Starknet - Bitcoin L2

#BitcoinL2



- 公式
  - Documents
- X
  - Starknet
  - Starknet Foundation
  - Startnet Japan
- リポジトリ
  - https://github.com/starkware-libs
    - Starknetが運用
    - CairoやSTWOなど
    - sequencerがフルノード？
  - https://github.com/Bitcoin-Wildlife-Sanctuary/scrypt-poc-bridge
    - `OP_CAT` のPoC(2025年2月くらい)
    - sCryptという、JavaScript風のプログラムをBitcoinスクリプトに変換するツールを使っている
  - https://github.com/keep-starknet-strange
    - おそらくStarknetが運用している
    - shinigamiは Cairo で Bitcoinスクリプトを実行するライブラリ

Starknet - ChatGPT

STRK PoS - ChatGPT

かいつまむ

- 2025年5月の段階では、 `OP_CAT` が動くsignetでのPoCが動いた
- Bitcoin に `OP_CAT` が取り込まれるかどうかは未定
- マルチシグでのフェデレーション方式とBitVM方式を進めている(並行して？)
- ファウンデーションを立ち上げた(前からあったのかもしれない)
- Starknet walletから Bitcoin を持たずに Inscription を刻むbroly というPoC を作った(blog)

https://github.com/keep-starknet-strange/broly

こんなこともできますよ、ということだろうが、

概要

StarkWare社が中心になって開発しているL2技術。Rollup系である。



zk-Rollup技術の中でもStarkWare社のzkSTARKを採用している。

Ethereum向けには既に稼働している。

ロードマップにはBitcoinのことは書いていないようだ(BitcoinともEthereumとも書いていない)。

Starknet 上でのスマートコントラクトは Cairo VM で動作する Cairo 言語(Rust風)である。

- CairoはStartnetやStarkExチェーンで使われている
- ZKP向けになっているそうだ
- Cairoで書かれたスマコンをEVMやBitcoinスクリプトに変換するのではない。Cairo VMで実行して計算の正当性を表す証明(STARK証明)を生成し、それをL1のスマコンなりBitcoinスクリプトなりによる Verifier によって確認されるということになっている。
  - Ethereumでは既に Verifier はスマコンになっている

What is Starknet: A Scalable Layer 2 Network for Ethereum

- EthereumからStarknetにデポジットして、終わったらウィズドローする、というのはLightning Networkと同じ。
  - EthereumのL2
- StarknetはEthereumとBitcoinの両方に同時に決済できるL2になることを目指している。
  - デュアルファイナリティ
    - BitcoinとEthereumの両方で同様の最新の状態を持つことを目指している
  - BitcoinとEthereumの資産を組み合わせて利用できる可能性がある
    - Bitcoinで取引を開始し、Ethereumで取引を完了し、最終的にBitcoinとして残高を得る、など。
  - Starknet内でのやりとりはトークンである STRK を使用されることがある(必ずではなく？)
    - デポジットするときに STRK を購入するイメージになるんだろうか？

Starknet on Bitcoin and Ethereum : 2025/03/11

- StarkNetは、Ethereum上での実績を活かし、Bitcoinのスケーラビリティと機能性を向上させることを目指しています。

1. EthereumとBitcoinの統合

   Starknet は Bitcoinと Ethereum の両方に対応する(両チェーンを単一レイヤーで統合する)

2. Bitcoinの課題とStarkNetの解決策

   STARK証明を使ってBitcoin上で複雑なアプリを実行できるようにする



3. ブリッジング手法の検討

   マルチシグベースのブリッジ

   `OP_CAT` が採用されない場合の代替策としてBitVMを使う

   `OP_CAT` の採用

4. エコシステムの拡大

   ウォレットを通じたLNとの連携も考えている

ブリッジ実装への取り組み(`OP_CAT` の代替策ともいえる)

   フェデレーテッドモデル(マルチシグ)

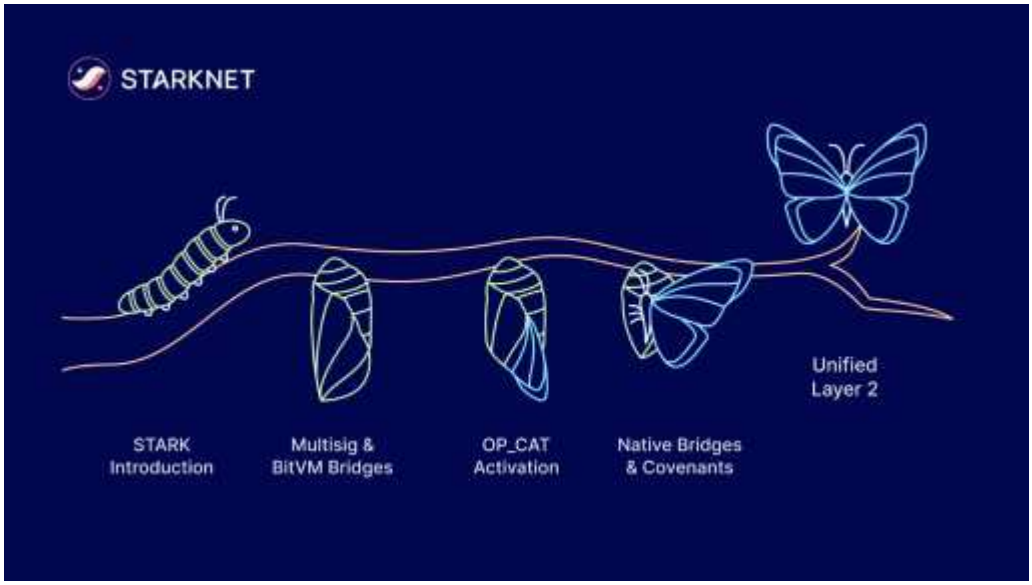
      共同署名者のグループがマルチシグを通じてStarknet上にロックしてmintされたBitcoinトークンを共同で保護する

      フェデレーションはブリッジされた量と同僚の wrapped Bitcoin を Starknet上にmintする責任を負う

      マルチシグブリッジは手数料の削減とUXの向上はあるものの、署名の大多数が誠実である必要があるので livenessが制限される(署名に時間がかかるので時間がかかることを言いたい？ 誠実な人を見つけるのが大変？)

   BitVM

      マルチシグの代わりに BitVMを使用すると、オペレーターの一人だけが正直であることを要求される



マルチシグやBitVMの研究をしている間に `OP_CAT` がアクティベートされるという目論見だろう。

用語: Cairo

https://github.com/starkware-libs/cairo

Starknet の VM 名(Cairo VM)でもあり、そのスマートコントラクトの言語名(Cairo言語)でもある。

用語: STWO ステュー

StarkWare社が開発中の次世代STARKプロバー（証明生成器）です。

現在は Cairo 向けの "SHARP" で、次世代が Cairo2 向けの "STWO"

StarkNetやStarkExの根幹にあるzk-STARK技術の性能・柔軟性を大幅に向上させることを目的としています。

特徴

zk-STARK証明の生成（プローバー）をより速く・汎用的に行う

1. 性能向上

   より効率的な証明生成により、計算コストを削減し、大規模DAppにも耐えうるスケーリング性能を実現。

2. マルチステップ証明（Recursive Proofs）

   「証明の証明を生成する」仕組み（recursive proofs）に対応し、複数ステート変更を一括で証明するなど、高度な構造が可能。

3. 柔軟なインフラとの統合

   Ethereumだけでなく、将来的にはBitcoinとの統合にも対応できるよう設計されている。

NotebookLMによる調査

doc

StarknetでのEthereum送金は、Ethereumのレイヤー2（L2）ネットワークとしてのStarknetの仕組みに基づいて動作します。Starknetは、Ethereumのスケーラビリティの限界を克服し、Ethereumのセキュリティと分散性を維持するように設計されたValidity Rollupです 。

EthereumをStarknetに送金する基本的な流れは以下のようになります。

1. **デポジット（入金）**：ユーザーは、自身のEthereumウォレットからStarknetネットワーク上の自身のアカウントにETHをデポジット（入金）します。このプロセスは、通常、EthereumのL1上でのトランザクションを伴い、ブリッジと呼ばれる仕組みを利用します。「Atomiq brings wBTC to Starknet, enabling Bitcoin DeFi」という記事 にもあるように、オンチェーンエスクローとBitcoin PoW検証を用いたブリッジの例が示唆されていますが、Ethereumに関しても同様のブリッジング技術が用いられると考えられます。
2. **Starknet上でのトランザクション**：ETHがStarknetにブリッジされると、ユーザーはStarknetの環境内で、より低い手数料とより速いトランザクション速度でETHを他のStarknetユーザーに送金したり、Starknet上の様々な分散型アプリケーション（dApps）を利用したりできます 。Starknetはオフチェーンで多数のトランザクションを実行し、それらを単一のSTARK証明にまとめます 。
3. **STARK証明による検証**：オフチェーンで実行されたトランザクションのバッチは、STARK証明によってその有効性が証明されます 。このSTARK証明は、EthereumのL1（親チェーン）に送信され、そこで検証されます。STARK証明は、高いセキュリティを提供し、トラステッドセットアップを必要としないという特徴があります 。
4. **ウィズドロー（出金）**：Starknet上のETHをEthereumのL1に戻したい場合、ユーザーはウィズドロー（出金）のリクエストを行います。このプロセスもブリッジを介して行われ、Starknet上でのトランザクションと、それに対応するEthereum L1上でのトランザクションによって資金が移動します 。

Starknetの重要な特徴として、**Native Account Abstraction** が挙げられます。これにより、すべてのアカウントがスマートアカウントとなり、開発者はプロトコルレベルではなく、独自にアカウントの振る舞いを決定できます。これは、より柔軟なアカウント管理と、指紋認証や顔認証などのより使い慣れたログイン方法によるユーザーエクスペリエンスの向上に繋がります 。

Starknetは、Ethereumのセキュリティと分散性を維持しながら、**レイヤー2スケーリング** を実現し、**即時かつ安価なトランザクション** を提供することで、Ethereumの送金をより効率的に行うことを目指しています。また、StarknetはEthereumだけでなくBitcoinとも連携し、両方のチェーンを単一のレイヤーでスケールすることを目指しており 、将来的にはBitcoinとEthereum間のより容易でトラストレスな資産の移動も可能になる可能性がありま

す 。

DeepReseachによる調査

Google Docs

Starknetは、イーサリアムブロックチェーンのスケーラビリティ問題を解決するために設計されたLayer 2（L2）スケーリングソリューションであり、近年、その戦略的焦点をビットコインにも拡大している。

Starknetは、単なるトランザクションのスケーリングにとどまらず、複雑な計算処理をオンチェーンで可能にすることを目指しており、これにより従来は実現不可能だった新しいタイプの分散型アプリケーション（dApps）の登場を促す。

そのビジョンは、ビットコインの持つ信頼性（Integrity）とイーサリアムの持つ実用性（Utility）を組み合わせることで、新たなDeFi（分散型金融）体験を創出し 、最終的には世界最大の2つのブロックチェーンのための統一された、高度にスケーラブルな実行レイヤーとなることである。

Starknetのロードマップにおける最も注目すべき動きの一つは、イーサリアムに加えてビットコインの実行レイヤーにもなるという、野心的な戦略的転換である。

戦略の目標

ビットコインのスケーリング: ビットコインの現在のトランザクション処理能力（約13 TPS）を、Starknet上で数千TPS以上にスケールさせる。

ビットコイン上での表現力向上: Starknetを介して、ビットコイン上でこれまで不可能だった複雑なアプリケーションやスマートコントラクト（DeFiなど）を可能にする。

エコシステムの統合: イーサリアムとビットコインという二大ブロックチェーンエコシステムを、単一のL2上で接続し、流動性と機能性を統合する。

技術的アプローチや関連する動き

技術要素

ビットコイン上でのSTARK証明の検証、トラストレスなブリッジを実現するためのビットコインのソフトフォーク提案（OP_CAT）の推進、OP_CATが採用されない場合の代替案（BitVMなど）の検討、ビットコイン上でのスマートコントラクト機能（Covenants）を可能にするための研究（Collider-script/ColliderVM。

具体的な取り組み

StarkWareによる戦略的ビットコイン準備金（SBR）の保有と拡大、主要なビットコインウォレットXverseとの統合（BTCとSTRK間のクロスチェーンスワップが既に稼働）、ビットコイン関連プロジェクトを対象とした助成金プログラム「BTCFi Season」の開始、Braavosウォレットを介したビットコインLightning NetworkでのSTRK支払い対応、AtomiqによるwBTCのStarknetへの導入、OP_CAT研究への100万ドルの資金提供。

業界の反応

イーサリアム共同創設者ヴィタリック・ブテリンを含む業界の著名人からも、安全性の高いビットコインL2のアイデアに対する関心や支持が示されている。

しかし、この戦略の完全な成功は、ビットコインプロトコルのアップグレード（OP_CATなど）といった外部要因に依存する部分もあり、戦略的なリスクを伴う大胆な賭けであると言える。

まとめ

Starknetの強みは、その先進的な技術（特にSTARKの特性）、明確な長期ビジョン、開発者中心のアプローチ、そして完全な分散化への強いコミットメントにある。一方で、Cairo言語の学習曲線、EVM互換性を優先する競合との激しい競争、そしてビットコイン戦略の成功が外部要因（プロトコルアップグレード）に依存する点などが課題として挙げられる。

動作状況

現状(2025/4月)では、StarknetはBitcoinとのトラストレスなブリッジを作ることはできていない。

BitcoinのOP_CAT

PoCで `OP_CAT` が有効になった signet 環境でのデモは動いたそうだ。

2024/11/28 Implementing a Bridge Covenant on OP_CAT-Enabled Bitcoin: A Proof of Concept

ChatGPTによる概要

`OP_CAT` が有効な環境を作り、ドメイン固有言語(DSL)の sCryptを使って Bitcoin上に再帰的コベナント(recursive covenant)を実装している。

sCrypt はハッシュ関数の scryptとは違う。Bitcoinスクリプトを作るのと、それを展開したりスクリプトを解いて展開したりもできるようだ。TypeScriptで疑似スクリプトを書くので、そのテストができそう。

ブリッジのしくみ

再帰的コベナント：各トランザクションが次のトランザクションの構造を強制し、連鎖的に状態を更新するしくみ

Schnorr署名とOP_CATを使ったCovenants - Develop with pleasure!

OP_CATで実現するトランザクション間の状態遷移 - Develop with pleasure!

状態管理： `OP_RETURN` にアカウントデータの merkle root を格納することで状態の検証と更新を行う

入金や出金でブリッジは更新される

バッチ処理：複数の入出金を merkle tree にまとめてBitcoinトランザクションで展開

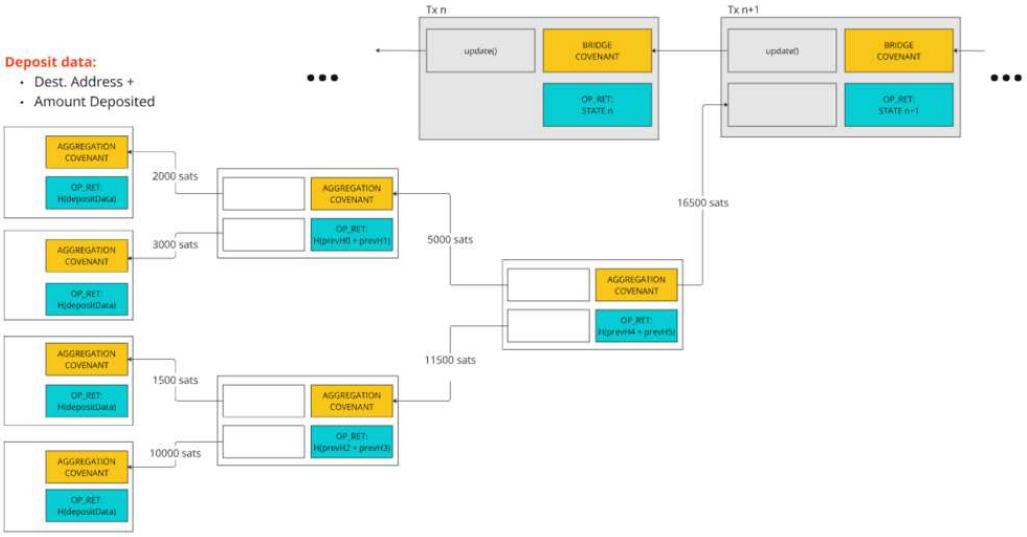
aggregation covenant と bridge covenant がある。

aggregation covenant から bridge covenant に入金している。

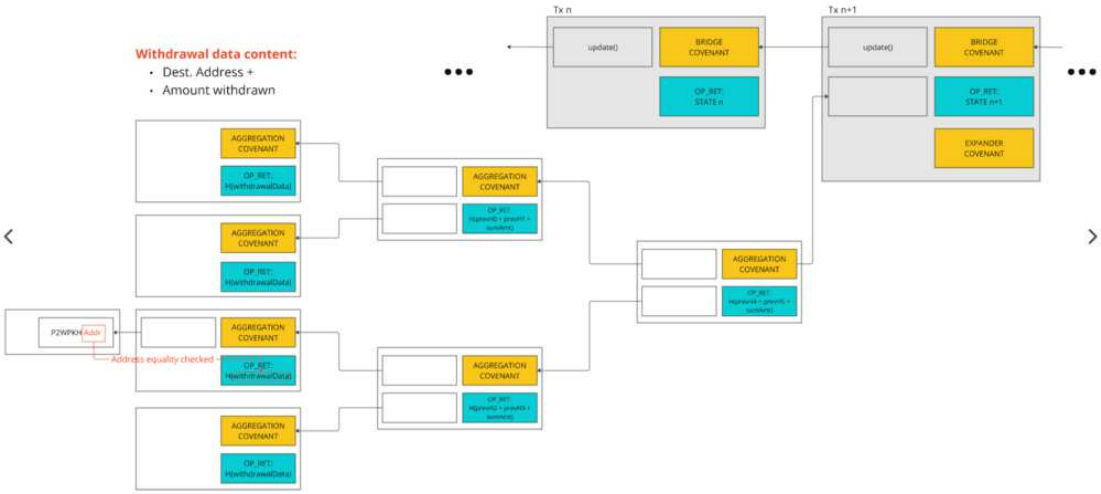
`OP_RETURN` の文字からすると、aggregation は merkle leaf、bridge は状態というところか。

入金は aggregation covenant の OUTPUT からしかできないようにしている？

merkle treeになっているが、1つしか INPUT がなければそれが merkle root になるのでこんなに面倒ではないか。



出金するアドレスは deposit tree のどれかのアドレスになるということをいっている？



GitHub

`OP_CAT` が有効になっている signet の `inquisition.taprootwizards.com` を使っている

`OP_CAT` だけではコベナンツは難しそう(BitcoinのOP_CAT#144301)だが、他の仕様を追加したような記述がない。

Operator を PoS で分散化

Operator を PoS で選定することで分散化させる計画がある。

https://www.neweconomy.jp/posts/435210