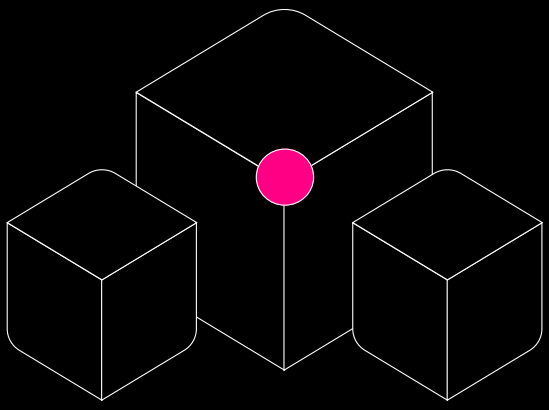


Darwinia Genepaper v2

Universal Cross-Chain Messaging Network

Revised 2022-06-20

Contents

Background

The blockchain industry has been evolving at a rapid pace, with more and more blockchain networks coming online every day. As believers and supporters of a multi-chain future, we foresee that there will be greater and greater need for interoperability between these different chains. Our focus while building a solution to this interoperability problem will not only be on safety, but versatility in the way that it will be generalized and programmable.

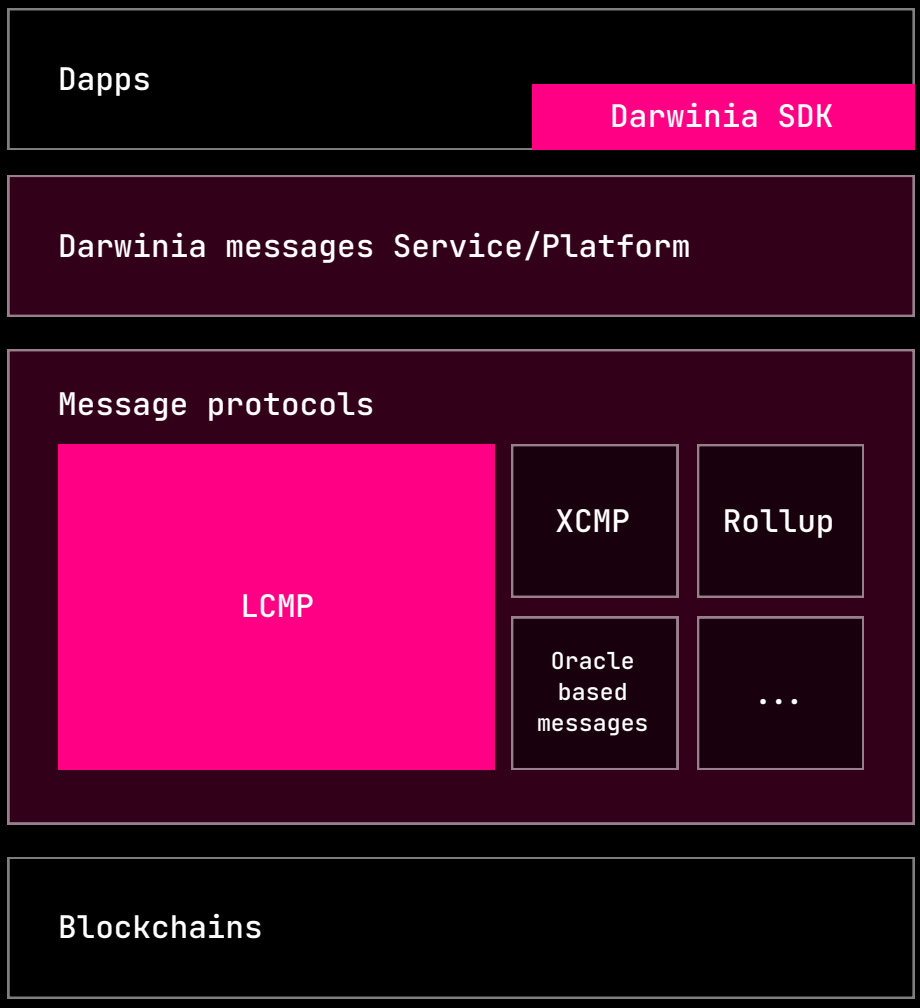
At the present time, several service providers provide various token bridges for token holders, but most focus on specific assets or use-cases, and are not generalized or programmable; and stacking application layer smart contracts on top of underlying cross-chain solutions complicate matters further, and make them less secure. Cross-chain Dapp developers need layered protocols, including a single-purpose, generalized, and programmable cross-chain messaging layer to serve their applications.

In the same way Ethereum transformed the industry through the introduction of smart contracts, which turned blockchain into a programmable platform and paved the way for the Dapp boom and DeFi summer; likewise, there will be an explosion of growth in blockchain functionality based on new and emerging cross-chain messaging technologies.

Darwinia will help kickstart this trend with its cross-chain messaging infrastructure. Darwinia provides a reliable and programmable cross-chain platform for decentralized applications, and empowers developers with a

software development kit (SDK) which allows them to easily integrate cross-chain functionality into their own Dapps.

Architecture



Blockchain networks are becoming layered and specialized, and while Layer 0 chains like Polkadot and Ethereum 2.0 beacon chain offer shared consensus and security, Layer 2 rollup and Application-specific chains further enhance scalability in their specific domains.

As cross-chain interoperability comes into focus, many different cross-chain messaging solutions are under

development, including Darwinia's Light-Client Message Protocol (LCMP), Polkadot's Cross-Consensus Message Protocol (XCMP), and others based on oracles, shards, Multi-Party Computation (MPC), etcetera.

Considering these circumstances, Darwinia provides developers with a consistent and easy to use message service via our SDK by further developing and integrating many of the existing cross-chain messaging protocols into our cross-chain infrastructure.

Decentralized application developers are able to use Darwinia SDK to build cross-chain Dapps from the ground up, and those desiring integration can increase the extensibility of their cross-chain messaging systems by utilizing Darwinia to support additional cross-chain messaging protocols.

Chains

Darwinia offers a number of different chains for development of messaging infrastructure and Dapp deployment, each with its own features and benefits.

Darwinia Chain is designed to be the primary chain for tokens and governance, main communication hub and routing point of LCMP, and will support most on-chain light clients for other public chains.

Darwinia Parachain is designed to be protected by the shared security of the Polkadot Relay Chain. It will integrate Polkadot’s XCMP, open channels with other parachains, and connect to Darwinia Chain via LCMP.

Darwinia Smart Chain (DSC) is an EVM-compatible smart contract platform hosted on Darwinia Chain, and is designed to provide greater programmability for Dapps and cross-chain users.

Darwinia Chain

Darwinia Network is a public chain that can operate independently with its own consensus and security model, with its core business and application services, including cross-chain functionality of each application chain, controlled by Darwinia Network itself.

Darwinia Smart Chain

Darwinia Smart Chain (DSC) adds an Ethereum-Compatible layer atop Darwinia Chain and provides users with the ability to create and interact with solidity smart

contracts. The DSC node provides an Ethereum-compatible RPC endpoint for reading chain states and sending transactions, which are committed to an Ethereum blockchain hosted on Darwinia Chain. Darwinia Smart Chain provides an intuitive interface and entry point for existing projects in the Ethereum ecosystem to migrate to Darwinia Network.

Darwinia Parachain

Darwinia Parachain is a branch of Darwinia Network that benefits from the shared security of the Polkadot Relay Chain, and connects to other parachains on Polkadot using XCMP, the Cross-Consensus Message Protocol.

At the same time, Darwinia Parachain will connect to Darwinia Chain through LCMP, a cross-chain messaging protocol based on on-chain light clients operating between chains with independent consensus.

Darwinia Parachain will use and share RING with Darwinia Chain, which will be used as the network native token. Tokens will be transferable from Darwinia Chain to Darwinia Parachain through bridges based on LCMP.

Darwinia Parachain is designed to take on a minimal role in the network in order to address sustainability in terms of parachain slot availability and current PLO incentivisation strategy, so many parachain functions such as governance, etc. will be offloaded to Darwinia Chain via LCMP. When it comes to routing and redirecting LCMP messages between connected chains, however, Darwinia Parachain will play an important role by combining and wrapping XCMP & LCMP messages.

Crab Chains

Crab Network (Crab) is an economically incentivized canary network secured by real value at stake, and is composed of three chains:

- Crab Smart Chain (CSC): Ethereum-compatible
- Crab Parachain (CP): Won the 22nd Kusama parachain slot
- Crab Chain (CC): Substrate-based

LCMP

The Light-client Cross-chain Messaging Protocol (LCMP) developed by Darwinia, is a cross-chain messaging protocol that allows blockchains with varied consensus models to send messages to one another. On the protocol layer, Darwinia is not strictly limited to the use of LCMP. It is only one of many cross-chain messaging protocols supported by Darwinia Network.

LCMP is based on an on-chain super light client which makes for a decentralized and highly secure bridge design that guarantees valid message delivery without placing trust in intermediary entities. Developers need only to trust the consensus of the source and destination chains, and the smart contract code, which is open source. It is a general purpose protocol which allows blockchains to exchange arbitrary messages between one another, as long as they have established messaging channels with each other. Being highly generalized, LCMP is extensible, and useful between all blockchains that support smart contracts; most of the blockchains that exist today.

Message SDK

The Message SDK provides the easiest method by which decentralized applications can become cross-chain applications. By simply importing a library, developers can integrate cross-chain messaging capabilities into their new or existing Dapps.

The Message SDK hides many details of LCMP and other protocols from developers, reducing the difficulty of using these cross-chain protocols. The Message SDK abstracts away the complicated cross-chain bits, and allows developers to focus on integrating only the capabilities they need, from the blockchains that provide them.

Using the Message SDK, developers are able to build multi-chain Dapps as easily as they would ordinary Dapps, by picking and choosing the features and functionality they need from any supported chain, and integrating them all into a single smart contract deployment.

Economic Model

RING Token

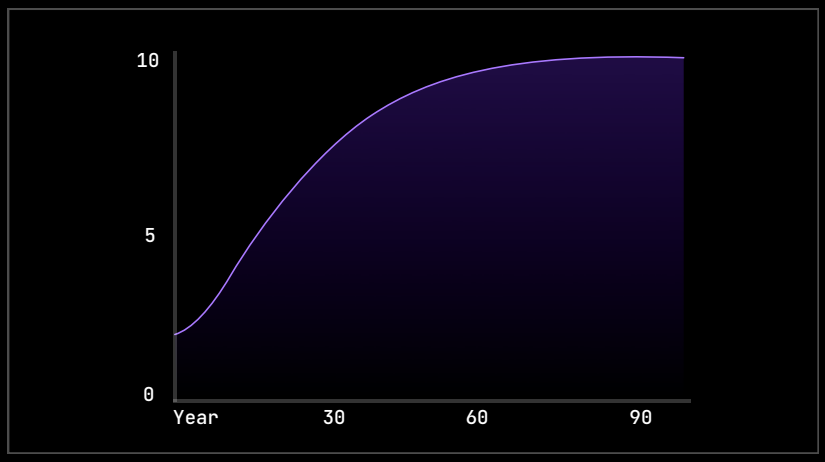
The native token for the Darwinia Network is RING, RING can be used for network fees, collateral for staking, relayer fee market, and governance.

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

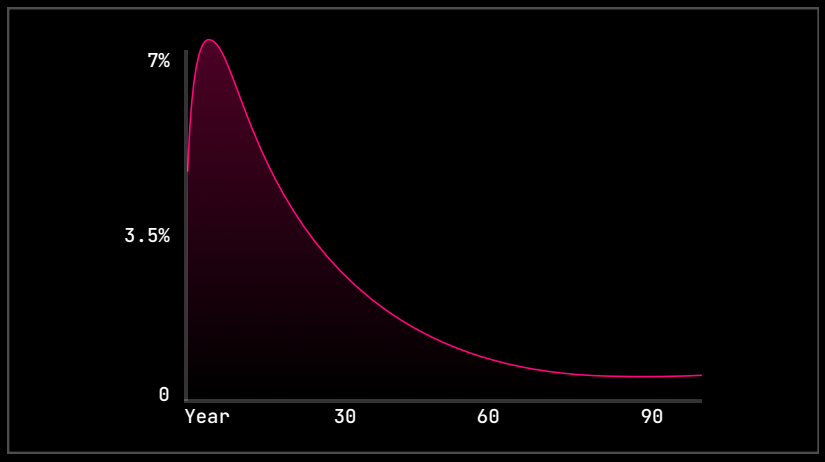
Supply

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

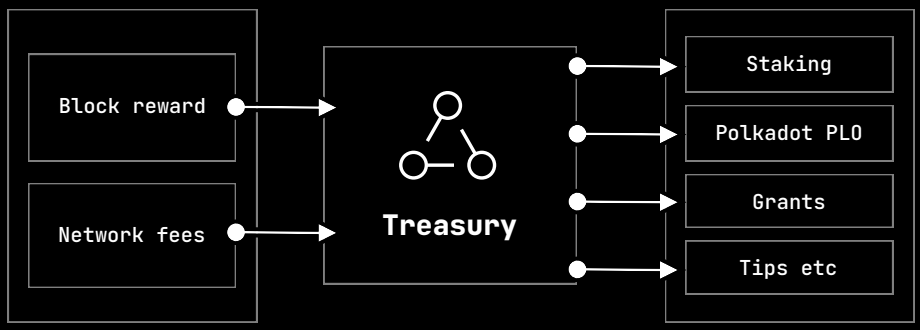
Total Supply	Total Remaining Issuable	Year	Issuable this year/Total remaining	Issuable this year	Inflation Rate
20	80	1	0.01	0.8	4.00%
20.8	79.2	2	0.014112789	1.11773288	5.37%
21.91773288	78.08226712	3	0.017257054	1.347469885	6.15%
23.26520276	76.73479724	4	0.0199	1.527022465	6.56%
24.79222523	75.20777477	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%

Treasury and Governance

Tokens minted after the initial supply is generated will be issued through Darwinia Chain's block reward to the treasury. And another source of tokens to treasury is network fees, the network fees include smart contract gas fees, cross-chain messaging fees, and other system income.

Block rewards and network fees will first go to the treasury, which is managed by the on-chain governance module. The treasury is primarily used for payment of treasury proposals, including staking, Polkadot PLO budget, grants, tips etc.

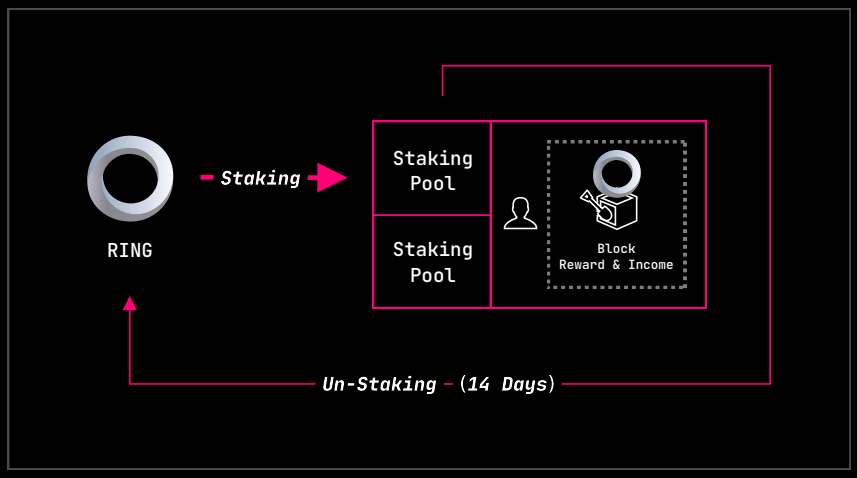
For example, to start, half of the tokens issued from block rewards will be allocated to the staking module to incentivize validators and nominators for protecting the security of the Darwinia Chain, by locking and bonding tokens.



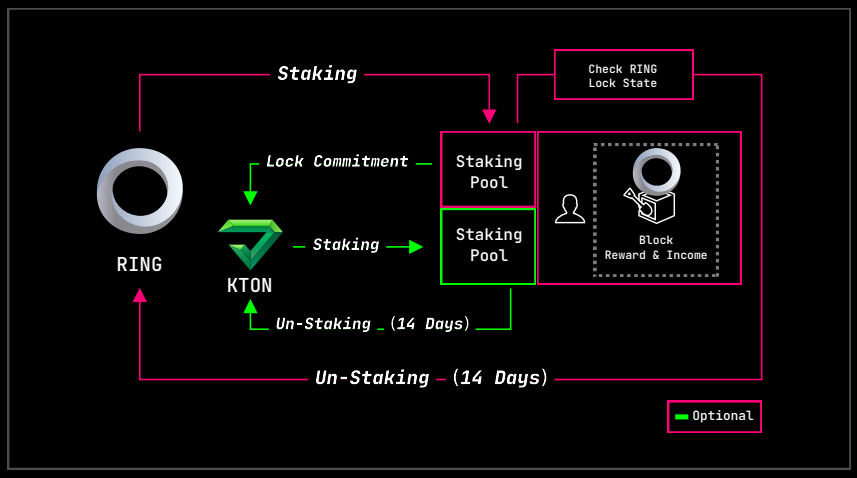
Staking

The treasury will distribute RING tokens from the new supply as incentives to the participants of Staking. The process of Staking can also be likened to the POS mining process, where the miner obtains Staking energy by pledging tokens for POS mining. The term POS mining refers to providing computing power based on traditional web and network services to serve the users in the Darwinia Network.

Generally speaking, users are able to perform POS mining by pledging the base token “RING”. If users want to retrieve their RING from the Staking pledge, the mining will stop, and the unpledged “RING” will take 14 days to release. Based on the role of staking participant, the participant may or may not provide the basic computing power and network bandwidth to the Platform. Only the staking participants that act as validators provide computing power to users in the Darwinia Network in order to insert and query the data on the network. The role is further documented in the section featuring the staking hash rate.



Basic Model



Advanced Model

KTON

To encourage users to make long term commitments and pledge, users can choose to lock RING for up to 36 months in the process of Staking, and the system will offer a KTON token as reward for users participating in Staking. During the committed pledge period, users cannot unlock their RING. (Unless they destroy triple the amount of KTON from their accounts as penalty).

As a result, during RING staking process, users can choose to lock RING for a period to receive KTON. The initial supply amount of KTON should be zero.

KTON can be pledged to receive Staking power, so as to participate in POS mining as well. Users may Stake via pledging KTON. However, if the user takes back his or her staking KTON, then the related POS mining will be stopped, and it will take 14 days for the unpledged KTON to arrive.

Staking Rule

Hash Rate is a term used in Proof-of-work (PoW) blockchain systems, such as Bitcoin. The value of the hash rate is based on the computing power provided by the account, and rewards for the account in a POW system is based on the hash rate.

In Darwinia Network, the ability to produce new blocks on the blockchain to receive token rewards is not based on computing power, but by the entity having a larger amount of RING and KTON pledged. This mechanism is called Nominated Proof-of-Stake (NPoS), and it is one of many different kinds of Proof-of-Stake (PoS) mechanisms. Herein, the Staking Hash Rate can be analogized to the Hash Rate in PoW and used to represent the current

contribution of Hash Rate of a certain account. The security of PoW systems is provided by computing power, but it is wasteful and time-consuming. The security of PoS systems is provided by the service or product provider using the utility tokens with higher frequency or larger volume.

In detail, there are two roles of the NPoS mechanism, the validator, and the nominator, and a time period for a completed process of an NPoS mechanism is an era. A validator can hold an entity in an era (a period of time), and nominators can participate in it. The era is a period of time of around 1 week, but could be delayed or advanced based on the different network and computing environments of the participants. An account participating in Darwinia Network can be a validator or a nominator at free will, but only one role per era.

The staking hash rate can be analogized to the Hash Rate in POW.

The staking hash rate for each account is determined by the amount of pledged RING and KTON, once unpledged, the corresponding hash rate provided to the Darwinia Network will vanish.

The Staking hash rate for an account is constantly changing based on the amount of tokens pledged.

Staking Hash Rate Percentage is the Staking Hash Rate Proportion of one account to the Total Staking Hash Rate (THE).

Staking Hash Rate = Total Staking Hash Rate (THE) × Staking Hash Rate Percentage

Staking Hash Rate Percentage for THE account = Staking Hash Rate Percentage(RING) + Staking Hash Rate Percentage(KTON)

Staking benefit of THE account:

Staking benefit of THE account = (Total number of additional RING generated on the Darwinia Network × Y) × Staking Hash Rate Percentage for THE account

Voting weight formula for THE account:

Voting weight = Total Voting weight × Staking Hash Rate Percentage for THE account

Remark 1: Default hash rate Contribution ratio of RING is 0.5.

Relayer Fee Market

An integral part of Darwinia Network's cross-chain messaging service are the off-chain relayers that send messages between chains. Relayers are open to anyone to operate and maintain, and ensure the network is decentralized. Relayers have no additional security assumptions outside the source and destination chain consensus; only a liveliness assumption.

Relayer incentives are based on a fee market model that balances the rewards and price level for successfully relaying messages. Relayers and users constitute a secondary supply-and-demand market, where prices rise when supply is low and fall when supply is abundant. Relayers who fail to relay messages as expected are punished.

Native tokens of the source chain are the only acceptable method of payment for message relay. Costs on the target chain are paid for by the relayer who claims the handling fee on the source chain, along with proof of delivery after delivery is completed successfully.

Participants

Researcher

The protocol and standard researcher's work is divided into two parts. The first part comes from the community. Darwinia Network accepts any RFC submission from the community, including new additions, improvements and modifications. These RFCs will be open to the community for full discussion and research to reach a consensus. The second part is from the core research team, which is responsible for organizing RFCs, organizing RFC peer audits and security audits, using Darwinia Network governance models and tools for protocol governance and voting, and forming a final agreement design draft for delivery to the protocol development team.

The submission and management of RFC documents is currently carried out on Github [3] and can be accessed if you are interested.

Developers

Developers improve Darwinia Network and related services, and develop applications and services using Darwinia Network. Early community open source software development, especially important infrastructure software development (including network protocol design, protocol implementation, node software, wallet, browser, etc.), will be sponsored and supported by the Darwinia Network Foundation, currently the main Darwinia Network open source software developer is Itering Tech.

In addition to infrastructure software development, the developer community includes protocol developers, integration developers, Dapp(smart contract) developers and application developers..

Protocol & SDK

Protocol developers include developers who design architecture, produce technical specifications, engineer core protocols, and design and develop Darwinia core facilities.

SDK developers design and develop application SDKs, which wrap Darwinia core capabilities and provide easy-to-use APIs for other developers. These SDKs could be built for different purposes, including applications, message sending in smart contracts, integration, connecting with more chains, etc.

Integration

Integration developers use the integration SDK to extend Darwinia cross-chain network and connect to more chains. To achieve this, they might need to build and integrate message protocols like LCMP, XCMP or other message protocols based on Oracles, Rollups, and more.

Dapp

Dapp developers include those who develop applications based on the Darwinia Smart Contracts module, as well as those who develop Dapps on public chains, such as blockchain games or Defi applications on platforms such as Ethereum, TRON or EOS.

App

Developers of applications such as web apps and tools.

User

Users of Darwinia Networks and related products and services.

Community

Different members and entities in the Darwinia community, including:

- Governance members including proposal originator, commentator/reviewer, voters, council members, technical committee etc.
- Staking participants including validators and nominators.
- Token holders.
- Relayers.
- Community Ambassadors and followers.
- Partners including infrastructure, integration, tech, advocate, business, marketing, liquidity, media etc.

Use cases

With the increasing amount of crypto tokens, the demands of crypto related payment, lending, pledge, leverage lease are rising as well. Apart from Defi applications, which are the majority for now, the combination of game NFT with Defi will also have actual demand. The requirements of the NFT trading market, NFT pledge and lease are apparent.

Multichain Gaming and Metaverse

We use Evolution land as an example to discuss the connection method of Darwinia Network. Evolution Land is a virtual management game based on blockchain and autonomy. It laughed continents are based on Ethereum, Tron, Heco, BSC, Matic, Crab chain etc.

Users playing in different continents(metaverse) and different chains will have requirements to send tokens and NFT in a cross-chain way. Darwinia’s cross-chain messaging service can help games/metaverse like Evolution land To build all kinds of cross-chain Dapp and features.

Cross-chain Assets Bridges

Cross-chain asset bridges allow you to move tokens of different standards (ERC-20, ERC-721, etc.) between blockchains.

Helix Bridge uses Darwinia's cross-chain messaging service to implement some of its asset cross-chain bridges.

NFT Marketplace

Users from one chain can bid on NFT auctions on a completely different chain.

Multiverse

Users can interact across metaverses in multiple metaverses.

The multiverse will be one of the biggest uses for cross-chain.

DEX

Allows users to exchange assets across multiple chains in one single transaction.

DAO governance

Allows for a unified multi-chain governance mechanism without moving assets between different chains.

Aggregator

Allows users to manage multi-chain assets from one chain.

Loan

Allows users to pledge on one chain and lend assets on a different chain.