ユーザー視点で見るEthereum 2.0

中村 龍矢（LayerX Inc.）

中村 龍矢

Twitter : @nrryuya_jp

ecosystem support program

MITOU

LayerX

LayerX Labs

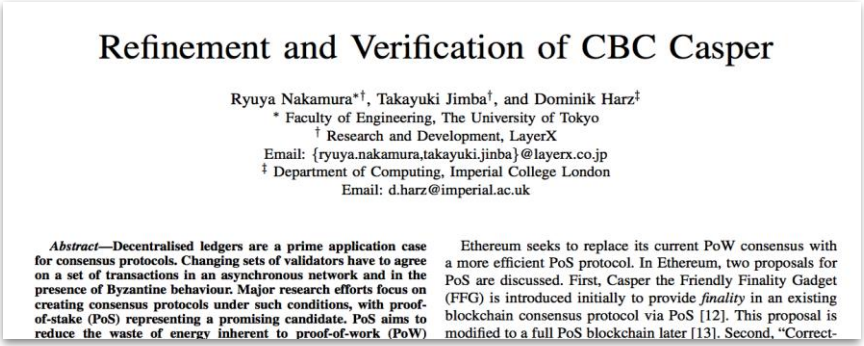
LayerX Inc. 執行役員 兼 LayerX Labs 所長

- LayerXに創業から参画
- Ethereum へのコントリビューション
  - 2019年 Ethereum財団 グラント採択（日本初）
- IPA 未踏人材発掘事業 2020
- 略歴: Gunosy Inc., Coubic Inc., 東京大学工学部

LayerX Labs

デジタル通貨	経済活動の最も基本的な要素である通貨のデジタル化を目指し、特に中央銀行デジタル通貨 (CBDC) に取り組む
スマートシティ	組織・分野横断的な連携における、データのセキュリティ・プライバシー問題の解決に取り組む
パブリックチェーン	暗号通貨によるメカニズム・デザインを、社会インフラを維持する新たな仕組みと捉え、特にEthereumへのコントリビューションを行う

Casperの研究



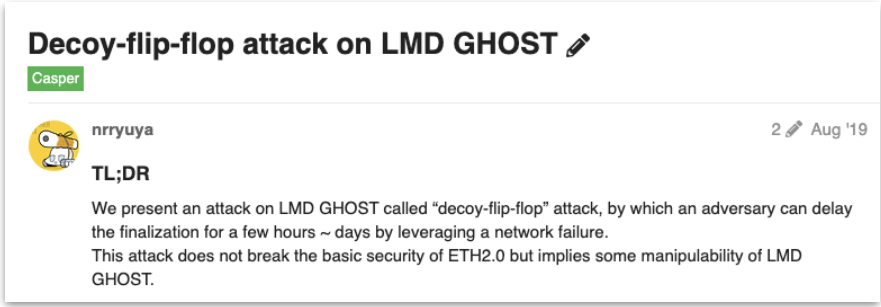
Refinement and Verification of CBC Casper

Ryuya Nakamura*†, Takayuki Jimba†, and Dominik Harz‡
* Faculty of Engineering, The University of Tokyo
† Research and Development, LayerX
Email: {ryuya.nakamura,takayuki.jinba}@layerx.co.jp
‡ Department of Computing, Imperial College London
Email: d.harz@imperial.ac.uk

***Abstract*—Decentralised ledgers are a prime application case for consensus protocols. Changing sets of validators have to agree on a set of transactions in an asynchronous network and in the presence of Byzantine behaviour. Major research efforts focus on creating consensus protocols under such conditions, with proof-of-stake (PoS) representing a promising candidate. PoS aims to reduce the waste of energy inherent to proof-of-work (PoW)**

Ethereum seeks to replace its current PoW consensus with a more efficient PoS protocol. In Ethereum, two proposals for PoS are discussed. First, Casper the Friendly Finality Gadget (FFG) is introduced initially to provide *finality* in an existing blockchain consensus protocol via PoS [12]. This proposal is modified to a full PoS blockchain later [13]. Second, "Correct-

CBC Casperの形式的検証
https://eprint.iacr.org/2019/415.pdf



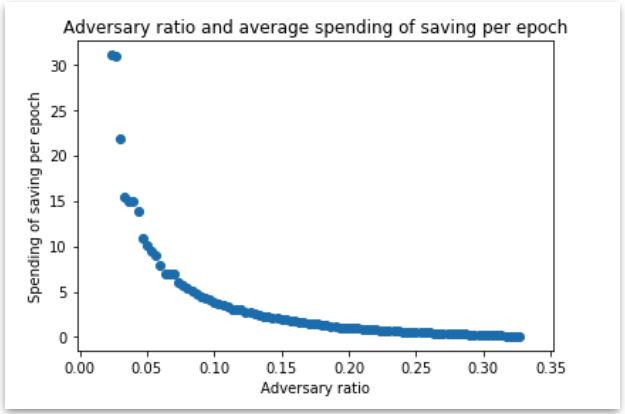
Decoy-flip-flop attack on LMD GHOST

Casper

nrryuya 2 Aug '19

TL;DR

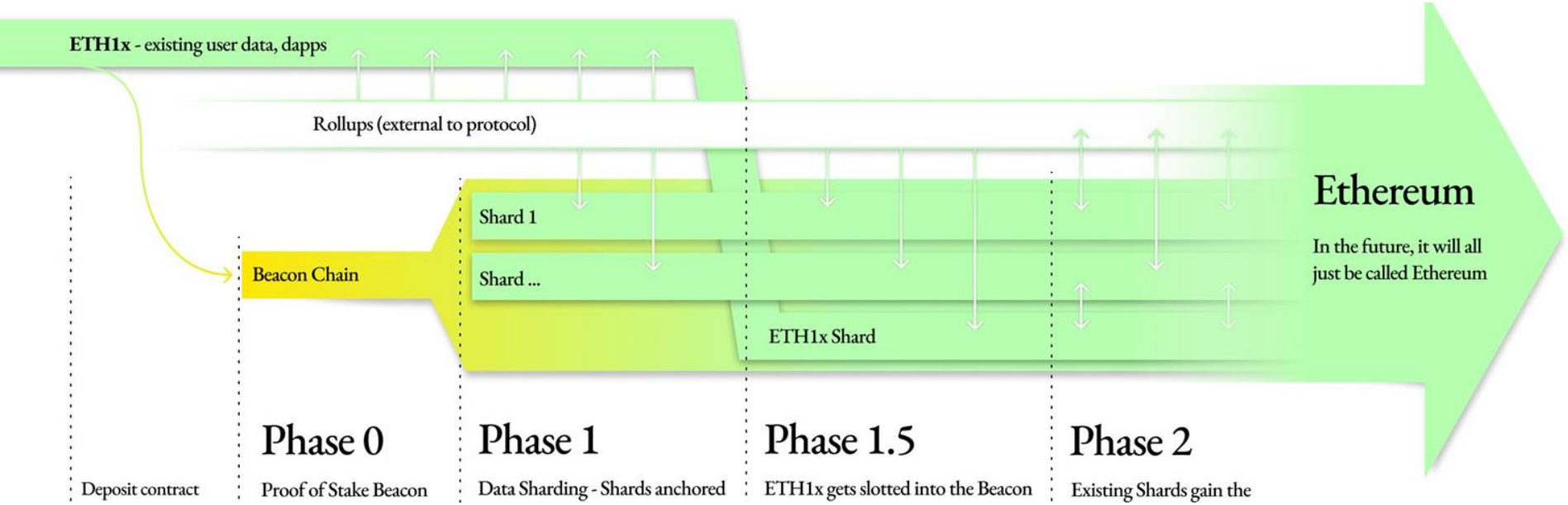
We present an attack on LMD GHOST called "decoy-flip-flop" attack, by which an adversary can delay the finalization for a few hours ~ days by leveraging a network failure.
This attack does not break the basic security of ETH2.0 but implies some manipulability of LMD GHOST.



Eth2のコンセンサスの脆弱性の発見と解決
（Spec v0.9.1にて導入）

本日のテーマ: ユーザー視点で見るEthereum 2.0

特に、シャーディングが導入されるPhase 1以降

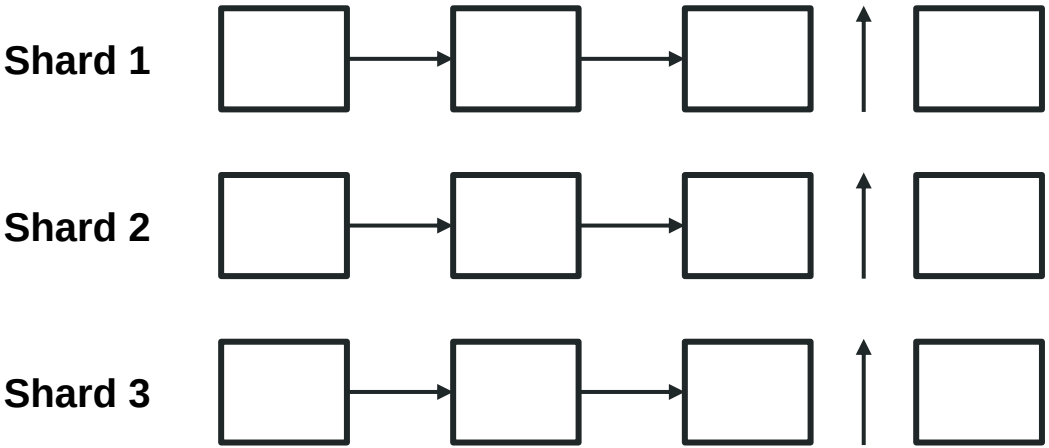


画像: https://twitter.com/trent_vanepps/status/1321936246332104705

シャーディングでのユーザー行動

シャーディングとは？

- 複数のブロックチェーン（シャード）に分割
- 個々のシャードが並列に実行される分スループットが向上



シャーディングがユーザーにとって
どんな影響があるのか、まだまだ未知数

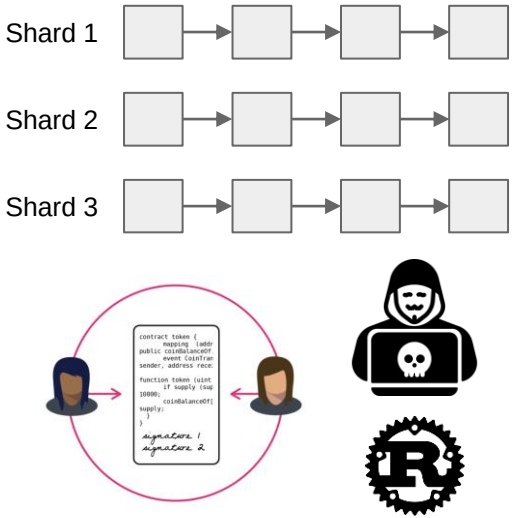
Shangri La

Supported by

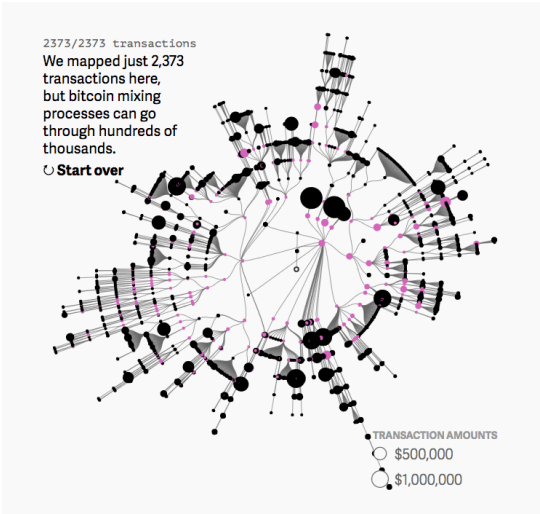
MITOU

Shargri-La

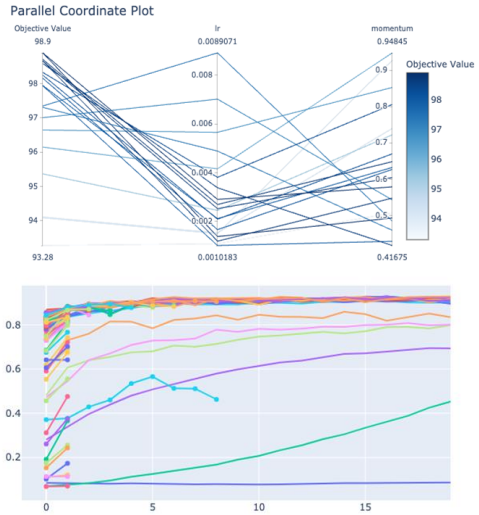
シャーディングプロトコルの開発支援システム



シミュレータ

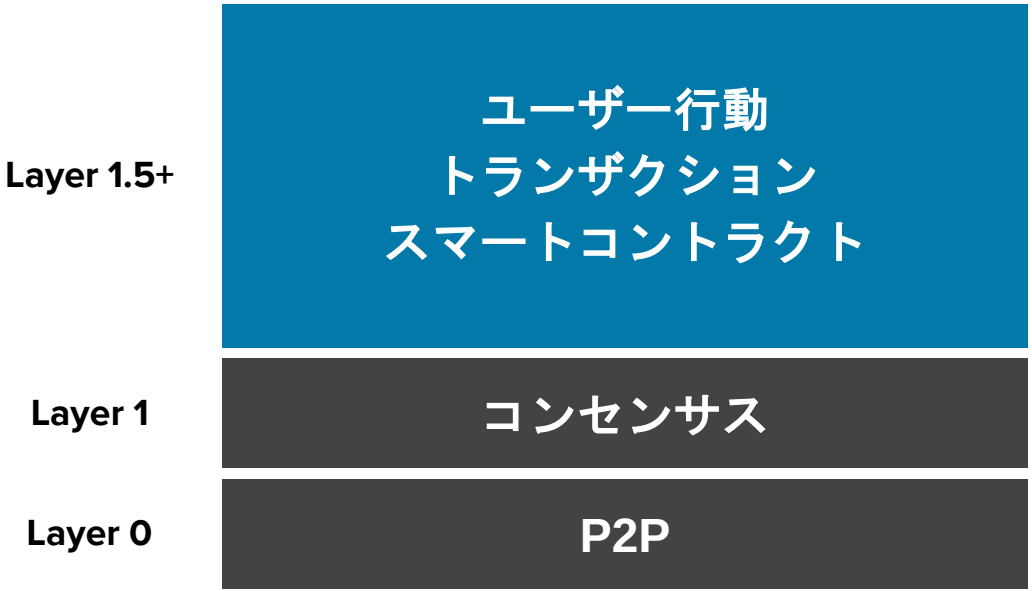


ビジュアライザ



最適化

シミュレーション対象



アプリケーションレイヤー

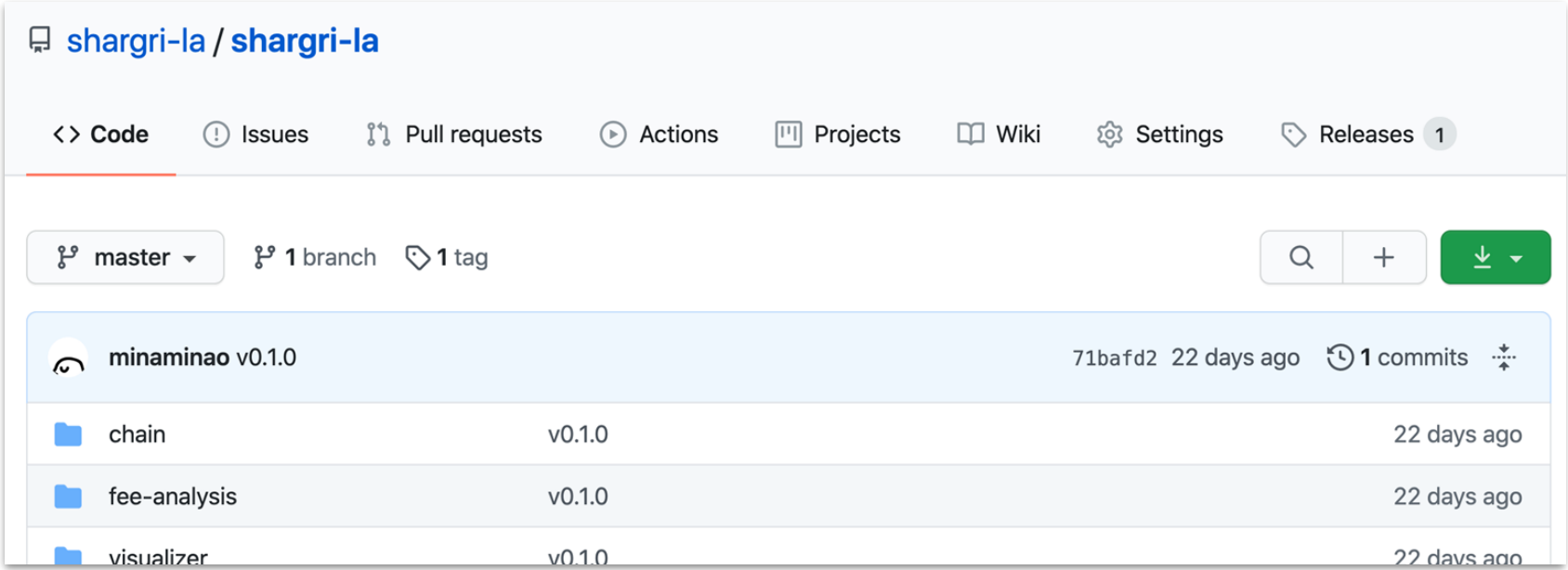
Version 0.1.0: 実装完了

- シミュレーターのコアはRust
- グラフ可視化はPython

  (Matplotlib, Pandas)

```rust
use crate::*;

1 implementation
/// Shard chain with the definition of the on-chain st
pub struct Shard {
    pub id: usize,

    pub blocks: Vec<ShardBlock>,
    pub states: Vec<ShardState>,

    // Included in a state but only needs to be kept i
    pub accounts: HashMap<Address, Account>,
    pub receipts: HashMap<TransactionHash, Receipt>,

    // Shard block proposer variables
    pub moving_accounts: HashMap<Address, Account>,
    pub mempool: Vec<(Transaction, Option<Receipt>)>,
    used_receipts: HashSet<TransactionHash>,
    account_nonce: HashMap<Address, Nonce>,
}
```

Version 0.1.0: リリース



https://github.com/shargri-la/shargri-la

Ethereum Research 投稿

ユーザー行動のシミュレーションを発表

Shargri-La: A Transaction-level Sharded Blockchain Simulator

Sharding ■ eip-1559 ■ cross-shard

minaminao 1 22d

Special thanks to Barnabé Monnot (@barnabe) for comments and feedback and Alex Beregszaszi (@axic) for answering questions about Eth1x64.

Authors

Naoya Okanami (@minaminao), LayerX/University of Tsukuba
Ryuya Nakamura (@nrryuya), LayerX

TL;DR

Shargri La

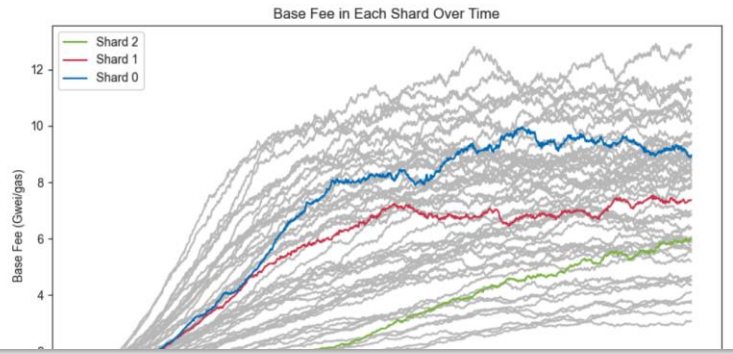
- We started a project called Shargri-La 17 , where we develop a transaction-level simulator for sharded blockchains. By using Shargri-La, testing against users' behavior on sharded blockchains will be available and help researchers to design or refine sharding protocols.

Results

Based on the model we have defined in the above, we perform simulations with a different set of assumptions.

Experiment 1: No user switches shards.

Before introducing the "shard switching" behavior of users in the simulation, we start with the case where users do not move from the shard they are allocated to at the start.

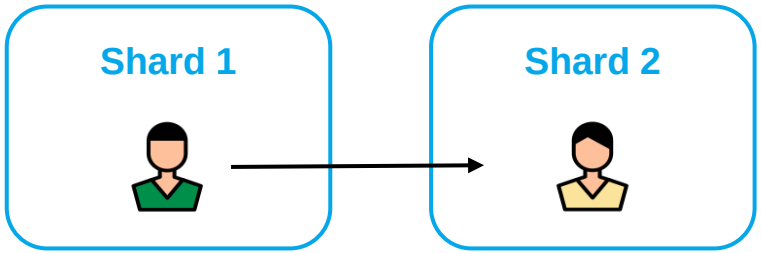


https://ethresear.ch/t/shargri-la-a-transaction-level-sharded-blockchain-simulator/7936

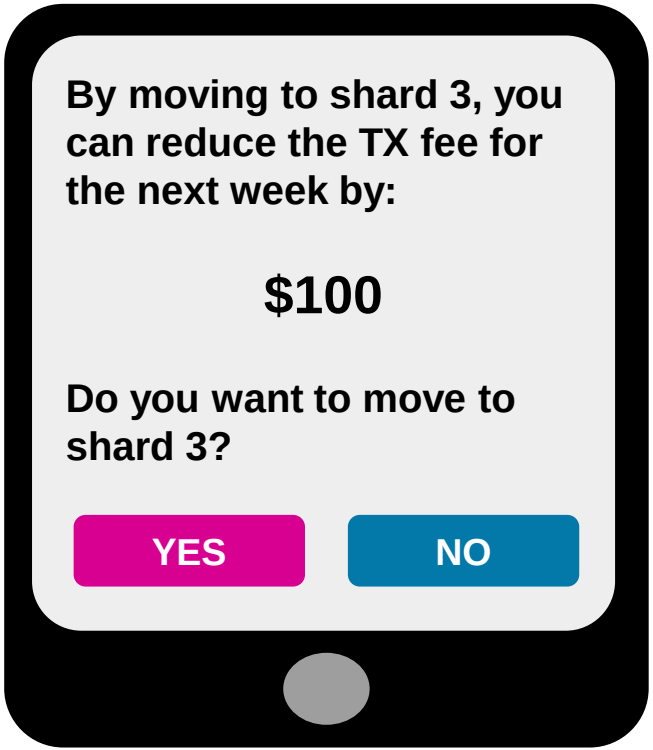
Shargri-Laでの実験結果の紹介

仮定: ユーザーは手数料が安いシャードに移動する

- 混雑しておらず、手数料が安いシャードを好む
- 自分の“お得意先”がいるシャードを好む（クロスシャードトランザクションによるコスト増加を避ける）

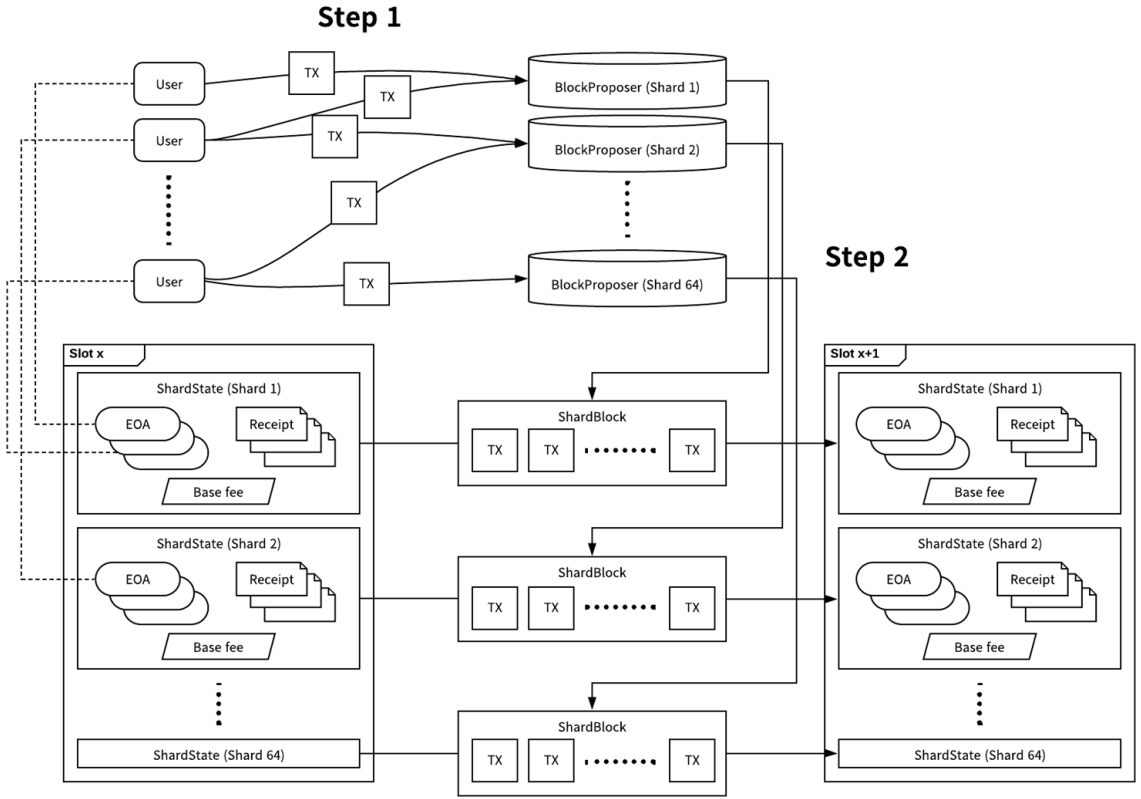


仮定: ユーザーは手数料が安いシャードに移動する



シャード移動は、ユーザーのクライアント（ウォレット）の機能と想定

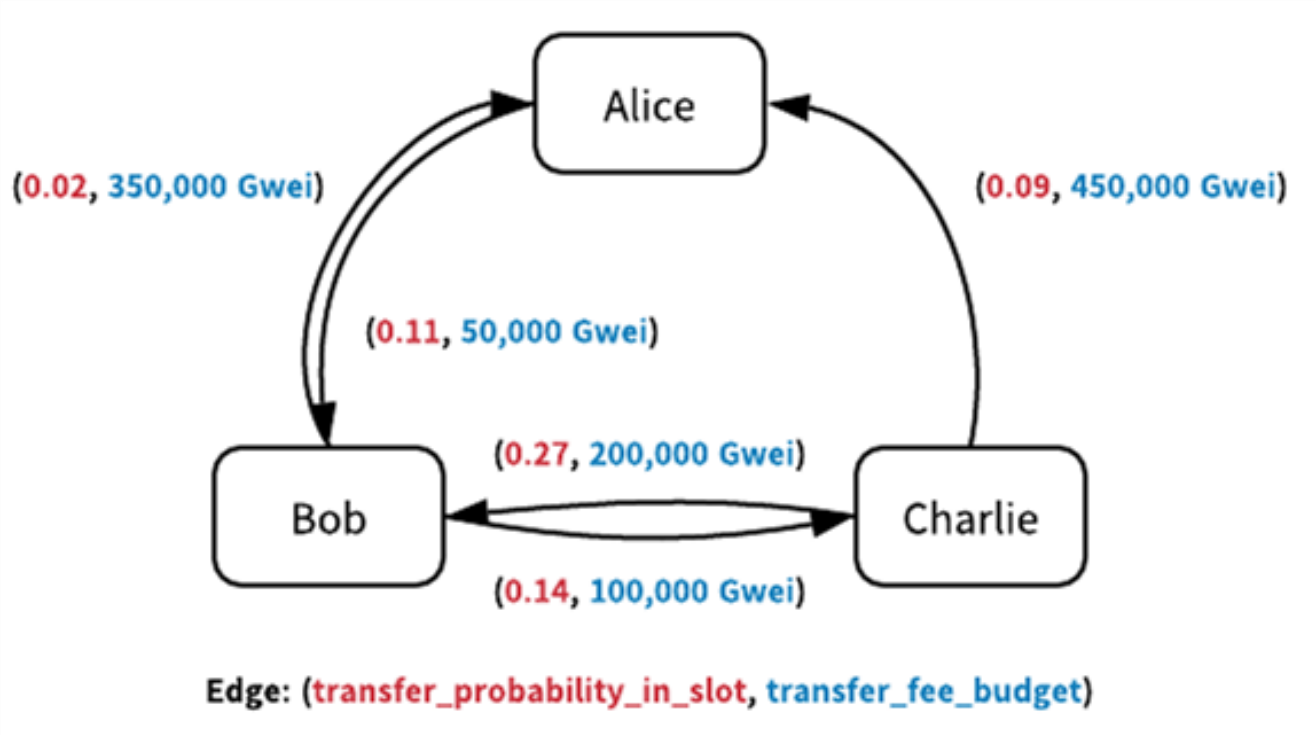
Shargri-La のシミュレーションモデル



トランザクション: ETHの送金のみ

- 一般的なスマートコントラクトの導入を断念
- 様々な点で複雑性が増すことを回避

UserGraph: トランザクションの需要のモデル



シミュレーション設定（抜粋）

- シャード数: 64
- ユーザー数: 10,000
- 一定割合のユーザーは100スロットごとにシャードを移動
  - 移動のアルゴリズムは複数定義（後述）
- UserGraphのパラメタは一様乱数により設定

手数料決定ルール: EIP-1559

- 現在のfirst price auctionを改良したルール
  - Eth1, Eth2で導入される見込み
- base fee (gas priceのデフォルト値のようなもの）が導入される
  - トランザクションの需要に応じて自動で調整される

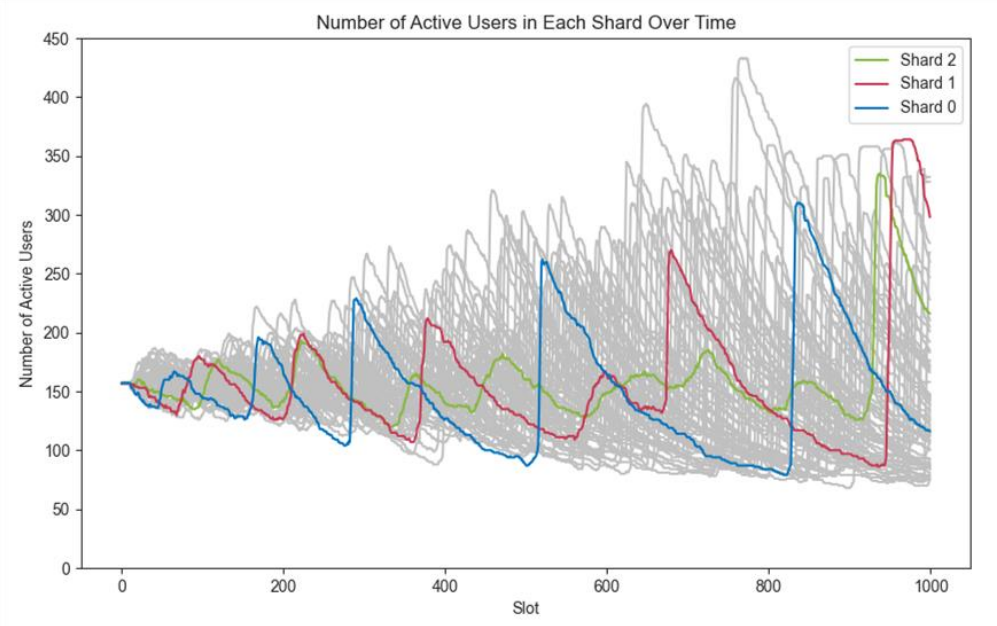
eip	title	author	discussions-to	status	type	category	created
1559	Fee market change for ETH 1.0 chain	Vitalik Buterin (@vbuterin), Eric Conner (@econoar), Rick Dudley (@AFDudley), Matthew Slipper (@mslipper), Ian Norden (@i-norden), Abdelhamid Bakhta (@abdelhamidbakhta)	https://ethereum-magicians.org/t/eip-1559-fee-market-change-for-eth-1-0-chain/2783	Draft	Standards Track	Core	2019-04-13

Simple Summary

A transaction pricing mechanism that includes fixed-per-block network fee that is burned and dynamically expands/contracts block sizes to deal with transient congestion.

実験内容、結果、考察（抜粋）

手数料期待値最小のシャードへ移動する場合

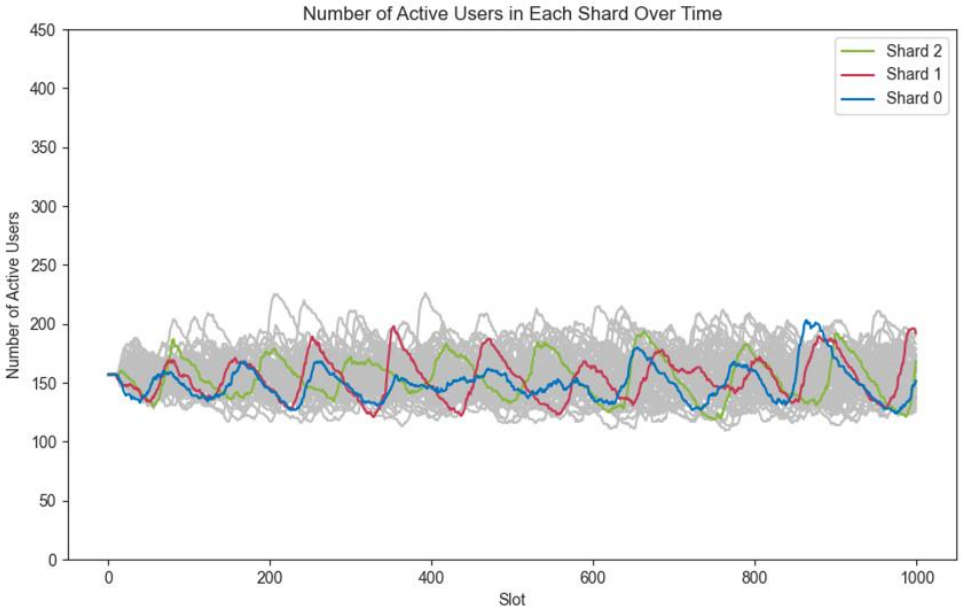


67%のユーザーが期待値最小シャードへ移動、
それ以外は動かない

- 手数料最小シャードにユーザーが殺到
- 「トランザクション詰まり」が起きていることが判明
- ユーザーにとって良いアルゴリズムとは言えないことが分かる

実験内容、結果、考察（抜粋）

手数料削減値の加重ランダムでシャード移動する場合

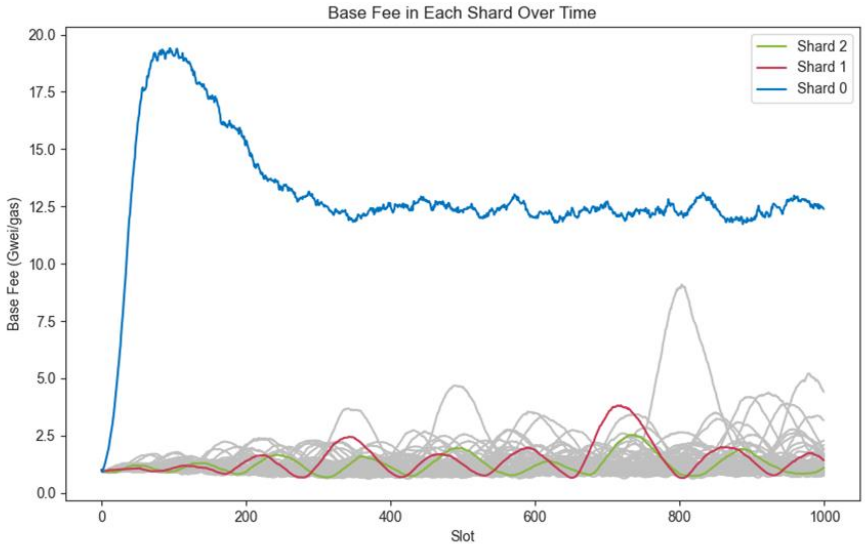


67%のユーザーが加重ランダムでシャードを移動、それ以外は動かない

- 特定シャードの急激な混雑やトランザクション詰まりは解決
- シャード移動しないユーザーに比べ、移動するユーザーの手数料減少を確認

実験内容、結果、考察（抜粋）

極端に人気なユーザーが存在する場合



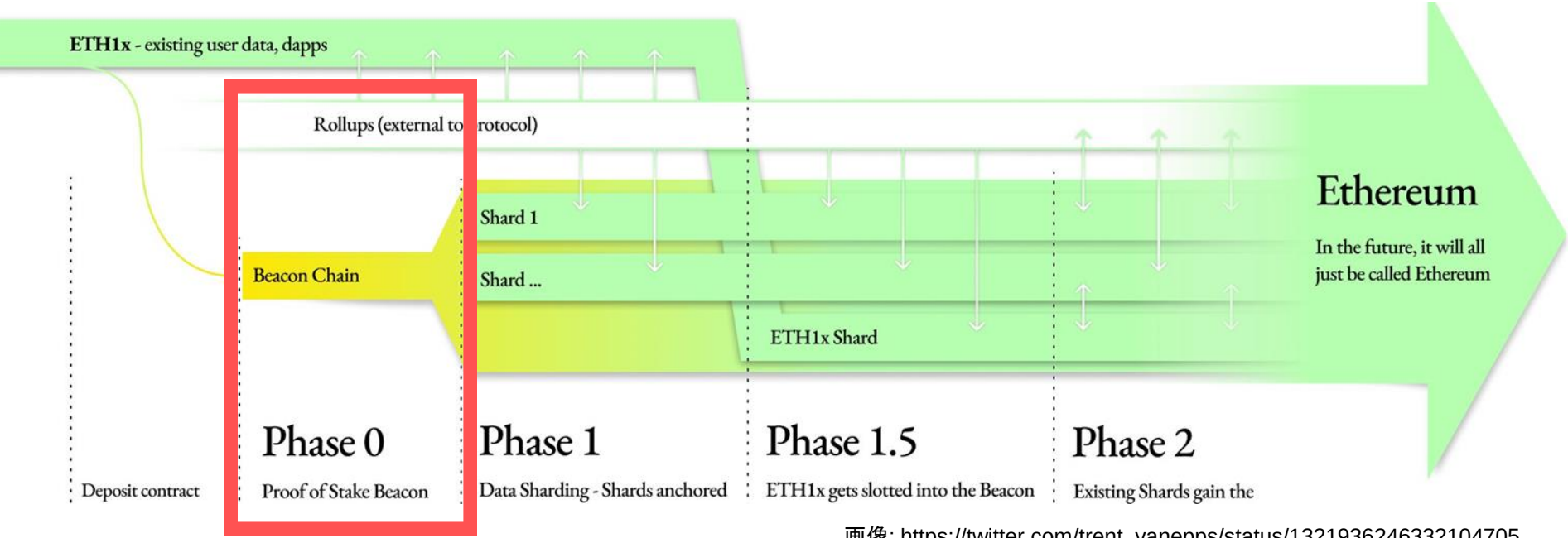
Shard 0に人気ユーザーが存在、67%のユーザーが加重ランダムでシャードを移動

- 人気ユーザー（全ユーザーの5%から送金される）が存在するシャードでは、手数料が高騰
- 一方、人気ユーザーと取引のないユーザーは手数料が安い他シャードに流れていく

Ethereum 2.0 Phase 1

Phase 0（ローンチ直前）

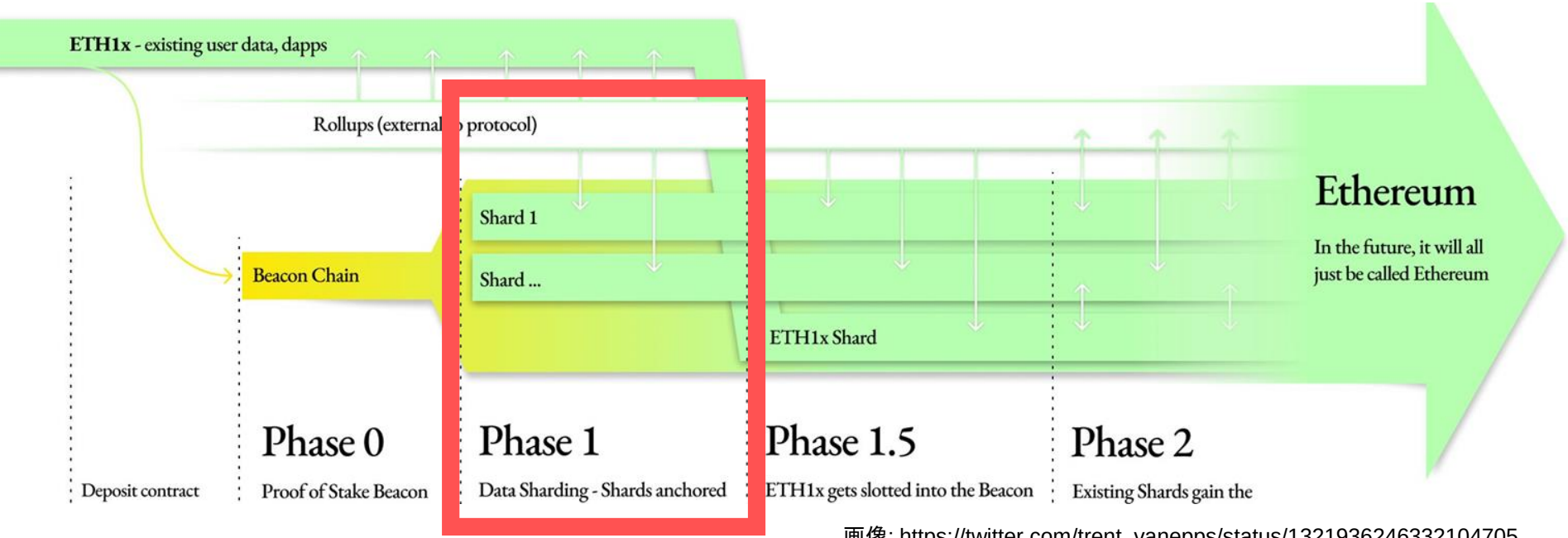
Beacon chainの導入のみ。シャードはなく、基本的に用途はない。



画像: https://twitter.com/trent_vanepps/status/1321936246332104705

Phase 1: Data Sharding

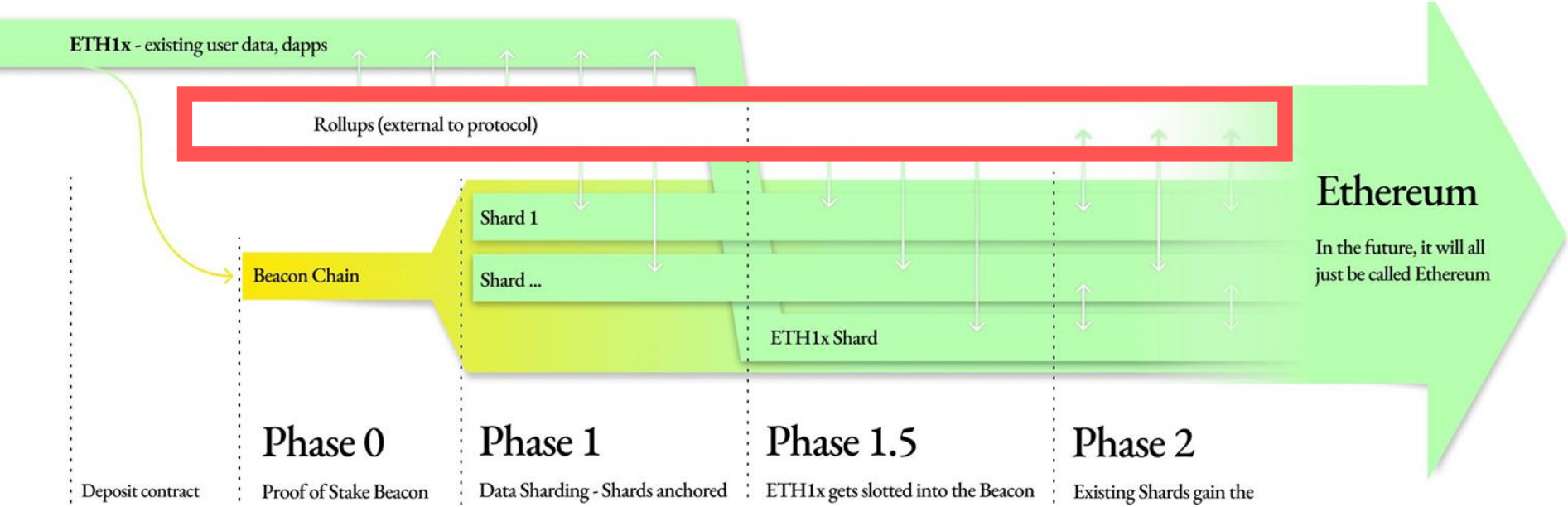
データが載せられるだけのシャーディング（後述）



画像: https://twitter.com/trent_vanepps/status/1321936246332104705

Rollup: Layer2のスループット向上技術

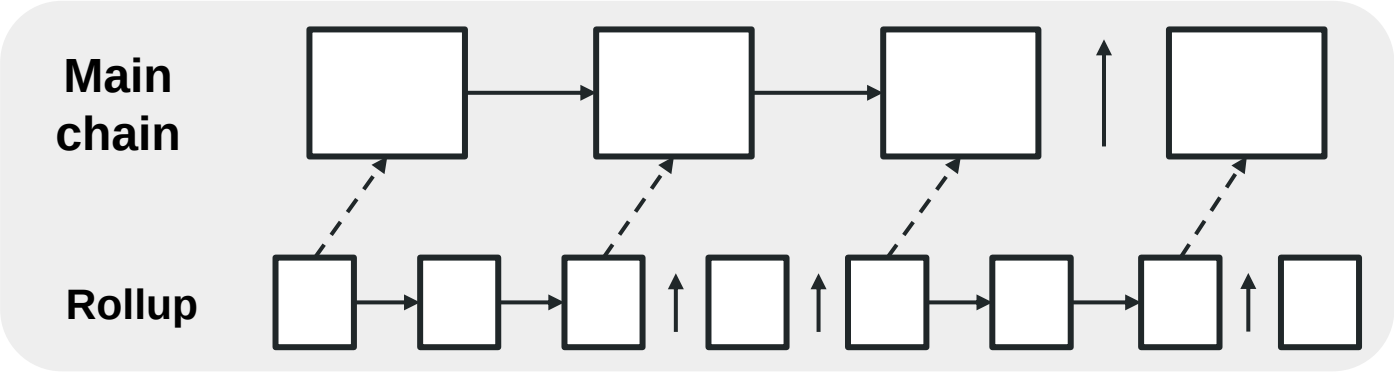
Ethereum 2.0のロードマップでも重要な役割



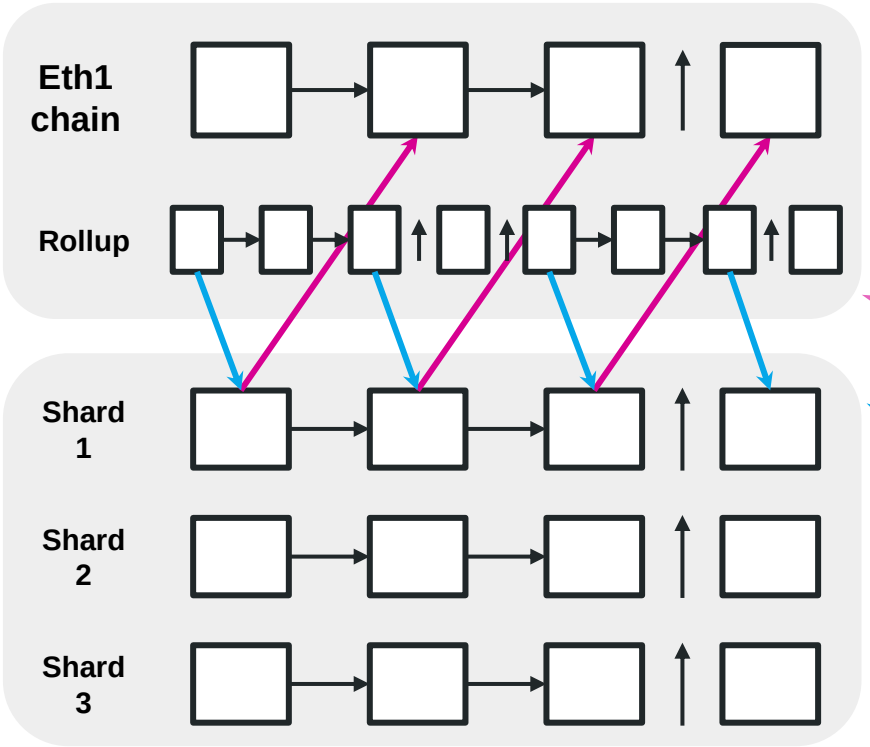
画像: https://twitter.com/trent_vanepps/status/1321936246332104705

Rollup: Layer2のスループット向上技術

- トランザクションはメインチェーンに置く（Plasmaとの違い）
- トランザクションの検証をオフチェーンで行う
  - ZK-SNARKsで検証の正しさを証明 → ZK Rollup
  - 不正な状態遷移をFraud proofで証明 → Optimistic Rollup



Phase 1: Rollupのデータ置き場



Eth1上にRollupのコントラクトが存在

Eth1では、Eth2のShardに書き込まれたデータのcommitmentを参照できる

Eth2のShardにRollupのトランザクションのデータが書き込まれる

Phase 1: Fee Market Contract

- Shard chainには「トランザクション」の概念がない
  - ブロック生成者がただbyte列を詰められるだけ
- Eth1上でRollup operatorは手数料を払う
  - デポジットをブロック生成者が引き出す形

ShardBlock

```
class ShardBlock(Container):
    shard_parent_root: Root
    beacon_parent_root: Root
    slot: Slot
    shard: Shard
    proposer_index: ValidatorIndex
    body: ByteList[MAX_SHARD_BLOCK_SIZE]
```

https://github.com/ethereum/eth2.0-specs/blob/dev/specs/phase1/beacon-

A fee market contract for eth2 shards in eth1

Sharding ■ fee-market

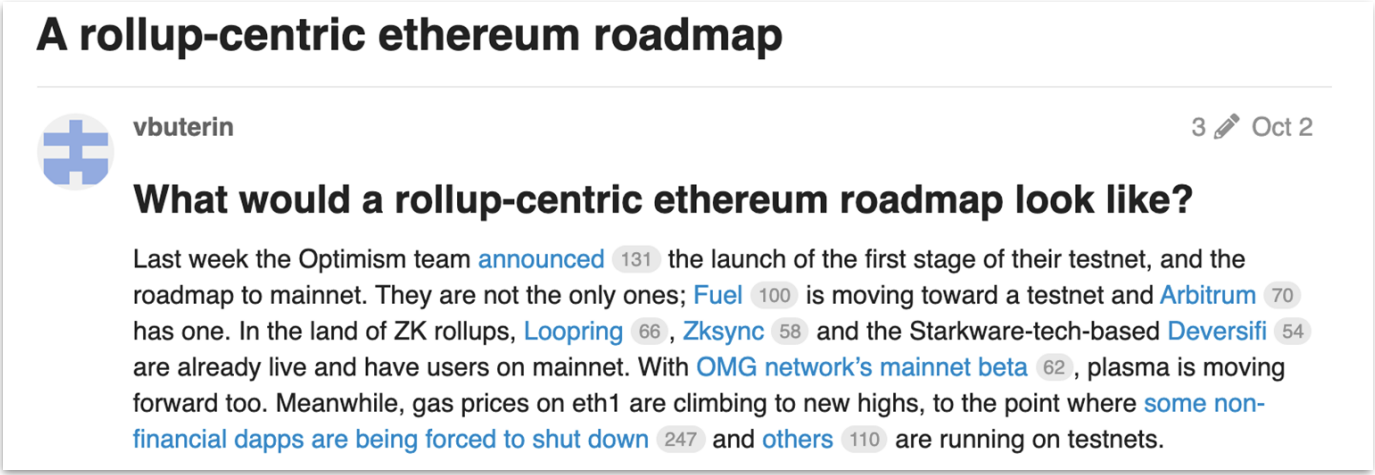
vbuterin 2 9d

The goal of this post is to propose a system that would live on the eth1 chain and provides incentives for validators to include their preferred data in eth2 blocks. This would allow sequencers and other users that want data published on eth2 to be able to do so in real-time without needing to run a large number of validators themselves.

https://ethresear.ch/t/a-fee-market-contract-for-eth2-shards-in-eth1/8124

“Phase 1.5 and done”

Rollupがあれば、Layer1にVMは不要？Eth1がEth2にシャードとして取り込まれる (Phase 1.5) たら、それで十分？



A rollup-centric ethereum roadmap

vbuterin — 3 Oct 2

What would a rollup-centric ethereum roadmap look like?

Last week the Optimism team announced 131 the launch of the first stage of their testnet, and the roadmap to mainnet. They are not the only ones; Fuel 100 is moving toward a testnet and Arbitrum 70 has one. In the land of ZK rollups, Loopring 66, Zksync 58 and the Starkware-tech-based Deversifi 54 are already live and have users on mainnet. With OMG network's mainnet beta 62, plasma is moving forward too. Meanwhile, gas prices on eth1 are climbing to new highs, to the point where some non-financial dapps are being forced to shut down 247 and others 110 are running on testnets.

https://ethereum-magicians.org/t/a-rollup-centric-ethereum-roadmap/4698

まとめ

- シャーディングの導入により、ユーザーの行動やアプリケーションの設計は大きく変わる
- Phase 1以降の方向性を決める重要な議論が進んでおり、将来的なユースケースに大きく影響する
- 積極的に意思表示をしていきましょう！

おしまい