Basically, there are two ways to scale a blockchain. One is to work on the main chain itself to improve transaction capacity. That is what Ethereum 2.0 is all about. The other way is to change how people use the blockchain. In other words, instead of putting all the interactions on the main chain, some can go off-chain to alleviate congestion.

That is a simple way to differentiate between Layer 1 and Layer 2 scalability solutions. For example, in a Layer-2 solution, the smart contract on the main chain could only have two tasks: (a) process deposits and withdrawals, and (b) verify proofs to ensure that everything happening off-chain is obeying the rules. And that brings us to Sharding.

**What Is Sharding?**

Sharding is ETH 2.0’s scalability solution that will take place when Ethereum moves its consensus mechanism from Proof of Work (PoW) to Proof of Stake (PoS). This is a complex, major upgrade, and it is a Layer-1 solution.

Sharding is a technique that takes large chunks of computational work and splits it into smaller pieces called “shards.” But Sharding won’t happen overnight as it’s only one part of the larger Ethereum upgrade.

The good news is that other solutions can take some of the pressure off Ethereum now, which makes the Sharding solution less urgent.

**Ethereum’s Layer-2 Scaling Solutions**

We’ll be covering the following Layer-2 solutions along with their different strengths and weaknesses.

* Sidechains
* State Channels
* Plasma
* Optimistic Rollups
* ZK-Rollups

**What Are Sidechains?**

Sidechains are independent blockchains that are considered more of a hybrid of Layer 2 and Layer 1. That’s because Layer 2 solutions rely on the security of the main chain. A Sidechain doesn’t do that because it has its own security properties. It also employs its own consensus mechanisms to process transactions.

To understand Sidechains remember that the Ethereum blockchain is the main chain. So if Ethereum is the main chain, then Sidechains are like sister chains. Essentially, Sidechains run alongside the main chain. Furthermore, these blockchains can communicate with each other so that assets can move between the chains.

To create a Sidechain, developers must first create another blockchain and a consensus mechanism like PoW, PoS, Proof of Authority (PoA), or Delegated Proof of Stake (dPoS).

Next, moving assets between the blockchains requires a smart contract on Ethereum. To get assets to the Sidechain, users would first deposit into an Ethereum smart contract and then recreate them on the Sidechain. Getting the assets back to Ethereum requires removing them from the Sidechain and unlocking them once they’re back on Ethereum.

**What Are State Channels?**

Think of State Channels as a way to conduct interactions off the blockchain that would normally be on the blockchain. For example, only the most important element of a chess game would get broadcast to Ethereum in State Channels—that would be the outcome.

To demonstrate how State Channels work, we’ll use the much-loved Bob and Alice characters. Let’s say that Alice sells Bob her internet service, charging him 10 cents per megabyte. But instead of creating a transaction on the main chain for each megabyte payment, they could use a State Channel.

First, Bob locks up some ETH into a smart contract to get things rolling. Next, he signs an off-chain message (ticket) that says he has paid 10 cents to Alice. Bob later signs another ticket that says he has paid 20 cents. This can continue until they conclude their business. Let’s say Alice wants to cash in when the payments reach $1. At that point, she publishes the ticket to the main chain. The smart contract verifies both of their signatures, pays Alice the $1 amount and returns Bob’s remainder.

**State Channels and Bi-Directional Payments**

State Channels can handle bidirectional payments between two parties like Alice and Bob, but they can also transact with others who have an open channel in common. For example, if Bob has an open channel with Ted, Alice can also interact with Ted.

But Channels are limited. Amongst other things, they can’t send funds off-chain to non-participants. Also, if things get more complex than recurring payments, the participants have to lock up large amounts of capital.

**What Is Plasma?**

Essentially, Plasma is made up of Merkle trees and smart contracts. This combination enables Plasma to create unlimited child chains, which are smaller versions of the main chain. Note that developers can build multiple chains on top of each child chain to create a tree-like structure. The smaller chains are called child chains or Plasma Chains.

Plasma’s secondary chains only need to interact periodically with the main chain for things like settling disputes. Notice that Plasma Chains and Sidechains are similar but not the same thing. It’s important to understand their differences because Sidechains and Plasma make different promises regarding securing funds.

**Plasma Deposits and Withdrawals**

To make a deposit, a user sends the asset to the smart contract that manages the Plasma Chain. The Plasma Chain will assign a unique ID to the asset. An operator then generates a batch of Plasma transactions they have received off-chain at intervals.

To withdraw an asset, the contract starts a “challenge period.” During this time, anyone can use Merkle branches to invalidate the withdrawal if they can prove the exit is fraudulent. After the challenge period is up, the user can withdraw the asset.

One advantage Plasma has over State Channels is that the capital requirements are a lot lower. Also, a user can send assets to participants who are not part of the system.

**What Are Rollups?**

We’ve touched on some of the strengths and weaknesses of the other scalability solutions. What users want is a solution as secure as Ethereum but fast and inexpensive. That’s why Rollups are all the rage. They are in a position to deliver and become Ethereum’s savior for now and the foreseeable future. But what exactly is this Rollup technology, and how does it work?

First of all, they’re called Rollups because they roll up transactions and fit them into a single block. Doing so thankfully relieves the Ethereum network from some of its congestion and makes transactions faster and less expensive. Rollups also help scalability because they process transactions off the main chain.

Ethereum’s co-founder Vitalik Buterin stated that transaction speeds could increase by a factor of 100 with Rollups. Eric Wall, CIO of Arcane Assets, said that he expects rollups to push transaction speeds up to 2,000-3000 per second.

So, while Plasma and State Channels try to move both the data and its computation off-chain, the security issues this causes demand that both solutions rely on what’s called “owners.”

**Rollups Improve Transactions Per Second (TPS)**

On the other hand, Rollups move state storage and computation off-chain but keep some of the data on-chain. This requires some compression tricks to improve efficiency, and while the main chain’s bandwidth still limits scalability for Rollups, it still retains a favorable ratio.

One estimate has an ERC-20 token transfer costing 45,000 gas on Ethereum costing less than 300 gas with only 16 bytes of space required on-chain with a Rollup. Other estimates predict Rollups might even do 10,000 TPS once Ethereum 2.0 Shards go live.

**Rollups Compression Tricks and on-Chain Data**

These kinds of numbers can only be possible because of superior encoding and some clever compression tricks. Compression is instrumental because, without it, Rollups are estimated to only make a 10x improvement to main chain scalability.

Putting data on-chain is also key. Offline operators or malicious actors can’t do damage or cause delays like they can with the other solutions. Also, Rollups don’t suffer the necessity of mapping assets to owners. Developers can even run an Ethereum Virtual Machine (EVM) inside a Rollup. This breakthrough makes it possible for developers to migrate their dApps to Rollups without any new code, so you can see why Vitalik and the Ethereum community are so excited about Rollups.

A big question regarding Layer 2 solutions is, “who controls the exits? With Rollups, the exits are under the control of Layer 1, and that is the Ethereum blockchain. While Google may use the slogan, “Don’t Be Evil,” Rollups take a “Can’t Be Evil” approach when it comes to fraud proofing their system.

**How Rollups Work**

The short version is that an on-chain smart contract maintains a state root with things like the account balances and contract code inside the Rollup. A batch is a compressed collection of transactions. When a user publishes a batch with the previous state root and the new state root with processed transactions, the smart contract makes sure it all matches up. Then it will switch the old state root to the new state root.

The next question is how to prevent a fraudster from submitting a post-state root that conveniently transfers the assets inside the Rollup to themselves? The solution to this potential problem is what has split Rollups into two different camps.

**What Is a ZK-Rollup?**

The Zero Knowledge Proof Rollup uses validity proofs. This means that every batch includes a Zero-Knowledge Proof (SNARK). The SNARK is cryptographic proof that proves the post-state root is correct after it executes the batch. Moreover, on-chain verification is quick regardless of the computation size.

Operators must generate a SNARK for every state transition, and this will be verified by the smart contract on the main chain. That means operators can’t steal the funds. Nor can they corrupt the Rollup state, so no monitors are necessary. User funds are guaranteed once a block is verified, even if operators become uncooperative.

Furthermore, ZK-Rollups have two types of users: transactors and relayers. Transactors create and broadcast their transfer to the network. Relayers create a rollup by collecting a large number of transfers and rolling them up together. Relayers are tasked with generating the SNARK proof. Anyone desiring to be a relayer can do so once they have staked their bond. This requirement encourages the relayer to play it straight and not tamper with the Rollups.