Designing a Gasless Swap Experience

Álvaro Martín | ERC-4337 & EIP-7702

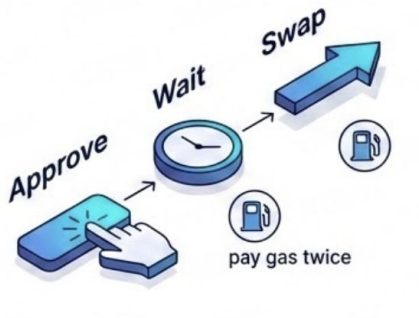
The Problem: The Current DeFi Barrier

Native Token Dependency

Users holding stablecoins are blocked from trading due to a lack of native "fuel" (ETH)

User are forced to onboard fiat, go to a CEX or a DEX just to pay fees.

Current Swap Flow



The "two step dance" of Approval + Swap

Approve -> Wait -> Swap (pay gas twice)

User has USDC but not enough gas (ETH)

Insufficient Gas Friction

High Cognitive Load: fee settings, failures, retries

Insufficient ETH for Gas

The Technical Solution Stack

Core Philosophy

Move complexity from the User to the Infrastructure.

The Toolkit

ERC-4337: Standardizes Bundlers & Paymasters.

EIP-7702: The bridge for existing users.

Target UX

One-Click like a CEX

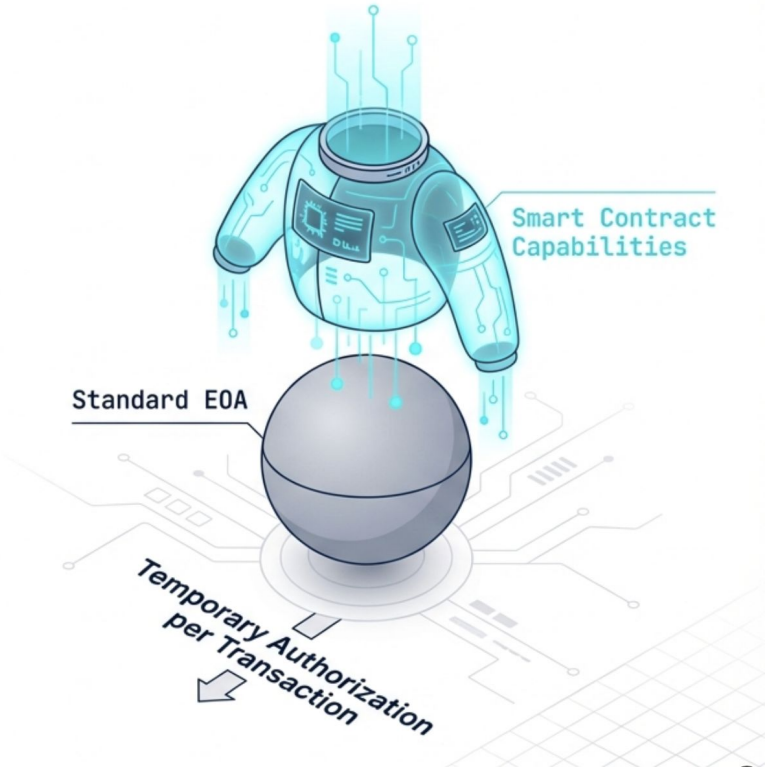
Without taking Custody and Privacy

Is this Solution Valid for all Metamask Users?

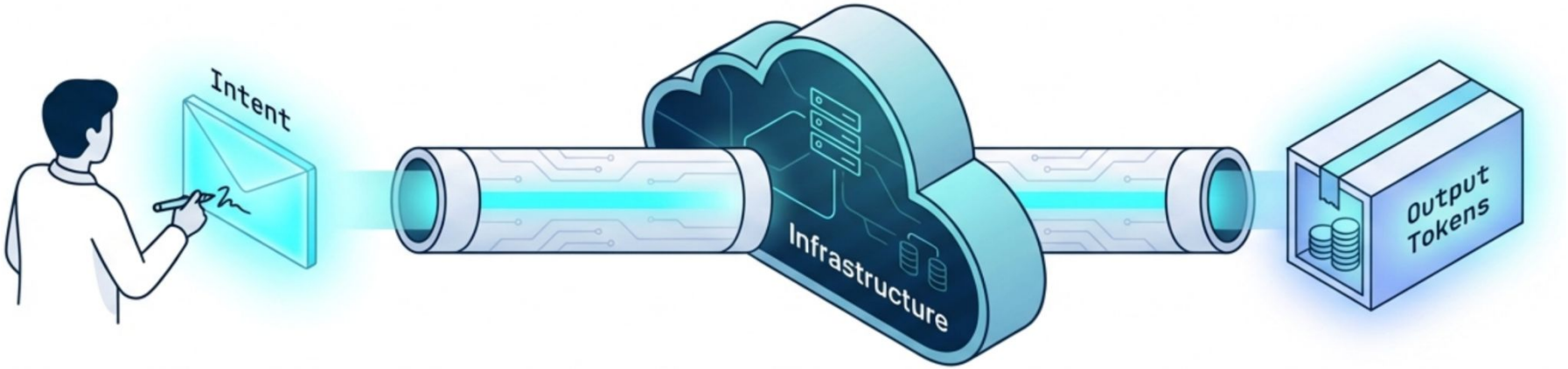
The Problem
ERC-4337 requires deploying new smart contract wallets, creating friction for millions of existing users with EOAs (Externally Owned Accounts).

The Fix (EIP-7702)
Allows an EOA to temporarily "authorize" code execution during a transaction. This enables a standard MetaMask account to utilize Paymasters and Bundlers for a single transaction without a permanent migration.

Impact
Instant gasless accessibility for the entire existing user base.



Moving from Transactions to Intents



One-Click Signature

The user signs an off-chain message (Intent) authorizing the swap of X token for Y token.
This signature costs zero gas to create.

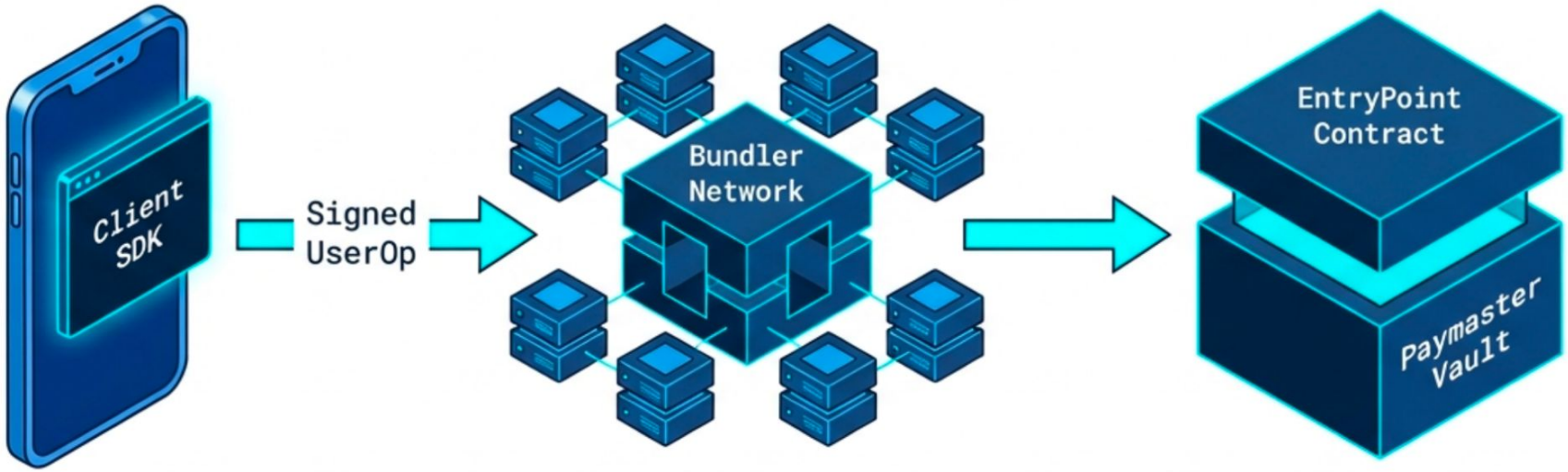
Gas Abstraction

The complexity of gas payment is shifted from the user to the infrastructure layer. The user technically pays in the input token (via spread), but the experience feels 'free'.

Self-Custody

Non-custodial at all times. Private keys remain with the user; Privacy remains king and the protocol never holds funds, only authorization.

High Level Architecture



User Layer

Generates the Intent
Signs EIP-712 Message.

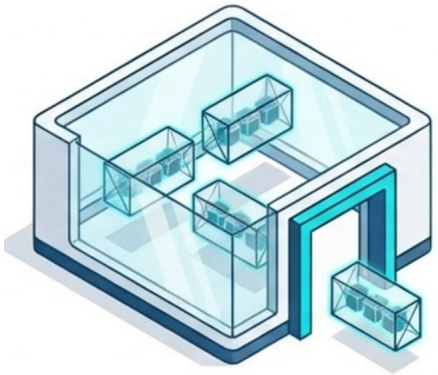
Infra Layer

Bundlers (Relayers)
Listens for Intents.
Packages UserOps.
Pays Initial ETH.

On-Chain Settlement

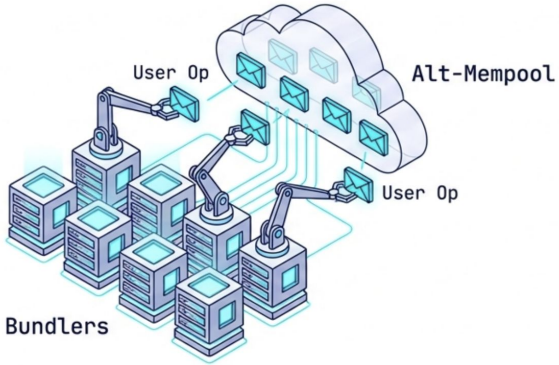
Paymaster - Vault
Validates Signature.
Sponsors Gas.
Executes Swap.

The Bundler & Alt-Mempool | ERC-4337 Account Abstraction



Alt-Mempool

"alternative memory pool" stores pending UserOperations.



Decentralization

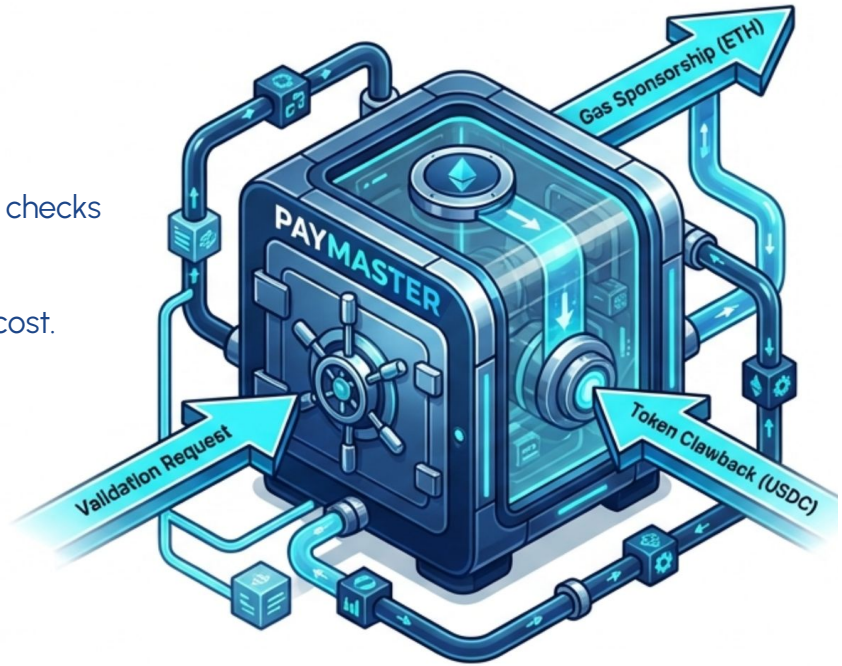
Unlike a single relayer server, an open Bundler network prevents censorship. If one Bundler ignores a user's intent, another can pick it up to claim the fee.

The Courier

Bundlers act as the bridge. They bundle multiple UserOps into a single transaction, paying the gas fee in ETH upfront to the validators.

The Financier: The Paymaster contract

1. Validation. The Paymaster checks if the user has enough USDC collateral to cover the swap cost.



2. Execution. The Paymaster releases ETH to the EntryPoint to compensate the Bundler.

3. Reimbursement. Post-swap, the Paymaster withdraws the equivalent gas value + fee from the user's new token balance.

The Paymaster: On-Chain Gas Sponsorship

Function

The Paymaster is a smart contract holding an ETH reserve. Its primary job is to validate that the user has sufficient USDC assets to cover the swap + fees before releasing ETH for gas.

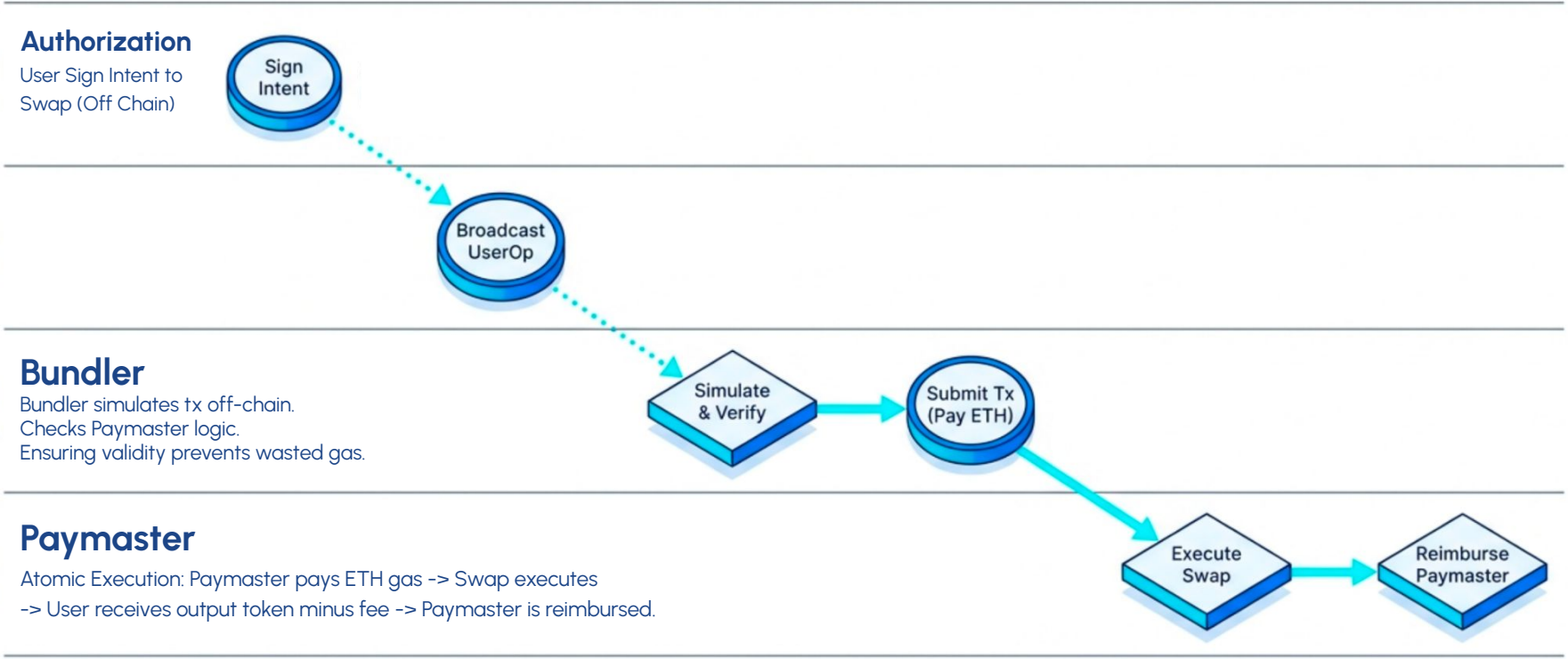
Mechanism

It uses the 'validatePaymasterUserOp* function to gatekeep the ETH treasury.

```
function validatePaymasterUserOp(
    UserOperation calldata userOp,
    bytes32 userOpHash,
    uint256 maxCost
) external view returns (bytes memory context, uint256 validationData) {

    // 1. Calculate required token amount based on current gas price
    uint256 gasPrice = userOp.maxFeePerGas;
    uint256 tokenCost = (maxCost * gasPrice) * EXCHANGE_RATE_PREMIUM;

    // 2. Verify user has enough stablecoin balance
    if (tokenContract.balanceOf(userOp.sender) < tokenCost) {
        revert InsufficientBalance();
    }

    // 3. Return context for postOp execution
    return (abi.encode(userOp.sender, tokenCost), 0);
}
```

Pseudocode logic ensuring protocol solvency before gas sponsorship is approved.

Execution Sequence: From Sign to Settlement

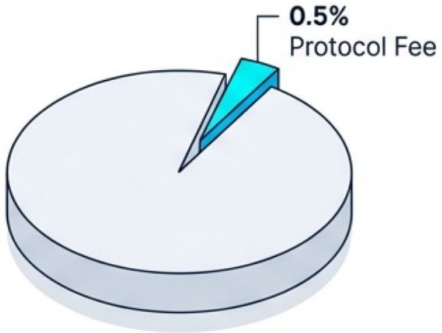


Unit Economics & Monetization Strategy

Cost Driver: L2 Necessity

Mainnet gas fees render retail gasless swaps insolvent. Deployment targets are strictly L2s (Arbitrum, Optimism, Base) or high-value Mainnet trades only.

Revenue Lever: Spread



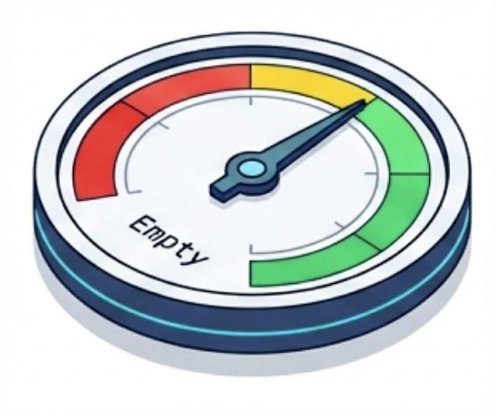
The protocol quotes a price marginally above market. This 'spread' covers the gas reimbursement + a small profit margin to refill the Paymaster reserves.

Selling the Order Flow

MEV-driven solvers (or bundlers) bid to fill the intent. The winning solver pays the gas in exchange for the arbitrage opportunity.

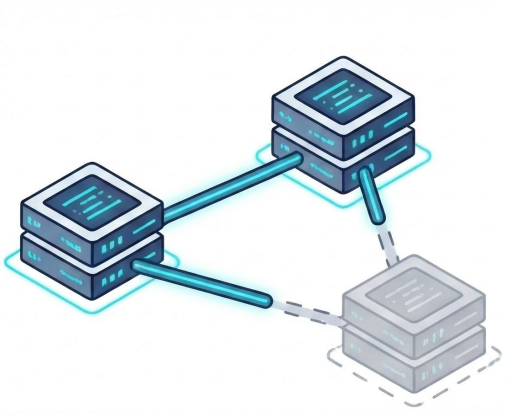
Operational Resilience & Security

Solvency Monitoring



Paymaster Auto-Refill
Automated off-chain scripts monitor ETH balances. Alerts trigger treasury transfers when reserves dip below 20% to prevent service denial.

Bundler Uptime



Redundancy
Avoid reliance on a single relayer. Use a decentralized P2P Bundler Network to ensure UserOps are picked up even if specific nodes fail.

Paymaster DDoS Protection

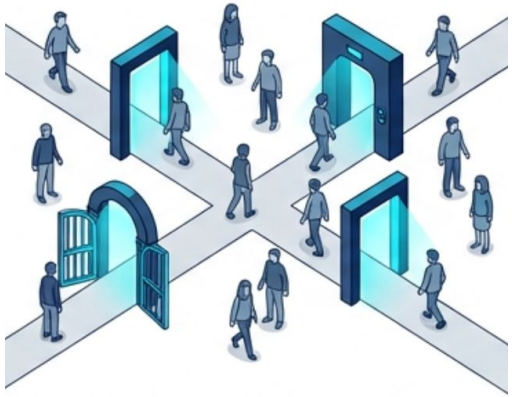
Rate Limiting
Restrict gasless requests per IP/Wallet address. Prevents attackers from draining Paymaster funds via spam simulations.

Decentralization & Censorship Resistance

The Risk

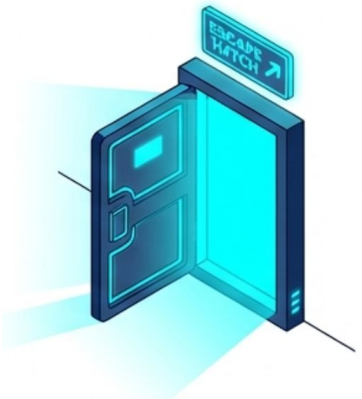
Relayer Censorship
If a single entity controls the Bundler, they can blacklist users and IPs (GeoLoc), effectively turning the DAP into a centralized bank.

The Solution



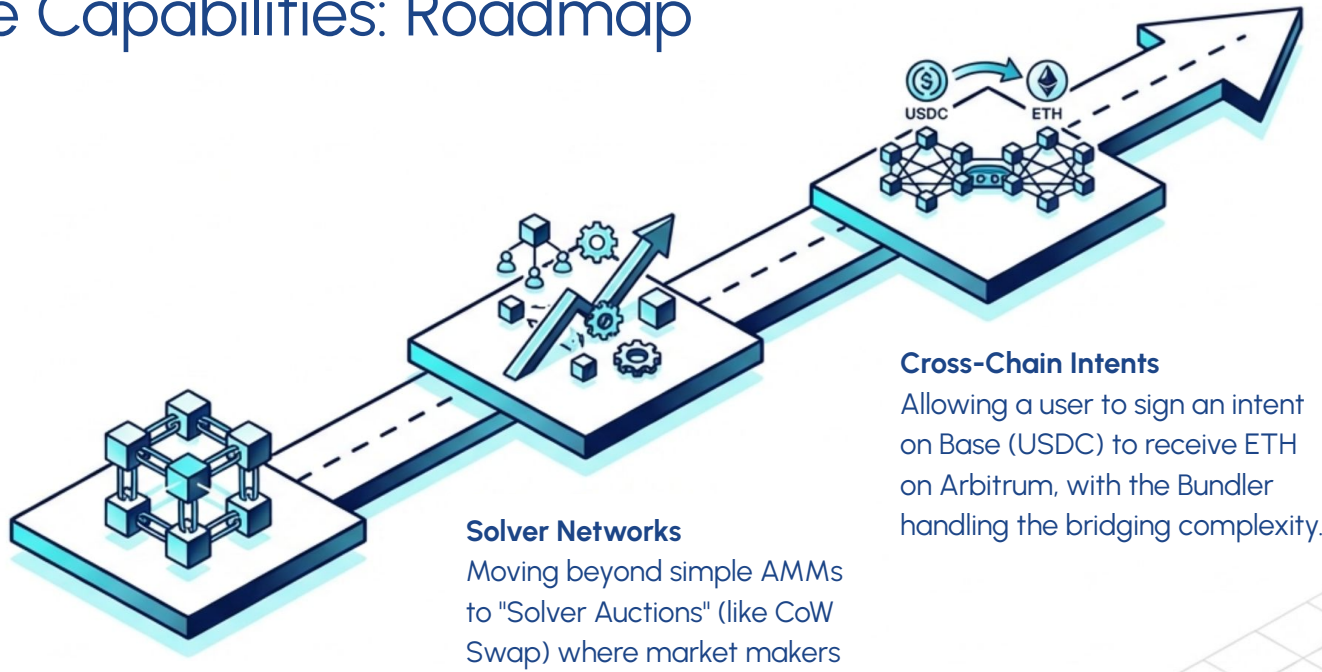
Permissionless Bundling
The architecture adheres to ERC-4337, allowing any third-party to run a bundler node and process transactions.

The Safety Valve



The Escape Hatch
The UI always retains a "Manual Mode." Users can choose to pay their own gas directly or blunder to the blockchain if the gasless infrastructure is unresponsive.

Future Capabilities: Roadmap



Multi-Chain Expansion
Deploying Paymaster contracts across all major EVM L2s (Optimism, Polygon).

Solver Networks
Moving beyond simple AMMs to "Solver Auctions" (like CoW Swap) where market makers compete to fill the order, minimizing MEV.

Cross-Chain Intents
Allowing a user to sign an intent on Base (USDC) to receive ETH on Arbitrum, with the Bundler handling the bridging complexity.

Summary of Proposition

EIP-7702
Allows to apply to the current millions userbase to swap in 1 click without paying gas.

ERC-4337
Allow to decentralize the actors who execute the swap and pay the gas creating a new economic environment.

Privacy Swaps
The proper combination of the architecture allow Consensys to act like a decentralized CEX on the click of a button.

L2
Make economically viable solution having a low fee generating revenue everywhere for the users removing the need of going to a CEX for the majority of the actions.

Market Expansion
A proper strategy can bring together cross-chain swaps just holding USDC accessing to thousands of monetization opportunities for the protocol to generate revenue.

Community
The majority of working protocols are the the ones who generate cash for their users, a bunch of new possibilities for passive income can be generated from liquidity pools, bundlers and paymasters.

[Questions & Discussion]