Korea Blockchain Week KBW

Complete Guide to Polygon: Tech & Business Insights

TABLE OF CONTENTS

1. Introduction

The crypto market is still in the midst of a bear market. The global macroeconomic situation is not favorable, and the aftermath of crypto-specific black swan events like Luna and FTX debacles have made it difficult to expect a recovery just yet. However, this is only from a price perspective. When looking at the overall blockchain industry, there is continuous technological advancement and various business cases are emerging.

Among several blockchain platforms, Polygon stands out as it continually pushes for technological progress and ecosystem growth, even with its established user base and active network. Even in the midst of a bear market, Polygon continues to develop its technology stack, including its ZK technology and has announced a new roadmap called Polygon 2.0.

In addition, governments, financial institutions, and enterprises are using Polygon to expand their services with blockchain. For example, the Monetary Authority of Singapore (MAS) and the Bank of Italy experimented with the introduction of blockchain with Polygon, asset management giants like Franklin Templeton (AUM: $1.5T) and Hamilton Lane (AUM: $818B) tokenized their funds on the Polygon network, and global companies like Starbucks, Nike, and Reddit are running their Web3 services on Polygons. How was Polygon able to achieve its current status?"

Polygon was founded in 2017 by a group of Mumbai-based software engineers and was initially called the Matic Network. It initially aimed to improve the scalability of the Ethereum network by utilizing plasma technology. As the Ethereum network became congested during the DeFi summer of 2020 and the crypto bull run of 2021, users began to look for faster and cheaper networks. Consequently, the TVL of the Polygon PoS network rapidly increased from $100M in March 2021 to $7B in July 2021.

However, the Polygon team did not stop there, clearly recognizing the limitations of plasma technology, and quickly pivoted in the direction of zk rollup and modular blockchains. The team has been aggressive in developing and expanding zk technology, acquiring Hermez for $250M in August 2021, and Mir Protocol for $400M in December 2021 Also, it received a total of $450M in investment from Sequoia Capital India, SoftBank, Tiger Global, and others in February 2022 to accelerate the expansion of the ecosystem and technology.

Starting with Polygon PoS, Polygon now operates and develops a number of technology stacks, including Polygon zkEVM, Polygon Miden, Polygon Supernets, and Polygon ID, and has been aggressive in business development, collaborating with various Web2 companies. This report will cover Polygon's various solutions and the Polygon 2.0 roadmap, and see what business cases are actually built on top of Polygon.

2. Polygon Solutions

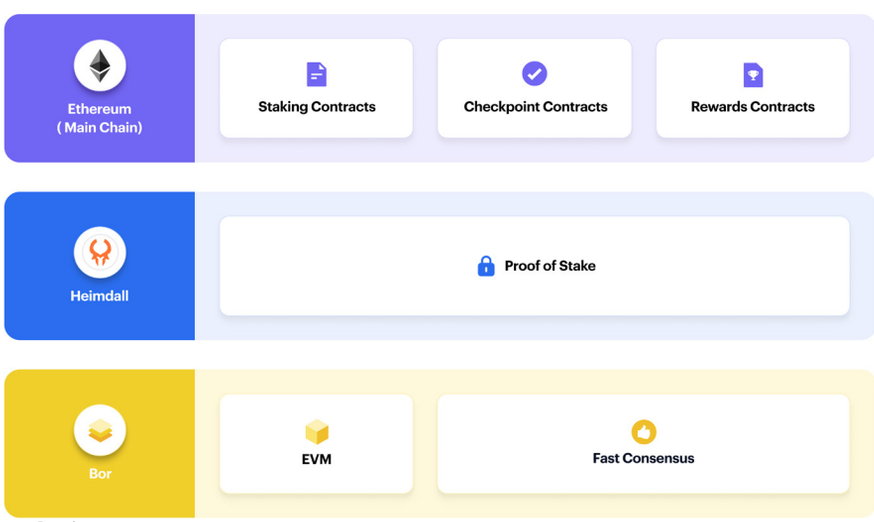
2.1 Polygon PoS

2.1.1 Overview

Polygon PoS is one of the most popular EVM-compatible networks with a TVL of around $800M, 300k-500k daily active wallets, and over 2M daily transactions. The execution layer is implemented in Geth, Ethereum's native client, so developers can easily deploy smart contracts using existing Solidity code, development tools, etc.

Polygon PoS does not have a fraud proof system, but it does periodically record state roots(a.k.a. checkpoints) on the Ethereum network, making it an intermediate between sidechain and plasma. However, in the recent Polygon 2.0 roadmap, there was a proposal to upgrade the Polygon PoS to a validium based on Ethereum, which we'll discuss in the Polygon 2.0 section.

2.1.2 Architecture



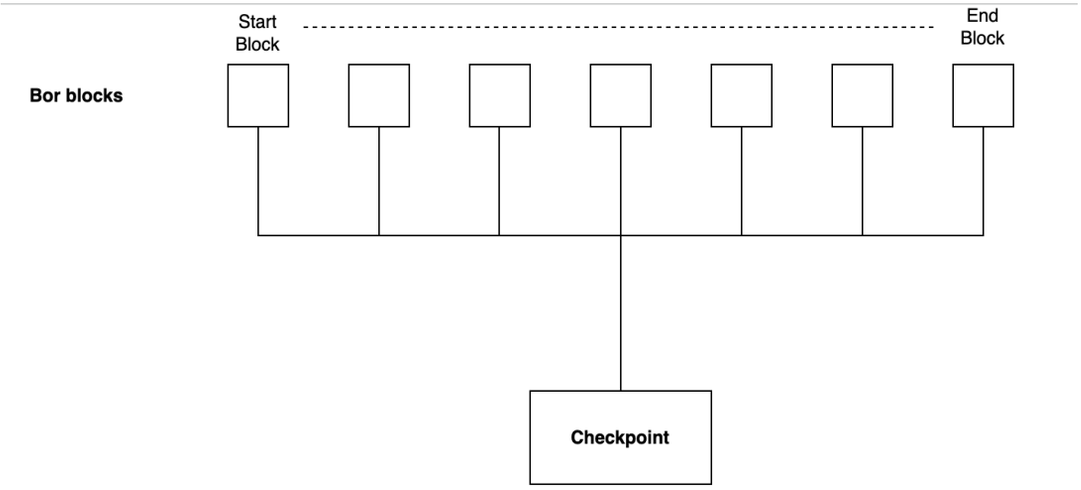
(Source: Polygon Docs)

Polygon PoS is composed of three layers:

Bor layer - It is an EVM-compatible network based on Geth, aggregating users' transactions to produce blocks.

Heimdall layer - It is a PoS validation layer based on Peppermint, a modified version of Tendermint. The Heimdall layer performs several roles, including 1) validating the blocks generated by the Bor layer, and 2) submitting checkpoints, which are state roots, to the Ethereum mainnet.

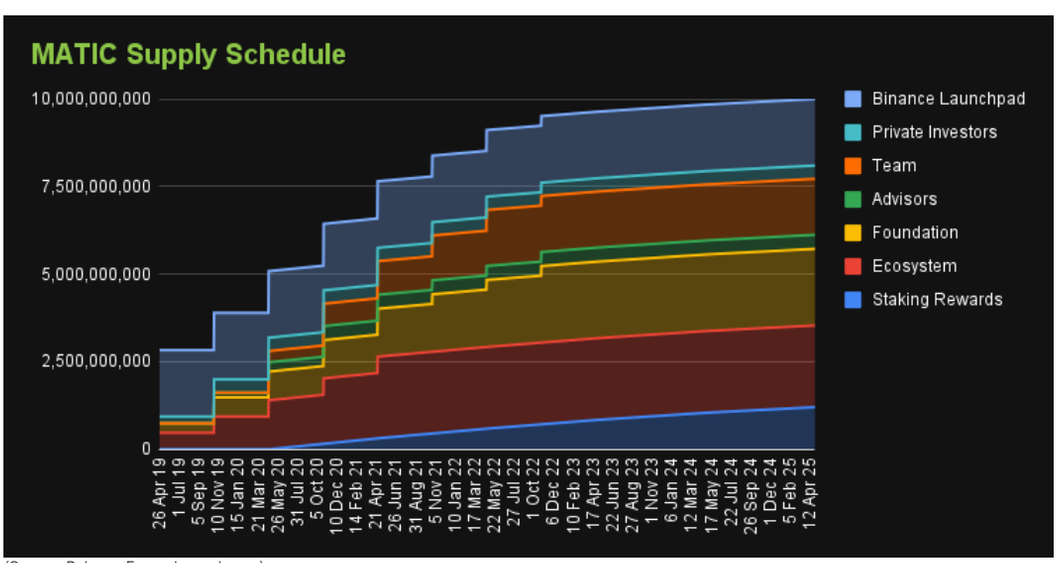
Ethereum layer - Smart contracts related to Polygon PoS exist on the Ethereum network. These contracts allow users to stake MATIC tokens to participate in validation or delegated staking. They also store checkpoints passed from the Heimdall layer.



(Source: Polygon Docs)

Checkpoints are a core feature of Polygon PoS and can be described as a snapshot of the state of the Bor layer. Checkpoints contain the state root, which is the Merkle root (a type of summary value) of the state of Bor blocks within a certain period. By submitting this to the Ethereum network, Polygon PoS can provide finality at the security level of the Ethereum network.

2.1.3 Economics



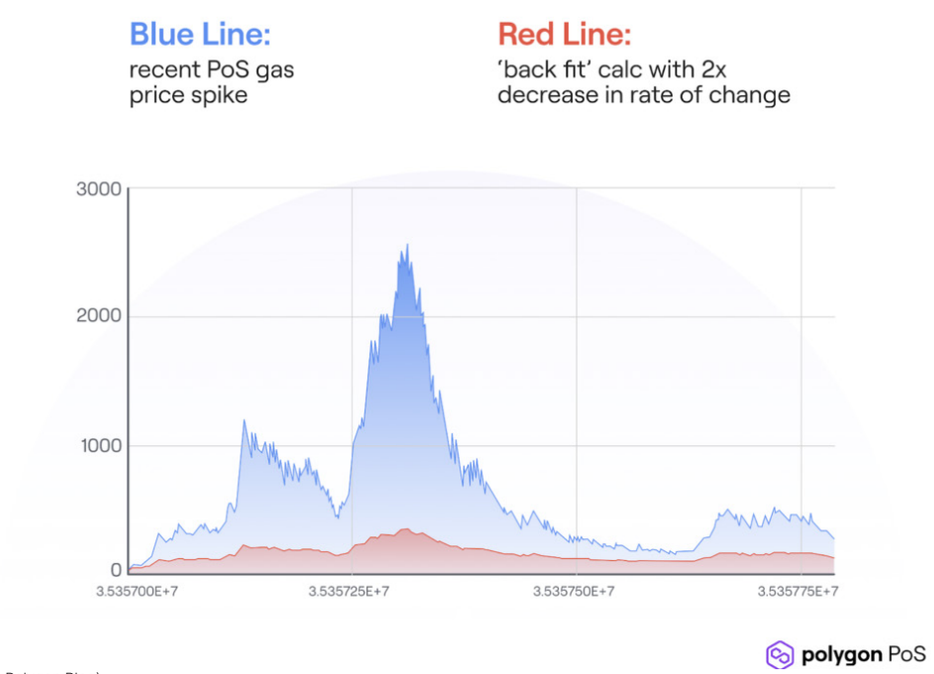
(Source: Polygon Forum by pedro_nv)

The primary currency of Polygon PoS is the MATIC token, which has utilities such as staking and transaction fees. Validators can receive block rewards and a portion of users' transaction fees by participating in the block creation process.

Originally, 10,000,000,000 MATIC tokens were to be issued. However, the forthcoming

Polygon 2.0 tokenomics proposed an annual 2.0% inflation. As of August 2023, approximately 9,300,000,000 tokens are in circulation, which gives it an advantage in terms of having lower inflationary pressure compared to other L1 networks.

Polygon PoS uses a modified version of the Ethereum network's EIP-1559 model for transaction fees. To briefly explain EIP-1559: 1) The gas fee for the next block is determined based on the usage of the previous block, and 2) all tokens equivalent to the base fee (excluding the priority fee) from users' transaction fees are burned. If the usage of the previous block is low, the gas fee for the next block will decrease, encouraging more usage. Conversely, if the previous block had high usage and the network was congested, the gas fee for the next block can be increased to discourage network usage.



(Source: Polygon Blog)

In the Ethereum network, the maximum fluctuation range of gas fees per block is limited to -12.5% to +12.5%. Polygon PoS also initially adopted the same figures, but in January 2023, they completed an upgrade to limit it to half, i.e., -6.25% to +6.25%. This measure was taken to prevent gas fees from skyrocketing when network usage surges.

From the perspective of token burning, the transaction fees on the Polygon PoS network are so low that there isn't a significant amount of burning. As of August 2023, approximately 16 million MATIC tokens have been burned.

Recently, along with the Polygon 2.0 upgrade, new POL tokenomics were unveiled, which will be discussed in the 'Polygon 2.0' section.

2.1.4 Thoughts on Polygon PoS

Polygon PoS records checkpoints on the Ethereum network, but due to the quick finality provided at the Bor layer, user-generated transactions can be quickly finalized. In other words, the latency experienced by users on Polygon PoS is extremely low, making it an attractive environment for businesses targeting general users. As we'll see later, many corporations (e.g., Starbucks, Reddit, Nike, and more) are already leveraging the Polygon PoS network.

Polygon PoS doesn't stop here. In the Polygon 2.0 roadmap, they plan to upgrade to validium. As outlined in the Polygon 2.0 roadmap, there are plans to transition to validium. After this shift to validium, the network is anticipated to offer enhanced security, decentralization, and scalability. Such advancements will likely open doors to fresh business prospects for numerous companies.

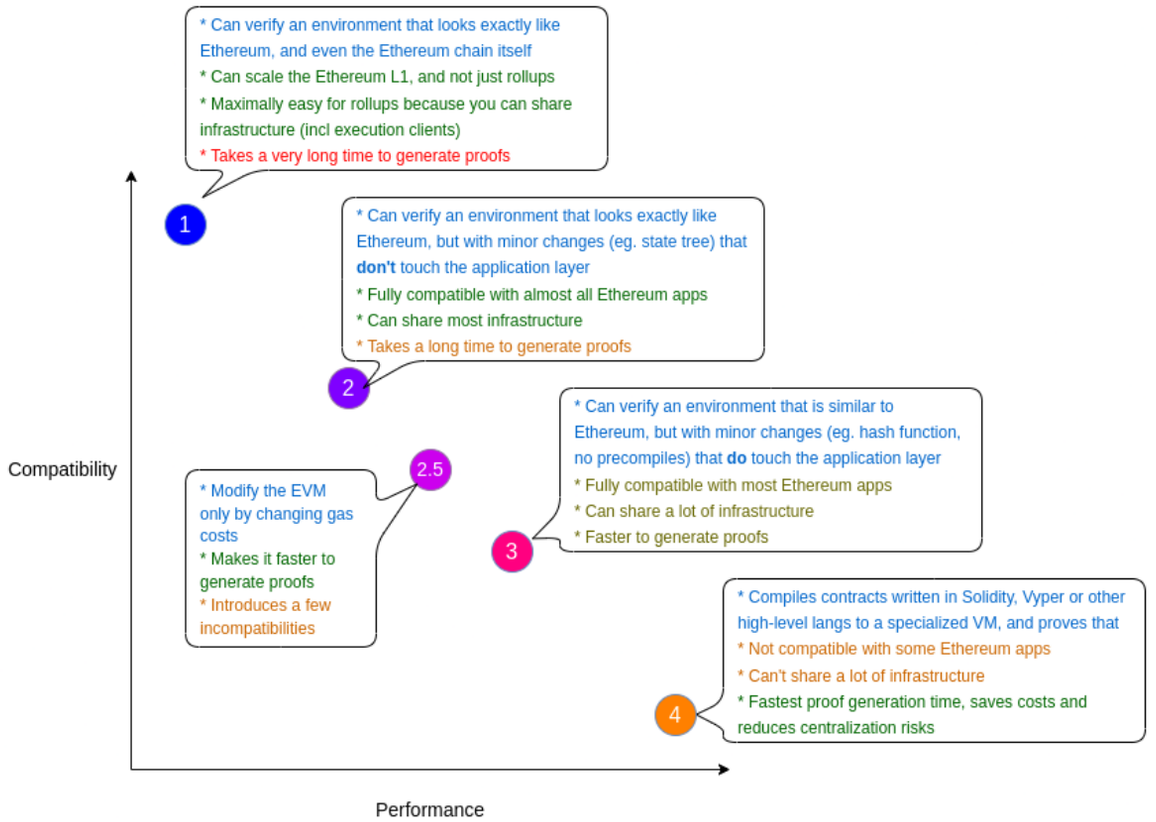
2.2 Polygon zkEVM

2.2.1 Overview

Polygon zkEVM is an EVM-compatible zk rollup, using Ethereum as a base layer. In the past, Polygon acquired zk technology teams Hermez and Mir protocol, and Polygon zkEVM is the result of utilizing their state-of-the-art technologies. Polygon zkEVM stores all transaction data on the Ethereum network, ensuring complete security backed by Ethereum while maintaining high scalability. Furthermore, due to its robust EVM compatibility, Polygon zkEVM offers a developer-friendly environment by allowing developers to use their existing Ethereum smart contract code with minimal changes.

2.2.2 zkEVM

A zk-rollup is a rollup network that proves the validity of executions through Zero-Knowledge Proofs (ZKP). However, the EVM wasn't originally designed with zero-knowledge technologies in mind. Therefore, generating ZKPs for EVM executions is quite challenging. In other words, implementing an EVM-compatible zk-rollup is technically very demanding.

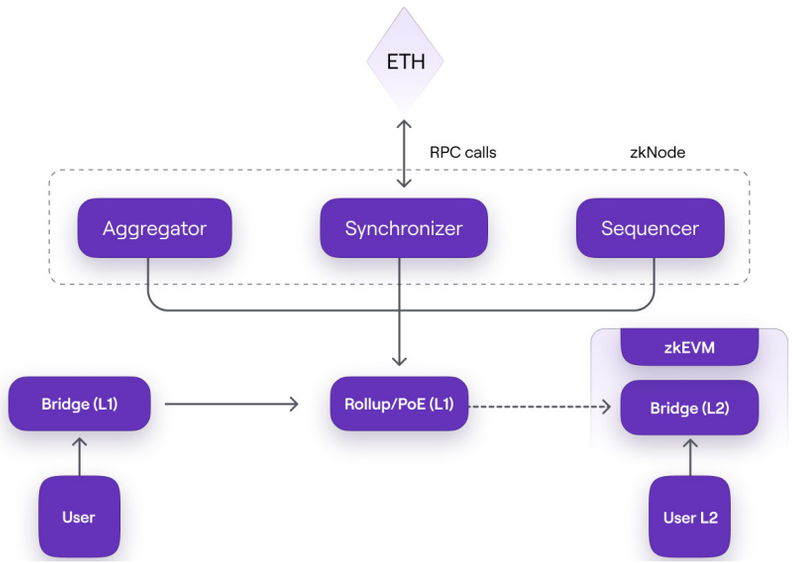


(Source: Vitalik Buterin)

Vitalik Buterin proposed categorizing various general-purpose zk-rollups into [five types](https://vitalik.ca/general/2022/08/04/zkevm.html) based on their EVM compatibility. In general, there is a tradeoff between EVM compatibility and network performance, with Type 1 being the most EVM-compatible and Type 4 being the least EVM-compatible. Polygon zkEVM is categorized under Type 3, alongside other significant projects like Scroll and Linea. Meanwhile, Starknet and zkSync Era belong to Type 4. Up to now, no network has reached Type 2.5 or above on the mainnet, and numerous initiatives are striving to enhance their EVM compatibility.

From Type 3 onwards, there's direct support for EVM bytecode, making it aptly termed "EVM-compatible". This lets developers use existing Ethereum network tools and smart contract code with minimal modifications. Though Type 4 offers superior ZKP generation capabilities, its requirement to adapt smart contract code to a zero-knowledge-centric language means it isn't entirely EVM-compatible, leading to a slightly less intuitive experience for developers compared to Type 3.

2.2.3 Architecture



(Source: Polygon Docs)

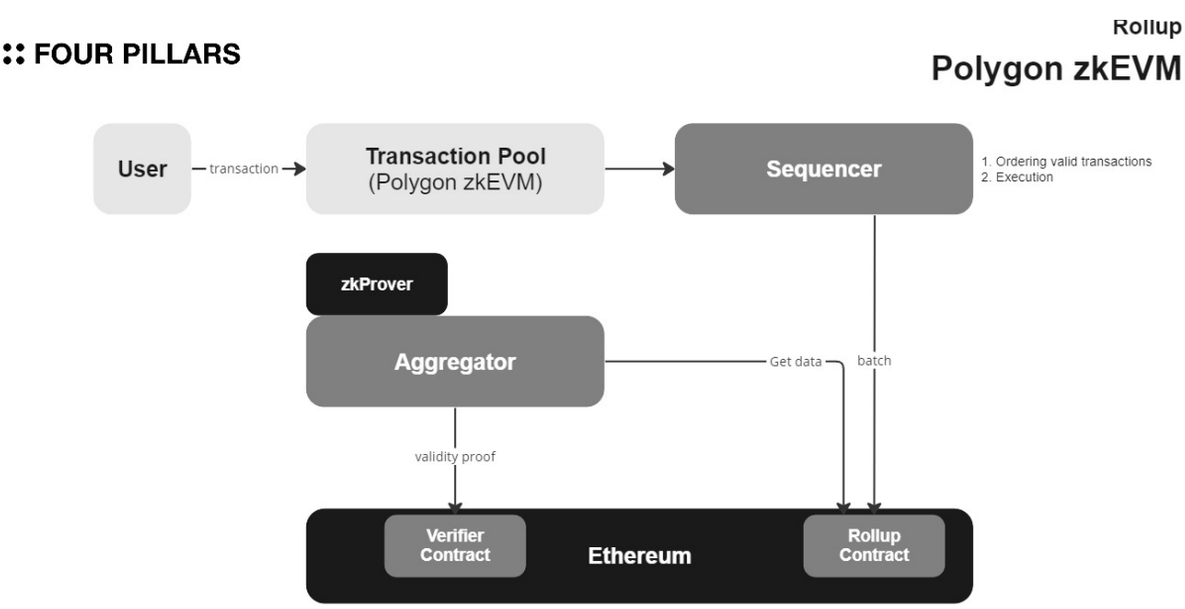
The Polygon zkEVM consists of the following components:

Consensus Contract (PolygonZkEVM.sol) - A rollup smart contract deployed on the Ethereum network that implements Polygon zkEVM's consensus mechanism, Proof of Efficiency (PoE), and plays various other pivotal roles. (See the Economics section for more on PoE)

zkNode - Polygon zkEVM's node client software. zkNode consists of a Syncrhonizer, Sequencers, Aggregators, and RPC. Sequencers and Aggregators are participants in the PoE consensus algorithm, which is currently centralized.

zkProver - Software that allows Aggregators to generate ZKPs.

zkEVM Bridge - a smart contract related to the transfer of funds between users' L1-L2, deployed on both the Ethereum mainnet and Polygon zkEVM.



(Transaction Lifecycle | Source: Modular Odyssey by Four Pillars)

User-generated transactions follow the lifecycle illustrated above:

1. Signed transactions generated from users' wallets are sent to the Sequencer node.

2. The Sequencer node checks the basic validity of transactions, determines the order of valid transactions, and executes them to update the L2 state.

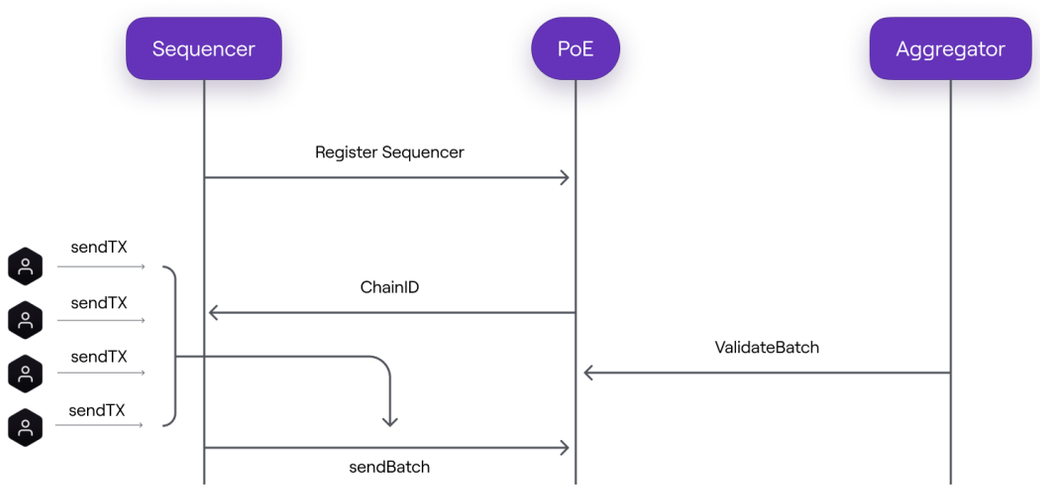
3. The executed transactions are put into a batch and sent to a smart contract on Ethereum.

4. The aggregator verifies the batch sent to the smart contract, generates a validity proof for it, and sends it to the verifier contract.

5. After validating the proof of validity in the Verifier contract, the user's transaction is finalized.

2.2.4 Economics

In the Polygon zkEVM network, transaction fees are paid in ETH, not MATIC. Most people tend to believe that for rollups, using native tokens like MATIC for transaction fees would better accumulate value for the MATIC token. However, this notion is incorrect. Rollup networks pay gas fees on the Ethereum network to store transaction data. So even if Polygon zkEVM used MATIC for transaction fees, it would eventually have to sell MATIC for ETH to cover gas expenses. Theoretically, this means that the net value accumulated in the MATIC token could be considered as zero.



(PoE | Source: Polygon Docs)

However, it's not that MATIC is not used at all in Polygon zkEVM; it is utilized in the PoE mechanism. The PoE process encompasses the ordering of user transactions, the generation of validity proofs, and the associated incentive scheme. The PoE process involves a Sequencer, which orders the user transactions, and an Aggregator, which generates validity proofs after observing the batch submitted to the smart contract.

The procedure goes as follows:

1. Sequencers collect and order transactions, create batches of them, and collect transaction fees (ETH) from users.

2. Sequencer submits batches to the Ethereum network and pays a basic L1 transaction fee and an additional MATIC token. (Sequencer makes a profit if the transaction fee received from users is greater than the L1 transaction fee + MATIC token).

3. The Aggregator listens to batch submitted to the smart contract and computes it to generate a validity proof. If it is successfully generated and submitted, it will receive the MATIC tokens paid by the Sequencer.

2.2.5 Thoughts on Polygon zkEVM

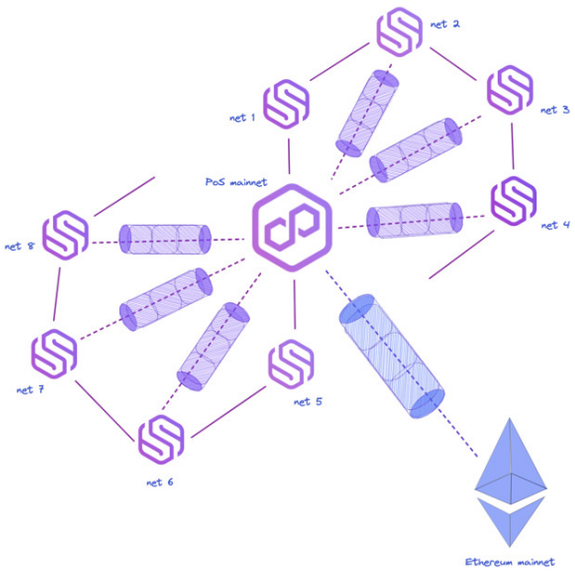
Polygon zkEVM hasn't been on the mainnet for very long. However, three key points make it promising for future business opportunities: 1) Unlike Polygon PoS, it relies on the security of the Ethereum network. 2) The upcoming EIP-4844 upgrade in the Ethereum network is set to enhance the scalability of rollups. 3) As Polygon's zk technology matures, there's significant potential for scalability improvements. Therefore, it's anticipated that many more business opportunities will emerge in the future.

2.3 Polygon Supernets (Polygon CDK)

(On August 30, 2023, an upgraded version called Polygon CDK of Polygon Supernets was released. Please refer to the appendix at the end of the report for details on Polygon CDK.)

2.3.1 Overview

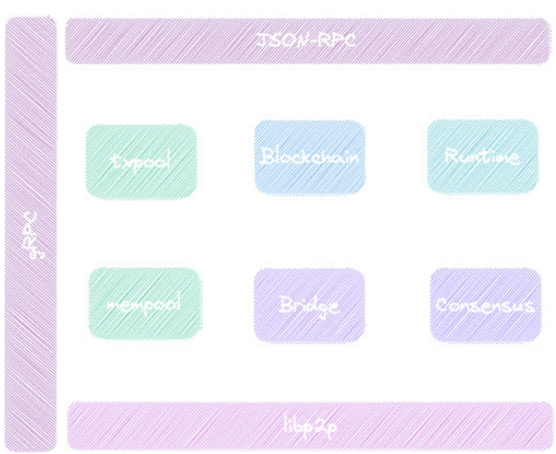
Polygon Supernets is an EVM-based app-specific chain in the Polygon ecosystem, similar to Cosmos' app-chain and Avalanche's Subnet. Since app-chain is a customizable blockchain, developers can configure and use the blockchain network according to the specific purpose of their enterprise or service.



(Source: Polygon Docs)

Currently, Polygon Supernets require a minimum of 3-4 and a maximum of 100 validators because they are an L1 network based on the Polygon Edge technology stack and the PolyBFT consensus algorithm. However, this will change significantly in the Polygon 2.0 roadmap, as Polygon Supernets will support not only L1 networks, but also zk rollup or validium modes utilizing ZK technology. Each Supernets chain will be able to utilize a common pool of validators from the Polygon 2.0 ecosystem, rather than operating their own pool of validators.

2.3.2 Architecture



(Source: Polygon Docs)

Polygon Supernets consist of the following components:

- **Consensus:** PolyBFT is the consensus algorithm for Polygon Supernets, and is based on IBFT 2.0, which is pretty much the same as PBFT in general. For the secure network, there must be at least 2/3 honest validators.
- **Bridge:** Polygon Supernets has a built-in bridge to communicate with EVM-compatible PoS chains.
- **Networking (libp2p):** PolyBFT utilizes a networking layer based on the libp2p protocol, which supports peer discovery to find other nodes in the network,

connection management with nodes, and secure messaging.
- **Runtime:** The default runtime for Polygon Supernets is EVM, which supports the same opcode set as EVM.
- **Memory Pool:** The storage space where pending transactions reside before being included in a block.
- **JSON-RPC, gRPC:** Various RPC protocols make it easy for users, developers, and nodes to interact with the blockchain.

2.3.3 Economics

Since Polygon Supernets is currently an L1 network, it has an economy similar to a exisiting blockchain network, and the fee token can be set to any token.

If the transition to Polygon 2.0 leads to the support of Polygon Supernets for zkEVM and validium modes, these won't follow the conventional economics because they rely on the security of the Ethereum network. The validators of Polygon Supernets act as sequencers determining the order of transactions, and in the case of validium, they ensure data availability. They can receive basic protocol rewards, transaction fees from participating in Polygon Supernets, and additional bonuses.

2.3.4 Thoughts on Polygon Supernets

Most companies tend to build their own network rather than using a public blockchain when they introduce blockchain technology. Polygon Supernets provide a solution that makes it easy to build such networks, making them an ideal solution for these companies. In fact, many businesses and protocols, such as Nubank, Gameswift, Palm network, and Nexon, are currently developing their networks using Polygon Supernets.

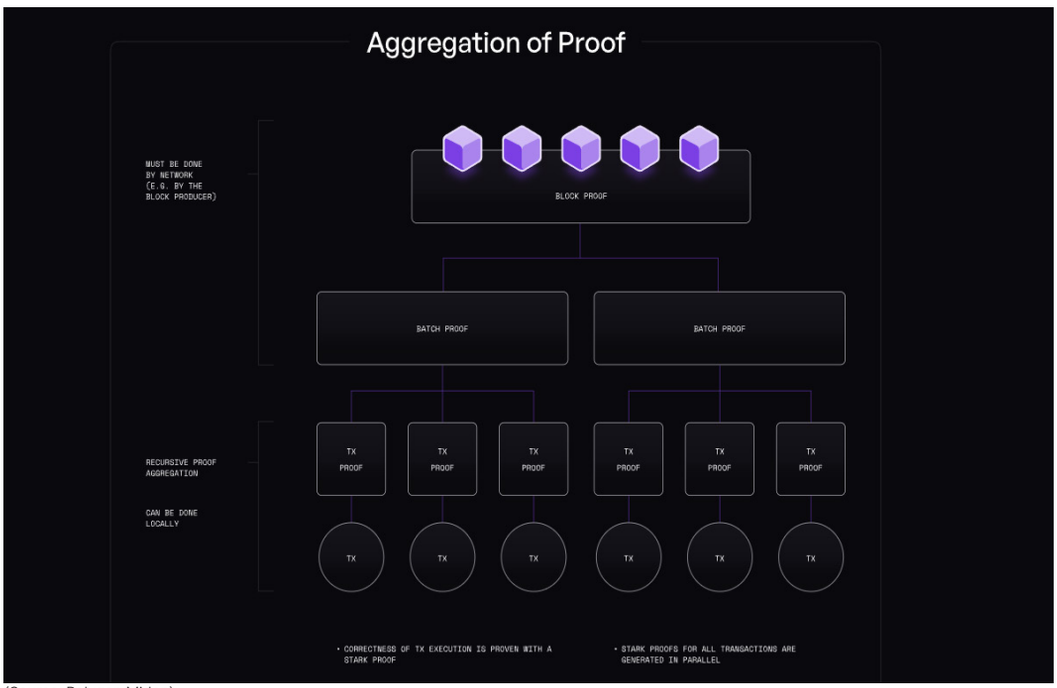
While Polygon Supernets currently only support L1 network development, they plan to expand their support to include zk rollup and validium modes, allowing businesses to build their own L2 networks that rely on Ethereum security. One of the major drawbacks when building an app-specific L1 network is its weak initial security, but with an L2 network, even this downside can be addressed. Hence, it's anticipated that more companies will use Polygon Supernets in the future.

2.4 Polygon Miden

2.4.1 Overview

Polygon Miden is a general-purpose zk-rollup network, similar to the Polygon zkEVM

network. However, it incorporates a zkVM called Miden VM instead of zkEVM, emphasizing performance over EVM compatibility. Polygon Miden uses STARK-based zero-knowledge technology.



(Source: Polygon Miden)

The process of creating a zero-knowledge proof can be largely divided into two approaches: client-side proving, where a user generates a transaction and simultaneously creates a local zero-knowledge proof to submit; and server-side proving, where the generation of the zero-knowledge proof occurs at the network level. Examples of the former include ZCash and Tornado Cash, while most zk-rollup networks belong to the latter category.

The reason client-side proving is challenging in zk-rollup networks is that generating a zero-knowledge proof requires significant computational power, including demanding hundreds of gigabytes of RAM. In Polygon Miden, users are able to generate zero-knowledge proofs locally, which reduces the burden on the network operator. Additionally, a large number of transactions can generate zero-knowledge proofs in parallel, resulting in high scalability.

In Polygon Miden, individual accounts can also maintain their unique state, executing smart contracts locally. This is secured by the presence of zero-knowledge proofs. Typically, in blockchain networks, all users and nodes refer to a single global state. However, in Polygon Miden, accounts can selectively update the states of other accounts, and the validity of their own state can be proven through zero-knowledge proofs. Thanks to this unique computational model, Polygon Miden can offer various features, including privacy.

In addition, Polygon Miden has a lot of other features, including:

- **UTXO Model:** Most smart contract networks use an account-based model, similar to the Ethereum network. However, Polygon Miden employs a state model similar to Bitcoin's UTXO, enabling the development of applications that were difficult to implement in traditional smart contract networks. Additionally, the UTXO model enhances security. In traditional account-based networks, if a token contract is attacked, it could impact all holders of that token. But in Polygon Miden, all assets are treated as native assets and are stored locally in individual accounts. To attack this, one would need to target every single account, which can be considered much safer.

- **Privacy:** Polygon Miden allows users to execute private smart contracts in a local environment, providing them with the option to maintain their privacy selectively.

2.4.2 Thoughts on Polygon Miden

Polygon Miden is still an under-development rollup network, but it incorporates numerous features that have not been seen in any blockchain networks so far. From the perspective of zk rollup, Polygon Miden is a network that prioritizes performance over EVM compatibility. Additionally, the network adopts features like the UTXO model and hybrid state models. Therefore, the developer environment is expected to be somewhat more challenging compared to the Ethereum network.

On the flip side, Polygon Miden offers an environment where a variety of features that were difficult to implement in existing blockchain networks can be experimented with. Due to its use of the UTXO model, Polygon Miden is less susceptible to bugs and therefore offers increased security. Additionally, it provides optional privacy features, allowing companies and financial institutions who have been hesitant to use blockchain due to transparency concerns to implement their business logic without worries.

Once Polygon Miden is launched and its development environment matures to a certain extent, it is expected to grow into a network with a unique position that encompasses scalability, security, privacy, and various other features.

2.5 Poygon ID

2.5.1 Overview

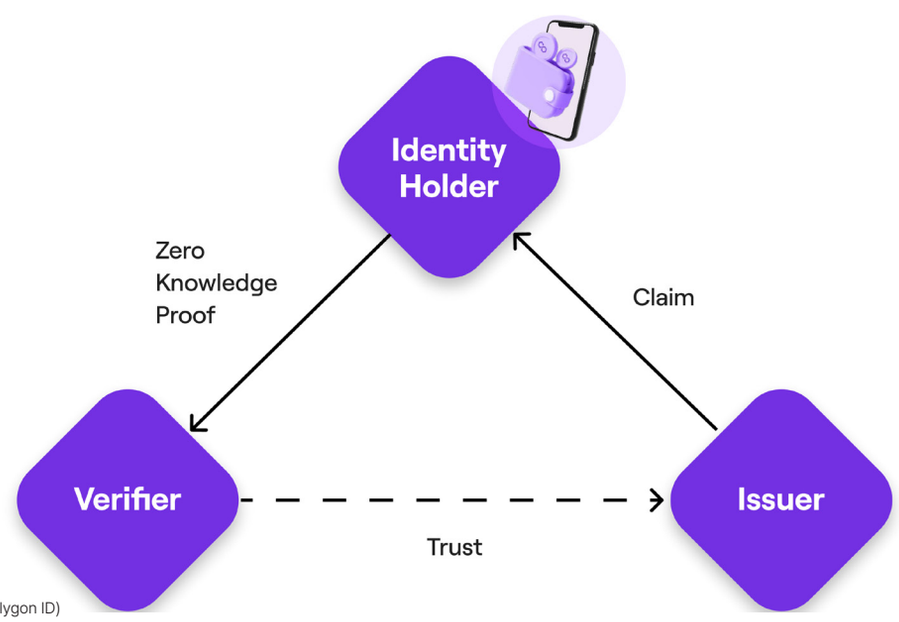
Polygon ID is a Web3 identity protocol that leverages zero-knowledge proofs to protect privacy while providing identity issuance and verification processes. In today's landscape, both offline and online identity checks typically require disclosure of ample personal data. However, with the incorporation of zero-knowledge proofs, one can confirm their identity without revealing specific personal information.

For instance, let's assume you are selling alcohol online. Legally, only customers over the age of 18 should access the website. However, to prove a customer is over 18, they need to verify their actual age and various other pieces of information. In contrast, using Polygon ID, customers can prove they are over 18 using zero-knowledge proofs, without revealing their actual age or other sensitive personal details.

The toolkit provided by Polygon ID is fully compatible with W3C's DID (Decentralized Identifier) standards. It also offers identity verification protocols and identity wallets in the form of SDKs, making it easier for various services to integrate it.

2.5.2 Core Concepts

In Polygon ID, the user's identity is stored in the form of Verifiable Credentials (VC). VC is any type of information related to a person, organization, or thing, from a person's age to a certificate from a specific institution.



(Source: Polygon ID)

A Polygon ID consists of 1) an Identity Holder, 2) an Issuer, and 3) a Verifier.

- **Identity Holder:** A holder who has a VC issued by an Issuer in their wallet. Holders can prove identity by generating a zero-knowledge proof for the VC they hold and sending it to the Verifier.

- **Issuer:** An entity that issues VCs to Identity Holders, and the issued VCs contain the cryptographic signature of the Issuer.

- **Verifier:** The entity that verifies the identity of the Identity Holder. After receiving a zero-knowledge proof corresponding to the VC, it checks that the VC contains the appropriate Issuer's signature, etc.

The key here is that a trust relationship must exist between the verifier and the issuer. This is because identity is all about trust, whether it's institution-driven or a social consensus. If there is an Issuer that issues fake college degree VCs, it is possible to generate a zero-knowledge proof for this VC, but the Verifier should not validate the VC from this Issuer. Therefore, the Verifier needs a trust relationship with the right Issuer in order to validate the VC.

2.5.3 Ecosystem

Polygon ID's diverse ecosystem includes:

Identity Tech Provider - Polygon ID has collaborated with Rarimo to extend the use of VCs to multi-chain, and with Civic to allow anyone with a Civic Pass to seamlessly use Polygon ID.

Issuer - There are currently 14 issuers in the Polygon Identity ecosystem.

SaaS Identity Service - Dock is the provider of the DID service, which makes it easy for developers to issue VCs to the Polygon ecosystem.

System Integrator - Kaleido and Megadev are blockchain platforms for enterprises, making it easy for businesses to integrate Polygon ID.

Trust Network - There are six Trust Network services in the Polygon ID ecosystem, including GateKeeper, Block, Blockchain Lock, and others, which act as middleware between verifiers and issuers.

Verifier - A crypto-payment service called Purple Pay provides KYB-like services by verifying VCs using zero-knowledge proofs.

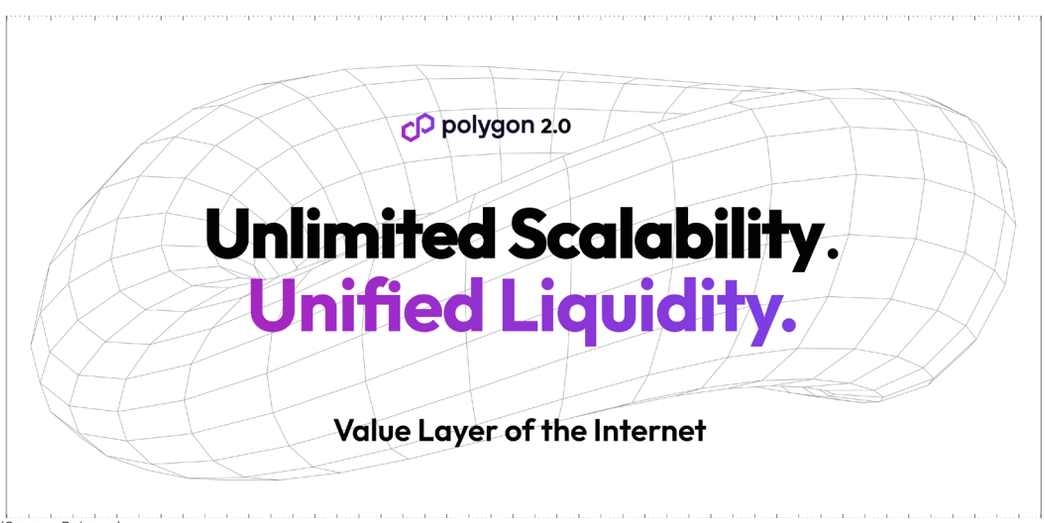
Wallet - Wallet services like Verida, CLV Wallet, WallID, and Altme have integrated Polygon ID's features.

2.5.4 Thoughts on Polygon ID

As IT technology advances globally, humanity is increasingly transitioning into a digital world. In the physical world, the existence of a person's entity makes identity verification relatively straightforward. However, in the digital realm, proving one's identity is a pressing issue. With the anticipated acceleration of AI technology, the digital world will be saturated with AI and content generated by AI, making online identity verification even more essential.

Online identity verification carries the significant concern of personal information leaks. Users of Polygon ID can securely store their identity in the form of VC in their private wallets. A significant advantage is that, during the verification process, zero-knowledge proofs make it impossible to leak personal information. Moreover, since Polygon ID adheres to W3C's DID standards and even provides SDKs for easy integration, it is expected to be widely adopted in various applications.

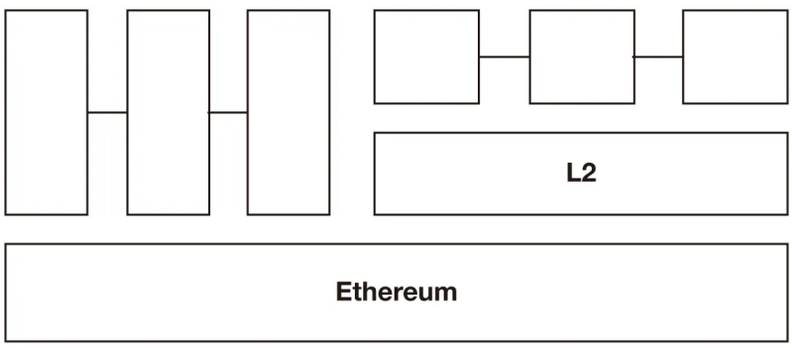
3. Polygon 2.0



(Source: Polygon)

3.1 Overview

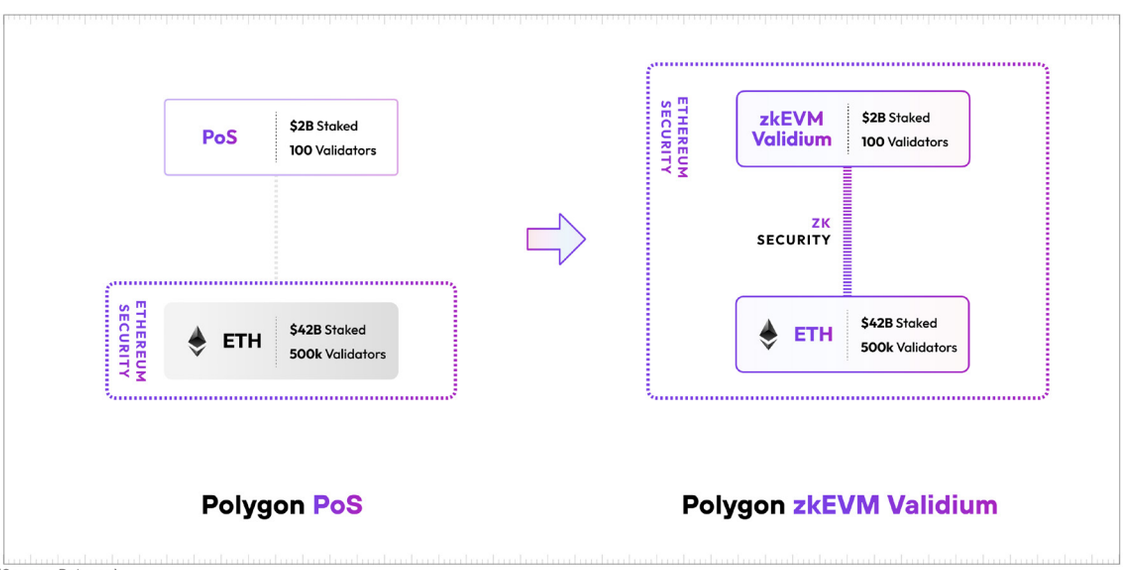
Despite successfully developing and operating numerous products to date, from Polygon PoS to zkEVM, Supernets, Miden, ID, and more, Polygon unveiled a new roadmap called Polygon 2.0 in July 2023. Polygon 2.0 aims to achieve mass adoption of blockchain by evolving it into the value layer of the internet.



Vertical + Horizontal Scalability

Polygon 2.0 is a network comprising numerous ZK L2 chains. Vertically, it benefits from Ethereum's security, and horizontally, by having multiple ZK L2 chains, it can achieve infinite scalability. The dual strategy of enhancing scalability both vertically and horizontally is similar to the objectives of rollup networks such as Optimism (OP-Stack), Arbitrum (Orbit), zk-Sync (ZK Stack), and Taiko (Inception Layer).

3.2 Polygon PoS → Validium



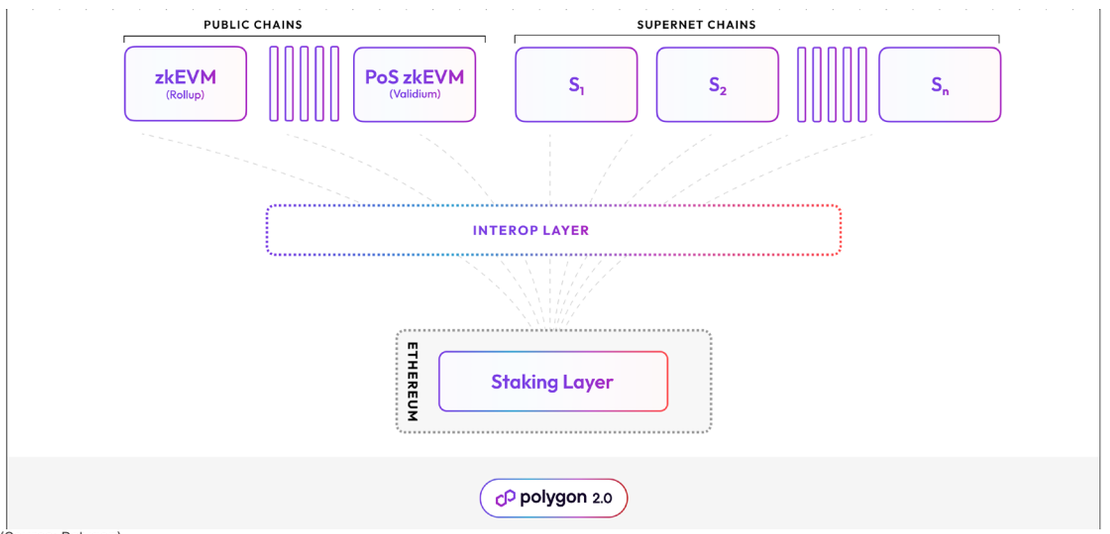
(Source: Polygon)

Polygon 2.0 has unveiled a proposal to upgrade Polygon PoS to validium as a first step towards achieving a network of ZK L2 chains. While Polygon PoS records checkpoints of the network state on the Ethereum network periodically, it doesn't have a fraud proof system, meaning it can't truly be said to rely on Ethereum's security.

Validium is an scalability solution that verifies the validity of computations on the base layer using validity proofs, but stores transaction data off-chain instead of on the base

layer. If Polygon PoS transitions to validium, it could achieve higher scalability than rollups by relying on the Ethereum network for computational validity while having transaction data managed by Polygon 2.0 validators.

3.3 Polygon 2.0 Architecture



(Source: Polygon)

According to the roadmap, the architecture of the Polygon 2.0 ecosystem will consist of four layers:

- **Staking Layer:** This is responsible for all matters related to Polygon 2.0 validators. Fundamentally, Polygon 2.0 validators undertake various roles such as sequencing transactions, generating ZKP (proving), ensuring transaction data availability, and can also participate as validators for multiple ZK L2 chains within the Polygon ecosystem.

- **Interop Layer:** This layer is responsible for interoperability in the Polygon 2.0 ecosystem. For instance, when sending a message from Polygon chain A to another Polygon chain B, a ZKP regarding the message from A is sent to the Interop Layer. Then, chain B processes it optimistically, with the ZKP being later verified on the Ethereum network. As all Polygon chains within the Polygon 2.0 ecosystem are securely and quickly connected through the Interop Layer, they can experience unified liquidity.

- **Execution Layer:** This encompasses the execution layers of the Polygon 2.0 ecosystem, including public chains such as the Polygon PoS validium and Polygon zkEVM, as well as various Polygon chains created via Polygon Supernets.

- **Proving Layer:** This layer has the role of generating zero-knowledge proofs within the Polygon 2.0 ecosystem. The prover being utilized is Plonky2, developed by the Polygon team.

3.4 $POL Tokenomics

The Polygon 2.0 roadmap includes a proposal to upgrade the existing MATIC token to a new POL token. The distinctions between the two tokenomics are as follows:

Inflation: While the total supply of the original MATIC was fixed at 10 billion, the POL token introduces a 2% inflation annually over a period of 10 years. Of this, 1% is intended for validator rewards, and the remaining 1% is designated for ecosystem support.

Community Treasury: A treasury dedicated to supporting the ecosystem is newly established and will be managed through governance.

3.5 Governance

In Polygon 2.0, the influence of governance is expected to expand significantly, focusing on three major governance sectors:

- **Protocol Governance:** This refers to decentralized governance related to the maintenance and development of the Polygon tech stack. It will be managed through the Polygon Improvement Proposal (PIP) framework.

- **System Smart Contract Governance:** This pertains to governance associated with upgrading smart contracts present on the Ethereum network. Initially, it's set to be managed in a multi-signature format through a select group known as the Ecosystem Council.

- **Community Treasury:** Governance regarding the management of the community treasury for ecosystem support. Initially, it will be overseen by a selected group called the Community Treasury Board. In the future, mechanisms like quadratic token voting are expected to be introduced, allowing a broader community to participate in its management.

3.6 Thoughts on Polygon 2.0 Roadmap

Solving the blockchain trilemma is crucial for the mass adoption of blockchain. Within the Polygon 2.0 ecosystem, numerous Polygon chains utilize zk technology. This allows them to depend on Ethereum's security while communicating seamlessly with each other, offering a user experience similar to a single network with infinite scalability.

From a tokenomics perspective, the introduction of inflation could dilute the token's value, which is a downside. However, the low 2% annual inflation rate presents an advantage by potentially fostering the network's long-term growth. It remains to be seen if the Polygon 2.0 ecosystem can effectively build its network effect over a minimum of 10 years.

4. Real Business Examples in Polygon Ecosystem

The Polygon network is currently being utilized and onboarded by a more diverse range of companies than any other network. How was the Polygon network able to secure such a dominant position in the business sector? There are many reasons why companies choose the Polygon network when integrating blockchain:

Scalability - The low fees and fast network speed of the Polygon PoS network make it easier for companies to implement business logic. Currently, the Polygon zkEVM network has also been launched, and according to the Polygon 2.0 roadmap, Polygon PoS will transition to validium mode, further enhancing scalability.

Variety of Solutions - Polygon offers a plethora of solutions, from Polygon PoS to zkEVM, Miden, Supernets, ID, etc. Companies can choose the right solution for their business needs.

Eco-friendly - Using a proof-of-stake system, the energy consumption is very low, making it environmentally friendly and suitable for ESG companies.

Ethereum Ecosystem - While it's currently hard to say that Polygon PoS is relying on Ethereum's security, Polygon zkEVM is a rollup network that does. With the transition of Polygon PoS to validium mode, all of Polygon's products are focused on expanding the Ethereum ecosystem. Ethereum's network, being the most secure and having the broadest ecosystem among smart contract networks, offers safety for companies.

User Base - Though the Polygon PoS network ranks 5th in TVL, it has an average of 400,000 daily active addresses and records over 2 million daily transactions. Excluding Ethereum, it's a network with higher activity than any other, making it ideal for businesses to tap into the established network effect.

Business Development - Polygon has already collaborated successfully with various companies. This provides many precedents for other companies considering the Polygon network.

Now, let's explore how governments, institutions, and businesses are actually using Polygon through various examples.

4.1 Finance

Given that the essence of blockchain is finance, the Polygon network is being utilized in various sectors related to real-life financial aspects, not just in DeFi. The most representative example is the tokenization of Real-World Assets (RWA). Tokenizing RWA on the blockchain offers numerous benefits: it can be managed transparently, operates 24/7, reduces management fees, and opens up traditionally closed markets to many

investors regardless of borders and the size of their funds.

Franklin Templeton, with an AUM (Assets Under Management) reaching $1.5T, has tokenized the Franklin OnChain U.S. Government Money Fund (FOBXX). Hamilton Lane, an alternative investment firm in the US with an AUM of $818B, has tokenized various investment funds and offers them on a platform called Securitize.

In addition, the Polygon network is used in various areas from a financial perspective:

- Nubank, the largest neo-bank service based in Brazil in Latin America, plans to utilize Polygon Supernets to build its own network for a loyalty program.

- Clearpool is an institutional-level lending protocol that offers unsecured loans based on credit to companies. Various firms, including Amber, Wintermute, Auros, and LedgerPrime, have used Clearpool.

- Robinhood, a fintech company in the US, supports the Polygon PoS network in its crypto wallet.

- Gnosis is an L1 network project. Recently, they unveiled the Gnosis Card, which allows for direct payments on the Gnosis Pay L2 network based on a Visa card. The Gnosis Card was designed based on the Polygon zkEVM technology stack.

- Ripio is Argentina's leading digital asset platform with 7 million users. It supports the Polygon network in its Ripio Trade, Ripio Portal, and Ripio Wallet services.

- Stripe provides an option for USDC on the Polygon PoS network when paying out to online creators, sellers, and the like.

4.2 Public Sector

The Polygon network is also frequently utilized in the public sector, including governments and public agencies. A prime example is the experimentation of blockchain adoption led by government-affiliated financial institutions. The Monetary Authority of Singapore (MAS) collaborated with JPMorgan, DBS Bank, and SBI Digital Asset Holdings to facilitate the trading of the Singapore dollar and the Japanese yen using a modified version of Aave Arc on the Polygon Network. Moreover, the central bank of Italy recently announced its collaboration with Polygon Labs for a securities token DeFi ecosystem project intended for institutions.

It's not just national governments; many local authorities also use the Polygon network:

- The southern Swiss city, Lugano, aspires to become the blockchain capital of

Europe. It is allowing its citizens to utilize Bitcoin, Tether, and a local stable coin on the Polygon network called LVGA for taxes, public services, and tuition fees, among other things.

- The regional government of Uttarakhand in India uses the SettleMint platform, which employs Polygon Edge technology, to store and track medical equipment across seven medical colleges.

- The northern Indian state of Uttar Pradesh has decided to adopt the Polygon blockchain to address issues arising from police corruption, ensuring transparency.

- The India International Road Federation uses the SettleMint platform, based on Polygon Edge technology, for road management aimed at reducing traffic accidents in India.

- The state government of Maharashtra uses the Polygon network to record and track caste certificates and COVID-19 test results.

- West Bengal's New Town Kolkata Development Authority has partnered with the Rollup-as-a-Service project Airchains to deploy a service through Polygon Supernets that manages land ownership by tokenizing it as NFTs.

4.3 Gaming

The gaming sector is one of the core applications that can enable the mass adoption of Web3, and it can be argued that the Polygon ecosystem is among the best equipped in the current blockchain networks for gaming. While various blockchain-native P2E (Play-to-Earn) games already exist, a significant number of existing Web2 game studios are also onboarding onto the Polygon ecosystem.

Many gaming companies choose the Polygon PoS network because of its high scalability based on the Ethereum ecosystem and the network's robust user base. Furthermore, if they don't want to deploy their game service as a dApp on the public network but wish to build their ecosystem, they can develop a network specialized to their gaming service using Polygon Supernets.

Prominent games utilizing Polygon PoS include Web3 metaverse games like The Sandbox and Decentral Games' Ice Poker. Numerous game studios from South Korea, a powerhouse in gaming, have also onboarded to Polygon. For instance, Neowiz operates the Intella X game platform, and 4:33's Delabs Games plans to release various games, including Rumble Racing Star, Space Frontier, and Meta Bolts.

There are also gaming services that, instead of onboarding to the Polygon PoS network,

utilize Polygon's tech stack to build their ecosystem. Nexon, the largest gaming company in Korea, is leveraging one of its most successful IPs, Maple Story, to develop Maple Story N through Polygon Supernets. Known for its game-specific blockchain, Immutable X recently collaborated with Polygon Lab to introduce Immutable zkEVM, utilizing the Polygon zkEVM tech stack. The Immutable zkEVM is currently in testnet, and the integration of Immutable's platform with zkEVM technology promises to construct a vibrant ecosystem.

Until now, many gaming services have utilized the Polygon PoS network. However, given the significance of establishing unique economic systems in games, many gaming companies would prefer to operate their network rather than onboard their services as dApps on public networks. If they operate their network in the form of L1, they face challenges like liquidity, user fragmentation, and the burden of network infrastructure operations. However, operating a gaming service as an L2 based on Ethereum can address these challenges. Therefore, as the zk-related technology and ecosystem within the Polygon framework mature, it is expected that more gaming companies will utilize Polygon zkEVM and Polygon Supernets.

4.4 NFT

NFTs, tokens that can verify the ownership of a digital file through the blockchain, are one of the easiest technologies for traditional Web2 companies interested in the blockchain to adopt. Polygon's products boast high scalability, eco-friendliness, and high EVM compatibility, making it easier for developers to start and therefore suitable for Web2 companies to begin their NFT business. Due to these advantages, Polygon has been utilized in Mastercard and Warner Music's accelerator programs and was also selected for the Disney 2022 accelerator program, which focuses on metaverse, AI, and AR.

There are countless ways Web2 companies can utilize NFTs. Firstly, the easiest method is to issue commemorative NFTs. An example of this is when Adidas Originals collaborated with Prada to issue a commemorative NFT named Adidas: Prada, re-source on the Polygon PoS network.

The second method is to use NFTs in the form of digital collectibles and operate an NFT marketplace. Draftkings, Reddit, and Bollywood are some entities that have adopted NFTs in this manner. Reddit, as one of the world's largest community sites, introduced avatar NFTs that can represent user accounts. Despite the current unfavorable market situation in the cryptocurrency market and over a year since its release, metrics related to Reddit avatar NFTs have remained positive. With approximately 17 million users now

holding these avatar NFTs, this has become one of the most successful cases of a business utilizing the Polygon network.

The third approach is to incorporate NFTs into loyalty programs. Since an NFT is an asset held by a user, leveraging it effectively can further entrench both new and existing users into a company's services.

- Dot Swoosh is Nike's Web3 fashion platform, aiming to become a hub for virtual clothing that metaverse avatars can wear. Within the platform, there's a royalty program with real-life benefits, and an economy centered around virtual clothing creators.

- Starbucks has launched a Web3 loyalty program called Starbucks Odyssey on the Polygon PoS. Users can earn an NFT called Journey Stamp and points by completing missions. Examples of missions include visiting a store, buying coffee beans, or using reusable cups, all designed to encourage repetitive visits to Starbucks. A key feature of Starbucks Odyssey is that it abstracts or hides blockchain-related concepts so that customers may not even realize they are using blockchain services. It even allows NFT purchases with credit cards, without needing a cryptocurrency wallet. This NFT-centric Web3 loyalty platform is very effective for retention and marketing.

- Flipkart, India's largest e-commerce company, plans to provide a Web3 experience to its users with a loyalty platform named Hang.

- Salesforce, the world's largest CRM (Customer Relationship Management) software company, offers an NFT-based loyalty program in partnership with Polygon.

- Lotte Group, one of the top five conglomerates in South Korea, has tokenized its Bellygom character into NFTs for use in its loyalty program. Users can enjoy various community activities through the Bellygom NFT and purchase services like actual tickets and food and beverages with the points they earn.

Regardless of the type of NFT business, for a successful NFT enterprise targeting the general public, user lock-in and experience are crucial. Unlike traditional loyalty programs, NFTs offer numerous mechanisms to grant ownership to users. Therefore, it's essential to capitalize on this and encourage users to feel attached to the service. However, this is only possible when the Web3 platform provides a good user experience. If the introduction of blockchain degrades the user experience, it can have the opposite effect.

In this regard, Starbucks, Reddit, and Dot Swoosh are examples of successful NFT businesses through Polygon. All these services are designed so that even users with no

knowledge or experience with blockchain can easily use them. Through well-designed loyalty programs, they can lock in users more effectively than traditional Web2 services.

In the future, as more successful business cases utilizing NFTs emerge within the Polygon ecosystem, many companies are expected to embark on NFT-based loyalty programs built on Polygon.

4.5 IT

Polygon is also actively collaborating with various tech companies. Opera's Crypto Browser and Adobe's creator community Behance have adopted Polygon PoS, while SK Telecom, South Korea's largest telecommunications company, supports Polygon PoS in its NFT marketplace and upcoming crypto wallet. Not only in software but we can also see collaborations with hardware companies, with smartphone manufacturer Nothing being a prime example. After conducting an NFT loyalty program on Polygon PoS, Nothing reportedly plans to integrate Polygon's products into its smartphone operating system, Nothing OS, in the future.

5. Final Thoughts

In this report, we have taken a comprehensive look at Polygon's various solutions, the Polygon 2.0 roadmap, and actual business cases. Based on its strong user base and network activity, Polygon has been able to offer various solutions, creating a conducive environment for businesses to engage in blockchain ventures. For simple businesses, such as tokenizing tangible assets or loyalty programs using NFTs, one can consider using Polygon PoS. If there's a need to build an ecosystem from scratch or when high technical security and scalability are required, one might look into Polygon Supernets and the Polygon zkEVM technology stack. For identity services, the Polygon ID can be considered.

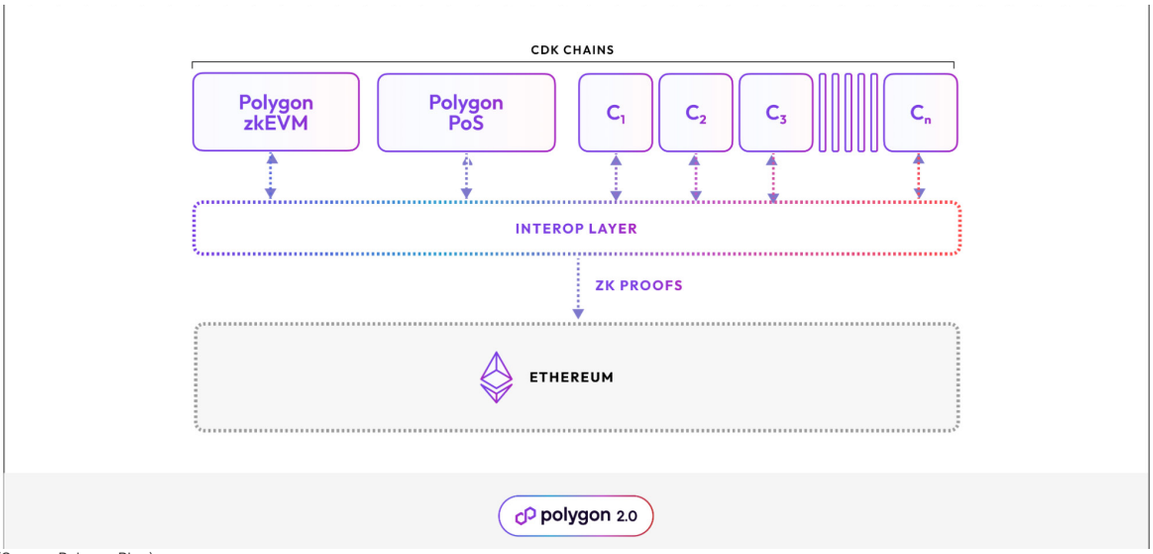
Most blockchain networks usually prioritize either technical expertise or business strategies, with few excelling in both areas. Yet, Polygon has demonstrated that with the right technical and financial backing, balancing both is attainable. Despite its success, Polygon still has several challenges to address.

A short-term challenge is the transition of Polygon PoS to validium. This update aligns with the direction of enhancing Ethereum's scalability. However, transitioning an already well-established network's runtime environment to zkEVM is expected to present technical challenges. Of course, the Polygon team is fully aware of these challenges and plans to upgrade over a sufficient timeframe (expected in Q1 2024). Given their proven expertise in zkEVM through the development of Polygon zkEVM, a successful transition is anticipated. Once Polygon PoS transitions to validium, it can achieve higher security, decentralization, and scalability. This will be compatible with the Polygon 2.0 ecosystem, leading to even more business opportunities.

A long-term challenge is sustainability. This concern applies to almost every network except Ethereum. For a blockchain network to be sustainable, it needs to generate transaction fee revenues that surpass the rewards given to miners and validators. For highly scalable networks that offer low fees, surpassing block rewards isn't easy. Polygon aims to address this issue through an ecosystem of numerous L2 networks. If many L1 and L2 networks are developed and successfully operated via Polygon Supernets, a significant increase in transaction fee revenue is expected.

The journey of the Polygon ecosystem is just beginning. Even now, it offers a favorable environment for businesses, but as the Polygon 2.0 upgrade is implemented, and as zk technology and the ecosystem mature, we should watch out for what new forms of businesses become feasible.

Appendix - Polygon CDK



(Source: Polygon Blog)

Polygon CDK (Chain Development Kit) is an open-source codebase as an upgraded version of Polygon Supernets, designed for easy development of ZK L2 networks. CDK Chains connect to the Interop Layer, allowing them to achieve interoperability with other CDK Chains using ZKP, providing a unified liquidity experience within the Polygon 2.0 ecosystem.

With the Polygon CDK, various components can be customized:

- **Mode:** Rollup, Validium
- **Virtual Machine:** zkEVM, Miden VM, ...
- **Data availability:** Ethereum, DAC, ...
- **Fee token:** ETH, Custom
- **Sequencer:** Centralized, Decentralized (WIP)
- **Whitelist:** Permissionless, Permissioned
- **ZKP** submission cycle

The role of Polygon Supernets in Polygon 2.0, which was previously ambiguous, has become much clearer with the introduction of the Polygon CDK. One of the biggest drawbacks of the app-chain ecosystem is the fragmentation of liquidity. In Polygon 2.0, the use of a ZKP-based cross-chain solution means that even with many ZK L2 networks emerging through Polygon CDK, there won't be any fragmentation of liquidity. Recently, many rollup projects have released their own blockchain development toolkits, but so far, no project other than Polygon CDK has clearly presented a cross-chain solution.