



LayerX Labs



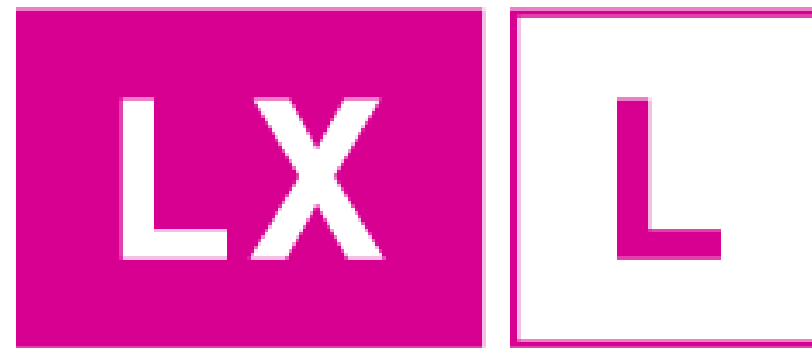
**Eth2 Data Sharding
@ETHTerakoya**

**2021/2/4
LayerX, Inc.**

自己紹介 & 会社紹介

LayerX Inc. 執行役員 兼 LayerX Labs 所長

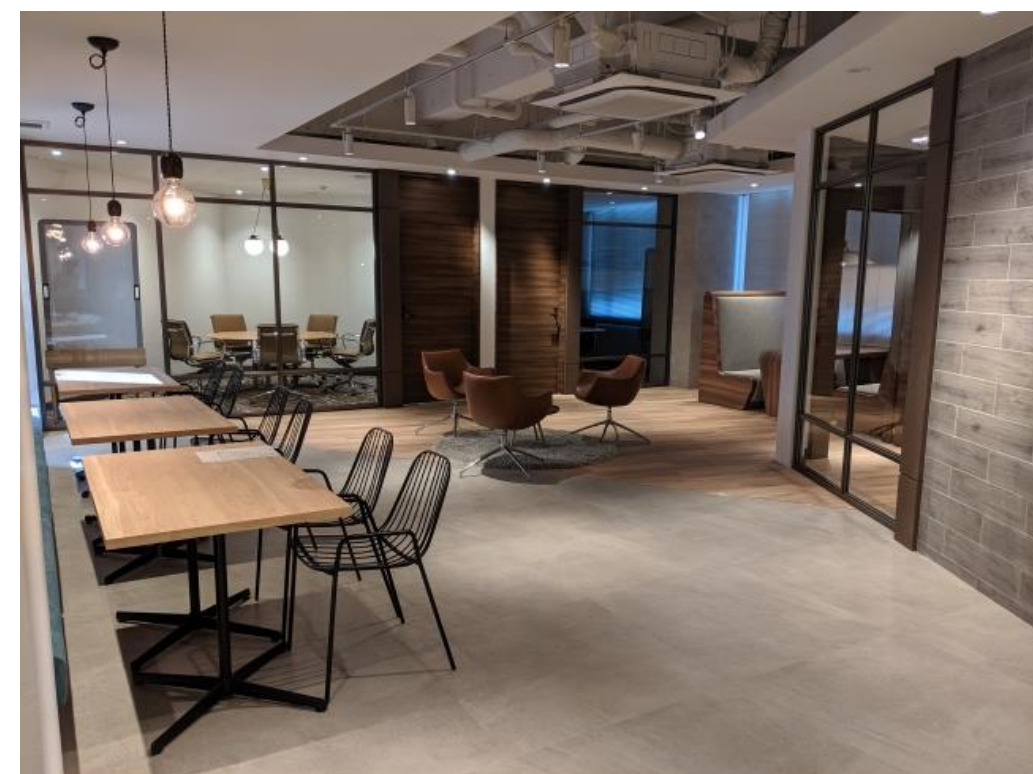
- LayerXに創業から参画
 - 研究開発、論文発表
 - パートナー企業・行政との共同プロジェクト推進
- IPA 未踏人材発掘事業 2020
- 略歴: Gunosy Inc., Coubic Inc., 東京大学工学部
- Twitter: [@nrryuya_jp](https://twitter.com/nrryuya_jp)



LayerX Labs



会社名	株式会社LayerX
代表取締役	福島 良典 (Gunosy創業者)
創立	2018年8月1日
資本金及び 資本準備金	31億円
事業内容	<ul style="list-style-type: none"> ・ 経済活動をデジタル化する支援全般（DX事業） ・ ブロックチェーン技術を活用した事業開発、ソフトウェア開発、R&D
従業員数	35名（2020年9月末現在）
本社所在地	〒103-0004 東京都中央区東日本橋2丁目7-1 Frontier東日本橋7階



2020年7月、行政・中央銀行等・学術機関との共同研究を手掛ける組織を設立

デジタル 通貨・決済

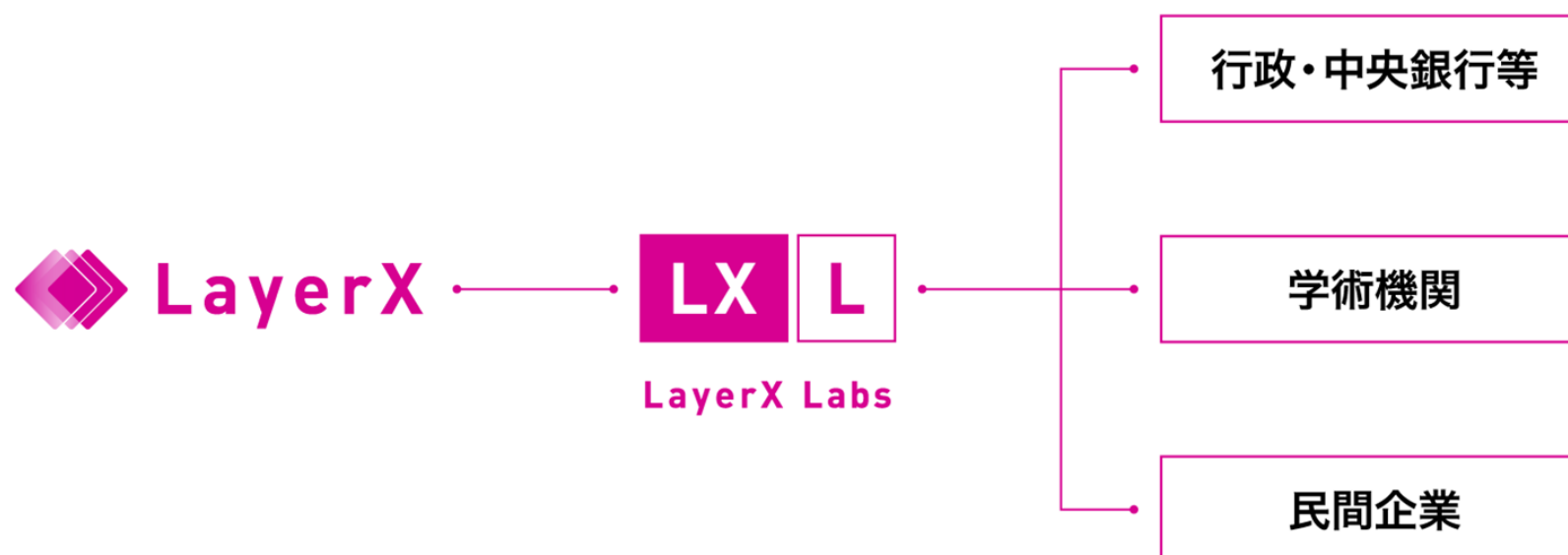
経済活動の最も基本的な要素である決済・通貨のデジタル化を目指す。
また、中央銀行デジタル通貨 (CBDC) のユースケースや技術を研究。

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。



JCBとLayerX、CBDC時代を見据え、複数企業間をつなぐ次世代BtoB取引履歴インフラに関する共同研究を開始 -プライバシーに配慮した上で、サプライチェーンをまたがる商流情報を活用する高度なサービスの実現を目指す-



<https://layerx.co.jp/news/pr201222/>

非金融サービス ワンストップで

三井住友フィナンシャルグループ（F&G）は、非金融サ

東証が復旧対応訓練

再発防止中間報告 来年4月から

東京証券取引所は21日、システム障害を受け、再発防止策の中間報告を公表した。株式取引システムを再起動する際の手順を整備し、証券会社への意見聴取プロセスや障害復旧の訓練を2021年4月から順次始める。証券業界全体で取り組む、当日中にすみやかに取引を再開する体制を

企業間取引に分散台帳技術

JCBなど基盤開発

クレジット大手のジェシービー（JCB）は、ブロックチェーン（分散台帳）技術を使った企業間取引システムを開発する。企業の受発注システムや会計ソフトをつなぎ、一定期間の支払いと受取金額を相殺して差額だけ決済する「ネットティング」の簡素化を図る。取引履歴を金融機関が融資にも活用できるようにする。

企業間取引にブロックチェーン JCBなど基盤開発

金融機関 + フォローする

2020年12月21日 19:30 [有料会員限定]

保存



クレジットカード大手のジェシービー（JCB）は、ブロックチェーン（分散台帳）技術を使った企業間取引システムを開発する。企業の受発注システムや会計ソフトをつなぎ、一定期間の支払いと受取金額を相殺して差額だけ決済する「ネットティング」の簡素化を図る。取引履歴を金融機関が融資にも活用できるようにする。

ブロックチェーン開発のLayerX（レイヤーX、東京・中央）と組み、2022年をめどにシステム基盤を実用化する。ネットティングは売買契約ごとに決済を行わずに済むため、振り込みや為替手数料を抑えられる利点がある。取引履歴をデジタル上で管理することで、請求や支払いといった事務処理にかかる時間も削減する。

取引履歴を金融サービスにも活用する。ブロックチェーンはネット上で取引の記録を互いに確認しながら管理するためデータの改ざんが難しい。正確な取引情報を把握することで、金融機関による融資や監査業務にも役立てる。取引情報は特定の金融機関や企業のみ閲覧できるように権限を設定し、事業者のプライバシーにも配慮する。

LayerX、つくばスマートシティ協議会に加入 &
スーパーシティ連携事業者として選定され、
公職選挙のインターネット投票を目指す



つくば市

○インターネット投票の実施

実施内容:

公職選挙においてスマートフォン等の端末からのインターネット投票を導入する。

効果と先進性:

投票所への移動が困難な高齢者や障害者の投票が容易になるほか、若年層の投票率の向上も期待できる。公職選挙におけるスマートフォンからのインターネット投票は国内はもちろん他国でもほとんど例がなく、世界最先端の取組となる。

つくば市、スーパーシティ構想で51事業者と連携

茨城 [+ フォローする](#)

2021年1月27日 19:40 [有料会員限定]



茨城県つくば市は政府の人工知能（AI）やビッグデータといった先端技術を活用した「スーパーシティ」の区域指定の申請に向け、計51の企業や大学、研究機関を連携事業者として決定した。市は今後、スーパーシティの基本構想をまとめ、3月ごろに内閣府に提出する予定。

つくば市スーパーシティ基本方針（案）

https://www.city.tsukuba.lg.jp/_res/projects/default_project/_page_/001/008/988/02-14supercityhonpen.pdf

日経新聞電子版（2021年1月25）

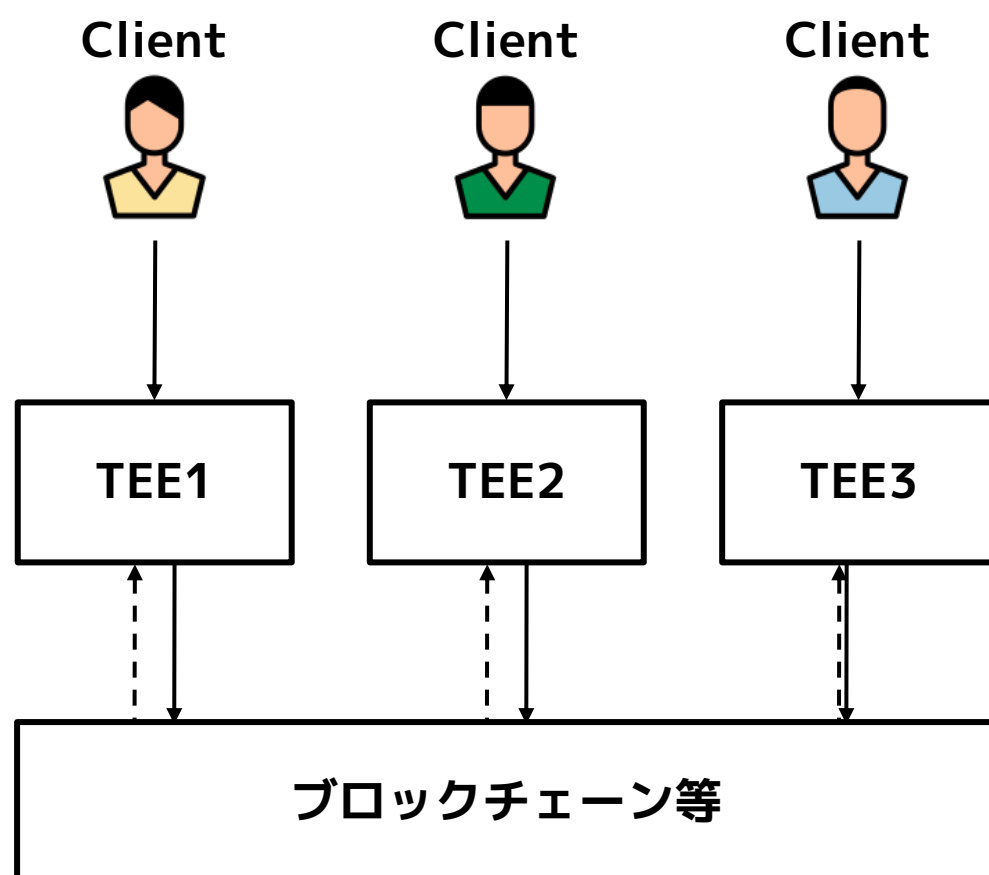
<https://www.nikkei.com/article/DGXZQOFB277AV0X20C21A1000000/>

石川県加賀市、xID、LayerX、市の政策に関する電子投票実現に向けた連携協定を締結 -全国に先駆け、ブロックチェーンとデジタルIDを活用した 安全かつ利便性が高い電子投票システム構築へ-



- 加賀市におけるブロックチェーン及びデジタルIDを活用した『安全かつ利便性の高いデジタル社会』の実現に向けて、連携協定を締結しました。
- 今後、行政サービスのデジタル化推進に向けた取り組みの一環として、加賀市の政策に関する電子投票実現に向けた検討を開始します。

Trusted Execution Environment (TEE) を用いた秘匿化・プライバシー保護技術（特許取得済）
様々なアプリケーション（金融、行政、投票）における匿名化・秘匿化を実現



Anonify: プライバシーを保護した検証可能な状態遷移モジュール
Anonify: A Module for Privacy-preserving State Transitions with Verifiability

須藤 欧佑 *
Osuke Sudo

恩田 壮恭 *
Masanori Onda

中村 龍矢 *†
Ryuya Nakamura

あらまし

社会のデジタル化が進む中で、ユーザのパーソナルデータを利用するサービスや、複数の企業や組織間で業務データ等を共有するシステムが誕生している。このようなシステムでは、用途に応じて、データを他の参加者やシステムの運営者に対して秘匿化したまま活用できることが望ましい。

本稿では、幅広いアプリケーションにおいて、状態データを秘匿化して記録したまま、ビジネスロジックを実行可能とするモジュールである Anonify を提案する。Anonify は Trusted Execution Environment (TEE) を用いることにより、データを秘匿化しつつ、実行されるプログラムの完全性を保証する。また、トランザクションをブロックチェーンに記録することにより、状態データの改ざんを困難とする。さらに、特定の主体に対してのみデータを開示する監査機能も提供する。

我々は Anonify のプロトタイプを実装し、デジタルアセット管理のアプリケーションにおけるパフォーマンス評価を行った。

学術論文として、国内学会「暗号と情報セキュリティシンポジウム (SCIS2021)」にて発表

Ethereum 2.0の脆弱性解決など、仕様策定に貢献 Ethereum Foundationのグラント・プログラムに採択（国内初）

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必要を増じてきている。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

Refinement and Verification of CBC Casper

Ryuya Nakamura^{*†}, Takayuki Jinba[†], 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
(国際学会CVC'19に採択)

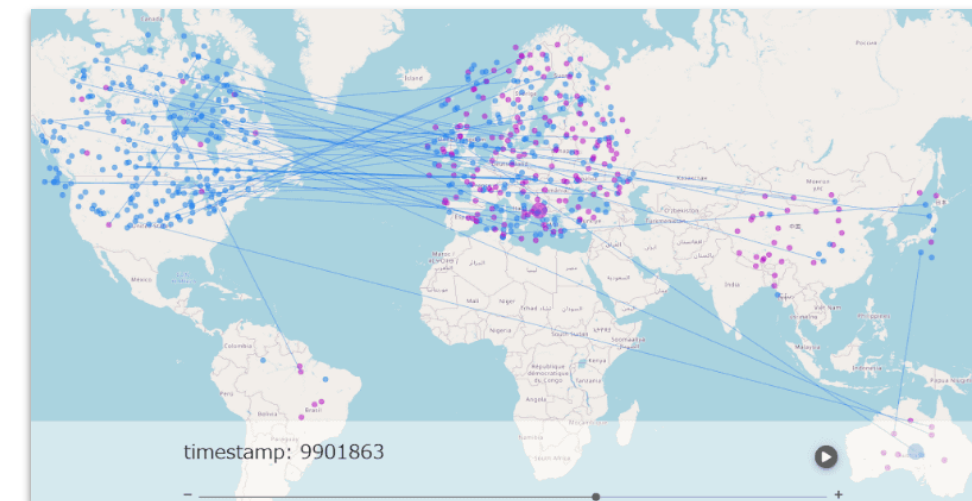


ecosystem support program

東京工業大学の首藤一幸准教授らの研究グループと、ブロックチェーンの基礎であるコンセンサスアルゴリズムに関する共同研究を実施

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



<https://layerx.co.jp/news/pr200828/>



Mousse

Eth2アプリローカルテスト用エミュレーター

「Eth2版のGanache」

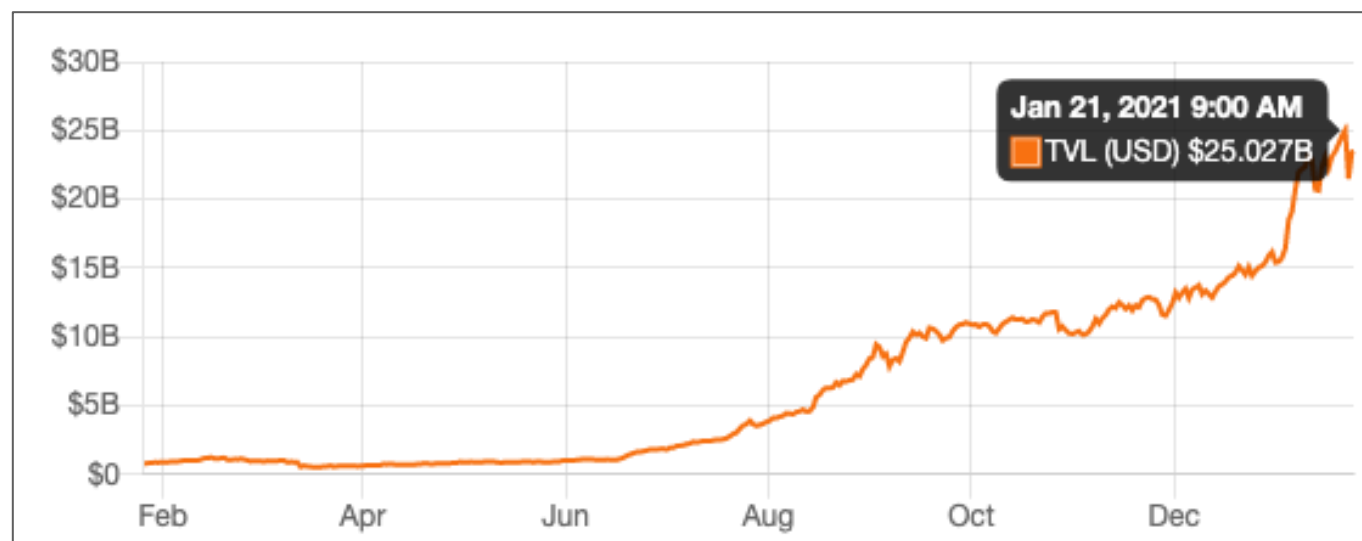
※2020年度 IPA未踏人材発掘事業で開発中

<https://github.com/ethereum-mousse/mousse>

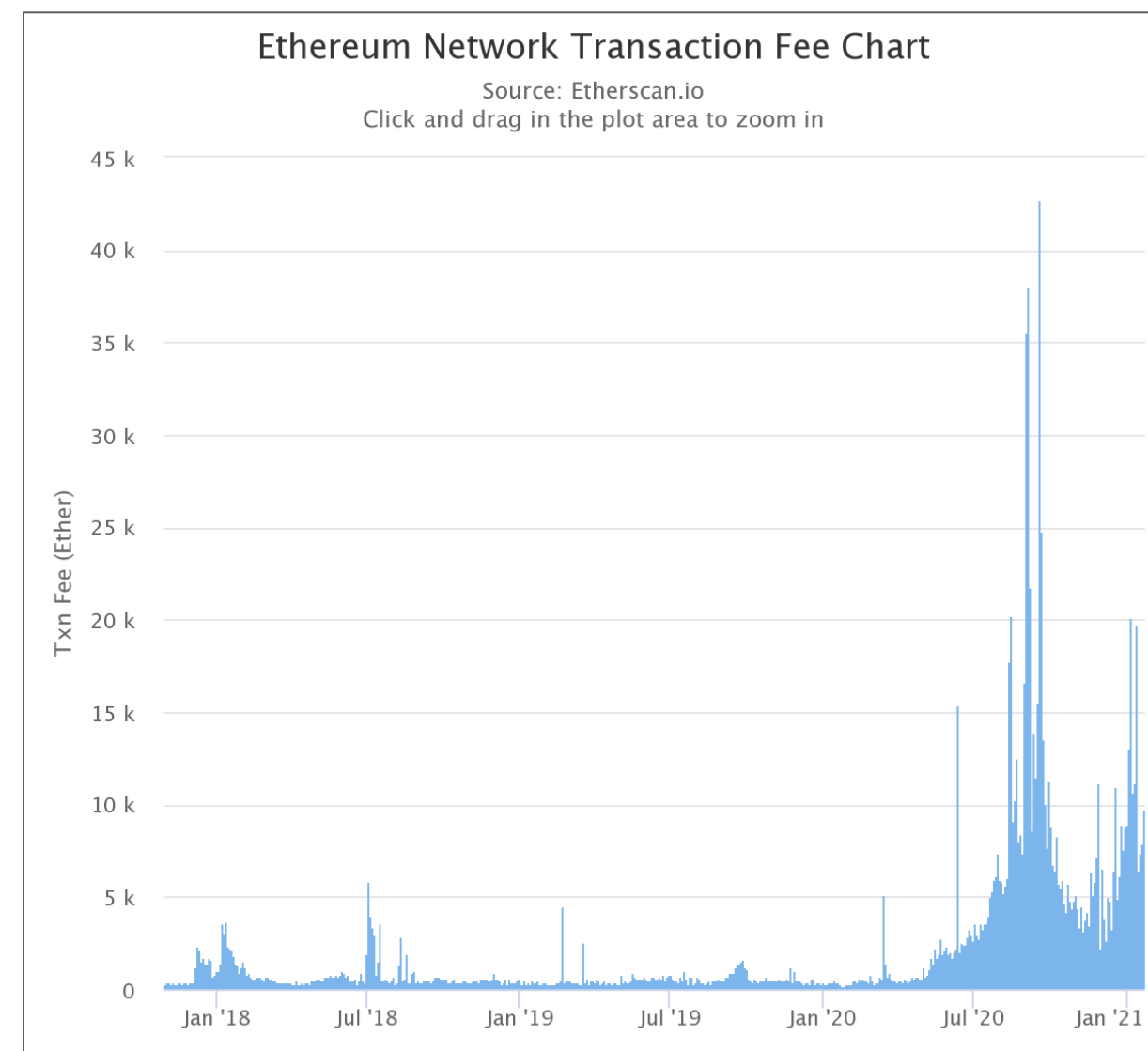
- **Ethereumのスケーリング概況**
- **Eth2 Data Shardingの概要**
- **Eth2 Data ShardingのDeep-dive**

Ethereumの スケーリング

Defi（分散型金融）の盛況もあり、トランザクション手数料が高騰
Ethereumのスケーリングが急務に



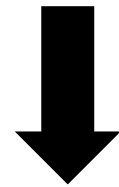
<https://defipulse.com/>



<https://etherscan.io/chart/transactionfee>

※ 実際のTPSはトランザクションの中身によって変わるため、あくまで参考値

15 TX/秒



2,000 TX/秒

Rollup

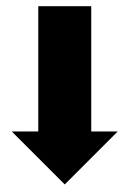


100,000 TX/秒

Ethereum 2.0 Data Sharding

※ 実際のTPSはトランザクションの中身によって変わるため、あくまで参考値

15 TX/秒



2,000 TX/秒

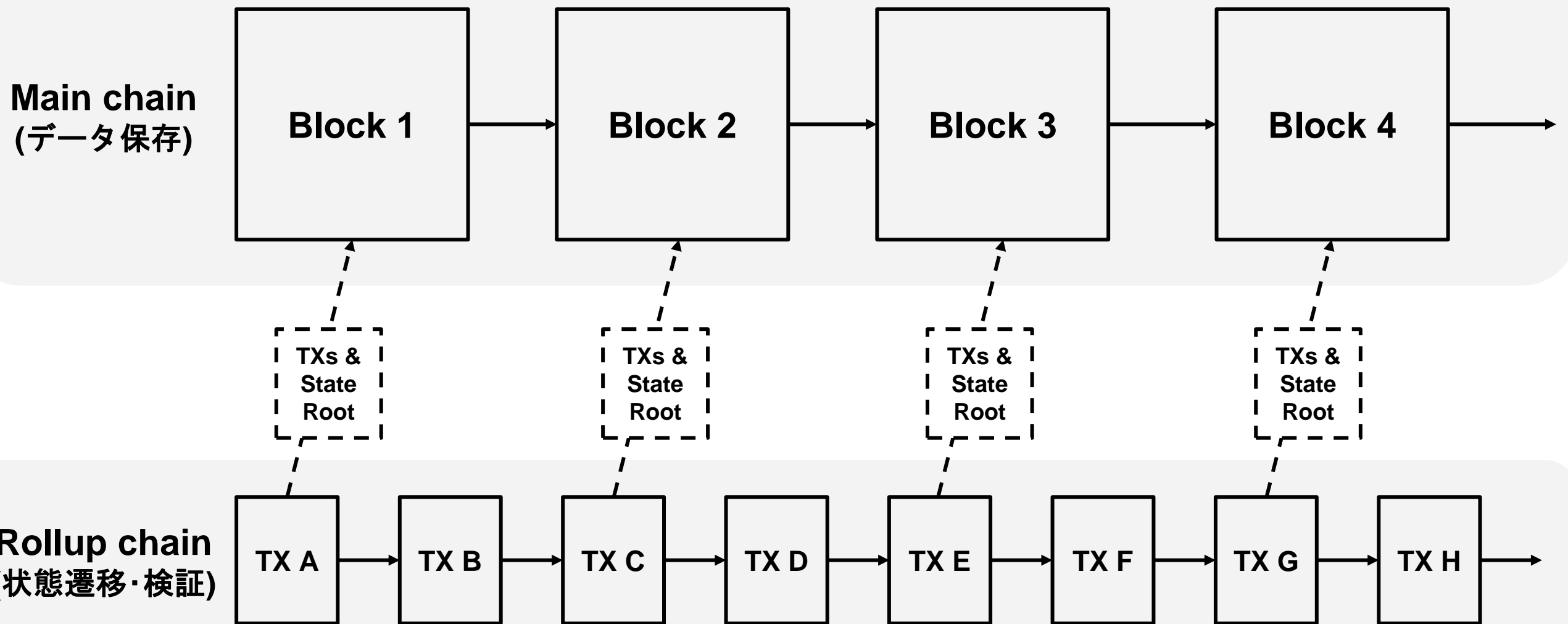
Rollup



100,000 TX/秒

Ethereum 2.0 Data Sharding

オフチェーンでトランザクションを集め、状態遷移を行い、結果だけをメインチェーンに書き込む
トランザクションデータ自体はオンチェーンに置いておく



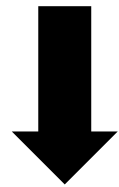
通常のトランザクションと異なり、Rollupのオフチェーンでの状態遷移はメインチェーンで検証しない
メインチェーンに置かれたトランザクションを使い、オフチェーンで効率的に検証するのが肝

- トランザクションの検証をオフチェーンで行う方法
 - 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

	Validity Proofs	Fault Proofs
Data On-Chain	ZK-Rollup	Optimistic Rollup
Data Off-Chain	Validium	Plasma

※ 実際のTPSはトランザクションの中身によって変わるため、あくまで参考値

15 TX/秒



2,000 TX/秒

Rollup



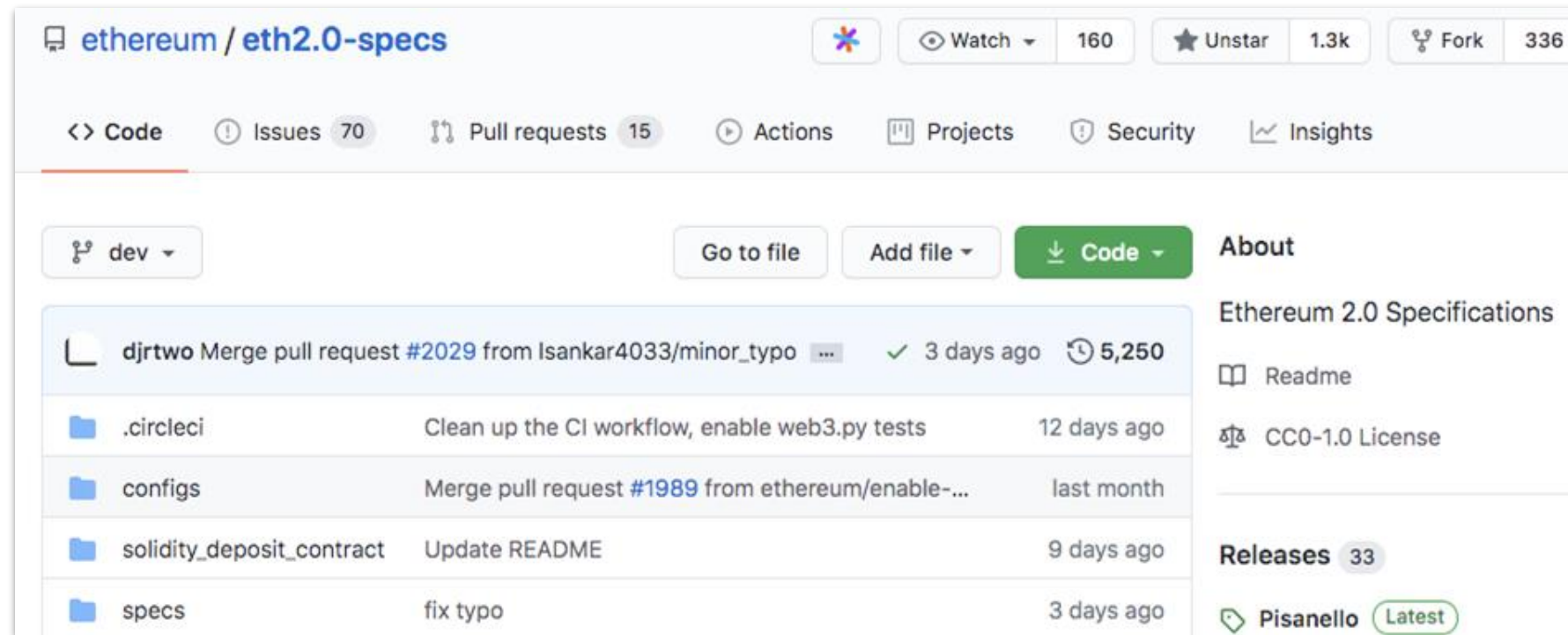
100,000 TX/秒

Ethereum 2.0 Data Sharding

Eth2 Data Sharding

～概要編～

Ethereum 2.0 (Eth2) は、Ethereumの抜本的なプロトコルアップグレードプロジェクト ShardingとProof of Stakeを導入し、スケーラビリティとセキュリティ向上を狙う



Devcon0
Berlin, November 2014



sharding workshop
Taipei, March 2018

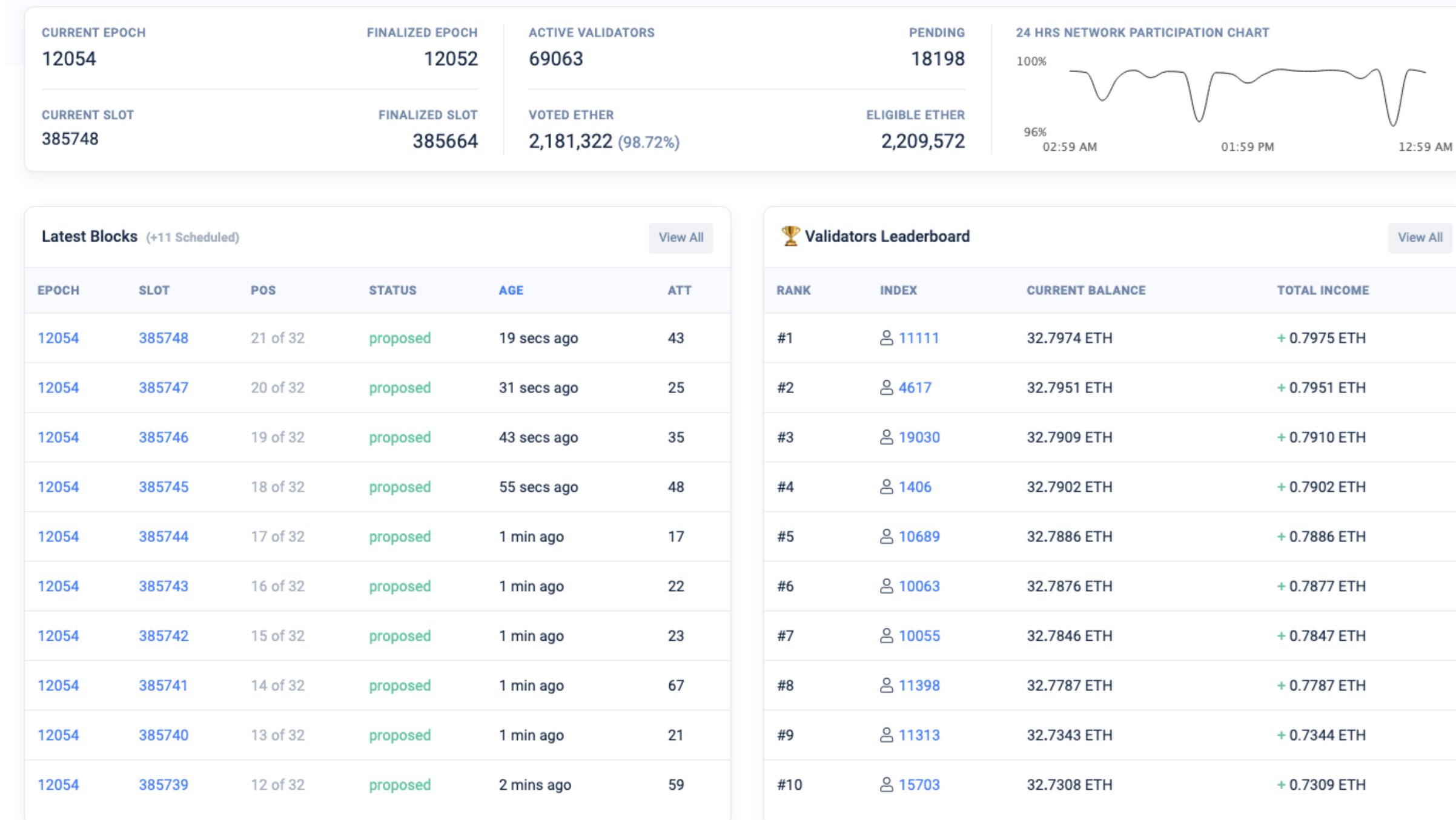


interoperability lock-in
Ontario, September 2019

https://docs.google.com/presentation/d/1I8_uRX_aP_WflsWJ1SrpXYrVaTtLMF3v8rHgDeMYe7I/edit

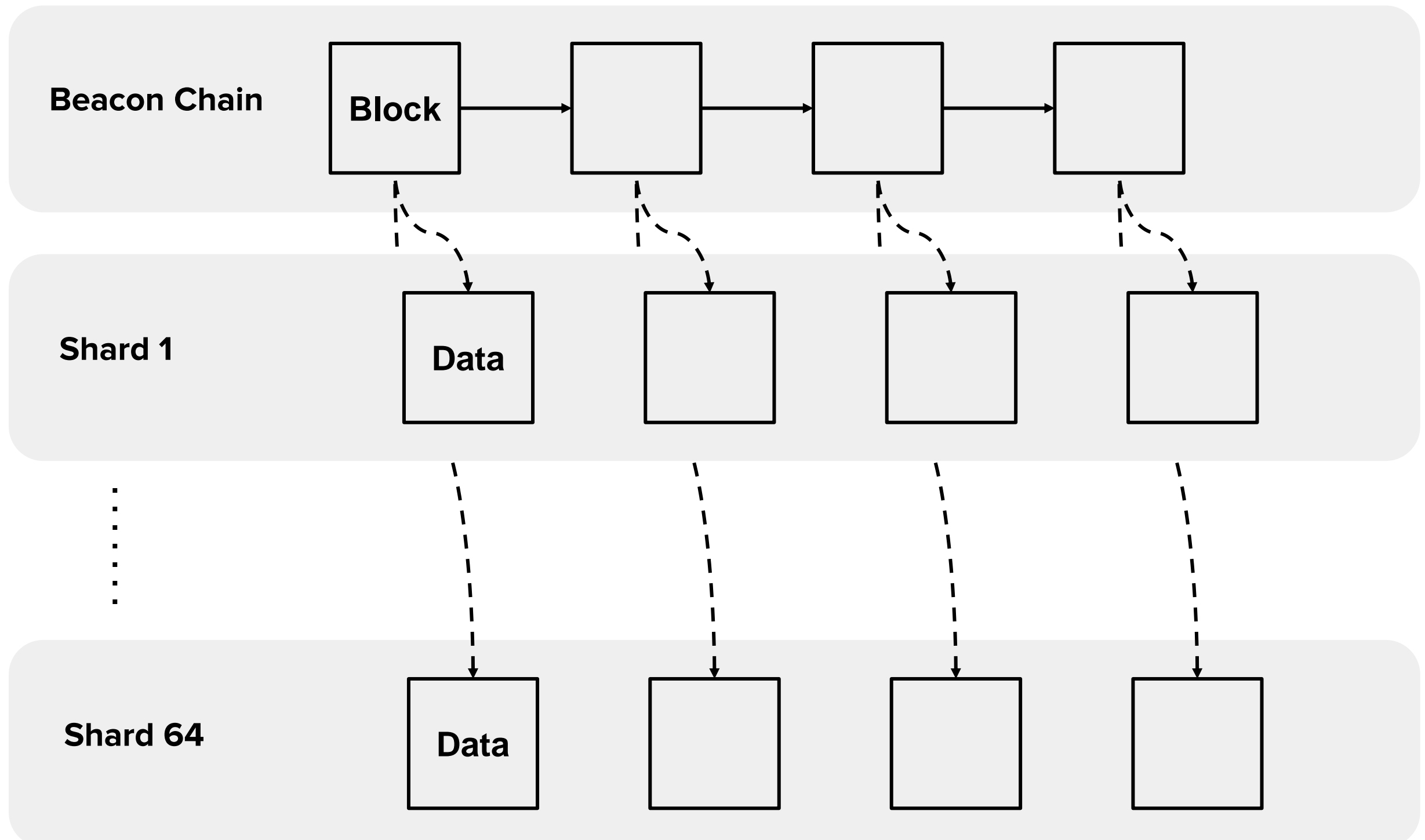
昨年12月 Eth2のBeacon chainがローンチ!

Beacon chainはシステム全体を管理するチェーンであり、単体ではユーザーは使えない
まずはPoSを導入、Shardingはまだない
あくまで最初の段階であり、これから機能が追加されていく

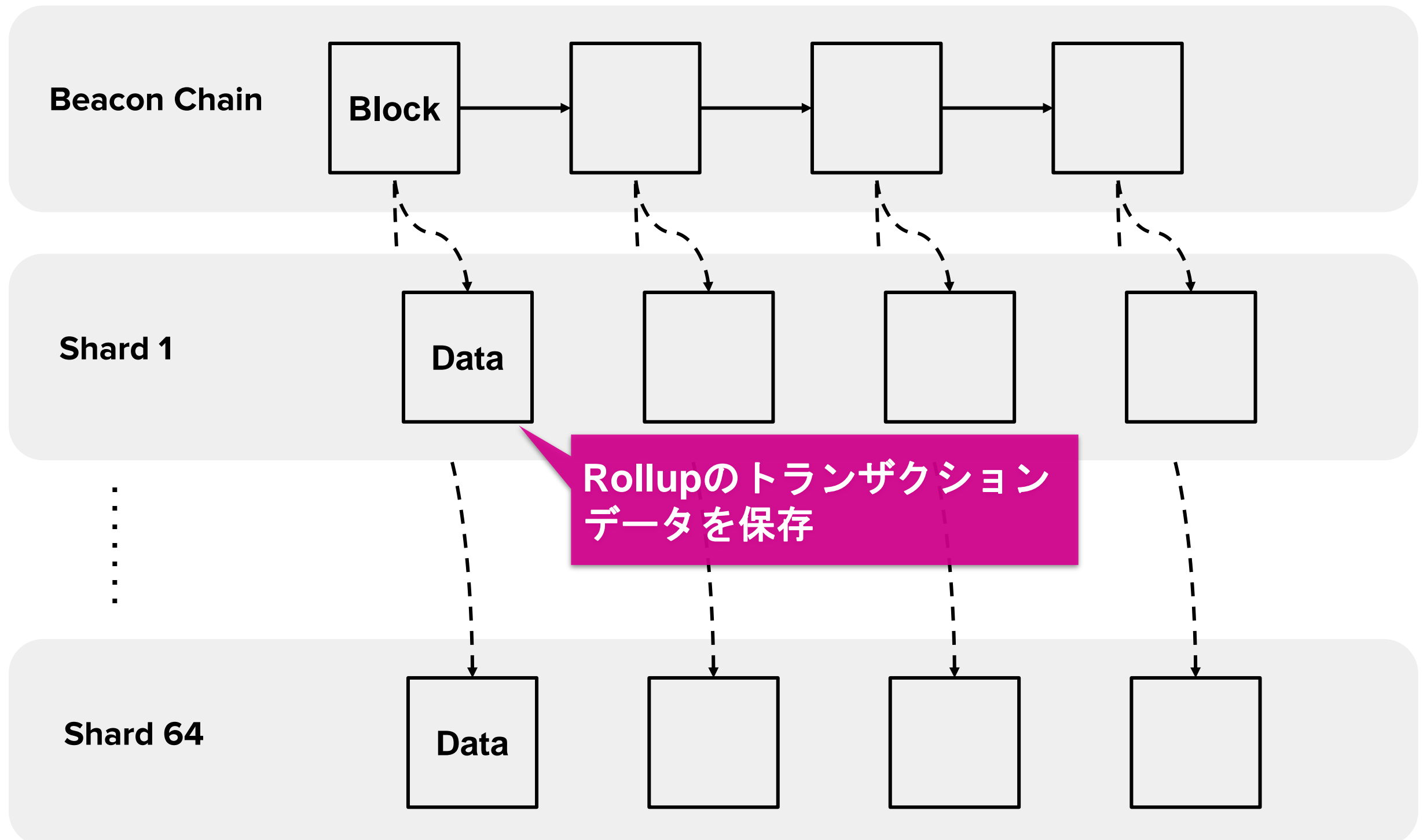


<https://beaconscan.com/>

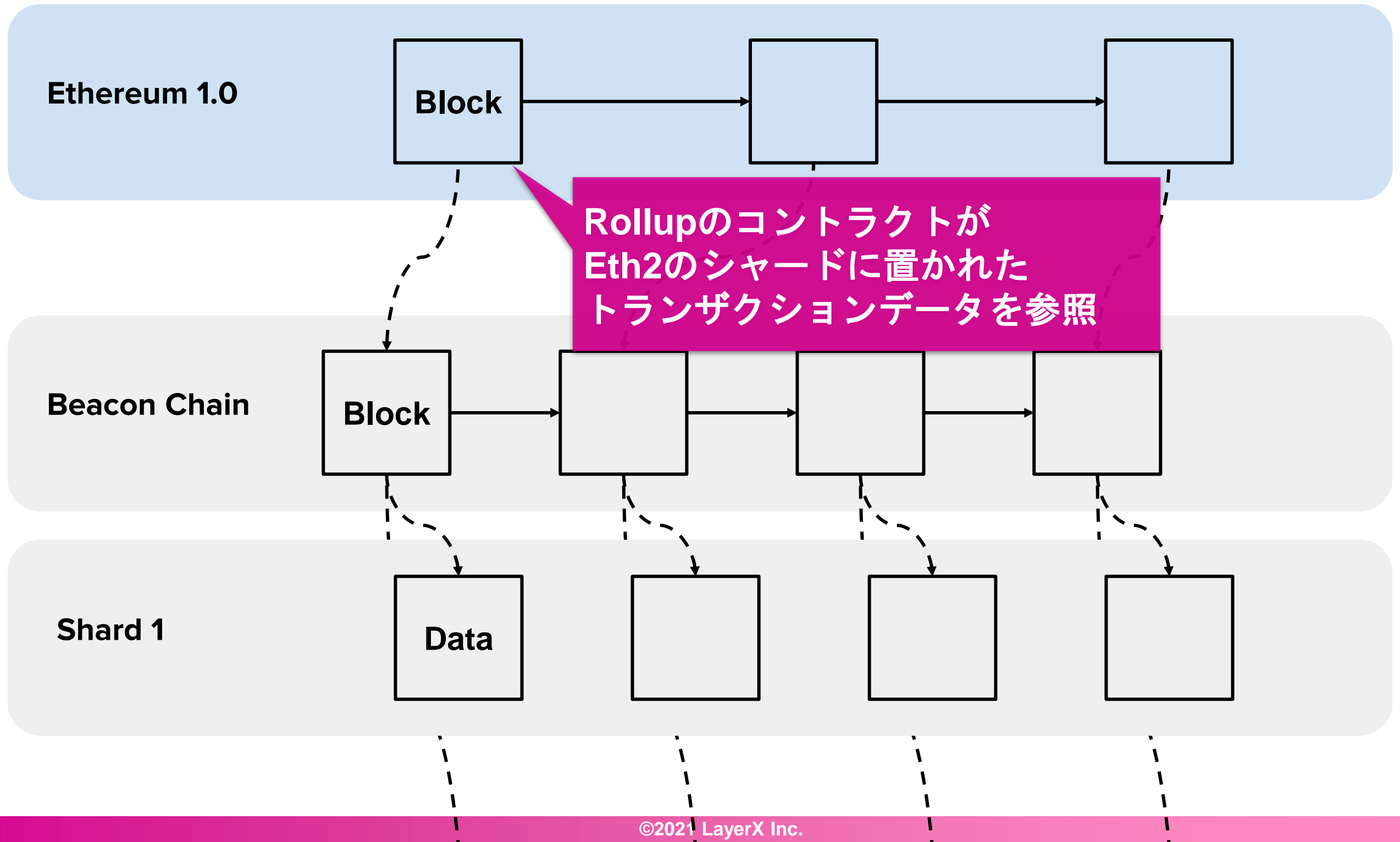
Beacon chainの次の大きなステップは、いよいよShardingの導入
ただし、各シャードは単にデータを乗せるだけの“Data sharding”



Data shardingでは、各シャードにスマートコントラクトはない（本当にただデータに乗せるだけ）
Rollupのトランザクションデータ置き場として使える！



Eth2のData shardingをEth1（現行のEthereumチェーン）のRollupと組み合わせるとのこと
Eth2 shardingにより「データ置き場」の容量が大幅に増えることで、Rollupがよりスケーラブルに



Eth1とEth2のマージ

Eth1+eth2 client relationship

Eth1-to-Eth2 Transition

djrtwo

1 Apr '20

eth1+eth2 client relationship

Since Vitalik proposed an [Alternative proposal for early eth1 <-> eth2 merge](#) in Dec 2019, there has been an active conversation about what this merger might look like from a software perspective and an eagerness to begin prototyping. The vision is a hybrid in which core consensus work is managed by an **eth2-client** and state/block-production is managed by an **eth1-engine** – together forming an eth1+eth2 client.

<https://ethresear.ch/t/eth1-eth2-client-relationship/7248>

Executable beacon chain

Eth1-to-Eth2 Transition



It's been a while since we've seen mkalinin — their last post was 7 months ago.



mkalinin

Nov '20

Special thanks to [@vbuterin](#) for the original idea, [@djrtwo](#), [@zilm](#) and others for review and useful inputs.

TL; DR an eth2 execution model alternative to executable shards with support of single execution thread enshrined in the beacon chain.

<https://ethresear.ch/t/executable-beacon-chain/8271>

シャードにコントラクト？

A rollup-centric ethereum roadmap



vbuterin

3 Oct '20

What would a rollup-centric ethereum roadmap look like?

Last week the Optimism team [announced](#) the launch of the first stage of their testnet, and the roadmap to mainnet. They are not the only ones; [Fuel](#) is moving toward a testnet and [Arbitrum](#) has one. In the land of ZK rollups, [Loopring](#), [Zksync](#) and the Starkware-tech-based [Deversifi](#) are already live and have users on mainnet. With [OMG network's mainnet beta](#), 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](#) and [others](#) are running on testnets.

The eth2 roadmap offers scalability, and the earlier phases of eth2 are approaching quickly, but base-layer scalability for applications is only coming as the last major phase of eth2, which is still years away. In a further twist of irony, eth2's usability as a data availability layer for rollups comes in phase 1, long before eth2 becomes usable for "traditional" layer-1 applications. These facts taken together lead to a particular conclusion: **the Ethereum ecosystem is likely to be all-in on rollups (plus some plasma and channels) as a scaling strategy for the near and mid-term future.**

If we start from this premise, we can see that it leads to some particular conclusions about what the priorities of Ethereum core development and ecosystem development should be, conclusions that are in some cases different from the current path. But what are some of these conclusions?

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

長期的にData sharding + Rollupで進む、もしくは、8個程度の少数のシャードのみでEVMのような実行環境をサポートするなどのアイデア

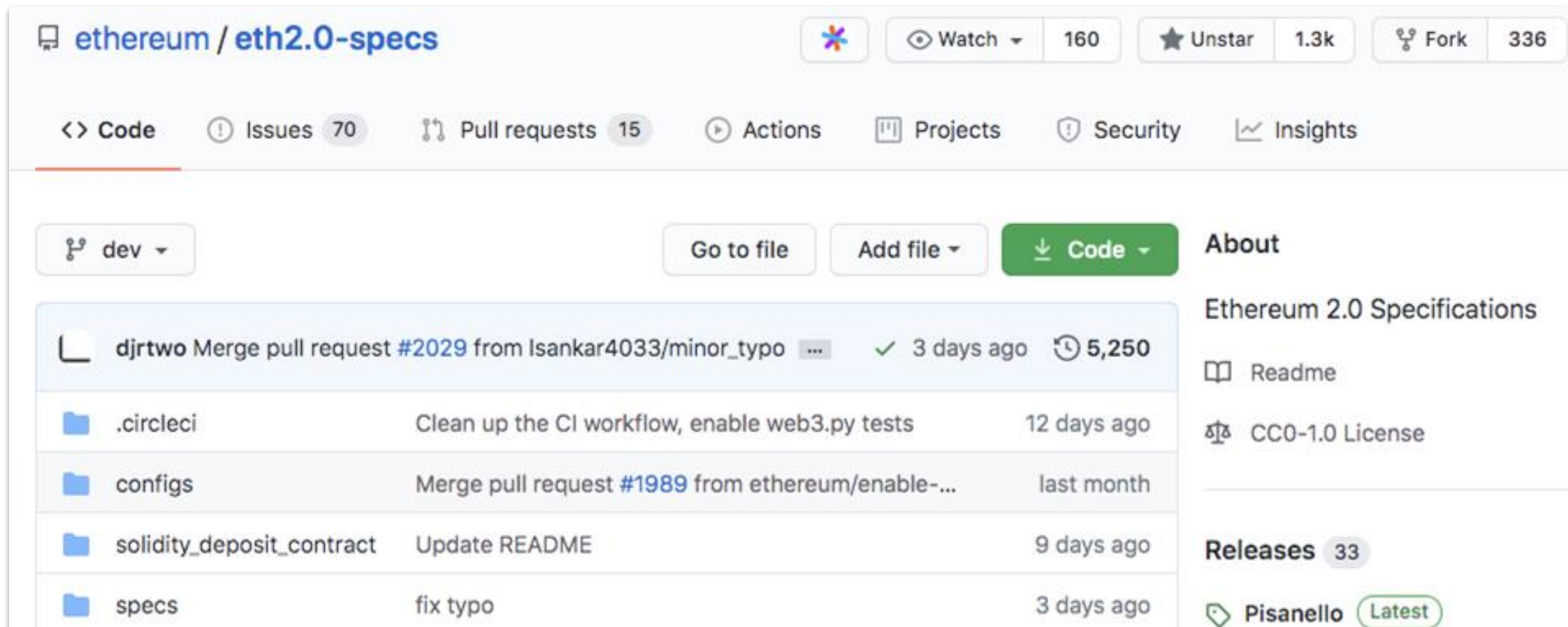
Data Sharding ～Deep-dive編～

**Q. Ethereum 2.0を
どうキャッチアップしたらいいの？**

**A. ブログ記事やプレゼンテーションで
概要を掴んだら、
技術詳細は公式のSpecを読みましょう**

**理由: 技術詳細については常に変わるので、
Spec以外の資料はメンテされないため
(Eth2チームにそんな人手がない)
(※Eth2 Shardingの方向性は徐々に固まりつつ
あるので、概要資料は今後増えるはず)**

今から、Data ShardingのSpecを例に、ライブ・リーディングしてみます
本日の目標: Specに対する恐怖心をなくす



The screenshot shows the GitHub repository page for `ethereum/eth2.0-specs`. The repository has 160 watchers, 1.3k stars, and 336 forks. The main navigation bar includes links for Code, Issues (70), Pull requests (15), Actions, Projects, Security, and Insights. Below the navigation bar, there are buttons for 'dev' branch, 'Go to file', 'Add file', and 'Code'. The repository description is 'Ethereum 2.0 Specifications'. The 'About' section includes a 'Readme' link and a 'CC0-1.0 License'. The 'Releases' section shows 33 releases, with the latest release being 'Pisanello'. The repository contains several folders: `.circleci`, `configs`, `solidity_deposit_contract`, and `specs`. A recent pull request by `djrtwo` is also visible.

<https://github.com/ethereum/eth2.0-specs>

- **GitHub eth2.0-specs**
 - [PR #2146](#)
 - [PR #2172](#)
- **HackMD**
 - [An explanation of the sharding + DAS proposal](#) by Vitalik

おしまい！



[@nrryuya_jp](#)



[@nrryuya](#)