

Darwinia Genepaper v3

Cross-chain programmable network

Revised 2023-06

Contents

Contents	2
Background	3
Solutions	4
Darwinia Chain	4
Native Token	5
EVM	7
Governance	7
Treasury	8
Consensus	8
Collators	9
Parachain XCMP Messaging	11
Darwinia Msgport	13
Architecture	13
Use Cases	15

Background

The blockchain industry has been evolving rapidly, witnessing the emergence of numerous blockchain networks. As proponents of a multi-chain future, we recognize the increasing need for interoperability among these diverse chains. While addressing this interoperability challenge, our focus extends beyond safety to encompass versatility, generalizability, and programmability.

Currently, several service providers offer token bridges for token holders. However, most of these solutions are limited to specific assets or use cases, lacking the desired level of generalization and programmability. Moreover, the complexity arising from layering application layer smart contracts on top of underlying cross-chain solutions further compromises security. To cater to the needs of cross-chain Dapp developers, there is a requirement for layered protocols, including a purpose-built, generalized, and programmable cross-chain messaging layer to support their applications.

Similar to how Ethereum revolutionized the industry by introducing smart contracts, transforming blockchains into programmable platforms, and paving the way for the Dapp boom and DeFi summer, we anticipate a significant surge in blockchain functionality driven by new and emerging cross-chain messaging technologies.

Darwinia aims to spearhead this trend with its cross-chain messaging infrastructure. It offers a dependable and programmable cross-chain platform for decentralized applications, empowering developers with Darwinia Msgport, a solution that facilitates seamless integration of cross-chain functionality into their own Dapps.

Solutions

The Darwinia Network consists of two solutions: Darwinia Chain and Darwinia Msgport. Darwinia Chain is an EVM-compatible smart contract platform that operates as a parachain on Polkadot, offering robust security and interoperability with Ethereum and other chains. Darwinia Msgport provides a flexible cross-chain messaging architecture, allowing seamless communication and interaction between different blockchains. Together, these solutions enable developers and users to build and use decentralized applications in a multi-chain environment.

Darwinia Chain

Darwinia Chain is a smart contract platform that offers compatibility with the Ethereum Virtual Machine (EVM) and leverages the strong security provided by the Polkadot network.

As a Polkadot Parachain, Darwinia Chain serves as a secure and programmable bridge between the Polkadot ecosystem and EVM-based chains such as Ethereum, Arbitrum, Binance Smart Chain, and more. Darwinia Chain operates as a Parachain on the Polkadot network, while its canary network, Crab Chain, functions as a Parachain on the Kusama network.



Native Token

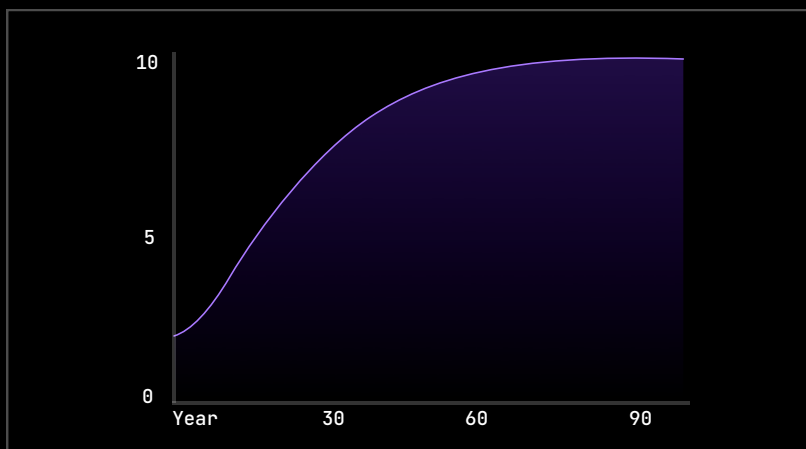
The native token for the Darwinia Chain is RING, RING can be used for network fees, collateral for staking, relayer fee market, and governance.

Network fees include transaction fees, message fees, smart contract gas, cross-chain gas and more.

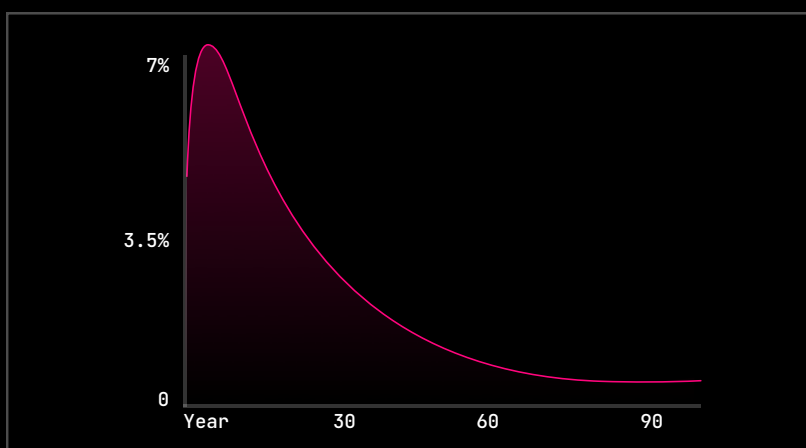
Supply Curve

RING's initial supply (INITIAL_SUPPLY) is 2 billion, after the initial supply is generated, the block reward of year N is $1 - (99/100)^{\sqrt{N}}$ of total remaining issuable, until reaching the hard cap of the supply which is 10 billion.

Total remaining issuable RING = HARD_CAP - CURRENT_SUPPLY



Total Supply (Billion)



Annual Inflation Rate

Supply Quick Calculator

Total Supply	Total Remaining Issuable	Year	Issuable this year/Total remaining	Issuable this year	Inflation Rate
20	80	1	0.01	0.8	4.00%
20.8	79.2	2	0.014112789	1.11773288	5.37%
21.91773288	78.08226712	3	0.017257054	1.347469885	6.15%
23.26520276	76.73479724	4	0.0199	1.527022465	6.56%
24.79222523	75.20777477	5	0.022222592	1.671311704	6.74%
26.46353693	73.53646307	6	0.024317638	1.788233108	6.76%
28.25177004	71.74822996	7	0.02624027	1.882692906	6.66%
30.13446295	69.86553705	8	0.028026407	1.958079974	6.50%
32.09254292	67.90745708	9	0.029701	2.016919383	6.28%
34.1094623	65.8905377	10	0.031282215	2.061201934	6.04%
36.17066424	63.82933576	11	0.032783764	2.092565869	5.79%
38.26323011	61.73676989	12	0.034216302	2.112403946	5.52%
40.37563405	59.62436595	13	0.0355883	2.121929846	5.26%
42.4975639	57.5024361	14	0.036906629	2.122221074	4.99%
44.61978497	55.38021503	15	0.038176948	2.114247617	4.74%
46.73403259	53.26596741	16	0.03940399	2.098891647	4.49%
48.83292424	51.16707576	17	0.040591755	2.076961416	4.25%
50.90988565	49.09011435	18	0.041743665	2.049201292	4.03%
52.95908694	47.04091306	19	0.042862671	2.016299179	3.81%
54.97538612	45.02461388	20	0.043951341	1.978892142	3.60%

EVM

Darwinia Chain is an EVM (Ethereum Virtual Machine)-compatible blockchain, designed to ensure seamless integration with the Ethereum ecosystem. This compatibility allows developers and users to leverage existing infrastructure, tools, and knowledge developed for Ethereum, providing a smooth experience for both Ethereum and Darwinia Chain users.

By supporting the same opcode set and execution model as the EVM, developers can rely on established Ethereum standards and programming languages to build and deploy their applications on Darwinia Chain. This compatibility enables Darwinia Chain to tap into the diverse range of applications, services, and innovations already thriving within the Ethereum community.

Governance

The governance structure of Darwinia Chain is derived from Polkadot, incorporating two distinct collectives: the Council and the Technical Committee.

The Council is an on-chain collective responsible for representing passive stakeholders. Its role involves proposing significant changes.

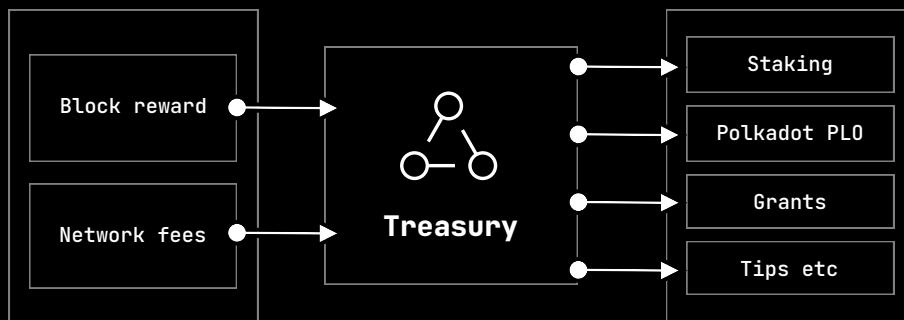
The Technical Committee (TC) aims to safeguard against malicious referenda, implement bug fixes, reverse faulty runtime updates, or add new but battle-tested features. The TC can fast-track proposals using the Democracy pallet and is the only origin that can trigger the fast-tracking functionality. We can think of the TC as a "unique origin" that cannot generate proposals but fast-track existing ones. Fast-tracked referenda are the only referenda that can be active alongside another active referendum. Thus, with fast-tracked referenda, it is possible to have two active referendums simultaneously. Voting on one does not prevent a user from voting on the other.

Treasury

The public referenda chamber in democracy pallet is one of the three bodies of on-chain governance. The other two bodies are the council and the technical committee.

The primary purpose of the Treasury is to finance treasury proposals, which encompass activities such as staking, budgeting for Polkadot Parachain Lease Offering (PLO), grants, and tips, among others.

Management of the Treasury is entrusted to the on-chain governance module, ensuring transparency and accountability in the allocation and utilization of funds.



Consensus

Darwinia functions as a Polkadot parachain and benefits from the shared security provided by the Polkadot Relay Chain, which assumes the responsibility for block production. Instead of producing blocks directly, Darwinia's blocks are sequenced and transmitted to Relay Chain Validators by Collators.

To maintain its status as a Polkadot parachain, the Darwinia Treasury participates in an on-chain auction to secure its Polkadot slot. This auction requires locking up a portion of DOT tokens for the duration of the lease.

- Data Availability

The blocks of Darwinia Chain are added to the Relay Chain through the Inclusion Pipeline, a component of the Parachain Protocol of Polkadot. This mechanism ensures that the data availability of Darwinia Chain is safeguarded by the Polkadot Relay Chain.

- State Validation

The validation of blocks follows Polkadot's Approval Process. Initially, the added block is in a pending state. It is then subject to approval by selected Polkadot Validators, and once approved, the block will be finalized on the Relay Chain.

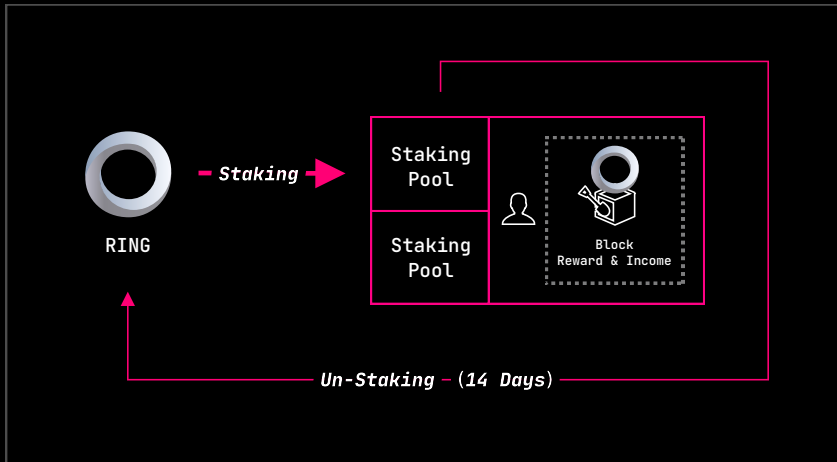
Collators

In Darwinia's block production mechanism, there are two key roles: [parachain collators](#) and relay chain validators. The parachain collators are responsible for collecting transactions and state transition proofs. They then send these blocks to the relay chain validators for finalization. The relay chain validators verify the blocks and subsequently produce relay chain blocks.

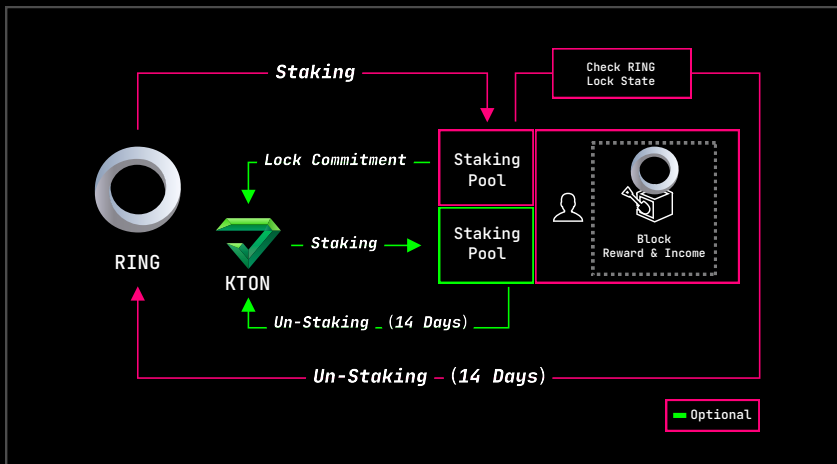
Darwinia Staking plays a crucial role in securing the Darwinia Chain while also capturing its network value. By participating in staking, users contribute their tokens and actively engage in the network's collator mechanism, which enhances the network's liveness and prevent transaction censorship.

Collator Staking

The treasury distributes RING tokens from partial of the new supply as incentives to participants in the Staking.



Basic Model



Advanced Model

KTON

In order to incentivize long-term commitments and token pledging, users have the option to lock their RING tokens for a duration of up to 36 months during the Staking process. As a reward for participating in Staking, the system will provide users with KTON

tokens. It's important to note that during the committed pledge period, users are unable to unlock their RING tokens unless they destroy triple the amount of KTON tokens from their accounts as a penalty.

Therefore, during the RING Staking process, users have the choice to lock their RING tokens for a specific period and receive KTON tokens in return. Initially, the supply of KTON tokens is zero.

KTON tokens can also be pledged to gain Staking power and participate in POS mining. Users can choose to Stake by pledging their KTON tokens. However, if a user decides to withdraw their staked KTON, the corresponding POS mining process will be halted, and it will take 14 days for the unbonded KTON tokens to become available.

Parachain XCMP Messaging

A Polkadot parachain is a sovereign blockchain that runs concurrently within the Polkadot Relay Chain. Parachains have the capability to serve as DeFi platforms, smart contract platforms, stablecoin protocols, liquidity platforms, privacy-focused app-chains, and more. They operate independently with their own governance and can interact with other parachains and the Polkadot network through XCMP (Cross-Chain Message Passing) messaging.

Darwinia Chain utilizes XCMP to establish communication with other parachains connected to the Polkadot network. XCMP is a protocol that enables the transfer of arbitrary data or assets between parachains, facilitating cross-chain interoperability and composability.

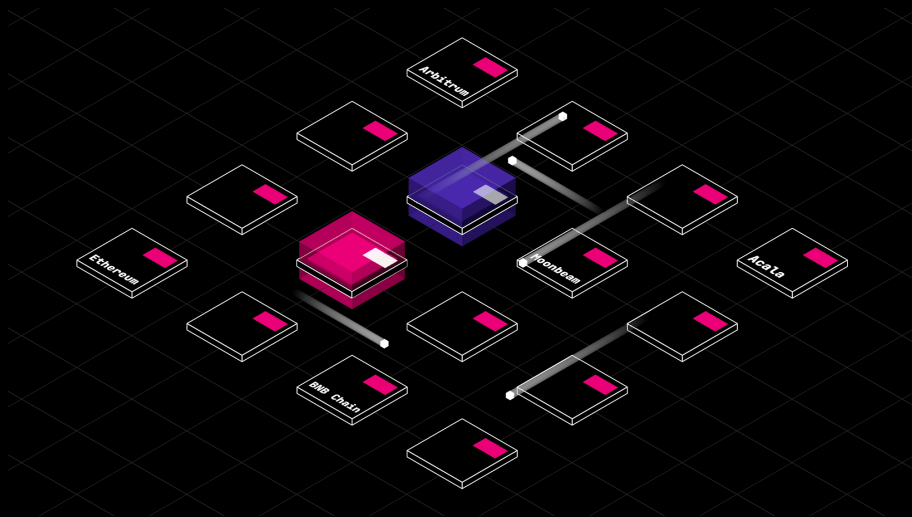
The messages transmitted through XCMP are encoded in XCM (Cross-Consensus Message), which serves as a standardized language for describing cross-chain transactions. Through the utilization of

XCMP, Darwinia gains the ability to access the features and services offered by other parachains.

Darwinia Msgport

Darwinia Msgport is a set of smart contracts designed for facilitating the exchange of messages between different chains. It enables cross-chain interoperability by allowing other smart contracts to send and receive in-chain message calls.

By leveraging these capabilities, Msgport-based cross-chain Dapps offer a user experience that closely resembles that of traditional single-chain Dapps. Darwinia Msgport opens up possibilities for a wide range of truly multi-chain Dapps.

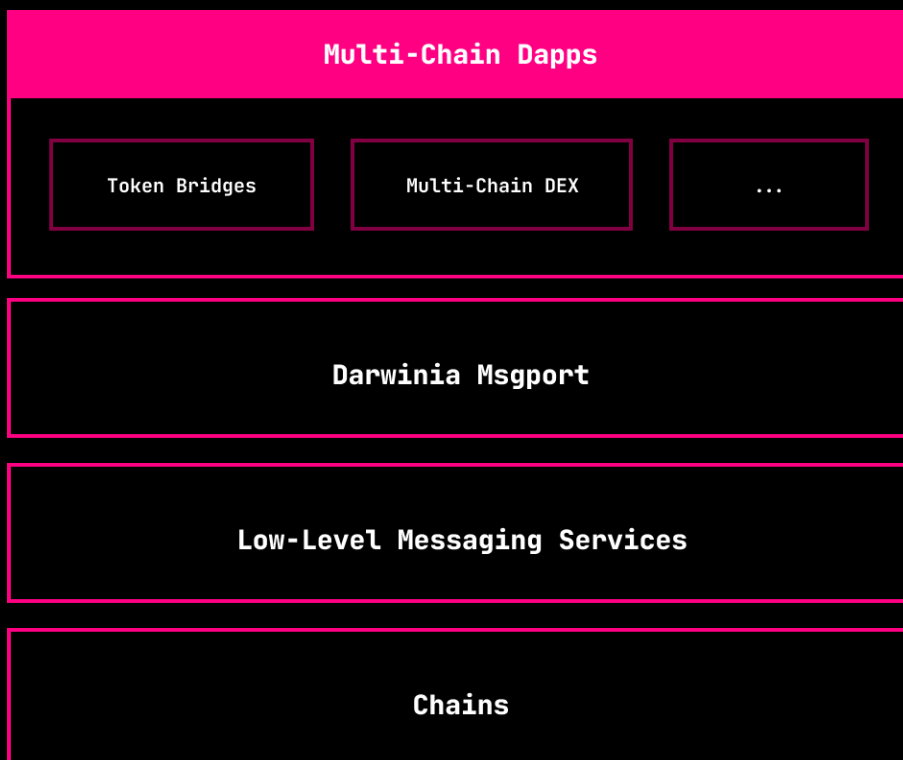


Architecture

Darwinia Msgport is built upon a flexible and modular architecture, allowing users to harness various cross-chain messaging layers that best suit their specific needs. Msgport provides support for sending arbitrary messages through different low-level cross-chain messaging services.

These underlying cross-chain messaging services offer diverse capabilities. Some may have low fees, while others prioritize high security at the cost of slower transaction speeds. Msgport is designed to select the most suitable cross-chain messaging layer for users based on a predefined algorithm, or it can allow users to manually choose their preferred cross-chain layer.

Through in-chain message calls to Msgport, smart contracts can establish communication and interaction across heterogeneous chains. Msgport employs distinct low-level messaging protocols to facilitate the transmission of messages between different blockchain networks, including EVM chains, Polkadot-based chains, and others.



Use Cases

Multichain Gaming and Metaverse

Darwinia Msgport facilitates cross-chain communication for applications like Evolution Land, a blockchain-based virtual management game with multiple continents on different chains. Users can transfer tokens and NFTs across chains, enabling seamless gameplay experiences across different blockchain networks.

Cross-chain Assets Bridges

Darwinia Msgport powers cross-chain asset bridges, enabling the transfer of tokens of different standards (such as ERC-20, ERC-721, etc.) between blockchains. [Helix Bridge](#), for example, utilizes Darwinia Msgport to implement some of its asset cross-chain bridges.

NFT Marketplace

Users can participate in NFT auctions on one chain, even if they belong to a completely different chain, allowing for increased accessibility and participation in NFT marketplaces.

Multiverse

With Darwinia Msgport, users can interact across different metaverses, bridging the gap between various virtual worlds and creating a unified multiverse experience.

DEX (Decentralized Exchange)

Darwinia Msgport enables decentralized exchanges to operate across multiple chains, allowing users to seamlessly exchange assets between different blockchain networks within a single transaction.

DAO Governance

Through Darwinia Msgport, decentralized autonomous organizations (DAOs) can establish unified multi-chain governance mechanisms without the need to move assets between different chains, facilitating efficient decision-making and coordination.

Aggregator

Darwinia Msgport empowers users to manage multi-chain assets from a single chain, providing an aggregation layer that simplifies asset management and monitoring across different blockchain networks.

Loans

Users can utilize Darwinia Msgport to pledge assets on one chain and lend them on a different chain, enabling cross-chain lending and borrowing functionalities.