BITCOIN LAYER 2 ECOSYSTEM

基礎編

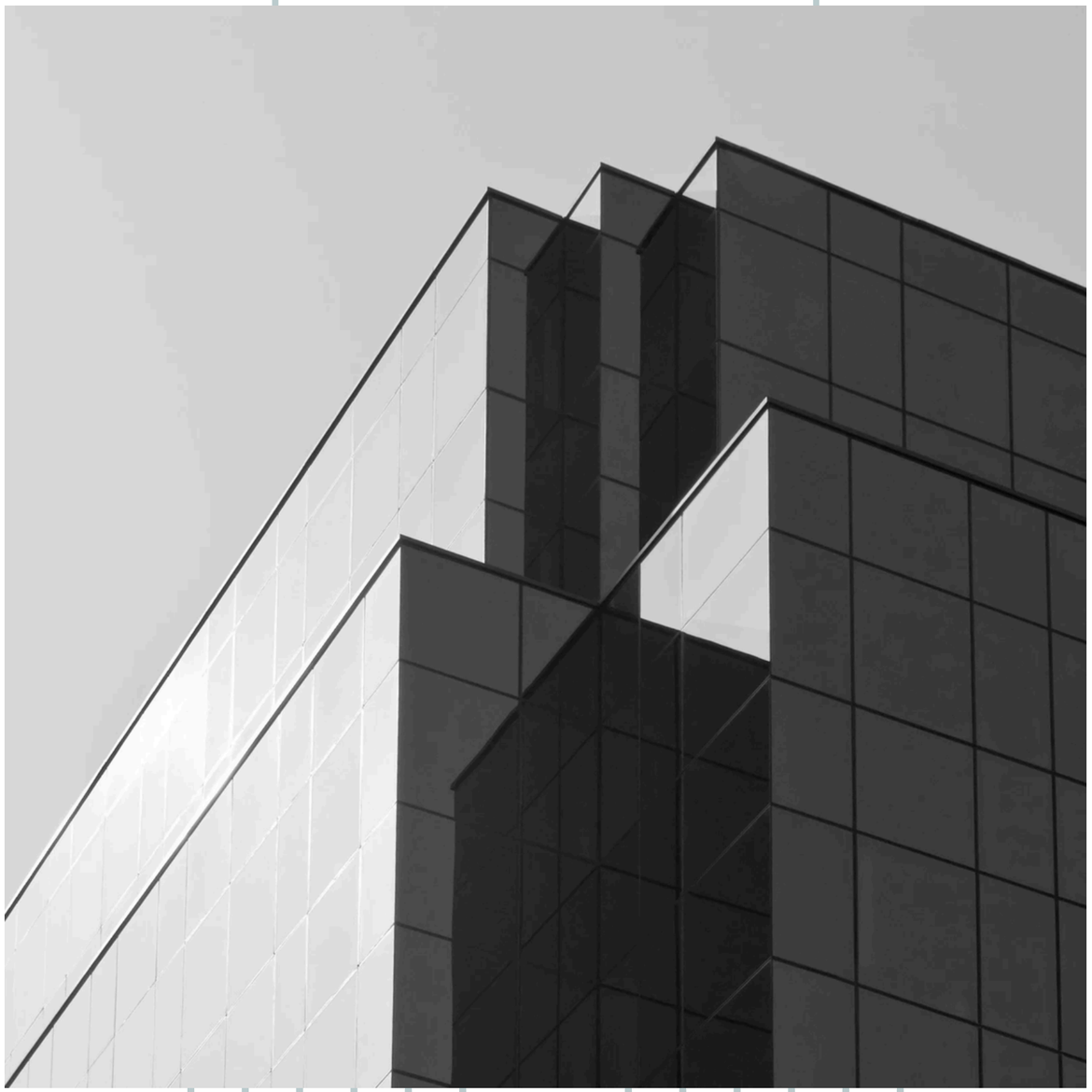
MAY - OCTOBER, 2025

本資料は、我々の内部資料を外部公開用に翻訳したものです。翻訳に一部不自然な箇所がございますが、情報の共有を優先しております。何卒ご了承ください。

主な方式

・State Channel方式
・Sidechain 方式
・Rollup方式

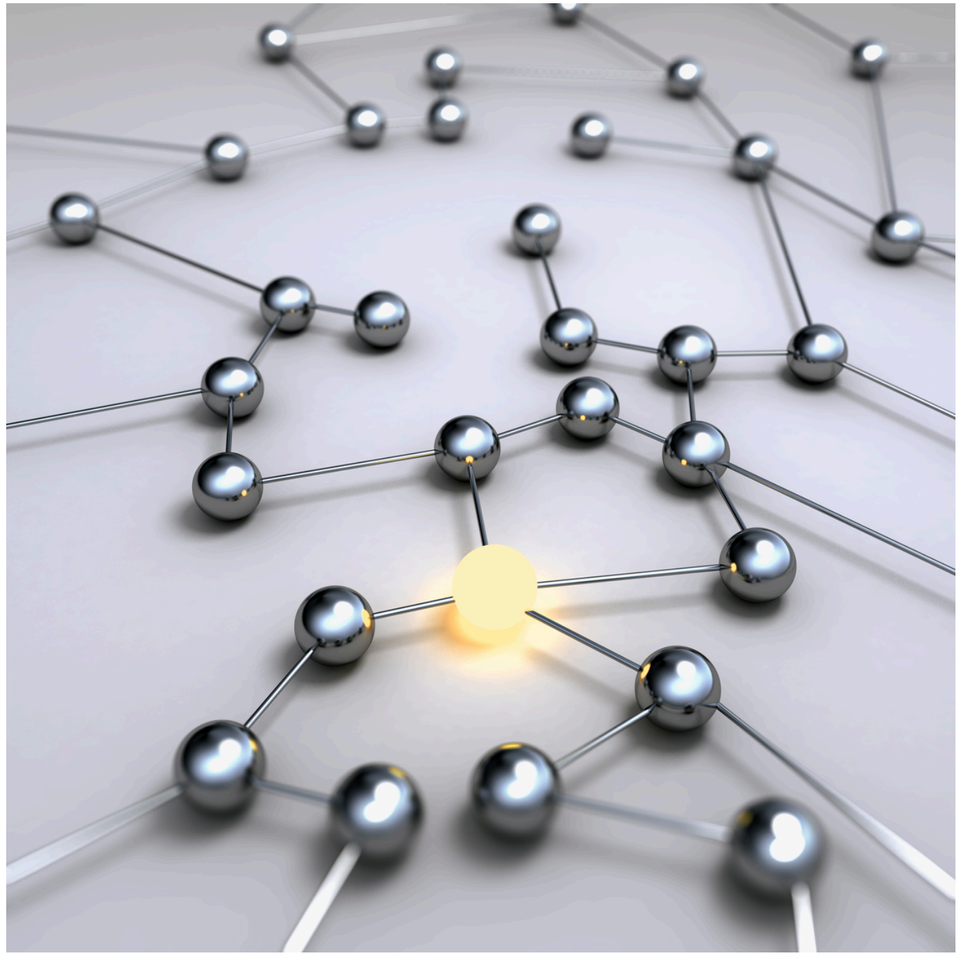
ただしこれ以外にも方式はいろいろある。単純にどれかの方式に当てはまるというプロジェクトは少ないだろう。



State Channel

State Channel方式は、二者間で作ったチャネルをオフチェーンで管理します。

この方式ではLightning Networkが有名です。



Sidechain

Bitcoinとは別のチェーンを運営し、
Bitcoinとは主にブリッジでのみつながります。
L2の自由度は高いですが、セキュリティはL2の検証者に依存します。

RootstockやLiquidがこのタイプです。



Rollup

Rollup方式もSidechain方式のようにBitcoinとは別にチェーンを作ります。複数のトランザクションをまとめて処理して、その処理を検証できるデータをL1に保存します。

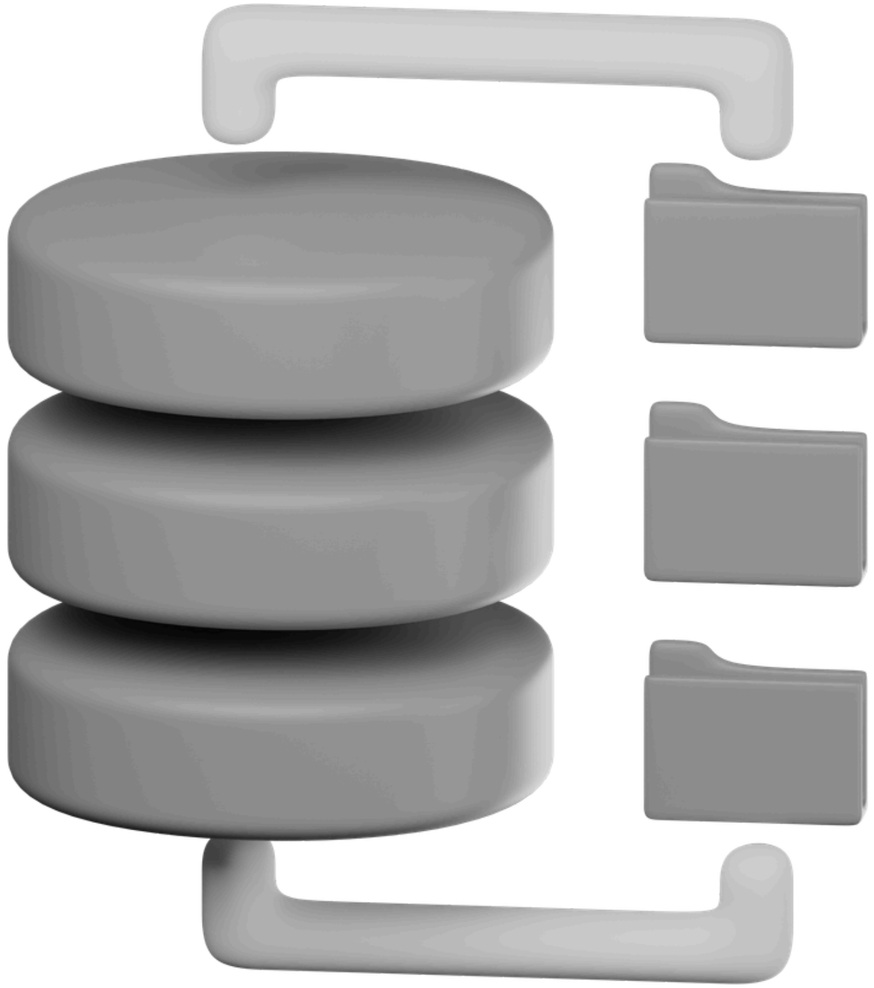
この方式はCitreaやBitlayerなどいろいろあります。



DA Layer

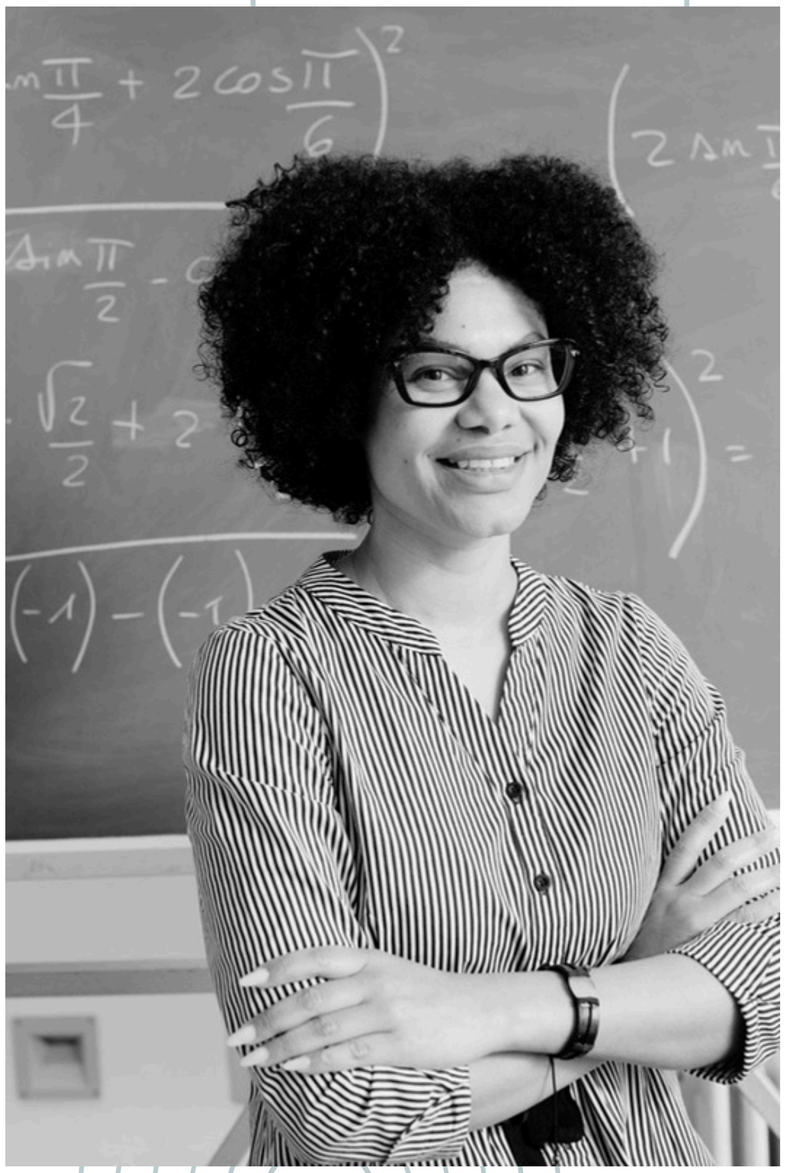
L2の状態を検証するデータを保存しておくストレージが必要です。Data Availability Layer(DA層)と呼ばれます。

Bitcoin L2の場合はBitcoin L1に保存することが多いです。



Sovereign Rollup

Bitcoinスクリプトでは複雑な計算ができないため検証はオフチェーンで行うのがほとんどです。
検証自体はオフチェーンで行ってその証明データだけをDA層に書き込む方式を Sovereign Rollup と呼びます。
Bitcoin L2で zkRollupと呼ぶ場合は、zk-proof データを用いた Sovereign Rollup であることがほとんどです。



証明メカニズムの違い

Optimistic Rollup	不正があれば正直な誰かが「チャレンジ」する
zkRollup Validity Rollup	ゼロ知識証明などの暗号学的手法で証明する

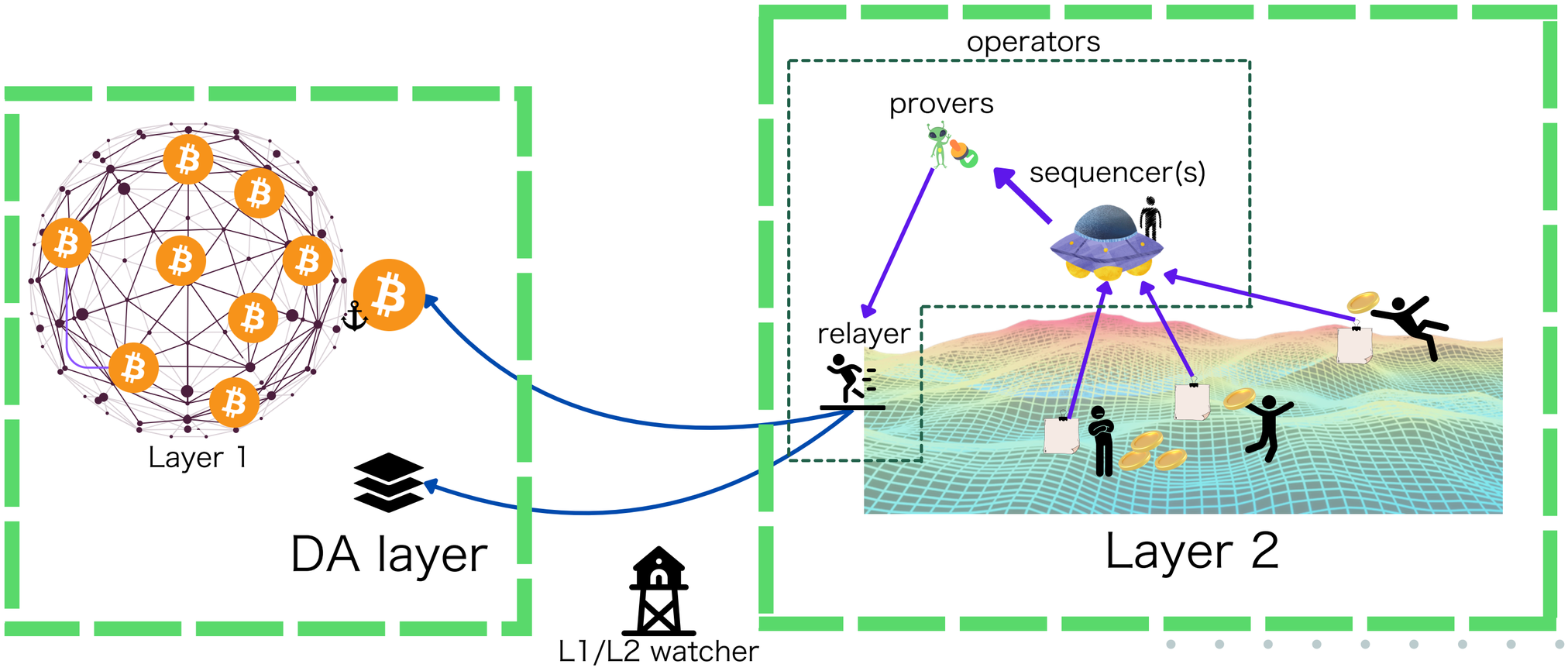
主権性

Sovereign Rollup	L2は独自に動作し、L1はデータ可用性(DA)のみ
Smart Contract Rollup	L2の状態をL1のスマートコントラクトが制御・検証



Rollup Structure

プロジェクトによってところどころ違いはありますが、おおよそこれらの要素があります。DA層はほとんどの場合L1と同じですが、この図では別にしています。



Transaction

L2上で送受金するとトランザクションデータが作成されネットワーク上に展開されます。

provers



sequencer(s)



relayer





Layer 1

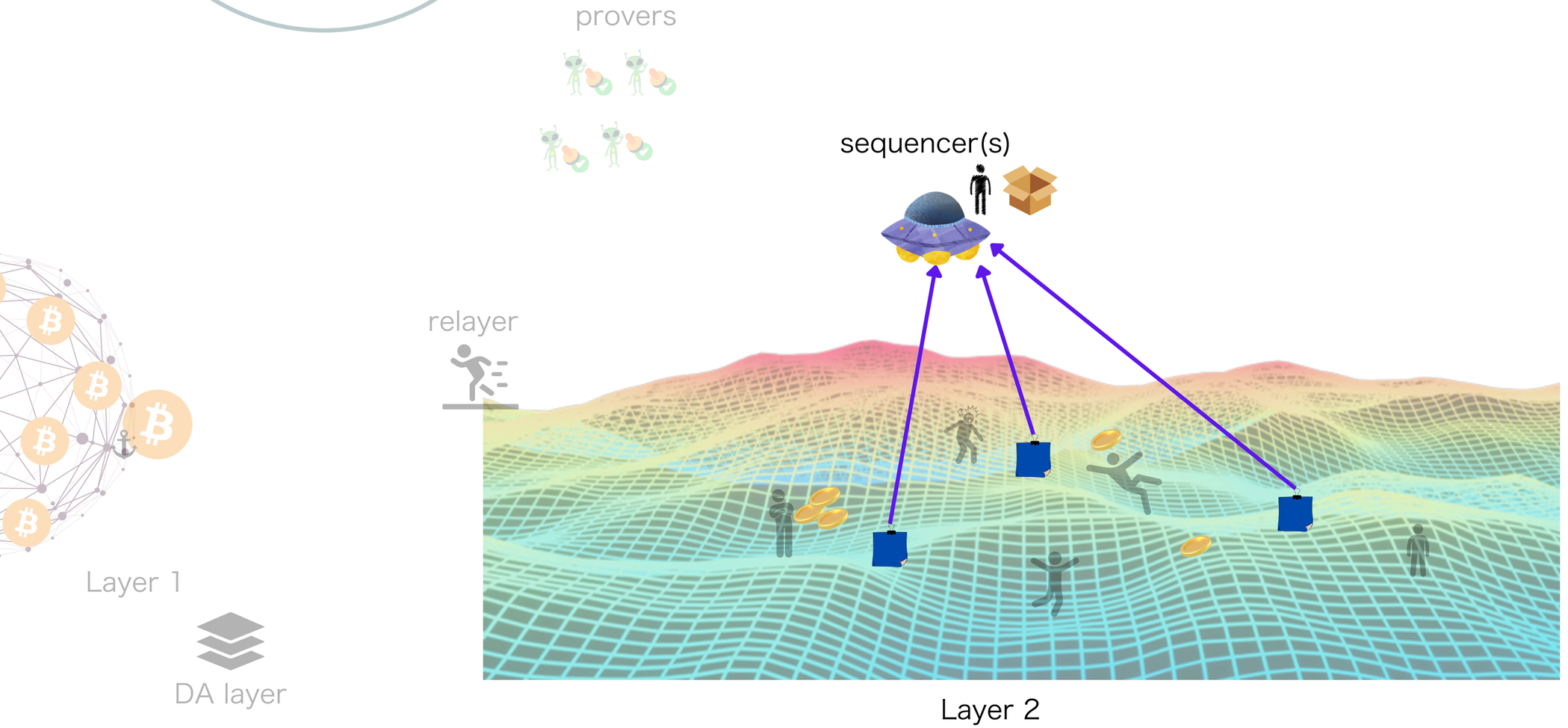


DA layer

Layer 2

Sequencer

トランザクションデータはSequencerが受け取ります。



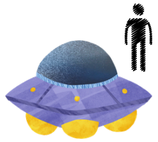
Sequencer

Sequencerはトランザクションに順番を付け、ブロックを作ります。
また、アカウントの残高などのステートを更新します。

provers



sequencer(s)





relayer





Layer 1

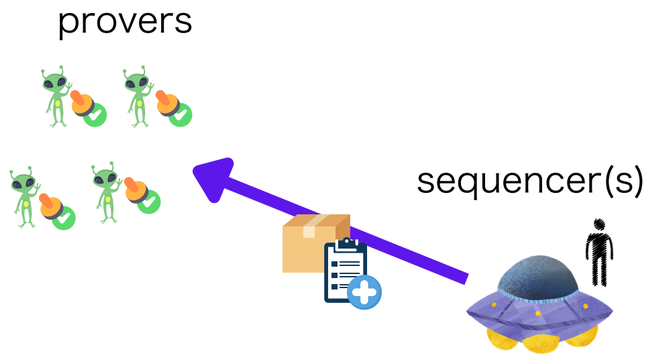


DA layer

Layer 2

Sequencer

生成したブロックデータとステートの差分データを
Proverに送ります。

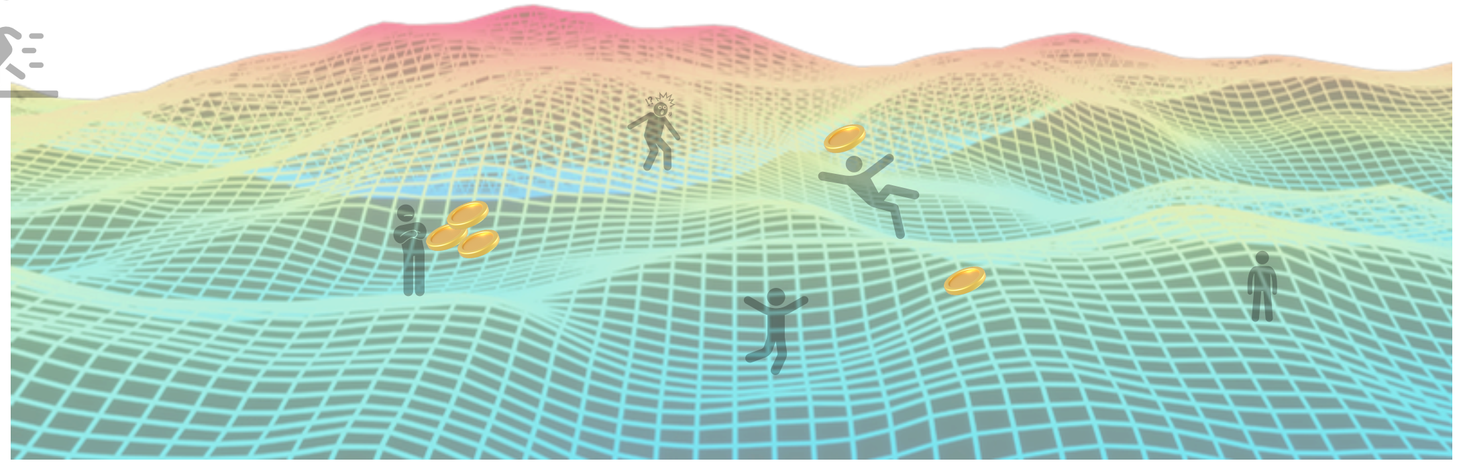




Layer 1

DA layer

relayer

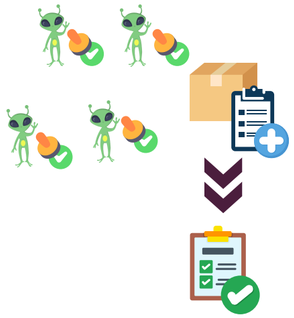


Layer 2

Prover

Proverはステートの変化が正当であることを確認し、それを証明するデータを作ります。

provers



sequencer(s)



relayer



Layer 2



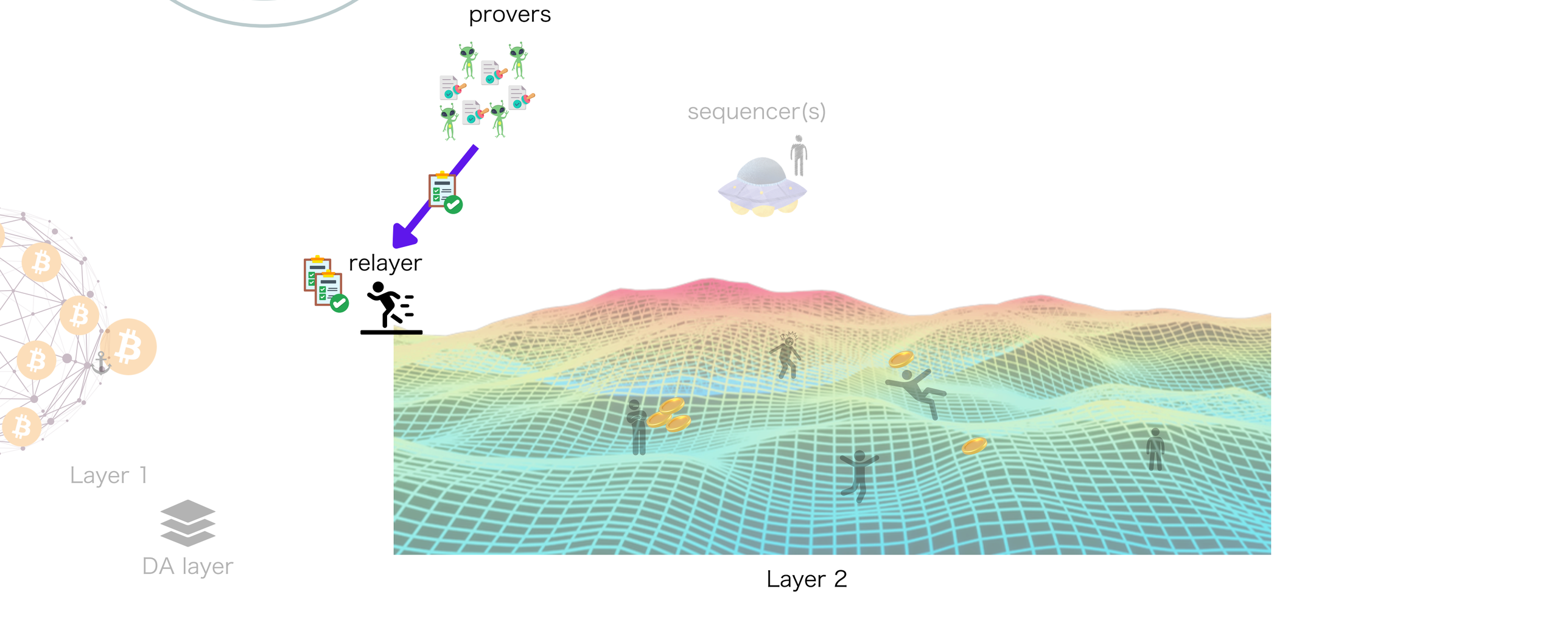
Layer 1



DA layer

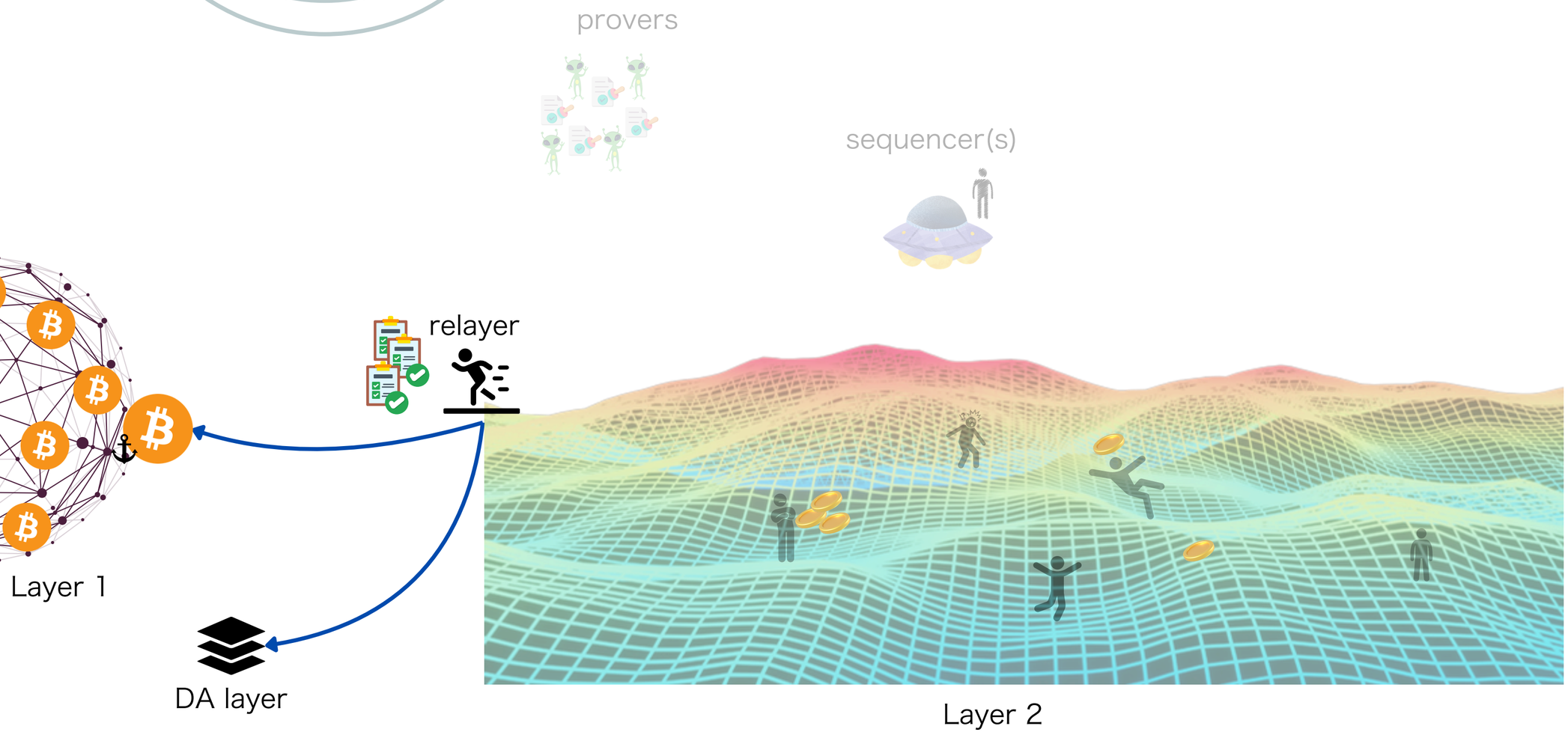
Prover

Proverは証明を作成してRelayerに渡します。



Relayer

Relayerは証明データをある程度まとまってからDA層に保存します。



Verifier

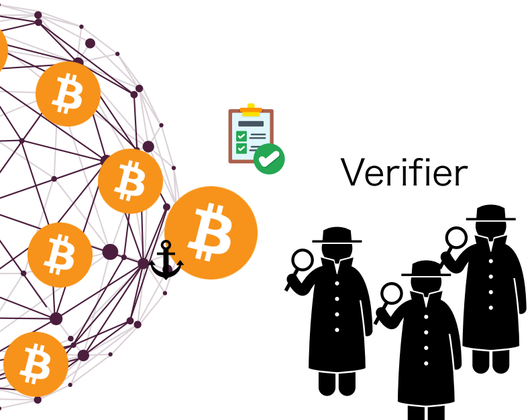
DA層に書き込まれた検証データをVerifierたちが検証します。
検証によって不正が発見された場合、資金が没収されるなどの
ペナルティが与えられます。

provers



sequencer(s)





Layer 1

Verifier

DA layer



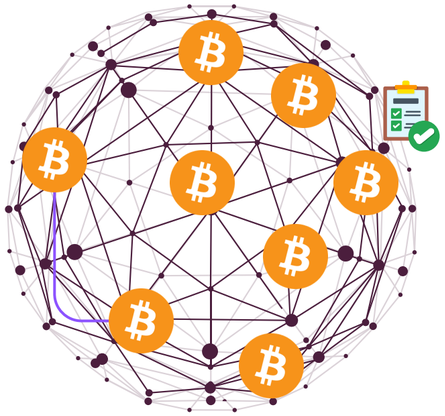
relayer



Layer 2

Verifier

Bitcoinスクリプトでは検証できないので、アプリで検証し、データが不正であれば申告する。それがOptimistic Rollup 方式である。
「楽天的(optimistic)」である理由は、不正を申告する人が誰もいなければOKとみなすからである。



Layer 1



Verifier



DA layer

- 検証に1人以上の正直な人がいないといけない
- 不正を申告するための期間をある程度とらないといけないので完了に時間がかかる
- 不正申告に対する証明はL1のトランザクションとして展開することになるため、それは運営側のコストになる。

BRIDGE

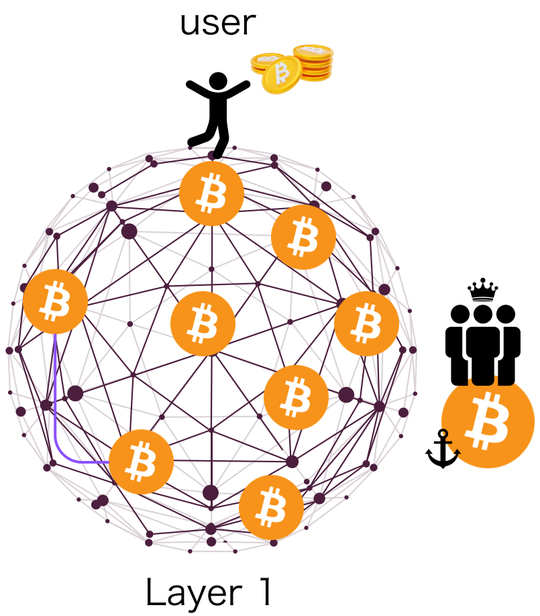
Bridge

ブリッジは異なるチェーン間でトークンの交換を行う機能です。
ユーザーが要求したL1資金を運営者がロックしてL2でのトークンを発行します。またユーザーL2でトークンを運営者に返してL1に資金を戻します。

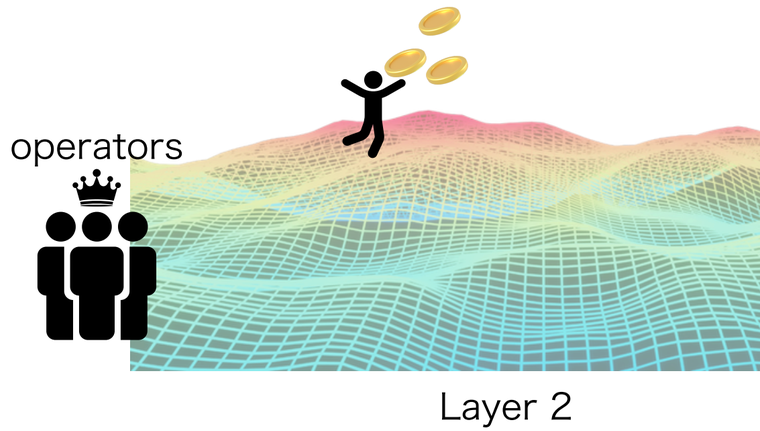


Bridge

L1で資金をロックしてL2に入金したり、
L2で焼却させてL1に戻したりします。
ブリッジはその運用者を信用したしくみになる傾向があります。





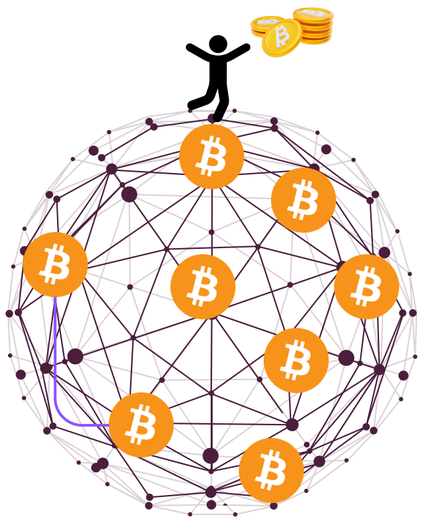




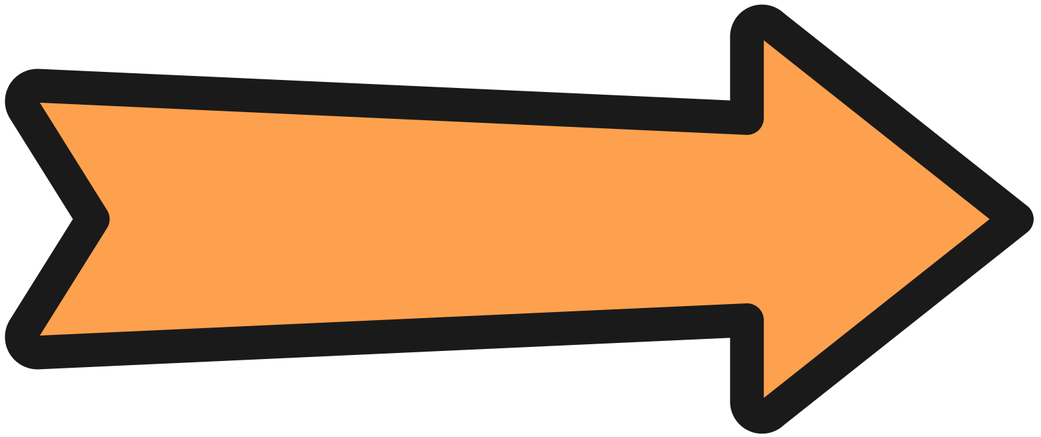
Peg-In

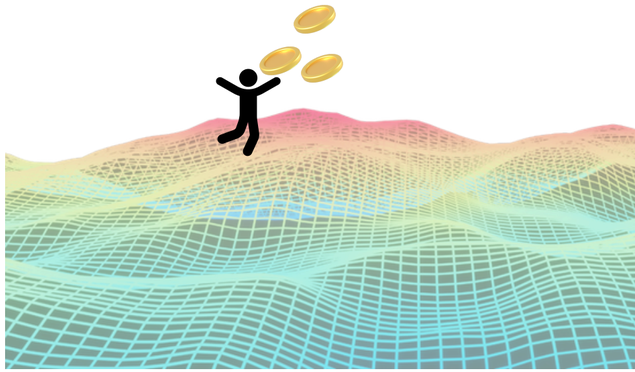
peg-in は L1 から L2 への入金です。

user



Layer 1

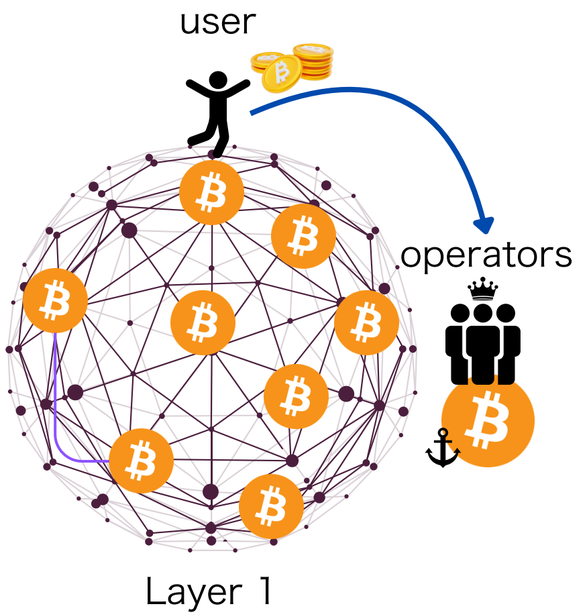


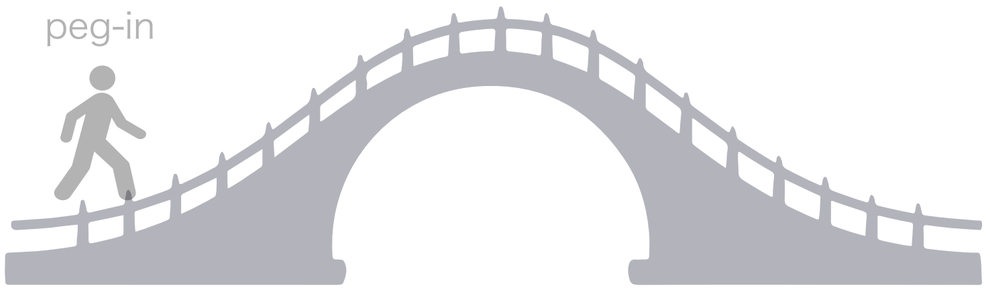


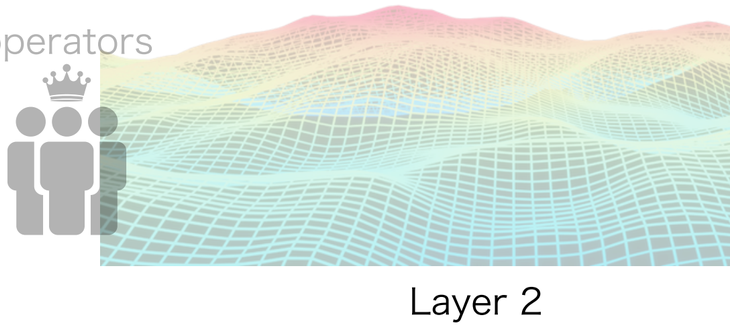
Layer 2

Peg-In

L1上でユーザーが管理者のアドレスに送金します。
(マルチシグアドレスがしばしば使われます。)





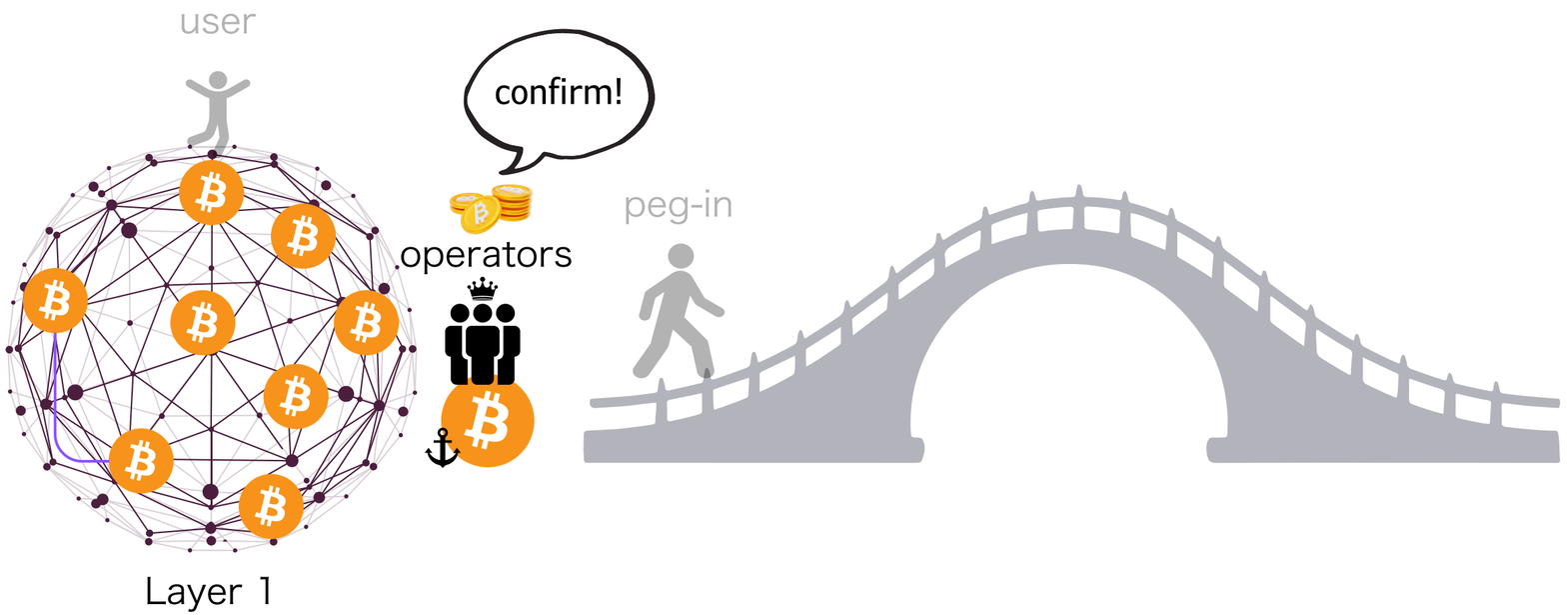




L1/L2 watcher

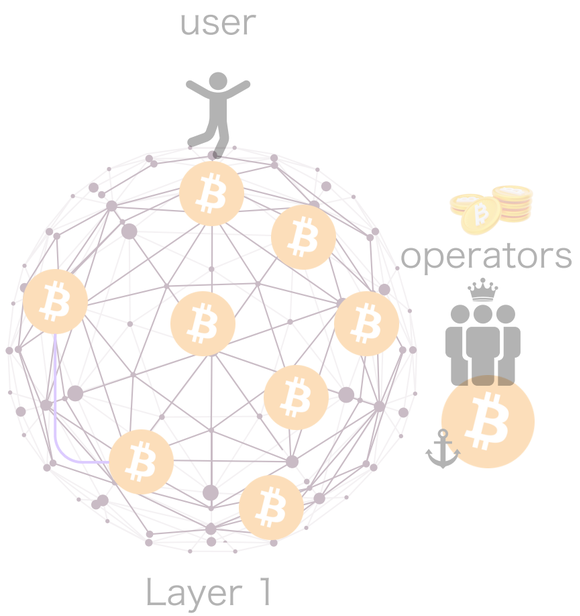
Peg-In

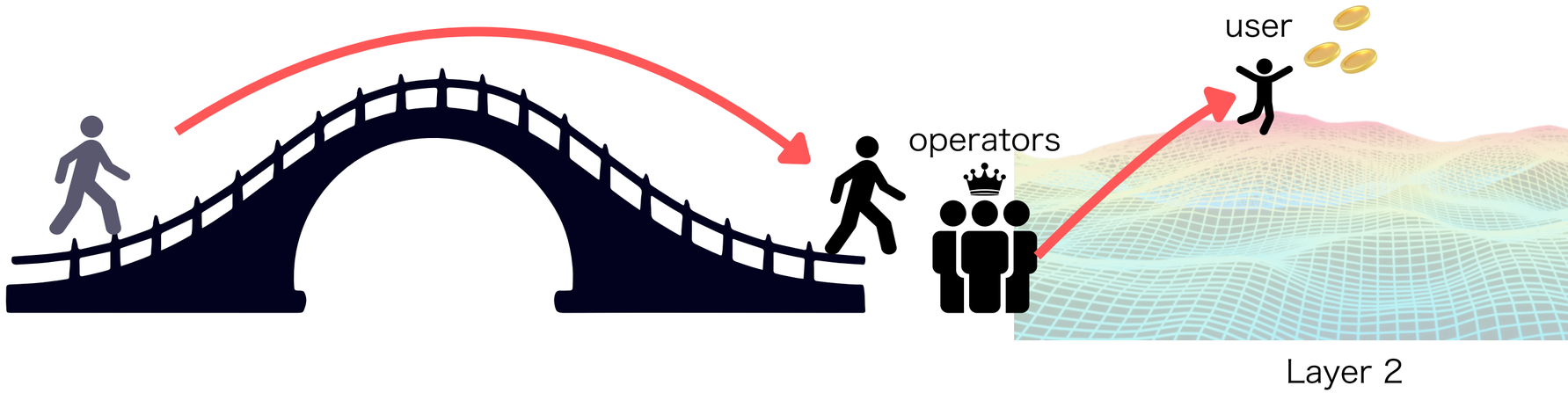
送金後、承認されて十分安定するまで待ちます。



Peg-In

運営がL1の資金がロックされたことを確認するとL2側のユーザに資金が送られます。



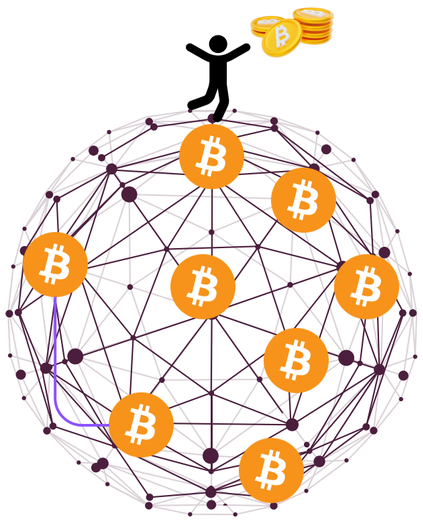




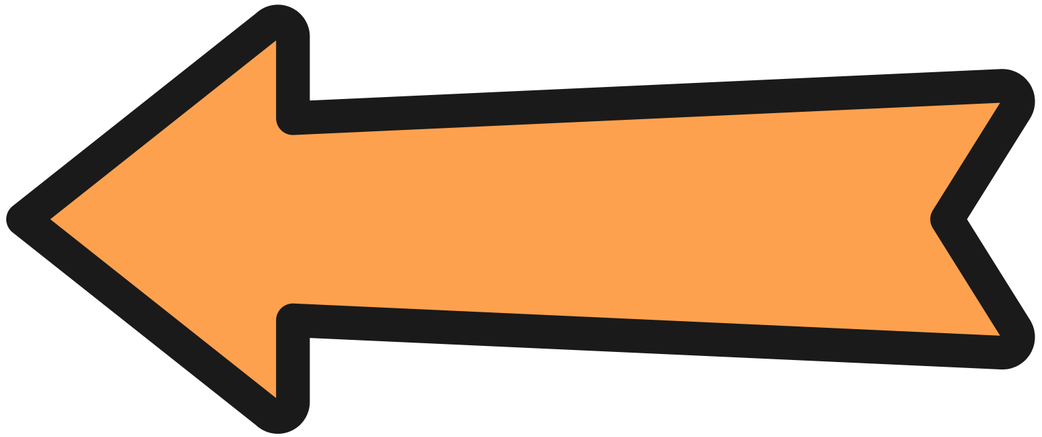
Peg-Out

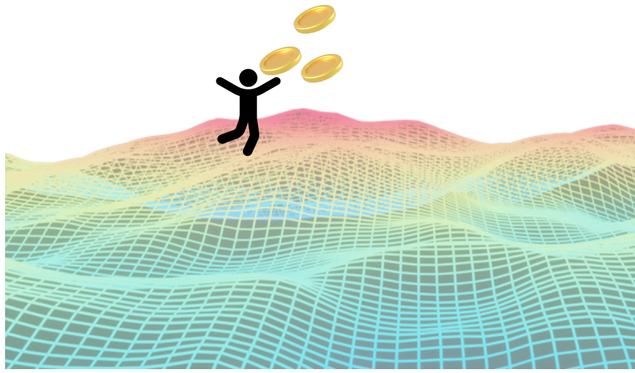
peg-out は L2 の資金を焼却して L1 に戻します。

user



Layer 1

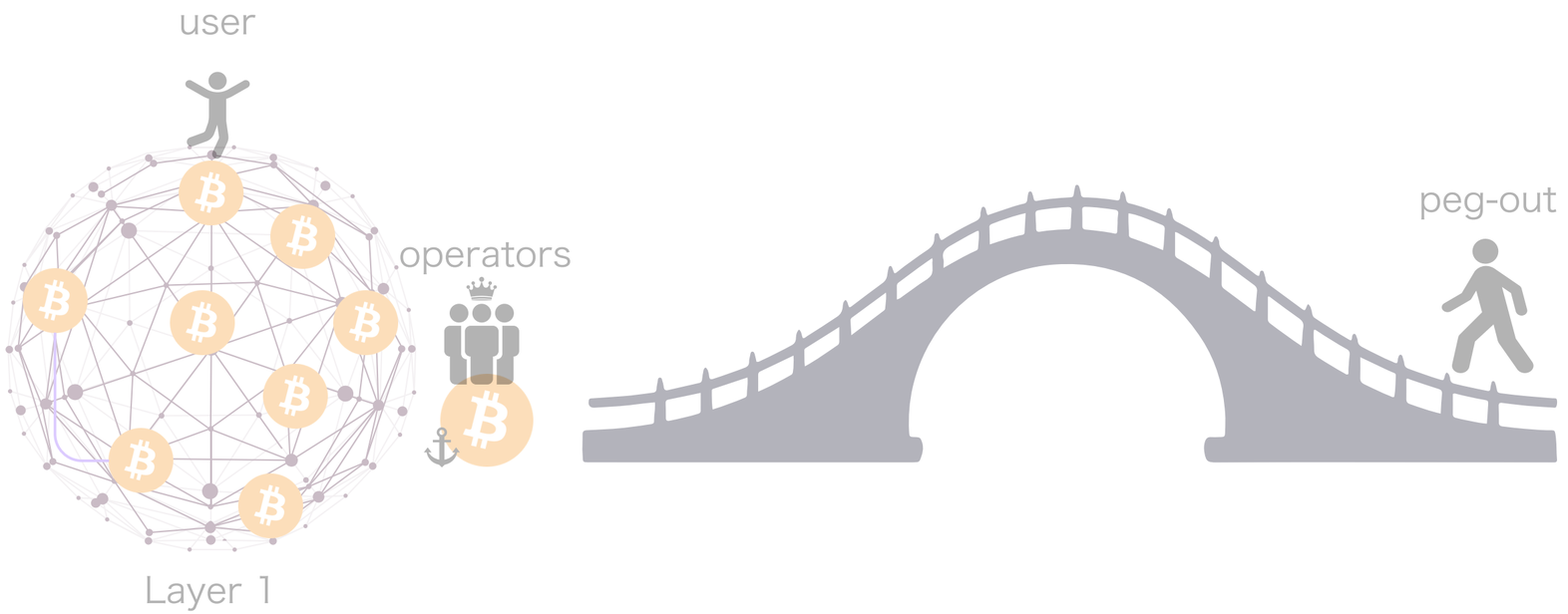




Layer 2

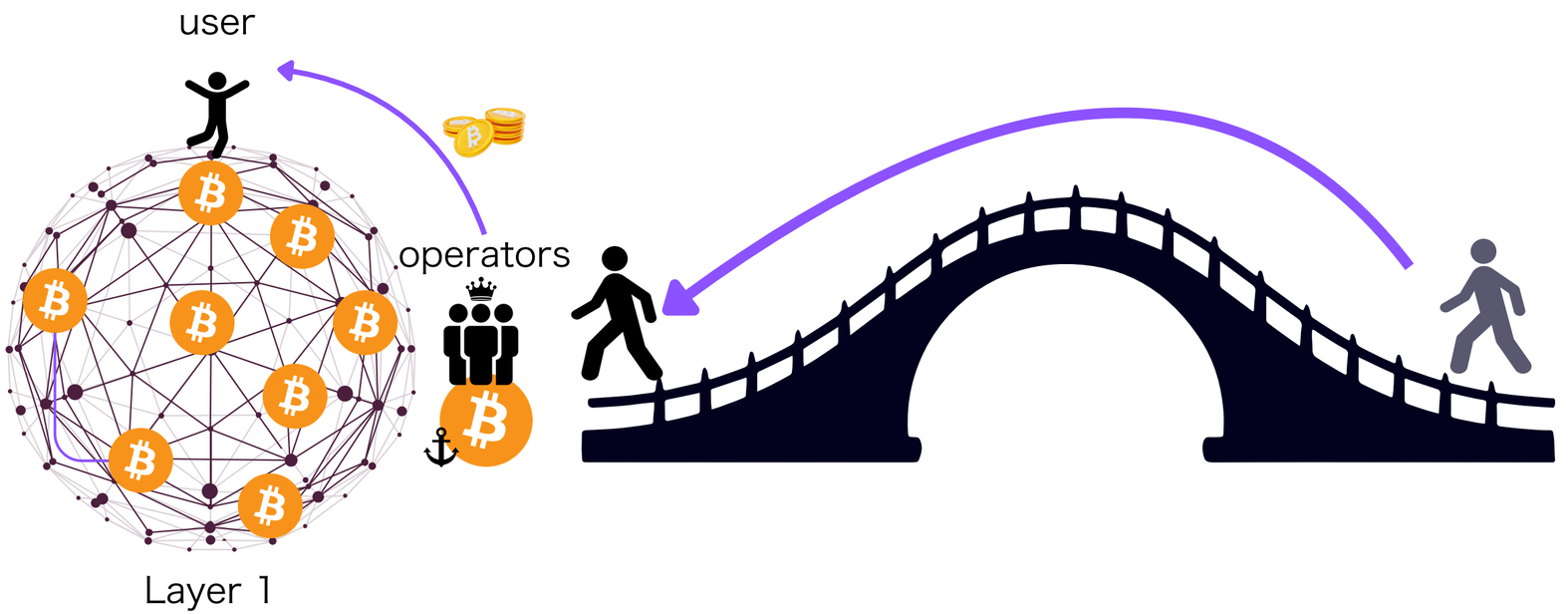
Peg-Out

ユーザーはL2上で焼却用のアドレスに送金します。
運営者はその送金が完了したことを確認できるまで待ちます。



Peg-Out

L1側のOperatorが管理するウォレットからユーザにBitcoinを払い戻します。
Rollupのように、L2側のユーザが資金を焼却した証明や検証が行われるでしょう。



BitVMブリッジ

BitVMはBitcoinスクリプトにEthereum並の機能を使えるようにしようとしているプロジェクトです。
証明メカニズムはOptimistic Rollupです。

BitVMを利用したブリッジも考案されています。

