

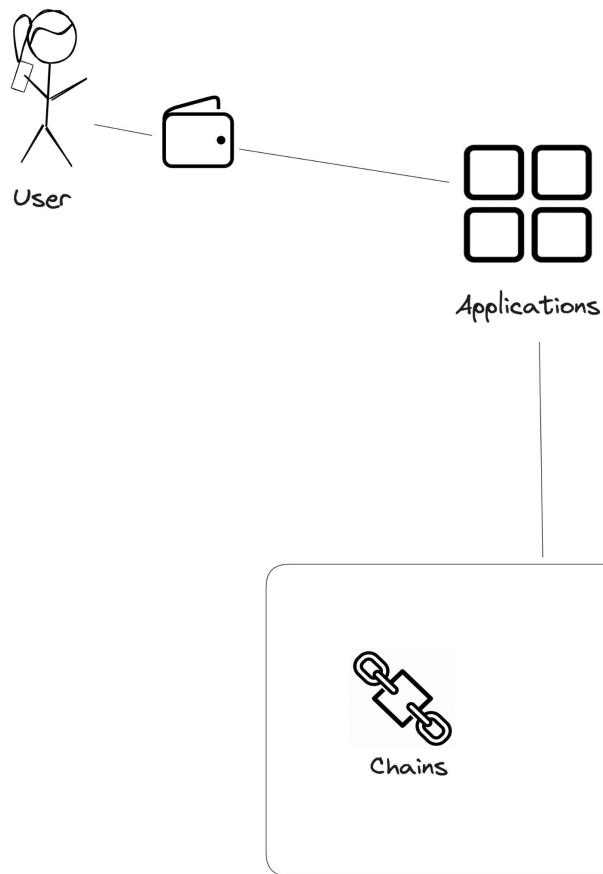
Chain abstraction is risk abstraction

Radina Talanova

L2BEAT



What is chain abstraction?



What can go wrong?

What can go wrong?



tempetechie.eth 3mo

Member

Careful When Using Degen Chain Bridge

Or How I Lost 785,000 DEGEN Bridging from Degen Chain to Base 🏆

What can go wrong?

90,000 DEGEN \leftrightarrow 0.069 ETH | 87% slippage

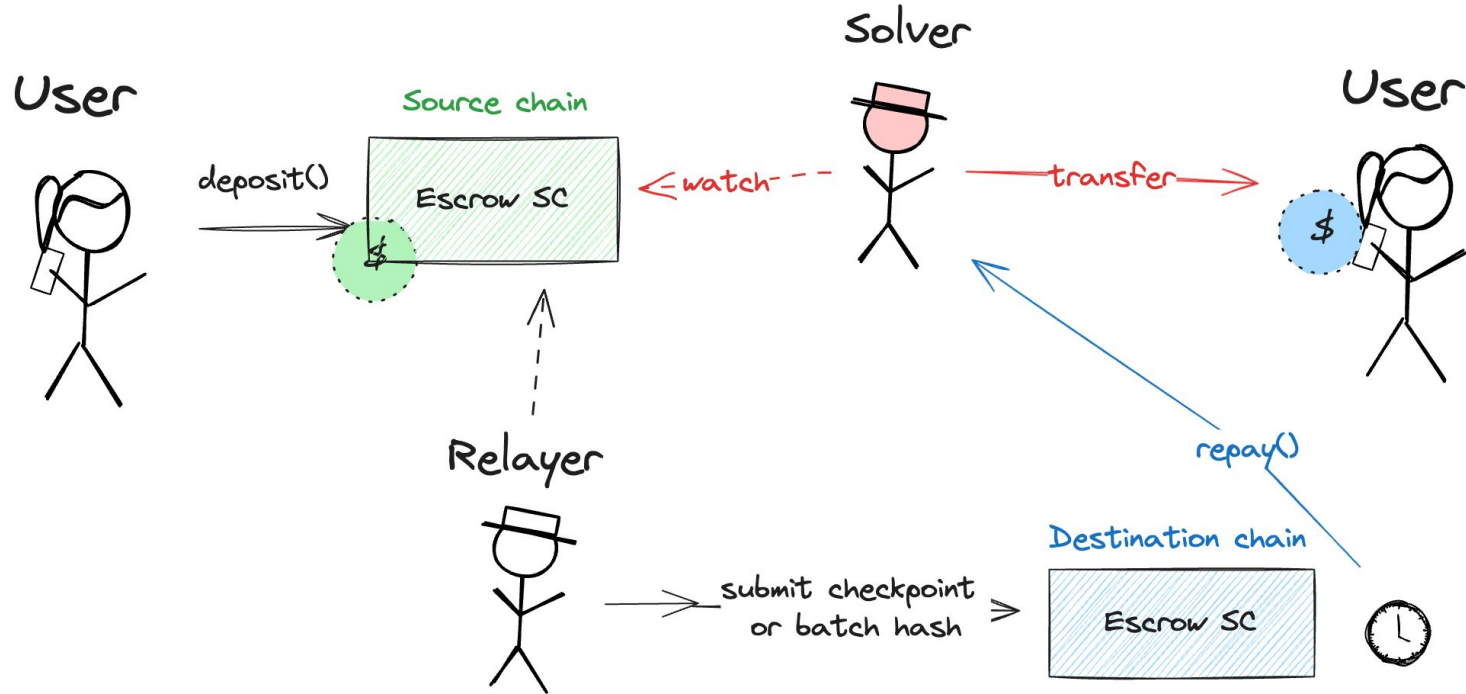
Degen chain
Base



0.069 ETH \leftrightarrow 38,000 DEGEN

How can we do abstraction better?

Intent-based protocols



Chain-abstracted balances?



APE on ApeChain, OFT, IOU

Native/gas token

Secured by canonical Arbitrum <> ApeChain bridge, LayerZero Omnichain Bridge



APE on Arbitrum, OFT, IOU

[0xE7B3A4b51ac8BC603BB041F50092633f5b0C3CC9](https://arbitrum.io/bridge/0xE7B3A4b51ac8BC603BB041F50092633f5b0C3CC9)

Secured by LayerZero Omnichain Bridge



APE on Ethereum, OFT, IOU

[0x02597D0F8B902cdA4FE29695bA2C561FC0f370F6](https://ethereum.org/bridge/0x02597D0F8B902cdA4FE29695bA2C561FC0f370F6)

Secured by LayerZero Omnichain Bridge



APE on Ethereum, Natively minted

[0xab73585fa4D65B68597747F16A425192B4b4d4Af](https://yuga.io/0xab73585fa4D65B68597747F16A425192B4b4d4Af)

Managed by Yuga Labs

Chain abstraction is risk abstraction

There are risks that users are not protected from, which can lead to a loss of funds. While users may be unaware of these risks, it's essential that they are informed.

Chain abstraction is risk abstraction

There are risks that users are not protected from, which can lead to a loss of funds. While users may be unaware of these risks, it's essential that they are informed.



There are risks, but users are not the ones who would bear the consequences if these risks materialize. Users can remain unaware of these risks.



APE on ApeChain, OFT, IOU | **High risk**

Native/gas token

Secured by canonical Arbitrum <-> ApeChain bridge, LayerZero Omnichain Bridge

- Upgrader can steal funds by upgrading the contract. There is no delay on code upgrades
- DVNs + Executor can steal by relaying and executing a malicious message
- LayerZero MS can steal by setting a malicious default security stack



APE on Arbitrum, OFT, IOU

[0xE7B3A4b51ac8BC603BB041F50092633f5b0C3CC9](https://arb1.arbitrum.io/address/0xE7B3A4b51ac8BC603BB041F50092633f5b0C3CC9)

Secured by LayerZero Omnichain Bridge

- DVNs + Executor can steal by relaying and executing a malicious message
- LayerZero MS can steal by setting a malicious default security stack



APE on Ethereum, OFT, IOU

[0x02597D0F8B902cdA4FE29695bA2C561FC0f370F6](https://etherscan.io/address/0x02597D0F8B902cdA4FE29695bA2C561FC0f370F6)

Secured by LayerZero Omnichain Bridge

- DVNs + Executor can steal by relaying and executing a malicious message
- LayerZero MS can steal by setting a malicious default security stack



APE on Ethereum, Natively minted

[0xab73585fa4D65B68597747F16A425192B4b4d4Af](https://etherscan.io/address/0xab73585fa4D65B68597747F16A425192B4b4d4Af)

Managed by Yuga Labs



Thank you!

