BITCOIN LAYER 2 ECOSYSTEM

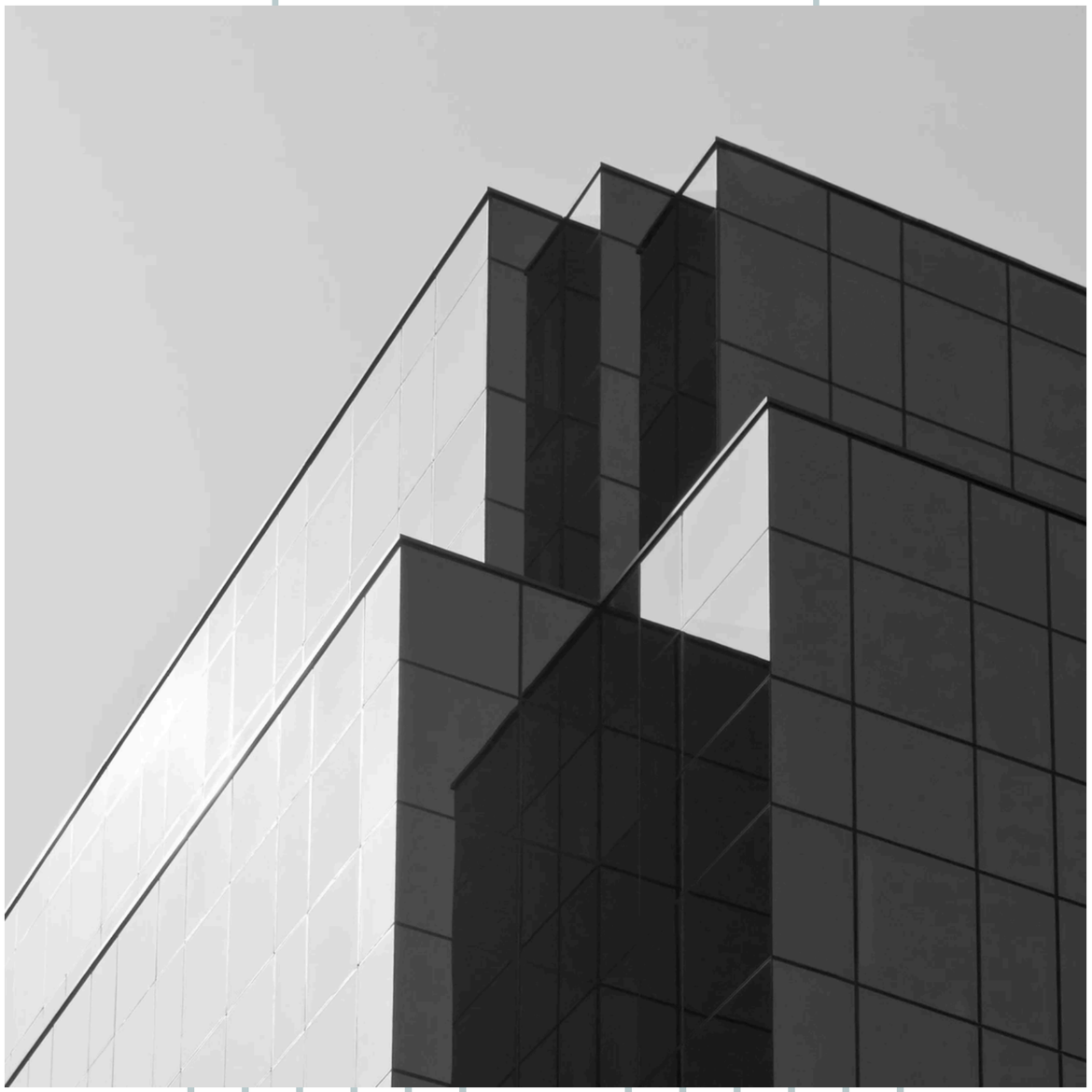
MAY - OCTOBER, 2025

"These slide summarizes the key findings from our one-year research project.
For the full research materials, please refer to:
・/Japanese/internal_research (Japanese)/"

Approaches

- State Channel approach
- Sidechain approach
- Rollup approach

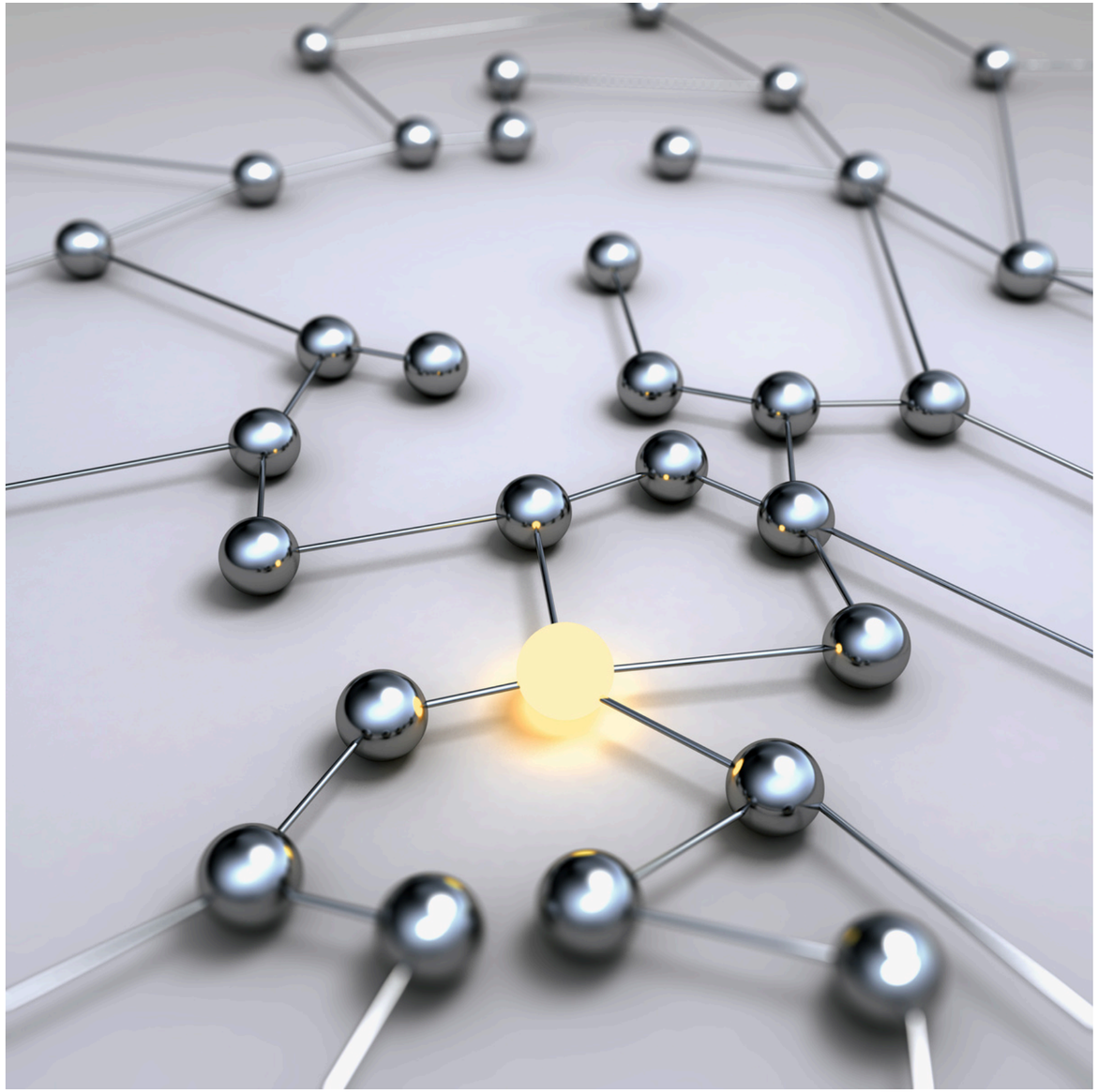
However, there are many other methods besides these.
There are probably few projects that simply fit into one of these methods.



State Channel

The State Channel method governs channels established off-chain between two parties.

The Lightning Network is a well-known example of this method.



Sidechain

It functions on a distinct chain from Bitcoin and is mainly linked to Bitcoin solely through bridges.
L2 offers a significant degree of freedom; however, its security is contingent upon the L2 verifier.

Rootstock and Liquid serve as examples of this category.



Rollup

Like the Sidechain method, the Rollup method creates a chain separate from Bitcoin. Multiple transactions are processed together and data that can be used to verify those transactions is stored in L1.

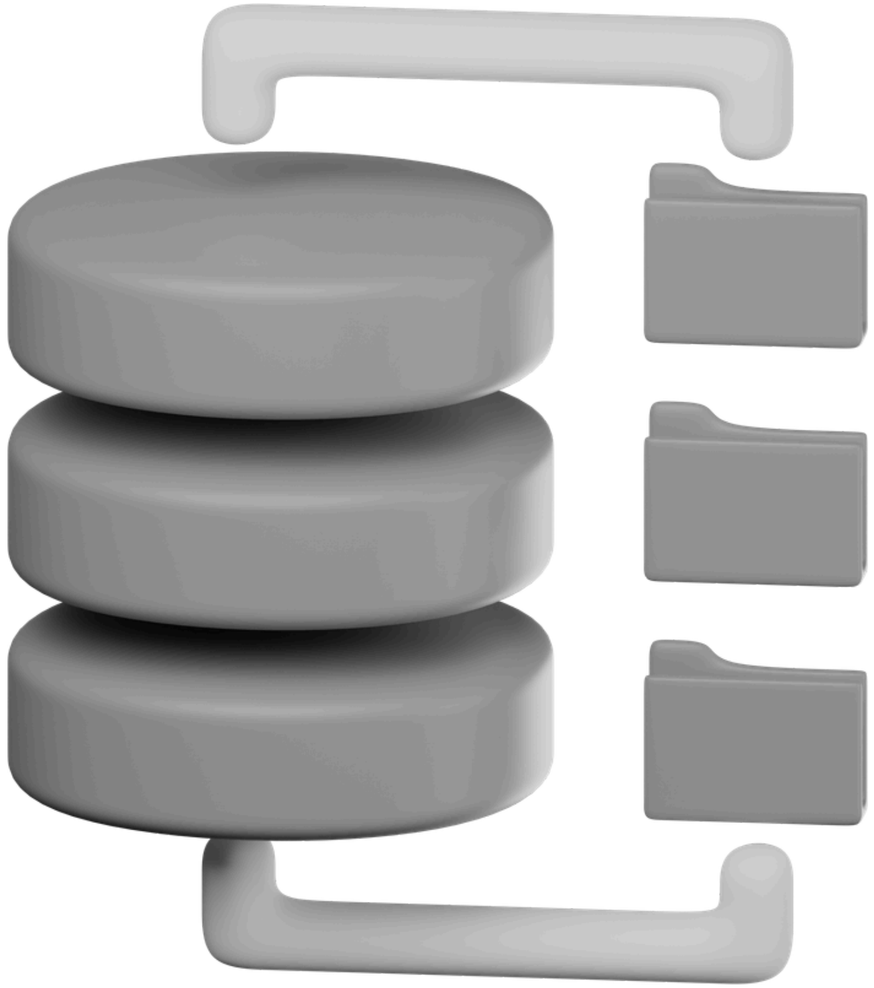
There are various other methods that use this method, such as Citrea and Bitlayer.



DA layer

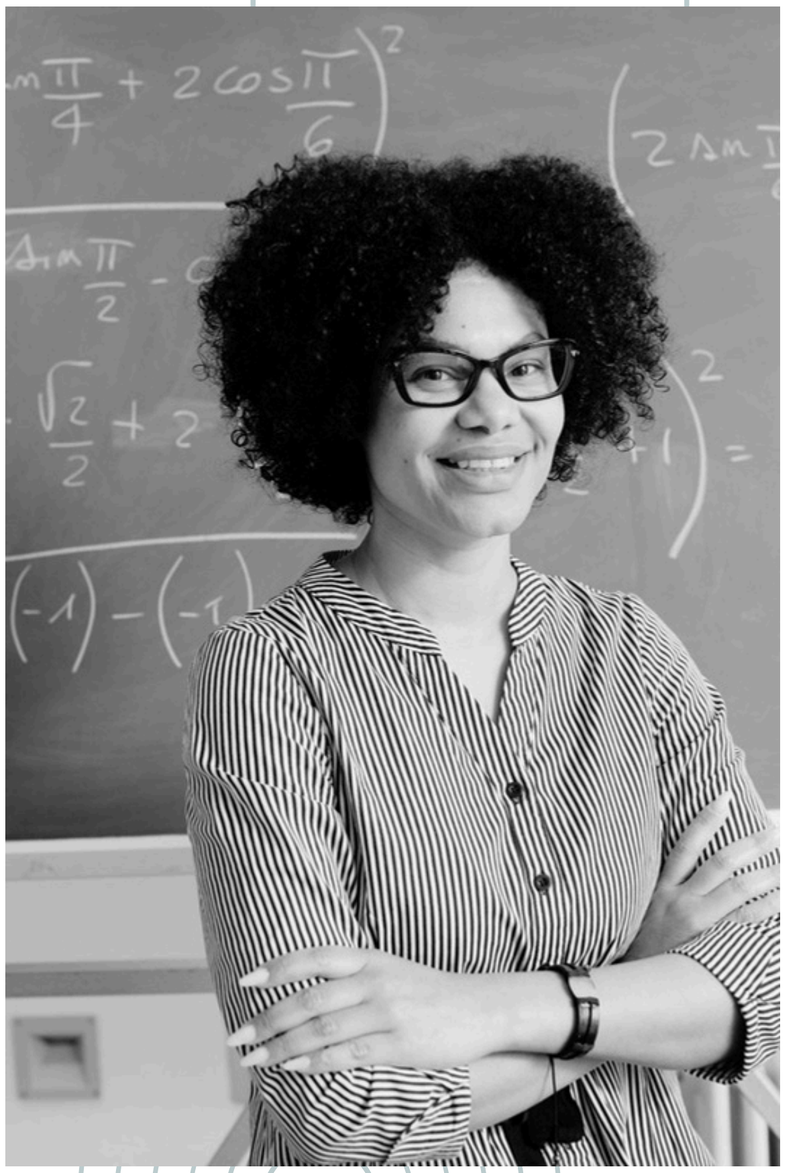
Storage is required to store data that verifies the state of L2, which is called the Data Availability Layer (DA layer).

In the case of Bitcoin L2, it is often stored in Bitcoin L1.



Sovereign Rollup

Bitcoin scripts cannot perform complex calculations, so verification is mostly done off-chain.
The method in which the verification itself is performed off-chain and only the proof data is written to the DA layer is called Sovereign Rollup.
When Bitcoin L2 refers to zkRollup, it almost always refers to Sovereign Rollup using zk-proof data.



Variations in verification mechanisms

Optimistic Rollup	If fraud is detected, someone honest will "challenge" it.
zkRollup Validity Rollup	Prove it using cryptographic techniques such as zero-knowledge proofs.

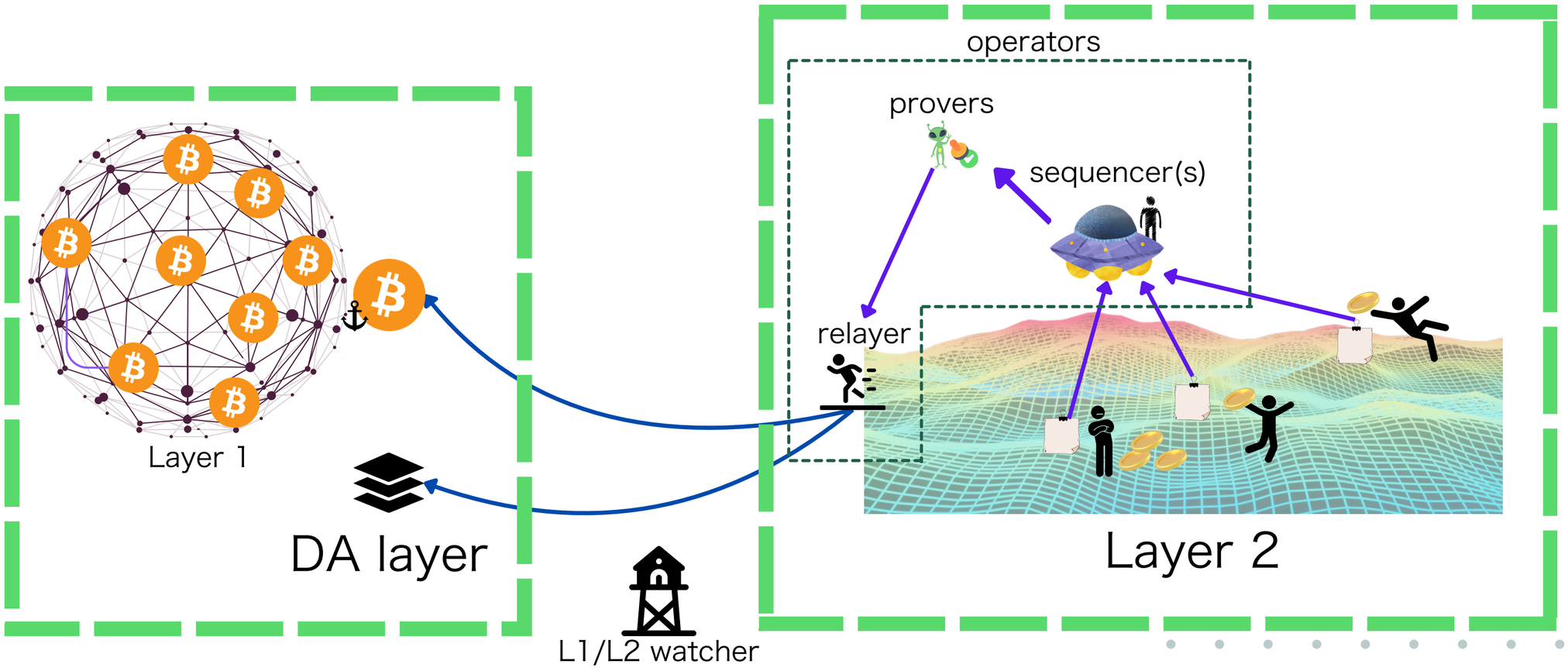
Sovereignty

Sovereign Rollup	L2 functions autonomously, while L1 serves solely as Data Availability (DA).
Smart Contract Rollup	The condition of L2 is governed and validated by the smart contract of L1.



Rollup Structure

While it differs from project to project, these are the fundamental elements. The DA layer is often the same as L1, but is shown separately in this diagram.



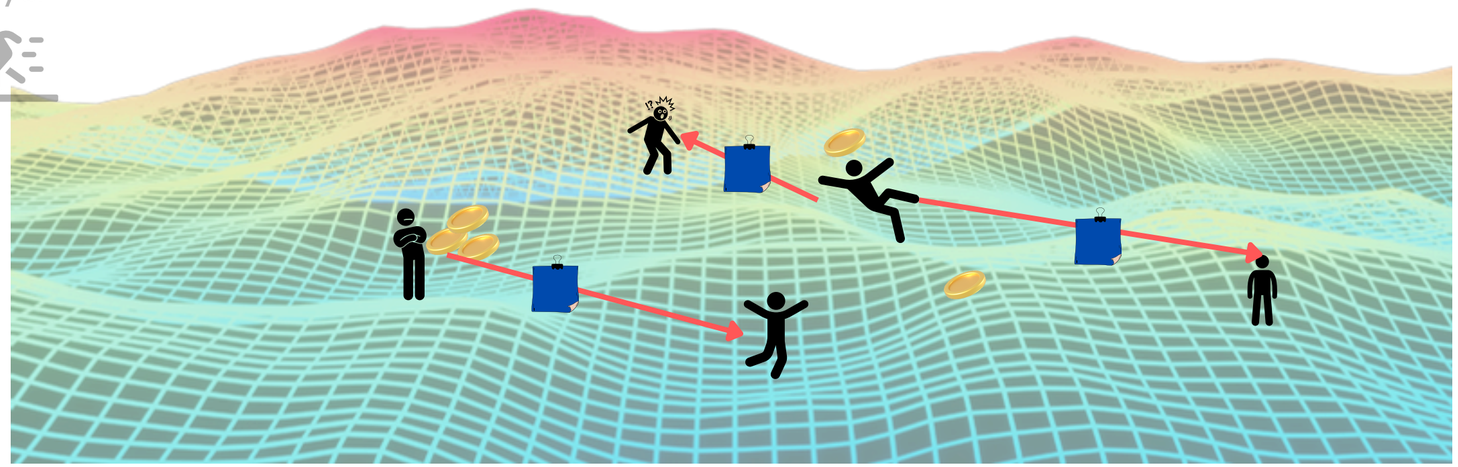
Transactions

When you send or receive funds on L2, transaction data is generated and broadcasted on the network.

provers

sequencer(s)

relayer



Layer 1

DA layer

Layer 2

Sequencer

The Sequencer receives the transaction data.

provers

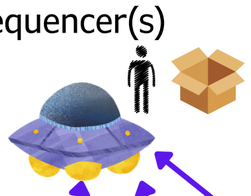


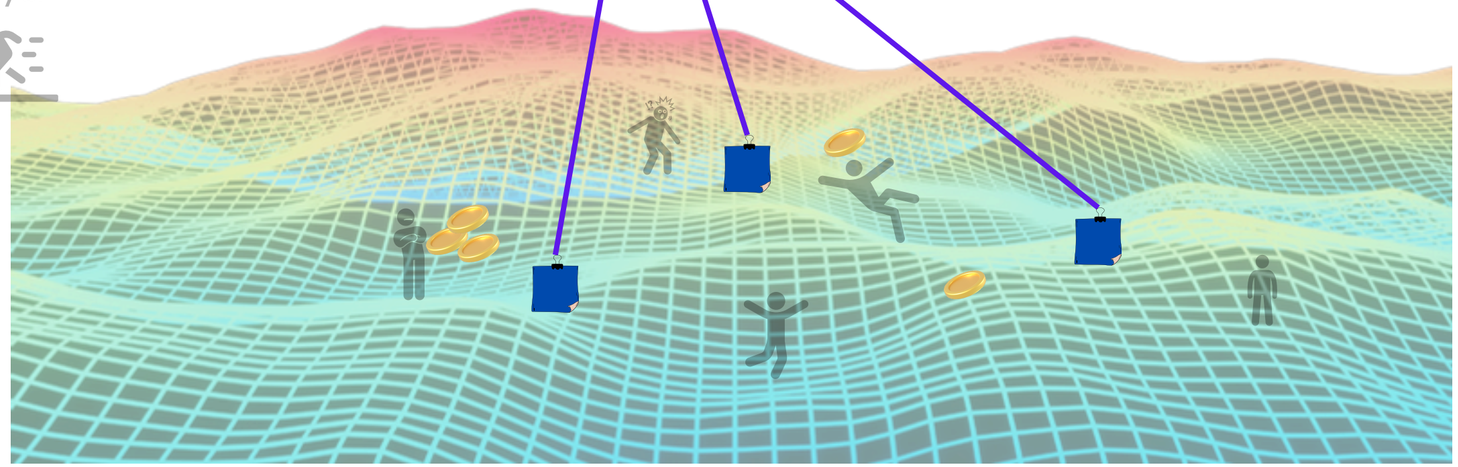


Layer 1

DA layer

relayer





Layer 2

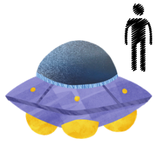
Sequencer

The Sequencer organizes transactions and generates blocks.
It also refreshes the account's status, including its balance.

provers



sequencer(s)





generate block

update state

relayer



Layer 2



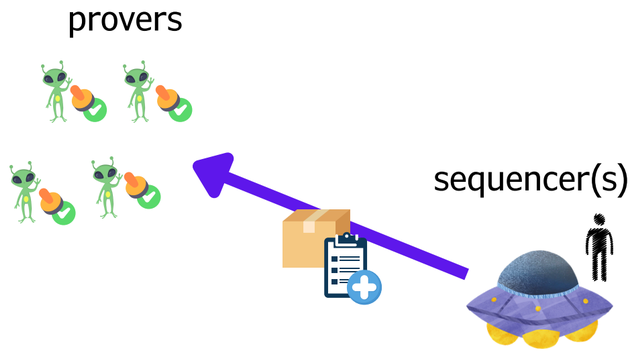
Layer 1



DA layer

Sequencer

The generated block data and state difference data are sent to Prover.

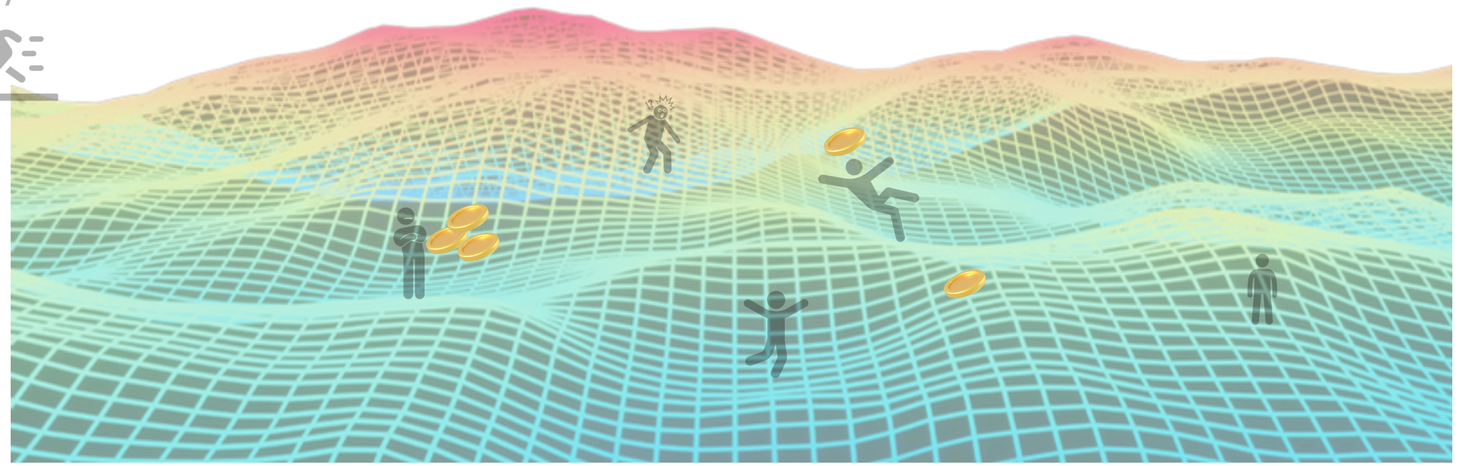




Layer 1

DA layer

relayer

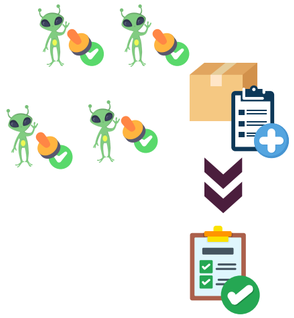


Layer 2

Prover

The prover validates that state changes are legitimate and generates data to substantiate this.

provers



sequencer(s)



relayer





Layer 1

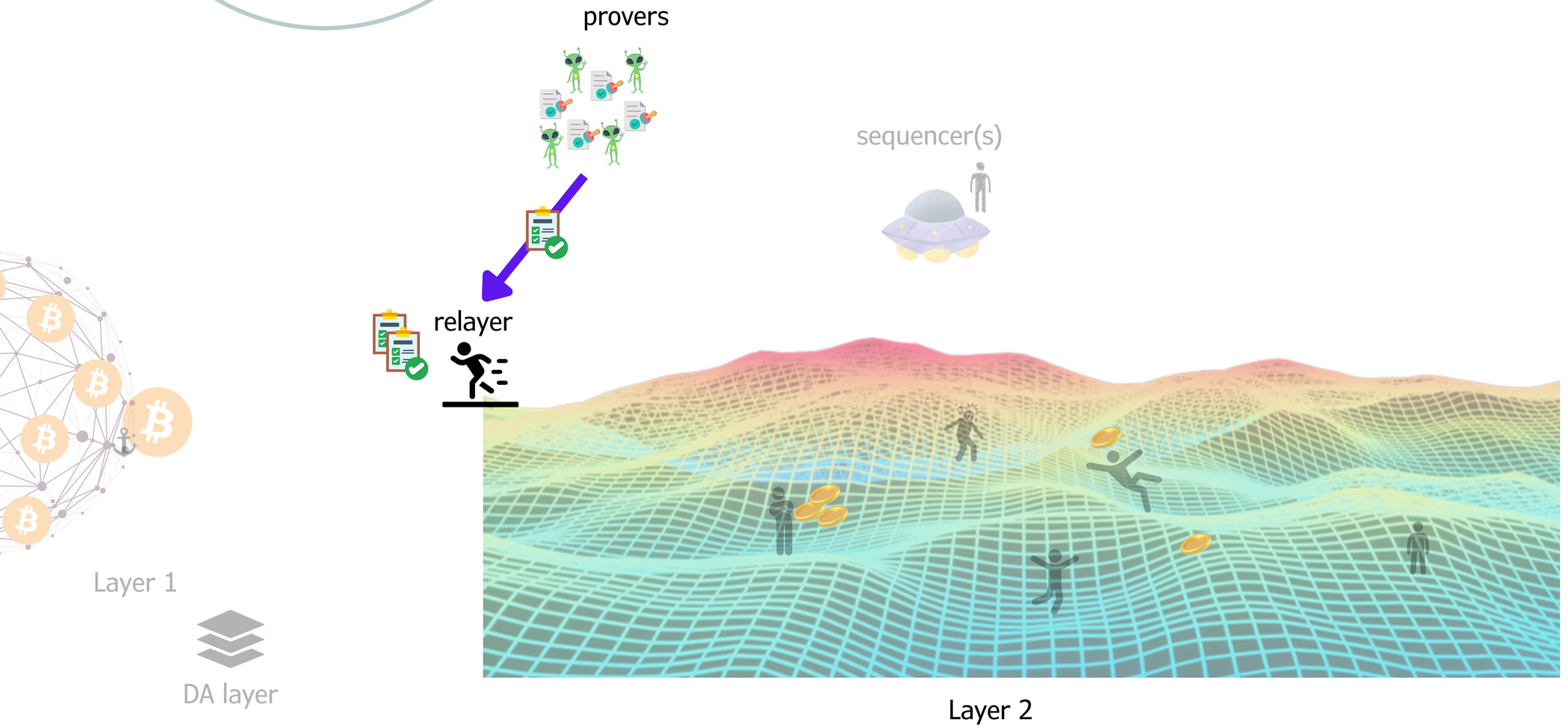


DA layer

Layer 2

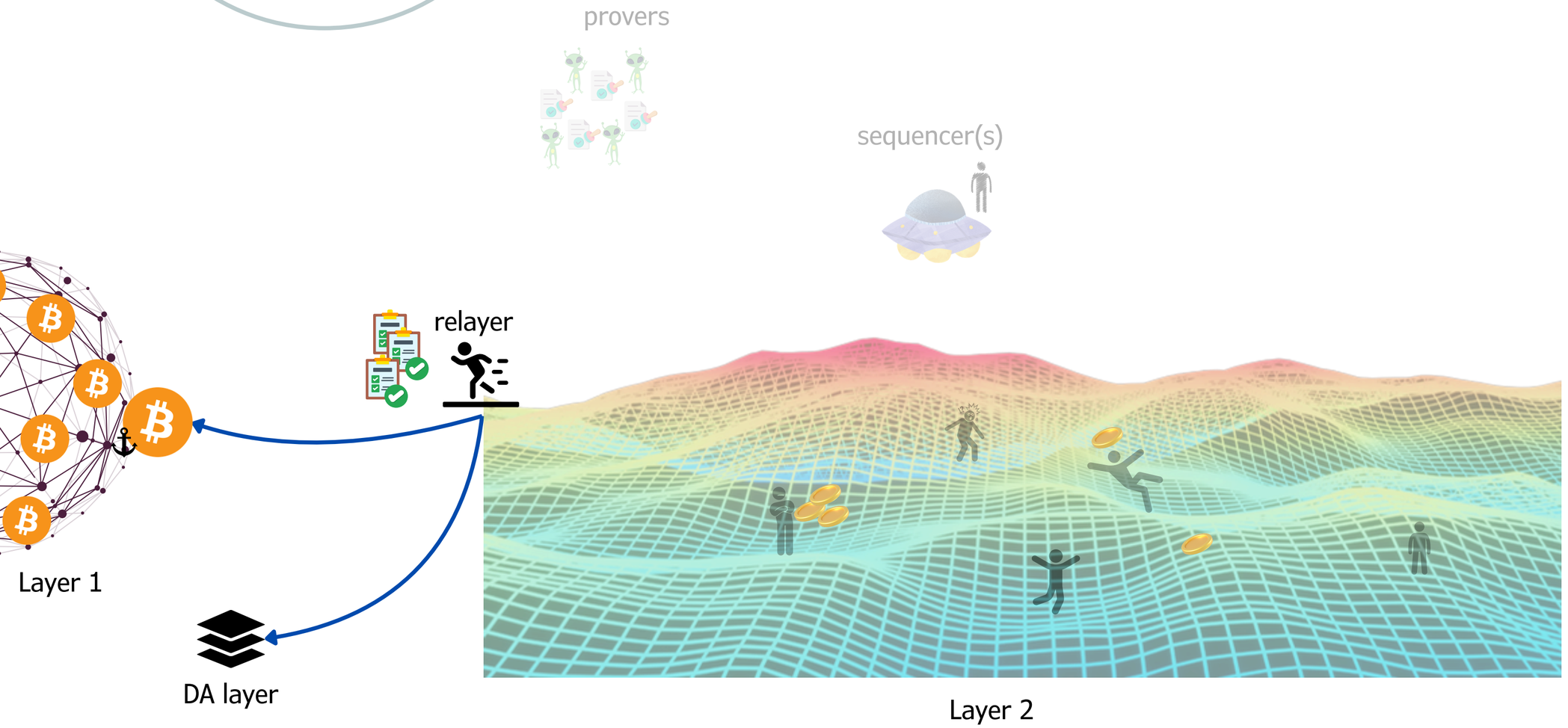
Prover

The Prover generates a proof and transmits it to the Relayer.



Relayer

The relayer collects a certain amount of proof data and then stores it in the DA layer.



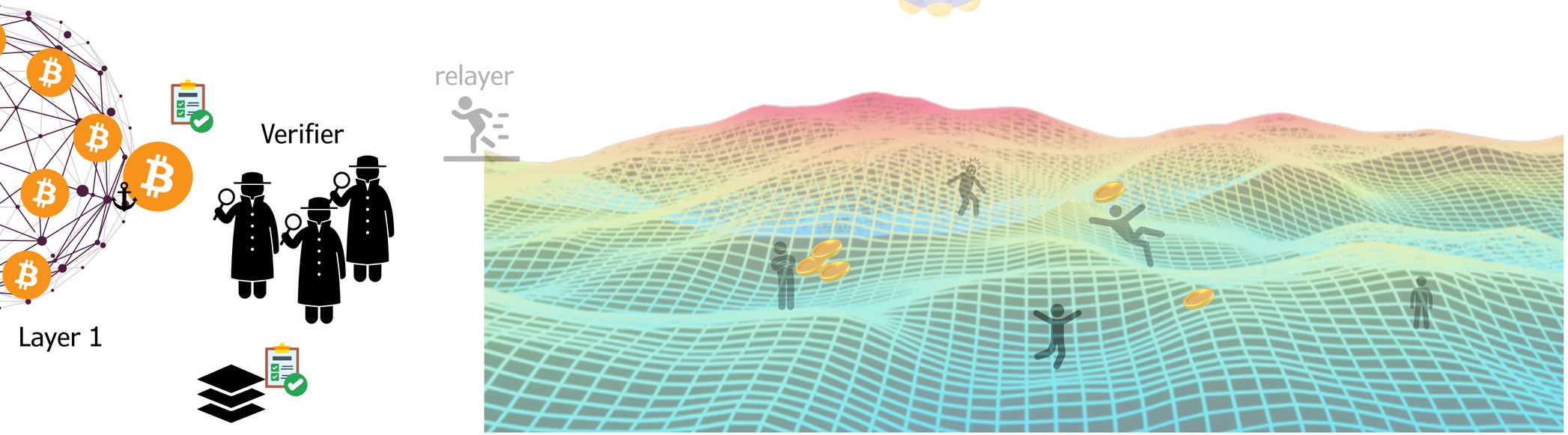
Verifier

Verifiers verify the verification data written in the DA layer.
If fraud is discovered during verification, penalties such as funds being confiscated will be imposed.

provers

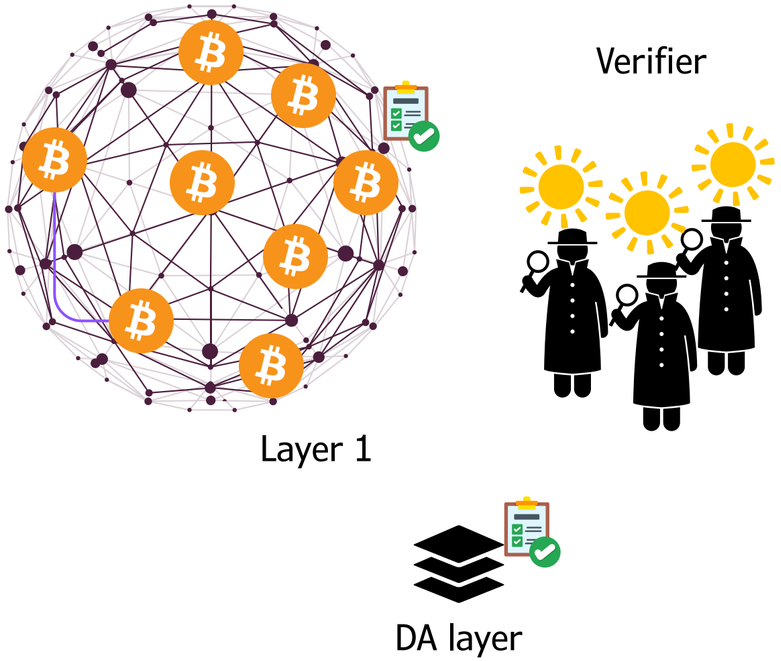
sequencer(s)

relayer



Verifier

Since the Bitcoin script cannot verify it, the app verifies it and reports any invalid data. This is the Optimistic Rollup method. The reason they are "optimistic" is because they assume it's OK as long as no one reports any fraud.



- At least one honest individual must be involved in the verification process.
- It takes time to complete in order to ensure time to report fraud.
- Proof of fraudulent claims will be deployed as an L1 transaction, which will incur costs for the operator.

BRIDGE

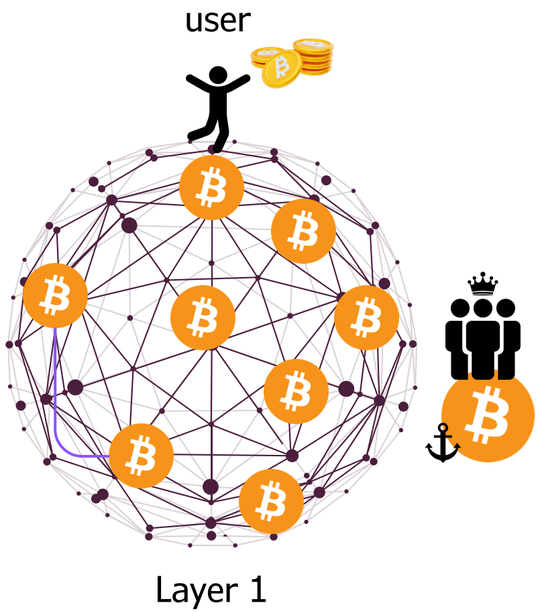
Bridge

A bridge is a feature that allows tokens to be exchanged between different chains.
The operator locks the L1 funds requested by the user and issues tokens in L2, and the user returns the tokens to the operator and returns funds to L1.

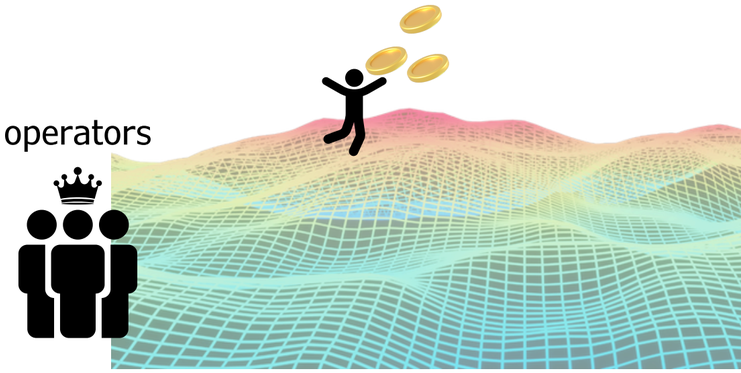


Bridge

Funds may be locked at L1 and subsequently deposited into L2, or burned at L2 and returned to L1.
Bridges tend to be systems that rely on trust in their operators.



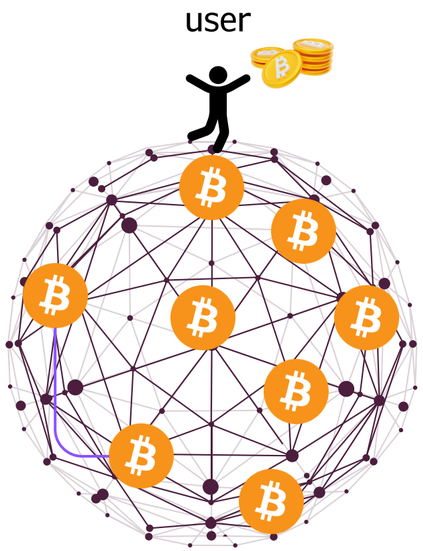




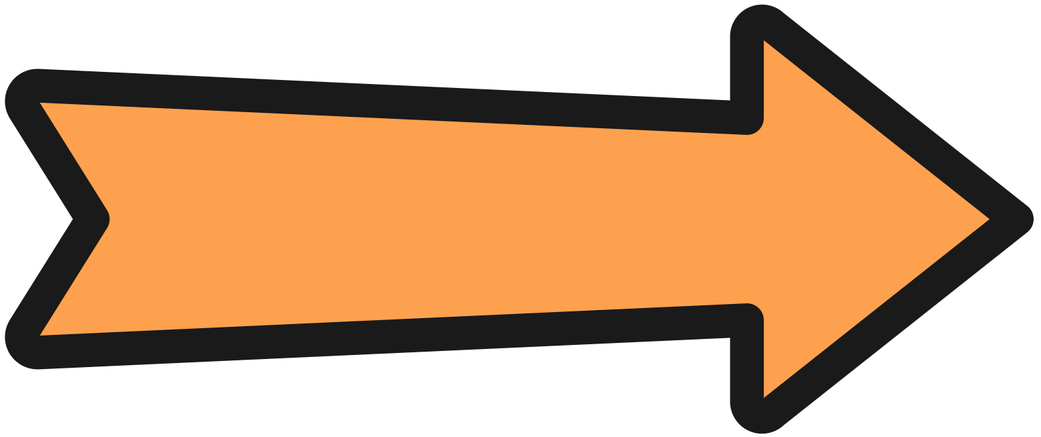


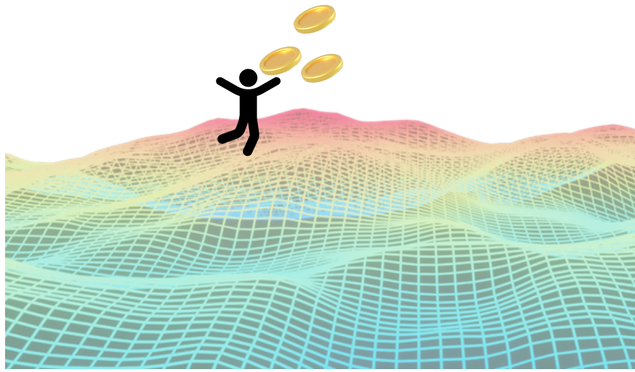
Peg-In

A peg-in refers to a transfer of funds from Layer 1 to Layer 2.



Layer 1

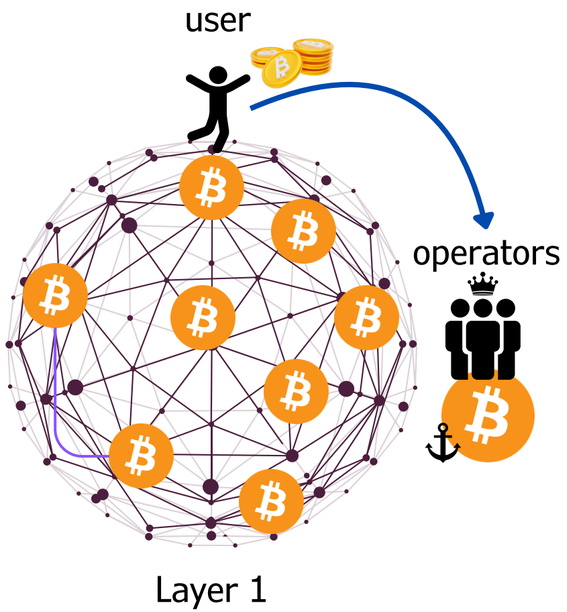


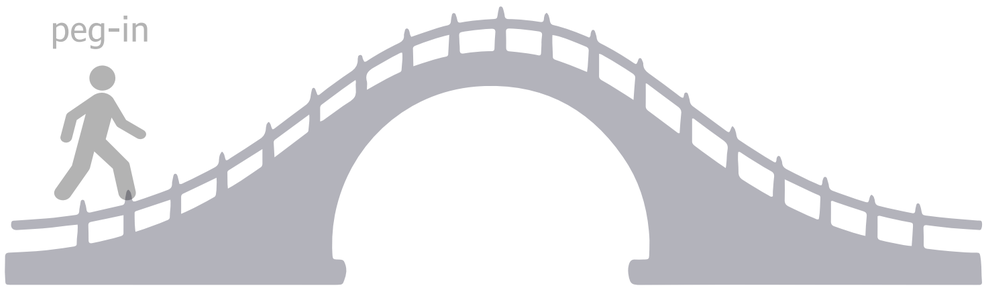


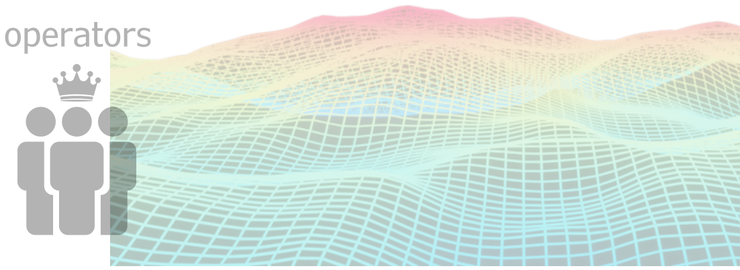
Layer 2

Peg-In

On L1, users transfer funds to the Bitcoin address(multisig addresses are often used).

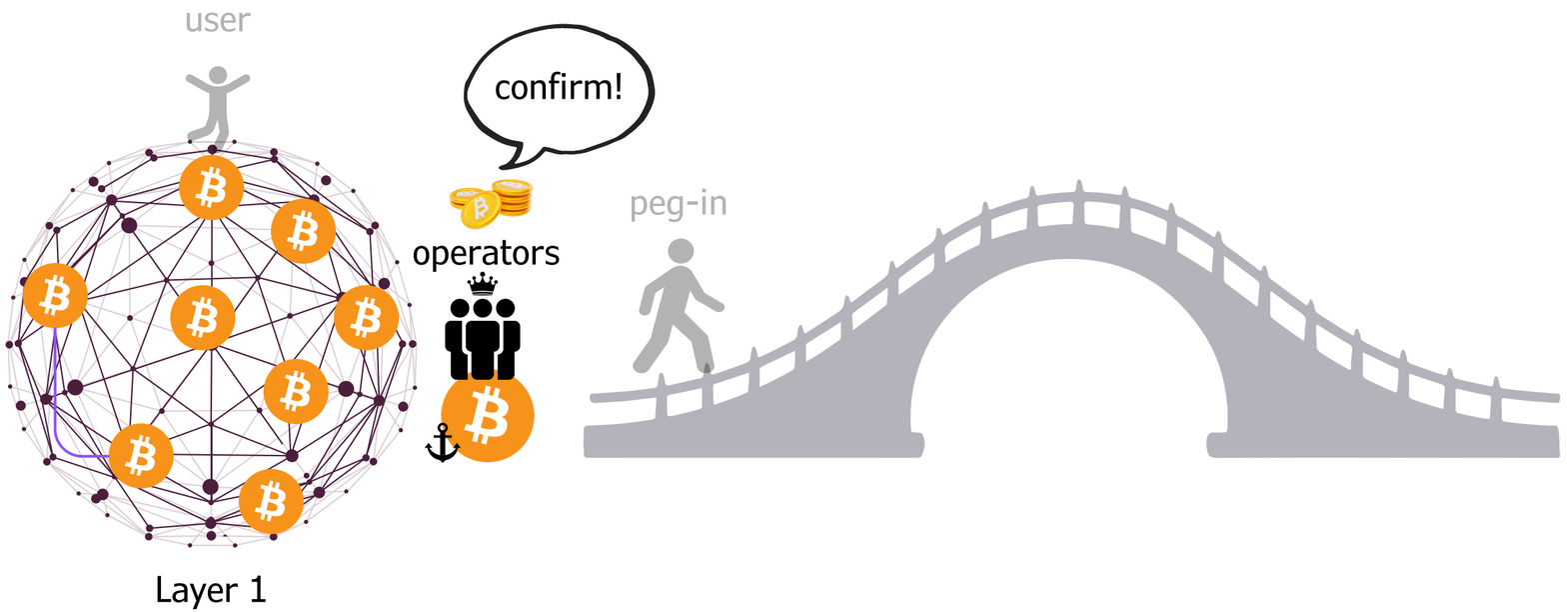






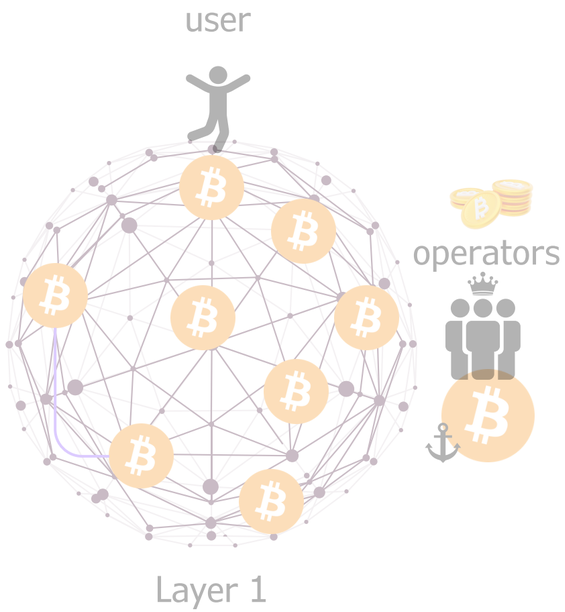
Peg-In

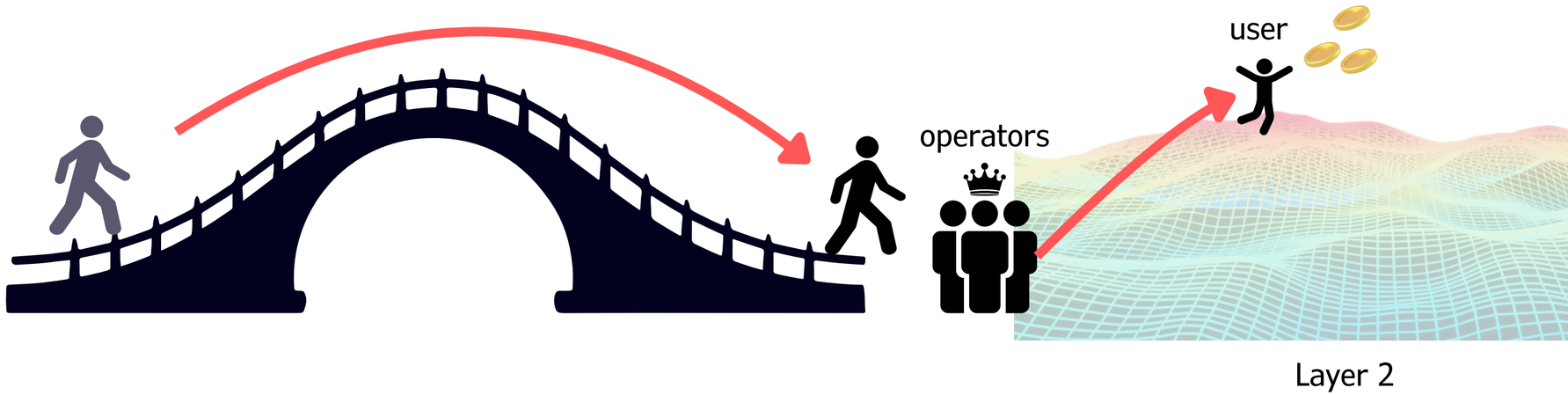
After the transfer, wait for the transaction to be well confirmed.



Peg-In

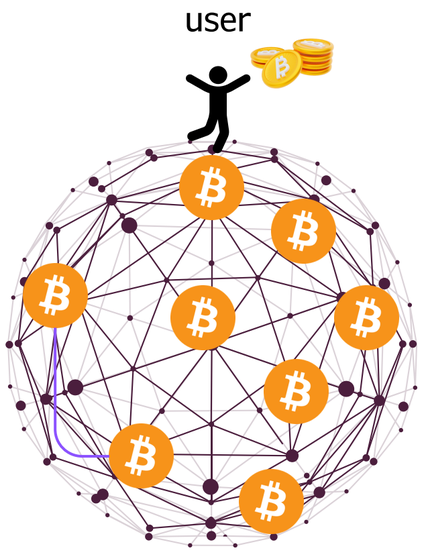
Once the operators confirm that the L1 funds have been locked, the funds will be sent to the L2 users.



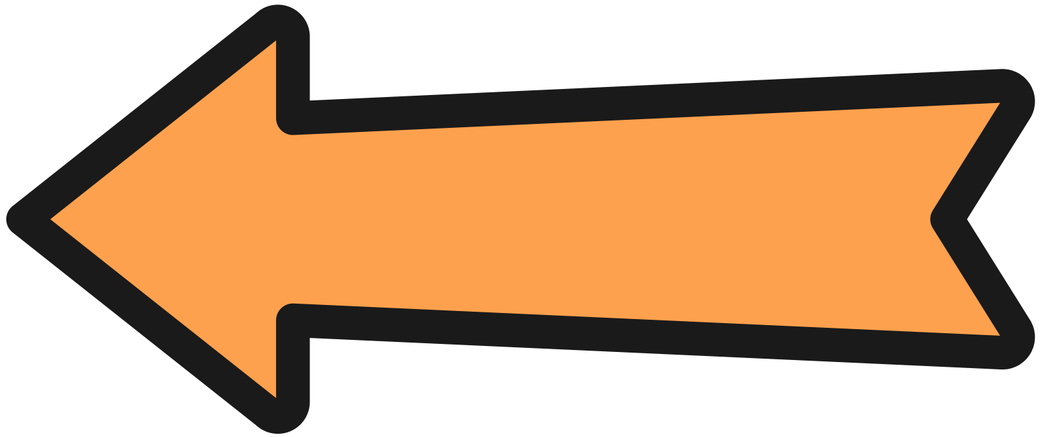


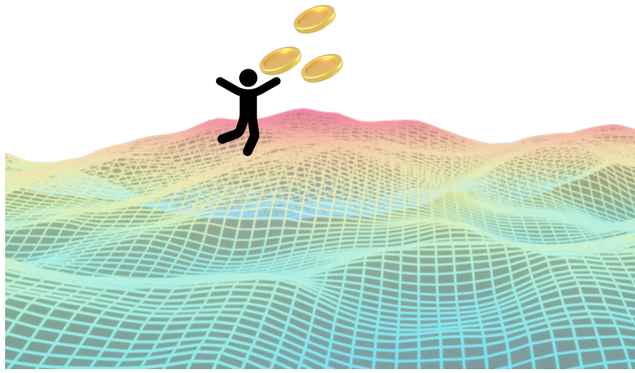
Peg-Out

A peg-out transfers L2 funds back into L1.



Layer 1



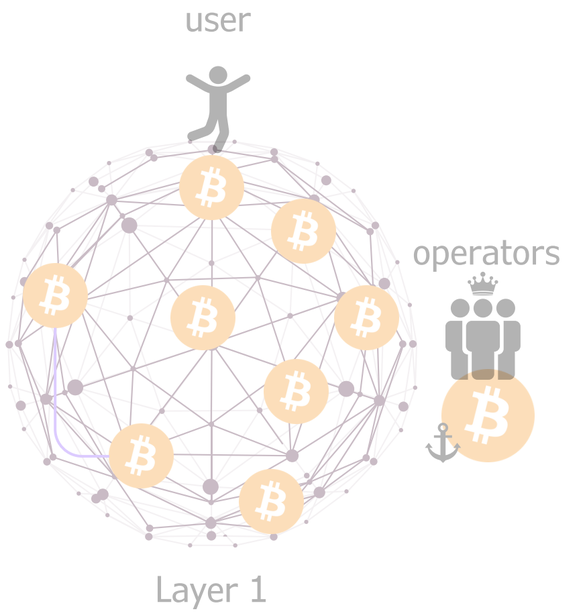


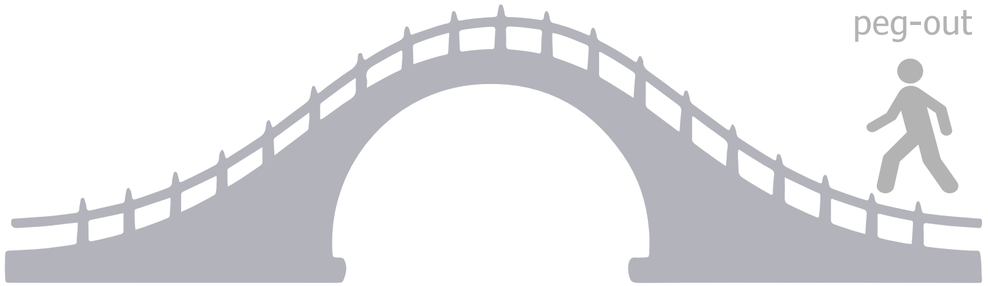
Layer 2

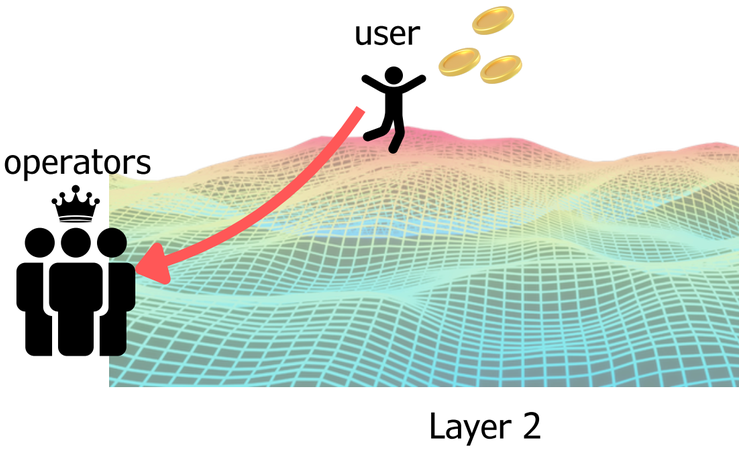
Peg-Out

Users transfer funds to the burn address on Layer 2.

And the operators wait until the transfer is approved.







Peg-Out

The Bitcoin will be refunded to the user from a wallet managed by the L1 operator. Like Rollup, there will be proof and verification that the L2 user has burned the funds.



BitVM bridge

BitVM is a project that aims to bring Ethereum-like functionality to Bitcoin scripts. The proof mechanism is Optimistic Rollup.

A bridge using BitVM is also being considered.

