Ethereumの近況・Ethereum 2.0

中村龍矢 (LayerX)
2020.09.25
第2回BSEC研究会

自己紹介: 中村龍矢

- 株式会社LayerX 執行役員 兼 LayerX Labs 所長
  - ブロックチェーンの研究開発
  - ブロックチェーンを用いた事業開発
- 世界経済フォーラム Global Shaper
- IPA 未踏 2020

研究活動: Ethereumへのコントリビューション

- 主にLayer1のセキュリティ周り
- 国際カンファレンスでの登壇
- Ethereum 財団 グラント採択 (国内初)

EDCON 2019 @シドニー

仮想通貨（暗号資産）ニュース

イーサリアム2.0、2020年初頭のリリースに向け監査・検証の段階へ

LayerX中村龍矢氏の研究で2つの脆弱性が修正済み

日下 弘樹　2019年11月11日 12:44

ツイート リスト　B! 2　Pocket 3　いいね！ 6　シェア

(Image: Shutterstock.com)

Ethereum財団は11月8日、Ethereum 2.0のアップデート情報を週次で報告する短信の第3回を公開した。2020年初頭を予定しているEthereum 2.0 フェーズ0のリリースに向け、アルゴリズムの監査や脆弱性の検証が需要を増してきている。短信では、LayerXの中村龍矢氏の功績が評価された。同氏の研究により、2つの脆弱性が解消されたという

研究活動: 論文発表

- 国内学会 (CSS'19, SCIS'20) への参加
- 国際学会 (FC'20) への参加

SCIS 2020 @高知

Workshop on Trusted Smart Contracts
@ Financial Cryptography 2020 (マレーシア)

研究活動: 自社ソフトウェア開発

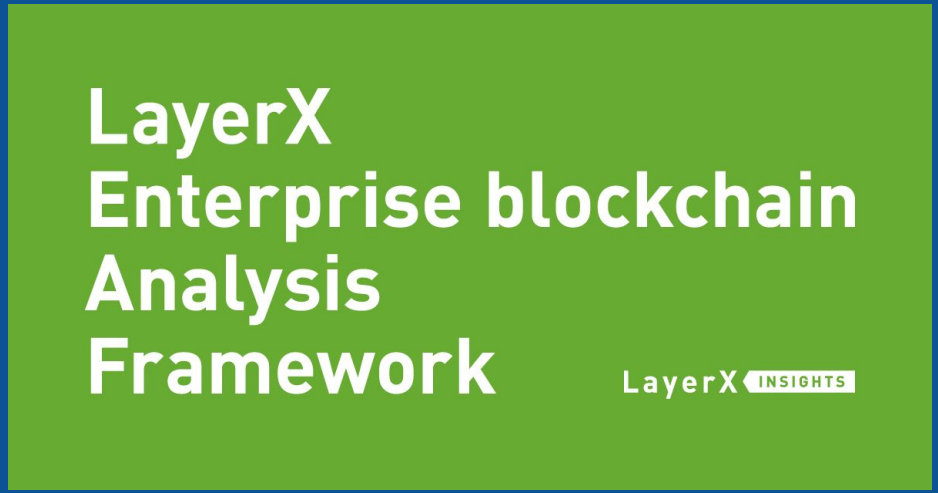
- 実際のブロックチェーン事業のニーズを元にソフトウェアを開発
- オープンソースとして公開

Anonify: プライバシーモジュール
https://github.com/LayerXcom/anonify

Cordage: クロスチェーンモジュール
https://github.com/LayerXcom/cordage

研究活動: エンタープライズブロックチェーンの比較

- Corda、Hyperledger Fabric、Quorumについての分析結果
- 実際のブロックチェーン開発での経験をもとに、弊社エンジニア中心にレポートを執筆



https://layerx.co.jp/publications/leaf_basic/

企業・大学との共同での研究活動・実証実験

LayerX Labs、東京工業大学 首藤研究室と ブロックチェーンのコンセンサスアルゴリズムに関する共同研究を開始 –国内外の学術機関とのオープンイノベーションを強化–

2020.8.28

LayerX　東京工業大学 Tokyo Institute of Technology

ブロックチェーン技術を活用したMaaS領域における実証実験を開始 -事故発生の自動検出と保険金支払い業務自動化の実証-

2020.8.17

SOMPO ホールディングス　SOMPO 損保ジャパン

NAVITIME　LayerX

ウフルとLayerXがIoT・ブロックチェーンで協業 –安全・安心なデータ流通の実現に向けて–

2020.8.3

uhuru　LayerX

交通の遅れ補償、申告なしで即時払い　損保ジャパン

金融最前線

2020/8/16 0:00 | 886文字 ［有料会員限定］

保存　共有　印刷　その他

損保ジャパンはJR埼京線などの遅延情報をもとにした実証実験を始める（東京・豊島の池袋駅）

今日のトピック

Ethereumエコシステムの近況を以下の項目別に紹介

- Eth1: 現行のEthereumチェーン
  - Defi（分散型金融）
  - Layer 2
- Eth2 (Serenity) : プロトコルアップグレードプロジェクト
  - PoS
  - Sharding
- Q&A

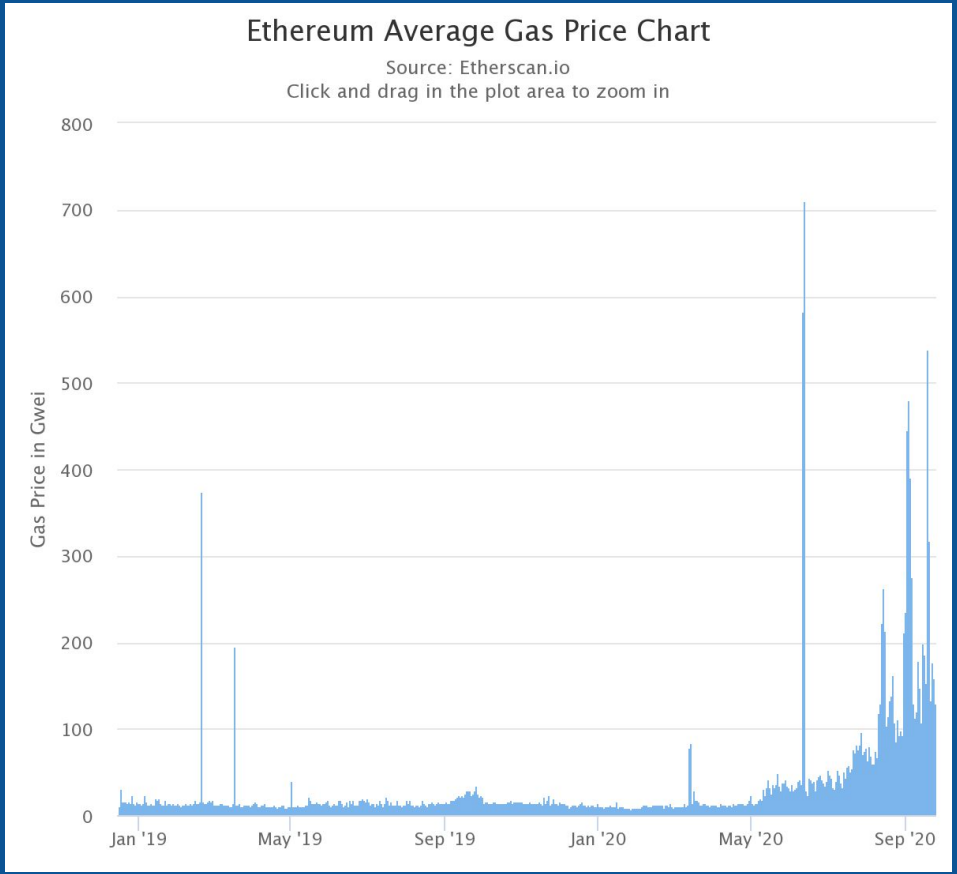
私とEthereumの関わり

2年間程度、セキュリティ関連のプロジェクトに従事

- 2018年: スマートコントラクトのセキュリティ
  - スマートコントラクト言語Vyperのコンパイラ開発への参加
  - Vyperコントラクトの形式的検証
- 2019年: コンセンサスプロトコルの理論研究
  - CBC Casperの形式的検証（CVC'19 採択）
  - Ethereum 2.0の脆弱性発見と解決策提案
  - Ethereum Foundation グラント採択（国内初）
- 2020年: シャーディングの研究
  - 負荷集中現象の分析（WTSC'20 採択）
  - シミュレーターの開発（IPA 未踏 2020 採択）

Eth1

最近のEthereum: トランザクション手数料が異常な高騰



- 単純なETH送金でも手数料が数百円から数千円まで。。
- 何が起きたのか？

Defi (分散型金融)

Ethereum上でのDefiの盛り上がり

- 分散型取引所 (DEX)
  - Uniswap (プール型DEX) の取引高の増加
- ステーブルコイン
  - Tether（運営企業による法定通貨等の担保）
  - Maker（スマートコントラクトでの暗号通貨担保）
- P2Pレンディング、etc.

Rank	Address	Fees Last 3hrs	% Used 3hrs	Fees Last 24hrs	% Used 24hrs
1	Uniswap V2: Router 2	$70,281.16 (201.73 Eth)	23.22%	$640,422.53 (1,838.23 Eth)	21.45%
2	Tether: USDT Stablecoin	$17,404.25 (49.96 Eth)	5.62%	$320,839.71 (920.92 Eth)	10.14%
3	0xe33c8e3a0d14a81f0dd7e174830089e82f65fc85	$10,379.02 (29.79 Eth)	2.33%	$58,861.32 (168.95 Eth)	1.63%

Uniswap

流動性プール型のDEX

- 交換するコイン（例: ETHとMKR）ごとに流動性プールが存在
  - ユーザーはコントラクトにデポジット（流動性提供の見返りとして報酬）
  - プールされているコインを買うことができる
    - ここで、それぞれのコインのプールの金額の積が一定になるよう価格調整
      - 例:（ETHのプール額）*（MKRのプール額）= 一定
- 一般的な（中央集権的な）取引所に匹敵or 上回る取引額
- 研究も徐々に進む
  - 形式化および価格の安定性の分析[AKC+19]
  - ボットによる裁定取引の調査[DGK+19] (IEEE S&P'20)

→ 今後はこのようなアプリケーションレイヤーの研究も盛んに

Layer2

Non-custodialを守りつつ、オフチェーンで状態遷移するスケーリング技術

- State channel
  - Payment channelの一般化
    - Ethereumでは、送金に限らず、様々なスマートコントラクトの実行や、デプロイすらも可能
  - ユーザー間でチャネルを開き、全員の合意の元状態遷移
- Plasma/Rollup (Commit-chain)
  - Operatorが別のチェーンを運営（Plasmaチェーン、Rollupチェーン）
  - ユーザーはこのチェーンに資産をデポジット・引き出し
  - Operatorはオフチェーンの状態のハッシュをオンチェーンに書き込む
    - Operatorの不正があってもオンチェーンで防御可能
      - Custodialなサイドチェーンとの違い

Layer2: Rollup

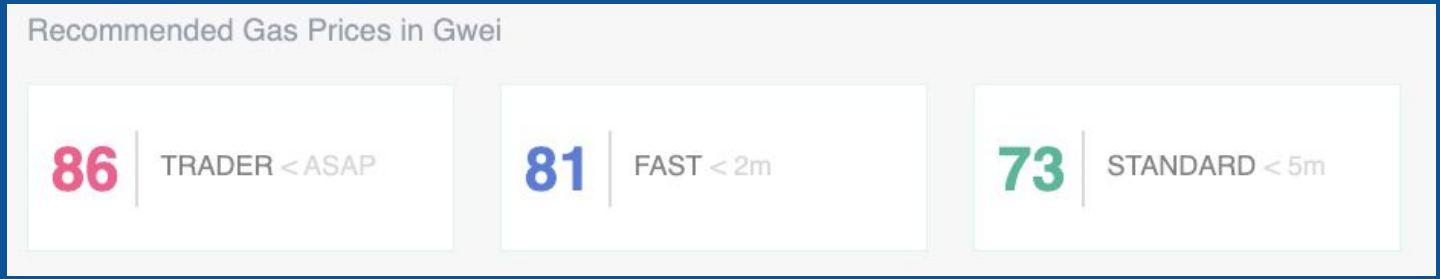
データはオンチェーンだが、検証をオフチェーンで行う手法

- Plasma（2017年誕生）の後継
  - Plasma: PlasmaチェーンのTXデータはオンチェーンにはない
    - ユーザーは自分に関係するOperatorの不正を自分でchallengeして守る
      - UXや柔軟性の課題、複雑さ
  - Rollup: RollupチェーンのTXデータはオンチェーン
    - Operatorの不正は誰でもchallengeでき、全体的にシンプル化
      - 複雑なアプリケーションも実行可能
- 二種類のRollup（状態遷移の検証方法の違い）
  - Optimistic Rollup: Challenge方式（一定のchallenge期間あり）
  - ZK Rollup: Operatorが状態遷移の正しさをゼロ知識証明(ZK-SNARKs)
    - ZK ZK Rollup: Zcashライクな状態遷移ルールにし、プライバシーも担保
- いくつかのRollupがメインネットで稼働中（さわれます）

EIP-1559: トランザクション手数料決定ルールを変更

トランザクション手数料決定ルールを変更

- 現在のBitcoin/Ethereumの手数料モデル: First price auction
  - ボラティリティが高く、予想しにくい
- EIP-1559: BASE FEEを導入
  - 手数料の「デフォルト値」のようなもの
  - 需要に応じてBASE FEEを調節
    - ブロックのキャパシティに対する
- Ethereum 2.0（後述）でも導入される見込み

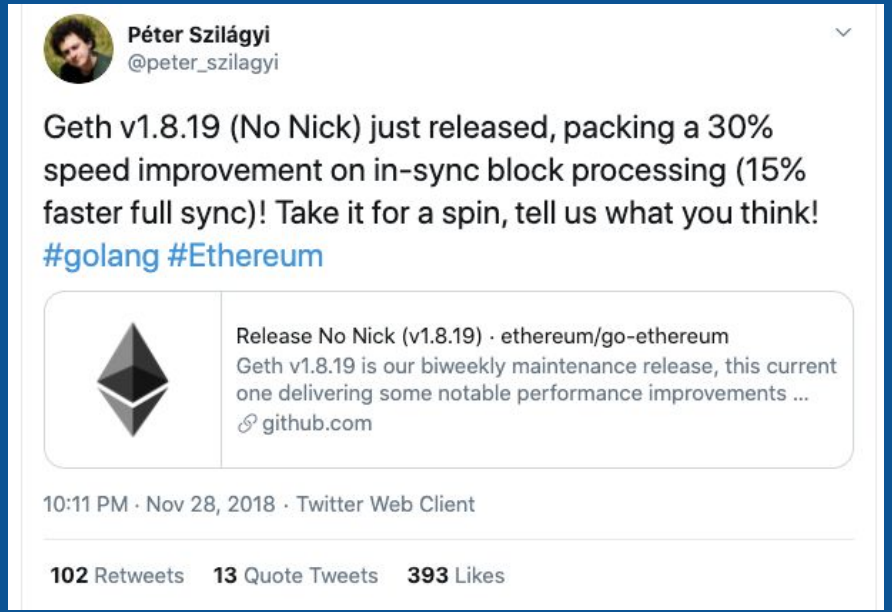


https://ethgasstation.info/

Eth 1.x

既存のPoWチェーンとその周辺エコシステムを改善するプロジェクト群

- Gethなどクライアントの改善
- EVMの改善
- EIPの管理
- 開発者向けツール



https://twitter.com/peter_szilagyi/status/1067767889342681088

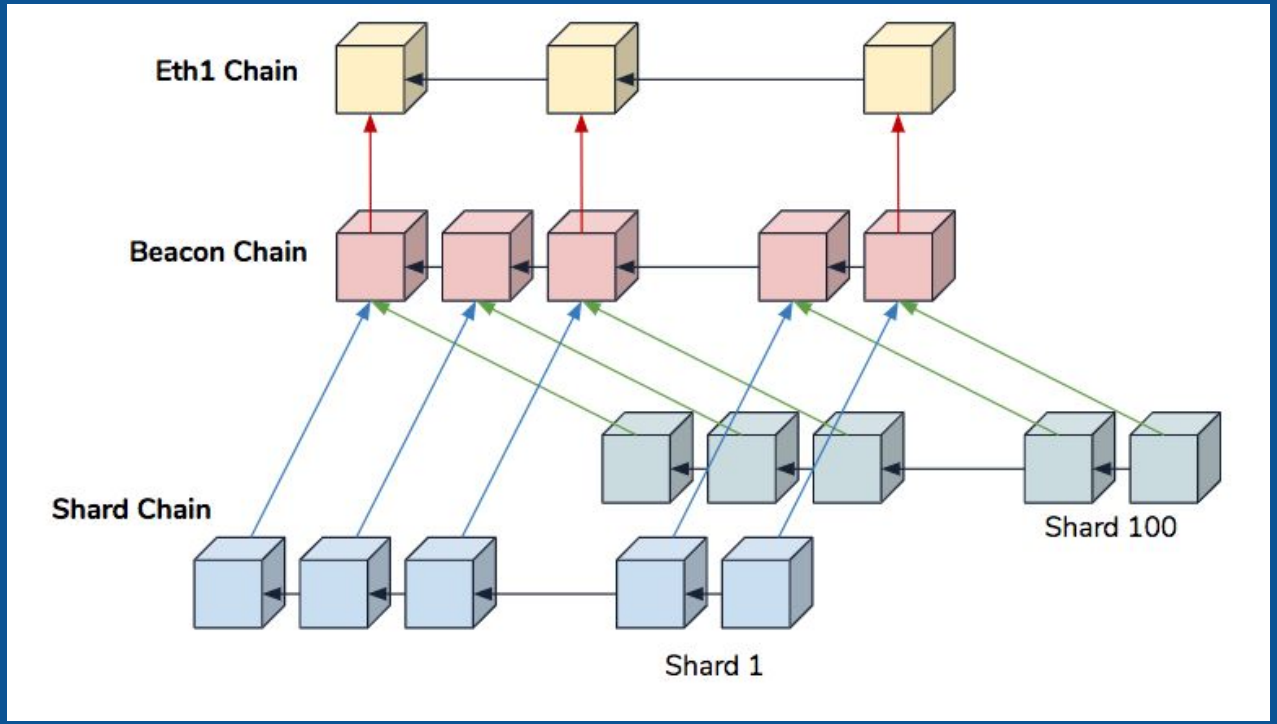
Eth2

Ethereum 2.0 (Eth2, Serenity)

Ethereumの抜本的なプロトコルアップグレードであり、最大のプロジェクト

- 複数の研究開発プロジェクトが包含されている
  - PoSとSharding導入
  - EVMのWASM化
  - Stateless client
  - etc.
- 2018年に各研究プロジェクトを統合する形で始動
  - 各プロジェクトは以前から動いていた
- Ethereum Foundationを中心に仕様策定 + 10前後の企業がクライアント開発に関与

Ethereum 2.0 アーキテクチャ

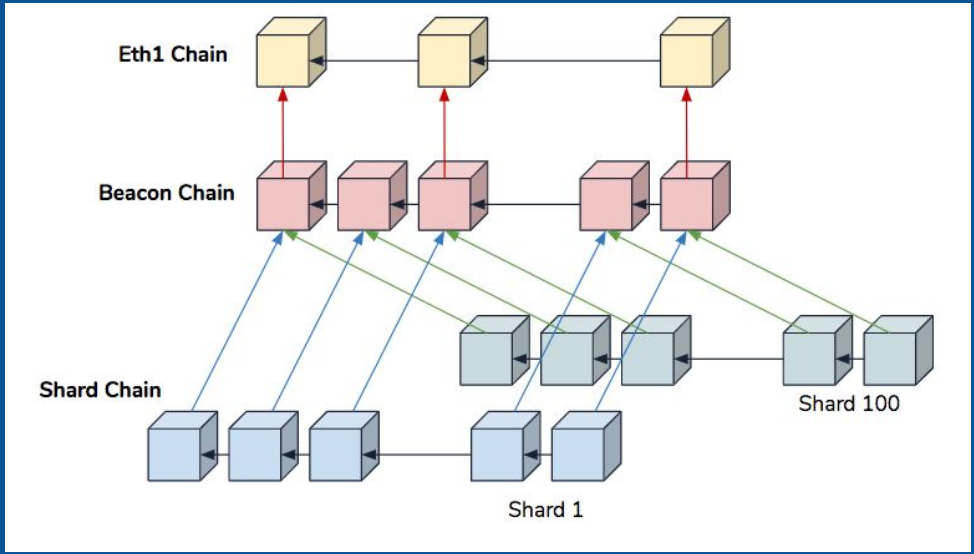


Slides are from Hsiao-Wei Wang:
https://docs.google.com/presentation/d/1G5UZdEL71XAkU5B2v-TC3lmGaRIu2P6QSeF8m3wg6MU/edit#slide=id.g3c326bb661_0_58

Eth1 Chain

現行のPoWチェーン

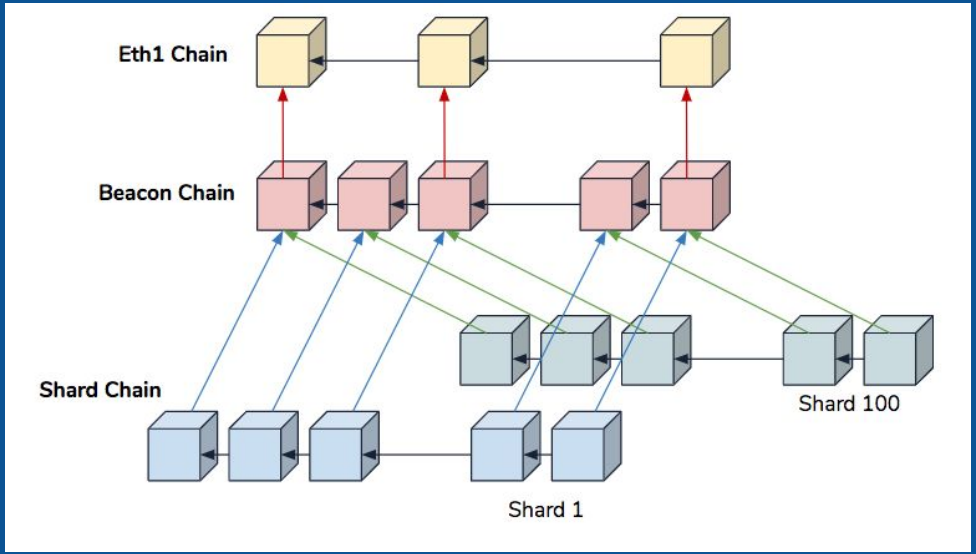
- Eth2は基本的に別のチェーンをゼロから作って、現状のチェーンと接続するプロジェクト
- デポジットコントラクトにETHをデポジットすることで、Beacon Chain側でアカウントが発行される（予定）



Beacon Chain

全体を管理するチェーン

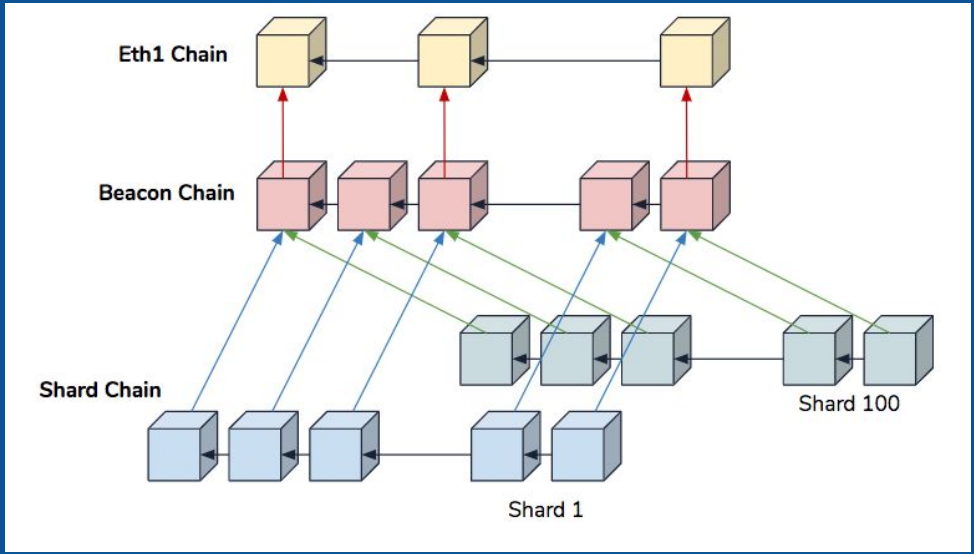
- 乱数生成、バリデータの各シャードへの割り当て
- 各シャードのstate rootを記録
  - これにより、Merkle proofを使ってシャード内のイベントを検知できる
  - これがクロスシャードコミュニケーションの基礎になる



Shard Chain

実際にユーザーが使うチェーン

- コントラクト・アカウントもここに置かれる



Ethereum 2.0 ロードマップ

- Phase 0: Beacon chainのみ
  - PoSの実験的な意味合いが強い(最初はETHのtransferすらできない)
  - 開発はほぼ完了、そろそろ開始
- Phase 1: Shard chain誕生
  - ただしデータ記録のみ(VMなし)
  - Rollupなどに使える
- Phase 1.5: Eth1チェーンを停止し、Eth2に取り込む
- Phase 2: シャード内でVM使用可能に
  - WebAssembly化されたEVM（eWASM）など
- Phase 3以降:
  - 上記以外の様々な改善

Ethereum 2.0 の現状

Phase 0の仕様は固まり、ローンチに向けたテスト・監査・検証が中心

- Phase 0の複数のテストネットが実施
  - テストネットMedallaでインシデント発生
    - 時刻同期周りのバグ→修正パッチで初期化処理をミス→バリデーターが大量にスラッシング
- Phase 0の開始タイミングはコミュニティで未だ議論中
  - （大雑把にいえば）慎重派vs 推進派
  - ましてや、Phase 1,2の開始時期は定まっていない

Phase 0のEIPがオープン

- Eth2のコアメンバーらによりPhase 0開始に向けたEIPが提案
- Eth2とEth1の別チームのメンバーが交わる
  - 「そもそもこれはEIPなのか？」から意見が分かれる

PoS/Casper

PoS

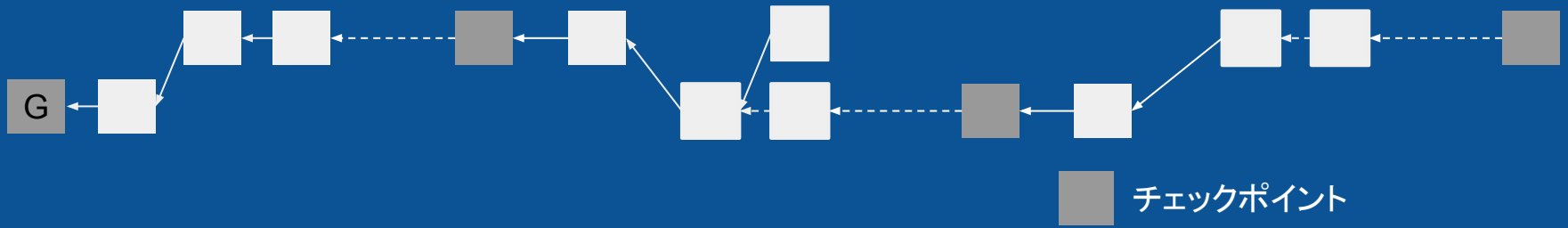
Eth2では、PoWからPoSに変更

- PoSも色々ある
- Eth2は、「Deposit型」「Validator数上限なし」「Slashあり」のPoS
  - 32 ETHをStakeすることでValidatorになることができる
    - ⇔ 暗号通貨保有者の中から勝手にValidator選出するPoS (Ouroboros)
    - ⇔ Validator数に上限があるPoS (Cosmos, Algorand, DPoS系)
  - 二重投票 (equivocation) や投票への不参加 (omission) によりStakeが没収
    - ⇔ Stakeの没収は行わないPoS (Avalanche)
- PoS向けのコンセンサスアルゴリズムとして、Casper FFG + LMD GHOSTを採用

Eth2のコンセンサス

LMD GHOSTでチェーンを収束させ、Casper FFGでファイナリティを与える

- 乱数でブロック生成者を選出、フォークチョイスルールMD GHOSTに従う
  - GHOST (FC'15) の亜種
- 一定間隔 (~6分) おきにブロックがチェックポイントと定義される
- ノードはメインチェーンのチェックポイントに対し**投票**を行う
- (大雑把に) 二回連続で2/3のノードが投票したブロックをファイナライズ
- “Finality Gadget” と呼ばれるアプローチ



Casper FFG

Finality gadget = ブロックチェーンにファイナリティを与える“パーツ”

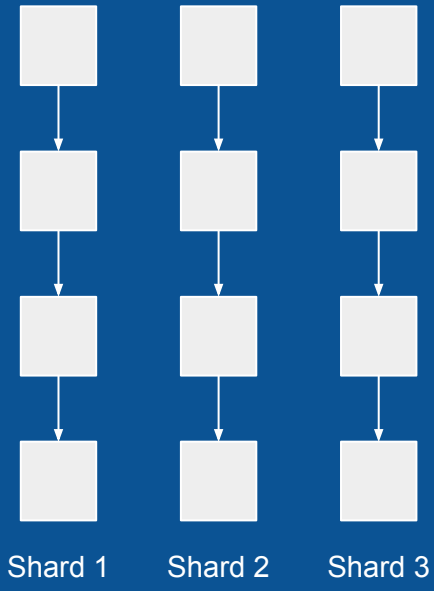
- Casper FFGのファイナリティは、本質的にPBFT等と類似
  - Hotstuff (PODC’19) で指摘
- メリット vs 対Nakamoto:
  - Asynchronous safety (ネットワーク分断等があってもsafetyが維持される)
    - Nakamoto consensusはsynchronous safetyのみ
- メリット vs 対BFT:
  - ブロック生成頻度とファイナリティのサイクルの分離
    - ブロック生成頻度を下げずにより多くのノードを扱える
    - ファイナリティにかかる時間とのトレードオフ

シャーディング

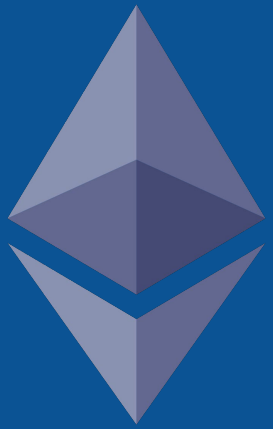
シャーディングとは

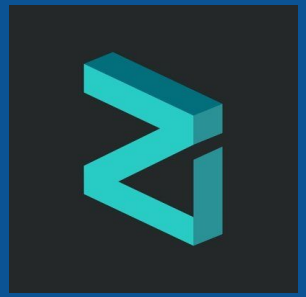
広義: 複数のブロックチェーンで一つの分散台帳を実現する

- それぞれのシャードは異なるブロックチェーン
  - 別々のアカウント・コントラクトを管理する
- 目的: スケーラビリティの改善
  - 非常に乱暴に言えば, シャード数だけTPSが上がる



シャーディング @パブリックチェーンコミュニティ





Polkadot.

シャーディング @アカデミア

トップ会議に論文が通っている

発表年	論文名	学会
2016	A Secure Sharding Protocol For Open Blockchains	CCS 2016
2017	OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding	S&P 2018
	Chainspace: A Sharded Smart Contracts Platform	NDSS 2018
2018	RapidChain: Scaling Blockchain via Full Sharding	CCS 2018
	Towards Scaling Blockchain Systems via Sharding	SIGMOD 2019
2019	Monoxide: Scale Out Blockchain with Asynchronous Consensus Zones	NSDI 2019

シャーディングとは

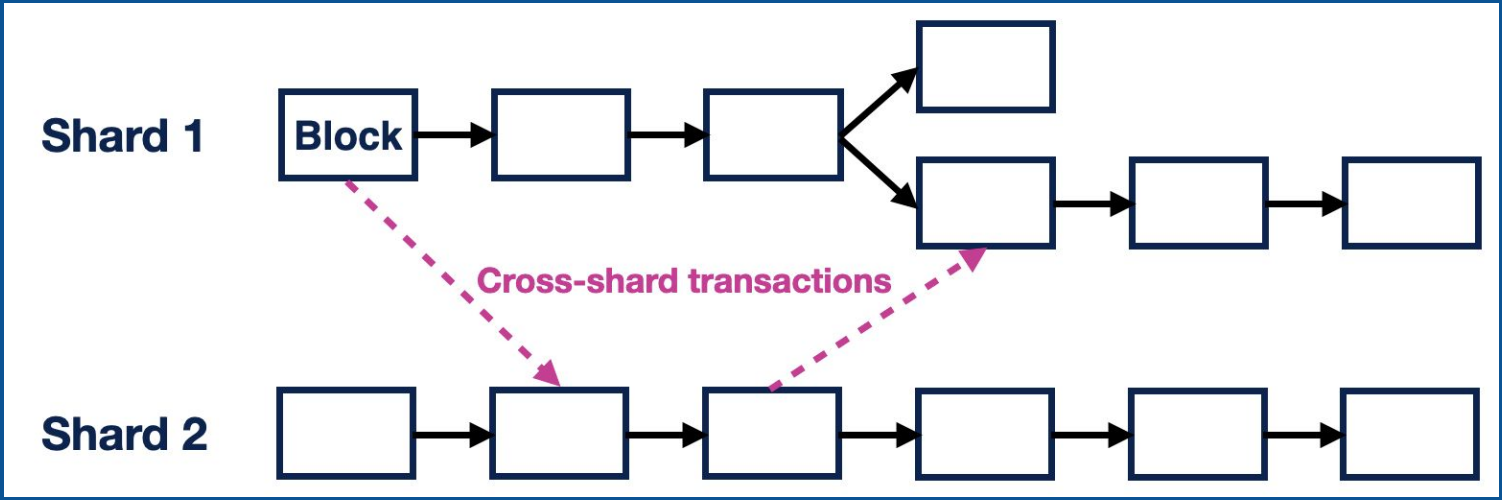
狭義: 複数チェーンに分けることに加え、以下の定義を満たす

- 条件 1: 各シャードに異なるノードが割り当てられる
  - 1ノード当たり管理するべきステートのサイズを増やさない
- 条件 2: セキュリティは“あまり”落ちない
  - 単純にN個に分割するとセキュリティは1/Nになる
  - 定番の手法（詳細は割愛）
    - 攻撃者が予測できない乱数を使ってValidatorをシャードに割り当てる
    - 特定shardで不正なブロックを検知したら全Validatorで巻き戻す

クロスシャードトランザクション

異なるシャードのウォレット・コントラクト間のやりとり

- 送金だけであればシンプル
  - 送金元シャードでburnして送金先でmintする



クロスシャードトランザクション

異なるシャードのウォレット・コントラクト間のやりとり

- “Train-and-hotel” 問題: Yankingによる解決
  - コントラクトを削除し、そのコピーを他シャードに移動
  - クロスシャードの操作を単一シャードの操作に落とし込める

```
contract HotelRoom123 {
        move_to_shard(uint256 shard_id)
        book()
}
```

私のシャーディング関連研究の紹介

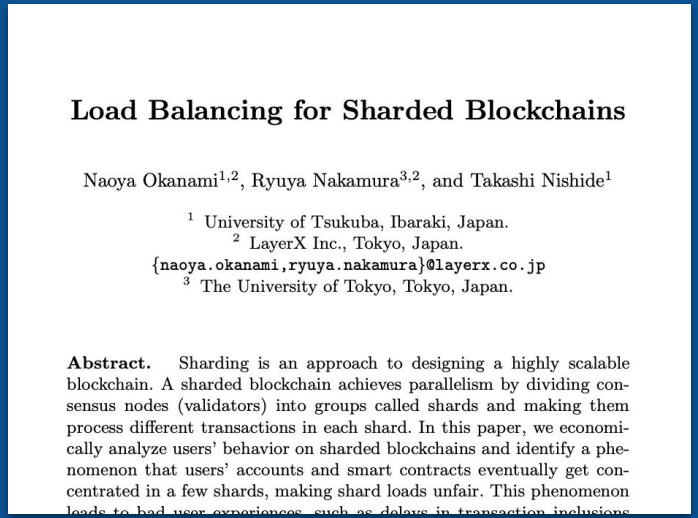
シャーディングのリサーチクエスチョン

シャーディングには色々な研究課題がある（現実で使われていないため、特にユーザー行動周りは未知数）

- クロスシャードTXのプロトコルはどれがベスト？パラメータは幾つに設定すべき？
- ユーザーは幾つのシャードにアクセスできる必要がある？
- 特定シャードばかり使われたらどうなる？
- 全体的にUX悪化しない？

負荷集中現象と負荷分散プロトコルの提案

岡南・中村・西出の論文@4th Workshop on Trusted Smart Contracts

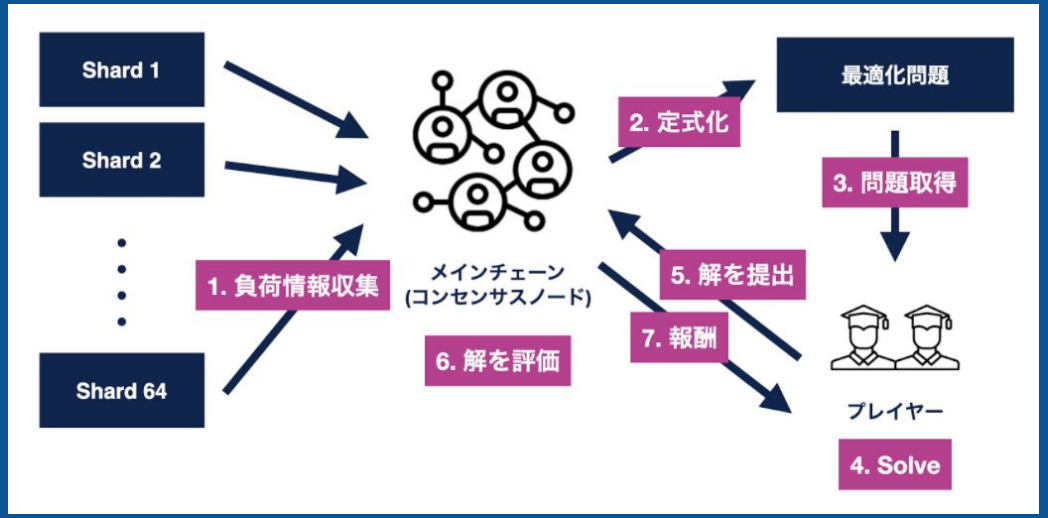


Load Balancing for Sharded Blockchains

Naoya Okanami[1,2], Ryuya Nakamura[3,2], and Takashi Nishide[1]

[1] University of Tsukuba, Ibaraki, Japan.
[2] LayerX Inc., Tokyo, Japan.
{naoya.okanami,ryuya.nakamura}@layerx.co.jp
[3] The University of Tokyo, Tokyo, Japan.

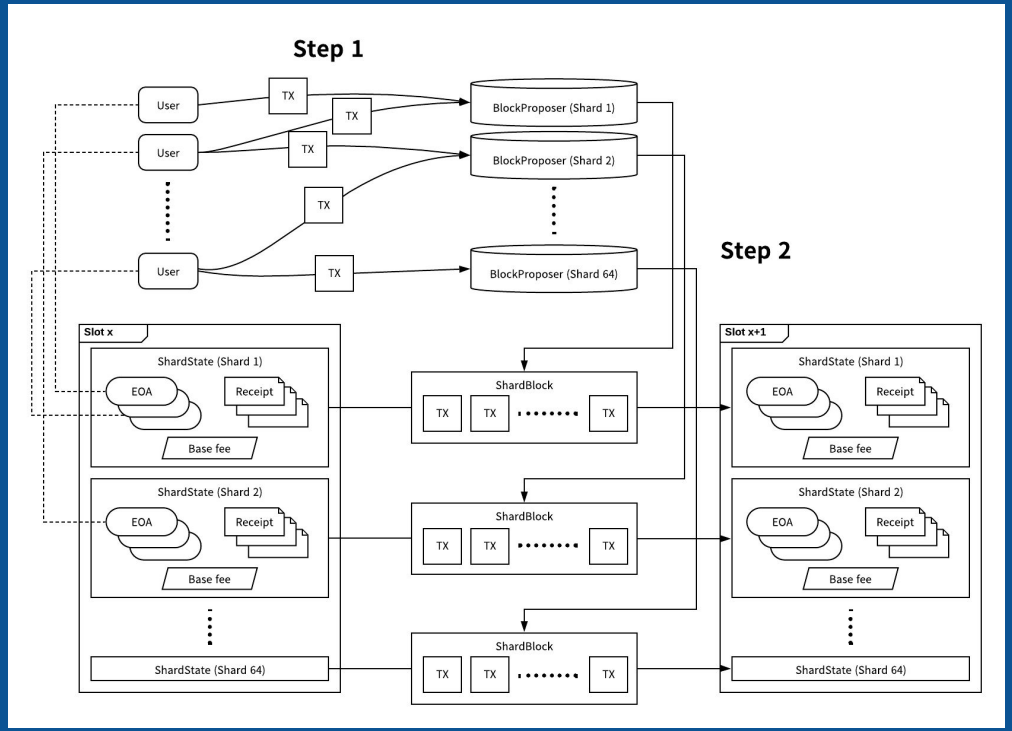
Abstract. Sharding is an approach to designing a highly scalable blockchain. A sharded blockchain achieves parallelism by dividing consensus nodes (validators) into groups called shards and making them process different transactions in each shard. In this paper, we economically analyze users' behavior on sharded blockchains and identify a phenomenon that users' accounts and smart contracts eventually get concentrated in a few shards, making shard loads unfair. This phenomenon leads to bad user experiences, such as delays in transaction inclusions

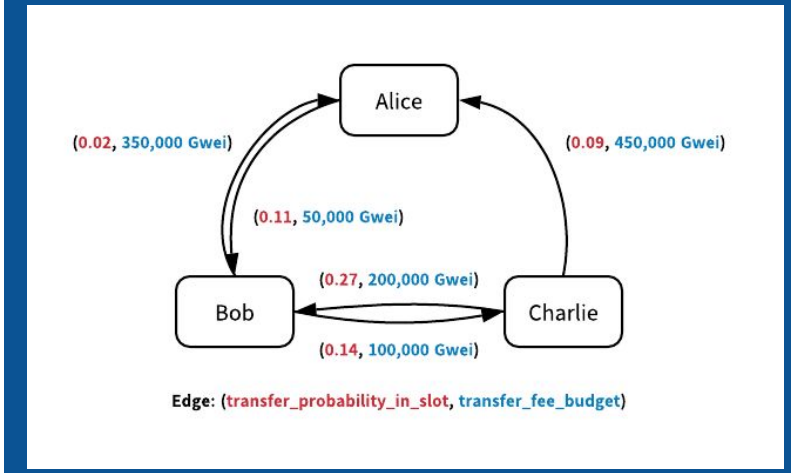


4th Workshop on Trusted Smart Contracts

Shargri-La (未踏 2020)

シャーディングでのトランザクションやユーザー行動をシミュレート

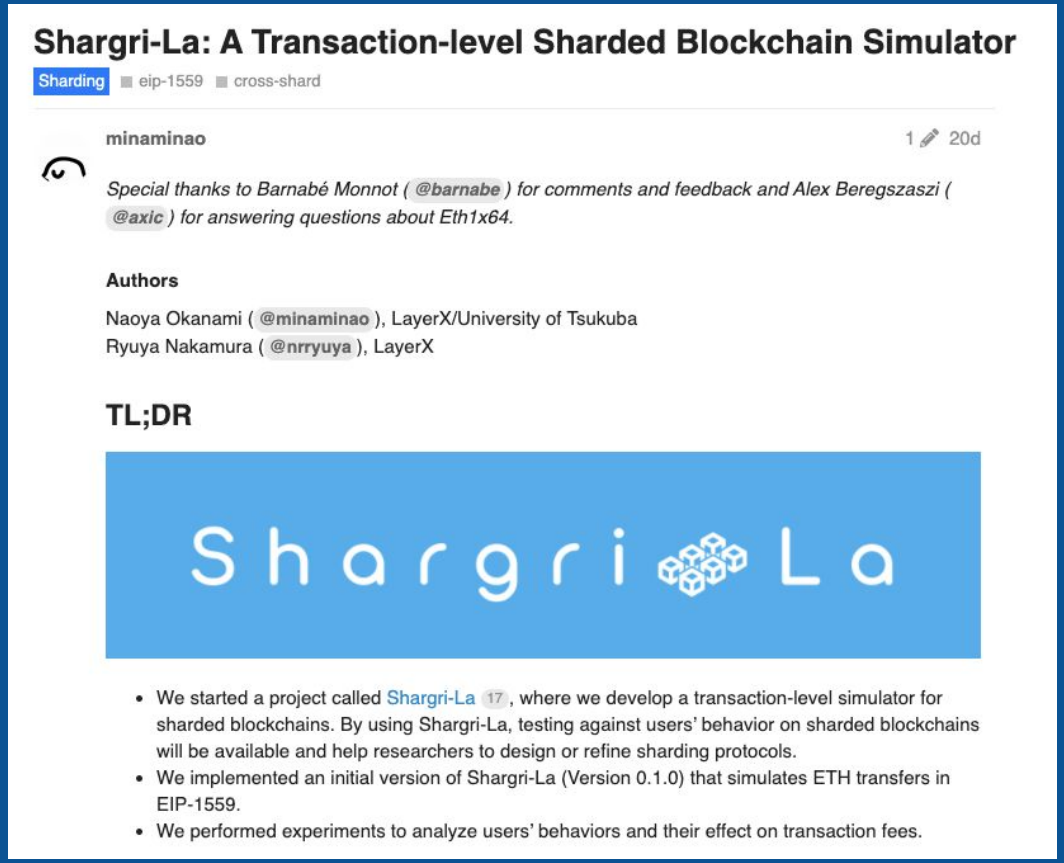




Shargri-La: 類似システムとの比較

	シミュレート対象			アーキテクチャ
	P2P (Layer 0)	コンセンサス (Layer 1)	ユーザーやTX (Layer 1.5+)	Sharding
shardSim	○	○	×	○
SimBlock	○	○	×	×
VIBES	○	○	×	×
Bitcoin-Simulator (ns-3 based)	○	○	×	×
Shargri-La	×	×	○	○

Shargri-La v0.1.0を公開



Shargri-La: A Transaction-level Sharded Blockchain Simulator

Sharding ■ eip-1559 ■ cross-shard

minaminao 1 20d

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

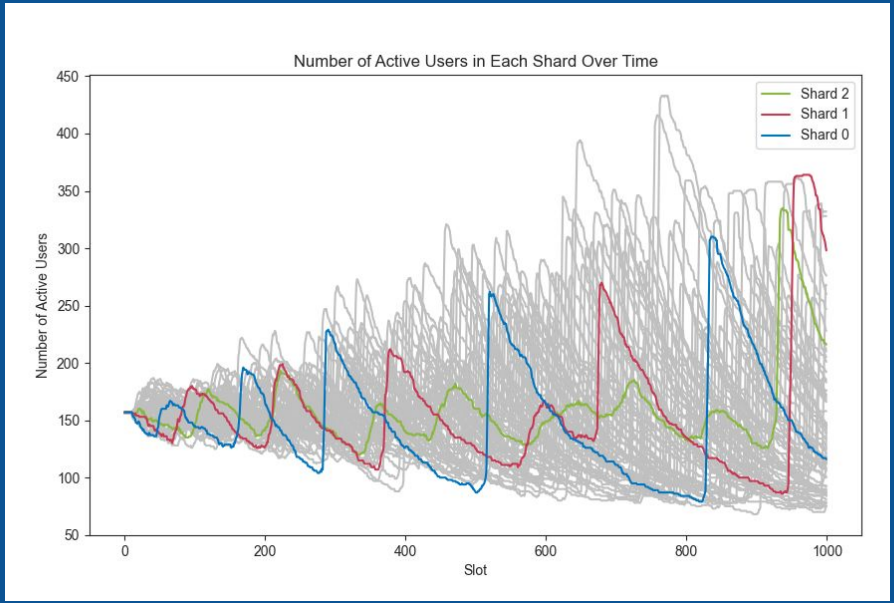
- We started a project called Shargri-La 17 , where we develop a transaction-level simulator for sharded blockchains. By using Shargri-La, testing against users' behavior on sharded blockchains will be available and help researchers to design or refine sharding protocols.
- We implemented an initial version of Shargri-La (Version 0.1.0) that simulates ETH transfers in EIP-1559.
- We performed experiments to analyze users' behaviors and their effect on transaction fees.

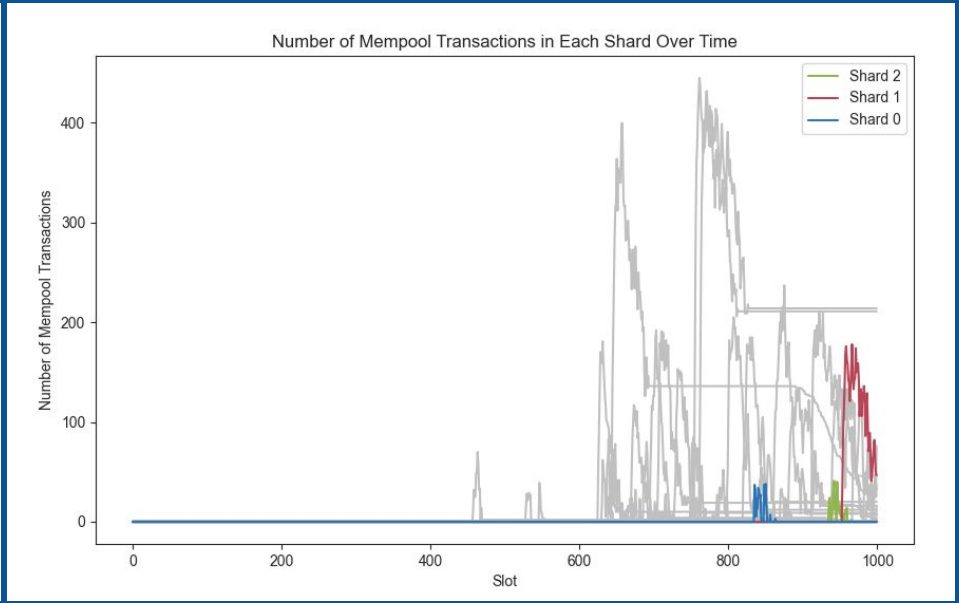
- Eth2でEIP-1559を採用したらどうなるか？を分析
- シャードごとの手数料の差により、ユーザーがシャードを「移動」する行動をシミュレート

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

Shargri-La v0.1.0 実験結果

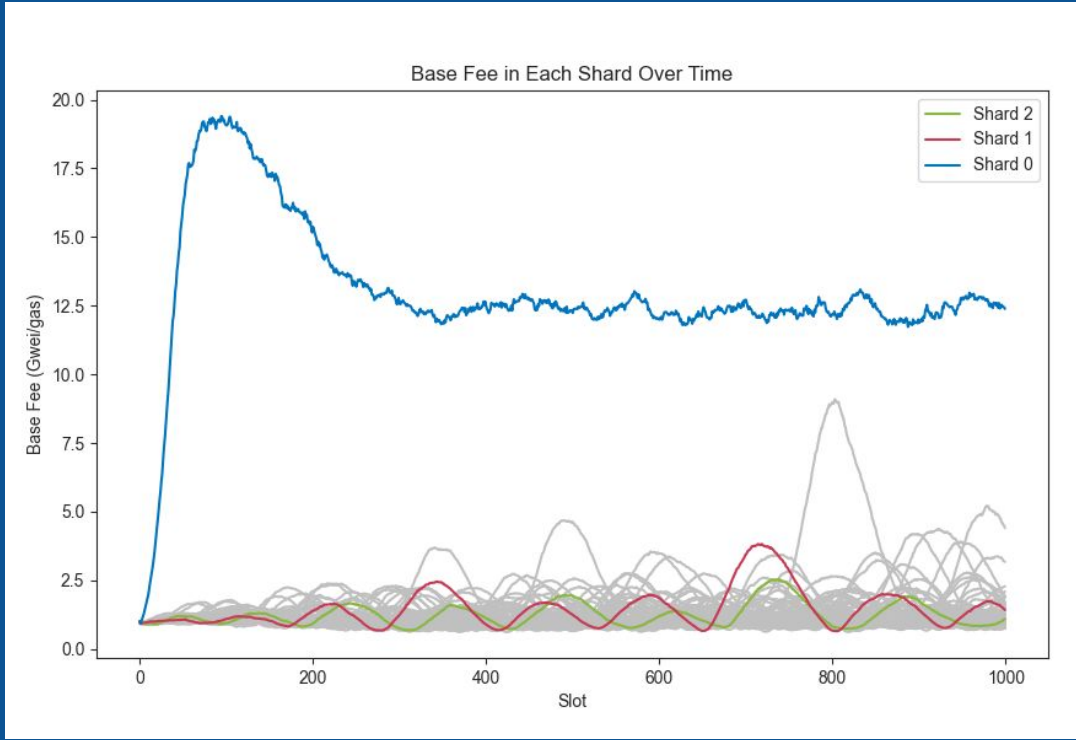
ユーザーが手数料期待値最小のシャードに移動する場合「特定のシャードに殺到→手数料増加やトランザクション詰まりの発生→他シャードに大移動」が繰り返される





Shargri-La v0.1.0 実験結果

“人気”なユーザーが存在（全ユーザーの5%から送金される）する時、そのシャードでBASE FEEが増大



最後に

Ethereumの情報キャッチアップ

- Week in Ethereum News
- What's New in Eth2
- 弊社もLayerX Newsletter（Tech編/Biz編）を毎週発行してます！
  - Tech編ではEthereum関連の話題も
  - Biz編の総まとめ版も公開

参考文献

- [BG17] Vitalik Buterin and Virgil Griffith. Casper the friendly finality gadget. arXiv:1710.09437, 2017.
- [ZRA+18] Vlad Zamfir, Nate Rush, Aditya Asgaonkar, and Georgios Piliouras. Introducing the ”Minimal CBC Casper” Family of Consensus Protocols. https://github.com/cbc-casper/cbc-casper-paper/blob/master/cbc-casper-paper-draft.pdf, 2018
- [AKC+19] Guillermo Angeris, Hsien-Tang Kao, Rei Chiang, and Charlie Noyes. An analysis of Uniswap markets.
- [DGK+19] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, Ari Juels. Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges
- [KM19] Ariah Klages-Mundt and Andreea Minca. (In)Stability for the Blockchain: Deleveraging Spirals and Stablecoin Attacks.
- [TAB+20] Alin Tomescu, Ittai Abraham, Vitalik Buterin, Justin Drake, Dankrad Feist, and Dmitry Khovratovic. Aggregatable Subvector Commitments for Stateless Cryptocurrencies.

参考文献

- [MNR19] Dahlia Malkhi, Kartik Nayak, and Ling Ren. Flexible byzantine fault tolerance. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS ’19, pages 1041–1053, New York, NY, USA, 2019. ACM.
- [YMR+19] Maofan Yin, Dahlia Malkhi, Michael K. Reiter, Guy Golan Gueta, and Ittai Abraham. 2019. HotStuff: BFT Consensus with Linearity and Responsiveness. In Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing (PODC ’19). Association for Computing Machinery, New York, NY, USA, 347–356.
- [BHK+19] Vitalik Buterin, Diego Hernandez, Thor Kamphefner, Zhi Qiao, Khiem Pham, Danny Ryan, Juan Sanchez, Juhyeok Sin, Ying Wang, Yan Zhang. Combining GHOST and Casper. https://github.com/ethereum/research/blob/master/papers/ffg%2Bghost/paper.pdf, 2019
- [CL99] Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance. In OSDI, volume 99, pages 173–186, 1999.
- [DLS88] Cynthia Dwork, Nancy Lynch, and Larry Stockmeyer. Consensus in the presence of partial synchrony. volume 35, pages 288–323. ACM, 1988.