最近のEthereumコミュニティおよびEthereum 2.0の概要

中村龍矢 (株式会社LayerX)
2019.10.29 @JCBA勉強会

自己紹介: 中村龍矢

株式会社LayerX

- ブロックチェーンの事業の開発・コンサルティング
  - 金融業界をはじめとする実社会へのブロックチェーン応用
- ブロックチェーンの R&D
  - セキュリティチーム (僕)
    - EthereumのLayer1研究へのコントリビュート
  - プライバシーチーム
    - 秘匿送金ブロックチェーン Zero Chainの開発

自己紹介: 中村龍矢

- 最近の研究活動
  - コンセンサスプロトコル
  - Proof of stake
  - シャーディング
- 以前の研究活動
  - スマートコントラクトの形式的検証
  - スマートコントラクト言語 Vyperへのコントリビュート

Casperに関する論文の執筆

Presented at Crypto Valley Conference'19

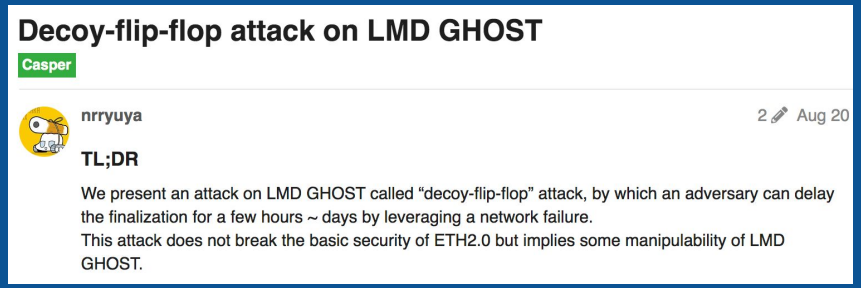
Refinement and Verification of CBC Casper

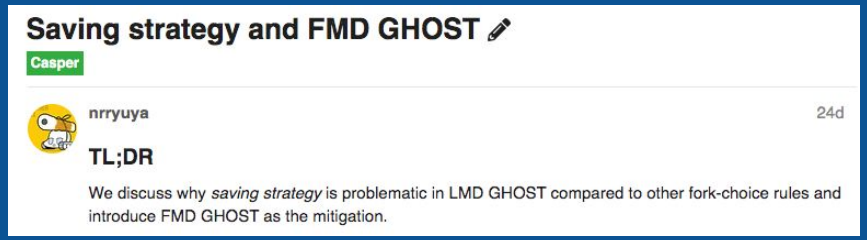
Ryuya Nakamura*†, Takayuki Jimba†, and Dominik Harz‡
* Faculty of Engineering, The University of Tokyo
† Research and Development, LayerX
Email: {ryuya.nakamura,takayuki.jinba}@layerx.co.jp
‡ Department of Computing, Imperial College London
Email: d.harz@imperial.ac.uk

https://eprint.iacr.org/2019/415.pdf

Ethereum Researchへの投稿

https://ethresear.ch/u/nrryuya

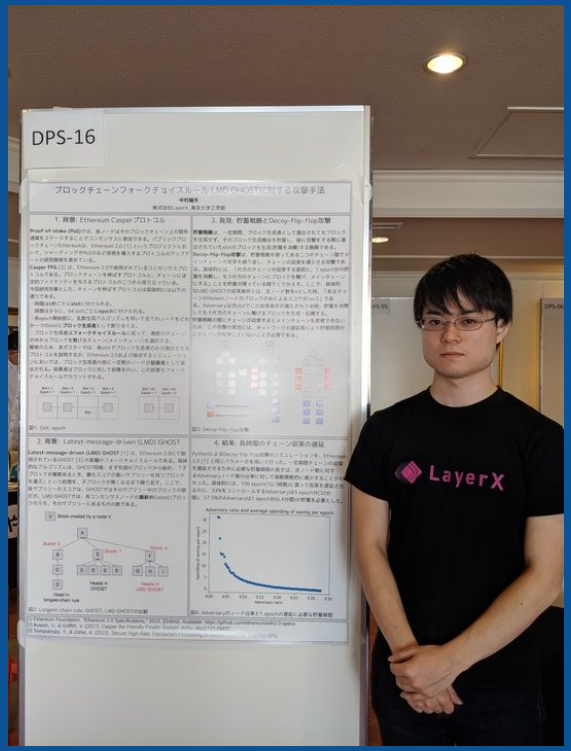




国内外のカンファレンスへの参加

- 今後はもっと国内のコミュニティに参加したい
  - 国内のブロックチェーン研究者ともっと交流
  - Ethereum界隈の最先端の研究課題を国内に紹介

EDCON 2019 @シドニー



コンピューターセキュリティシンポジウム2019 @長崎

アジェンダ

- DEVCON Vの様子
- Ethereumコミュニティの最近
- Ethereum 2.0概要
- Ethereum 2.0の影響

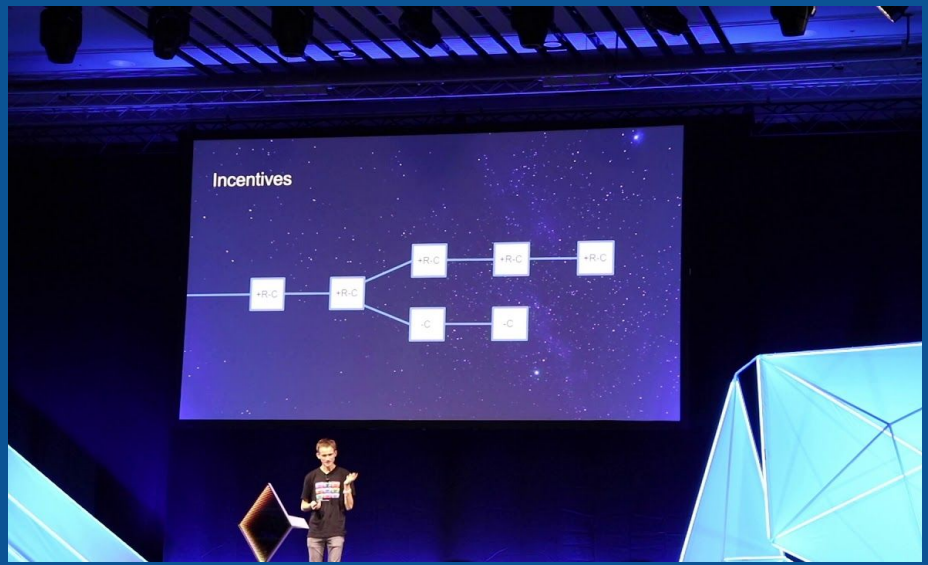
DEVCON Vの様子

DEVCON V @大阪 (10/8 ~ 11)

- DEVCONとは
  - Ethereumの開発者・研究者が集まる年 1回のカンファレンス
    - Ethereum関連の人はほとんど来る
  - Ethereum Foundationが運営する唯一のイベント
  - Ethereum以外のプロジェクトの人も来る
    - ZCash, Polkadot, Cosmos, アカデミア, Libra(!?), etc.
- 第五回の今年は大阪で開催
  - 大阪港湾部, ATCホール
  - 去年はプラハ、その前はカンクーン
  - 3000人(?)が参加
  - 日本のEthereumコミュニティの今後にとっては貴重なイベントだった
    - Ethereum Foundation エグゼクティブ・ディレクター 宮口さんの尽力

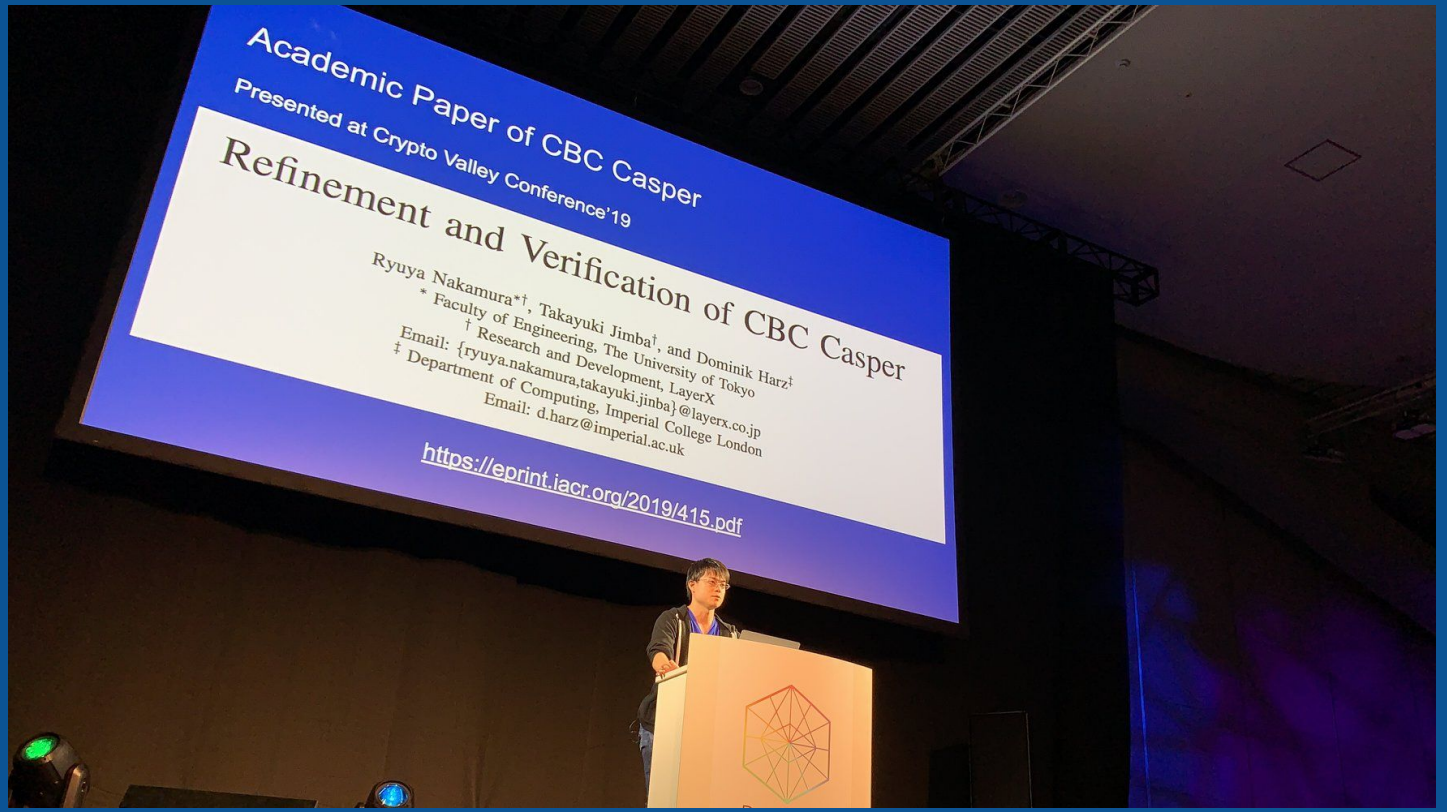
DEVCON V

DEVCON V



DEVCON V

LayerX @DEVCON



LayerX @DEVCON

DEVCON V サテライトイベント

- 例年、夜は色んな企業・チームがイベントを行う
- 日本のEthereumコミュニティも有志で活動の運営
  - 数ヶ月前から “Road to DEVCON” という勉強会シリーズが開催
  - “Osaka Blockchain Week” サイトの運営や外国人の手助け

Ethereumコミュニティの最近

そもそもEthereumコミュニティとはなんなのか

- Ethereumに関する様々なプレイヤー達から成る分散的な集まり
  - Ethereum Foundationは中心にあるが、その外側にたくさんの人がいるのが特徴
  - スタートアップ、大企業、フリーランス、大学の研究者
  - 取り組んでいることも、インフラレイヤーからアプリケーションまで様々
- 全体に精通している人はほぼいない(と思う)
  - 当然僕も一部しか知らない
  - 見えている範囲で直近のアップデートについてご紹介します

Ethereum 2.0

VitalikをはじめとするEthereum Foundationコアリサーチャー達の最大のプロジェクト

- PoS, Shardingを導入
- 昨年から本格的に実装に向かい始め、徐々に本番投入が始まる予定
- 後半で詳しく話します

Ethereum 1.0

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

- 主なトピック
  - Gethなどクライアントの改善
  - EVMの改善
  - EIP, 標準化, ガバナンス
  - 開発者向けツール
- Ethereum Magiciansというコミュニティがある
  - オンラインフォーラム (ethereum-magicians.org)やワークショップの開催

Layer2

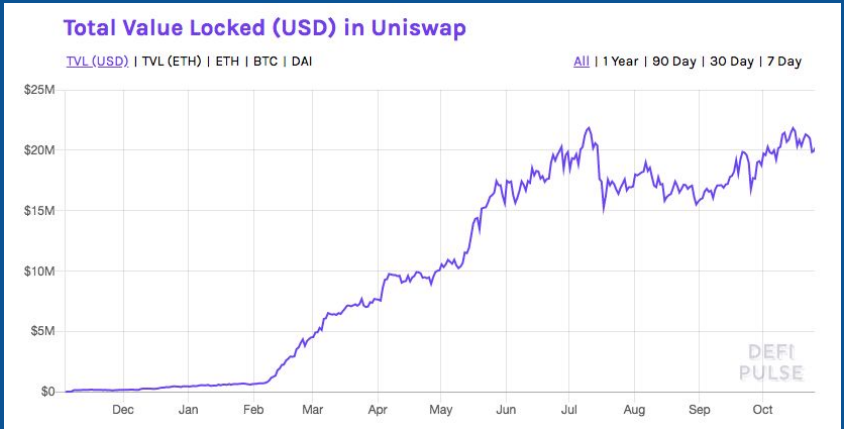
State channel, Plasmaをはじめとするlayer2のプロトコルの開発

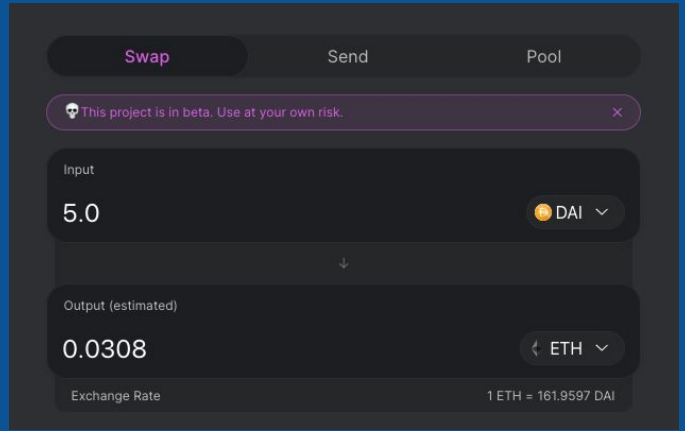
- State channel
  - 引き続き開発が進んでいる、複数チームが協力し仕様を標準化する流れ (statechannels.org)
  - 2019年度末までに標準化プロトコルの v1をリリース予定
- Plasma
  - 昨年研究の大ブームを迎えたが、研究過程で課題が整理された
  - 根本: Data availability
  - 結果: 実現できるアプリケーションの少なさ、インセンティブ含めた設計の複雑さ
- Rollupの登場
  - Optimistic Rollup: Plasmaと異なり、トランザクションは全てオンチェーンに置かれる
    - Plasmaより対象が広い: DEVCONでUniswap(DEX)を動かすデモを発表
  - ZK Rollup: ゼロ知識証明(ZK-SNARKs)

Uniswap

プール型の分散型取引所(DEX)

- EF Grantで個人開発者がスタート、今年 Paradigmから資金調達
- Vyperで開発されたコントラクトとしては初めて大規模に使われている
- Ethereumコミュニティで愛されている (と思う)





Ethereum 2.0概要

Ethereum 2.0とは

Proof-of-stake (PoS)とシャーディングの導入

- スケーラビリティの改善、セキュリティの向上
- 昨年から本格的にスタート
  - 以前は別々に研究されていたが、研究開発上かなりオーバーラップするので、 Ethereum 2.0として一つのプロジェクトになった
  - PoSの最初のステップとして“PoWとPoSのハイブリッド”というハードフォークもかなり進められていたが中止になった
- チーム: Ethereum Foundation + 10前後の企業
  - Prysmatic Labsのようなスタートアップも、Consensys, Parityのようなジャイアントも

Proof-of-stake (PoS)

PoS: 暗号通貨をステークすることでコンセンサスに参加できるようにする

- 注: PoWやPoSはコンセンサスプロトコルではなく、シビルコントロールメカニズム
- 主なメリット
  - コスト削減、ひいてはリワードの削減
  - Punishmentを用いたインセンティブ設計
    - “悪意あるマイナーのASICを燃やせるようなもの” by Vlad
    - いわゆるNothing-at-stake問題を解決する

Casper

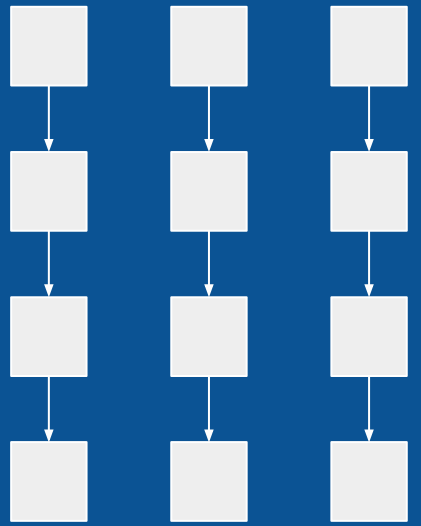
Casper: EthereumのPoS + コンセンサスプロトコルのプロジェクト名

- Ethereum Foundationは昔からPoS移行を計画しており、Casperも数年かけて進化し、現在は二つのプロトコルに分岐
- Casper FFG: Vitalikらが提案、Ethereum 2.0で採用予定
- CBC Casper: Vladが提案、新規性が高くポテンシャルは高いが、まだ詳細な仕様がない

シャーディング

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
  - 異なるノード(バリデーター)が割り当てられる
  - 別々のアカウント・コントラクトを管理する
- シャーディングに取り組んでいるプロジェクト
  - Ethereum, NEAR, Harmony, Polkadot, etc.
- 目的: スケーラビリティの改善
  - TPS = (1ブロックチェーンあたりの TPS) * (シャード数)
- でもセキュリティは(なるべく)落とさない
  - この点がPolkadotとCosmosの違い

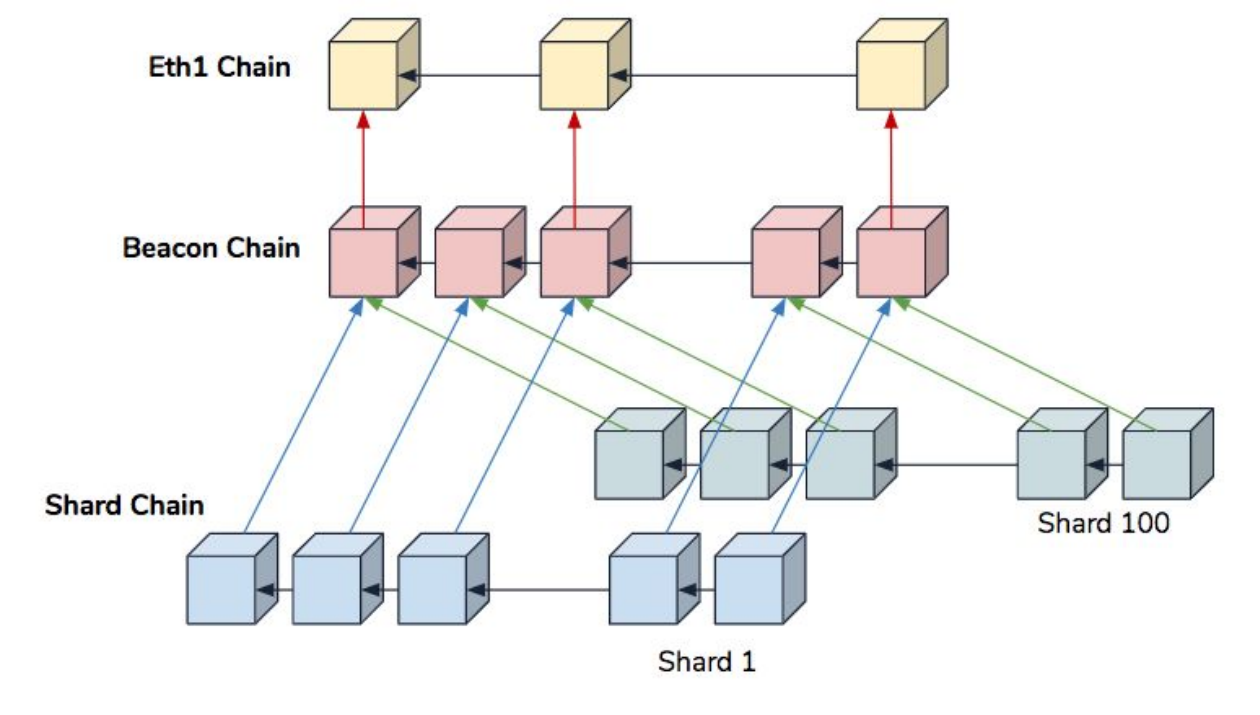


Disclaimer

Ethereum 2.0に関しては、「決まってない」と説明せざるを得ないことが多いです

- 研究開発の具合により多くのことが変更する可能性があるので、間違った情報を伝えないためです
- 「100%確定していない」というだけで、その裏には多くのアイデアが提案され議論されているので、「何もしてない」わけではありません

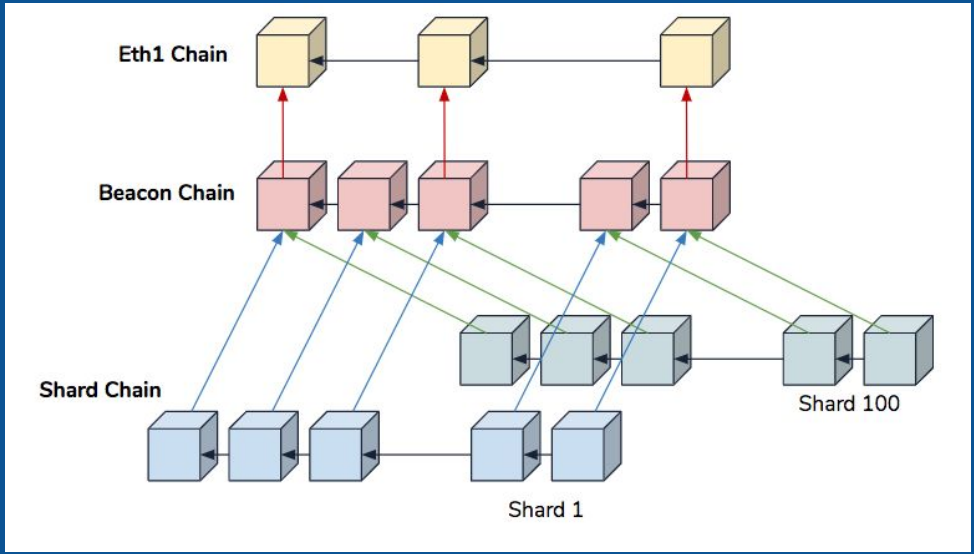
Ethereum 2.0 アーキテクチャ



Eth1 Chain

現行のPoWチェーン

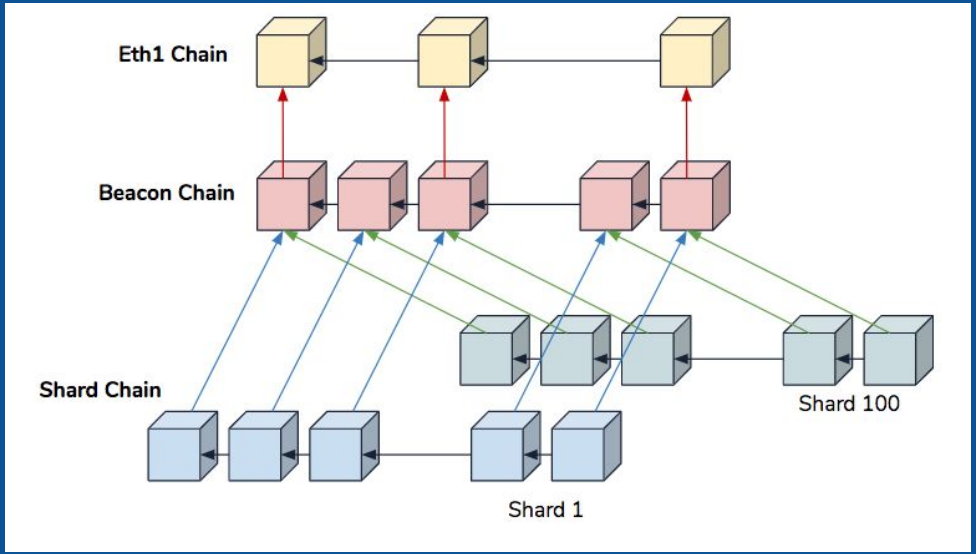
- Eth2は基本的に別のチェーンをゼロから作って、現状のチェーンと接続するプロジェクト
- デポジットコントラクト(まだない)にETHをデポジットすることで、Beacon Chain側でアカウントが発行される



Beacon Chain

全体を管理するチェーン

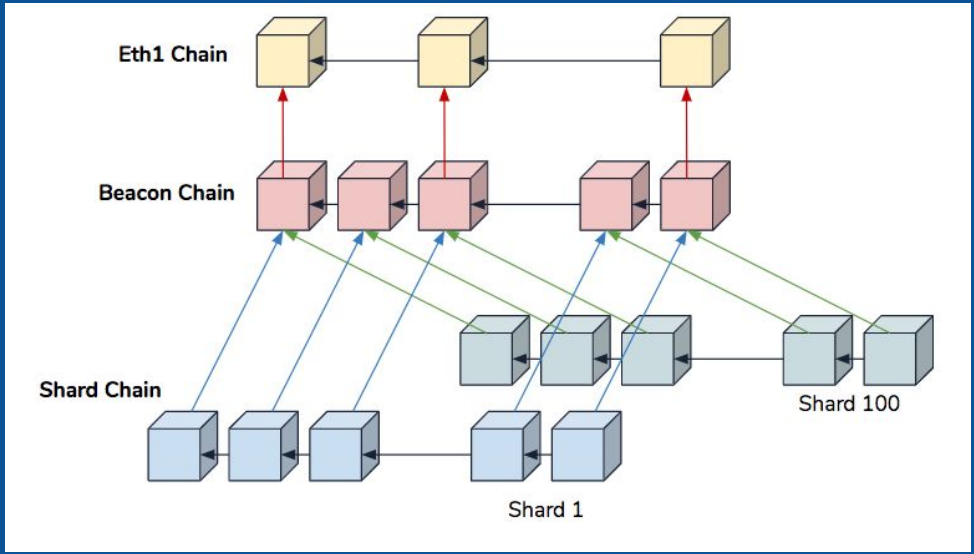
- 乱数生成、バリデータの各シャードへの割り当て
- 各シャードのstate rootを記録
  - これにより、Merkle proofを使ってシャード内のイベントを検知できる
  - これがクロスシャードコミュニケーションの基礎になる



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 2: シャード内でVM使用可能に
  - eWASM: EVMのWebAssebmly化と並行して研究開発

- Phase 1,2の開始時期はあまり定まっていない

FAQ: 既存のEth1チェーンはどうなっちゃうの？

前提: Eth2の安全性を確かめながら、徐々にEth2に統合していく(予定)

1. Eth2は分離されたチェーン
    a. 最初はEth1自体がハードフォークするわけではない
    b. Eth1 -> Eth2は一方通行
    c. もしEth2が壊れてもEth1には影響なし
2. Eth1 <> Eth2の統合
    a. Eth1 <> Eth2のTwo-way peg
        i. それぞれのセキュリティがお互いに影響する
    b. Eth2を使ってEth1にファイナリティを与える
3. 既存のEth1チェーンを破棄
    a. Eth1のデータはシャードのどこかに記録され、Eth2で使える

Ethereum 2.0の影響

過渡期(Phase 0 ~ 2)の影響

- 大規模なPoSチェーンのローンチ
  - マイニングと異なり、個人・企業が参入しやすい
- 2つの通貨ETHの誕生
  - Two-way pegまでは価格がかなりズレるかも
    - Pegの最近スケジュールを早める機運が高まっている
- 実際のアプリケーションは引き続き既存のEth1チェーンが使われると予想

長期的な影響

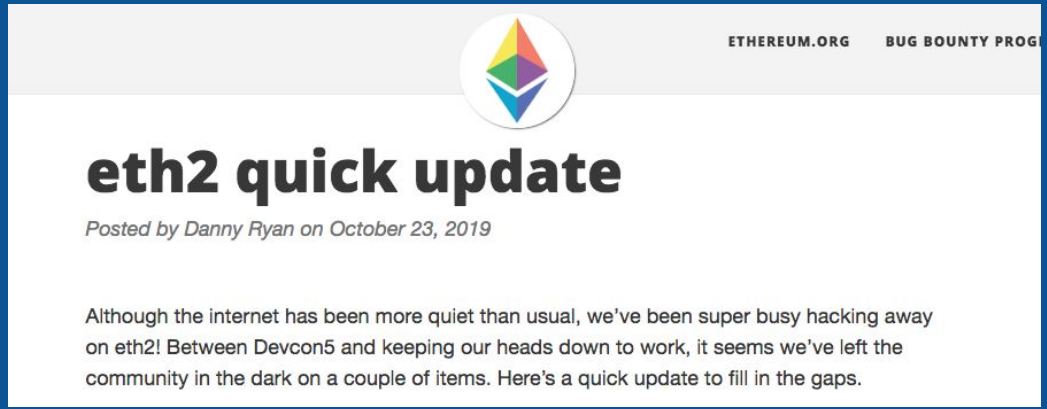
- Layer1のパワーアップ
  - スケーラビリティ、プライバシー (?)
  - ゼロ知識証明などもやりやすく
- アプリケーション開発の仕方やUXの変化
  - アプリケーションによっては複数のシャードとやりとりする必要がある
  - VMが変わる -> ERC20などの実装方法も変わる

どうキャッチアップすればいいか

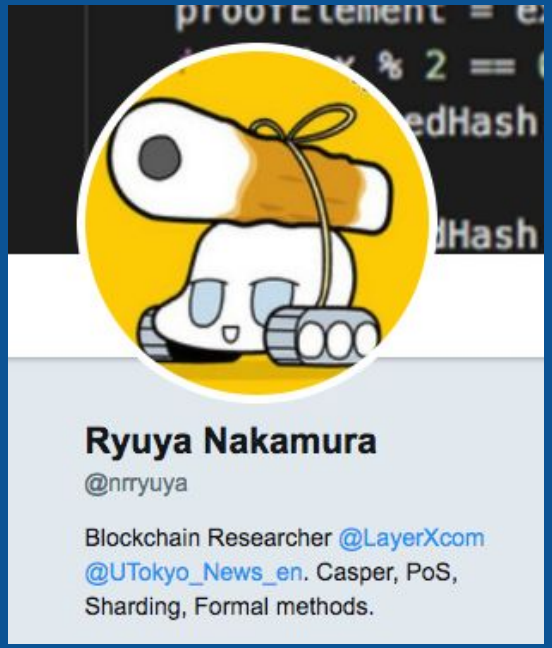
- 技術的なアップデートは情報源が色々ある
  - 大元: https://github.com/ethereum/eth2.0-specs
  - What's New in Eth2: https://notes.ethereum.org/@ChihChengLiang/Sk8Zs--CQ
  - 僕がメンテしているリンク集 : https://scrapbox.io/layerx/ETH2.0:_Resources
- 課題
  - 技術を追わずビジネス的な影響だけに絞って追いかけるのはかなり難しい
  - 当然ながら日本語で最先端の情報はほぼない
    - 日本人でETH2.0にコントリビュートしている人がいないので仕方ない

どうキャッチアップすればいいか

- Twitterで色々流れてくる
  - Ethereum Foundation公式: @ethereum (公式のブログにたまにアップデートがある)
  - 2.0のコアリサーチャー: Vitalik, @dannyryan, @drakefjustin
  - @nrryuya (僕) (頑張ります)



Thank you!



@nrryuya