BUILD UP
for Web3 エンジニア

2023.3.27 Mon
19:00 - 21:00

参加無料

東京都渋谷区桜丘町16-13
桜丘フロントII 3F

CryptoBase

SKYLAND VENTURES
The Seed Maker.

開発者が抑えておきたい
2023年のイーサリアムエコシステムに起きること
～ Solidity開発者のための Study&Meetup ～

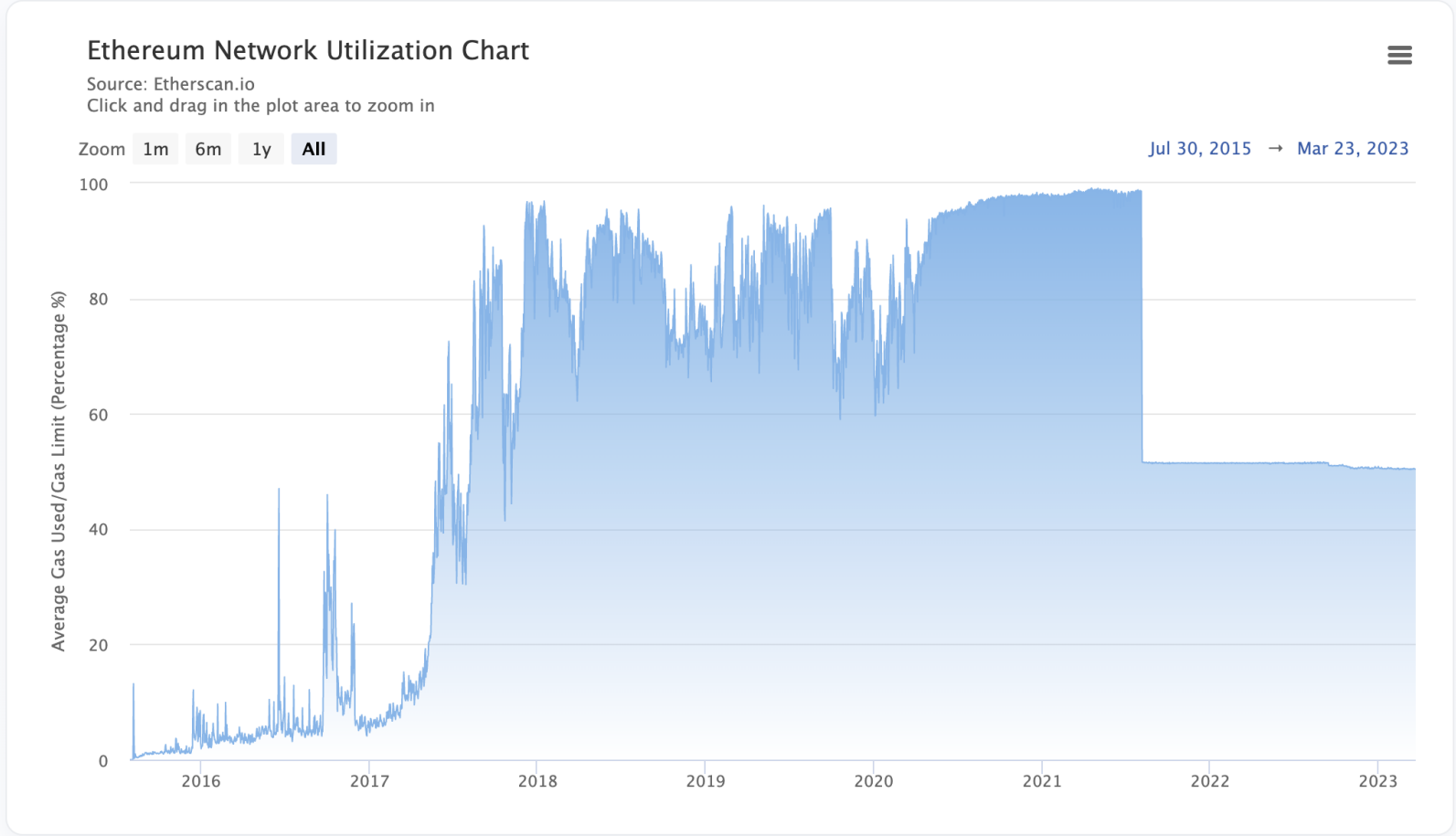
荒巻 陽佑
Web3 開発者

よんくろう
Skyland Ventures

目次

- 開発者として押さえておくべきイーサリアムアコシステムの現状とこれから
- ブロックチェーンをどう捉えるか
- ETH Tokyoに向けてサービスの事例紹介

Ethereumの課題



Ethereumの現状

- もっぱらscalabilityに注力
- ScalabilityのひとつとしてのLayer2
- L2の実態はスマートコントラクト
  - ORのトランザクションをまとめてL1に書き込んでいる、その情報を元にL2のnode/sequencerを構築
  - ZKRの場合はstate diffのみを書き込んでる

Ethereumの現状 : 分類

Optimistic Rollup

Arbitrum

Optimism

Modular chain

Celestia

mantle

ZK Rollup

zkEVM

type 1
scroll, taiko

type2
zkSync, Polygon zkEVM

type3

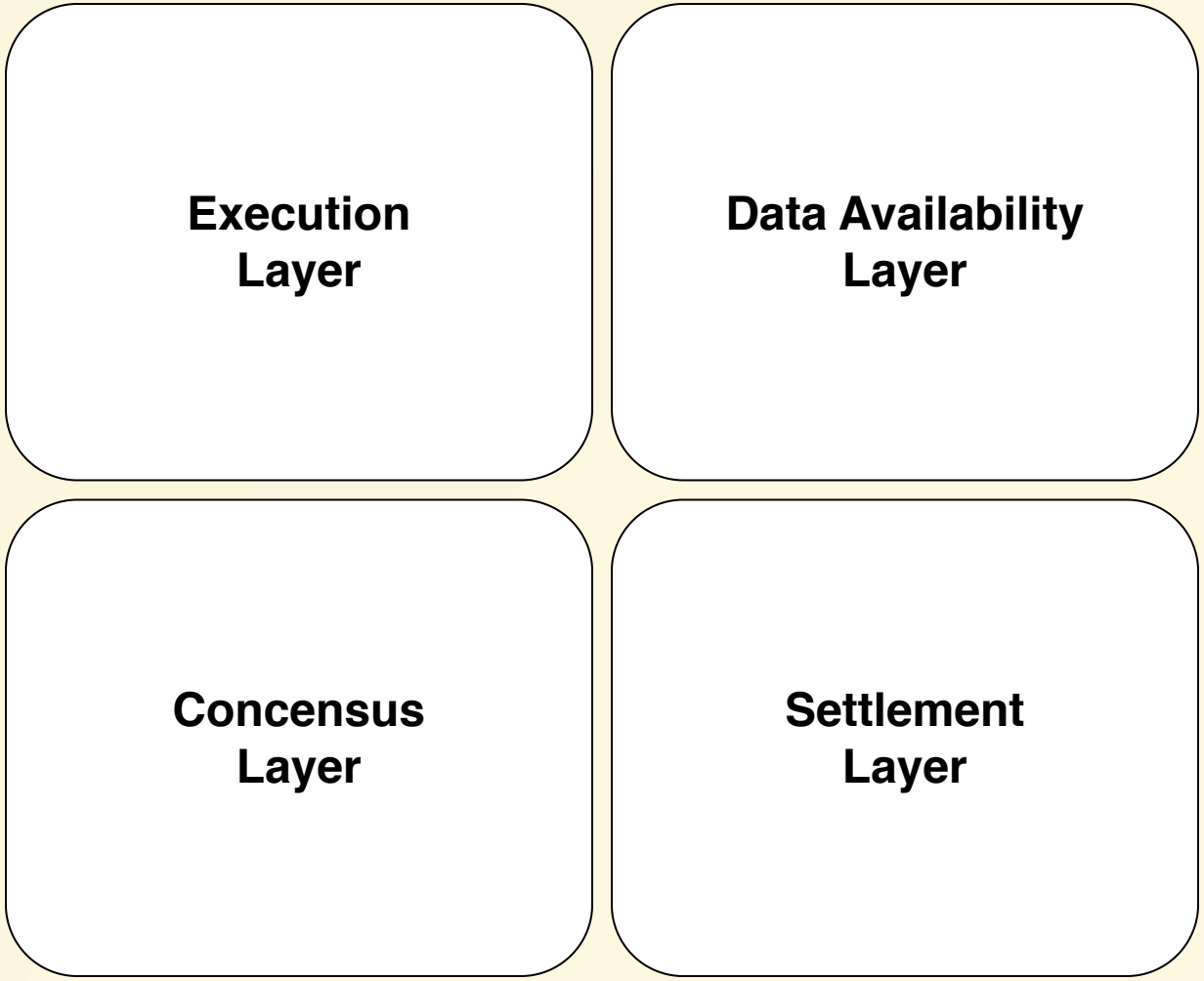
type4
starknet with Nethermind

---

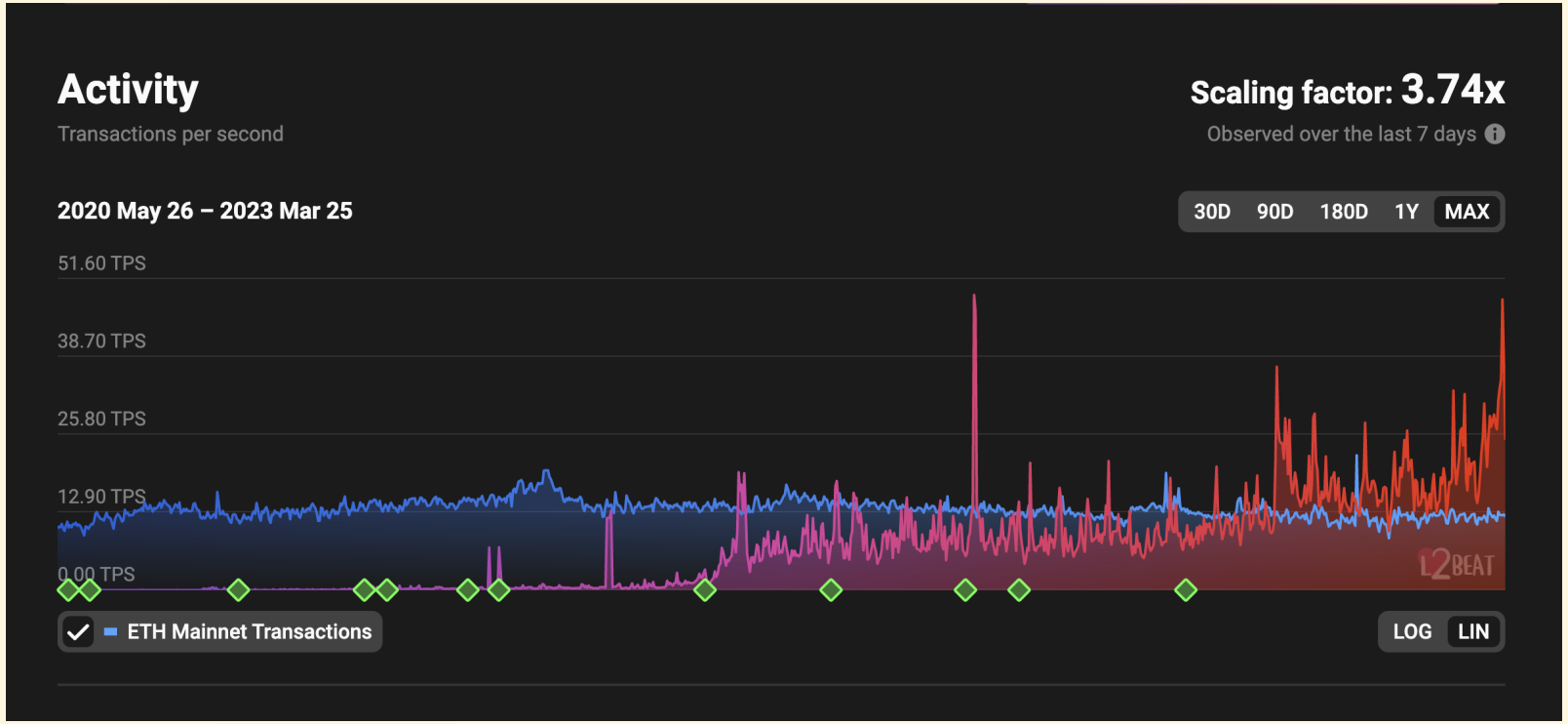
zkEVM 以外

starknet

Ethereumの現状 : Modular とは



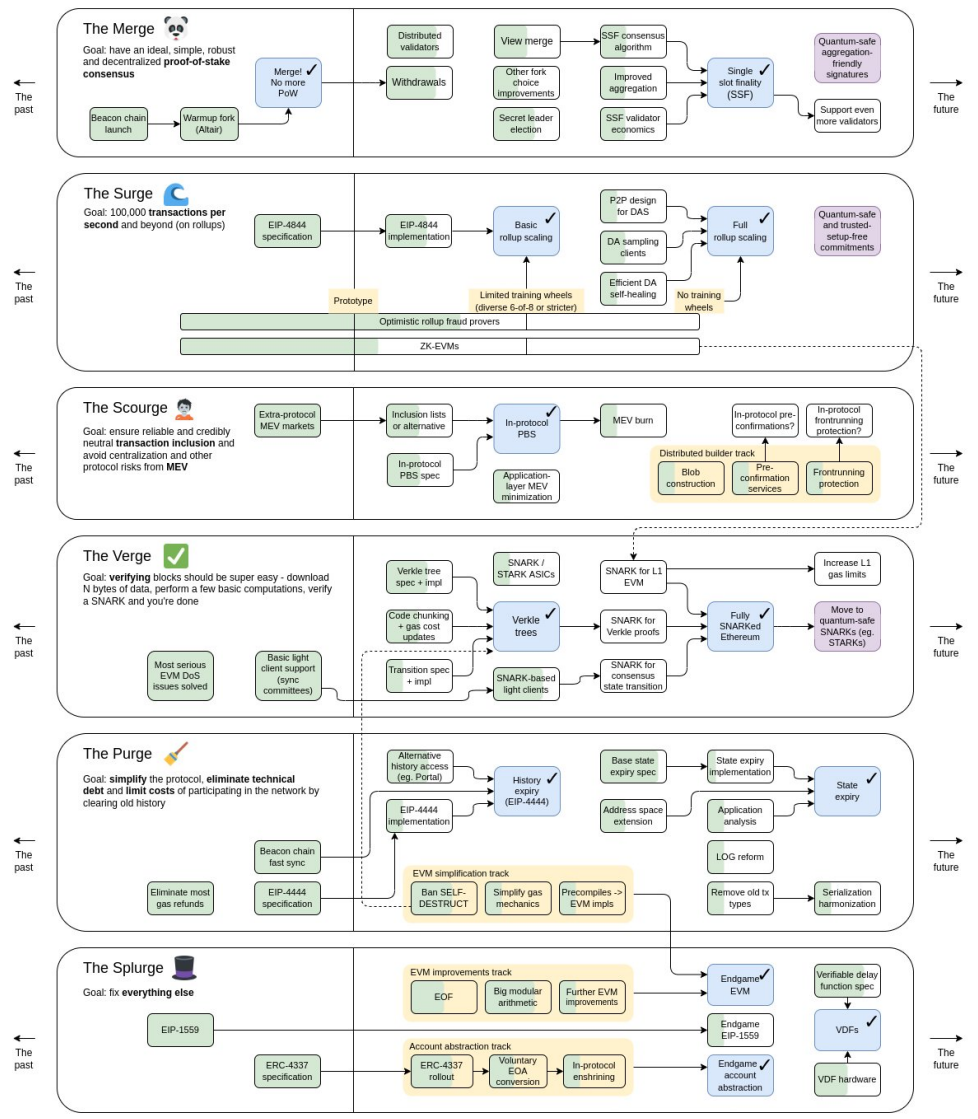
Ethereumの現状 : L2の現状



Ethereum現状をどう捉えるか

- 23年はOR、それ以降はZKR
- ORにもよさはある
- StarkNetは独自路線を進んでいて長期でみると面白い。
- Polygonがどこまで伸びるか
  - Supernets / Avail/ Nightfall/Miden
- L3が増えるかmodular chainが台頭するかは要観察
  - Optimism op stack / Arbitrum AnyTrust / Polygon Avail / zkSync zkPorter / StarkNet starkWar

Ethereumの今後：ロードマップ



by @_ywzx

Ethereumの今後 : アップデート

- Shanghai
  - ETHの引き出しが可能
  - Selfdestructの廃止
- Cancun
  - EIP-4844: Shard Blob Transactions
  - EOF

Ethereumの今後をどう捉えるか

- Ethereumはよりセキュリティーを担うレイヤーになる
  - PolkadotのRelay Chainによるshareｄ securityやCosmosHubのInterchain security, mesh security
- L2の足並みが揃ってないので、Ethereum全体としての成長が鈍化しそう
- 開発者へのアップデートが少ない
- ただ、まず今求められている最低限のものを実装している、ゆえにシンプルで複雑なものを上に作りやすい
  - Ethereum界隈の開発スピードはかなり早いしまだ中心になっている

Ethereumの今後をどう捉えるか

- "it's okay if no single person can understand the whole protocol, because we can specialize"
- "We don't know exactly what the needs of 2032 will demand"
  - by vitalik

開発者としてブロックチェーンをどう捉えるか

- ブロックチェーン = Ethereumはstate machine ≒ DB
- スマートコントラクト = stateの書き込みと読み込みの定義 ≒ API
  - お金を払えば誰でも書き込みができる、読み込みはタダでできる
  - その書き込まれたデータは恣意的に変更できない（セキュリティー）
  - **価値がつかなかったものに価値をつける / 流動性の低かった資産の流動性を向上させる**

ETH Tokyoに向けてサービスの事例紹介

- スマートコントラクトのアプリケーションは大きく分けると２つがメイン
  - EIP（特にERC20とERC721）によって生まれたアプリ
    - ERC20は保有量を管理したテーブル → DeFi
    - ERC721は保有者を管理したテーブル → NFT
  - コントラクトウォレット

ERC20 / ERC721の拡張

- EIPの規格にさえ準拠=関数名と引数さえあっていれば、関数のロジックはなんでもいい
- ERC20の例
  - AAVEのaToken : 利子分を追加して残高を返却
  - Compoundのcomp : tokenの移転と同時にdelegateも移転
  - Ampleforth : MoneySupplyの増減で価格を維持
    - balanceOf / rebase
- ERC721
  - Uniswap V3 LP : SVGとparamでNFTを型から生成

ERC20 / ERC721の拡張 : まとめ

- EIPはInterfaceの定義のみなので、それさえ守ればその先の可能性は無限大
- 規格を作ることができる
  - ブロックチェーンを利用したLGBTカップル調印式 by famiee

コントラクトウォレットとメタトランザクション

- アカウントは２つ：EOA / Contract Account = スマートコントラクトなので拡張性は様々
- Multisig : Gnosis Safe
  - コアはexecuteのみ。call() or delegateCall()で叩き先を指定するので、全てのtxに柔軟に対応できる
- AA : Patch wallet
  - txの実行をbundlerに移譲
- メタトランザクション : txの署名と実行の分離
  - EIP2612(permit) / EIP3009

番外編 : tornado cashとzkp

- ZKP (zero knowledge proof)とは
  - ある情報を知っているということを伝えようとする者（証明者）が，その情報を知っているという事実以外の情報を，証明を検証しようとする者（検証者）に与えることなく，検証者に対して証明者がその情報を知っていると証明すること。
- SNARK（Succinct Non-Interactive Argument of Knowledge）
  - 簡潔に対話なしで知識の根拠を署名できる = コントラクトに対して一回の通信で証明できる

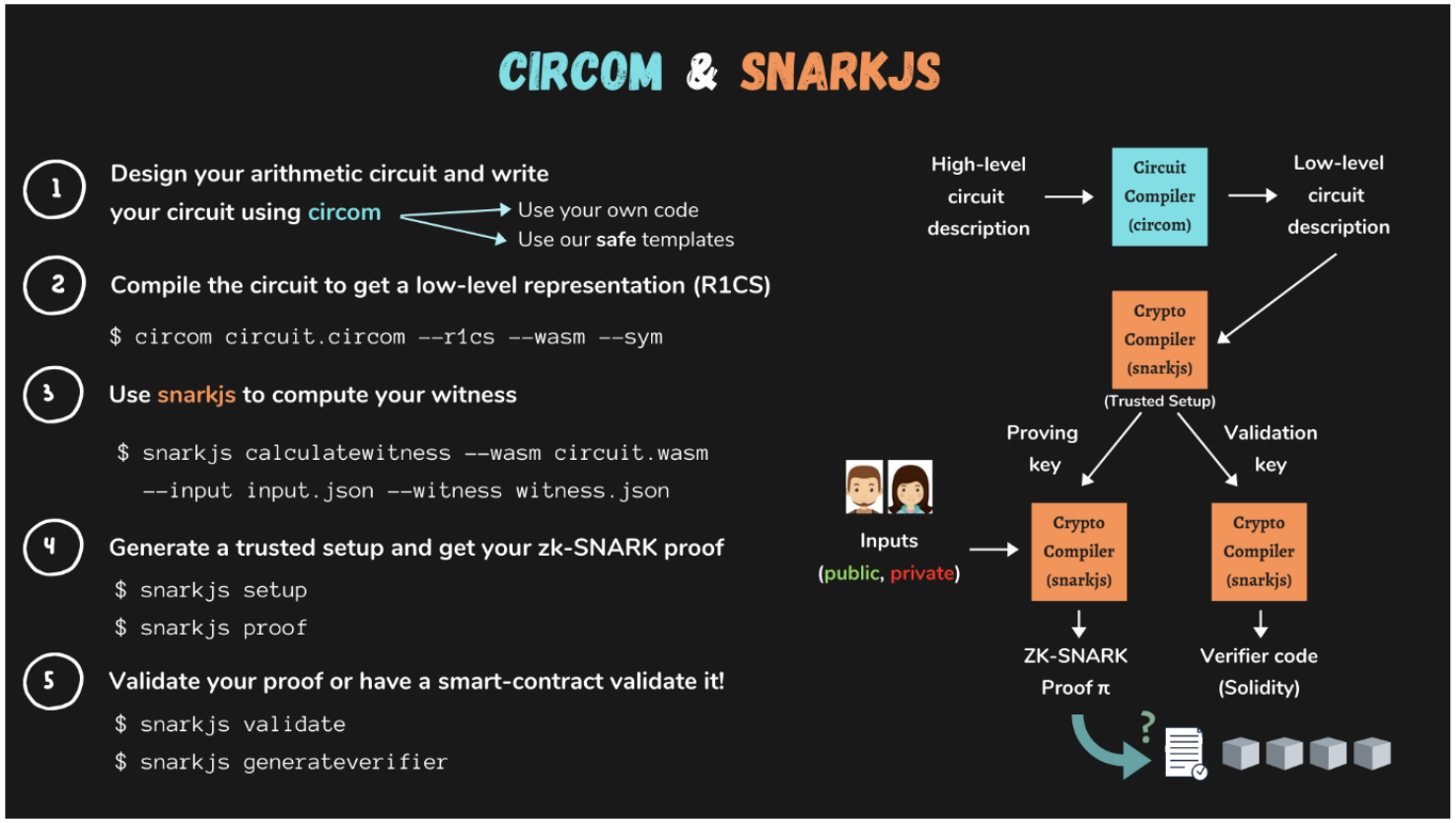
番外編 : tornado cashとzkp

- tornado cash : 暗号資産のミキシングサービス

番外編 : tornado cashとzkp : 仕組み

- シークレット値の生成
  - nulifier + secret をハッシュ化する
- deposit
  - ハッシュ値を資産とともtxを実行し登録（commitment）
- zk-snarkを利用してproofを作成
  - commitmentの元となったnullifierとsecretを所有していることを証明するproof
- withdraw
  - proofを提出することで、nullifierとsecretを明かすことなく資産を引き出すことが可能

番外編 : tornado cashとzkp



tornado cashとzkp : まとめ

- zkpとはスマートコントラクトはオープンであるけど、情報を明かすことなく情報を持っていると証明できる
- ZKPがあると何がいいのか
  - データ量/計算量の圧縮：ZKRだとtxの情報を全て渡すことなくtxの検証ができる
  - データの秘匿化：オープンが前提のブロックチェーンにプライベートの概念を持ち込むことができる
  - プログラミングパラダイムシフト by 日置さん(intmax)