crypto.com

Layer-0: Infrastructure For Customised Blockchains

June 2023

Research and Insights

Crypto.Com Research and Insights Team

Published on 3 Jul 2023

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

Published on 3 Jul 2023

Key Takeaways

- Layer-0 protocols provide the foundational infrastructure that customised Layer-1 blockchains can be built on, enabling developers to focus on applications instead of consensus and security.
- Layer-1 blockchains on Layer-0 networks gain flexibility by being able to, for example, choose their own token issuance model, optimise network parameters, and curate their own ecosystems of dApps.
- Interoperability solutions provided by Layer-0 allow Layer-1 blockchains to communicate and exchange value, empowering cross-chain applications and helping to unlock the full potential of the blockchain ecosystem.
- Promising Layer-0 projects like Cosmos, Polkadot, Avalanche, LayerZero, and zkLink use different technologies to achieve interoperability. However, each solution's unique architecture comes with its own set of constraints.
- Looking forward, Layer-0 networks have the potential to foster blockchain innovation by enabling a multitude of specialised and interoperable Layer-1 blockchains.

1. What Is Layer-0?

Layer-0 protocols form the foundation that Layer-1 blockchains are constructed on. Serving as infrastructure for blockchain networks and applications, Layer-0 protocols represent one solution striving to tackle issues confronting the industry, including scalability and enabling interoperability between blockchains.

Layer-0 is the base infrastructure that enables developers to launch independent blockchains optimised for different needs. Layer-0 platforms can allow application-specific blockchains to optimise for different elements of the scalability trilemma.

1.1 Base Layer For Customised Layer-1s

Layer-0 protocols enable developers to launch customised Layer-1 blockchains designed for specific applications or use cases. With the support of Layer-0s, developers can focus on applications instead of consensus and security.

Notable Layer-0 protocols like Cosmos, Polkadot, and Avalanche provide software development kits (SDK) that allow developers to launch their own Layer-1 sidechains connected to the Layer-0 mainchain while maintaining independent operation. This functions as an infrastructure for building new specialised blockchains.

Generally, a Layer-1 Proof-of-Stake (PoS) blockchain network requires its own set of validator nodes. These validators are responsible for confirming transactions, reaching consensus, and producing new blocks. Having the ability to build their own blockchain from the ground up gives developers tremendous flexibility.

- Developers can choose the token issuance model that fits their needs - whether inflationary or deflationary.
- By changing parameters, the network can be optimised for different tradeoffs, and it is relatively easy to set up permissioned or permissionless chains.
- Developers can curate the types of decentralised applications that are built on their network, fostering their own ecosystem of dApps and users.

1.2 Interoperability

Layer-0 protocols aim to allow the Layer-1 blockchains built on them to communicate and interoperate, which provides users with a seamless experience across multiple networks.

At its core, interoperability refers to the ability of different networks to exchange and make use of information seamlessly. To understand the significance of interoperability for blockchains, we can think of individual blockchains as different cities. Each one has its own value and advantages, but to enable true economic activity and growth, these cities need connections, or "bridges", between them. Layer-0 enables independent blockchains to exchange data through various cross-chain transfer protocols.

This allows tokens, value, and information to flow across multiple blockchains, empowering developers to build applications that span different chains. Additionally, this aids blockchain innovation and boosts use cases as well.

Without interoperability solutions provided by Layer-0 networks, individual blockchains would largely operate in isolation. This limits their utility and hinders the networking effects that arise when systems can communicate and interact with each other.

How Layer-0 compares to other layers is summarised below:

Layer Descriptions crypto.com | RESEARCH

Layer	Description	Examples
Layer-2 (L2)	L2 is a collective term to describe a specific set of scaling solutions for L1.	Optimistic-Rollups ZK-Rollups
Layer-1 (L1)	Generally refers to a blockchain with a native cryptocurrency. It includes the basic rules and protocols that govern how the network operates and how transactions are processed and validated.	Bitcoin Ethereum Cronos
Layer-0 (L0)	Refers to the underlying infrastructure that supports the operation of L1s, helping with scalability and interoperability.	Cosmos Polkadot Avalanche

Source: Crypto.com Research

1.3 How Does a Layer-0 Work?

A number of notable Layer-0 protocols adopt the relay-sidechain based infrastructure. This mainly constitutes three components: A mainchain supports the data transfer between Layer-1s; the sidechains are application-specific Layer-1s connected to the mainchain; and the interchain communication protocol acts as a standard for data exchange among the Layer-1s.

Sidechain/Relay Based Layer-0 Components crypto.com | RESEARCH

Component	Description	Examples
Mainchain	This acts as the primary blockchain within a Layer-0 network, often storing transaction records from connected Layer-1 sidechains.	Cosmos Hub Polkadot Relay Chain Avalanche Primary Network
Sidechains	Independent Layer-1 blockchains with their own sets of validator nodes and consensus mechanisms. Although they operate independently, sidechains often benefit from the security of the mainchain by integrating it in various ways.	Cosmos Zones Polkadot Parachains Avalanche Subnets
Cross-chain transfer protocol	The mechanism that enables tokens and data to be transferred trustlessly and securely between connected blockchains. This allows value and information to flow across the Layer-0 network, powering interoperable applications.	Cosmos IBC Polkadot XCMP Avalanche Warp Messaging

Source: Crypto.com Research

In summary, the mainchain provides security for the whole network while sidechains offer flexibility and customisation potential. The cross-chain protocol facilitates interoperability between these different blockchains, maximising their combined utility.

Currently, **Cosmos**, **Polkadot**, and **Avalanche** are prominent examples of Layer-0 networks that use the relay-sidechain structure, while there are newcomers like **LayerZero** and **zkLink** that represent the next progression of multichain

interoperability. We will explore each of these in more detail in the following sections.

Prominent Layer-0 Networks crypto.com | RESEARCH

	Cosmos	Polkadot	Avalanche
Consensus	Tendermint Core	Nominated Proof of Stake	Avalanche Consensus (X-Chain), Snowman Consensus (P and C-Chains)
Ecosystem Structure	Hub — Zones	Relay Chain — Parachains	Subnets (No sharding)
L1 Chains in Ecosystem	Zones	Parachains	Subnets
Cross-Chain Technology	Inter-Blockchain Communication Protocol (IBC)	Cross-Chain Message Passing (XCMP)	Avalanche Warp Messaging (AWM)
Development Toolkit	Cosmos SDK	Substrate	Avalanche-CLI
Finality	~3 seconds for finality	12 to 60 seconds for finality between parachains. External blockchains take longer (~60 minutes)	Sub 3-second finality, with the majority happening in sub 1-second
Security (Mainnet & L1s)	Shared security is supported by Interchain Security	Shared security	Shares nodes, but doesn't share security

Source: Crypto.com Research

2. Notable Cross-Chain Protocols

2.1 Cosmos

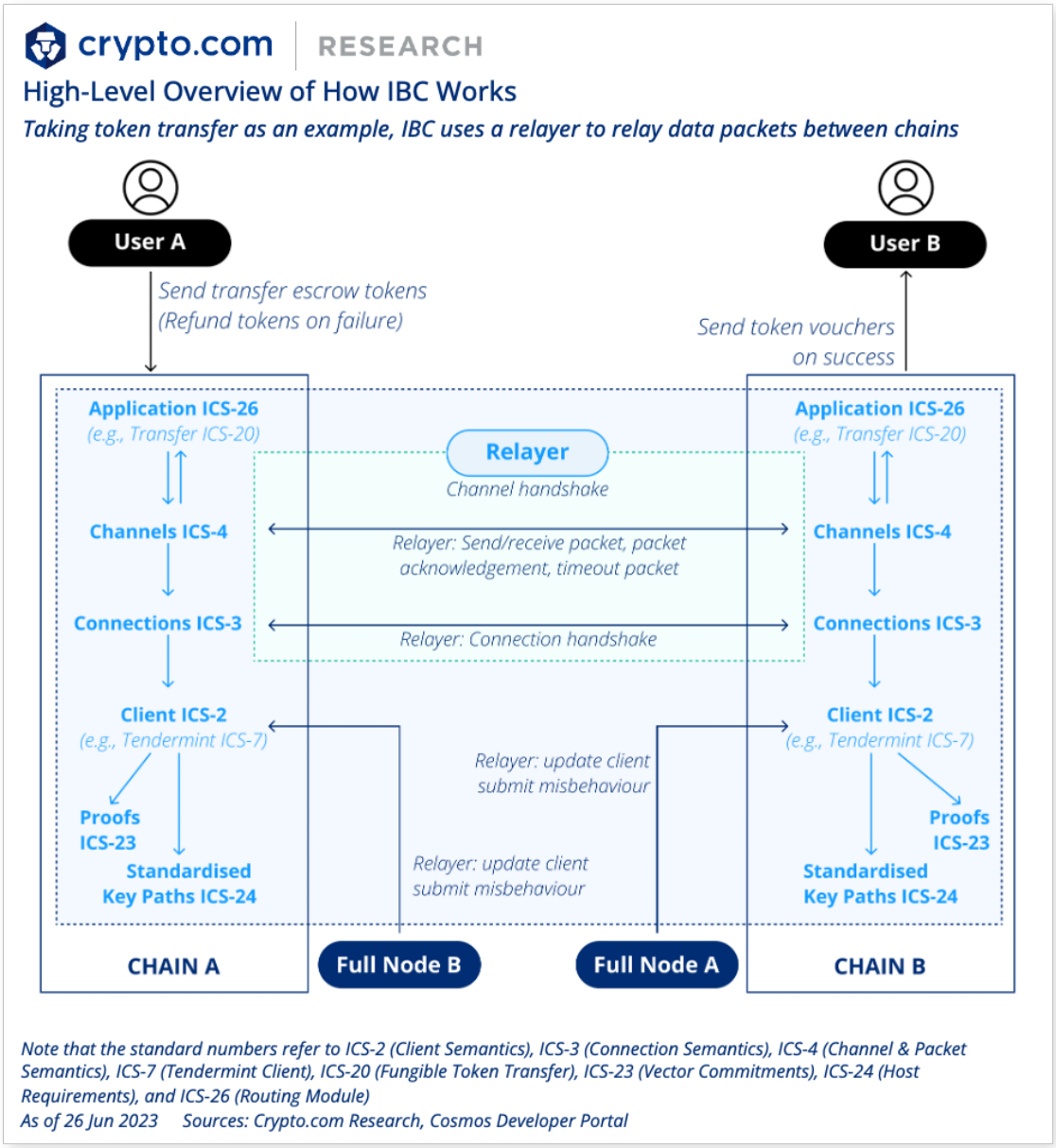
Launched in 2016 by Ignite (formerly Tendermint), Cosmos is designed as a decentralised network of independent parallel blockchains and it aims to be the 'internet of blockchains'. There are three major components in Cosmos: **CometBFT (Tendermint Core + ABCI), Cosmos SDK,** and **Inter-Blockchain Communication (IBC) protocol** (for cross-chain communication).

CometBFT is a platform that consists of a blockchain consensus engine (based on Tendermint Consensus) and a generic application interface called ABCI (Application BlockChain Interface). Tendermint Core provides the networking and consensus layers of a blockchain, while ABCI is the protocol that provides the interface where applications can be built and managed.

Cosmos SDK is a framework for building application-specific blockchains. The software development toolkit provides composable modules so developers can select and modify components to assemble their own blockchain.

IBC is an interoperability protocol for communicating arbitrary data between independent chains. The **Interchain Standards (ICS)** list the essential functions that IBC necessitates, but they don't impose any restrictions on the network topology or consensus algorithm. As a result, IBC is compatible with various blockchains or state machines. Unlike many trusted bridging technologies, IBC facilitates the transmission of data packets between blockchains in a permissionless manner. IBC aims to guarantee reliable, ordered, and authenticated general-purpose communication.

There are two important layers in IBC: the transport layer (TAO) and the application layer. The transport layer facilitates the secure connection establishment and packet authentication between chains, while the application layer specifies the packaging and interpretation of data packets by the sender and receiver chains.



Transport Layer

Messages communicated over IBC are transported within data packets. The transport layer is responsible for transporting, authenticating, and ordering these data packets. **Its key components are light clients, relayers, connections, and channels**:

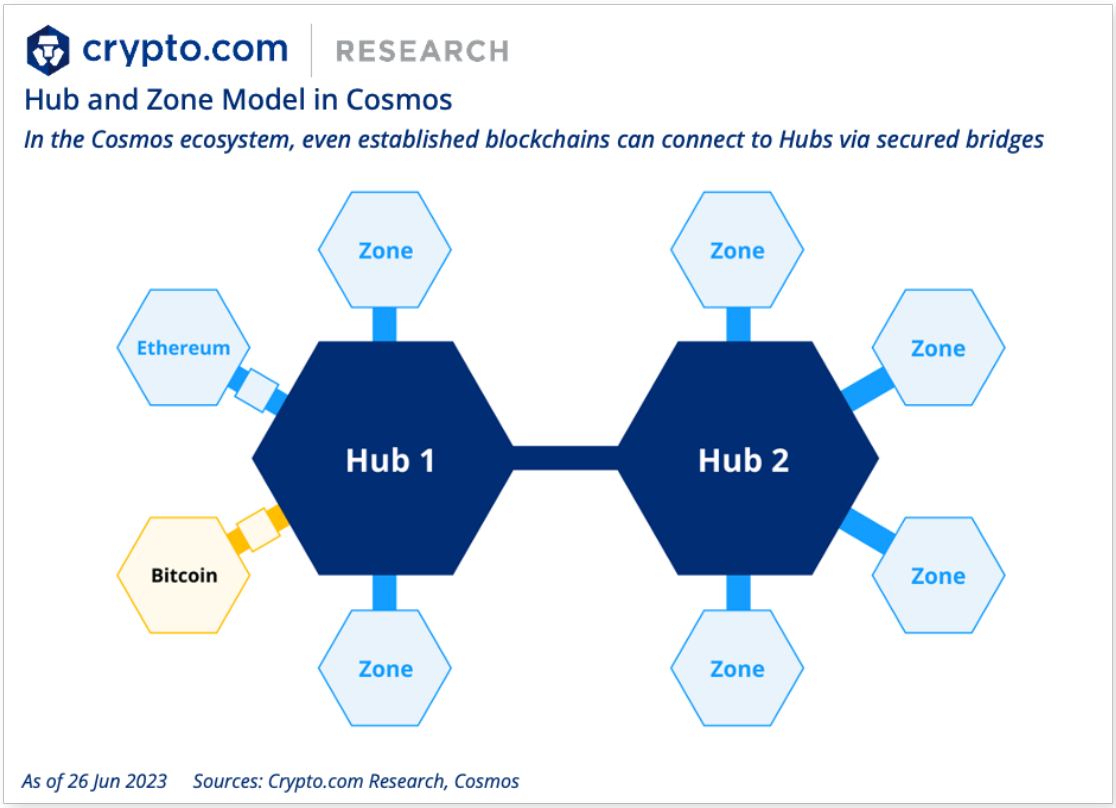
- **Light Client**: A light client is a lightweight representation of a blockchain. Unlike a full node, light clients don't keep a record of the complete history of all messages in a blockchain, nor do they carry out transactions. Instead, they are created to connect to a full node and authenticate block headers, which summarise the data stored within a block. This approach enables light clients to be storage- and computation-efficient. **It is this use of light clients in IBC**

that allow blockchains to exchange messages with one another without the need for a trusted third party.

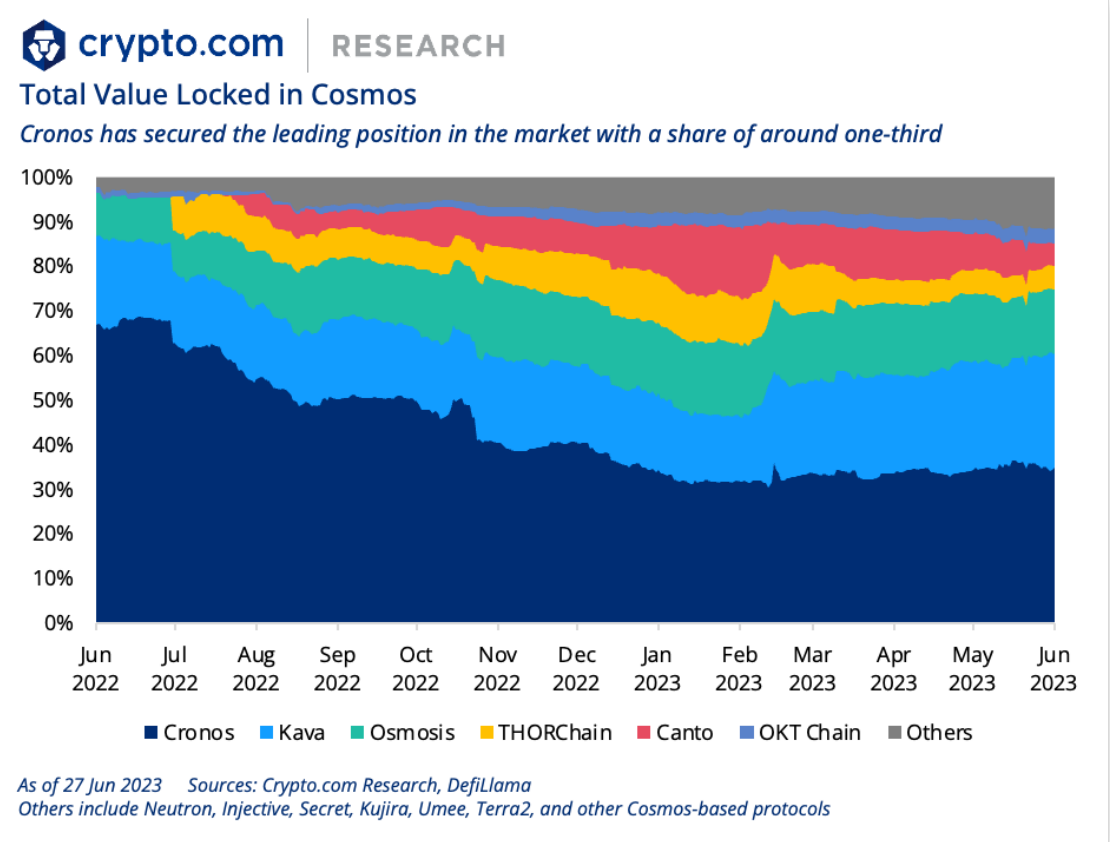
- **Relayers**: Relayer is a permissionless off-chain process, constantly observed for cross-chain messages.
- **Connection**: Connection is responsible for connecting light clients on two different chains.
- **Channel**: Channel serves as a pipe for transferring packets between modules on these different chains. Therefore, while connections are chain-specific, channels are module-specific.

*Read more about Cosmos in our exclusive feature report: **Layer-0: Deep Dive Into Interoperability Solutions**.*

The Cosmos ecosystem is made up of two types of blockchains: Hubs and Zones. Hubs are specifically designed to connect Zones by acting as routers and facilitating the flow of information. Zones are regular heterogeneous blockchains, and they only need to establish a single connection to a Hub to be interoperable with all other Zones connected to that Hub. Cosmos Hub (whose native token is ATOM) is the first hub and the central chain in the Cosmos ecosystem that connects other independent networks, including Cronos (CRO).



At the time of writing, there are 59 Zones (chains) in the Cosmos ecosystem. Cronos has the largest TVL market share at over one-third.



2.2 Polkadot

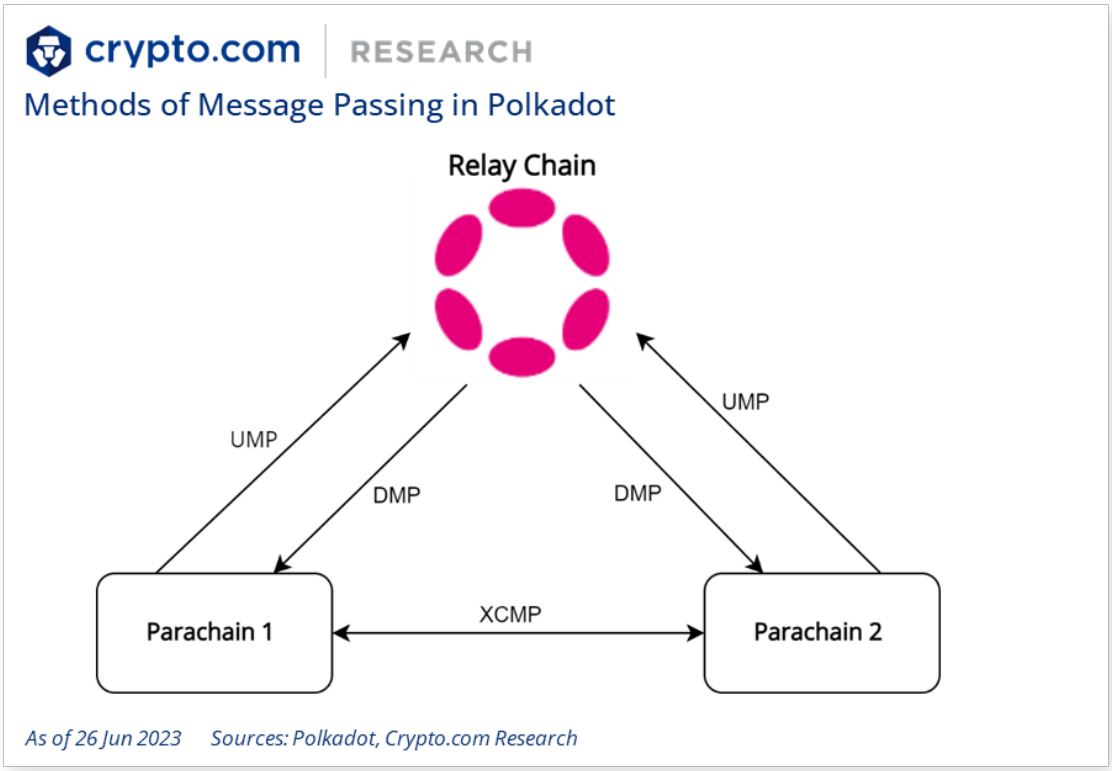
Created by Ethereum co-founder Gavin Wood in 2020, Polkadot (whose native token is DOT) claims to be a "scalable, heterogeneous multi-chain network" featuring components that enable security and interoperability. In a nutshell, Polkadot is a fully-sharded blockchain network powered by Nominated Proof-of-Stake — a consensus mechanism that uses voting to determine validators — and is designed to support various, interconnected Layer-1 blockchains known as **parachains**.

Polkadot is designed to operate two types of blockchains: the **relay chain** (single base platform) and **parachains** (application-specific chains).

- **Relay Chain:** This provides trustless interoperability among all parachains. It does not support application functions but instead hosts all validators and is tasked with securing, governing, and connecting these parachains.

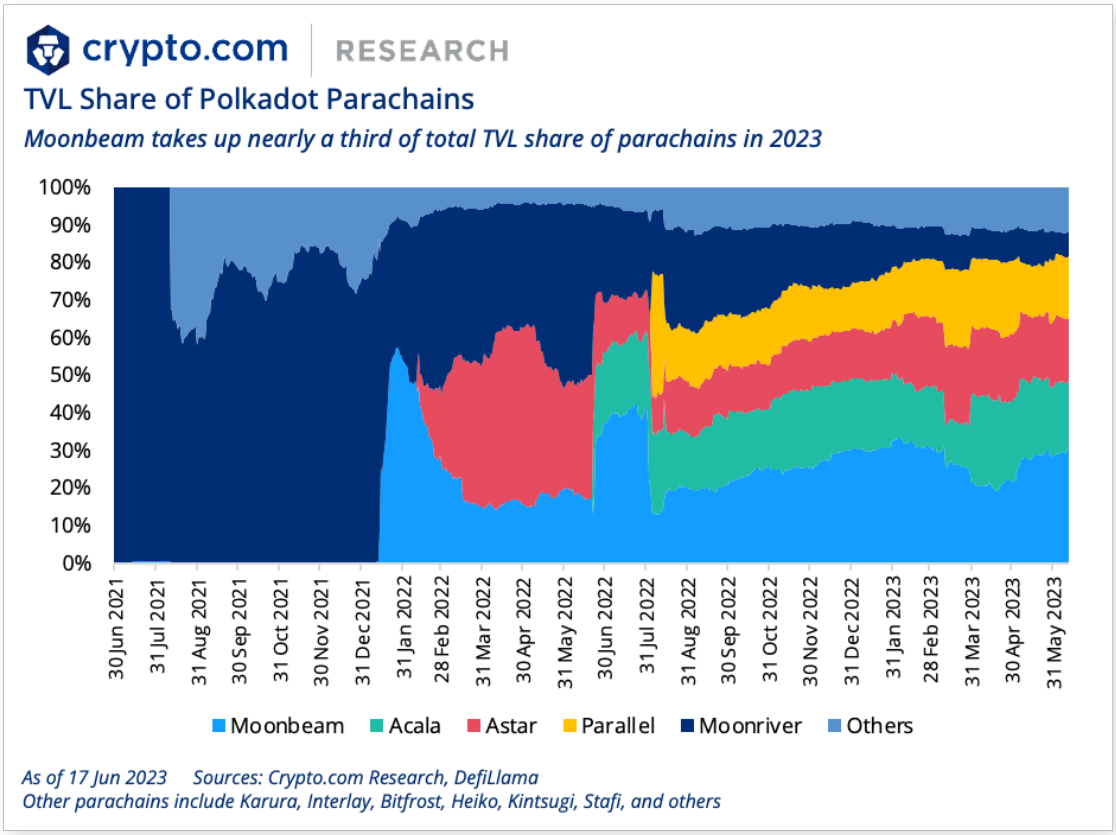
- **Parachains:** The independent parachains are application-specific chains that plug into a single base platform known as the Relay Chain. Parachains are heterogeneous Layer-1 chains — they have their own autonomy over their architecture, collator set, and governance system. Delegating the consensus responsibilities to the Relay Chain frees up parachains. This allows them to focus their resources and efforts to design and maintain specialised Layer-1 chains instead.

The core component for Polkadot's communication among parachains is through Cross-Consensus Message Format (XCM). This is a messaging format and language used to communicate between consensus systems. Like IBC in Cosmos, XCM is a generic format amongst chains with different consensus systems. However, XCM doesn't define the mechanism of how data is transmitted. Instead, it provides instructions for how to compose, send, and interpret cross-chain messages. **Cross-Chain Message Passing (XCMP)** is the actual network-layer protocol to deliver XCM-formatted messages to other participating parachains.



Read more about Polkadot in our exclusive feature report: ***Layer-0: Deep Dive Into Interoperability Solutions*****.**

Some of Polkadot's notable parachains are **Moonbeam, Astar, Acala, Parallel, and Moonriver**. Their share of the total value locked (TVL) in parachains is shown below:



2.3 Avalanche

Avalanche (whose native token is AVAX) is a Proof-of-Stake smart contract platform that provides infrastructure for building decentralised applications and blockchains. It was founded and launched by Ava Labs in 2019, and one of its unique value propositions is that it offers fast time-to-finality and low fees.

Avalanche can be seen as a heterogeneous network of blockchains. The app-specific chains in the Avalanche ecosystem are called subnets. A subnet is an independent network that establishes its own guidelines for membership and token economics. It comprises a flexible group of Avalanche validators collaborating to reach a consensus on the status of one or multiple blockchains. Each blockchain is verified by only one Subnet, but a Subnet can verify multiple blockchains.

Avalanche's Primary Network is a special subnet running three blockchains:

- **X-Chain**: Avalanche *Exchange* Chain, which handles sending and receiving funds (*note that X-Chain is a directed acyclic graph, or DAG, and is not used in DeFi platforms*).
- **P-Chain**: Avalanche *Platform* Chain, which works as the metadata blockchain that keeps track of subnets, where new subnets are created, and where Avalanche validating and staking occur.
- **C-Chain**: Avalanche *Contract* Chain, the default smart contract chain and the main blockchain where smart contracts and applications are built on (*EVM blockchain*).

Subnets are all connected through the Primary Network (a subnet in itself), serving as a scaling solution to the network and diverting a significant portion of the traffic congestion away from the Primary Network. They also offer customisable options to blockchain developers, even with their own virtual machines — something that Layer-2 solutions typically do not offer.

As part of its AvalancheGo Banff5 upgrade, Avalanche introduced a **communication protocol for subnets called Avalanche Warp Messaging (AWM)**. AWM is a critical component of how interoperability is facilitated in the network, as it allows subnets to natively share data and crypto assets. Previously, this could only be achieved through the use of complex bridge systems.

In 2023, the network experienced significant growth across several important measures. For instance, the number of daily active addresses has risen from approximately 45,000 in the first quarter to over 100,000 in June. This increase can be attributed to the expansion of stablecoins and the rapid deployment of subnets in recent months, which resulted in greater utility and activity. At present, there are approximately 21 subnets available, with most featuring blockchain gaming and DeFi applications.

3. Emerging Layer-0 Protocols

3.1 LayerZero

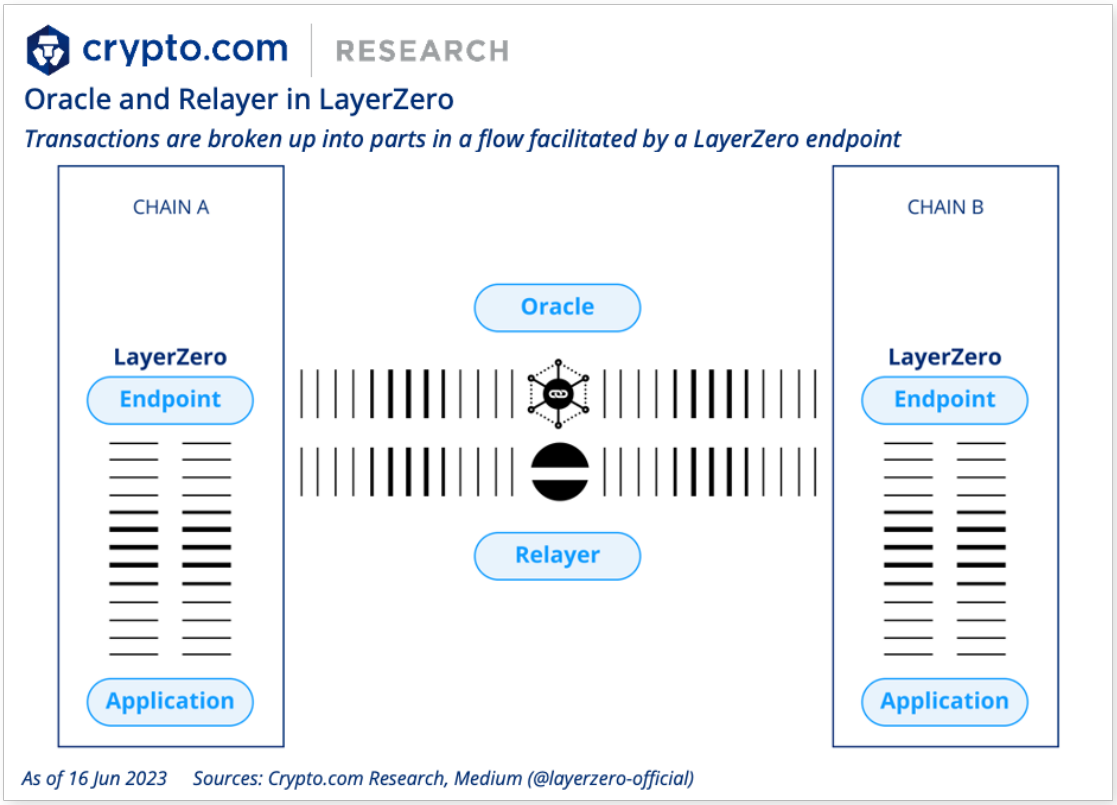
LayerZero Labs aims to build an ”omnichain interoperability protocol” that unifies decentralised applications across multiple blockchains in the form of the LayerZero protocol. It is a cross-chain messaging layer for smart contracts (via endpoints) to natively communicate between blockchains.

LayerZero is a protocol that mainly operates off-chain via ultra light nodes, smart contracts that securely transfer messages between chains. Ultra light nodes introduce a new model for blockchains, **minus the hefty cost of running light nodes while being more secure than running a sidechain-based model**.

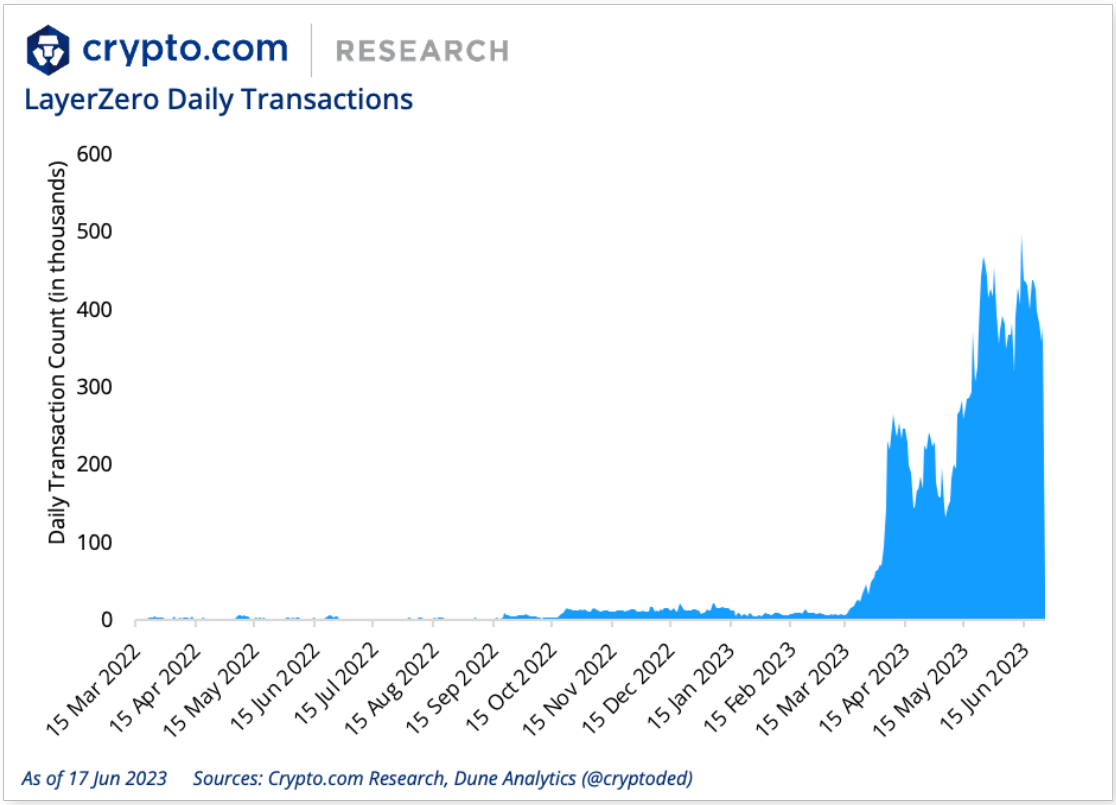
The key concept underpinning LayerZero secure data transfer lies on two off-chain entities represented by the **Oracle** and **Relayer**.

- The Oracle (Chainlink and Band) is the entity that provides the block header, and the Relayer provides proof of said transaction. LayerZero endpoints are the other key components to these transactions, which are found on each supported chain. These endpoints serve as the user-facing interface that lets users send a message using the protocol.

- The job of the Oracle and Relayer is to pass messages from one endpoint to another. The Oracle forwards a block header from Domain A to Domain B, while the Relayer passes in parallel transaction proof from A to B. If the two match and the proof is cross-verified with the header, then the message can be considered as successfully forwarded to the destination domain.



LayerZero has been gaining traction, as shown in the growth of daily transactions on the protocol since March 2023:



3.2 zkLink

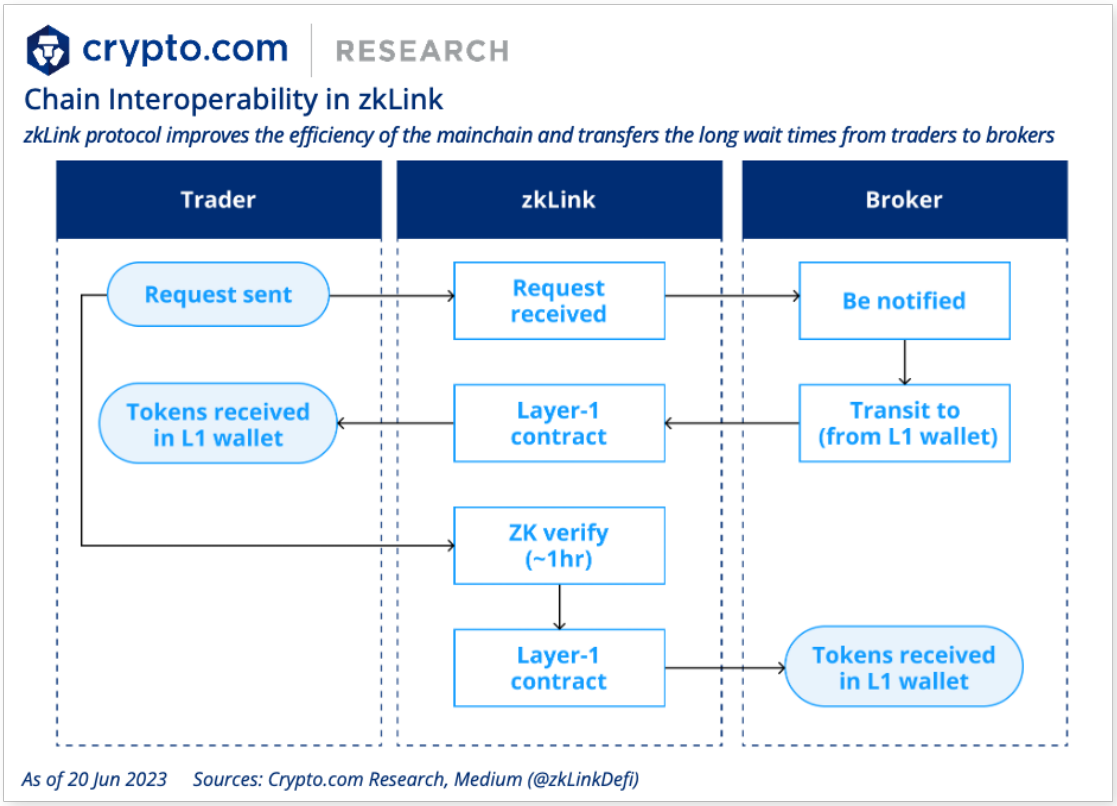
zkLink is a trading-focused multichain Layer-2 scaling solution. It takes a more unique approach to interoperability compared to previous projects mentioned: It provides unified liquidity through **zero-knowledge proof technology (ZK-SNARKs)** to enable secure, scalable, and interoperable transactions across multiple blockchains. Its ecosystem is made up of interconnected Layer-1 and Layer-2 chains that lets developers and traders leverage unified liquidity from isolated chains.

zkLink aims to build a 'DeFi-verse' by providing multi-chain trading infrastructure. Its key features are:

- **Zero-knowledge proofs (ZK-SNARKs)**: ZK-SNARK is a cryptographic technique that allows for secure and confidential transactions. ZK-SNARKs are used by zkLINK to reduce the amount of data that needs to be transmitted between blockchains. In turn, this makes the network more efficient. This also makes zkLink the first protocol to apply ZK-SNARKs to multichain scenarios.

- **Cross-chain liquidity aggregation**: zkLink allows users to trade assets across multiple blockchains. This is done by aggregating liquidity from different blockchains into a single pool.

Through ZK-SNARKs, zkLink is able to compress transaction data and aggregate liquidity from different chains into a single pool. This potentially revolutionises the way trading is done on most DeFi venues: zkLink aggregates the liquidity on third-party Layer-1 decentralised exchanges (DEXs) first. Then, the most cost-effective route and best exchange rate will automatically be located for traders. Lastly, tokens are 'officially' swapped on zkLink Layer-2 liquidity pools. This ultimately aims to provide a secure and scalable solution to transfer assets between chains, and a seamless trading experience for users.



*Read more about ZK-Rollup technologies in our feature report: **The Development of ZK-Rollups**.*

4. Conclusion

In summary, Layer-0 protocols represent a promising new approach to tackling the scalability and interoperability issues facing the blockchain industry. By acting as the foundational infrastructure upon which independent Layer-1 blockchains

can be built, Layer-0 protocols aim to help unlock the full potential of the blockchain ecosystem.

Having the ability to build their own Layer-1s without needing to focus on consensus and security gives developers tremendous flexibility in choosing token models, optimising for different tradeoffs, and curating their own applications and ecosystems.

Interoperability solutions provided by Layer-0 networks allow independent blockchains to communicate and exchange value. This empowers developers to build applications that span multiple chains. Without interoperability, individual blockchains would operate in isolation and their benefits would be limited.

Promising Layer-0 projects like Cosmos, Polkadot, Avalanche, LayerZero, and zkLink represent different approaches to achieving multichain interoperability. However, with each of these solutions' unique architecture comes a unique set of constraints — and therefore, some risks and drawbacks. For example, Avalanche's overlapping subsets of its validators act as the security on the subnets. This overlapping topology translates to different levels of security across connected chains: It opens the network to inter-shard attacks as messages from one (less secure subnet) could affect a transition on another (more secure subnet).

Additionally with LayerZero, it only works as long as both the off-chain entities (Oracle and Relayer) are not colluding. A bad actor could theoretically reconfigure applications deployed on LayerZero so that these two components can either be bypassed or controlled by the same party, which can make it vulnerable to theft.

In the coming years, Layer-0 protocols have the potential to usher in a new wave of blockchain innovation by enabling the growth of multiple specialised Layer-1 blockchains that interoperate seamlessly. Several technical and adoption challenges still remain, but Layer-0 could *lay* the foundation for a more open, productive, and composable blockchain ecosystem.

Read our exclusive report ***Layer-0: Deep Dive Into Interoperability Solutions*** to explore Layer-0 and blockchain interoperability in greater detail. *Become a Crypto.com Private member and get access to the report today.*

References

Cointelegraph. “What’s the difference between blockchain layers L0 and L1?” *Cointelegraph.com*, https://cointelegraph.com/learn/whats-the-difference-between-blockchain-layers-l0-and-l1/. Accessed 20 June 2023.

Dela Rosa, Olivia. “Layer-0: Deep Dive Into Interoperability Solutions.” *Crypto.com/Research*, https://www.crypto.com/vip/report/signin/1/. Accessed 20 June 2023.

Wu, William. “The Development of ZK Rollups.” *Crypto.com/Research*, https://crypto.com/research/zkrollup/. Accessed 3 July 2023.

e. contact@crypto.com

Published on 3 Jul 2023