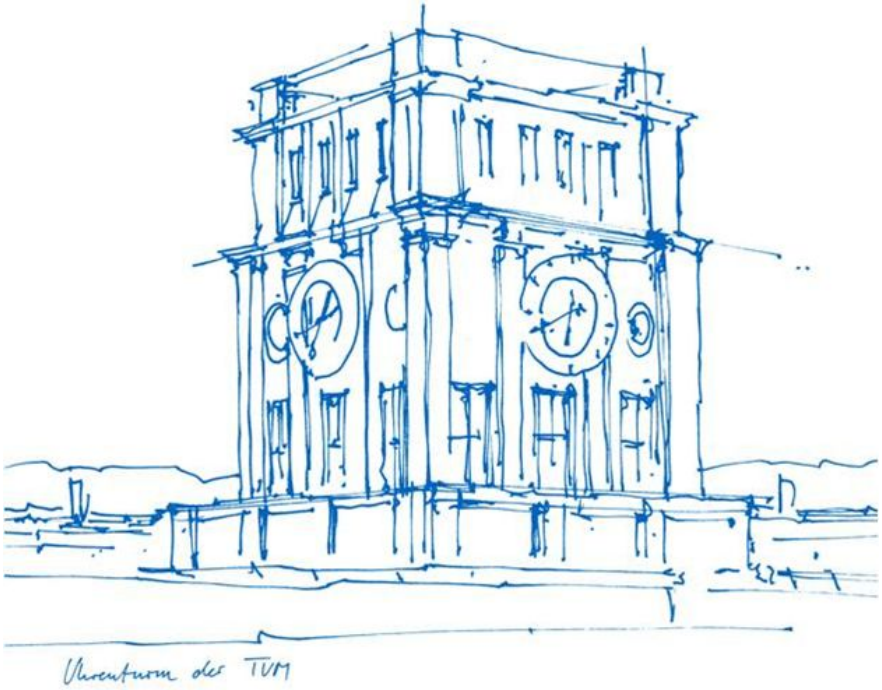


TUM
Blockchain Salon

Bridge Security in Blockchain

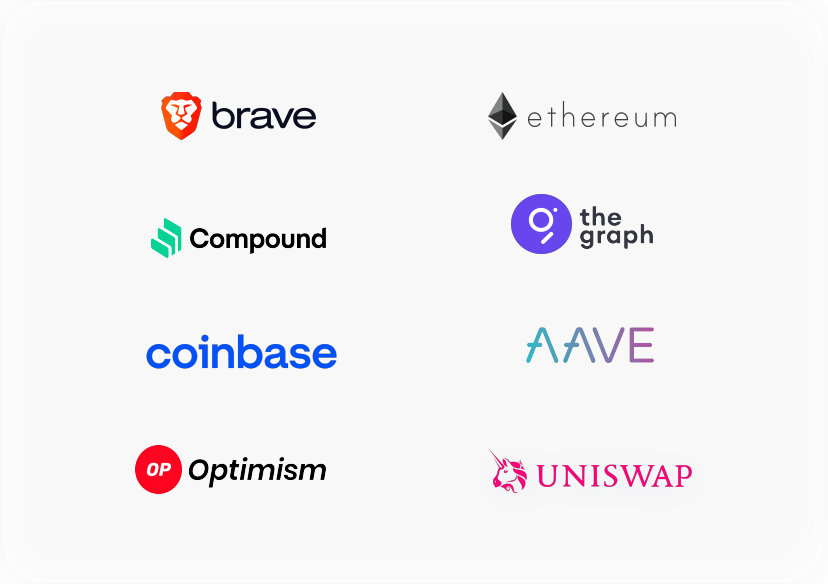
OpenZeppelin

ABOUT OPENZEPPELIN

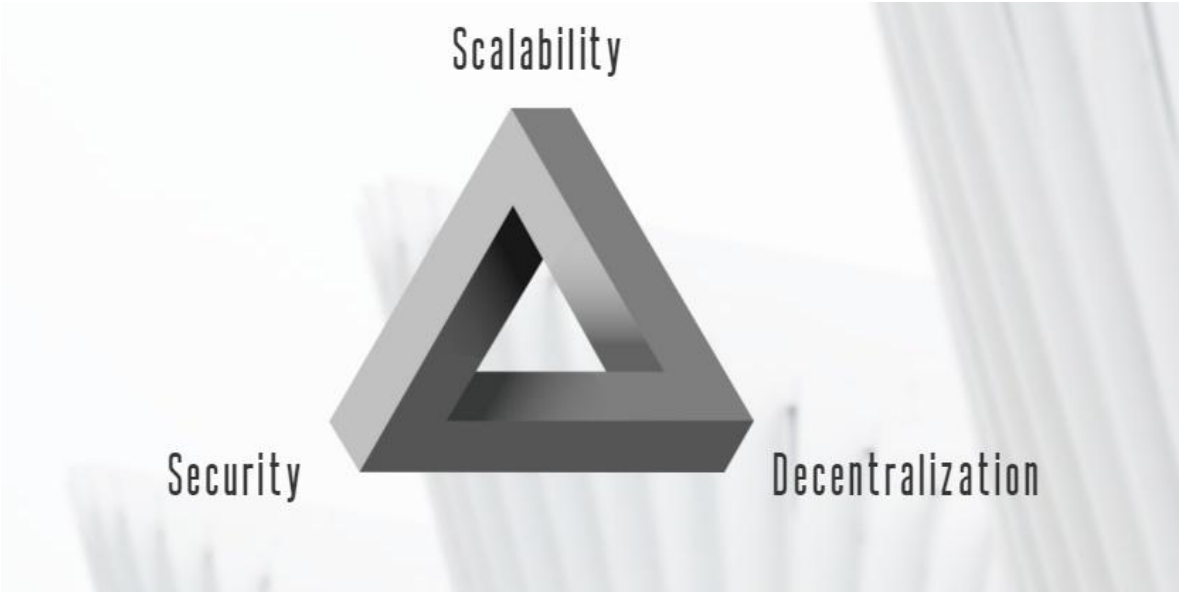
Our mission is to protect the open economy

OpenZeppelin is a software company that provides **security audits** and **products** for decentralized systems.

Projects from any size - from new startups to established organizations - trust OpenZeppelin to build, inspect and connect to the open economy.



Blockchain Trilemma



Solution

Layer 1 Changes:

- Proof of Stake
- Sharding

Layer 2 Innovations:

- Sidechains
- State Channels
- Rollups

Here comes bridges!

Definition of a bridge

- A blockchain bridge connects two blockchain ecosystems
- Allows the cross-chain transfer of assets and data
- promoting interoperability and creating a more connected blockchain ecosystem

Why do we need a bridge?

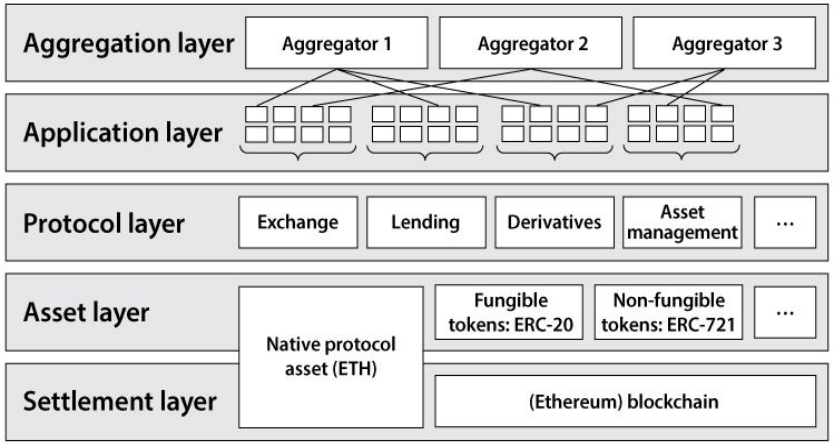
- Efficiency: Lower transaction fees
- Cross-chain collateral: use BTC on Eth Dapps
- Explore blockchain ecosystems
- Own native crypto assets

What are the types of bridges?

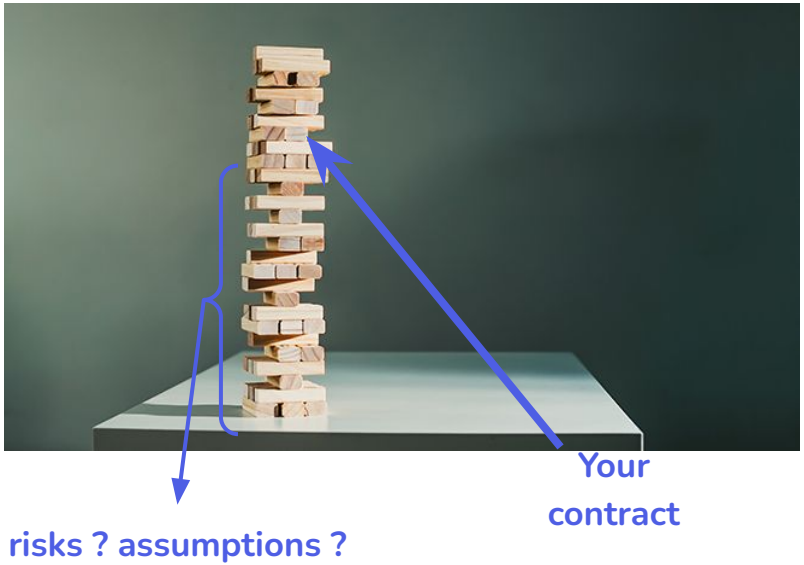
- Trusted bridges : rely on third parties to validate transactions while acting as custodians of the bridged assets
- Trustless bridges : rely purely on smart contracts and algorithms to store custody assets

Security Risks

Composability



Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets
by Fabian Schär



OpenZeppelin

Risks of using bridges

Bridges are in the early stages of development. It is likely that the optimal bridge design has not yet been discovered.

Interacting with any type of bridge carries risk:

- **Smart Contract Risk :** the risk of a bug in the code that can cause user funds to be lost
- **Technology Risk :** software failure, buggy code, human error, spam, and malicious attacks can possibly disrupt user operations
- **Integration Risk :** other components that the bridge is interacting with

Moreover, since trusted bridges add trust assumptions, they carry additional risks such as:

- **Censorship Risk :** bridge operators can theoretically stop users from transferring their assets using the bridge
- **Custodial Risk :** bridge operators can collude to steal the users' funds

Hacks

RONIN Network hack

- In March 2022, the private keys of the validators were compromised to steal tokens worth approximately $624 million from the Ronin Bridge.
- Ronin network was created as an Ethereum side-chain to support the transaction throughput required for Axie Infinity.
- Developed by Sky Mavis, the Ronin Bridge connects the Ronin Network to Ethereum.
- To increase transaction per second (TPS), the Proof of Authority model was used instead of decentralization and trustlessness, using nine validators
- Of these nine validators, four are operated by Sky Mavis
- Hacker targeted these 4 nodes, gaining majority of signatures
- Additionally, Axie DAO had granted Sky Mavis access to sign on its behalf to deal with high user volumes, but this access was not revoked, creating a potential backdoor.

What went wrong?

Read in detail: https://rekt.news/ronin-rekt/

Harmony hack

- Harmony's Horizon bridge provides a trustless way to move assets between the Harmony, BNB Smart Chain and the Ethereum blockchains.
- In June 2022, Horizon bridge was exploited for $100M after their private keys were compromised.
- The approval process used a multi-signature system with five validators. However, the bridge was only using a 2-of-5 validation scheme.

What went wrong?

Read in detail: https://rekt.news/ronin-rekt/

Wormhole hack

- Wormhole is a bridge between Ethereum and Solana which helps the users benefit from Solana's high speed and low cost.
- In February 2022, the Wormhole bridge was hacked for $325M worth of tokens (ETH, USDC and SOL).
- The attacker was able to bypass the signature verification by exploiting a deprecated and insecure function in the code, faking a deposit of 120k ETH on Ethereum and minting equivalent amount of wrapped whETH on Solana.
- The vulnerability was immediately patched and the bridge resumed work the next day.
- Hacker was offered $10M in bug bounty to return the stolen funds, as a whitehat agreement.

What went wrong?

Read in detail: https://rekt.news/wormhole-rekt/

Consequences of security breaches

- Loss of assets
- Network disruption
- Regulatory scrutiny
- Damage to reputation

Closing thoughts

Best practices

- Multi-Signature Transactions
- Threshold on Number of Signatures
- Consensus Among Validators
- Smart Contract Security
- Key management
- Use of timelocks
- Regular Audits
- Real-time monitoring and IR

With love, from the OpenZeppelin research team

Assume your users wont use your contracts as you want them to be used

Have a plan for key management (multi-sig arrangements) for admin accounts

Get someone to break your contracts as early as possible (like bug bounties)

Read about other DeFi hacks - they open your eyes to what attacks are possible

Launch slowly, first deploying in testnets

Don't reinvent the wheel but do know how it works

Security is worth investing in!

Audits are not enough

Documentation is key for others to analyze your code

Decentralize governance slowly

Set up monitoring systems

Encourage your community to know the limitations of your code and security knowledge. Educate them

The importance of testing, auditing & bug bounties

Design first, code later.

Code slowly

OpenZeppelin

We're hiring!

Open Roles

- Blockchain Security Engineer
- IT Security Engineer
- Strategy and Operations Associate
- Sales Account Representative ...

Check out more

zpl.in/join

OpenZeppelin

Thank you

Smriti
Verma

@smritinverma
smriti@openzeppelin.com