MPSSDEGB
कौशल से रोजगार, समृद्धि अपार

FITT
Foundation For Innovation And Technology Transfer

Layer 2 Solutions and Types

S. No	Topic
1	An Overview of Blockchain Layers
2	Introduction
3	What is Layer-2 Scaling Solution?
4	Characteristics of Layer 2 Solutions
5	Elements of Layer 2 Solutions
6	Types of Layer 2 Scaling Solutions
7	Advantages of Layer 2 Solutions
8	Challenges and Risks of Layer 2 Solutions
9	Use Cases of Layer 2 Solutions
10	Layer-1 vs. layer-2 Scaling Solutions
11	The Future of Layer 2 Solutions
12	Summing Up

An Overview of Blockchain Layers

Blockchain technology has brought about a revolutionary change in the world of finance and beyond. However, the complexity of the technology can be intimidating for newcomers, especially when trying to understand the different layers that make up the blockchain ecosystem. To make it easier to understand, the blockchain ecosystem is often divided into layers. Blockchain layers are the different levels of infrastructure that work together to enable the operation of a blockchain-based system. Each layer has its unique characteristics and purposes and it builds on top of the previous one, with each layer leveraging the infrastructure of the previous layer. In this section, we will explore each layer:

Layer 0: Software Infrastructure

It is the base layer. It consists of the hardware, the Internet, and the connections that allow Layer 1 blockchains to run smoothly and efficiently. Also in this layer are the protocols from which entire blockchains can be built, allowing interoperability between these networks.

A very popular protocol at this layer 0 is Cosmos, which provides open-source tools that allow blockchains created with this protocol to be interoperable and communicate with each other, while still allowing projects to meet their own blockchain needs. Therefore, gas costs can be reduced without affecting throughput too much.

Layer 1 (or simply "L1″): Blockchains/Networks

It is the blockchain itself and the layer responsible for security. This layer 1 ensures that blockchain network protocols are followed and implemented. It runs consensus mechanisms, programming languages, and other technical processes to finalize transactions on the network. In short, Layer 1 is generally concerned with creating and adding new blocks to the network.

The widely known Bitcoin and Ethereum are examples of L1 blockchains. The Bitcoin blockchain uses proof of work (PoW) as its consensus protocol as it offers greater security by requiring miners to decode complex algorithms. However, PoW is resource intensive and the difficulty of decoding makes it slow. Therefore, the Ethereum blockchain recently migrated from PoW to proof of stake (PoS), with the aim of becoming a faster — albeit less secure* network.

Layer 2: Sub-Blockchains (or software upgrades)

Layer 2 focuses on scalability and is where applications run. It acts as a third-party integration that primarily handles all transaction authentications, being built on top of the L1 and continuously communicating with it. This allows more nodes to be added to the network, which increases throughput without clogging L1 too much.

Polygon is an example of a layer 2 network created to help scale the Ethereum blockchain. It runs alongside Ethereum, grouping multiple transactions into one and posting them back to L1. This allows for faster transactions, which ultimately reduces gas fees.

Layer 3: Decentralized Applications (DApps)

Layer 3 is where the action happens. Decentralized applications (DApps) built on top of blockchains are the main attraction of Layer 3. DApps are software applications that run on a blockchain network and provide a decentralized user experience. They range from simple applications like cryptocurrency wallets to complex financial applications like decentralized exchanges, lending protocols, and prediction markets. DApps are built on top of different blockchains, and each blockchain has a different consensus model and smart contract capabilities.

Why do we need these layers?

Think of blockchain as a multi-layered cake. Each layer of the cake represents a distinct part of the blockchain. Just like a cake has its base, creamy filling, and a decorative top, each part of the blockchain has its own role. The base layer might handle the fundamentals, the creamy filling can add extra features and enhancements, and the decorative top can be the user-facing applications.

Even though each layer is different, they come together to make the whole cake — or in this case, the entire blockchain system. Just as every bite of the cake gives everyone a bit of each layer, in blockchain, all these layers work in harmony to deliver a seamless experience. And just like a cake, it's the combination of all these layers that make it so delightful. So, in the grand scheme of things, layers in the blockchain makes everything organized, efficient, and adaptable

In short, each layer serves a unique purpose and is essential to the operation of the blockchain ecosystem. Without a strong foundation in the lower layers, the upper layers would not be able to function properly. Therefore, it's crucial to have a good understanding of each layer to fully appreciate the potential of blockchain technology.

Layer 2 Solutions and Types

Introduction

We know that blockchain technology with its underlying structure of decentralized networks faces a unique challenge known as the Blockchain Trilemma: the balancing act between decentralization, security, and scalability within a blockchain infrastructure. Blockchain decentralization refers to the meaningful distribution of computing power and consensus throughout a network, while security reflects a blockchain protocol's defenses against malicious actors and network attacks. Both are considered non-negotiable to the function of a blockchain network. Also essential is scalability, which refers to a blockchain network's ability to support high transactional throughput and future growth.

Scalability is crucial because it represents the only way for blockchain networks to reasonably compete with legacy, centralized platforms with rapid settlement times. A commonly used comparison to indicate the gulf in scalability is that Bitcoin processes between 4–7 transactions per second (TPS). Visa, on the other hand, processes thousands of TPS. In order to compete with these existing systems, blockchain technology must match or exceed these high levels of scalability. There now exists an entire sub-sector of the blockchain industry that is working towards improving scalability.

Today, a whole new generation of blockchains and scaling solutions built specifically to solve this transaction-capacity problem is exponentially increasing the scaling limits of blockchain and making meaningful progress. These projects address scalability in two different ways: Layer-1 and Layer-2 scaling solutions.

In the decentralized ecosystem, a Layer-1 network refers to a blockchain, while a Layer-2 protocol (sometimes called the Data Link Layer (DLL)) is a third-party integration that can be used in conjunction with a Layer-1 blockchain. Like the second floor of a house, a Layer 2 network is a secondary protocol built on top of an existing blockchain (Layer 1). This additional layer aims to increase the transaction speed and efficiency of the network by taking transactions off the mainnet and processing them separately. Bitcoin, Litecoin, and Ethereum, for example, are Layer-1 blockchains.

Now coming to scaling solutions, Layer-1 scaling solutions augment the base layer of the blockchain protocol itself in order to improve scalability. A number of methodologies are currently being developed — and practiced — that improve the scalability of blockchain networks directly such as Consensus Protocol Improvements (Ethereum shifting to a Proof-of-Stake consensus mechanism), Sharding etc. Layer-1 solutions change the rules of the protocol directly to increase transaction capacity and speed, while accommodating more users and data. Layer-1 scaling solutions can entail, for example, increasing the amount of data contained in each block, or accelerating the rate at which blocks are confirmed, so as to increase overall network throughput.

Here in this section, we will be focussing on Layer-2 scaling solutions, which intend to **solve the issue of scalability,** operate on top of a base blockchain (Layer 1), allowing for faster transaction speeds and better scalability without compromising the underlying blockchain's security. These solutions handle transactions off-chain or in a more optimized manner, periodically batching or consolidating them to the main chain.

Now, let us picture layer-1 as a bustling highway, occasionally bogged down by excessive transactions, akin to too many cars on the road. layer-2, on the other hand, is akin to constructing an exclusive express lane positioned above the highway, designed exclusively for the swiftest vehicles. These vehicles navigate without hindrance, evading congestion and facilitating an expedited journey overall.

What is Layer-2 Scaling Solutions?

Layer-2 Scaling Solutions entails shifting a portion of a blockchain protocol's transactional burden to an adjacent system architecture, which then handles the brunt of the network's processing and only subsequently reports back to the main blockchain to finalize its results. By abstracting the majority of data processing to auxiliary architecture, the base layer blockchain becomes less congested — and ultimately more scalable. This makes it more accessible for developers to build decentralized applications (dApps) and for users to interact with them. Moreover, L2 solutions can improve the privacy and security of transactions by reducing the volume of data that requires processing on-chain.

Aim of Layer 2 Solutions: Layer 2 solutions are crafted to enhance blockchain scalability, ensuring networks can handle increased global adoption. They also focus on reducing transaction costs, making every blockchain interaction, big or small, more affordable. All these improvements aim to elevate user experience without compromising the core security principles of blockchains.

Characteristics of Layer 2 Solutions

- **Scalability:** Enhanced transaction throughput compared to traditional Layer 1 solutions.
- **Cost-Efficiency:** Drastic reduction in transaction fees, enabling micro-transactions.
- **Speed:** Quick transaction confirmation times compared to often sluggish Layer 1 confirmations.
- **Interoperability:** Some solutions offer seamless interactions across different blockchains.
- **Maintained Security:** Many solutions retain the security features of the underlying Layer 1 blockchain, ensuring data integrity and user trust.

Elements of Layer 2 Solutions

- **Smart Contracts:** Many Layer 2 solutions use smart contracts to enforce rules and validate transactions off-chain.
- **Validators or Relayers:** Entities responsible for ensuring the off-chain data is correct before it's batched to the main chain.
- **Fraud Proofs:** Mechanisms to challenge the validity of transactions, ensuring malicious actors can't manipulate the system.
- **Commit-chains:** Record a compressed version of Layer 2 data onto the main chain, ensuring data integrity and traceability.

Types of Layer 2 Scaling Solutions

Layer 2 scaling solutions can be divided into 4 categories: Channels, Roll-Ups, Plasma and Sidechains.

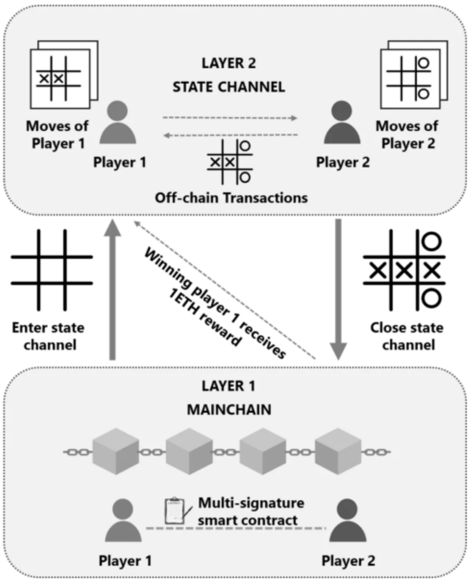
Channels

The first type of scaling solution is channels, which allow creating a peer-to-peer channel between two parties. The parties can exchange an unlimited amount of transactions off-chain (on layer 2) while only submitting two transactions to the mainchain layer 1, which are:

1. One is the first transaction that opens the connection between mainchain layer 1 and channel layer 2.
2. Another transaction stored on layer 1 is the transaction that closes the connection between layer 1 and layer 2.

By taking most of the transactions away from layer 1 (off-chain transactions), layer 2 channels improve transaction speed and reduce network congestion, transaction fees, and transaction delays. The most popular types of channels are state channels and payment channels.

(a) State Channels: State channels deal with the state update on a Blockchain network. Let's understand state channels through an example. Suppose two players want to play game tic-tac-toe on Ethereum Blockchain. For this,

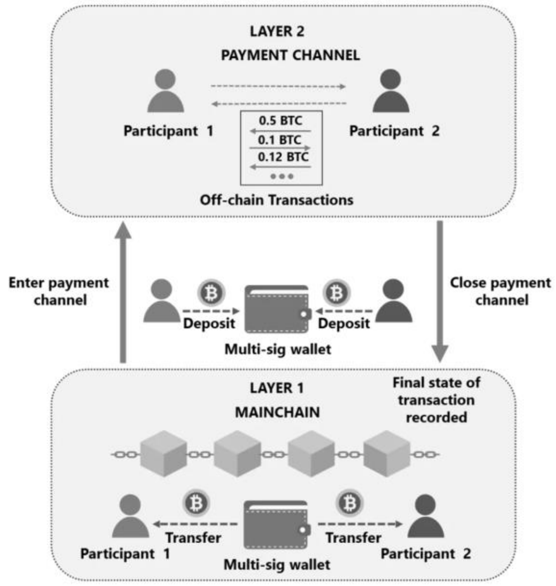


(i) First, the players create a multi-signature smart contract on the Ethereum mainchain that contains the rules of tic-tac-toe, information about the players, and prize money 1ETH for the winner.

(ii) Then, players enter the state channel and begin playing the game. Each move of the player creates an off-chain transaction that is stored on the smart contract.

(iii) When there's a winner, the players close the channel by signing the final state and submitting it to the multi-signature contract. The final state of the contract is then stored on the Ethereum mainchain, and the prize money 1ETH is transferred to the winner.

(b) Payment Channels: Payment channels are similar to state channels, but they deal with payments only. For instance, the payment channel used by Bitcoin Blockchain is the Lighting network, and the payment channel used by the Ethereum Blockchain is Raiden. The channels enable the creation of peer-to-peer payment channels between two parties. The two parties can transfer funds between themselves indefinitely without the involvement of layer 1. Eventually, when the two parties decide to finish transacting, they can close the channel. The final state of the transaction is then recorded on Blockchain layer 1.



(i) To open a payment channel like a Lighting network, the two participants must first deposit some coins in the muti-signature wallet (greater than the total amount involved in the subsequent transactions). It is the first transaction to open the channel and is recorded on Bitcoin layer 1.

(ii) After the money is deposited, both participants can make unlimited transactions without interaction with layer 1. This can happen unlimited times as long as there is sufficient balance in the wallet.

(iii) If one of the participant cheats, all funds in the channel will be sent to another participant as a penalty.

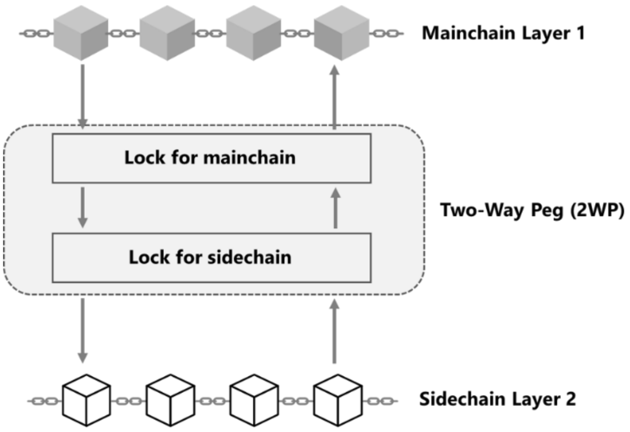
(iv) When the participants are done with transactions, they sign on the final state of the transaction with their private keys, and the channel is closed. The final state of the transaction is then recorded, and the balance is transferred to the participants on the mainchain.

Only two transactions (opening and closing of payment channel) are recorded on the main Blockchain. This significantly reduces the transaction load on the Bitcoin network.

Examples: Examples of channels are the Celer network, Connext, Kchannels, etc.

Sidechains

Sidechains are separate Blockchains that are connected to the main Blockchain through a two-way peg to help process some of the data from the main Blockchain.



Each of these chains has its own set of rules, functionalities, and purposes. Unlike other layer 2 solutions- channels, plasma, and roll-ups, which leverage the security of layer 1, sidechains are responsible for their own security. Another important point about sidechains is that they need their own nodes to validate transactions and create a block. They also have their own consensus mechanisms (such as POW, POS, Proof of Authority, DPoS, etc.) and block parameters. The block validating nodes earn the rewards for their work in a sidechain in the same manner that all other Blockchains work. Although sidechains remain independent from one another, together they form an entire ecosystem.

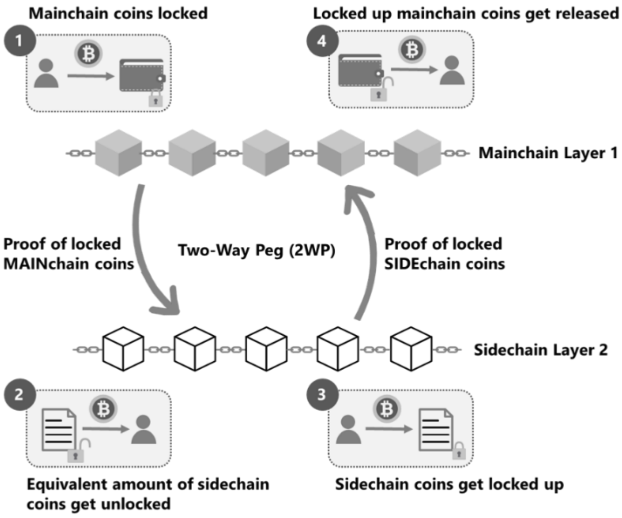
How do sidechains work?

The main job of sidechains is

- processing and validating data for the mainchain
- or adding functionality, such as running smart contracts for Blockchains that are unable to do that, like Bitcoin.

Sidechains communicate with the mainchain via a two-way peg (2WP); thus, the sidechains are also called pegged sidechains.

(i) Two-way peg (2WP): The 2WP acts as an intermediary to facilitate the transfer of assets or coins from the mainchain (layer 1) to the sidechain (layer 2) and vice versa. Under the hood, coins are not transferred; instead, they are temporarily locked on the mainchain by creating a transaction. A second transaction is generated to unlock the same amount of equivalent coins in a sidechain. The coins on the mainchain can be unlocked only when the equivalent amount of coins on the sidechain are locked again. This is done to avoid the presence of free coins on both chains and prevent a double-spending problem. 2WP system enables the interested parties to get into a transaction on the sidechain without revealing the information to the entire network.



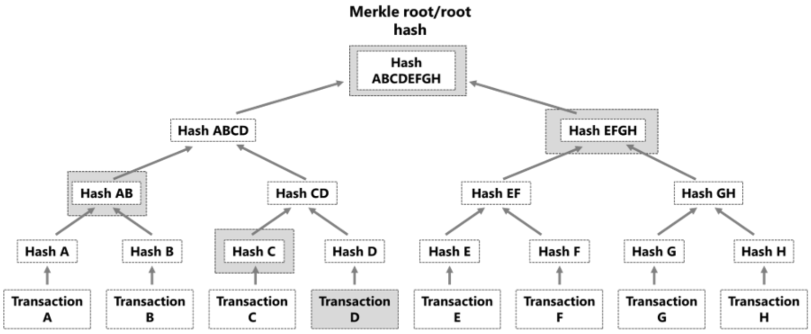
(ii) Presence of the third-party: The third-party/authority is in charge of the locking and releasing functions between the sidechains and mainchains. A transaction to lock coins is initiated. After the consensus is reached among the nodes, the signed block is submitted to the mainchain. This automatically locks the coins on the mainchain.

The trusted authority who controls the 2-way peg then issues an equivalent sum of coins in the sidechain to the transaction parties. The parties can then have a bunch of transactions within the confines of the sidechain. Once the transactions are done, the authority then verifies the transactions and releases the corresponding coins in the mainchain by unlocking the coins.

The whole sidechain construct is based on the 2-way peg and the trusted authority for maintaining the integrity of transactions between the two chains. The presence of authority can bring centralization in the network by giving it too much power.

(iii) SPV proofs: SPV (Simple Payment Verification) proof is a way to cryptographically prove that the coins are locked on the mainchain for their use on the sidechain. Rather than checking all the previous transactions, which would be slow, an SPV also proves whether the transaction initiated on the mainchain is valid and is a part of the valid block. Through SPVs, the nodes on the sidechain are not required to download the whole main Blockchain every time the verification process is needed. The Bitcoin and Ethereum Blockchains support SPVs in the form of Merkle proofs. The Merkle Proofs include the Merkle Root and the Merkle Path.

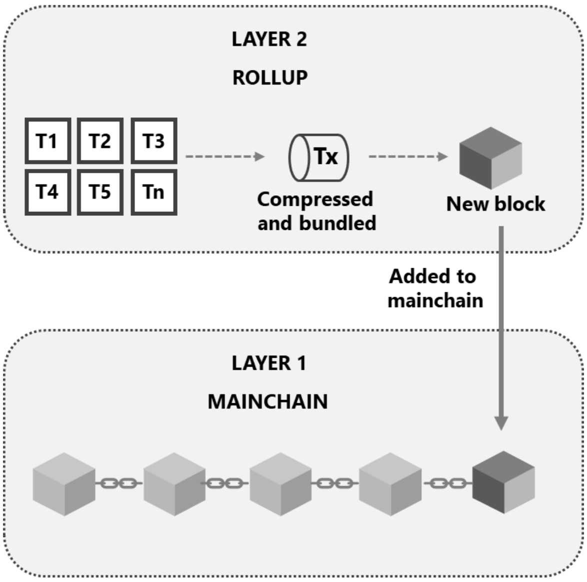
Each pair of hashed transactions is hashed together by the hash function and so on until there is one hash for the entire block, which is called Merkle Root or Root hash. On the other hand, the Merkle path is the set of hash values required for generating root hash. For instance, the Merkle path for transaction D will be the hash values Hash C, Hash AB, Hash EFGH, and Merkle root.



The nodes of the sidechain repeat the hash operation to compute the root hash value. If the root hash value obtained by the process matches with the root hash value present in SPV, it means the transaction has been initiated that locked coins on the mainchain.

Rollups

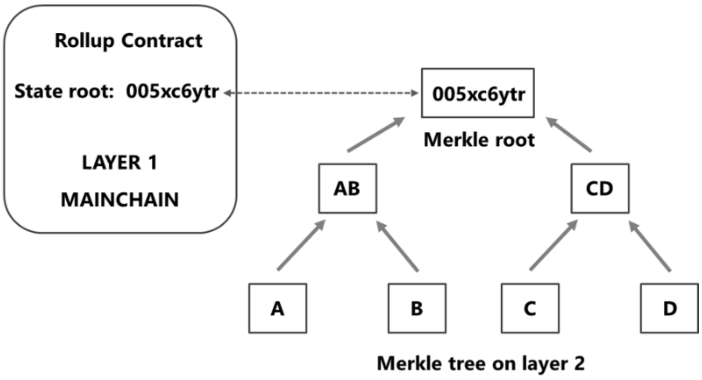
Like channels, sidechains, and plasma, rollups are also scaling solutions that use both layer 1 and layer 2 Blockchains. In rollups, the transactions initiated on the mainchain are executed on layer 2. Then the data of the executed transactions are bundled or rolled up into a single block and then posted to the mainchain layer 1. Thus the scaling solution got the name "rollups." As a result, Layer 1 is eased up as all the computation work is done off-chain on layer 2. Because of this, more transactions can be processed in parallel, making the Blockchain network scalable. Additionally, like channels and plasma, rollups also rely on the security of the mainchain.



A version of the Ethereum Virtual Machine or EVM is run inside the rollup layer. It means that any transaction possible on the Ethereum mainchain is possible to execute on the rollup. Additionally, it allows the existing Ethereum applications to migrate to rollups without writing any new code.

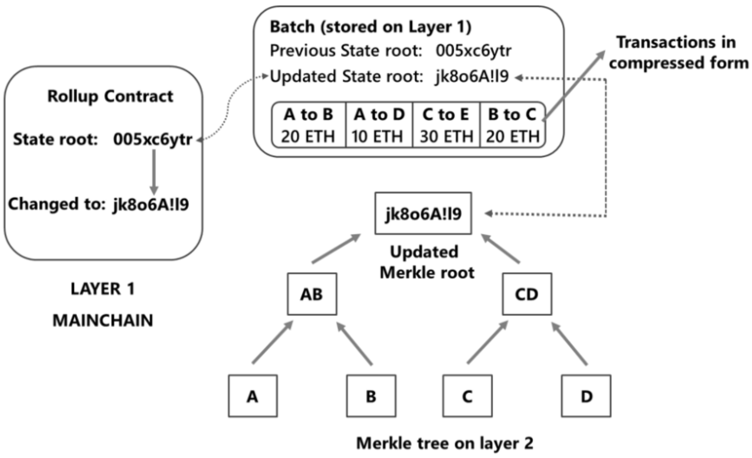
How do rollups work?

(i) There's a "rollup contract" on the mainchain that stores the state root of the rollup layer. The state root is the Merkle root of the current state of the rollup. Merkle tree is derived from all the transactions on the rollup.



(ii) When transactions happen on the rollup layer, state root (Merkle root) changes. That means the state root needs to be updated on the rollup contract on the mainchain. For this, the executed transactions are compressed, batched, and posted on the rollup contract together with updated state root. Along with the updated state root, the batch of executed transactions includes account balances of the users, addresses, contract code, etc. The entire Merkle tree is stored on the layer 2 rollup, not on the mainchain.

(iii) The batch of executed transactions is stored on the mainchain in a highly compressed form along with the previous state root (Merkle root before processing transactions) and the new state root (Merkle root after processing transactions).



(iv) The rollup contract checks that the previous state root in the batch matches its current state root; if it matches, it switches the state root to the newly updated state root.

Types of rollups: There are two types of roll-ups based on the proofs to validate that the state roots in the batches are correct. Zk roll-ups and Optimistic roll-ups

1. **Optimistic Rollups:**

A new batch of transactions is compressed, bundled, and posted to the mainchain along with the state root. The rollup contract keeps track of the entire history of state roots of each batch. At the time of posting, it is not actually validated that the transactions have been executed correctly. In other words, we are "optimistically" posting the new state root and transaction data to the rollup contract on the mainchain. If someone discovers that one batch with incorrect state root has been published to the rollup contract, they can generate a "fraud-proof." The fraud-proof incudes:

- Proof of pre-state root, or the Merkle root that should be before processing transactions
- Proof of new state root, or the Merkle root that should be after processing transactions
- Proof of the executed transactions

The fraud-proof is posted to the rollup contract on the mainchain. The rollup contract verifies the proof and compares the result to its state root. If there's a mismatch, the contract rolls back the batch and all the batches after it until it reverts to the last known valid batch. Examples of Optimistic rollups include: Optimism and Arbitrum.

A major limitation of Optimistic rollups is the longer withdrawal time. If anyone suspects a transaction to be fraudulent, they can challenge it and submit fraud-proof within the time duration of 7 days. Thus, users have to wait around one week to withdraw their assets from layer 2 rollups.

2. **Zero-Knowledge Rollups (ZK-Rollups)**

ZK-Rollups are an exciting development in the Layer 2 scaling landscape. Since the optimistic rollups work on the "innocent until proven guilty" belief, ZK rollups rely on the "don't trust, verify" belief. They leverage cryptographic proofs, specifically zk-SNARKs. The batch of bundled transactions is updated on the mainchain only when validity proof called SNARK (succinct non-interactive argument of knowledge) is submitted. SNARK is cryptographic proof that proves the new state root is the correct result of executing the batch of transactions in the ZK-rollup layer. The validity proof is posted to the rollup contract, so anyone can use it to verify transactions in a particular batch on the rollup layer.

SNARKs are also called Zero-Knowledge Proofs or ZK Proofs because they allow anyone to verify that the transactions are valid without revealing any information about the transaction. In other words, anyone can verify that the data existed, even if they don't have access to the data itself.

Example: A zero-knowledge proof is a method of establishing the truth of a proposition without exposing it. ZK rollups are like an express lane at a toll booth. Imagine if every car had to stop at the toll booth and the drive has to show the driver license and pay individually, the process would be time-consuming, and the queue would be long. Now, on the express lane, the system instantly detects the car plate for record-keeping purposes, eliminating the need for individual payments on site. The system efficiently bundles all the pending payments within a given period (say, in an hour) into batches. And then, it settles each payment batch with the bank by deducting the corresponding amount from the car owners' accounts. This process greatly reduces the transaction turnaround time on the lane, leading to a swift and seamless flow of traffic.

Examples of ZK rollups include: Loopring, Hermez and Starkware

Plasma

Plasma is another layer 2 scaling solution. Plasma leverages smart contracts and Merkle trees to create an unlimited number of child chains copies of the parent Blockchain mainly (Ethereum Blockchain). Offloading transactions from the mainchain (layer 1) into child chains (layer 2) allows fast and cheap transactions. Like sidechains, each child chain is treated as a separate blockchain with its own consensus mechanism, nodes, block size, and block time.

Like channels, plasma leverages the security of the mainchain. The mainchain and child chains are tied together through 'smart contracts' that contain the rules guiding each child chain. The contracts act as the bridge that lets the participants move digital assets/coins between the mainchain and the child chains. Initially, all transactions have to be created on the mainchain.

If any suspicion or fraud is detected in the plasma child chains, plasma users can exit the plasma chain and move to the mainchain.

How does Plasma work?

(i) The child chain operator lays down the rules in which the child chain will operate.

(ii) Processed transactions stay at the plasma chains. But the block headers (containing Merkle roots) of each block of the plasma chains are submitted and recorded in the blocks of the mainchain. This reduces the mainchain network congestion and thus, allowing tens of thousands of transactions to be processed simultaneously in plasma chains.

(iii) The data on child chains is validated using "fraud proofs." Fraud proofs are a mechanism by which anyone can determine if the data is invalid using Merkle proofs. For example, when fraud occurs in a plasma chain, whether it is a double-spending case or one cash out more than they have in all accounts, anyone can provide a fraud proof to prove the transaction is invalid. If the transaction is proven fraud, it will be rolled back.

Apart from the above mentioned four, there are:

1. **Bitcoin Layer 2 Scaling Solutions**

Bitcoin Lightning Network

The Bitcoin Lightning Network is one of the best-known layer 2 solutions for Bitcoin. Like other layer 2 solutions, it takes transaction bundles from the main chain to be dealt with off-chain before transferring that information back. The Lightning Network also brings smart contracts to Bitcoin, which is a big improvement to the network overall. Bitcoin lightning network promises the following benefits: instant payment, scalability, low cost and cross blockchains swaps.

As the name suggests, this layer 2 solution will introduce lightning-fast payments on the Bitcoin blockchain, as fast as milliseconds. The current Bitcoin average transaction time is about 10 minutes. However, it can vary largely if the network is congested. The Bitcoin lightning network also claims that it is capable of processing millions to billions of TPS, which is many times higher than legacy payment providers like Visa. By settling transactions off-chain as layer 2 solution, fees are greatly reduced, allowing for instant micropayments.

Finally, cross-chain atomic swaps can occur off-chain as long as the chains support the same cryptographic hash function. Bitcoin uses the SHA-256 cryptographic has function in its algorithm.

2. **Ethereum Layer 2 Scaling Solutions**

1. Starkware

Starkware is a Ethereum layer 2 scaling solution provider. It has three products: StarkNet, StarkEx and Cairo.

- **StarkNet** is a permissionless decentralized ZK-rollup layer 2 solution for the Ethereum blockchain. Developers are now able to deploy their smart contracts permissionlessly on StarkNet's testnet. The main advantage is the ability for dApps to achieve unlimited scale, while still benefitting from Ethereum's composability and security. More information on StarkNet can be found here.
- **StarkEx** is a layer 2 scalability engine that has been proven and deployed on mainnet since June 2020. It has been deployed in various use cases, and notable customers are DeversiFi, Immutable and dYdX. The main benefits of StarkEx is trustless scalability using ZK-STARK technology, ability to design self-custodial dApps, and robust and secure scaling solution for a wide range of uses. More information on StarkEx can be found here.
- **Cairo** is Starkware's Turing-complete language behind both StarkNet and StarkEx. It allows for the scaling of dApps using STARKs.

2. Optimism

Optimistic Ethereum is an Ethereum Virtual Machine (EVM) compatible optimistic rollup chain. The main benefits of deployed on Optimism is that it is fast, simple and secure. Users can move assets in and out of the network using Optimistic Ethereum Gateway, and projects looking to deploy can submit a form to get whitelisted by Optimism. Projects that meet their launch criteria will be approved within 2 weeks. On July 2021, Uniswap V3 announced its alpha launch on Optimistic Ethereum mainnet.

3. Arbitrum

Arbitrum is a layer 2 solution designed to boost the speed and scalability of Ethereum smart contracts, while adding additional privacy features. The layer 2 platform allows developers to run unmodified EVM contracts and transactions on layer 2, without compromising on layer 1 security. Arbitrum positions itself as the ideal scaling solution for DeFi apps, with the ability to use Arbitrum rollup to scale any Ethereum contract. Offchain Labs, the company behind Arbitrum, rolled out Arbitrum One, their Ethereum mainnet beta on Aug. 31, 2021, and announced $120 in series B funding, valuing the firm at $1.2 billion.

4. Polygon

Polygon is another layer-two solution for Ethereum, leveraging different technologies to enhance Ethereum's scalability:

- Polygon PoS: EVM-compatible sidechain.
- Polygon Miden: a zk-rollup based on Starkware.
- Polygon Hermez: an open-source zero-knowledge rollup.
- Polygon Avail: a standalone layer-2 chain with a data availability focus.
- Polygon Zero: a zk-rollup chain.
- Polygon Nightfall: a privacy-focused rollup chain.

In July 2022, Polygon also announced the launch of Polygon zkEVM, a zero-knowledge version of the Ethereum Virtual Machine. Its aim is to reduce transaction costs and improve Ethereum's scalability before the switch to proof-of-stake.

Other Ethereum Layer 2 Scaling Solutions include: Aztec, POA Network, Loopring, SKALE Network, ZKSync etc.

Each of these Layer 2 solutions provides unique advantages and caters to specific needs within the blockchain ecosystem. The choice between them often depends on the specific requirements of a project or platform.

Advantages of Layer 2 Solutions

Layer 2 scaling solutions offer several advantages over traditional on-chain scaling. These advantages include:

Increased Scalability: Layer 2 scaling solutions can significantly increase the transaction throughput of a blockchain. This is achieved by processing transactions off-chain and settling them on the main blockchain. This increased scalability allows for more efficient and cost-effective use of the blockchain.

Lower Fees: With Layer 2 scaling solutions, transaction fees can be significantly lower than on-chain transactions. This is because transactions are processed off-chain and settled in batches on the main blockchain, reducing the overall cost of transactions.

Faster Transaction Times: Layer 2 scaling solutions can significantly reduce transaction times. This is because transactions are processed off-chain, allowing for faster confirmation times and reducing the overall time required for transaction settlement.

Enhanced Privacy: Layer 2 scaling solutions can enhance privacy by allowing for off-chain transactions that are not recorded on the main blockchain. This can be useful for applications that require increased privacy and confidentiality, such as financial transactions.

Improved Security: Layer 2 scaling solutions can improve security by reducing the load on the main blockchain, which can reduce the risk of attacks such as double-spending attacks. Additionally, Layer 2 scaling solutions can enable more efficient and secure smart contract execution.

Challenges and Risks of Layer 2 Solutions

While Layer 2 scaling solutions offer several advantages over traditional on-chain scaling, they also come with their own set of challenges and risks. These challenges include:

Centralization: Some Layer 2 scaling solutions may require a central authority or operator to function, which can introduce centralization risks.

Complexity: Layer 2 scaling solutions can be complex and difficult to implement, requiring significant development resources and expertise.

Security Risks: Layer 2 scaling solutions can introduce new security risks, such as the risk of malicious actors exploiting vulnerabilities in the off-chain network or the risk of faulty smart contract execution.

Interoperability: Interoperability between different Layer 2 scaling solutions can be a challenge, as different solutions may use different protocols and technologies.

User Experience: Layer 2 scaling solutions can introduce additional complexity and friction for users, such as the need to transfer funds between on-chain and off-chain networks.

Maintenance and Upgrades: L2 solutions may require continuous maintenance and upgrades to remain secure and effective, which can be a challenge.

Use Cases of Layer 2 Solutions

Layer 2 scaling solutions can enable a wide range of use cases for decentralized applications. Some of the most promising use cases include:

Decentralized Finance (DeFi): Layer 2 scaling solutions can significantly increase the transaction throughput of DeFi applications, making them more accessible and affordable for users. Additionally, Layer 2 scaling solutions can enhance the privacy and security of DeFi transactions.

Non-Fungible Tokens (NFTs): Layer 2 scaling solutions can enable the creation and trading of NFTs at a much lower cost and with much faster transaction times than on-chain solutions. This can unlock new use cases for NFTs, such as in gaming and digital collectibles.

Micropayments: Layer 2 scaling solutions can enable the processing of micropayments at a much lower cost than on-chain solutions, making them useful for applications such as content monetization and pay-per-use services.

Supply Chain Management: Layer 2 scaling solutions can enable more efficient and secure supply chain management by enabling the processing of transactions off-chain, reducing costs, and increasing scalability.

Gaming: Layer 2 scaling solutions can significantly increase the transaction throughput of gaming applications, enabling real-time gameplay and reducing the cost of in-game transactions.

As Layer 2 scaling solutions continue to develop and mature, we can expect to see many more exciting use cases emerge.

Layer-1 VS layer-2 Scaling Solutions

Brief description of Layer 1 Scaling Solutions

On-chain scaling solutions, sometimes referred to as layer-1 scaling solutions, are techniques used to boost the efficiency and capacity of the underlying blockchain network. These solutions concentrate on enhancing the blockchain's basic layer, which comprises the fundamental protocol and consensus mechanism. layer-1 solutions attempt to increase the network's capacity, speed, and overall performance by strengthening the base layer.

Segregated Witness (SegWit): Segregated Witness (SegWit) was introduced in August 2017 as a soft fork to enhance Bitcoin's efficiency by splitting transactions into two parts and removing unnecessary information. This removed information refers to the transaction signatures, also known as witness data, which are a part of Bitcoin transactions.

Increasing the Block Size: In theory, this enhances transaction capacity, however, issues arise when trying to solve scalability by enlarging the block size. As the block size in MB increases, challenges emerge from both theoretical and practical standpoints.As the continual expansion inflates block sizes, making transfer challenging due to intra-blockchain bandwidth limitations. These larger blocks trigger centralization concerns. As individual users struggle to efficiently propagate blocks and verify numerous transactions within a set timeframe, this situation may ultimately lead to a scenario where only a centralized entity can function as a full node.

Block Compression: TXID: Txilm, protocol based on BIP-152 employs a unique approach to enhance the efficiency of transactions within the blockchain. BIP-152 compresses transactions in each block to save the network's bandwidth. It is achieved by utilizing shortened codes to represent individual transactions. This technique not only conserves space but also improves the overall efficiency of data storage within blocks. The core idea is to reduce the amount of data required for transmitting transactions across the network.

Storage Scheme Optimization - CUB: Consensus-unit based (CUB) introduces an innovative strategy by grouping nodes into Consensus Units. Each unit is responsible for storing specific block data segments. To better understand, one may think of 'grouping nodes' as people and 'Consensus Units' as teams, where each unit is responsible for storing specific parts of the blockchain data puzzle sections. Each node in the consensus unit or team has a specific section of the blockchain data puzzle to work on. Instead of everyone working on the same blockchain puzzle together, which slows down the process, the blockchain puzzle gets divided into smaller parts and each person or node is assigned what to work on.CUB optimizes the way data is stored and accessed, which helps reduce storage costs and makes the blockchain system work faster and more effectively.

Comparison of both Layer-1 and layer-2 Scaling Solutions

Despite layer-1 scaling solutions like making consensus protocol changes and sharding attempting to make blockchains like Bitcoin and Ethereum more scalable, they are still a work in progress with multiple projects currently working on bringing to market user-friendly solutions. Both methods, however, are trying to solve the "scalability trilemma," a term coined by Ethereum founder Vitalik Buterin that alludes to the unsolved problem in distributed ledger technology-based networks where every node that validates transactions cannot simultaneously achieve decentralization, security and scalability. While the jury is still out on how successful these could be, layer-2 solutions are already facilitating transaction speeds and fees that are ideal for scaling the blockchain ecosystem so as to unleash the full potential of this path-breaking technology. Numerous DApps are already employing these solutions to provide previously impossible experiences in the spheres of gaming, Decentralized Finance (DeFi) and the Metaverse, in addition to overhauling traditional sectors like finance, corporate governance, auditing and many more.

Despite the advantages, the way these blockchains validate transactions needs to be evaluated based on the use case, and the possibility of validators on the layer-2 blockchain committing fraud needs to be analysed carefully. That said, new layer-2 scaling solutions are being developed constantly and this space will continue to attract a lot of attention, plaudits and criticism.

	Layer 1 Scaling Solutions	Layer 2 Scaling Solutions
Concepts	Enhances base blockchain layer for more TPS	Builds on Layer 1, processes off-chain for increased through-put.
Advantages	Security, decentralization, direct innovation access.	High scalability, fast transactions, reduced fees.
Disadvantages	Upgrade complexity, slow development, centralization risk.	Security reliance, interoperability complexity, centralization potential.
Implementation	Fundamental protocol changes.	Techniques like payment channels, rollups, sidechains.
Security& Decentralization	Highly secure, decentralized due to consensus.	Depends on underlying Layer 1 security.
Innovation flexibility	Direct access to the base layer for features.	Enhancements built on existing blockchain.
Self-contained	Implementation doesn't rely on external layers.	Utilizes infrastructure.
Scalability focus	Improving base blockchain capacity.	Increasing transaction throughput by off-chain processing.
Transaction speed	May vary based on protocol changes.	Near-instantaneous transaction confirmation and settlement.
Transaction cost	Can be impacted by consensus changes.	Reduced fees due to decreased main chain congestion.
Upgrade challenges	Complex, community consensus needed.	Complex development and interactions, but not as fundamental as Layer 1
Interoperability	Generally, less complex, less reliant on other layers.	Interaction between Layer 2 solutions or with Layer 1 can be intricate.
Centralization risk	Rapid changes can lead to centralization risk.	Some solutions might require intermediaries, impacting decentralization.

The Future of Layer 2 Solutions

The future of Layer-2 blockchain solutions is intertwined with the development and advancement of Layer-1 networks, such as Ethereum or Bitcoin. As Layer-1 blockchains evolve and improve in scalability, Layer-2 solutions will also reap the benefits, inheriting all core features and improvements of their underlying Layer-1 blockchains.

Demand for blockchain technology is increasing rapidly, as is the total value locked (TVL) in Layer-2 solutions. As this trend continues, Layer-2 networks will become the de facto choice for users seeking to benefit from faster, cheaper transactions. Every day, new decentralized finance (DeFi) projects are being launched on Layer-2 blockchains, underlining their growing importance and relevance in the blockchain space.

Looking ahead, the future of Layer-2 solutions is not just about scalability and cost reduction. Privacy and security of users' data will also become central themes. Zero-knowledge networks, such as Starknet and zkEVM, are gaining popularity due to their ability to protect user data while still providing the benefits of blockchain transparency. In these networks, transactions are verified without revealing any details about the transaction itself, thereby enhancing user privacy. This privacy feature is becoming more and more important as the issue of data protection continues to gain prominence in the digital world.

Summing Up

Layer-2 solutions will continue to evolve and adapt, driven by the increasing demand for scalable, secure, and privacy-preserving blockchain technology. As Layer-1 networks like Ethereum continue to grow and mature, so too will Layer-2 solutions, bringing us ever closer to the vision of a truly scalable, secure, and user-friendly blockchain ecosystem.

References

https://tatianarevoredo.medium.com/blockchain-layers-e2240baa649a

https://crypto.com/university/what-are-layer-2-scaling-solutions

https://coinmarketcap.com/academy/article/what-are-cryptocurrency-layer-2-scaling-solutions

https://dailycoin.com/types-of-layer-2-comparing-different-ethereum-scaling-solutions/

https://www.gemini.com/cryptopedia/blockchain-layer-2-network-layer-1-network#section-layer-1-scaling-solutions

https://www.cronj.com/blog/layer-2-blockchain-types-advantages-challenges-use-cases/

https://medium.com/techskill-brew/layer-2-blockchain-scaling-solutions-channels-sidechains-rollups-and-plasma-part-16-79819e058ef6

https://www.ccn.com/education/layer-1-and-layer-2-blockchain-scaling-solutions/