crypto.com

Scaling Blockchains: Layer 1 vs Layer 2

An Overview of Scaling Solutions

June 2022

Research and Insights

Research Analyst
Panagiotis Simatis

Research Manager
Kevin Wang

Published on 27 Jun 2022

RESEARCH DISCLAIMER

The information in this report is provided as general commentary by Crypto.com and its affiliates, and does not constitute any financial, investment, legal, tax, or any other advice. This report is not intended to offer or recommend any access to products and/or services. The views expressed herein are based solely on information available publicly, internal data, or information from other reliable sources believed to be true.

While we endeavour to publish and maintain accurate information, we do not guarantee the accuracy, completeness, or usefulness of any information in this report nor do we adopt nor endorse, nor are we responsible for, the accuracy or reliability of any information submitted by other parties. This report includes projections, forecasts, and other predictive statements that represent Crypto.com's assumptions and expectations in light of currently available information. Such projections and forecasts are made based on industry trends, circumstances, and factors involving risks, variables, and uncertainties. Opinions expressed herein are our current opinions as of the date appearing in this report only.

No representations or warranties have been made to the recipients as to the accuracy or completeness of the information, statements, opinions, or matters (express or implied) arising out of, contained in, or derived from this report or any omission from this document. All liability for any loss or damage of whatsoever kind (whether foreseeable or not) that may arise from any person acting on any information and opinions contained in this report or any information made available in connection with any further enquiries, notwithstanding any negligence, default, or lack of care, is disclaimed.

This report is not meant for public distribution. Reproduction or dissemination, directly or indirectly, of research data and reports of Crypto.com in any form is prohibited except with the written permission of Crypto.com. This report is not directed or intended for distribution to, or use by, any person or entity who is a citizen or resident of, or located in a jurisdiction, where such distribution or use would be contrary to applicable law or that would subject Crypto.com and/or its affiliates to any registration or licensing requirement.

The brands and the logos appearing in this report are registered trademarks of their respective owners.

Contents

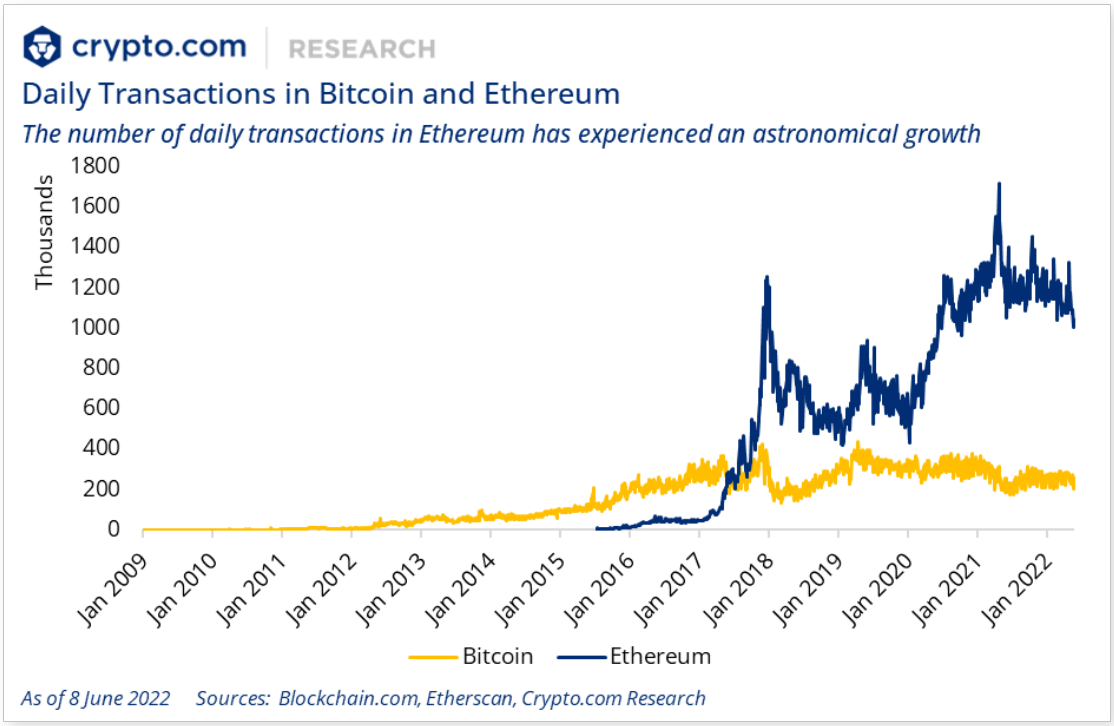
Executive Summary

Scaling solutions facilitate swift transactions in blockchains. Depending on their focus, **they are categorised as Layer 1 or Layer 2**.

- Layer 1 solutions enhance scalability by modifying the base protocol. These modifications include the parameters and data structure of the blockchain:
  - **Block Reparameterisation:** It refers to **optimisations in the block's data structure**. The goal is to increase the throughput by packing more transactions into a block.
  - **Sharding: The blockchain is divided into smaller networks called shards**. Each shard is responsible for the transactions within its partition. While sharding provides benefits, it significantly increases the blockchain's complexity.
  - **Consensus Mechanisms:** The difficulty of scaling blockchains is mainly due to their consensus since it **requires all participants in the network to agree on which transactions are valid**. Therefore, alternatives to Bitcoin's PoW emerged in an attempt to solve the problem.
  - **Directed Acyclic Graph (DAG): DAG reshapes the blockchain to a tree-like structure.** Thus, multiple processes may run on different branches simultaneously.
- Layer 2 solutions enhance scalability by offloading transactions off the main chain:
  - **Payment Channels:** Peer-to-peer networks where participants can transfer funds without publishing all transactions to the main blockchain. **The settlement finality in the Lightning Network takes milliseconds, while Bitcoin's confirmation time is over ten minutes**.
  - **Rollups:** Rollups aggregate transactions inside a smart contract. **Rollups offer scaling benefits up to 100 times and even higher if combined with sharding.** They come in two categories, Optimistic Rollup and ZK Rollup.
    - **Optimistic Rollup** assumes that transactions are valid unless **fraud proof** is submitted.
    - **ZK Rollup** makes no such assumption and generates a validity proof for every bundle of transactions.
  - **Sidechains:** Blockchains that exist alongside a mainchain and use their own mechanisms. **Polygon is a suite of sidechain protocols which can potentially handle 65,000 TPS.**

1. Introduction

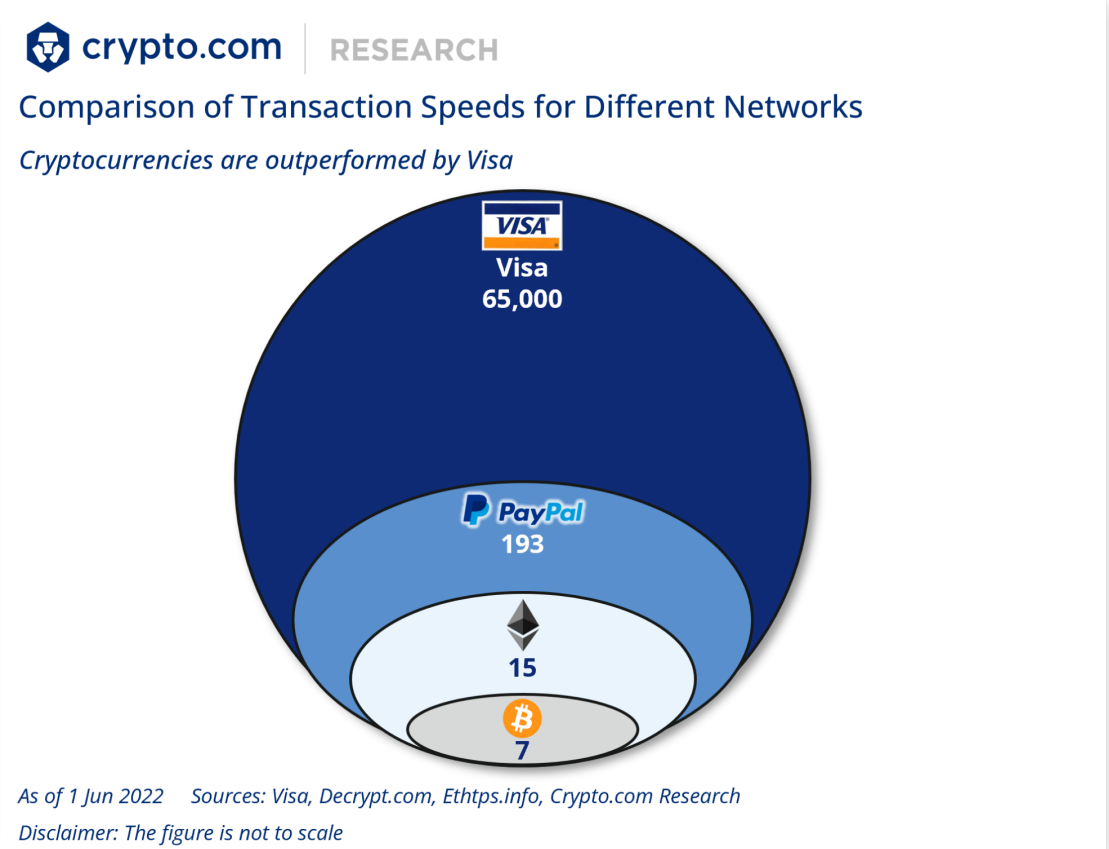
In 2010, the first recorded crypto transaction took place. It was a purchase of two pizzas for 10,000 Bitcoin (i.e., US$150M per pizza in today's value). Less than two decades later, cryptocurrencies have experienced a meteoric rise in popularity. When Satoshi Nakamoto published the Bitcoin paper, nobody expected its user base to grow into the millions, including the wealthiest man on the planet and governments.



Over 250 thousand Bitcoin transactions occur daily. In addition, Ethereum's smart contracts gave birth to billion-dollar markets, such as NFTs. This dramatic increase in users and transactions is testing the limits of blockchain technology. **It is thus mandatory that blockchains scale and satisfy the increasing demand.**

However, there is still a roadblock for cryptos to overcome in order to achieve mass adoption like Visa and PayPal, not only for merchant acceptance but also on the technical side. Currently, centralised financial services outperform cryptocurrencies in terms of transaction speed.

For example, Visa boasts up to 65,000 transactions per second (TPS), while Bitcoin handles around seven.



The blockchain scalability problem is widely discussed in the industry, and this report focuses on surveying scaling solutions in the blockchain space. The task at hand is not straightforward for several reasons.

Firstly, blockchain technology is highly dynamic, with new ideas published around the clock and older solutions thrown out of the window. Secondly, there is occasionally no standardised terminology. The lack of rigorous definitions is a natural consequence of rapid development, and it is occasionally confusing when scientific and marketing jargon intertwine.

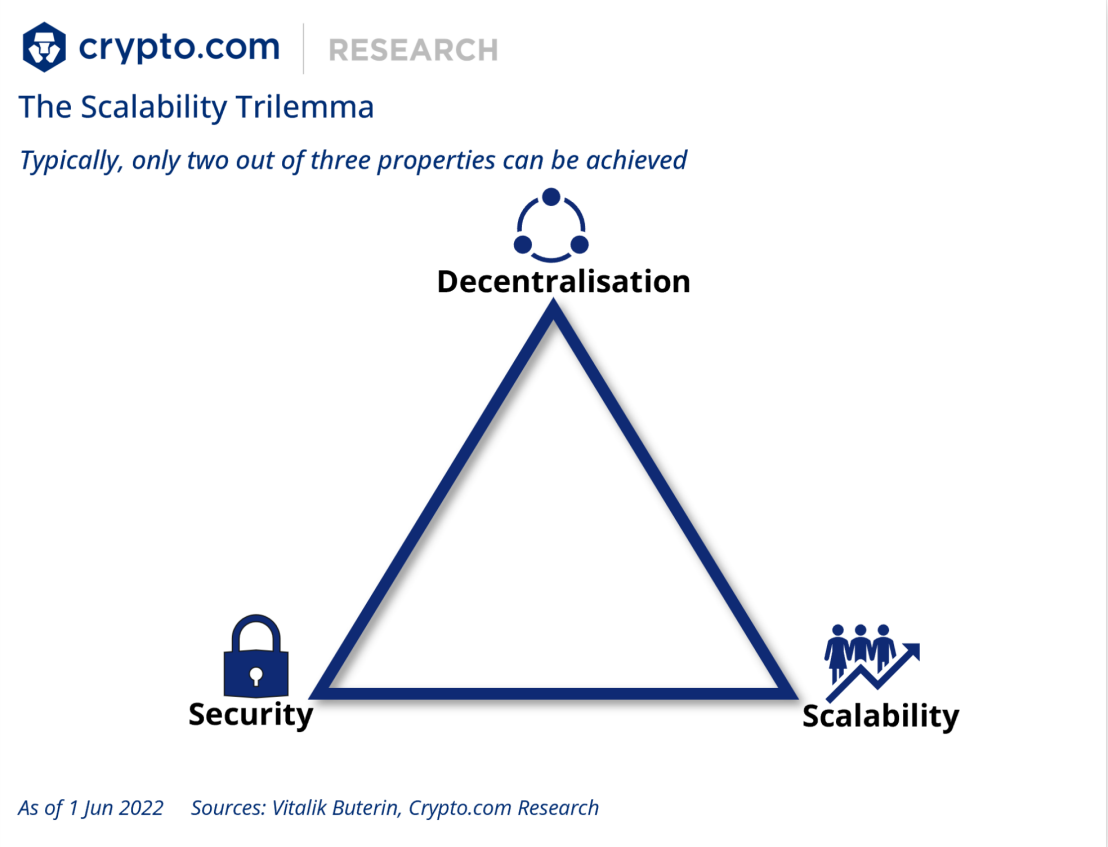
1.1 Why Is Efficiency Not Trivial?

Simply put, **scalability** **is the ability of a system to process growing volumes of work gracefully by adding more resources**. In a perfect world, blockchains would scale indefinitely and efficiently accommodate any number of transactions without adverse side effects.

However, it's difficult for a blockchain system to purely increase throughput while keeping the same level of decentralisation and security (i.e., the other two key blockchain features). Enter the so-called **Scalability Trilemma**, which illustrates

that **a blockchain system has to make a trade-off between the fundamental properties of scalability, decentralisation, and security, as only two can be achieved, but never all three.**

Vitalik Buterin, the co-founder of Ethereum, was the first to coin the term 'scalability trilemma'. Note that the trilemma is more of a rule of thumb than hard mathematical proof, and some developers believe solutions hitting all three targets are possible.



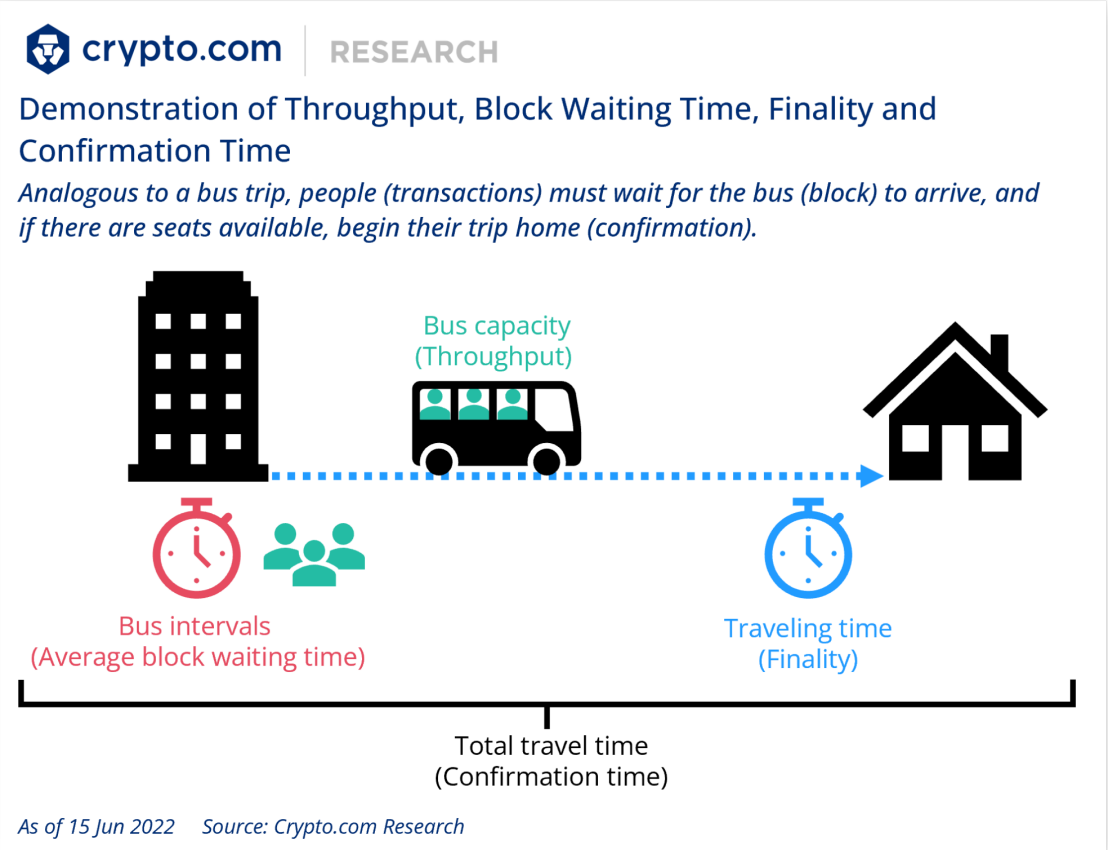
Throughout this report, **scalability refers to the ability of a blockchain to maintain efficiency without undermining security and decentralisation due to the number of transactions or participants.**

Various metrics measure the scalability of a system:

- **Throughput** is the amount of information processed in a given time interval measured in transactions per second (TPS).
- **Finality** is the guarantee that a transaction is accepted by the protocol (i.e., it will not be reversed). It requires a fixed waiting time (e.g., in Bitcoin, six block confirmations are required to secure a transaction).
- **Average block waiting time** is the time needed to create a new block (e.g., ten minutes for Bitcoin).

- **Confirmation time** is the total time elapsed from a transaction's occurrence until it is recorded in a confirmed block.

Please note that none of these metrics suffice by themselves. For example, a protocol with 100,000 TPS is worthless if its confirmation time is a week.

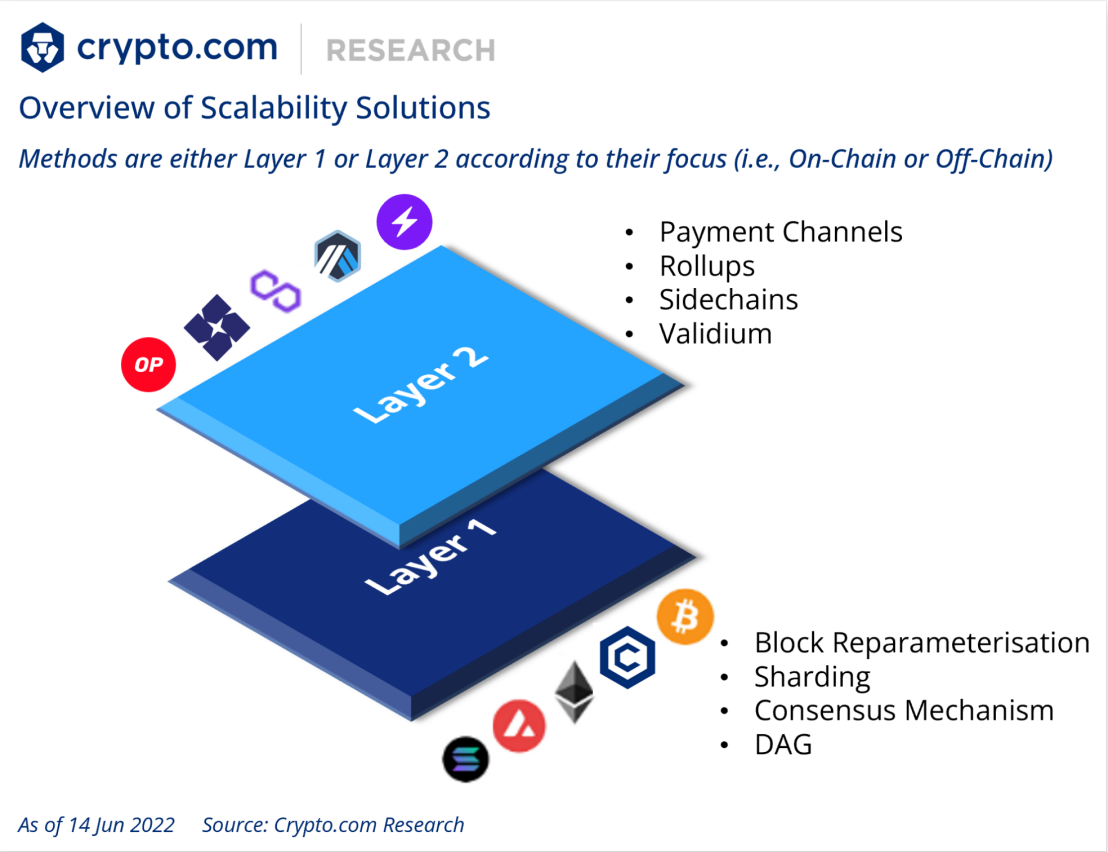


Scalability is crucial for a blockchain to enjoy widespread adoption. In layman's terms, nobody wants to wait ten minutes or even more to confirm the transaction of buying a coffee via Bitcoin. Beyond improving user experience, **scalability enhances accessibility**. It breaks down barriers and opens up blockchain technology to the public, bringing new use cases and ideas.

Blockchain developers need to strike a balance of secure, decentralised, and scalable protocols. The problem is not trivial, and many different solutions have been proposed. So far, none of the developed methods have been declared a winner, and **the race for scalable blockchains is ongoing**. Fortunately, many great minds are working on scaling blockchains, delivering significant results.

1.2 Solutions of Scalability

Scalability solutions come in a plethora of shapes but are broadly categorised as Layer 1 or Layer 2 solutions, depending on whether they focus on or off the blockchain. **Layer 1 solutions focus on upgrading the blockchain itself, while Layer 2 solutions construct a third-party layer (network) on top of the main blockchain to improve its features.** For example, the Lightning Network is a Layer 2 solution built on top of Bitcoin, which is considered Layer 1.



Layer 1 solutions enhance scalability by modifying the base protocol. These modifications include the parameters and data structure of the blockchain, such as block capacity and block creation rate. In addition, they might even facilitate or enable Layer 2 solutions.

However, **Layer 1 upgrades are blockchain-specific**. Namely, an upgrade in Bitcoin does not necessarily apply to Ethereum. Furthermore, they are often controversial and spark debates in the community, which **may lead to a hard fork of the network**.

Layer 2 solutions aim at transferring the transaction burden off the main blockchain. Essentially, they reduce congestion by enabling the delegation of data. **The two layers communicate only when necessary** (e.g., finalising multiple transactions).

Layer 2 systems remain dependent on the main blockchain. Nevertheless, they are general methodologies which can be applied to any blockchain satisfying their prerequisites (e.g., support for smart contracts). Layer 2 solutions are an ever-growing field delivering promising results, reaching US$4B of total value locked (TVL) solely in Ethereum.

The following chapters delve into popular scalability methodologies both on-chain and off-chain. We categorise them into distinctive groups providing a general taxonomy to minimise overlap between the methods. Then, we present their strengths and shortcomings while also linking them to real-life blockchain uses and upcoming implementations.

Taxonomy of Scalability Solutions

crypto.com | RESEARCH

Category	Sub-category	Examples
Layer 1: On-Chain	Block Reparameterisation	SegWit, Taproot, Bitcoin-Cash, LTCP, Txilm
	Sharding	Elastico, Ethereum, Near, Monoxide
	Consensus Mechanism	Nakamoto Consensus (PoW), Proof of X (PoS) Classical Consensus (pBFT), Leaderless Consensus (Avalanche)
	DAG	Avalanche, Fantom, IOTA
Layer 2: Off-Chain	Payment/State Channel	Lightning Network, Raiden Network, Hydra
	Sidechain	Plasma, Polygon
	Rollup	Optimism, Arbitrum One, Boba Network, Loopring, zkSync, dYdX
	Validium	Immutable X, DeversiFi

As of 1 Jun 2022 *Sources: Qiheng Zhou et al., Vitalik Buterin, Crypto.com Research*

2. On-Chain (Layer 1) Solutions

Layer 1 solutions concentrate on the blockchain's technical/architecture design, including the data structure, network architecture, and consensus algorithms. They essentially modify the base protocol to improve scalability from the ground up. Furthermore, **Layer 1 optimisations may lay the foundation for future Layer 2 solutions**.

While Layer 1 solutions provide significant benefits, their implementation is not always straightforward. **On-chain optimisations often require radical changes to the structure** of the network. In addition to the challenging implementation, **they may lead to community disagreements and hard forks.**

Currently, the Layer 1 solutions discussed the most include **block reparameterisation**, **sharding**, **consensus mechanisms**, and alternative data structures (i.e., **DAG**).

Comparison Table of Layer 1 Solutions crypto.com | RESEARCH

Solution	Example	Throughput	Finality
Block Reparameterisation	SegWit	Minor TPS improvement	Same as Bitcoin
Sharding	Polkadot	~1,000 TPS without without parachains; ~1,000,000 TPS with parachains	12-60 seconds
Consensus Mechanism	DPoS (used in EOS)	3,996 TPS	3 seconds
DAG	Avalanche	4,500+ TPS	1 second

As of 1 Jun 2022 *Sources: Crypto.com Research*

2.1 Block Reparameterisation

Block Reparameterisation refers to optimisations on the block's data structure. The goal is to increase the throughput by packing more transactions into a block. The methodology used varies according to the project.

For example, Bitcoin Cash increased the block size to 32MB to fit more transactions than Bitcoin, which limits blocks to 1MB. Other techniques (e.g., LTCP, Txilm) reduce the storage overhead by compressing data. This section introduces some prominent solutions that achieve scalability by tweaking the block layout.

SegWit

Segregated Witness (SegWit) is a protocol upgrade of Bitcoin defined in BIP141, which went live in 2017. Its original goal was to facilitate scalability and improve security by preventing transaction malleability. SegWit's soft fork slimmed down the transaction data and improved Bitcoin's throughput.

SegWit reduces the size of a transaction by splitting it into two sections. The block maintains the sender and receiver data (e.g., their addresses). The digital signatures that verify the ownership and availability of funds, also known as the **witness data**, are removed from the original portion but remain in the blockchain as a separate structure.

Removing the witness data reduces the transaction size, thus making it possible to fit more transactions in a block without increasing capacity. SegWit increased the number of transactions in a full block from roughly 1,650 to around 2,700.

Nevertheless, **SegWit was a highly contentious upgrade**. In response to SegWit, several users initiated hard forks (e.g., Bitcoin Cash). To this day, SegWit has not been accepted by the entire Bitcoin community, even though its adoption has risen significantly.

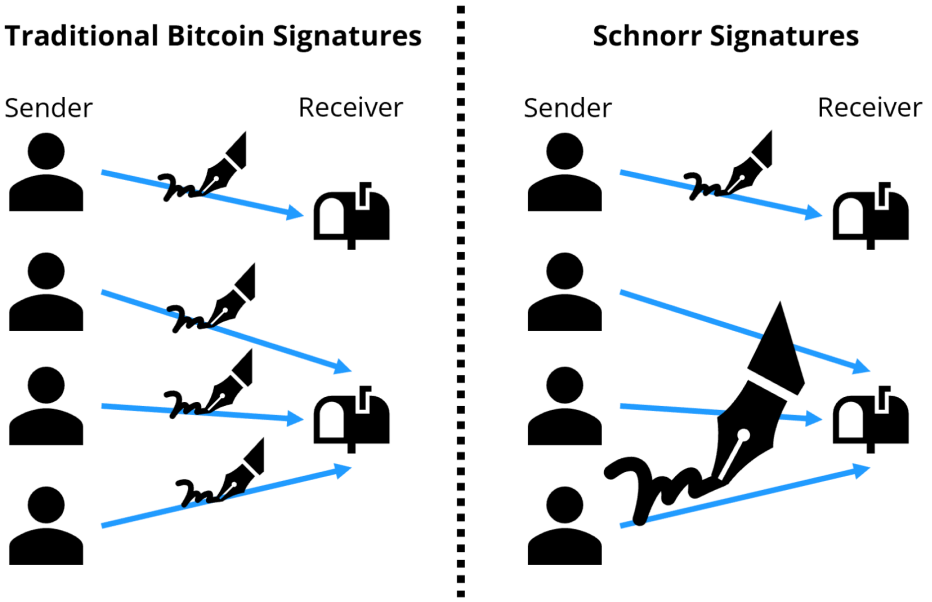
Taproot

Taproot, released in 2021, is the most significant upgrade to Bitcoin since SegWit. It is a soft fork consisting of multiple BIPs (i.e., BIP340, BIP341, BIP342) aiming to improve the blockchain's privacy and efficiency. **A major update is the implementation of Schnorr signatures, which facilitate efficient and secure validation of transactions.** Schnorr signatures reduce the transaction size by aggregating multiple signatures (used in multi-signature transactions) into one. The aggregation of signatures also allows complex transactions to be verified quickly in batches rather than individually as a single transaction.

crypto.com | RESEARCH

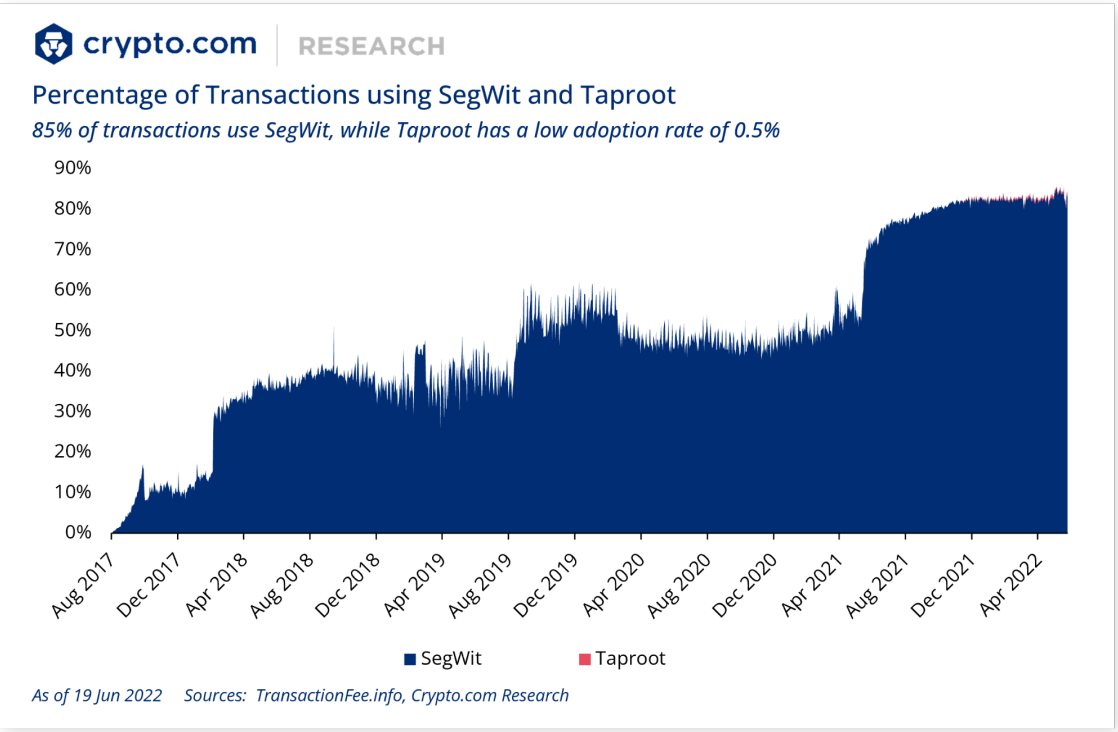
Taproot's Schnorr Signatures

After the Taproot upgrade, signatures are aggregated to reduce data



As of 15 Jun 2022 *Sources: Bitcoin.com, Crypto.com Research*

Nevertheless, both SegWit and Taproot are ad hoc solutions rather than general scaling methodologies. While they improve scalability, their utility is restricted to Bitcoin-based blockchains. In addition, such proposals cause significant amounts of contention in the community. Nevertheless, **SegWit is widely adopted, with 85% of the total transactions using it, in sharp contrast to Taproot's 0.5% adoption rate**. Thus, the benefits of Taproot, although promising, have not yet materialised.



2.2 Sharding

Sharding is a data partitioning technique first introduced in database systems, and it is based on the **divide and conquer** paradigm. **The idea is to break down large data sets into smaller, easily managed partitions.** Thus, it drastically improves processing and query performance.

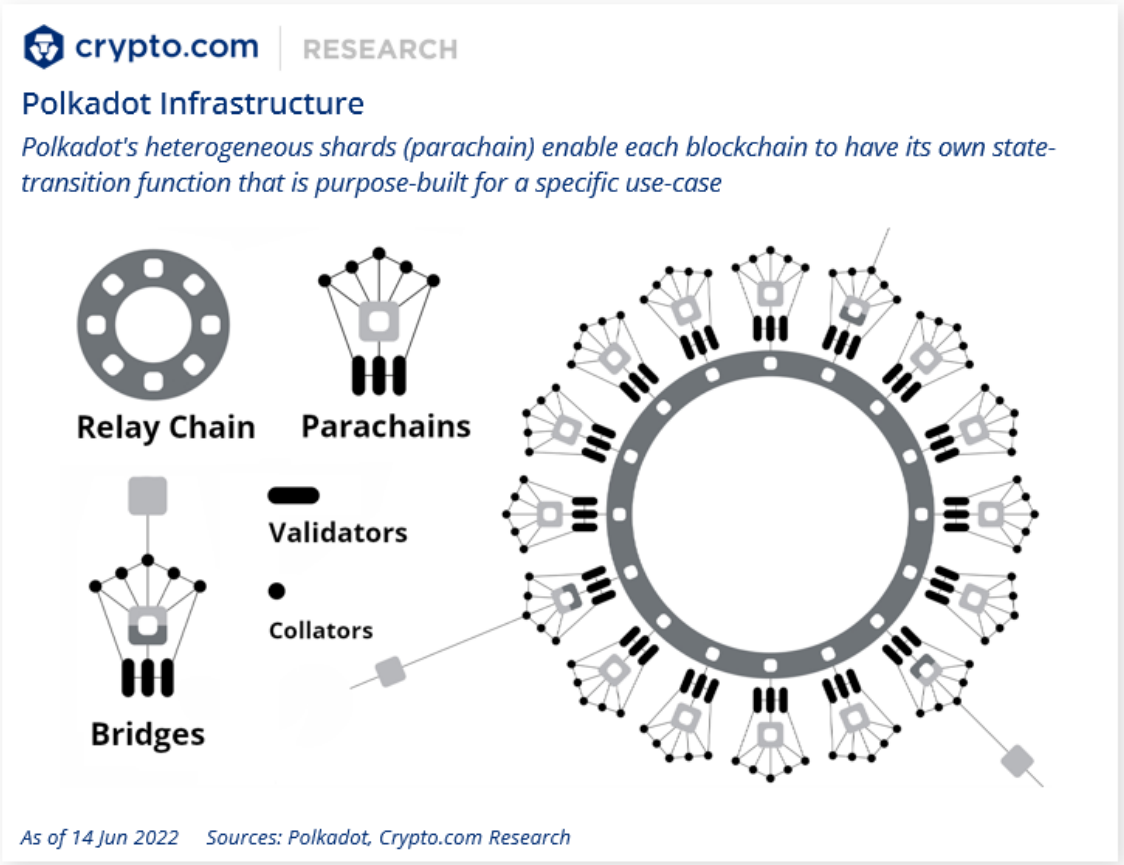
Zilliqa is the first public blockchain platform to have implemented sharding. **The blockchain is divided into smaller groups of nodes called shards. Each shard is responsible for the transactions within itself**, thus reducing pressure on the nodes. Specifically, nodes store and execute data solely for their shard, not the entire network. In addition, the shards can run in parallel, significantly increasing the throughput of the whole network.

Despite its benefits, **sharding introduces a great deal of complexity and remains a field of active development.** Blockchains that utilise sharding must consider aspects such as shard consensus and a protocol to handle inter-shard transactions.

Polkadot

Polkadot is a sharded blockchain with heterogeneous shards. The shards are called **parachains** (since they work in parallel) and define their own logic to

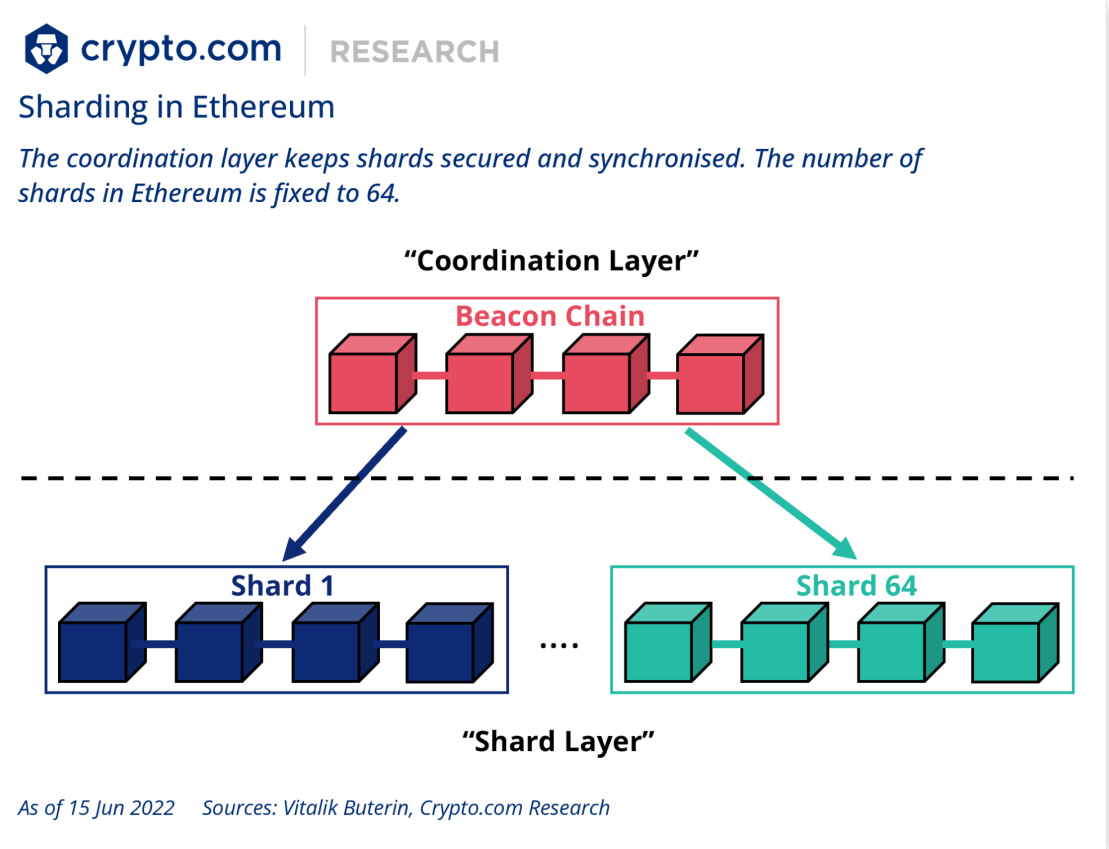
facilitate specific use cases. Parachains are referenced and secured by a core network called the **relay chain.** By design, the relay chain has limited functionalities (e.g., no smart contract support), and it focuses on coordinating the system (e.g., governance), while delegating work to parachains. Parachains communicate with the relay chain through dedicated slots that can be shared on a block-by-block basis to increase efficiency using **parathreads**. The parallel processing and strict assignment of duties significantly enhance scalability. Lastly, parachains can communicate with external networks (e.g., Ethereum) using bridges.



Ethereum

Ethereum plans to introduce sharding after **The Merge** (formerly called Eth2). **The Beacon Chain will coordinate 64 shards to alleviate network congestion and improve data handling.** The goal is to increase efficiency and reduce hardware requirements. Sharding's rollout schedule consists of multiple phases. Initially, shards will be used as data depots for the network without smart contract capabilities.

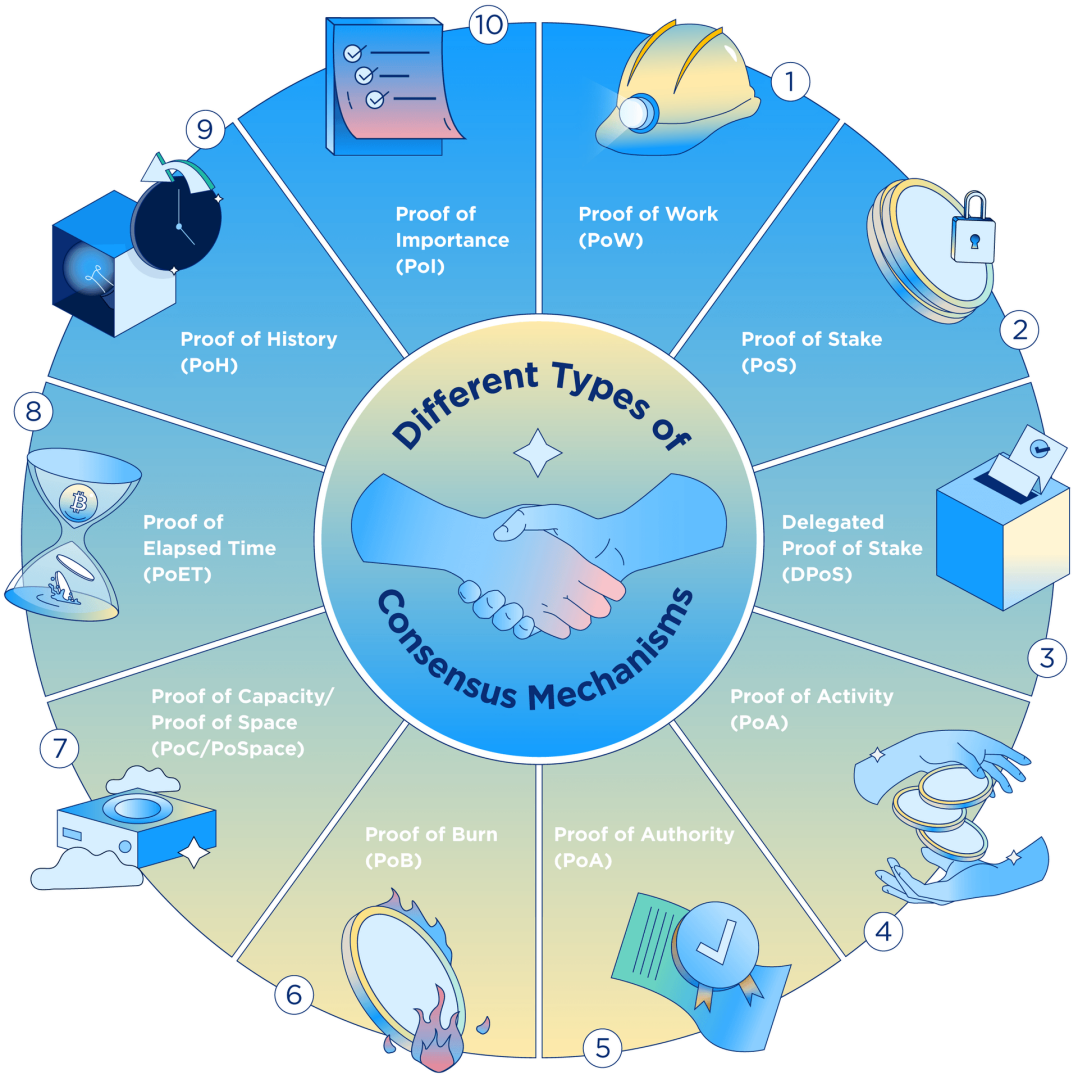
Ethereum's developers are still debating on additional functionalities. The upgrade is planned to occur in 2023 after the Mainnet merges with the Beacon Chain.



NEAR

NEAR is another blockchain that has begun transitioning to sharding with the launch of **Nightshade**. Unlike Ethereum, which has a fixed number of 64 shards, Near introduces **Dynamic Resharding**, in which the protocol can split or merge shards based on demand. **Dynamic resharding can accommodate both spikes and troughs by reorganising its structure** according to the required resource utilisation.

2.3 Consensus Mechanisms



As of 1 Jun 2022 *Sources: Crypto.com University*

Blockchains use consensus mechanisms to reach an agreement among participants without relying on trust. **The difficulty of scaling a blockchain is mainly due to its consensus since it requires all participants in the network to agree on which transactions are valid.**

Proof of work (PoW), which is used in Bitcoin and Ethereum, suffers from slow transactions and expensive fees due to its inherent mathematical limits (e.g., block frequency) set to maintain security. In addition, while a simple CPU sufficed for mining in the early days, the complexity grew significantly, making powerful GPUs and ASICs mandatory.

The great cost of resources in PoW raises concerns about its environmental impact. Thus, new consensus algorithms have been designed to tackle the above-mentioned drawbacks.

Comparison Table of Consensus Mechanisms crypto.com | RESEARCH

Category	Consensus	Example	Throughput (TPS)	Finality	Cost (USD)
Nakamoto Consensus	PoW	Bitcoin	7	1 hour	~$2.5
Proof of X	PoS	Cardano	250	10–60 minutes	$0.17
	DPoS	EOS	3,996	3 seconds	0[1]
	PoA	Cronos	Thousands	5~6 seconds	<$1
	PoH	Solana	50,000	2.5 seconds	$0.00025
Classical Consensus	pBFT	Hyperledger Fabric	1,800	0.36 seconds	0[2]
	dBFT	NEO	10,000	15 seconds	~$0.003
	FBA	Stellar	3,000	3-5 seconds	$3e-8
Leaderless Consensus	Avalanche	Avalanche	6,909	0.3 seconds	~$0.03
	IOTA	IOTA	1,000	10 seconds	0[3]

1. Participants are required to stake tokens

2. Nodes are owned by participants

3. Requires users to verify transactions before sending new ones

As of 17 Jun 2022 Source: Crypto.com Research

Proof of X

The Nakamoto Consensus (mostly known as PoW) paved the way for a new type of consensus mechanism called **Proof of X (PoX). The idea is to utilise a scarce resource dubbed 'X', which is difficult to obtain**. A network member must therefore invest in 'X' to verify blocks. In this chapter, we discuss the most popular algorithms in this category.

Proof of Stake

Proof of stake (PoS) is a consensus mechanism introduced as an eco-friendly and scalable alternative to PoW. In PoS, instead of mining, **users stake an amount of cryptocurrency as collateral for a chance to validate a block**. This staked blockchain native token can be destroyed if the validator behaves in a dishonest or lazy way. It is possible that in some PoS systems, users with greater stakes have higher chances of validating the next block and earning a reward.

The main criticism of PoS is that it favours users with a higher number of tokens, potentially leading to centralisation. Ethereum (The Merge) avoids centralisation by choosing validators randomly. Validators are required to stake 32 ETH as an initial stake. In addition, each validator's voting weight is capped at 32 ETH. Popular cryptocurrencies that implement PoS include **Cardano**, **Polkadot**, **Tezos**, and in the near future, **Ethereum**.

PoS has many variations, such as **Delegated Proof of Stake (DPoS), which partially sacrifices decentralisation for speed.** In PoS, anyone who stakes tokens may participate in block validation. However, DPoS uses an electoral system to select a committee of validators. Essentially, stakeholders elect witnesses to validate the next block on their behalf, and unreliable witnesses are voted out.

Users vote proportionally to their stake for witnesses to verify transactions and receive a reward. **The reward is then shared between witnesses and their voters.** In addition, if a witness fails or acts maliciously, no reward is distributed, and they lose part of their stake. **EOS** and **Tron** are popular chains using DPoS.

Proof of Authority

Proof of Authority (PoA) is a modified version of PoS proposed by Ethereum co-founder Gavin Wood. **In PoA, validators are selected based on reputation, and their identities must be verifiable**. In order to validate blocks, validators don't stake coins but their reputations. Thus, **they are incentivised to defend the transaction process** to maintain their validator rights and avoid damaging their reputation.

Blockchains using PoA differ from the norm, in which participation remains anonymous. Since only a selected group may participate, PoA results in slightly more centralised systems. On the other hand, **the cost of PoA is minimal, and it is one of the most efficient consensus mechanisms**, making it highly scalable. Popular blockchains using PoA are **Cronos** and **VeChain**.

Other Proof of X

There is an abundance of consensus mechanisms. Most of them are modifications or hybrid versions of those mentioned above. Some examples include **Proof of History** used in **Solana**, **Proof of Capacity** used in **Burstcoin**, and **Proof of Burn** used in **Slimcoin**.

Classical Consensus

Classical consensus is a class of protocols which reach consensus through voting. Many classical consensus mechanisms predate blockchain technology. These protocols generally confirm transactions fast, relative to PoX, but require a limited network size, thus making scalability impractical. Some noteworthy examples include **Practical Byzantine Fault Tolerance (pBFT)** used in **Hyperledger Fabric** and **Elastico**, **Delegated Byzantine Fault Tolerance (dBFT)** used in **NEO**, and **Federated Byzantine Agreement (FBA)** used in **Stellar**.

Leaderless Consensus

Typically, consensus mechanisms are leader-based. In simple terms, the whole network elects a leader (e.g., through voting or winning a competition) to propose blocks and the rest of the participants vote on the proposal. A drawback of leader-based consensus is that the network relies on the leader, who may be unresponsive or slow, thus slowing down the entire network.

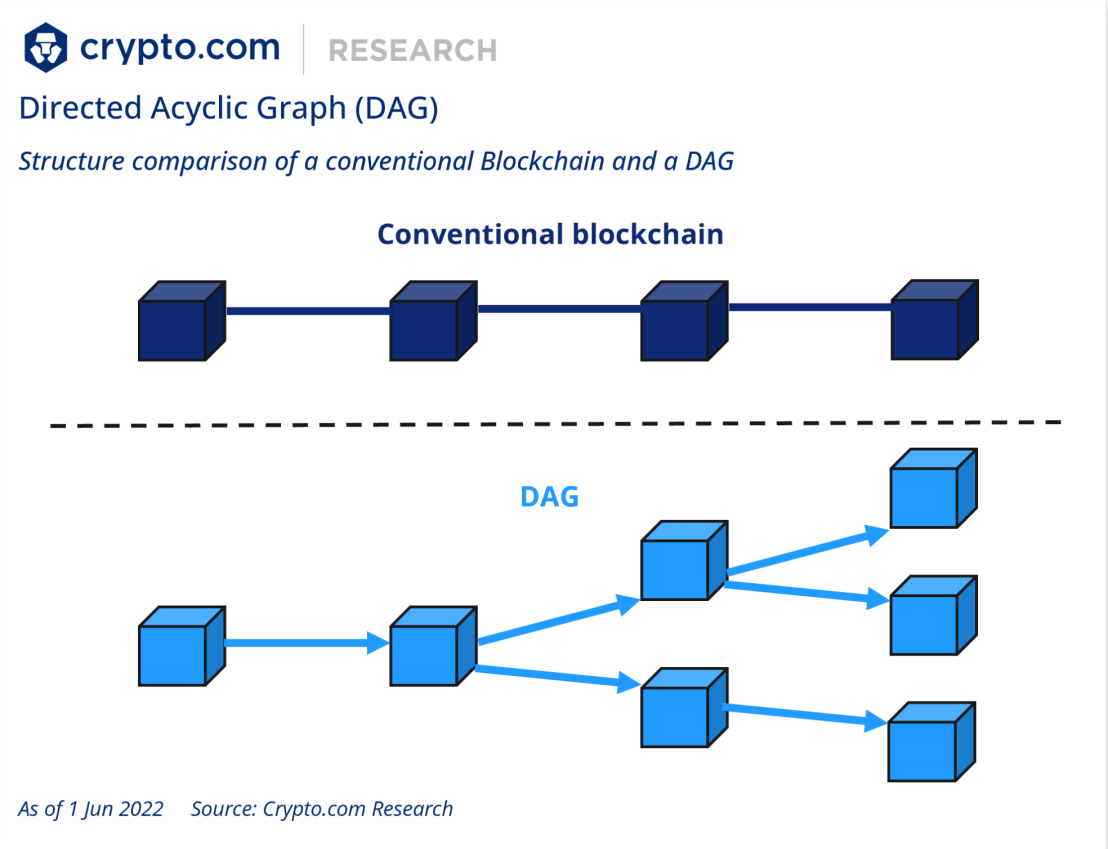
For this reason, **Leaderless Consensus mechanisms which require no leader have been devised**. In general, they work by performing multiple rounds of random sampling until the possibility of a fraudulent transaction converges to zero. Today, leaderless consensus mechanisms remain largely experimental, with popular examples being Avalanche and IOTA.

2.4 DAG

Conventionally in blockchains, data is grouped into blocks. Every new block created is linked to the previous one, which forms a chain. Hence the name blockchain. This linked list limits the system's throughput, as new blocks cannot be generated concurrently. To tackle this, **some projects replace blockchains with more general structures to improve scalability**.

A novel idea is to use a **Directed Acyclic Graph (DAG)**. In computer science, **a DAG is a data modelling structure with no loops**. A blockchain can be transformed into a DAG by treating each transaction as a vertex. Because each vertex can connect to multiple previous vertices, **the DAG structure allows**

numerous transactions to be validated simultaneously. Thus, each new vertex must reference previous vertices to get accepted.



Compared to blockchains, **DAG-based networks are highly scalable and well suited for large numbers of transactions**. However, DAG methods used in cryptocurrencies remain in their infant state, and further experimentation is necessary.

Avalanche

Avalanche uses a combination of methods to solve the scalability trilemma. **The network features three interoperable blockchains (i.e., X-Chain, P-Chain, C-Chain)**. Each chain follows different rules (e.g., consensus mechanisms) and offers different functionalities.

The **X-Chain (eXchange Chain)** acts as a decentralised platform and is used solely to transfer funds. This specialisation enables tailor-made optimisations relating to transfers. The **P-Chain (Platform Chain)** coordinates validators and handles subnets, a sharding-inspired scaling solution. Finally, the **C-Chain (Contract Chain)** handles smart contracts, allowing the Avalanche Network to be used as a smart contract platform. **Separating duties increases efficiency compared to using one chain for all processes.**

In contrast to most blockchains where agreements are reached through a leader (e.g., a miner), **Avalanche's consensus mechanism is a DAG-optimised leaderless consensus,** promising low latency and high throughput**.** Specifically, validators select a sample of the network and query whether a transaction is valid. After repeated sampling, the probability of a fraudulent transaction reduces to zero.

Fantom

Fantom is a smart contract platform with multiple features to address scalability issues. A significant difference with other blockchains is that **a new blockchain is created for each smart contract deployed**. In addition, Fantom is further enhanced by a novel consensus mechanism called **Lachesis**. Lachesis **utilises the DAG model to store and query transactions efficiently.**

3. Off-chain (Layer 2) Solutions

Layer 2 solutions enhance scalability by offloading transactions off the main chain. They are essentially add-ons, building a new computational layer on the top of the main blockchain. Thus, there are no changes required in the Layer 1 protocol.

Layer 2 solutions drastically improve throughput, decongest the main chain, and minimise transaction fees. This is achieved by reducing the transaction data footprint and communicating with the main chain only when necessary.

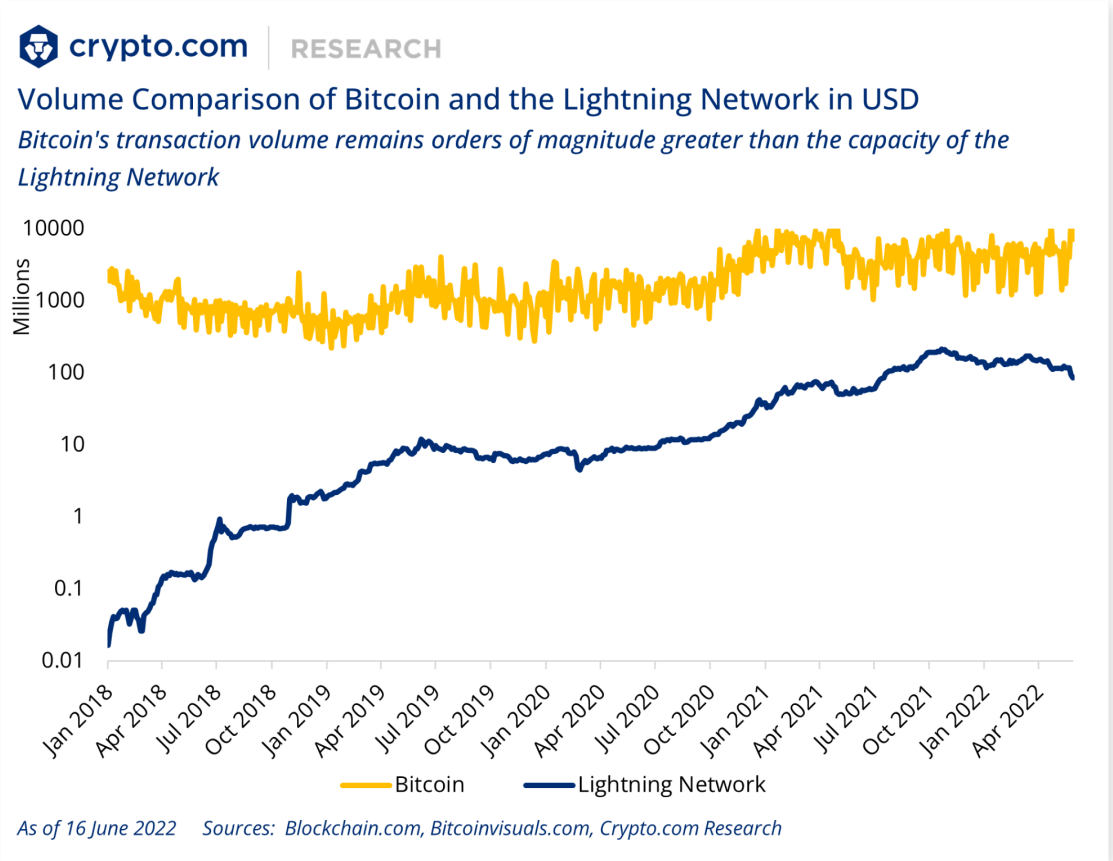
Lastly, most Layer 2 solutions are general methodologies and are not blockchain-specific. Thus, they can be applied across different blockchains.

Comparison Table for Layer 2 Solutions crypto.com | RESEARCH

Solution	Pros	Cons	Throughput	Finality
Payment Channel	- High throughput - Low cost, apt for micropayments	- No open participation - Not apt for single transactions - Parties must remain online	25 million TPS[1]	Nearly instant[1]
Sidechain	Permanent once created	Less decentralised	65,000 TPS[2]	2.1 seconds[2]
Optimistic Rollup	EVM-compatible	Slow withdrawals	4,500 TPS[3]	1 week[3]
ZK Rollup	No withdrawal delay	- Limited to token transfers - Resource intensive	2,000 TPS[4]	~10 minutes[4]
Validium	Higher throughput than ZK	- Limited smart contract support - Resource intensive	9,000 TPS[5]	~10 minutes[5]

Note: 1. Lightning Network; 2. Polygon; 3. Arbitrum One; 4. zkSync; 5. StarkEx
As of 1 Jun 2022 Sources: Ethereum.org, Crypto.com Research

In general, L2 solutions are based on the two most prominent blockchains (i.e., Bitcoin and Ethereum). For Bitcoin, a widely adopted scalability solution is the Lightning Network, an off-chain solution known as a **state channel** (described in the next chapter). Since it went live, it has reached a capacity of 4,000 BTC, with 17,500 nodes and 85,000 unique channels.



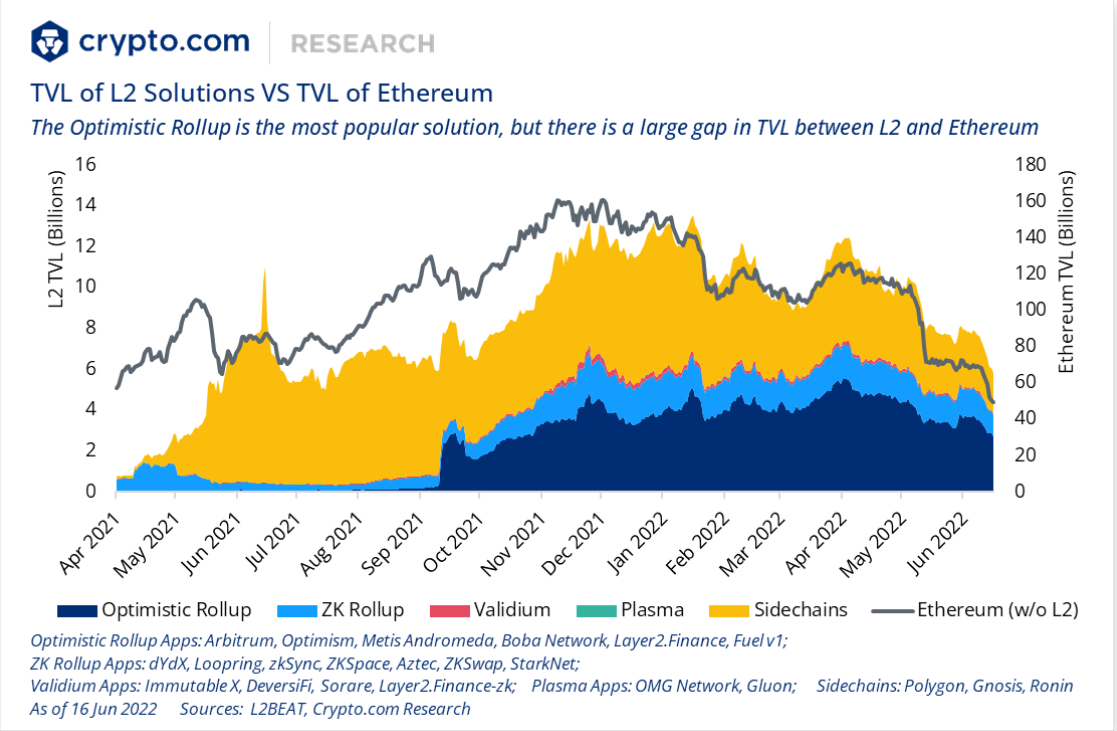
The Ethereum ecosystem is firmly aligned that Layer 2 scaling is the only way to solve the scalability trilemma while remaining decentralised and secure. Thus, a great variety of Layer 2 solutions has been developed for the Ethereum blockchain.

Classification of Layer 2 Solutions crypto.com RESEARCH

	Validity Proofs	Fraud Proofs
Data on-chain	ZK Rollup	Optimistic Rollup
Data off-chain	Validium	Plasma

As of 17 Jun 2022 *Sources: Coinmonks, Crypto.com Research*

The L2 solutions mainly focus on Rollups and Sidechains. From the chart below, we can derive that **the Optimistic Rollup is currently the most popular solution, with over US$2.7B locked in protocols**.



3.1 Payment Channels

Payment channels are temporary Layer 2 protocols set up by individuals who often transact with each other. They aim to decongest the main blockchain, reduce transaction fees, and enable micro transactions. **Participants may transact numerous times while only reporting to the blockchain twice** (i.e., in the opening and closing of the channel).

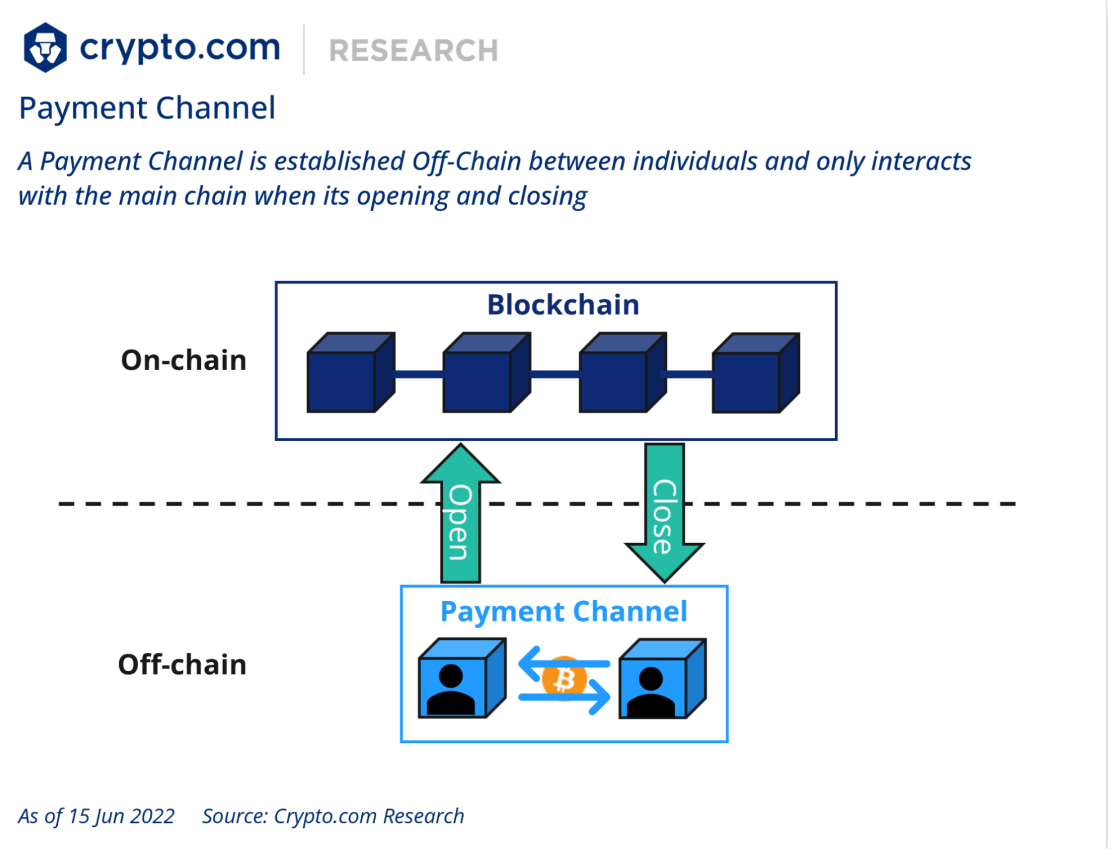
The channel opening requires individuals to lock funds into a multisig contract. Then, transactions take place efficiently off-chain. When the participants complete their dealings, one final transaction is committed to the blockchain, settling the transfers and unlocking the funds.

Despite their benefits, **payment channels have several limitations**. Firstly, they are unsuitable for one-off transactions since the time and cost associated with using the channel exceeds that of the blockchain. Secondly, users must remain available to keep the channel alive, which is inconvenient. Additionally,

participants might wait a long time to receive funds from unresponsive peers. Lastly, the set of participants is strictly defined by the contract, making open participation infeasible.

Lightning Network

The Lightning Network is an off-chain solution designed to make Bitcoin transactions fast and affordable. **It is essentially a peer-to-peer network, where participants keep a separate tab from the Bitcoin blockchain**, only settling it when necessary. Its adoption ranges from private companies (e.g., Twitter) to countries (e.g., El Salvador).



To create a payment channel in the Lightning Network, a pair of users must sign a smart contract to lock their assets. **Once the channel is established, they can perform a vast amount of Bitcoin transactions in nearly instant time and pay minimal routing fees.** These benefits are possible since only the opening and the channel's closing are reported to the Bitcoin network. As a result, fees and delays associated with the core chain are minimised.

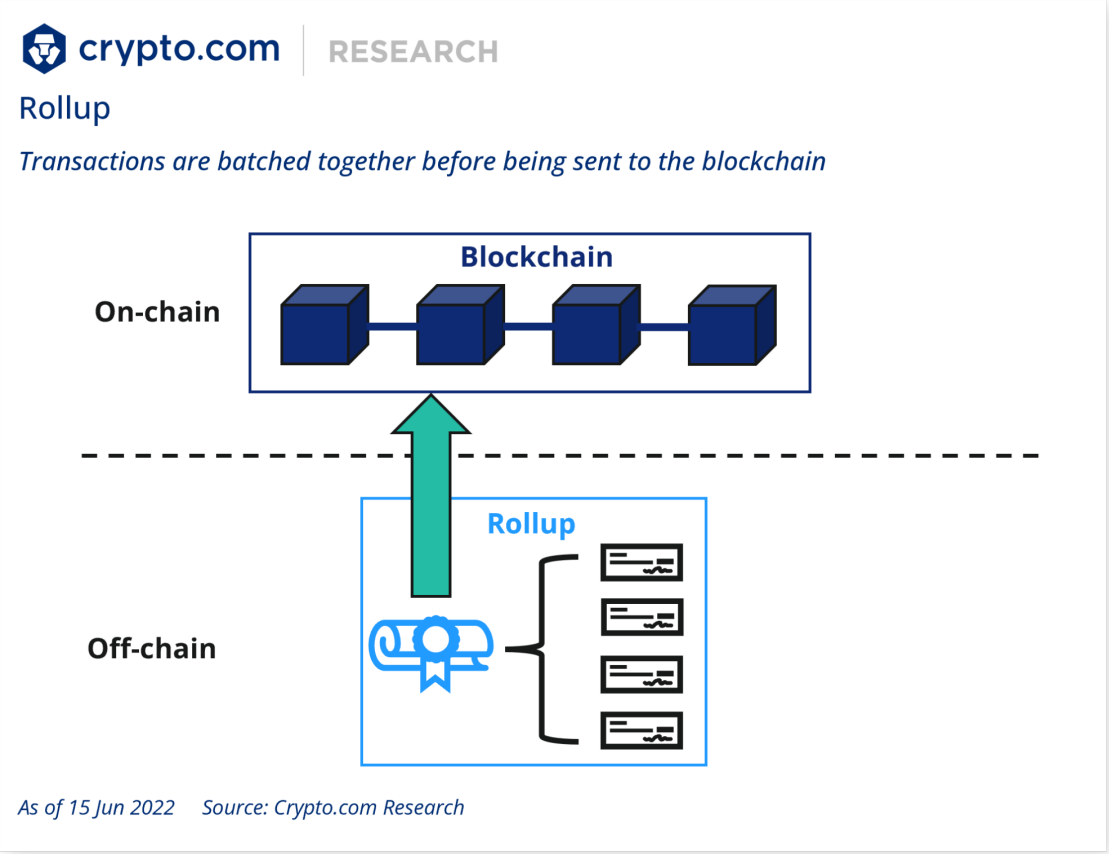
While the Lightning Network improves scalability, its criticism stems from the opposite edge of the trilemma. Namely, **prominent businesses may become**

hubs leading to a centralised network. Furthermore, the Lightning Network has all the drawbacks mentioned above. For example, **participants must constantly be online to keep the channel operational,** which is impractical.

Other Payment and State Channels

The **Raiden Network** **is a payment channel for Ethereum which supports transactions with all ERC20 tokens**. It contrasts with the Lightning Network, which is limited to Bitcoin. Nevertheless, its adoption has been minimal. **Cardano** is also developing its own state channel called **Hydra**, which is expected to launch in 2022.

3.2 Rollups



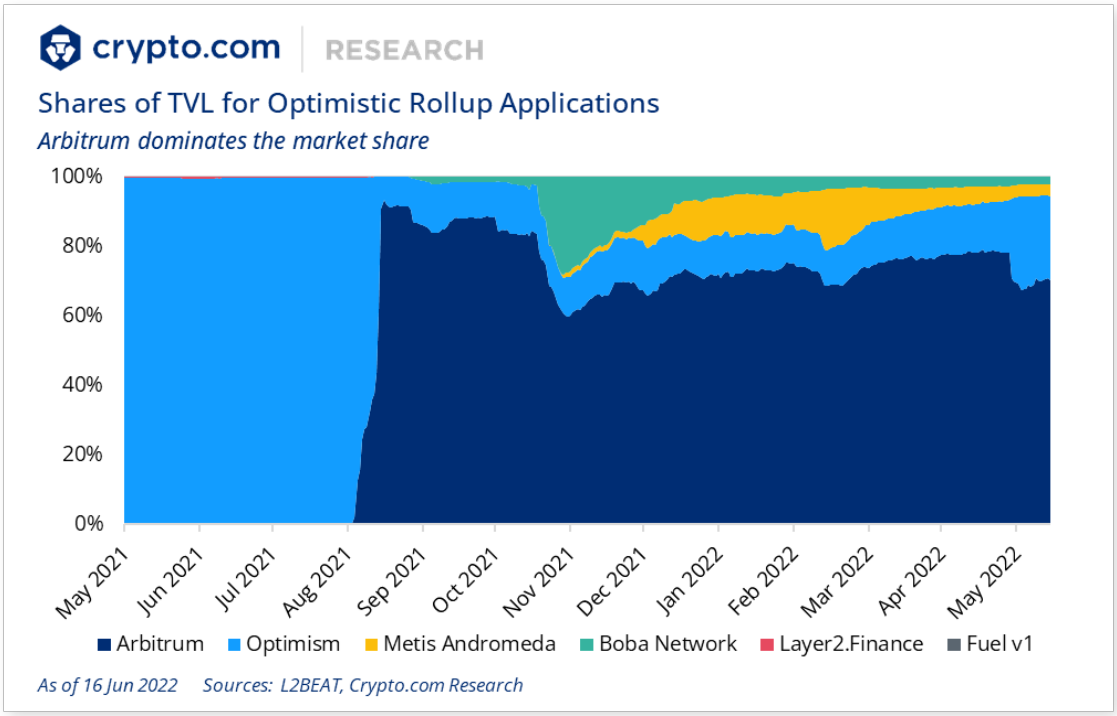
Rollups are the new and upcoming Layer 2 solution. In simple terms, **they start by executing a bunch of transactions off-chain**. Then, **the transactions are 'rolled up' into a single transaction, which is sent back to the main blockchain**.

By settling transactions off-chain and only posting the transaction data on the main chain, **Rollups achieve high scalability and leverage Layer 1's security mechanisms.** In addition, they reduce fees by amortising the cost. Specifically, the more transactions included in a batch, the more the cost is spread out.

Nevertheless, **Rollup fees are relatively expensive compared to alternative Layer 1 blockchains**. For example, a simple transaction in Cronos costs around $0.10, but Optimism is $0.28 at the time of writing. Furthermore, their user experience remains subpar. The users are currently required to bridge the assets between the layers and may experience long withdrawal times.

Rollups are a hot topic in the blockchain world, with US$1.38B in total value locked in a relatively short time. They are an active field of research and come in various flavours. In this section, we explore some prominent Rollup architectures and their capabilities.

Optimistic Rollups

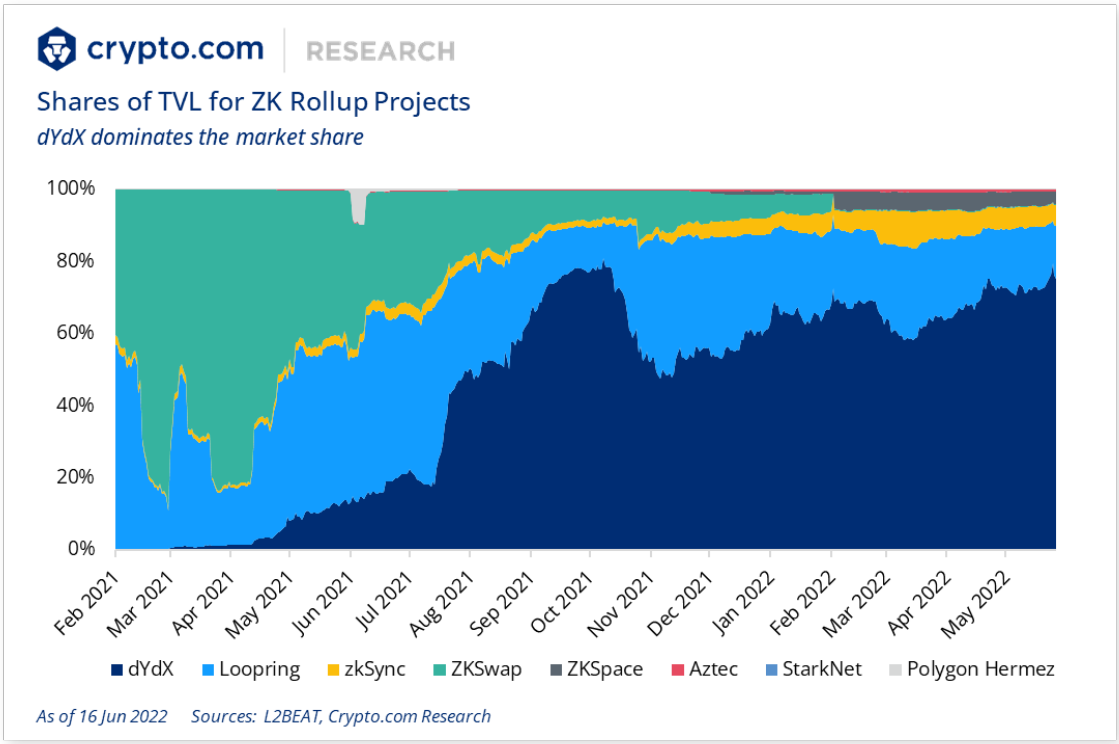


Optimistic Rollups **assume that the submitted transactions are valid** (hence the optimism). This assumption speeds up processing by omitting unnecessary work. However, **users can dispute the validity of a batch by submitting a fraud proof**. If a batch is proven fraudulent, the invalid transactions are discarded. **Optimistic Rollups compress the entire transaction history before sending it to the main chain to roll back any invalidated transactions**. This

way, the main blockchain's security mechanism can thoroughly examine the contentious dealings. Another benefit is that most Optimistic Rollups are compatible with the Ethereum Virtual Machine (EVM), making it easy for Ethereum developers to deploy smart contracts. Some projects that use Optimistic Rollups include **Uniswap v3**, **Optimism**, **Arbitrum One**, and the **Boba Network**.

The Achilles heel of Optimistic Rollups is the long withdrawal times. Long dispute periods are required to allow sufficient time for fraud proofing. While short dispute periods improve user experience, they lack security. In general, withdrawals in Optimistic Rollups may take up to a week. Some projects provide instant liquidity by charging a small fee to eliminate long waiting times. In addition, **Optimistic Rollups require that at least one honest party exists to function correctly**.

ZK Rollups



Zero-Knowledge Rollups (ZK Rollups) batch transactions off-chain and produce a zero-knowledge cryptographic proof (i.e., SNARK or STARK). These validity proofs are sent to the Layer 1 blockchain along with state differentials (i.e., changes in account balances of the entities involved). Thus, **batches with invalid proofs are rejected straight away**. ZK Rollups only need the validity proof instead of the entire transaction history, unlike their Optimistic counterparts. Thus, this significantly reduces the size of the data transferred. In addition, verifying proof is less computationally expensive than generating them. Therefore,

validation using ZK Rollups is efficient and inexpensive, with withdrawals concluding significantly faster than Optimistic Rollups. Popular ZK-Rollup projects include **Loopring**, **dYdX**, and **zkSync**.

On the other hand, producing the validity proof of a **ZK Rollup is computationally intensive**. Such demanding computations increase the hardware requirements, which stifles their adoption. Furthermore, **ZK Rollups remain largely incompatible with EVM** due to their complexity. Nevertheless, ongoing research is taking place, with some projects designing their own EVM-compatible virtual machines.

3.3 Sidechains

Sidechains are semi-independent blockchains that work together with the main chain to improve their speed and capabilities. A **two-way peg** enables seamless asset transfers between the main chain and its sidechains. Sidechains are not bound by Layer 1 protocols and may follow their own rules (e.g., consensus mechanisms).

For example, **Ethereum uses PoW, but Polygon uses PoS**. In addition to enhancing scalability, the plurality of sidechains offers users the ability to try out new technologies built on sturdy foundations of well-established blockchains.

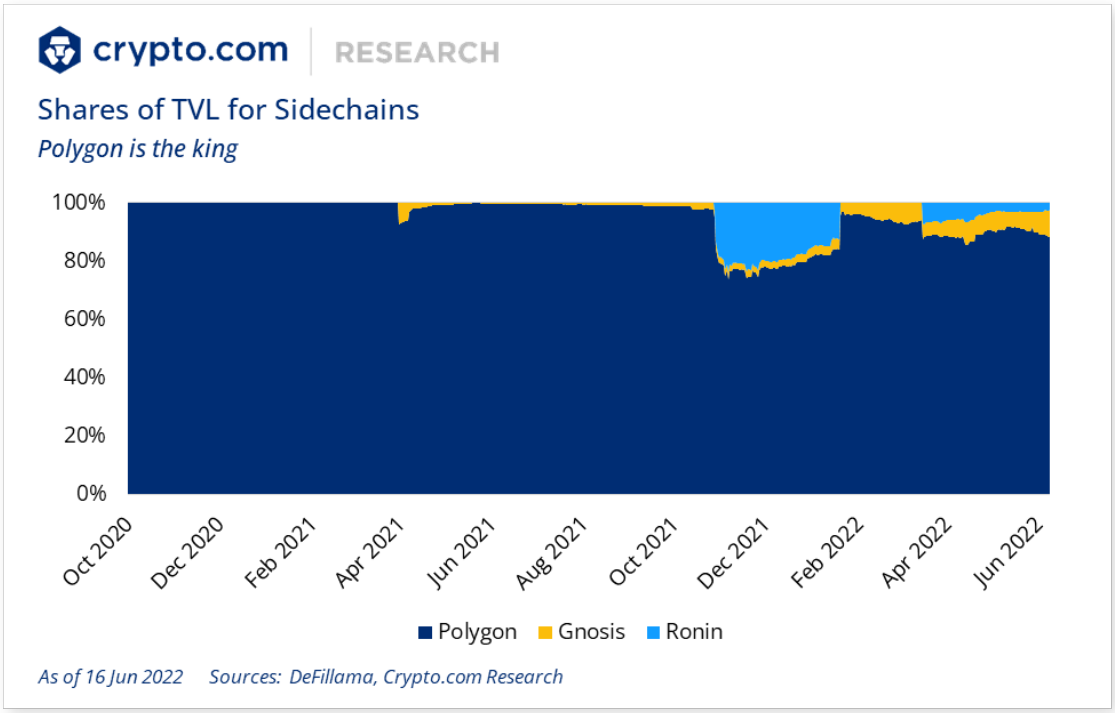
Polygon

Polygon (formerly known as Matic) is a platform for building sidechain projects on Ethereum. It consists of several interoperable chains, which intend to address the shortcomings of the Ethereum blockchain (e.g., throughput and gas fees).

Polygon is often called Ethereum's 'internet of blockchains' since the sidechains can communicate both with each other and Ethereum. Polygon offers an arsenal of different scaling solutions, such as the **Supernets** of **Polygon Edge**, which allow developers to build customisable networks inexpensively.

Polygon's backbone is the PoS Chain, arguably the most widely adopted sidechain. It utilises PoS and rewards users with its native token MATIC for helping as validators or delegators. Validators verify transactions and receive a cut of the fees in addition to the newly created MATIC. However, they must run a node full time and stake MATIC.

In case of malicious behaviour or simply an error, their rewards are slashed. Delegators receive MATIC from other users and select validators. They share rewards with the validators too; thus, research is required to avoid unreliable validators.



Plasma

A plasma chain is a separate blockchain anchored to the main Ethereum chain and uses fraud proofs (e.g., optimistic rollups) to arbitrate disputes. These chains are referred to as **child chains**. Child chains are miniature copies of the Ethereum blockchain, branching out of it in a tree-like fashion.

Similar to other Layer 2 solutions, Plasma provides significant throughput gains by taking execution off the main chain. In contrast to the Lightning Network, **Plasma does not require participants to be simultaneously online to transact**. In addition, users can transfer assets between a child chain and Ethereum and even **safely withdraw their assets in case of malicious behaviour**.

Nevertheless, **Plasma adoption has stagnated, mainly due to its impractical exit mechanisms.** Firstly, participants must monitor transactions to detect fraudulent behaviour, adding significant overhead. Furthermore, withdrawal time is slow, taking up to two weeks.

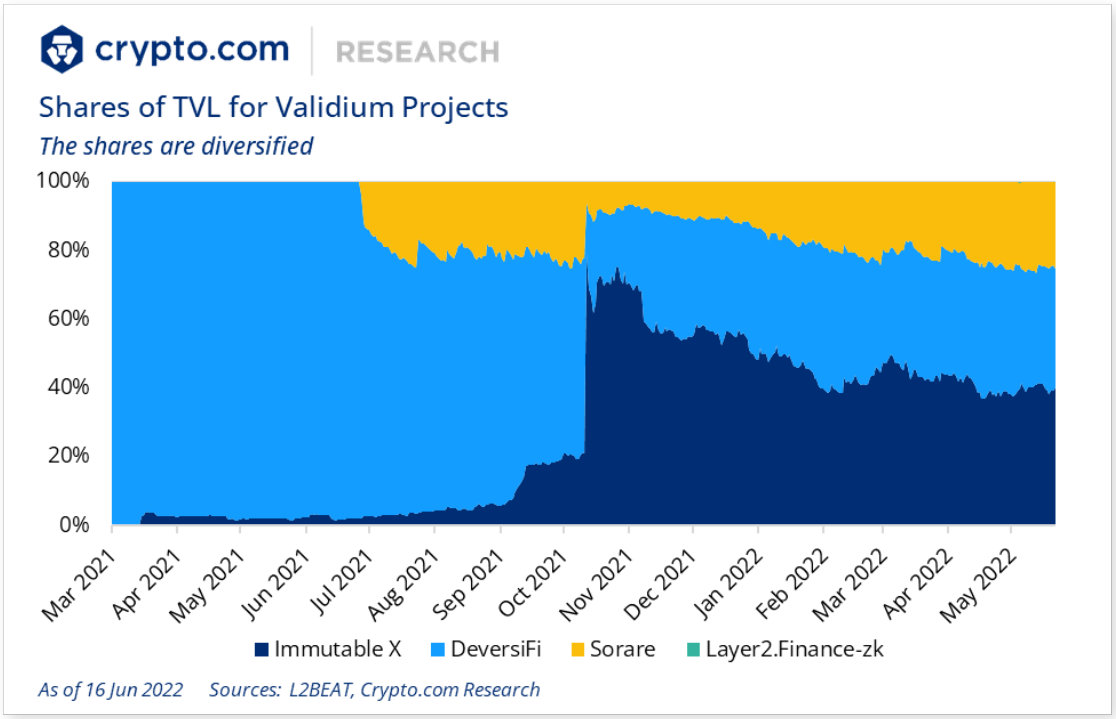
Currently, **the interest has shifted to newer methods such as Rollups**. A prominent example is the **OMG Network** (Plasma based) which has been outshined by the **Boba Network** (Rollup based).

3.4 Validium

Similarly to ZK Rollups, **Validium** uses validity proofs to verify transactions. Their main difference is data storage. **While ZK Rollups send data to the Layer 1 blockchain, Validium stores transactions off-chain**. Off-chain storage improves throughput and reduces costs by minimising communication with the main blockchain.

However, in ZK Rollups, the availability of the data is stored and secured by Layer 1. **In Validium, necessary proofing data may be unavailable** (e.g., due to a malicious operator), resulting in adverse side effects. For example, users might be unable to withdraw their assets.

Various solutions attempt to safeguard data accessibility. One approach is to appoint a **Data Availability Committee (DAC)**. A DAC handles the data and provides proof of availability when requested. Another method is **bonded data**. Bonding requires data managers to stake tokens as bonds in a smart contract.



This bond reduces trust assumptions since if the participants fail to provide proof, their bond is slashed. **The benefit of bonded data compared to DACs is that it minimises centralisation and the trust required**.

Despite Validium's benefits, the off-chain data storage significantly increases complexity. **Volition is a combination of ZK Rollups and Validium, which aims**

to provide the best of both worlds according to the problem at hand. Nevertheless, both Validium and Volition remain highly experimental projects and necessitate further research.

4. Conclusion

4.1 Towards Scalable Blockchains

Blockchain scalability is a critical aspect of cryptocurrencies. **The rapid growth in users mandates designing systems able to accommodate the demand**. Currently, cryptocurrencies are unable to compete with the throughput provided by major centralised financial institutions.

Scalability is not a trivial task since it is impeded by the blockchain trilemma, among other challenges. Nevertheless, **a lot of novel work takes place by multiple competing parties**. These works are drawing a promising and exciting future for the crypto space.

4.2 Concluding Remarks

This report surveys the plethora of scalability solutions focusing on Layer 1 and Layer 2. We examine their strength and vulnerabilities and compare them with each other. **We are optimistic that blockchain technology will become more scalable, accelerating the world's transition to cryptocurrency.**

Published on 27 Jun 2022

References

B. Bondi, André. “Characteristics of scalability and their impact on performance.” *WOSP,* September 2000, https://doi.org/10.1145/350391.350432. Accessed at June 17 2022.

Back, S.A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A.K., Poelstra, A., & Timón, J. “Enabling Blockchain Innovations with Pegged.” *Blockstream*, https://blockstream.com/sidechains.pdf. Accessed May 27 2022.

Crypto.com. “How to Agree: Different Types of Consensus for Blockchain” *Crypto.com University,* 9 June 2022, https://crypto.com/university/different-types-of-consensus-for-blockchain. Accessed 29 May 2022.

Crypto.com. “What are Sidechains? – Scaling Blockchain on the Side” *Crypto.com University,* 4 February 2021, https://crypto.com/university/what-are-sidechains-scaling-blockchain. Accessed 29 May 2022.

Crypto.com. “A Deep Dive Into Blockchain Scalability” *Crypto.com University,* 3 January 2020, https://crypto.com/university/blockchain-scalability. Accessed 29 May 2022.

Crypto.com. “In Search of Interoperabiity: An Overview of the Cross-Chain Market”, *Crypto.com Research*, 30 October 2021, https://crypto.com/research/an_overview_of_the_cross_chain_market-2. Accessed 2 June 2022.

Ethereum.org. “Scaling” *Ethereum.org*, https://ethereum.org/en/developers/docs/scaling/. Accessed 2 June 2022.

Frankenfield, Jake. “Consensus Mechanism (Cryptocurrency).” *Investopedia*, https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp. Accessed 24 May 2022.

Q. Zhou, H. Huang, Z. Zheng and J. Bian. "Solutions to Scalability of Blockchain: A Survey" *IEEE Access*, 17 January 2020, doi: 10.1109/ACCESS.2020.2967218. Accessed 1 June 2022.

Ren, Ling. “Analysis of Nakamoto Consensus.” *IACR Cryptol*, 2019, https://www.semanticscholar.org/paper/Analysis-of-Nakamoto-Consensus-Ren/9201a47fcbe4f748dbd02fead1581f57680b4684. Accessed 30 May 2022.

Goldwasser, S., Micali, S., and Rackoff, C. . “The knowledge complexity of interactive proof-systems.”, *STOC*, 1 October 1985, https://dl.acm.org/doi/10.1145/22145.22178. Accessed 5 June 2022.

Vaibhav S. “ConsensusPedia: An Encyclopedia of 30+ Consensus Algorithms”, *Hackernoon*, https://hackernoon.com/consensuspedia-an-encyclopedia-of-29-consensus-algorithms-e9c4b4b7d08f. Accessed 30 May 2022.

Croman, K. & Decker, C., Eyal, I. & Gencer, A. E. & Juels, A., & Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E., Song, D. Wattenhofer, R.. “On Scaling Decentralized Blockchains (A Position Paper)”, *3rd Workshop on Bitcoin and Blockchain Research,* 2 February 2016, https://www.researchgate.net/publication/292782219_On_Scaling_Decentralized_Blockchains_A_Position_Paper. Accessed 29 June 2022.

e. contact@crypto.com

Published on 27 Jun 2022