LX L

LayerX Labs

Eth2 Data Sharding @ETHTerakoya

2021/2/4

LayerX, Inc.

Self Introduction & Company Introduction

Self Introduction: Ryuya Nakamura

LayerX

Executive Officer of LayerX Inc. & Director of LayerX Labs

- Participated in LayerX since its launch
  - R&D, academic publications
  - Promotion of joint projects with partner companies & government agencies
- IPA Frontier Talent Discovery Project 2020
- Brief CV: Gunosy Inc., Coubic Inc., University of Tokyo (Faculty of Engineering)
- Twitter: @nrryuya_jp

LX L

LayerX Labs

MITOU

©2021 LayerX Inc.

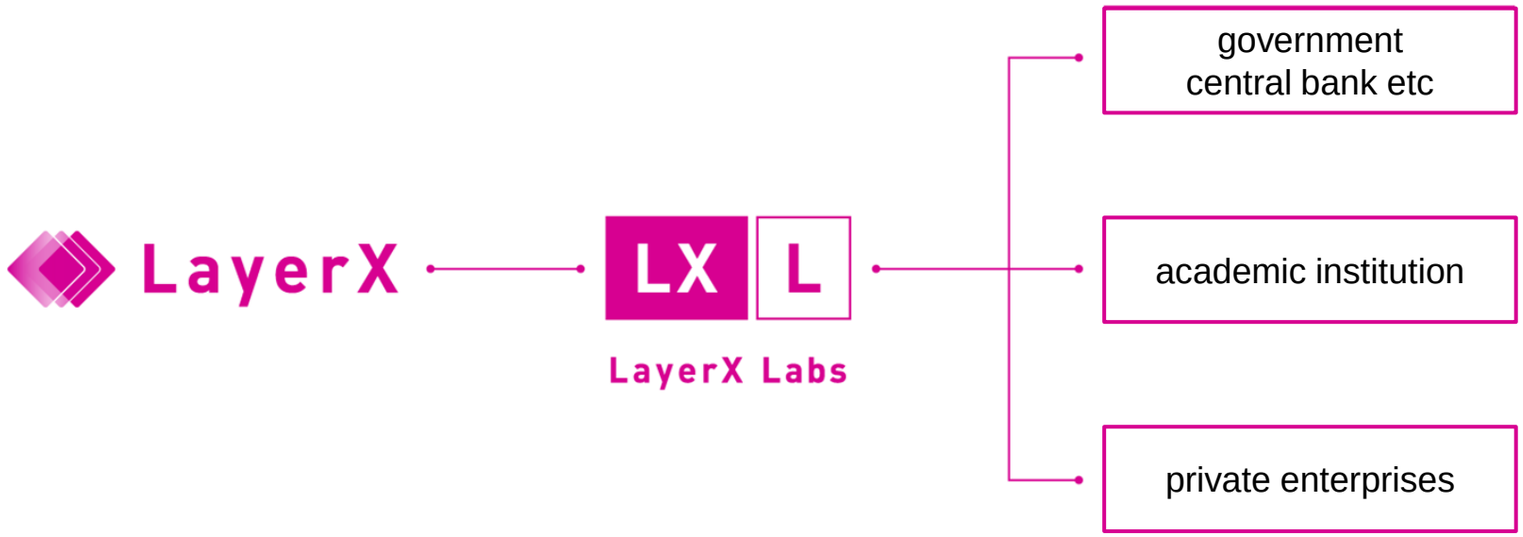
Company Introduction

Company name	LayerX Inc.
CEO	Yoshinori Fukushima (Founder of Gunosy)
Founded	August 1st, 2018
Stated capital & Capital reserves	3.1 billion yen
Business description	・General support for the digitalization of economic activities (digital transformation) ・Business development, software development, and R&D using blockchain technology
Number of employees	35 (as of the end of September 2020)
Address	〒103-0004 Frontier Higashi-nihonbashi 7F, Higashi-nihonbashi 2-7-1, Chuo-ku, Tokyo

Research Themes at LayerX Labs

LayerX Labs was founded in July 2020 to conduct joint research with the government, central banks, and academic institutions.

Digital currencies & payment	**We aim to digitize payments and currencies, the fundamental elements of economic activity. We also study the use cases and technologies of central bank digital currencies (CBDCs).**
Smart cities	**We work on tackling data security and privacy issues that crop up during cross-organizational and interdisciplinary collaboration.**
Public chains	**We approach the design of cryptocurrency-based mechanisms as a novel means to maintain our social infrastructure, and we contribute to Ethereum projects in particular.**



©2021 LayerX Inc.

Digital Payment: Joint Research with JCB

JCB and LayerX have launched a joint research project on next-generation B2B transaction history infrastructure that can connect multiple companies in the CBDC era.
This project aims to develop advanced services that harness commercial information across the supply chain while taking privacy considerations into account.

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

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た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み、当日中にすみやかに取引を再開する体制を整える。

再発防止の協議会は来年3月をめどに最終報告書をまとめる。4月以降に復旧にかかるシステム機能や業務フローなど運用を確認する訓練を継続的に行う。東証で復旧のめどがついた際に取引参加者に聞き取りを行うなど、新たな再発防止策の実効性を担保する。

野村HDなどは本格導入の前段階として、技術的な課題などを洗い出す。顧客情報や株式取引情報の疑似データを量子暗号を用いて伝送する実験に取り組む。「秘密分散」と呼ぶ手法により、複数のサーバーにデータを分散保管して安全性を高める仕組みも併せて検討する。国内の金融機関で量子暗号に必要な装置を実際に設置し、検証するのは初という。

サイバー攻撃の脅威が高まり、金融業界では顧客情報保護などの重要性が増している。世界で次世代計算機の量子コンピューターの開発が進み、現在普及している暗号技

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（FG）は、非金融サ

に、銀行と証券、信託でブランドや戦略、商品を共通化する」一方で、準富裕層には「デジタルを活用し、（顧客ひとりひとりに照準を合わせた）『パーソナライズドマーケティング』を深耕する」方針だ。

北京―上海間に巨大なネットワークを築く中国が先行して導入を進めるほか、米欧でも検討が活発化している。

企業間取引に分散台帳技術

JCBなど基盤開発

クレジットカード大手のジェーシービー（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。

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ーシービー（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 has joined the Tsukuba Smart City Council and has been appointed as a Super City Collaborator with the aim of making Internet voting for public offices elections a possibility.

LayerX Labs

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。

Tsukuba City Super City Basic Policy (draft)
https://www.city.tsukuba.lg.jp/_res/projects/default_project/_page_/001/008/988/02-14supercityhonpen.pdf

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]

保存

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。

Digital edition of Nikkei Shimbun (January 25th, 2021)
https://www.nikkei.com/article/DGXZQOFB277AV0X20C21A1000000/

©2021 LayerX Inc.

Public Administration: Making Internet Voting a Possibility

LayerX

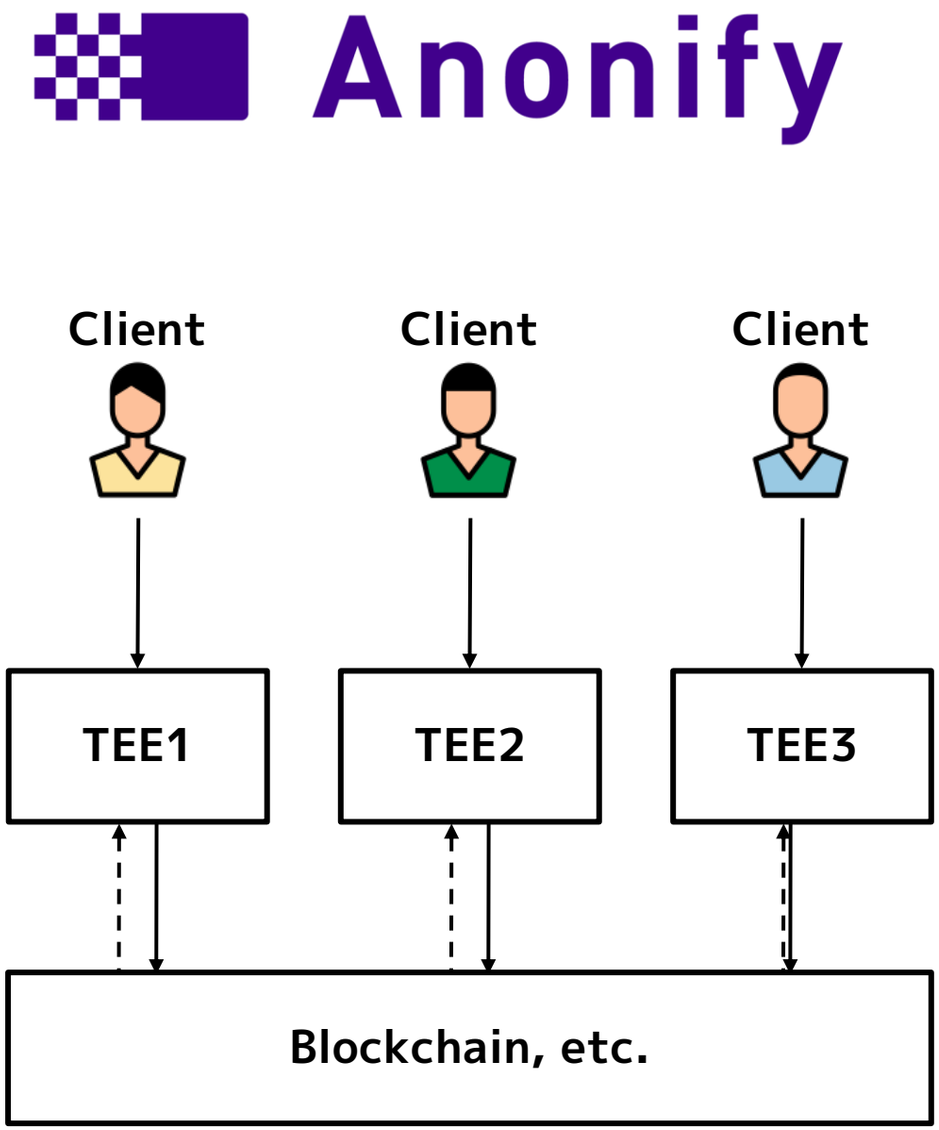
Kaga City in Ishikawa Prefecture, xID, and LayerX have signed a partnership agreement to implement electronic voting for municipal policies as the city hopes to become the first in Japan to set up a secure and convenient electronic voting system using blockchain technology and digital ID.

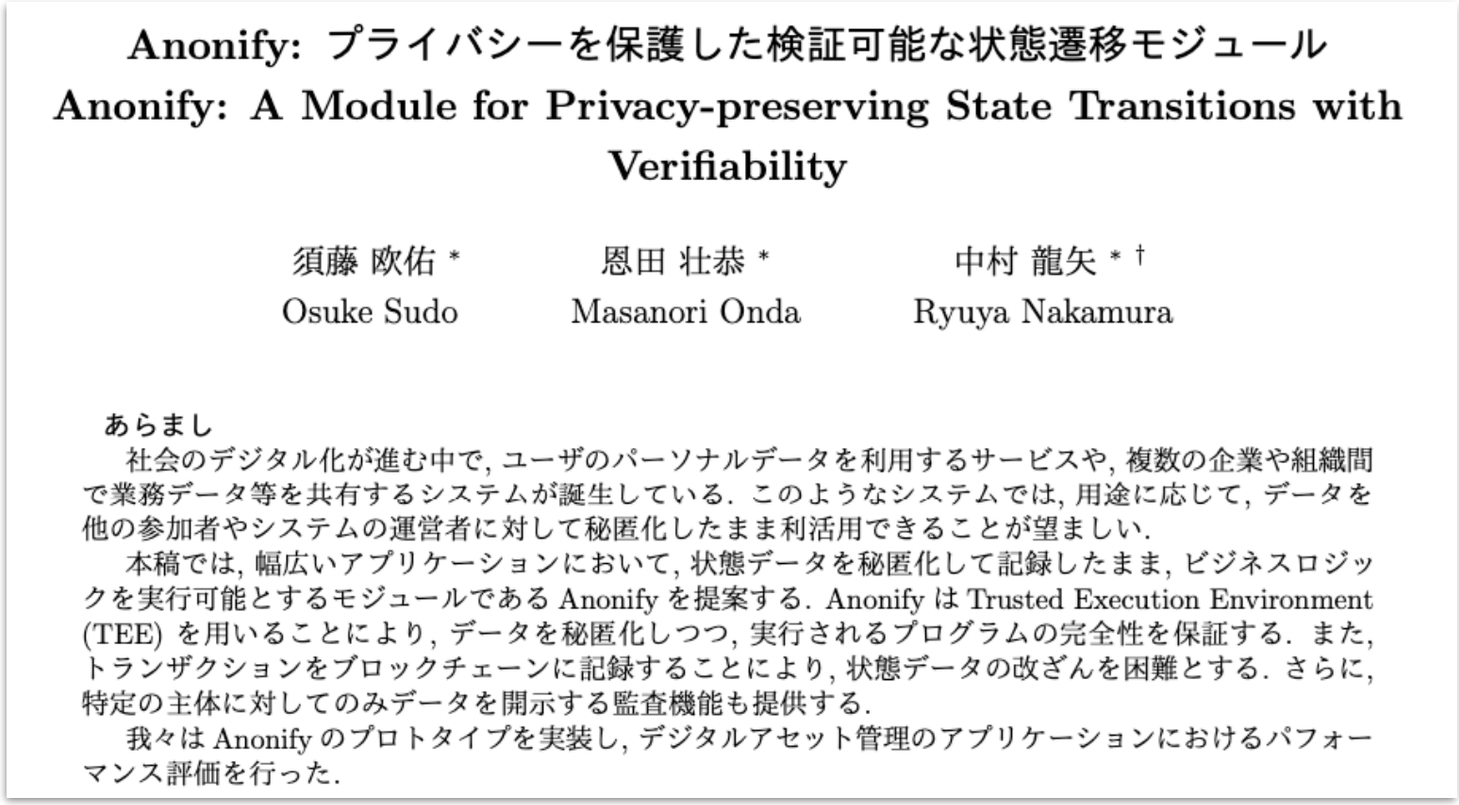
- We have signed a partnership agreement to **establish a “safe and convenient digital society”** in Kaga City using blockchain technology and digital ID.
- We have started to study the possibility of **implementing electronic voting for the municipal policies of Kaga City** as part of our efforts to promote the digitalization of administrative services.

©2021 LayerX Inc.

Development of New Technology: “Anonify,” LayerX’s Anonymization Module

Anonify is our patented anonymization and privacy protection technology based on Trusted Execution Environment (TEE) that allows for the anonymization and protection of identity across various applications (finance, public administration, voting, etc.)





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 * 恩田 壮恭 * 中村 龍矢 * †
Osuke Sudo Masanori Onda 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利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.

The above academic paper was presented at the conference “Symposium on Cryptography and Information Security 2021 (SCIS 2021)” held in Japan.

©2021 LayerX Inc.

Public Chain: Contributions to Ethereum

LayerX

We have contributed to the development of Ethereum 2.0 specifications, including the resolution of its vulnerabilities, and we were the first company in Japan to be selected for the Grant Program of Ethereum Foundation.

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

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-

Formal verification of CBC Casper
(Accepted for the international conference CVC'19)

ecosystem support program

Academic Research: Joint Research with the Tokyo Institute of Technology

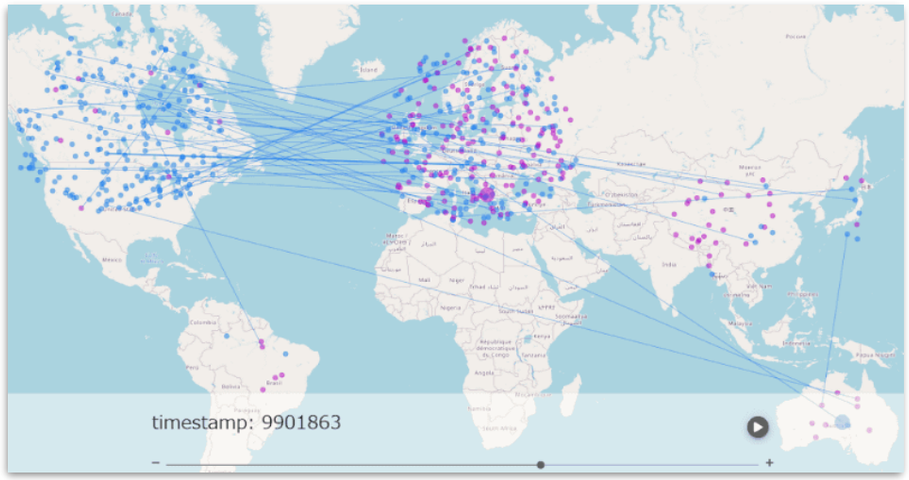
LayerX

We have conducted joint research on consensus algorithms, the foundation of blockchain technology, with a research group at the Tokyo Institute of Technology led by Assoc. Prof. Kazuyuki Shudo, et al.

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



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

©2021 LayerX Inc.

Mousse

An Emulator for the Local Testing of Eth2 Applications

“The Eth2 version of Ganache”

※Development ongoing under the
IPA Frontier Talent Discovery Project 2020

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

Today's Agenda

- An Overview of the Scaling of Ethereum
- An Overview of Eth2 Data Sharding
- A Deep Dive into Eth2 Data Sharding

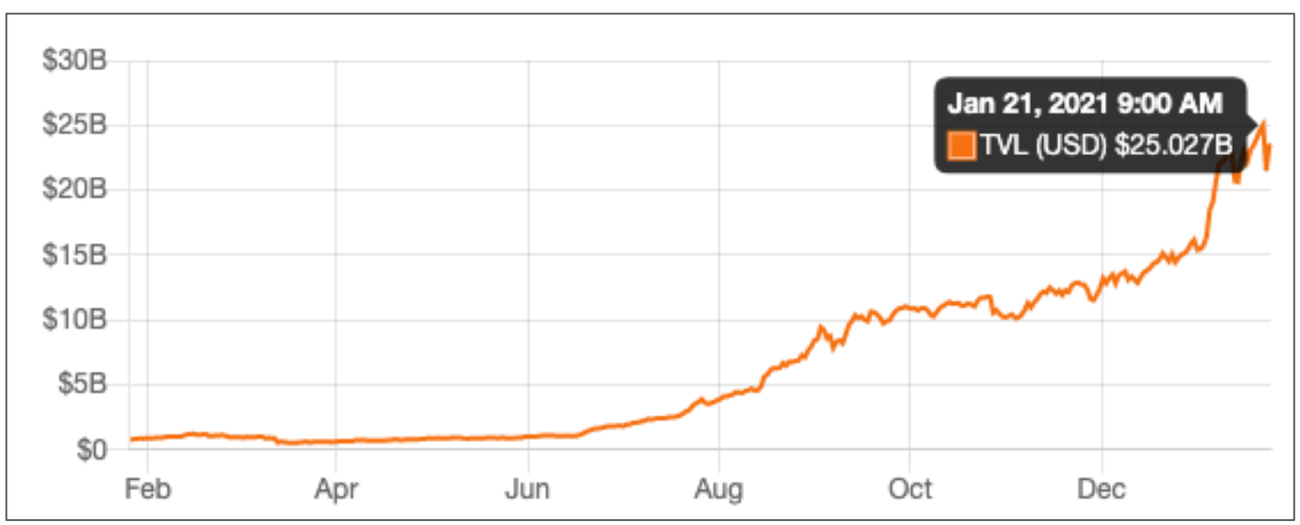
©2021 LayerX Inc.

The Scaling of Ethereum

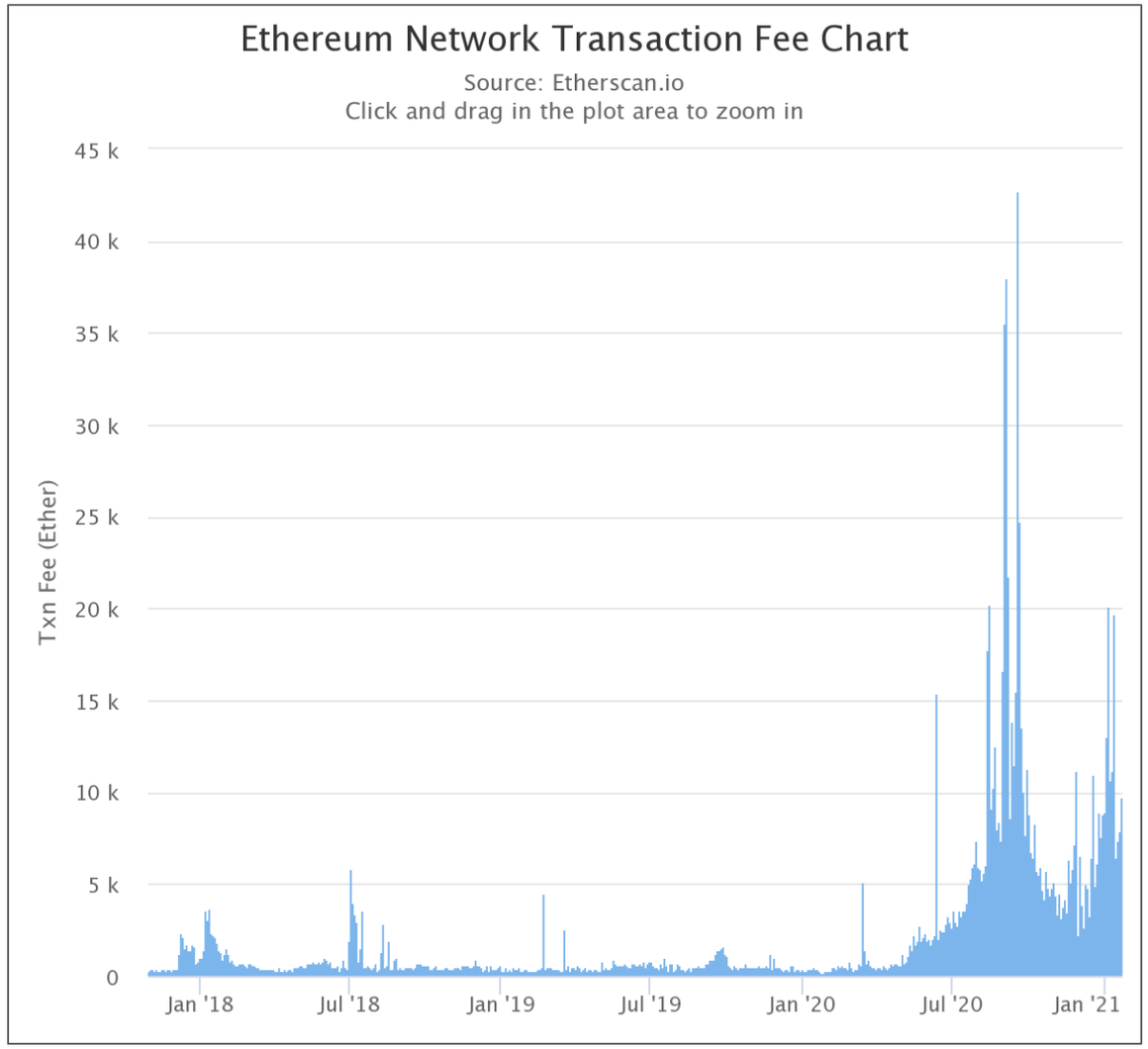
©2021 LayerX Inc.

The Latest Developments in Ethereum

Transaction fees have soared as Defi (decentralized finance) gains traction.
The scaling of Ethereum is now an urgent priority.



https://defipulse.com/



https://etherscan.io/chart/transactionfee

©2021 LayerX Inc.

Improving the Scalability of Ethereum

LayerX

※The following values are for reference only as the actual TPS value depends on the content of the transaction in question.

15 transactions/second

↓ **Rollup**

2,000 transactions/second

↓ **Ethereum 2.0 Data Sharding**

100,000 transactions/second

©2021 LayerX Inc.

Improving the Scalability of Ethereum

LayerX

※The following values are for reference only as the actual TPS value depends on the content of the transaction in question.

15 transactions/second

↓ **Rollup**

2,000 transactions/second

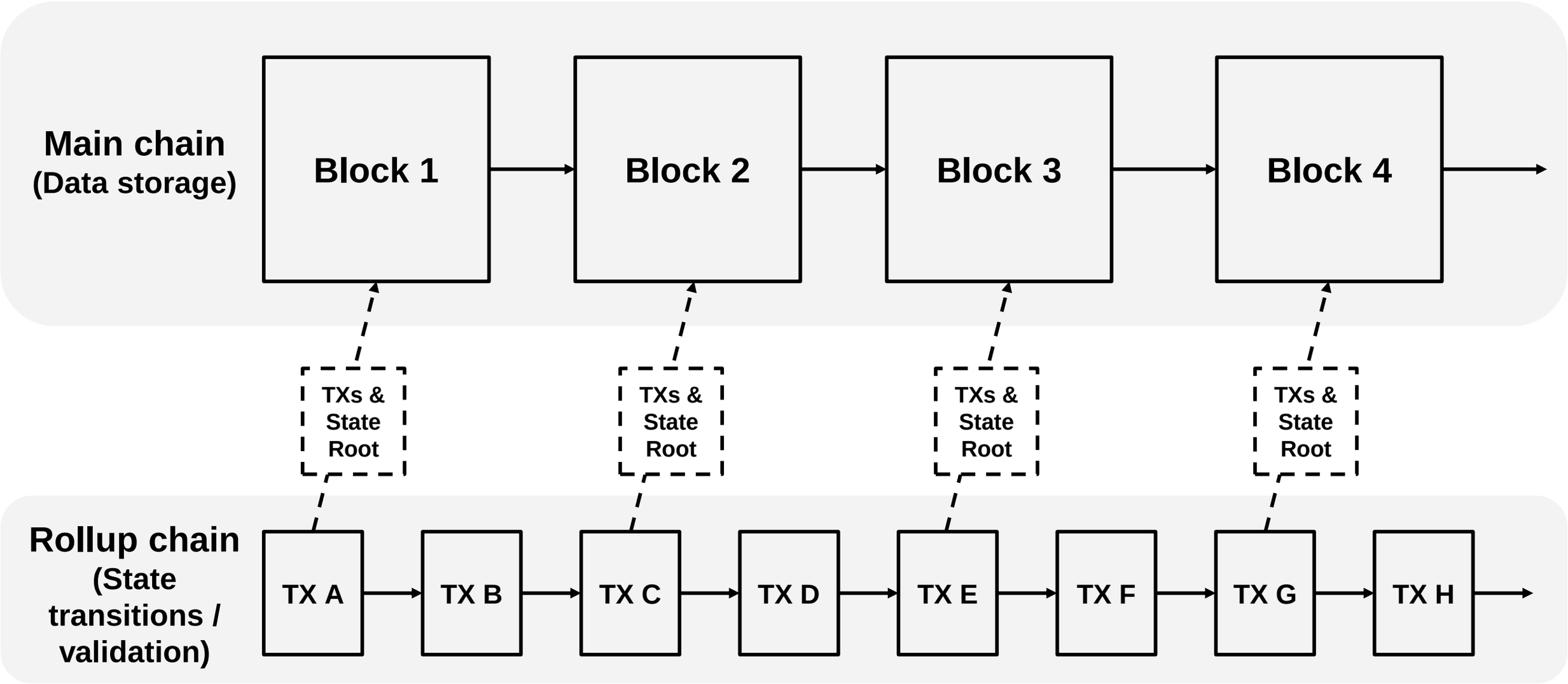
↓ **Ethereum 2.0 Data Sharding**

100,000 transactions/second

©2021 LayerX Inc.

Layer2 Scaling Technology: Rollup

Transactions are collected off-chain where state transitions are carried out, with only the results written to the main chain. The transaction data itself is stored on-chain.



©2021 LayerX Inc.

Layer2 Scaling Technology: Rollup

LayerX

Unlike normal transactions, state transitions in the Rollup off-chain are not validated in the main chain. The key is to use the transactions stored on the main chain to perform efficient validation off-chain.

- Methods of validating transactions off-chain
  - Proof of the accuracy of validation using ZK-SNARKs → ZK Rollup
  - Proof of invalid state transitions using Fraud proof → Optimistic Rollup

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

STARKWARE

https://medium.com/starkware/volition-and-the-emerging-data-availability-spectrum-87e8bfa09bb

©2021 LayerX Inc.

Improving the Scalability of Ethereum

LayerX

※The following values are for reference only as the actual TPS value depends on the content of the transaction in question.

15 transactions/second

↓ **Rollup**

2,000 transactions/second

↓ **Ethereum 2.0 Data Sharding**

100,000 transactions/second

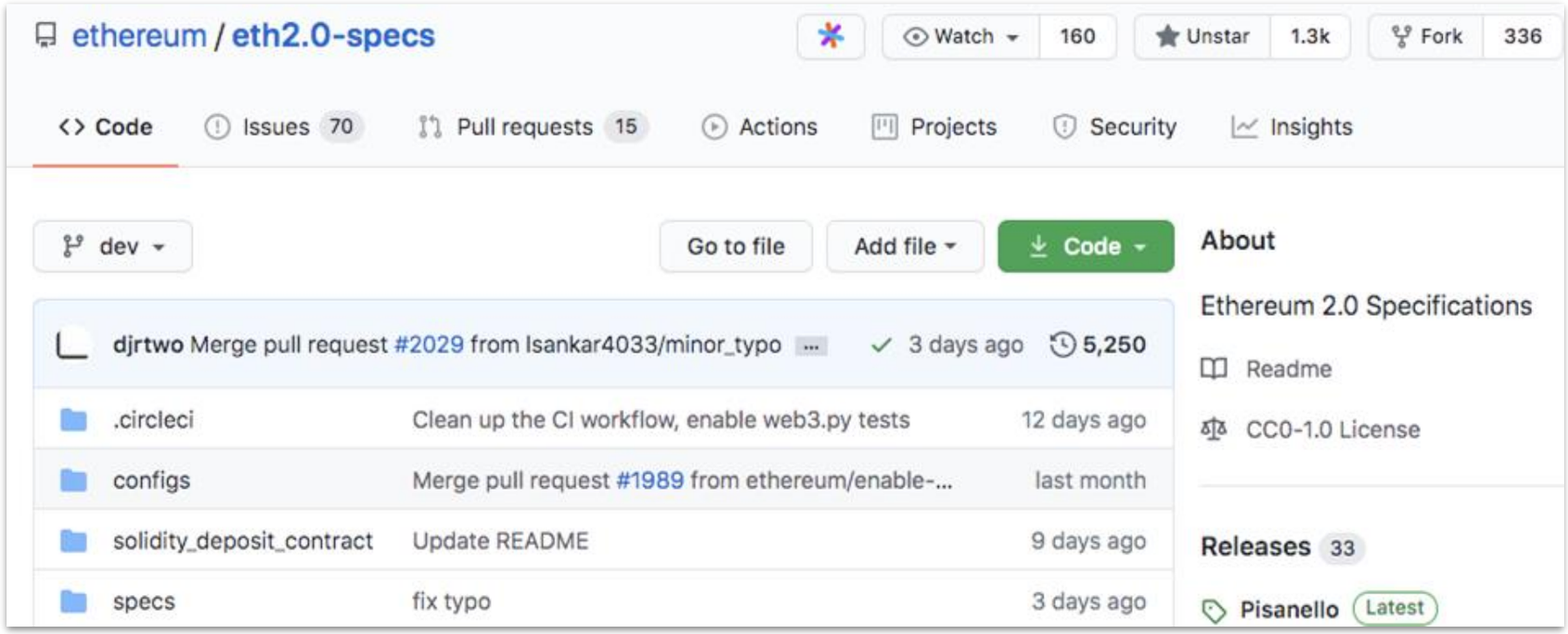
©2021 LayerX Inc.

Eth2 Data Sharding (Overview)

What is Ethereum 2.0 (Eth2)?

LayerX

Ethereum 2.0 (Eth2) is a sweeping protocol upgrade project for Ethereum.
It aims to prove the scalability and security of Ethereum by implementing ideas such as "sharding" and "proof of stake."



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

©2021 LayerX Inc.

Launch of the Eth2 Beacon Chain in December Last Year!

LayerX

The Beacon Chain is a blockchain that manages the entire system, and is not something that users can utilize on its own. PoS has been implemented, but sharding has not. This is just the first phase of a massive project, and more features will be introduced moving forward.

CURRENT EPOCH	FINALIZED EPOCH	ACTIVE VALIDATORS	PENDING
12054	12052	69063	18198
CURRENT SLOT	**FINALIZED SLOT**	**VOTED ETHER**	**ELIGIBLE ETHER**
385748	385664	2,181,322 (98.72%)	2,209,572

24 HRS NETWORK PARTICIPATION CHART

Latest Blocks (+11 Scheduled) View All

EPOCH	SLOT	POS	STATUS	AGE	ATT
12054	385748	21 of 32	proposed	19 secs ago	43
12054	385747	20 of 32	proposed	31 secs ago	25
12054	385746	19 of 32	proposed	43 secs ago	35
12054	385745	18 of 32	proposed	55 secs ago	48
12054	385744	17 of 32	proposed	1 min ago	17
12054	385743	16 of 32	proposed	1 min ago	22
12054	385742	15 of 32	proposed	1 min ago	23
12054	385741	14 of 32	proposed	1 min ago	67
12054	385740	13 of 32	proposed	1 min ago	21
12054	385739	12 of 32	proposed	2 mins ago	59

Validators Leaderboard View All

RANK	INDEX	CURRENT BALANCE	TOTAL INCOME
#1	11111	32.7974 ETH	+ 0.7975 ETH
#2	4617	32.7951 ETH	+ 0.7951 ETH
#3	19030	32.7909 ETH	+ 0.7910 ETH
#4	1406	32.7902 ETH	+ 0.7902 ETH
#5	10689	32.7886 ETH	+ 0.7886 ETH
#6	10063	32.7876 ETH	+ 0.7877 ETH
#7	10055	32.7846 ETH	+ 0.7847 ETH
#8	11398	32.7787 ETH	+ 0.7787 ETH
#9	11313	32.7343 ETH	+ 0.7344 ETH
#10	15703	32.7308 ETH	+ 0.7309 ETH

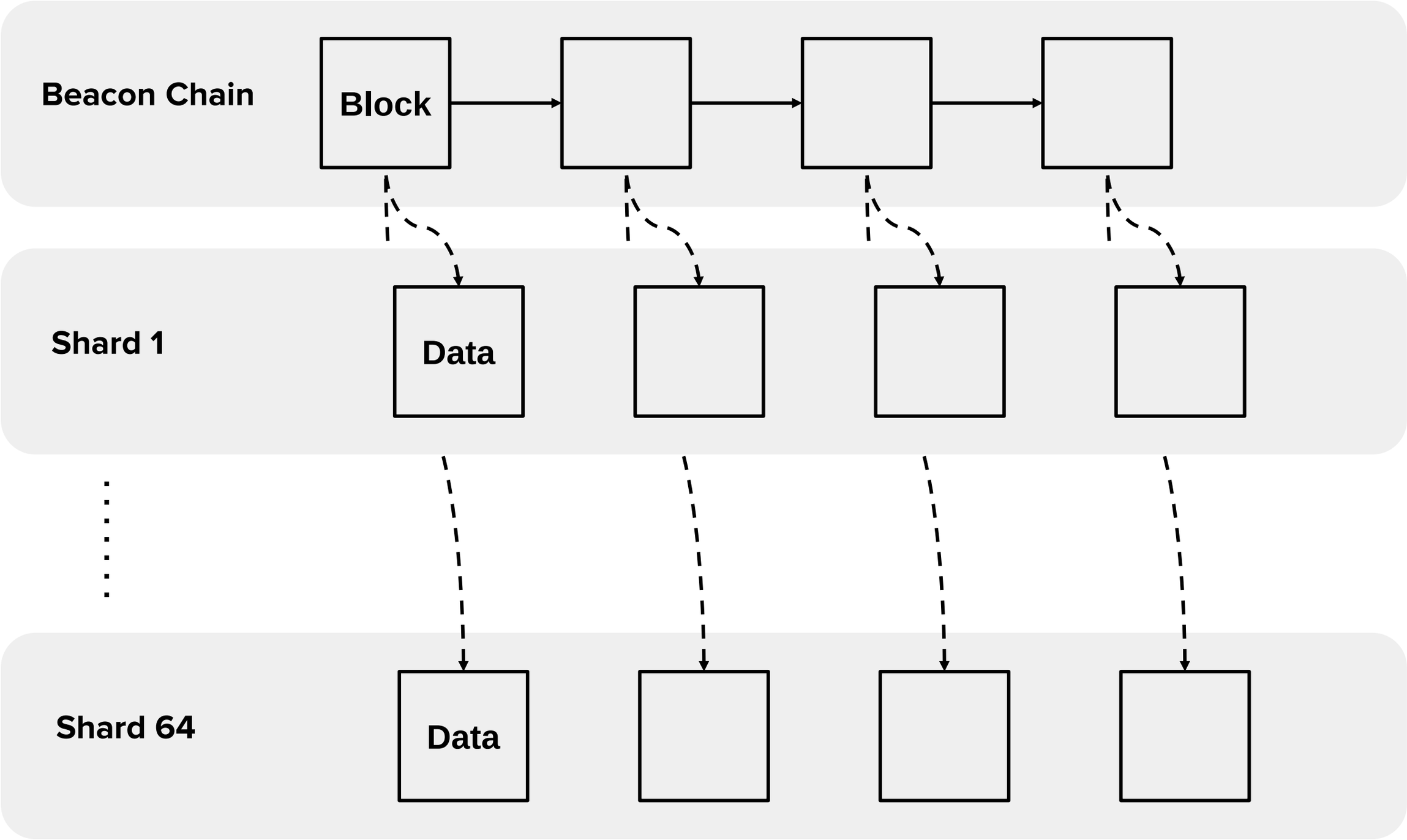
https://beaconscan.com/

©2021 LayerX Inc.

The Next Step for Eth2: Data Sharding

LayerX

The next big step for the Beacon Chain is to finally implement sharding.
However, individual shards only serve to hold data through "data sharding."

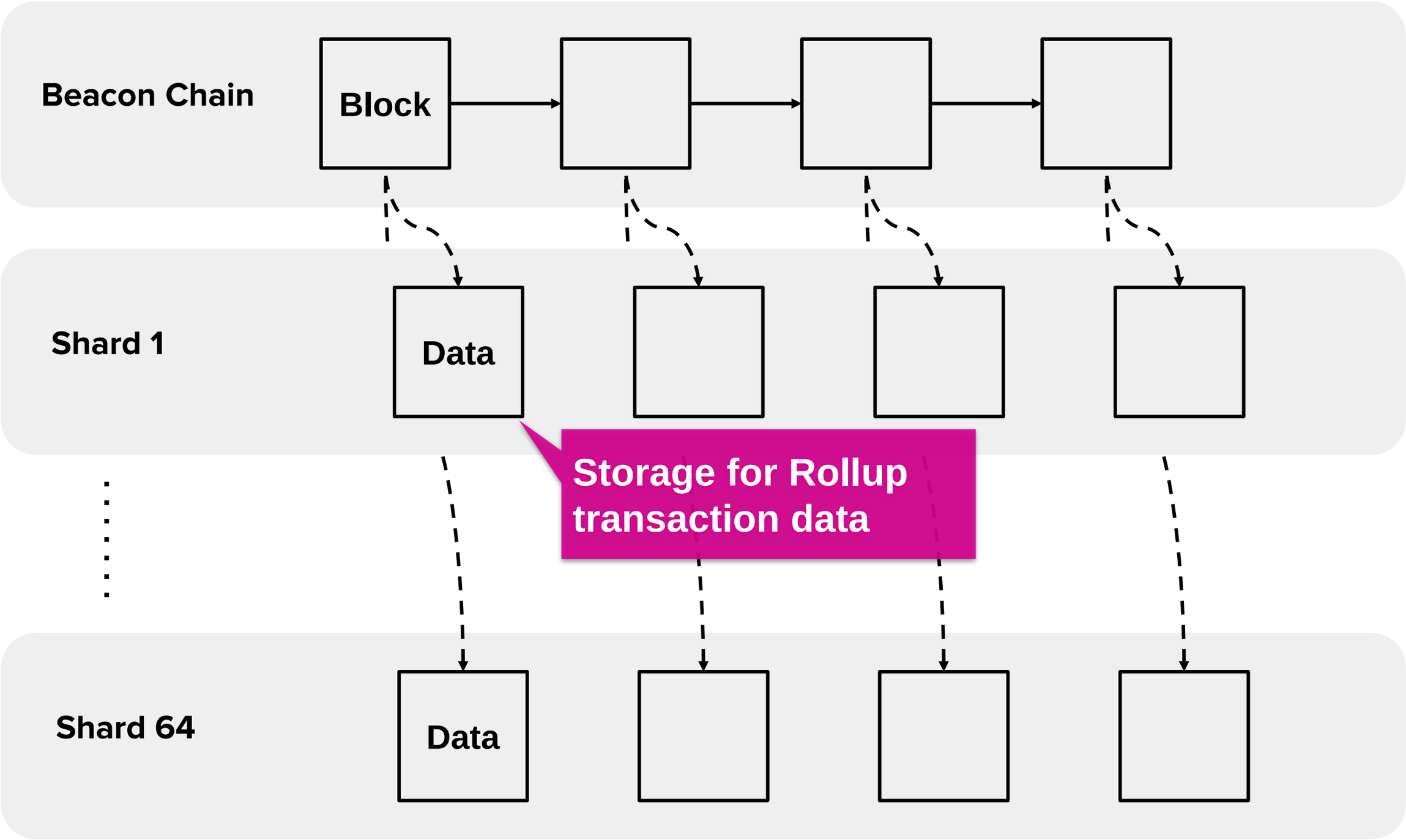


©2021 LayerX Inc.

The Next Step for Eth2: Data Sharding

LayerX

With data sharding, there are no smart contracts on each shard (as the shards only serve to hold data). Thus, shards can be used as a repository for Rollup transaction data!

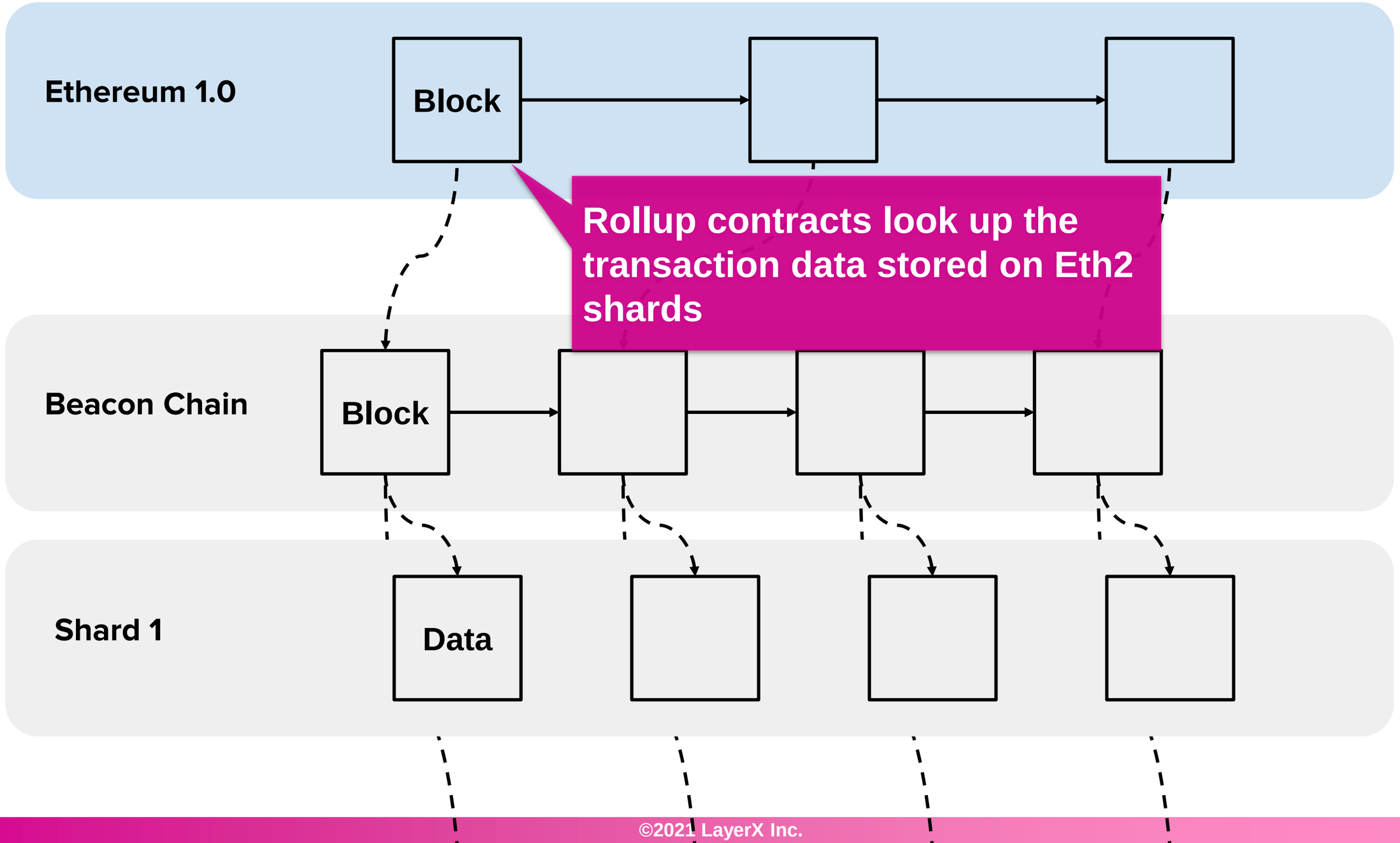


©2021 LayerX Inc.

The Next Step for Eth2: Data Sharding

LayerX

Eth2 data sharding will be integrated with Rollup in Eth1 (the current Ethereum blockchain). The introduction of Eth2 sharding will greatly increase the capacity for "data storage," which will make Rollup more scalable.



©2021 LayerX Inc.

What is the Future of Data Sharding?

LayerX

Merging Eth1 with Eth2

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* 41 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

Contracts on shards?

A rollup-centric ethereum roadmap

vbuterin 3 Oct '20

What would a rollup-centric ethereum roadmap look like?

Last week the Optimism team announced 178 the launch of the first stage of their testnet, and the roadmap to mainnet. They are not the only ones; Fuel 126 is moving toward a testnet and Arbitrum 97 has one. In the land of ZK rollups, Loopring 90, Zksync 82 and the Starkware-tech-based Deversifi 74 are already live and have users on mainnet. With OMG network's mainnet beta 83, 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 311 and others 130 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

Some longer-term ideas include moving forward with data sharding + rollup, or supporting an EVM-like execution environment with only a small number of shards (e.g., around 8 shards)

©2021 LayerX Inc.

Data Sharding
～Deep-dive～

Q. How do I catch up on Ethereum 2.0?

©2021 LayerX Inc.

LayerX

A. Once you have gained a basic understanding from blog posts and presentations, read the official specifications for the technical details.

©2021 LayerX Inc.

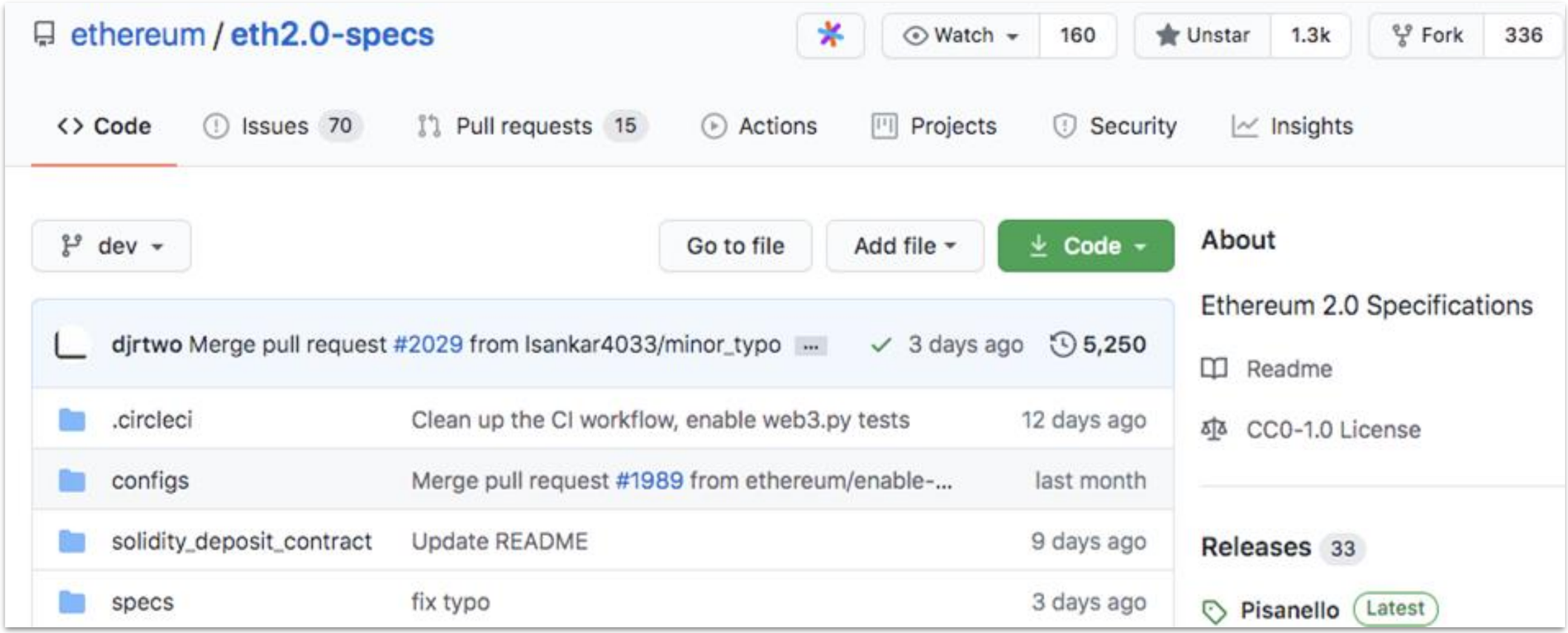
Reason: The technical details are constantly evolving, and materials other than the specifications may not be up to date (since the Eth2 team does not have the manpower for that). (※There should be more introductory materials in the future as Eth2 sharding becomes increasingly established)

©2021 LayerX Inc.

Let’s Try Reading Eth2 Specifications

LayerX

Next, we will try to do some on-the-spot reading of specifications on data sharding as an example.
Today’s goal: Overcome your fear of specifications



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

©2021 LayerX Inc.

Some Online References for Today

- **GitHub eth2.0-specs**
  - **PR #2146**
  - **PR #2172**

- **HackMD**
  - **An explanation of the sharding + DAS proposal by Vitalik**

©2021 LayerX Inc.

The End!

@nrryuya_jp

@nrryuya