ETHTerakoya × Blockchain EXE

Rollupとは何か？

2021/02/04

Shuhei Hiya@Cryptoeconomics Lab

Cryptoeconomics Lab

Agenda

Rollupとは何か?

Optimistic Rollupとは何か？

Zk Rollupとは何か？

ORUとzkRUの比較

Products of ORU & zkRU

名前	特徴
Optimism(synthetix)	SolidityでSmart Contractが書けるORU
FuelCore	UTXO型のORU
Arbtrum	AVMという独自のVM。二分法的な紛争解決モデル
zkSync(curve, balancer)	スマートコントラクトプラットフォームを目指すzkRollup
zkSwap	zkSyncの技術を利用したAMM
Loopring	現在取引ボリュームトップのL2 DEX($10M ボリューム)
StarkEx, StartNet	Validium, Rollupプラットフォーム型

いまRollupを学ぶ意味

Rollupはリサーチから実用段階へ、そしてプラットフォーム化しようとしています。つまり実際にRollup上でアプリケーションを開発することが、可能な段階になって来ています。

今回は、「なぜRollupはEthereumのスループットを向上できるのか？」、その基本的な部分についてご紹介します。

特定のプロダクトというよりは、できるだけプロトコルの本質的な部分をご説明するような形になっています。

Agenda

Rollupとは何か?

Optimistic Rollupとは何か？

Zk Rollupとは何か？

ORUとzkRUの比較

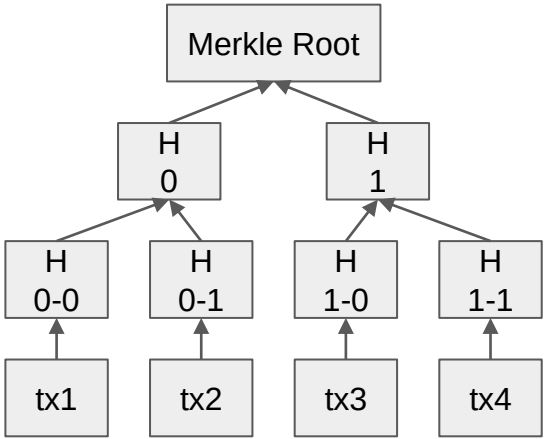
Why Scaling

Ethereumのキャパシティを増やすため

現在のEthereum
約 15 tps

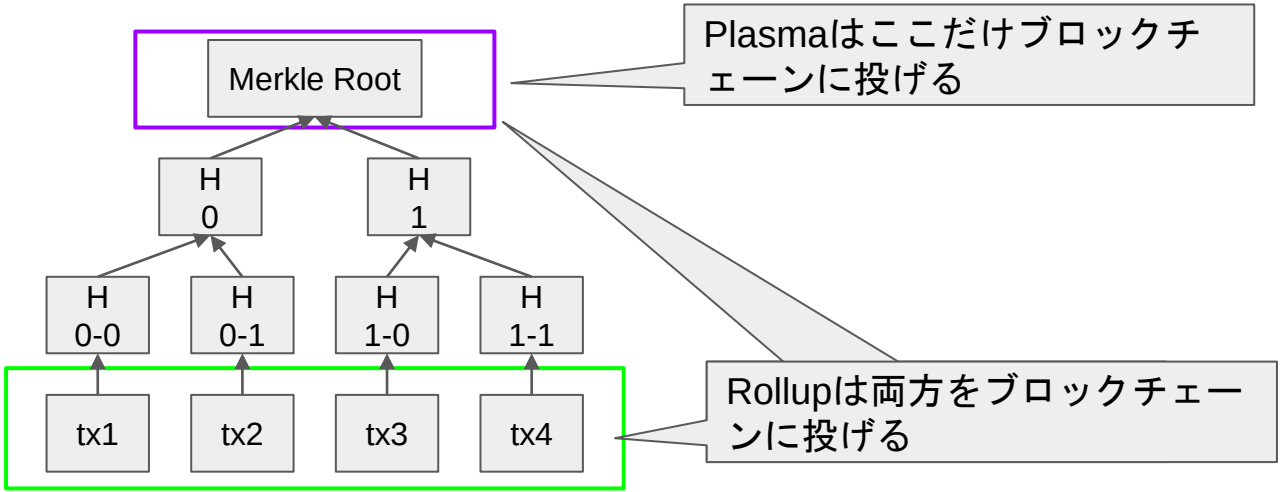
EthereumのLayer 2によるキャパシティ向上

トランザクションをブロックチェーンに送信するタイミングを減らす



What’s Rollup?

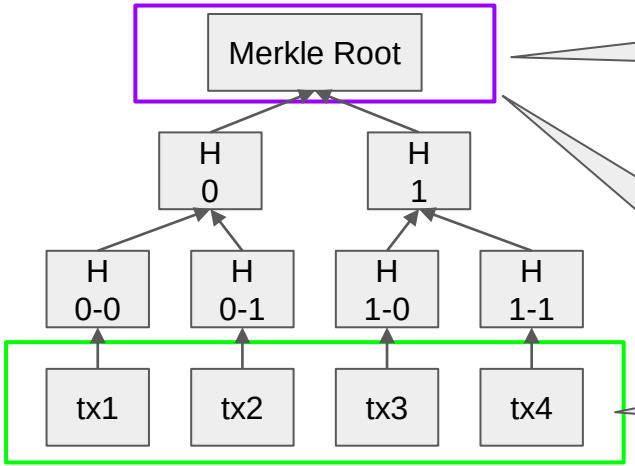
Data Availabilityを保ちながらスループットを向上する技術
トランザクションデータをブロックチェーンにCalldataとして投げるが、
Stateとして保存するのはMerkleRootだけ



What’s Rollup?

１秒間に処理できるトランザクションの数

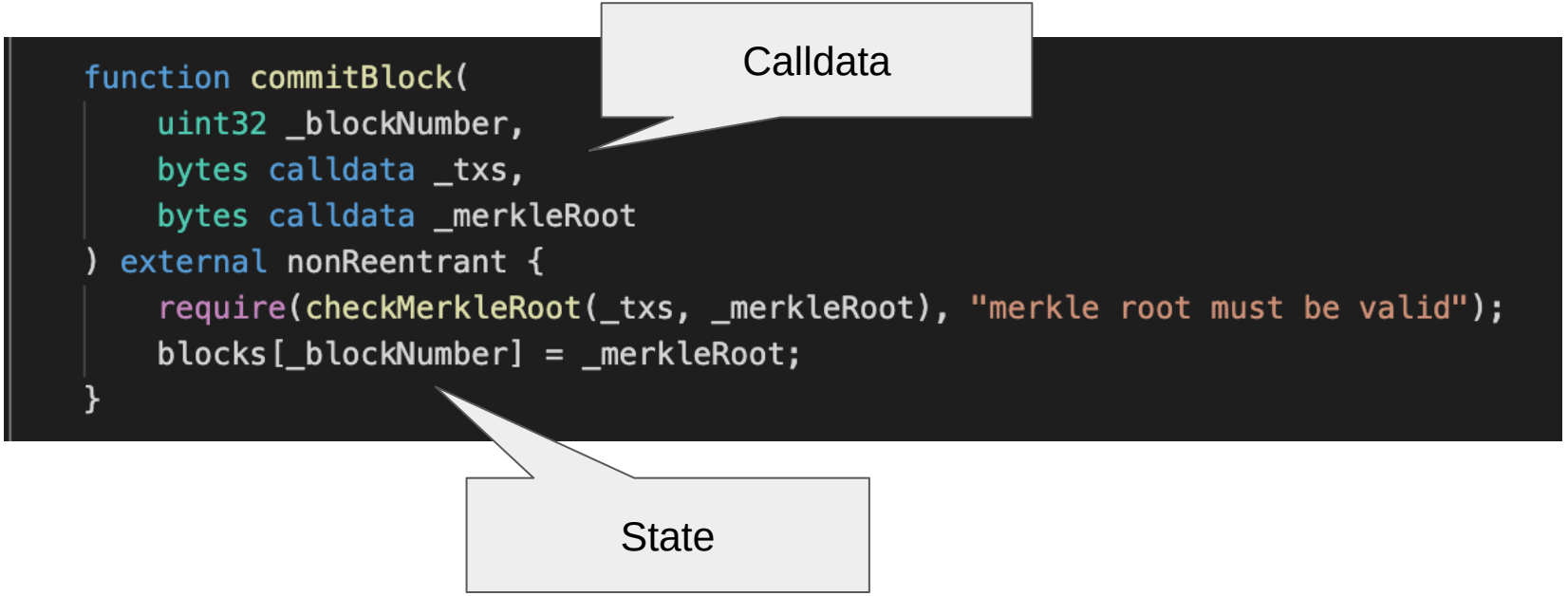
Data Availabilityを保ちながらスループットを向上する技術
トランザクションデータをブロックチェーンにCalldataとして投げるが、
Stateとして保存するのはMerkleRootだけ



Plasmaはここだけブロックチェーンに投げる

Rollupは両方をブロックチェーンに投げる

トランザクションのCalldataとStateの違い



トランザクションのCalldataとStateの違い

- 現在のEthereumのStateのサイズは、~45GB、Chain Size全体は300GB
- トランザクションとは異なり、Stateはフルノードで切り落とすことができない。
- トランザクションを検証するためには、Stateへの多くのランダムアクセスを実行しなければならないため、StateをRAMに保持する必要がある

要するに**Stateは高い、トランザクションのCalldataは安い**

https://etherscan.io/chartsync/chaindefault

Data Availabilityがない状態とは？

txが正しいのか不正なのかがわからない

?

h = Hash(tx)

txの中身がわからない状態

例）PlasmaのExit Game

もとのtxを知るために**特別な仕組み**が必要になってしまい、実現できることも少なるなる。**これを汎用的に解決できるのがRollup。**

What’s Rollup

Data Availabilityを保ちながらスループットを向上する技術

Optimistic Rollup
問題が起こった場合のみブロックチェーンでトランザクションの検証を行う

ZK Rollup
(zk-)SNARKにより毎回ブロックチェーンでトランザクションの検証を行う

Gasコスト削減の観点での比較

EthereumではState, Computation, Calldataがトランザクション数に比例して増えます。
RollupやPlasmaではStateやComputationによるgas消費は一定になります。

	State	Computation	CallData
Ethereum	O(n)	O(n)	O(n)
zkRollup	C	C or log(n)	O(n)
Optimistic Rollup	C	C	O(n)
Plasma/Sidechain	C	C	C

nはトランザクションの数、Cは定数

トランザクションあたりのGasコスト比較（概算）

送金では10倍程度、Dexのような複雑なトランザクションでは大きな効果が出る。

	送金	Dexのswap
L1	22,000 gas	約80,000 gas
ORU	2,576 gas	3,600 gas
zkRU	1,153(833+320) gas	4,406(3750+656) gas

zkRUではブロック当たり360txが格納でき、検証コストに300,000 gasかかることを想定。

スループットの計算

block gas limitを前のスライドの「tx当たりのgas」で割ることで、**ブロック当たりの最大トランザクション数**が算出できる。しかしzkRUでは、circuitサイズと証明生成時間がボトルネックになる。

仮に最大のgas limitを10Mとした場合に、**ブロック当たりの最大トランザクション数**は以下の表ようになる。このブロックをどのくらいの頻度でL1に登録するかで、スループットが決まる。

	送金	Dexのswap
L1	30 tx per block	8.3 tx per block
ORU	258 tx per block	185 tx per block
zkRU	320 tx per block	80 tx per block

zkRUのキャパシティは、まだまだ改善の余地があることに注意

仮に320txのブロックの証明生成に600秒かかるとすると。ブロックタイムを60秒（つまりtps=5.3）にするのに、10台のマシンが必要になる。

Why Rollup

Data Availabilityを犠牲にしないことで、色々なメリットがある。

Agenda

Rollupとは何か?

Optimistic Rollupとは何か？

Zk Rollupとは何か？

ORUとzkRUの比較

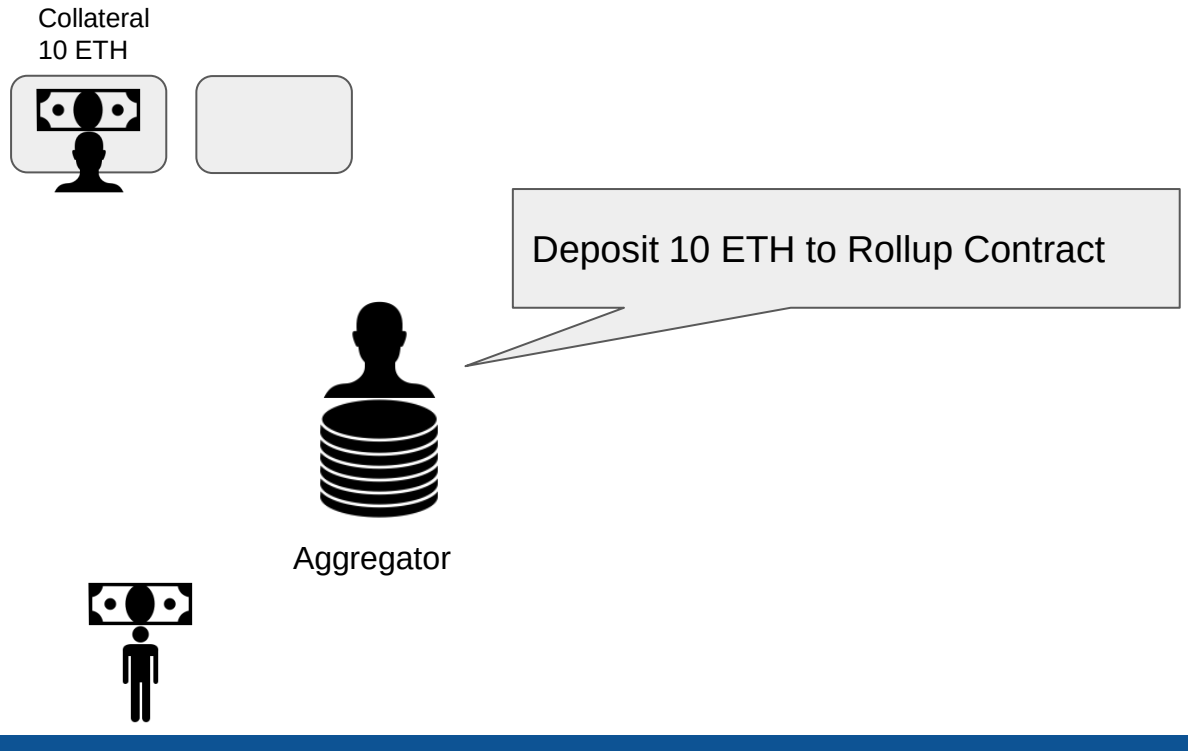
What is Optimistic Rollup

問題が起こった場合のみブロックチェーンでトランザクションの検証を行う

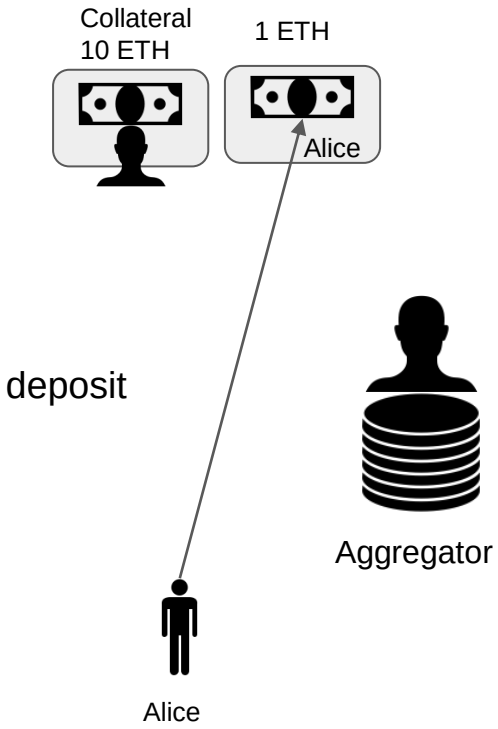
- アグリゲータがパーミッションレスである
  - 誰でもトランザクションのバリデーションができる
- EVMとの互換性を持たせやすい
- L1の引き出しに一週間程度かかる
  - L1とL2の間でトークンを即時交換する方法もある

How Optimistic Rollup works

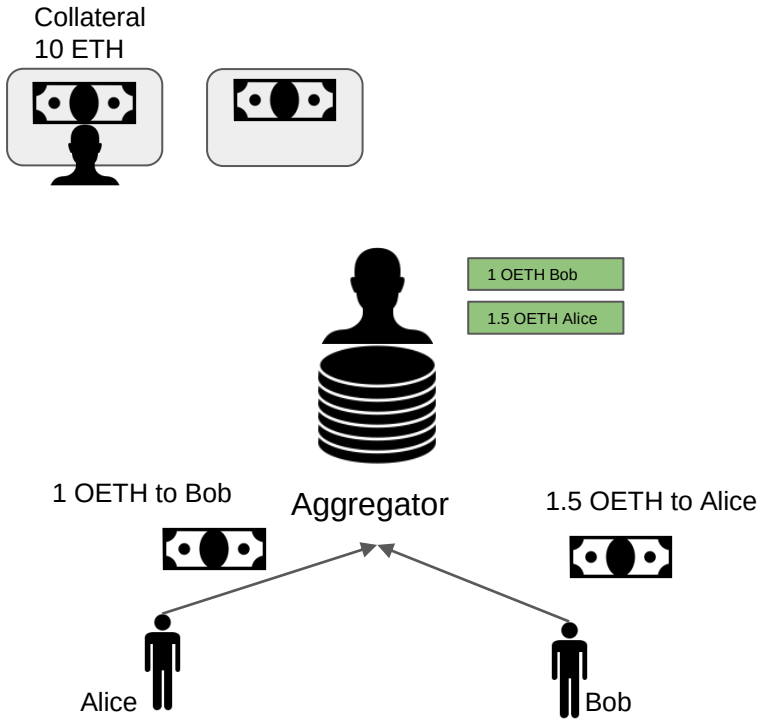
How Optimistic Rollup works



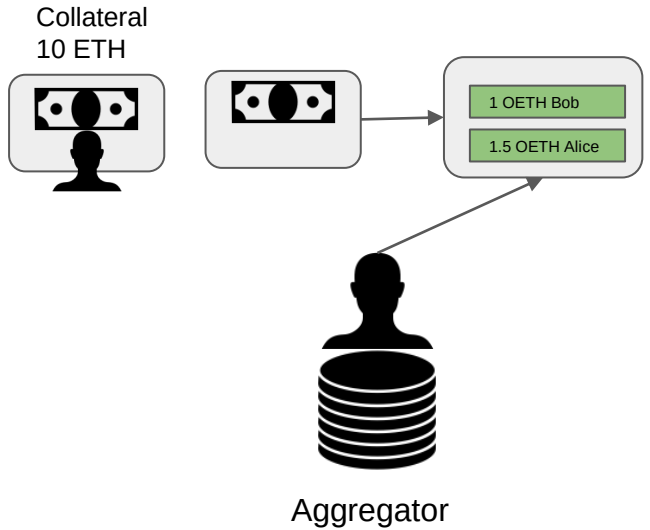
Deposit



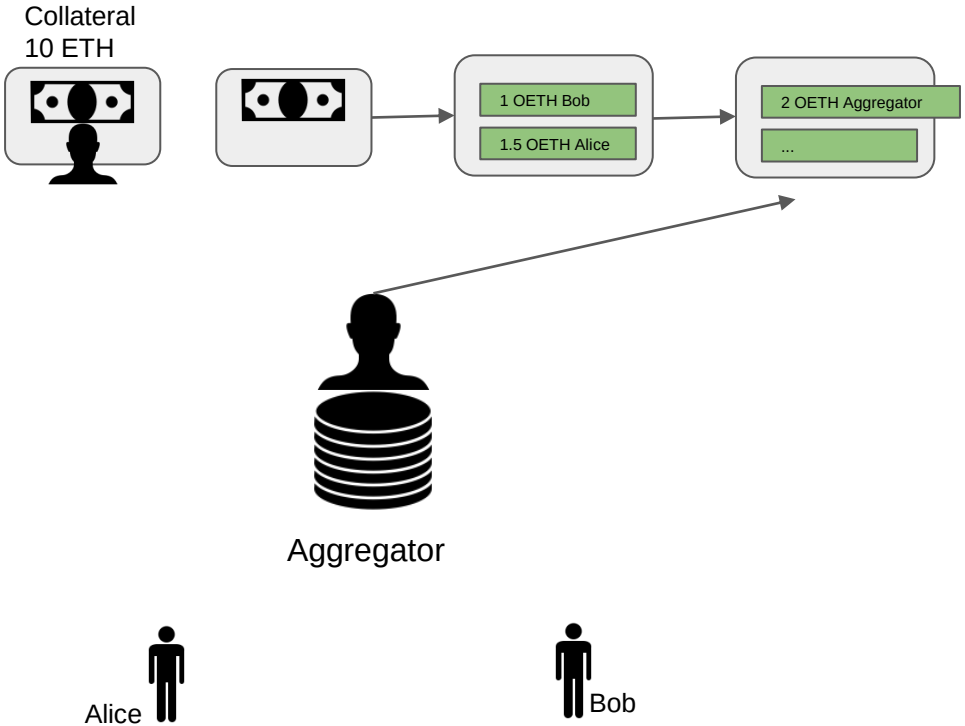
Sending Transaction



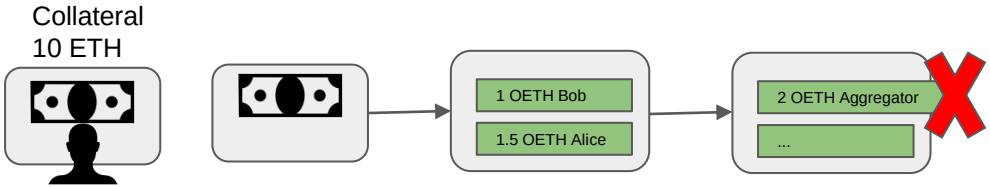
Sending Transaction



不正なブロックを作成された場合



不正なブロックを作成された場合

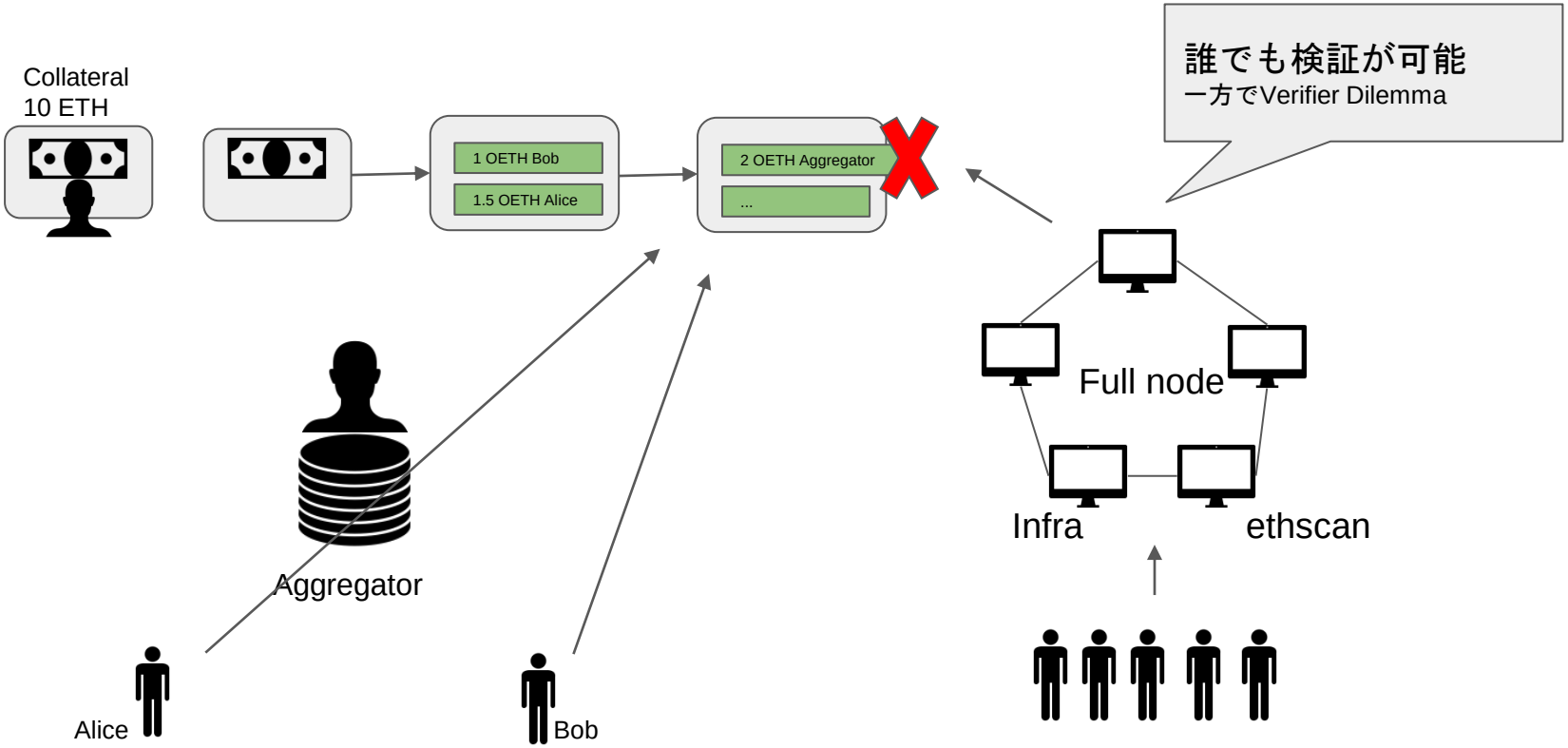


Aggregator

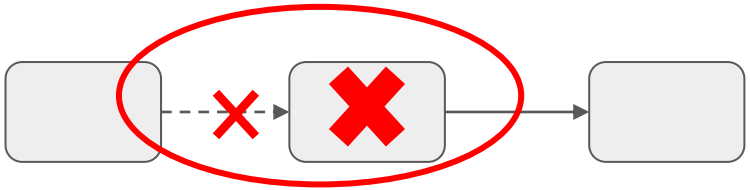
Alice

Bob

不正なブロックを作成された場合



不正証明（Fraud Proof）



不正なブロック=不正な状態遷移を含むブロック
不正証明は不正な状態遷移の証明

‘EVM互換の状態遷移での不正証明を可能にする仕組み’としてOVM（Optimisic Virtual Machine）がある。

Exploring ORU

問題が起こったときにFraud ProofによりブロックをEVMで検証する。そのため

- L1への引き出しに一週間程度かかる
- アプリケーションはEVM互換にすることが可能

今回説明できていないトピック

- OVMの仕組み
- MEVAuctionやSequencerについて
- BLS Signature aggregationによるトランザクションコストのさらなる削減

Agenda

Rollupとは何か?

Optimistic Rollupとは何か？

Zk Rollupとは何か？

ORUとzkRUの比較

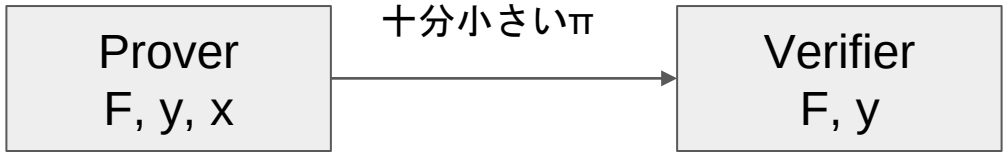
How zkRollup works

zkRollupでは、(zk-)SNARKによりブロックの正しさをL1で検証する。

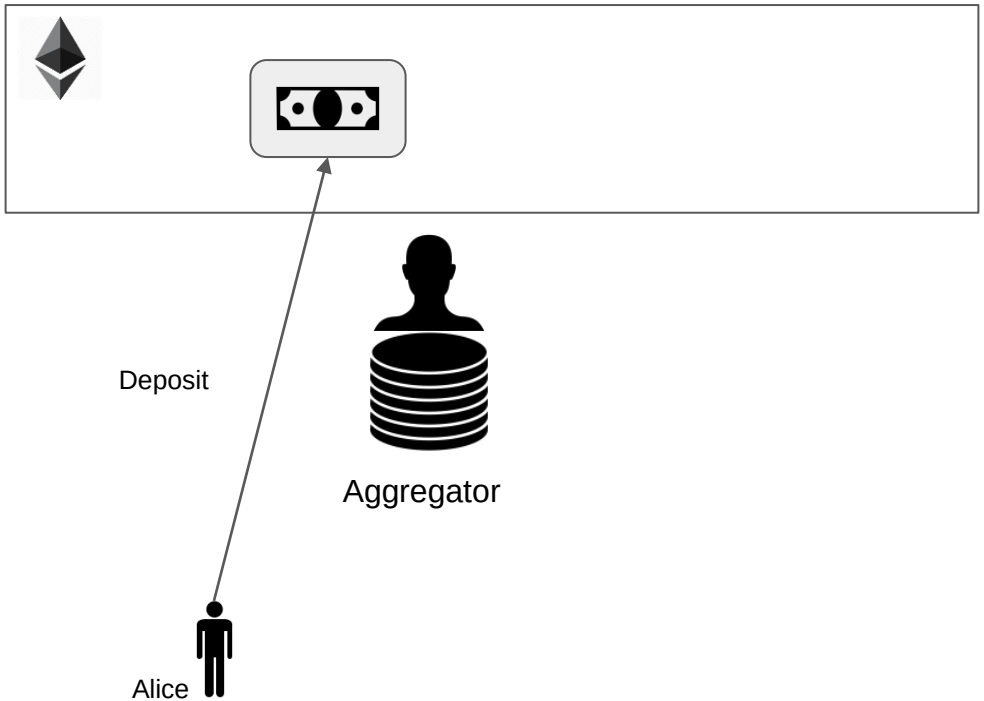
- ORUと同様に、アグリゲータはパーミッションレスである
- L1への引き出しは数分しかかからない
- ブロック実行の証明生成が、スループット向上のボトルネックになる
- スマートコントラクト開発に制約がある
- ORUに対してセキュリティ上のアドバンテージがある

SNARKの性質

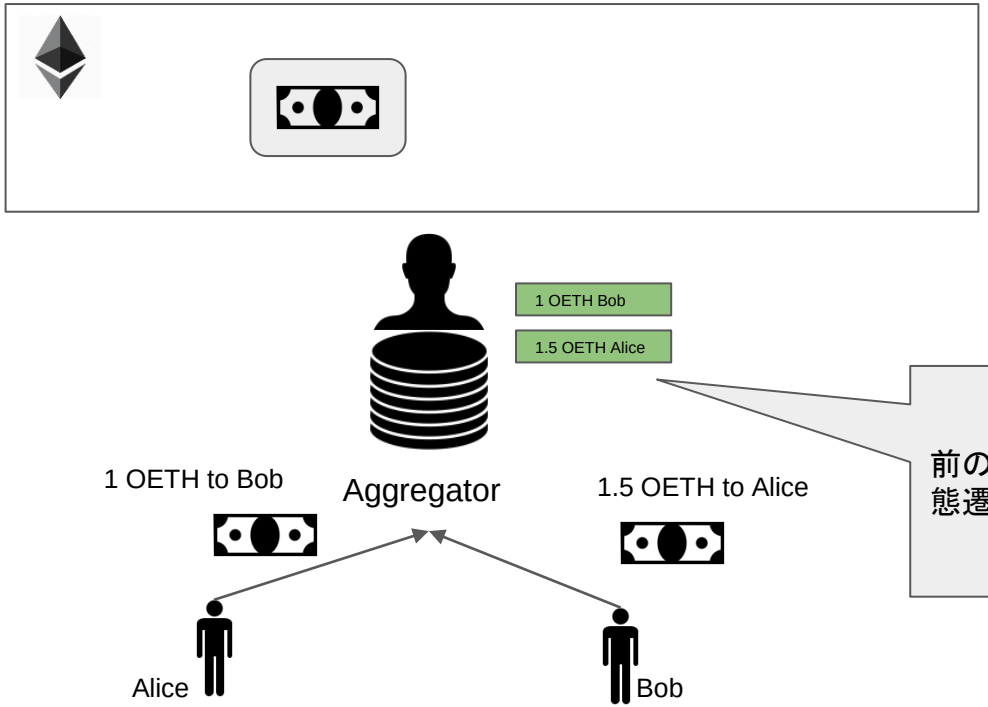
$$F(x) = y$$



How zkRollup works

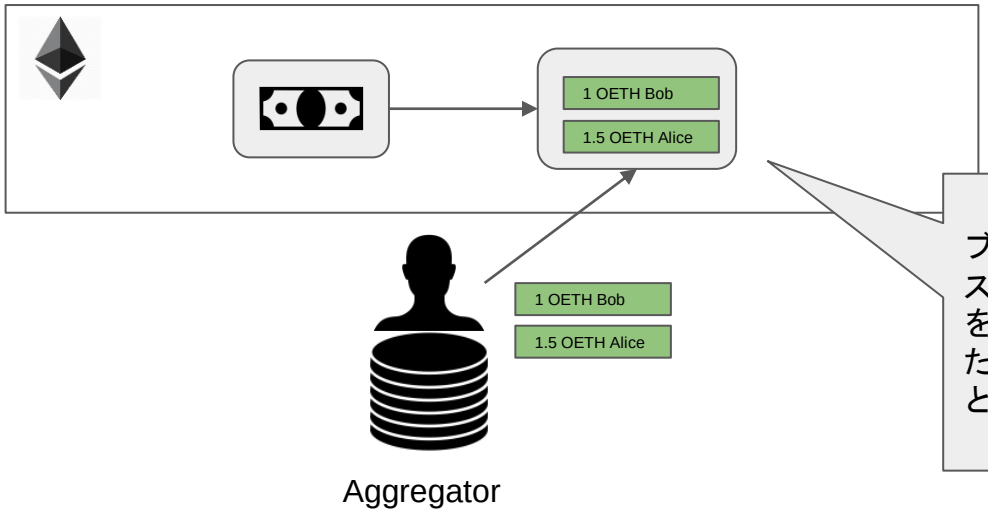


How zkRollup works



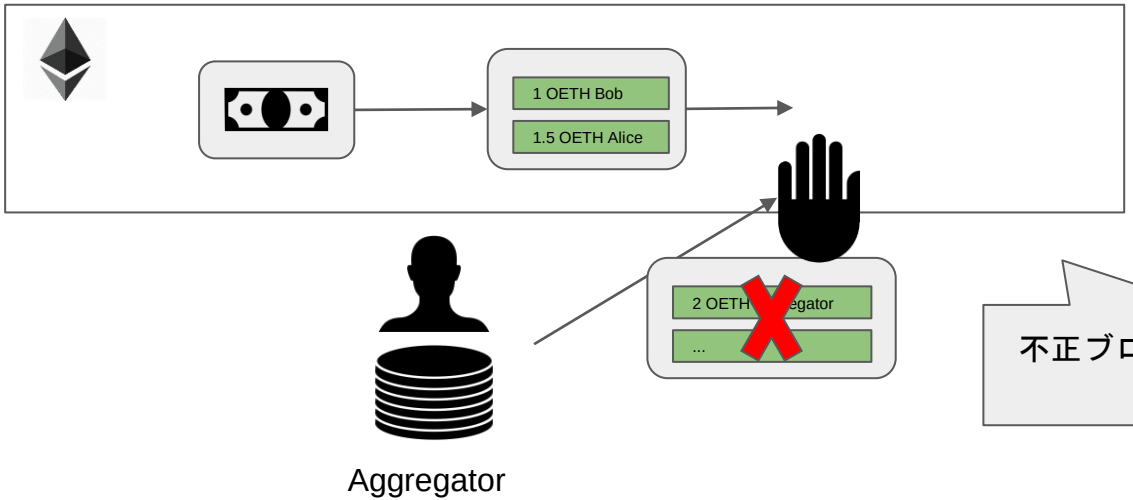
前のmerkle rootから次のmerkle rootへの状態遷移を証明するZk proofを生成する。

How zkRollup works

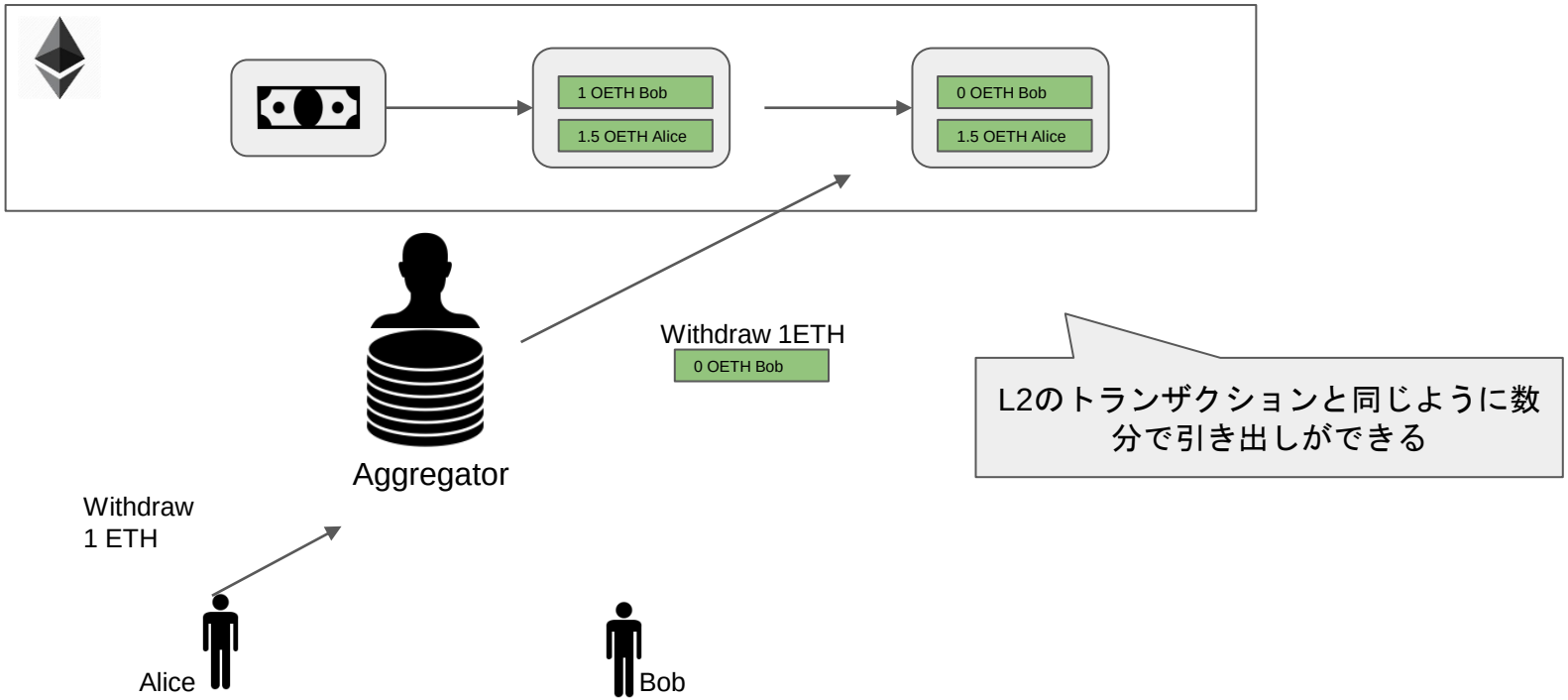


ブロック実行の証明（Zk Proof）を使って、毎回スマートコントラクトでトランザクションの検証をするので、L2ブロックは常に正しい。
ただしトランザクションの登録（commitBlock）と検証（verifyBlock）には時間差がある。

How zkRollup works

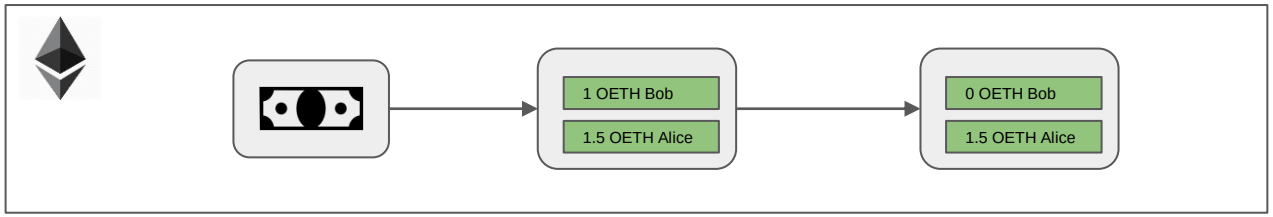


How zkRollup works

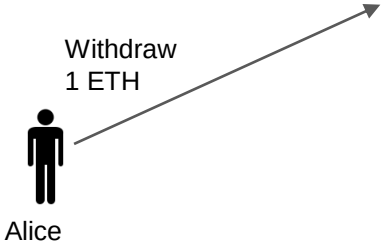


L2のトランザクションと同じように数分で引き出しができる

How zkRollup works



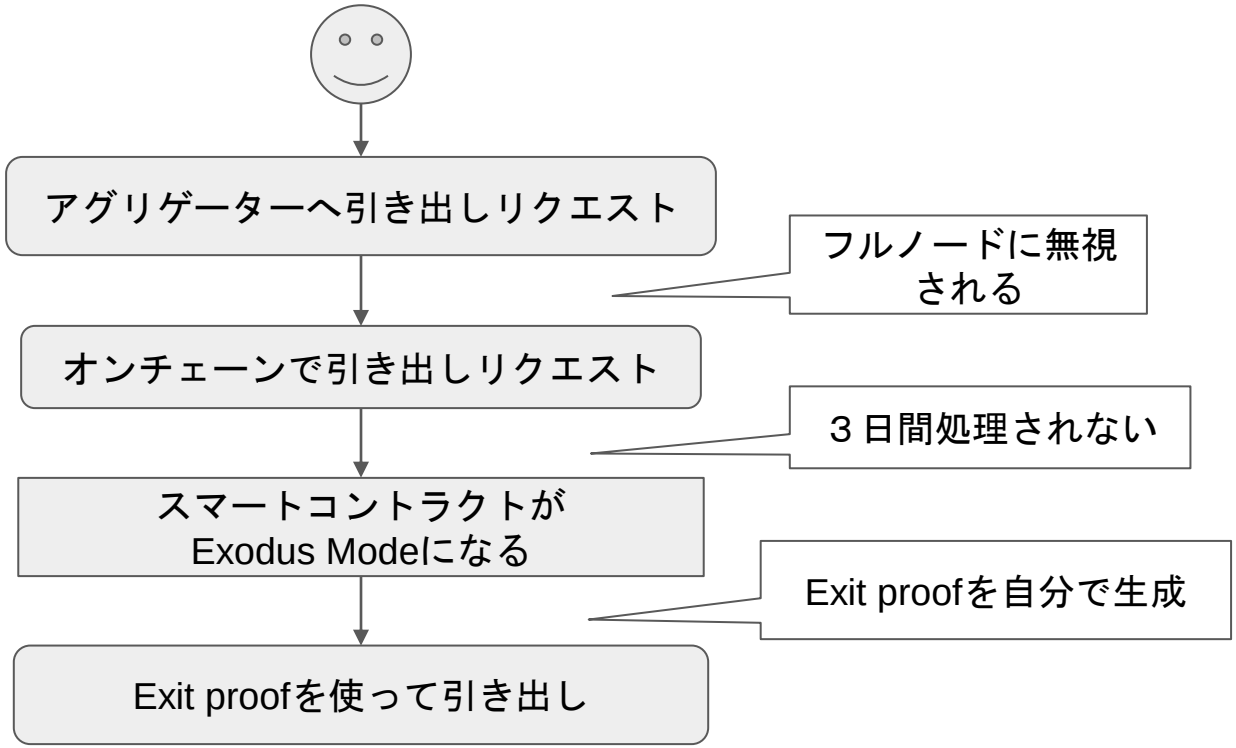
理論的には複数のフルノードを想定できる



Exodus mode

全てのフルノードに引き出し要求を無視された時のために、オンチェーンに直接引き出し要求を投げることができる。引き出し要求が処理されない場合、**Exodus Mode**という緊急モードになる。

緊急時の資金引き出し手順



zk-SNARKプロトコルの比較

	Proof size	Verification cost	Proving Time	
Groth16	188 bytes	約200k gas	quasiliner	Trusted Setupが必要。
Plonk	500 bytes	約300k gas	quasiliner	Universal Trusted Seup=セットアップの参加者を増やせるので、徐々にセキュアになる。異なるプログラムで同じセットアップが使える。
Redshift	96-234kb (2^20-2^28 constraint)		quasiliner	Trusted Setupが必要ない。
Stark	80kb- (786k hash invocations)	約1M- gas	quasiliner	Trusted Setupが必要ない。

実用上は下に行くほど早くはなっています

Conclusion zkRU

zkRollupはブロックが正しいことが検証できているため、安全性のための十分な数のバリデーターを想定する必要がなく、またすぐにL1に資産の引き出すことができます。

今回説明できていないトピック

- zk-SNARKプロトコルの発展
- zkプログラミング(Zinc, Cairo)
- zk-SNARKプロトコルの証明生成時間の改善
    - AWS F1インスタンスを使った改善。https://medium.com/matter-labs/worlds-first-practical-hardware-for-zero-knowledge-proofs-acceleration-72bf974f8d6e

Agenda

Rollupとは何か?

Optimistic Rollupとは何か？

Zk Rollupとは何か？

ORUとzkRUの比較

ORU vs zkRU（ユーザ側）

レイテンシ(txが検証可能になるための時間)

- ORUは即時の経済的ファイナリティ、紛争期間後（1-7日程度）にL1でのファイナリティを得る
- zkRUは即時の経済的ファイナリティ、ブロックの証明生成後（1-10分程度）にL1でのファイナリティを得る

L1への引き出し

- ORUは引き出しに1週間かかる
- zkRUは引き出しがすぐできる

https://vitalik.ca/general/2020/08/20/trust.html

ORU vs zkRU（開発者、ノード運営側）

プログラマビリティ

- ORUはEVM互換性を持たせられる。
- zkRUはプログラマビリティにクセはあるが、Cairoやzincでかなり改善されている。

コスト面

- ORUは安いマシンで運用できるが、複数のバリデーターに分散している必要がある。
- zkRUは証明生成にハイスペックマシンが必要で、スループットを向上させるには複数台のマシンが必要になる。

https://vitalik.ca/general/2020/08/20/trust.html

ORU vs zkRUどちらが安全？

安全でない＝不正なブロックがL1でファイナリティを得てしまう
と定義する。

	安全性に必要な仮定
ORU	マイナーの多数が正しい行いをする
zkRU	なし

ORUは資産の安全性のために、L1に一定の検閲耐性を仮定しないといけない。zkRUでは引き出しなどが検閲されても資産は安全に保たれる。一方でzk-SNARKsプロトコルによっては、セットアップした人を信頼しなければいけない場合もある。

https://vitalik.ca/general/2020/08/20/trust.html

Products of ORU & zkRU

名前	特徴
Optimism(synthetix)	SolidityでSmart Contractが書けるORU
FuelCore	UTXO型のORU
Arbtrum	AVMという独自のVM。二分法的な紛争解決モデル
zkSync(curve, balancer)	スマートコントラクトプラットフォームを目指すzkRollup
zkSwap	zkSyncの技術を利用したAMM
loopring	現在取引ボリュームトップのL2 DEX($10M ボリューム)
StarkEx, StartNet	Validium, Rollupプラットフォーム型

今日お話できていないが、面白そうな分野

- アグリゲーター周りのエコノミクス（MEVAuction）
- 秘匿送金系（opzkru, zkzkru）
- フロントランニング(MEV-Geth)

まとめ

Ethereumのスケーリング技術である、Rollupについてお話しました。

- RollupはEthereumの安全性、分散性をできるだけ維持したまま、スループットを向上させることができる。
- スループットは数十倍から数百倍になる。
- ORUはEVM互換のスマートコントラクトの実行ができます、zkRUもスマートコントラクト開発のボトルネックが急速に改善されている。
- zkRUは安全性がより高く、L1への引出し期間が数分で済む。