively contributing to the ecosystem. Jordi is joined by David Schwartz as Project Lead and Antoni Martin as Business Lead.

Polygon Miden: STARK-based ZKR

Polygon Miden is building a STARK-based ZKR that supports fast-proof generation even on a consumer laptop. The project is being built around Miden VM, a Virtual Machine optimized for STARKs.

Key specs of Miden	
Prover system	STARK
EVM-compatible	Yes (Programming-language level)
Throughput	1,000-2,000 TPS
Transaction fee	N/A
Status	Miden VM available on Github

Miden VM is **not** an EVM, i.e. it does not emulate the Ethereum Virtual Machine. This is by design: Miden VM aims to be Ethereum-compatible at the high-level programming language level so it can support Solidity and other blockchain-centric languages like Vyper, Move and Sway.

The team is led by Bobbin Threadbare (not his real name), a former Facebook's core ZK researcher who has made multiple contributions in the field of STARK-based proving systems, such as genSTARK library as well as AirScript and AirAssembly, languages supported by the Ethereum Foundation.

Polygon Avail: Data Availability (DA) Layer

Any blockchain—be it standalone or sidechains or even rollups—can outsource the DA layer to Avail. With rollups, we have seen 100x improvements in cost and scalability by taking just the execution off-chain. DA providers such as Avail, Celestia, and zkPorter allow chains to take the transaction data storage off-chain and post only the proof to Ethereum, thus eliminating 80-95% of their costs.

By using a DA provider, a ZKR basically becomes a Validium—a rollup that still sends validity proofs to Ethereum but takes transaction data off the chain. Validiums like Immutable X takes data availability off-chain by running a Data Availability Committee (DAC), a small, permissioned group of entities that attests to the availability of the data off-chain. This should trigger the decentralization maxis among us because if DAC were to act maliciously, they could freeze all funds on the chain by hiding the data.

Avail, in comparison, is a blockchain complete with validator nodes, block producers, and consensus algorithms. Avail intends to have hundreds of nodes working together to guarantee network security, in contrast to DACs currently that only have as few as five participants. The network will also be permissionless, making it possible for anybody to join as a validator.

The obvious disadvantage of using a DA-layer provider is that users would be adding a new trust assumption with a new protocol that may take years to build up security to the same order of magnitude as Bitcoin or Ethereum.

We think that this is where Polygon Avail can beat the competition, such as Celestia and zkPorter, as they have already built a significant validator set for their Polygon PoS chain. It is possible that they offer their network of validators better incentives to run Avail nodes in the future if they want to.

VII. Vision, Strategy, and Execution

Polygon's vision is founded on a clear premise: to become the go-to technology provider to build on for anyone, from retail to institutions. In other words, the main goal of Polygon is to become the AWS of Web3 development. To that end, the speed of expansion is the top priority for Polygon. The Foundation has been aggressive in growing its ecosystem via incentives and acquisitions of the right technology and the right people. To grow even faster, Polygon has recently raised more VC financing.

Polygon has committed $1 billion to invest in its ZK thesis. Last year, it has spent $650 million in acquiring Hermez and Mir. This means that Polygon still has an appetite of up to $350 million to acquire more ZK solutions as it deems fit. While the balance on Polygon Foundation's wallet is now left with a quarter of its allocation at launch (~600 million MATIC worth US$530 million), it raised another $450 million just in February this year. Taking both into consideration, it still has about close to a runway of US$1 billion dollars, more than enough to support its ZK ambition.

Acquisition

It acquired Hermez in August 2021 for $250 million, and Mir Protocol in December 2021 for $400 million as part of Polygon's expansion into zero-knowledge (ZK) proofs.

The acquisitions inevitably compete with one another and with Polygon's existing solutions, but Polygon is not afraid to acquire competing solutions. In fact, what is admirable about Polygon is they have been able to get different competing Layer-2 solutions to work with one another seamlessly. It is because of carefully planned technological investments like these that Polygon looks to be able to deliver zkEVM ahead of its competition.

The acquisitions were funded mostly from the Polygon Foundation's treasury because it only closed the $450M round after the acquisitions.

Fundraising

Polygon has raised roughly $460 million in funding, including US$5m that Polygon raised through public sale on Binance Launchpad in 2019. They did raise another round from Mark Cuban for an undisclosed amount.

Date	Round	Number of Investors	Money Raised	Lead Investor
Jul 13, 2022	Grant	1	$120K	Disney Accelerator
Feb 7, 2022	Venture Round	40	$450M	Sequoia Capital India
May 26, 2021	Seed	1	Undisclosed	Mark Cuban
Apr 30, 2019	Seed round	2	$450K	Coinbase Ventures
Apr 25, 2019	Token public sale	N/A	$5M	N/A

Exhibit 5 Polygon's Past Fundraising (Source: Crunchbase)

VIII. Key People

Polygon has been growing the number of top talents the same way it grows the number of offerings. They have been adding the founders of the acquired projects as co-founders of Polygon. By doing so, Polygon ensures that the success of any single project also implies the success of other projects under its umbrella.

The Matic Network was initiated in 2017 by three co-founders:

- Sandeep Nailwal, who was previously the co-founder & CEO at ScopeWeaver.com, a marketplace for professional services, and the Head of Technology and Supply Chain at Welspun Group, a conglomerate operating in steel, energy, and textile industries, and software engineer at Computer Sciences Corporation
- Jaynti Kalani, who was the Data Scientist at Housing.com, a real estate search platform, and senior software engineer at Persistent Systems, an IT services company
- Anurag Arjun, who is the only non-programming co-founder of Polygon. As a product manager, he has had stints with IRIS Business, SNL Financial, Dexter Consultancy, and Cognizant Technologies

In December 2020, Mihailo Bjelic joined as the fourth co-founder. Mihailo is a prominent Ethereum community member and researcher who was working on a similar solution to Matic Network.

With the acquisition of the Mir protocol, Polygon added two more co-founders:

- Brendan Farmer built tech tools used on national political campaigns before studying pure math and philosophy as an AB Duke Scholar. He became interested in cryptography after the Snowden leaks.
- Daniel Lubarov came from Google, where he worked on Glass and Pixel Buds. Prior to that, he worked at Square building scalable and fault-tolerant payment systems. He studied computer science at Harvey Mudd.

Three more co-founders joined Polygon in August 2021 as Polygon and Hermez merged:

- David Schwartz, the project lead for Hermez, has over 20 years of experience in the IT industry, having held different engineering and executive positions in telecom operators, consulting firms, and technology providers. Since 2018, he has been leading projects at iden3 and Polygon Hermez.
- Jordi Baylina is the technical lead for Hermez. He is a high-impact contributor in the Ethereum community, and the co-founder of iden3 as well as the White Hat Group, which played a major role in rescuing funds from TheDAO and Parity Multisig hacks.
- Antoni Martin is the Business Development lead for Hermez. He previously worked on a digital asset platform at Deutsche Bank and cofounded iden3 with David Schwartz and Jordi Baylina.

Finally, in November 2021, Polygon announces that Bobbin Threadbare, the core developer of both Distaff VM—the first practical STARK-based virtual machine, and Winterfell—a highly-performant STARK prover developed at Facebook's Novi, is joining as a co-founder to lead the development of Polygon Miden.

The team is additionally supported by a community of reputable advisors, including Mark Cuban, Hudson Jameson from the Ethereum Foundation, Ryan Sean Adams from Bankless, Anthony Sassano from EthHub & SetProtocol, Pete Kim from Coinbase, and John Lilic – ex ConsenSys.

X. Tokens

Polygon's native token, MATIC, is currently used for only its PoS Chain but the company has confirmed that MATIC will be redesigned.

PoS Chain

MATIC is used as a currency for users to pay gas fees, and for validators to receive incentives for processing and verifying transactions. To be a validator, one needs to run a full validator node and stake MATIC. To be a delegator, one only needs to delegate MATIC to a validator. Both validators and delegators earn staking rewards, but validators have the option to charge a commission on the reward earned by delegators. In addition, validators also earn transaction fees collected in each block.

This also means that the staking rewards are not financed by transaction fees at the moment. Polygon allocates 12% of its total supply of 10 billion tokens to fund the staking rewards. This is to ensure that the network is seeded well enough until transaction fees gain traction. These rewards are primarily meant to jump-start the network, while the protocol in the long run is intended to sustain itself on the basis of transaction fees generated.

While annual inflation of ~3% of circulating supply is not high compared to many L1 and L2 protocols, we do this continuing as transaction fees will not cover staking rewards anytime soon. The total transaction fees paid over the past year is 18.8 million MATIC tokens, while the staking reward pool paid out last year is ~250 million MATIC. It is not an easy fix because for transaction fees to match staking rewards, Polygon PoS needs to increase its transaction volume or increase gas fees by 10x.

Beyond PoS Chain: Token Redesign

The company has not given out any details about the token redesign, but based on the interviews with the co-founders, our best guesses are:

- MATIC will remain the only token powering the Polygon ecosystem and will be used across chains; instead of creating additional assets, MATIC's use cases will expand
- On Hermez, Nightfall, Miden, and Avail, MATIC will be used for paying transaction fees happening on L2. The transaction fees are then paid as rewards to those running a node. In the case of Hermez, for example, aggregators are incentivized with MATIC fees
- For zkEVM specifically, we expect zkProver—the node that generates validity proofs—to be decentralized in the future and MATIC will be used for rewarding those running a zkProver node for providing validity proofs
- MATIC will also become a governance token. The tokens allow the user to be part of the upcoming Polygon DAO where token holders can vote on protocol changes including raising transaction fees or adding new features to the protocol.

Any of the above would increase the demand for MATIC and therefore be bullish for the token price. **In fact, as soon as 3-6 months from now, we expect Hermez 2.0 to hit the mainnet, increasing the demand for MATIC.**

XI. Technical Analysis

Since the beginning of 2022, MATIC experienced a similar big drop as NFT-related names like FLOW and other smaller blockchains like AVAX and ADA. FLOW in particular trades very closely to MATIC. This suggests that **investors often view Polygon PoS as a similarly NFT-centric chain.**

Exhibit 6 MATIC vs. AVAX, ADA, FLOW, DOGE

Exhibit 7 MATIC vs. FLOW

However, since the Luna crypto crash in June 2022, the correlation between MATIC and some of the bigger protocols ETH and BNB has become high. We would also note that MATIC enjoyed a sharp rally in July 2022 on news of its acceptance into Disney's annual accelerator program. However, the subsequent trading has been quite correlated, which suggests to us that **the potential for MATIC's increased role in an expanded ecosystem in 2023 has not yet been priced in.**

Exhibit 8 MATIC vs. ETH

Exhibit 9 MATIC vs. BNB

XII. Valuation

We examine the relationship between Polygon and Ethereum, Avalanche, and Flow, in terms of their valuation based on Market Cap to Transaction Volume. Additionally, we add Solana and OpenSea to the mix to capture broader market trends.

	Circulating Market Cap (in mil)	Annualized Txn Volume 30D (in mil)	Circulating Price/Volume	Month of Peak Txn Volume	Circulating Market Cap at Peak Txn Volume (in mil)	Annualized Peak Txn Volume 30D (in mil)	Price/Volume at Peak Txn Volume	Current trend: % Change in Txn Volume Last 30D	YTD trend: % Change in Txn Volume Jan 2022 vs. 30D	Peak to now: % Change in Txn Volume Peak vs. 30D
	A	B	C = A / B	D	E	F	G = E / F	H	I	J
Polygon PoS	7,935	976.37	8x	Jun 2021	8,800	2502.77	4x	-2.20%	41.60%	-61.85%
Ethereum	193,256	404.87	477x	May 2021	372,990	540.66	690x	-1.03%	-9.39%	-25.89%
Avalance	5,585	57.44	97x	Mar 2022	20,084	327.88	61x	1.82%	-79.56%	-82.16%
Solana*	11,935	11906.16	1x	Nov 2021	67,500	18120.00	4x	-25.50%	-38.40%	-51.05%
Flow	1,752	367.81	5x	Jun 2022	2,040	407.79	5x	-25.69%	146.72%	-32.98%
OpenSea	N/A	18.79	N/A	Jan 2022	N/A	33.79	N/A	-20.28%	-55.67%	-55.67%
*) Solana's transaction volume is inflated because of its zero transaction fees										

Exhibit 10 Valuation of Polygon PoS vs. Various Chain

Basis the table above, we believe that Polygon is currently undervalued and should be worth at least as much as Solana's ~$12 billion circulating market cap. Our thesis is supported by:

- Polygon PoS has had an annualized transaction volume of 976.37 million in the last 30 days. For context, it is much bigger than most chains and is second only to Solana's— and Polygon is valued at single digit P/V multiple. Only Flow (NFT-centric and powered by a single studio) and Solana are cheaper -- but we highly discount Solana's volume figures because Solana is famous for spam transactions due to its zero fees. (Heavy spamming is also the key reason for Solana's frequent network outages.)
- Compared to Ethereum specifically, Polygon's transaction volume is 2.4x Ethereum's, and yet its market cap is 1/60th of Ethereum's.
- Further, the YTD number of transactions on Polygon PoS has been resilient as compared to other chains. While down from its peak transaction volume, like all other networks, Polygon has been relatively stable recently while having bounced from the low at the beginning of 2022. We think the strength of Polygon's broader ecosystem is reflected in this resiliency.
- Finally, as Polygon launches its four L2 solutions over the next 6-18 months, Polygon will be worth significantly more. Optimism, with a single L2 solution, has a fully diluted market cap of $4 billion while its circulating market cap will be ~$2 billion by mid-2023. We believe that Polygon's Hermez 2.0 zkEVM solution will be at least as competitive as Optimism and Arbitrum, despite a later launch, and we believe Hermez 2.0 alone can add an additional $2+ billion to Polygon's market cap. Success by Nightfall, Miden, and Avail will only increase this value accretion.

We present our base case of MATIC's valuation as $12 billion, or roughly $1.37 per token, giving us an upside of 50% from the current price. We believe that the re-pricing of MATIC tokens will happen in Q1 2023, thanks to three catalysts:

- Polygon zkEVM's will be launched on mainnet, which not only is positive news but also from a fundamental perspective, increases the demand for MATIC
- The launch will likely be in a better macro condition, as we start to see early signs of the slowdown of Fed tightening
- As Polygon launches zkEVM, we expect them to also unravel the redesigned MATIC. We expect MATIC to be used not only for gas and staking on the PoS chain. Instead, the use cases will be extended to gas and staking for all projects, and governance for Polygon DAO, making MATIC clearly more valuable

Scenarios	***Thesis***
Bullish Target: US$2.00 Probability 15%	Polygon's L2 projects are launched on time, perform better than alternatives and overtake Arbitrum and Optimism as the market leader in L2.
Base Case (mostly likely) Target: US$1.37 Probability 60%	Polygon's L2 projects are launched on time, perform mostly as expected and garner comparable adoption as Arbitrum and Optimism.
Bearish Target: US$0.75 Probability 25%	Polygon's L2 projects are delayed, perform worse than expected, and/or fail to gain less adoption than alternatives.