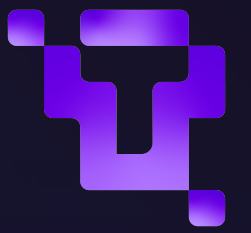
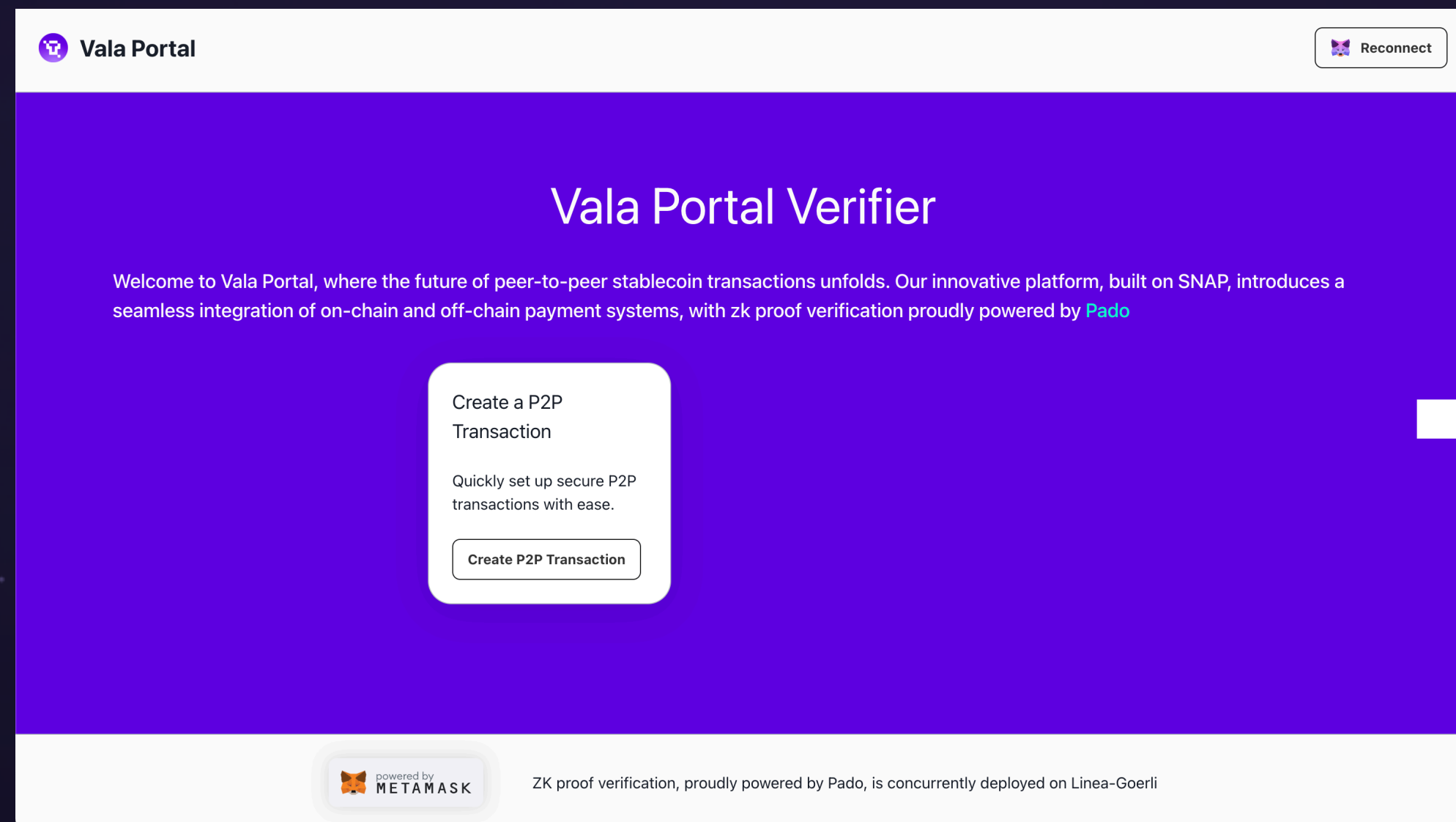


# Vala Portal

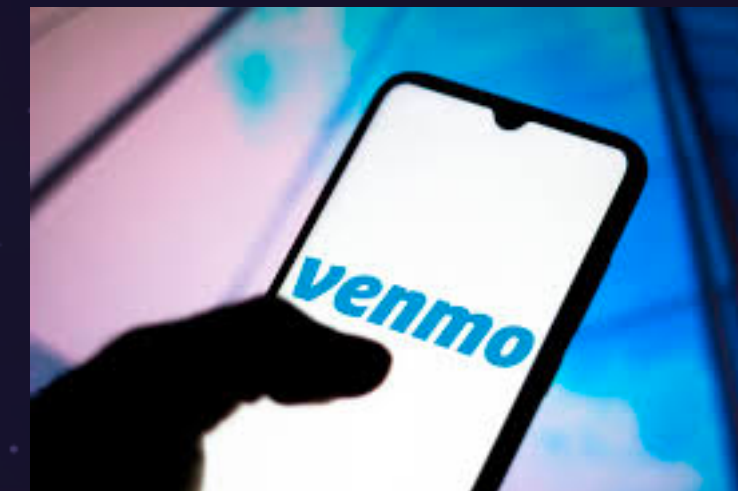
Empowering P2P Finance with Advanced ZK-Proof Technology



# How it work?



**Initiator initiates P2P trade, collateral tokens**

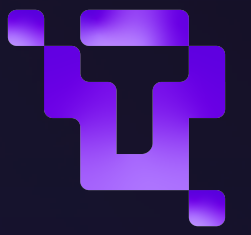


**Verifier completes off-chain payment, validates from Pado.**

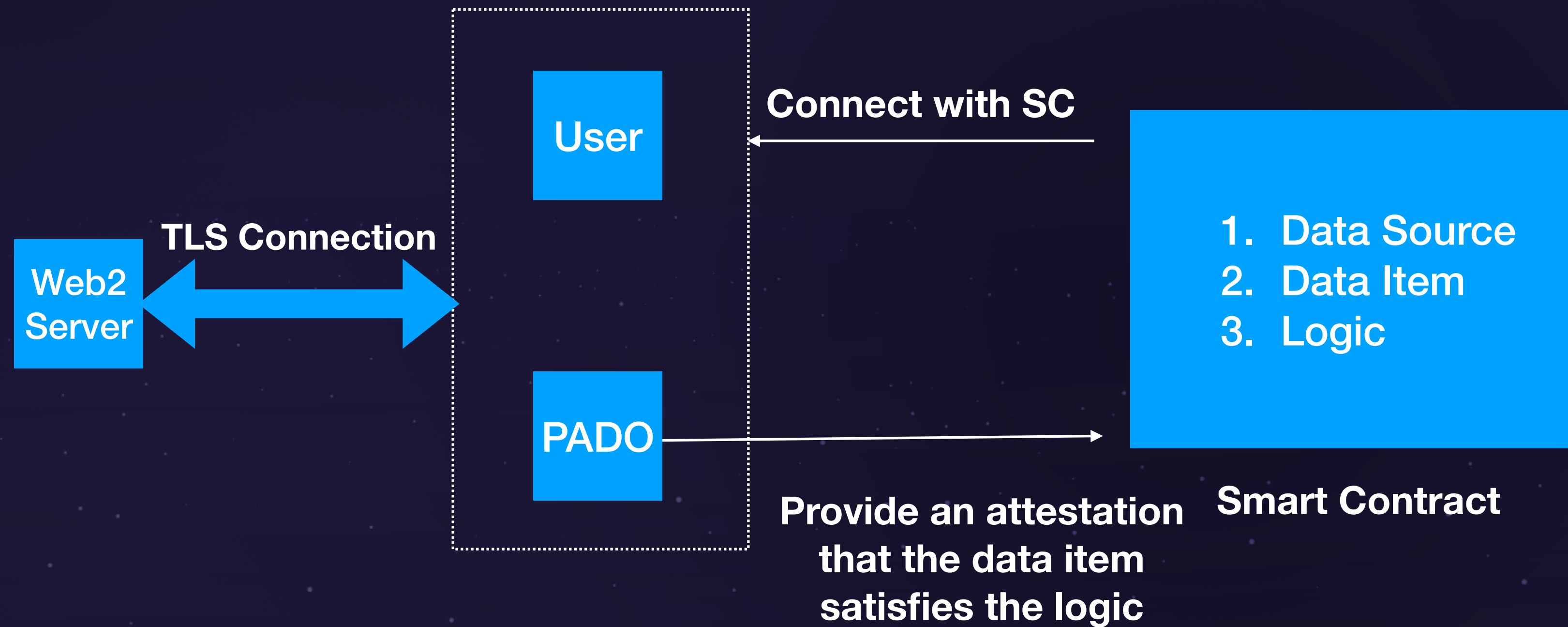
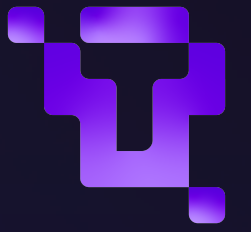


**Verifier claims tokens, finalizing P2P transaction**

# Abstracting Zero-Knowledge Proofs for Versatility



- **Flexible Zero-Knowledge Validation:** Vala Portal enabling a range of validations far beyond Venmo, and opening doors to diverse financial interactions
- **Expanding P2P onChain usecase:** Our platform is a gateway to Web 2.0 financial services, seamlessly connecting with various ecosystems and enhancing P2P transactional capabilities.
- **Leveraging SNAP:** we're shifting to client-side verification using WebAssembly, boosting speed and security. This move marks a significant step towards a more decentralized and efficient P2P transaction ecosystem



1. PADO is a privacy-preserving verifiable internet (web2) data provider for on-chain Dapps.
2. PADO enables Dapps to customize any data source (access with TLS), data item, and business logic (on the data).

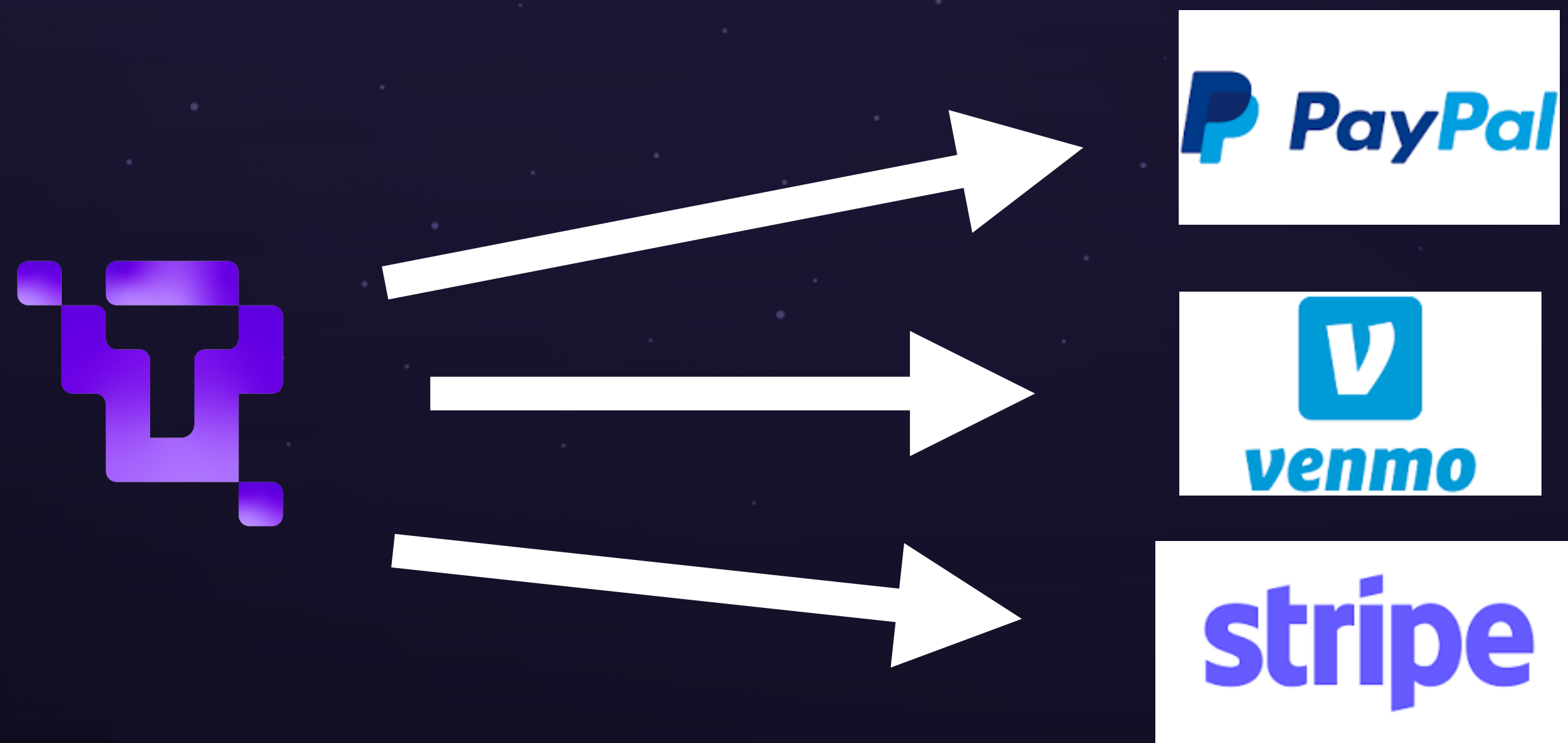
PADO achieves the goal by doing the following two steps. (<https://eprint.iacr.org/2023/964.pdf>)

1. The User and PADO run an MPC-TLS and IZK (interactive zkp) protocol with the web2 server. PADO attests that the User's data is actually from the intended source. In the whole process, PADO only authenticates the ciphertext, not any plain information.
2. The User proves that the data item satisfies the business logic. Two ways can be used.
  - User and PADO run an IZK protocol, to convince PADO that the data is valid. If PADO accepts, PADO will sign the result and upload it to the smart contract.
  - The user locally generates a proof using zk-snarks and provides this proof to the smart contract.

# Beyond Magic, But All Real

## Abstracting Validation in Finance with Vala Portal

Vala Portal redefines financial verification with its abstracted, compliance-focused ZK-proofs. Beginning with Venmo, we aim to extend to PayPal, Stripe, and beyond, setting new standards for secure, versatile financial interactions



**HACK Web 2.0  
in compliance way!**

Welcome to Vala Portal, where the future of peer-to-peer stablecoin transactions unfolds. Our innovative platform provides seamless integration of on-chain and off-chain payment systems, with zk proof verification proudly powered by zkSync.

Create a P2P Transaction

Quickly set up a transaction

Create P2P



Welcome to Vala Portal, where the future of peer-to-peer stablecoin transactions unfolds. Our innovative platform provides seamless integration of on-chain and off-chain payment systems, with zk proof verification proudly powered by zkSync.

Create a P2P

Welcome to Vala Portal, where the future of peer-to-peer stablecoin transactions unfolds. Our innovative platform provides seamless integration of on-chain and off-chain payment systems, with zk proof verification proudly powered by zkSync.

Create a P2P Transaction

P2P Transaction

amount

claimer

Close Create

P2P Transaction

amount

claimer

Close Create

MetaMask Notification

Linea Goerli test network

Account 2 0x8eEc3...2a9Bb

http://localhost:8000

**0x8eEc3...2a9Bb : CONTRACT INTERACTION**

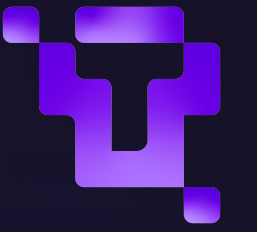
DETAILS DATA HEX

[Site suggested](#)

**Gas** (estimated) **4.864 4.864 LineaETH**  
 Very likely in < 15 seconds **Max fee:** 4.864 LineaETH

---

**Total** **4.864 4.864 LineaETH**  
 Amount + gas fee **Max amount:** 4.864 LineaETH



**THANK YOU!**