One Face, One DID, a rapid and privacy-preserving solution to combat bot and sybil attacks.

**Use case summary**

The "One Face, One DID" concept is a powerful tool in the fight against bots and sybil attacks. By requiring users to verify their identity through facial recognition, zkMe ensures that each user has a unique DID. This makes it much more difficult for bad actors to create multiple accounts and manipulate the system. With zkMe, businesses can be confident that their interactions are with real people, and not bots or fake accounts.

**Benefits**

**Build a secure, trusted and high quality community**

* Prevent abusive behavior
* Establish new governance models
* Ensure fair reward systems

**Why choose MeID for Anti-Sybil / Anti-Bot protection?**

* Private-by-Design
* Instant Check
* Recoverable
* Reusable

**How does it work?**

1. Liveness check [zkMe App]
2. Face graph generation [zkMe App]
3. Fully homomorphic encryption [zkMe App]
4. Encrypted face graph cross-check [zkMe Registry]
5. Unique zkMe DID creation [On-Chain]
6. Final report check

**Applications to benefit:**

* Fair airdrops
* Fair NFT mint
* Fair funding
* Fair voting
* Quadratic Funding
* Anti-Spam

zkKYC is a privacy-enhancing technology that allows for secure and private identification verification.

# Use Case Summary

With zkMe's zkKYC solution, institutions can confidently participate in DeFi without compromising their regulatory requirements. zkMe leverages ZKPs and MPC to protect user identity information and ensure KYC compliance. This brings trust and reputation to the DeFi space, creating a more secure and efficient financial system for all.

Permissioned DeFi refers to decentralized finance systems that require permission to access or join. This is in contrast to traditional DeFi systems that allow anyone to participate without needing approval from a centralized authority. Permissioned DeFi is often used by institutions or corporations that want to maintain some level of control over their financial activities on the blockchain.

Permissioned DeFi may require Know Your Customer (KYC) or Know Your Business (KYB) procedures to be completed before granting access to the network. These procedures are used to verify the identity of users and ensure compliance with relevant laws and regulations. They are often implemented to prevent fraud, money laundering, and other illicit activities.

# Overview of Permissioned DeFi Pools using zkMe

### ****Institutional Funds****

Institutions seeking to engage in the DeFi market and generate yields for managed funds can benefit from permissioned DeFi systems. These systems offer enhanced control over blockchain financial activities while retaining access to decentralized finance advantages. By implementing KYC/KYB procedures, institutions can maintain compliance with relevant regulations while capitalizing on yield-generating opportunities in the DeFi market.

### ****Crypto-friendly Banks****

Crypto-friendly banks often facilitate fiat on-ramps and off-ramps for institutions, enabling seamless fund transfers between permissioned DeFi systems and traditional finance. This is particularly vital for institutions needing regular fiat and cryptocurrency conversions to participate in the DeFi market.

### ****Crypto Custodian Service Providers****

Crypto custodian service providers offer secure vaults and management dashboards, assisting institutions in safeguarding their cryptocurrency funds within permissioned DeFi systems. Services such as cold storage, multi-signature wallets, and insurance coverage help protect against theft and fund loss. Notable examples include BitGo, Coinbase Custody, and Anchorage.

### ****Institution-Grade Wallets (Metamask Institution)****

Institution-Grade Wallets such as Metamask Institutional provide enhanced security, operational efficiency, and compliance features tailored to institutional needs. Their integrated KYT framework evaluates transaction risk and flags suspicious activity. Real-time reporting enables prompt network activity monitoring and threat response. Integrating KYT frameworks supports regulatory compliance while interacting with DeFi and Web3.

### ****DeFi Protocols****

Permissioned DeFi protocols enable institutions and corporations to create new liquidity while maintaining blockchain financial activity control. These protocols often mandate Know Your Customer (KYC) or Know Your Business (KYB) procedures for network access. Through these integrations, institutions can ensure regulatory compliance while exploiting yield-generating opportunities in the DeFi market.

### ****zkMe Network****

The zkMe network offers a zero-knowledge proof (ZKP) based KYC solution for retail users and a KYB verification solution for institutions. It generates credentials for counterparties, allowing only whitelisted wallet addresses to participate in permissioned DeFi pools. This grants greater control over blockchain financial activities while retaining decentralized finance benefits, ensuring regulatory compliance and access to yield-generating opportunities.

### ****Retail Investors****

Retail users can also engage in permissioned DeFi pools by supplying liquidity and generating yields. However, they must undergo Know Your Customer (KYC) procedures to participate in the permissioned DeFi system. By providing liquidity, retail users contribute to maintaining balanced, healthy permissioned DeFi pools.

# What zkMe can do for permissioned DeFi

## Issue KYB credentials on-chain

* Proof-of-KYB status

## zkKYC for Retail Users

* Liveness check
* Uniqueness check
* Citizenship check
* Residence check
* Proof-of-Funds
* PEP
* Sanction list check

## KYT

* On-going transaction monitoring

# Why choose zkMe zkKYC solution?

* Private-by-Design
* Decentralized
* Fulfill compliance requirement
* Reusable zkKYC
* Full security
* Seamless integration

## How does it work?

1. zkMe App / popup
2. Facial recognition / document OCR
3. Raw document file threshold encryption
4. ZKP generation
5. SBT minting
6. SBT Verification
7. zkKYC

Web Data Attestations - Connecting web2 Identities to blockchains

# Use case summary

zkMe's identity oracle enables users to bring their personal data (e.g. credit scores, social network statuses) to the chain. Web3 protocols can then use this data to create tailored features that meet users' needs and preferences. For instance, a DeFi protocol can determine loan eligibility based on credit scores, while a social network can recommend content based on social network status. With zkMe's identity oracle, a more personalized and efficient digital world is made possible for each user.

## Benefits

**Build a more secure and trustworthy protocol**

### Trusted Identity Data

* Creates more possibilities for protocols
* Computational trust / reputation for people-powered networks: identity attributes can be expressed as claims (or attestations) which can be combined to create compound proofs.

### Protect User Privacy

* 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 middle man to execute interactions with users
* Ability to compose validation by interacting with generic Smart Contracts or NFTs, but with privacy

# What data feeds does zkMe bridge to blockchain?

| **Demographic data** | **Personal data** | **Web2 data** | **Web3 data** |
| --- | --- | --- | --- |
| Name | Education | Social media |  |
| (twiter, reddit, discord, facebook, github, youtube) | Transaction history |  |  |
| Age | Occupation | Web indexes | Smart contract activity |
| Ethnicity | Income | Browsing history | POAP |
| Gender | Credit score | Online purchases | DAO voting history |
| Citizenship | Social security number | Communication patterns | Asset/NFT ownership |
|  | Biometric data | Web2 platform achievement |  |
|  | Phone numbers | Gaming status |  |
|  | Email addresses | Membership status |  |
|  | Physical addresses |  |  |
|  | Employment history |  |  |
|  | Professional certifications |  |  |
|  | Medical history |  |  |

# Why choose zkMe Identity Oracle?

* **Private-by-Design**
* **Reliable**
* **Multi-chain**

As blockchain-agnostic infrastructure, zkMe identity oracle supports any and all blockchain networks, updating at the native speed and cost of each chain

Standardized interface for smart contracts to send messages to any blockchain network. With a single method call, developers can communicate across any blockchain.

* **Seamless connection to any API**

Build on a flexible framework that can retrieve data from any API, connect with existing systems, and integrate with any current or future blockchain.

* **Scalability**

# How does it work?

1. Data feed API
2. TLS (1.2 & 1.3)
3. MPC
4. ZKP
5. SBT
6. zk-Bridge
7. Smart Contract

# zkMe Web Data Attestation Use Cases

### zkCredit Score

* zkMe Identity Oracle can be used to develop a credit scoring system for decentralized finance (DeFi) applications. This system could allow individuals to obtain credit loans without the need for traditional credit checks or collateral.

### zkIdentity Social Network

* zkMe Identity Oracle can enable trustless interactions between users, as no party needs to rely on a central authority to verify the other's claims. This promotes a more secure and decentralized environment.

### zkIdentity DAO Management

* zkMe Identity Oracle can allow DAO members to cast their votes without revealing their identity or choice, maintaining the privacy of voters while still ensuring the integrity of the voting process. This can lead to more honest and unbiased voting outcomes.
* zkMe Identity Oracle enable domain-expertise reputation systems in DAOs. Members can prove their expertise in a particular domain (e.g., development, finance, legal, etc.) without revealing their full identity.
* DAOs can implement merit-based governance models, where members with proven expertise in specific areas have more influence over decision-making.

### zkGaming Status

* **Privacy-Preserving Gaming Status:** zkMe Identity Oracle can enable players to prove their gaming status, such as level, achievements, or rank, without revealing their identity or additional information. This protects player privacy and ensures that sensitive data remains secure while interacting with in-game economies or other players.
* **Secure Asset Ownership:** zkMe Identity Oracle can be used to establish the ownership of in-game assets, like non-fungible tokens (NFTs), without exposing the owner's identity. Players can prove they own specific assets without revealing their account details, thus maintaining privacy and reducing the risk of targeted attacks or theft.
* **Trustless Trading and Marketplace:** zkMe gaming status can facilitate trustless trading of in-game assets and currencies in decentralized marketplaces. Buyers and sellers can prove the authenticity and ownership of assets without revealing their identity, enabling secure and private transactions.
* **Skill-Based Earnings:** In GameFi platforms that reward players based on their skills or achievements, zkMe Identity Oracle can help verify players' gaming status without compromising their privacy. Players can prove they have reached certain milestones or possess specific skills to access rewards and opportunities, all while keeping their personal information secure.
* **Fair Play and Anti-Cheat Mechanisms:** zkMe gaming status can help ensure fair play by allowing players to prove their accomplishments without revealing their strategies or gameplay data. This can be used to implement anti-cheat mechanisms that maintain the integrity of the gaming experience without compromising privacy.
* **Cross-Game Interoperability:** zkMe gaming status can enable players to prove their achievements and assets across multiple games within the GameFi ecosystem. This promotes interoperability and encourages the development of interconnected gaming experiences where players can leverage their accomplishments and assets from one game to another.