Polygon ID

Polygon ID uses a decentralized identity system to create trusted interactions with Web3 services, it uses a different set of tools used by developers to facilitate trusted and secure relationships between apps and users.
These tools enable developers to use polygon Id to enable the exchange of verifiable credentials secured by cryptography and the blockchain.
They are designed for developers with a strong focus on privacy, decentralization, user data,self-sovereignty and verifiable credentials.
Issued according to the W3C Standards and are signed under cryptography to guarantee tamper-proof.
Mainly performed by issuers that are trusted organizations or companies.
In the real world, this could include your government, university, or bank. In WEB3 this could include KYC providers, Oracles, DAOs, reputation services, etc.
For these issuers, Polygon ID includes the Issuer Node, a self-hosted API capable of creating these credentials.
Credentials are not created in the void. They are created when a user requests them to prove something. The user then has to request, collect, and store the credentials. This is done through an identity wallet. In the same way, a crypto wallet holds your crypto private keys, and an identity wallet holds your identity keys and your credentials.
These credentials are meant to give the users some "power" -the power to prove something about him/herself to the dApp or smartContract(the Verifier of the credentials).
For the Verification part of the process, Polygon ID includes the Verifier SDK and smart contracts for off-chain and on-chain.
These libraries allow the Verifier to compose different queries (questions) without having to deal with the complexities of reconfiguring the underlying cryptocurrency.

Topics that we will cover in this article are _

1. What is Polygon ID?
2. Core concepts of Polygon ID,
3. Why Polygon ID,
4. Polygon ID Wallet App

What is Polygon ID?

Polygon ID, from the creators of Polygon, enables programmable privacy, a way for users to interact with Web3 services that are decentralized, controlled by users, and privacy-focused.

Using their own zkSnark tech to ensure cryptographic protections, Polygon ID achieves a scalable model for permissionless and censorship-resistant digital identities,
Polygon ID is a decentralized and permissionless identity framework for Web2 and Web3 applications. It works on the principles of Sovereign Identity (SSI) and cryptography that lets individuals own and control their identities.

Core concepts of Polygon ID

There are four concepts that should proceed with Polygon ID. This area,

1. Claim
2. Issuer
3. Identity Holder
4. Verifier

Claim
The claim represents any type of information related to an individual, enterprise, or object. For ex- A claim can represent your age or your University Degree.

The person who generates the claim is called the Issuer and he sends this claim to the Holder.

Issuer
An issuer is an entity or an organization that issues claims to the Identity Holder. These claims are cryptographically signed by the Issuer Organization or an entity.

Identity Holder
Identity Holders are the end users like us who hold the claims in their Polygon ID Wallet,

With the help of these claims, the Holder can generate a zero-knowledge proof of the claims in his wallet and present these zero knowledge-proofs to the Verifier.

Verifier
Verifier verifies the proof presented by a Holder. verifier requests the proofs based on the claims that Holder holds in his wallet.
Verifier can add additional checks to see if the holder’s claim satisfies the criteria needed by him. For ex- Verifier can add a check that the Holder has the claim that satisfies >18 age criteria and the claim is issued to the holder by a reputed and trusted issuer.

NOTE: There should exist a trust between the verifier and the Issuer for verifying the claim of the holder because the Claim just resembles the cryptographically verifiable and doesn't guarantee its truth. The Verifier here should see to it that the Claim is coming from a trusted Issuer.

Now there are two types of verifications —

Onchain verification
Off-Chain verification

On-chain Verification allows Dapps to verify users' claims inside a Smart Contract using zero-knowledge proof cryptography.

Off-chain Verification provides all the elements to create a customized Query, set up a verifier server, and generate a QR code on the client side to request proof from the user.

However, The proof generated is the same for both cases; the only difference is in the verification process.

Why Polygon ID

Now we have some overview of Polygon ID, Let's recap through what advantages Polygon ID provides us.

Polygon ID lets people prove their identity without exposing their crucial information to the people. The user's Identity here is secured by zero-knowledge cryptography. Let's discuss some of the advantages that Polygon ID provides —

Privacy Using Zero-Knowledge
As we saw above the Identity Holder without revealing his sensitive information can send cryptographic proof to the verifier with the help of his claim.

An ex-identity holder with the help of the claim given to him from the verified Issuer that he is >18 years of age can get verified from the verifier without actually revealing his age to anyone. This ensures minimum data exposure and hence ensures the safety of any sensitive data.

NOTE: The issuer can't track the claim that is issued to the holder i.e. holder can use that claim anywhere.

On Chain Verification

Verification of Proofs unlike previously that was done off-chain can now be done on-chain with the help of smart contracts.

For ex- Any verifier can allow access to their website to only those identity holders who are >18 years of age and who meet the criteria.

Self-Sovereignty

Self-sovereignty means that the holder is in full control of his/her sharing of data, private keys, etc. There is no Issuer who can track where the claim has been used.

Transitive Trust

Trust here refers to the relation between Issuer and Verifier. The claim issued by Issuer can be used with multiple verifiers but it is important to note here that every verifier accepts the claim issued by the Issuer. For this, it is important to have trust between Issuer and Verifier.

Another trust here refers to between Issuer and Holder. The holder collects the claims from the trusted Issuers then he can have a hassle-free verification at the verifier's end.

Which Tools are Included in Polygon ID?

The Core Polygon ID technology stack is available under an open-source license in a self-service / self-hosted fashion with support for DID and verifiable credentials.

These tools help developers integrate decentralized identity solutions into their applications, provide On-chain verifiable capabilities, and help build the ecosystem of Trust.

The Polygon ID tools are:

- Polygon ID Wallet SDK

Allow builders to create identity wallets or try to incorporate identity solutions into their existing crypto wallet offerings.

- Polygon ID Wallet App

A reference implementation created by a Polygon ID team to help builders understand one way to incorporate the Wallet SDK into their wallets.

- Polygon ID Issuer Node

The Issuer node is where issuers can host themselves to keep in control of their data. It exposes API methods that can be issuers to issue Verifiable Credentials and a User Interface.

- Polygon ID Verifier SDk

Allow developers, for example, dApps, to set verification credentials and construct queries for users.

- Polygon ID JS (Beta Version)

Java Script Libraries to create client applications are browser extensions, which allow users to issue credentials about themselves, store credentials and a key, and then generate proof of having these credentials.

How is Blockchain used in Polygon ID?

There are three main uses of the Blockchain for Polygon ID.

1. Issuing a **Merkle Tree Proof(MTP) signature** to a credential: The Issuer can issue a credential with an MTP that holds information about the Issuer state tree published On-chain.

2. **On-chain Verifiable:** The Verifier can use an On-chain smart contract to verify credentials. In the future, additional uses of blockchain will be built for Polygon ID such as to enable **revocation of credentials,** where the Issuer publishes the revocation tree on-chain so the user (identity Holder) can include the revocation or (non-revocation) information inside the zero-information proof they send to the Verifier.

On Which blockchain can Polygon ID run?

Polygon ID can run on any EVM-compatible chain. At the moment, the necessary smart contracts are deployed onto Polygon Testnet (Mumbai) and Polygon PoS Mainnet, but they could be deployed to any other EVM- EVM-compatible chain.

POLYGON WALLET APP

The Polygon ID Wallet is a Privacy By Default wallet that helps protect a user's identity (and other metadata) by using zero-knowledge proofs. The wallet interacts with an Issuer to fetch claims and with a Verifier for sharing zkProofs based on these claims.

Polygon ID wallet app has the following features —

1. Privacy by Design and Self-sovereignty
2. Open and Permissionless.
3. Fetching, storing, and managing claims.
4. Generating cost-optimized zero-knowledge proofs for claim verification.
5. Communication with Issuer and Verifier.
6. Identity recovery using seed phrases.

However, don’t confuse the Polygon ID wallet app with Metamask or any other crypto wallet because they are used for sending the transactions on the chain whereas Polygon ID Wallet is used for creating and storing unique identities for the wallet so that these identities can be used to authenticate with the Issuer and the Verifier.

INTRODUCING POLYGON ID ZERO-KNOWLEDGE IDENTITY FOR WEB3.

At Polygon, we believe that putting people firmly in control of their digital identities is at the core of Web3's promise to empower users over networks. We have been working behind the scenes to fulfill this promise and today are proud to introduce Polygon ID, the self-sovereign, decentralized, and private identity for the next iteration of the Internet.

What makes this new identity platform unique is that it is the first ever to be powered by zero-knowledge (ZK) cryptography, privacy, and blockchain scaling technology. Polygon has made ZK a centerpiece of its strategic vision and has committed $1 billion to related projects. Polygon ID is the latest product in this rapidly growing portfolio.

POLYGON ID HAS THE FOLLOWING PROPERTIES :

- Blockchain-based ID for decentralized and self-sovereign models
- Zero-knowledge native protocols for ultimate user privacy
- Scalable and private on-chain verification to boost decentralized apps and decentralized finance
- Open to existing standards and ecosystem development
- Polygon ID leverages internal expertise to reduce the complexity that comes with the use of Circom 2.0 to compile zero-knowledge cryptographic constructions known as zkSNARKs circuits.
- Onboarding for developers and partners is done via the ID client toolkit will include native apps, SDK, and white-label solutions.

Polygon ID leverages the Iden3 protocol and Circom ZK toolkit. Moving forward, both of the projects will be sponsored by Polygon while keeping the original spirit of community initiatives to provide open-source protocols and tools to the broader ecosystem of developers.

“Polygon ID is private by default and offers on-chain verification and permissionless attestation. There is nothing in the digital identity space now that ticks all these boxes,” said Mihailo Bjelic, Polygon's co-founder. “It is also a great showcase for how zero-knowledge proofs can help us create a better world.”

For end users: Convenient Privacy for all

Privacy is a fundamental human right and Polygon ID empowers the users to reclaim it. Because it is private by default, access control is based on proving verifiable information rather than sharing it with the verifier.

Most advanced privacy that can still run on a user's device
Right of access to apps with user anonymity
Aligned with Web3 privacy ethos.

For WEB3 Protocols: Advanced and Private On-chain Verification

Polygon ID allows for the construction of new forms of reputations. Some examples include a decentralized credit score for financial primitives and social payments in DeFi; decentralized sybil score, voting power/delegation, and domain-expertise reputation for DAOs to enable new decision-making and governance models; player reputation profile for Web3 games; private and censorship-resistant P2P communication and interactions for social applications.

Identity reputation can be cryptographically verified in a privacy-preserving way directly on-chain to trigger trustless execution/action
No need to rely on a middleman to execute interactions with users
Ability to compose validation by interacting with generic Smart Contracts or NFTs, but with privacy.

For Organization and Businesses: Open Ecosystem For Trust Management

Polygon ID is a complete platform that can be used to construct a variety of identity and trust services. The team is creating an open and enterprise-ready ecosystem for trust markets and trust management to build new attestation and access services with an incentive layer.

dAccess-as-a-Service
An environment where existing solutions can be deployed and new ones created
KYC, KYB, attestation
A distribution channel with a variety of options to leverage emerging cryptosystems.

Polygon ID Developer Use Cases.

Developers can unlock a host of new use cases by leveraging Polygon ID. The applications are as diverse as the Internet itself and range from Proof of Uniqueness and Immediate onboarding to use by Decentralized Autonomous Organizations (DAOs) and Decentralized Finance (DeFi). Here are just some of the possible use cases.

- DAOs: Members often wish to remain anonymous online, while still participating in DAO governance which requires trust and proof of reputation. Using Polygon ID tools, DAOs can verify membership without needing their members to disclose their identity.
- KYC: Identity verification in traditional finance still relies on data-heavy KYC practices and DeFi appears to be moving in the same direction. With Polygon ID, developers can build solutions that allow their end users to prove their eligibility once to receive a KYC

credential, and then re-use that credential for financial and other high-value services without necessarily disclosing their personal information again.

- E-commerce Customer Onboarding: Customers are increasingly using online and mobile payments to purchase goods and services. Polygon ID provides an identity layer for e-commerce customers that can be used to increase payment security while reducing the costs of storing customer and payment data.
- Passwordless Login: Users have, on average, hundreds of passwords that are often insecure and hard to track. Passwordless logins exchange encrypted verifiable credentials by simply scanning a QR code or connecting to a desktop wallet. Organizations can benefit from improved security, a better user experience, and the productivity of their system administrators whose time is not taken up by password resets.
- Undercollateralized Lending: Undercollateralized decentralized lending requires both risk assessment for loan approval and identifiable information in case of default. Current unsecured lending has an off-chain risk assessment and stores identity data. Polygon ID can be used to bring these elements on-chain by coupling the private on-chain credit score to a persistent identity. The identity retrieval system enables minimized data to be shared by being cryptographically secure with embedded access control. Eventually, as fully on-chain identities are created, Polygon ID can provide those same benefits to that on-chain identity.
- Portable Avatars & Reputation: Within a traditional game, a user’s items and achievements can only be used within the game itself. With the rise of in-game asset purchases and the customization of avatars, users can’t take their progress elsewhere. Polygon ID can enable users to store and update digital assets (including avatars and objects), achievements, and progress to be used across different games and across the metaverse.