



DARWINIA

GENEPAPER

Preview Version v0.9.1

Architecture Design	6
Darwinia Bridge Chain	8
Solo Mode	9
Polkadot Connection Mode	11
Appchain SDK	12
Non-fungible Token Identifiability	13
Native Token	14
Benefits Distribution	17
Staking	18
KTON	20
Staking Hash Rate	20
Slash Algorithm	24
Protocol Researcher	24
Developer	25
Dapp Developer	25
AppChain Developer	26
Ecosystem & Application	26
Open Gaming Application	26
Defi Application	26
Darwinia System	26
Polkadot Ecosystem	27
Polkadot Slot Bid Incentive Proposal	27
Node and Validators	28
User	28
Core Team	29

Background

The world is being blockchainized and tokenized. Fungible tokens, which has been generally used in the financial industry, together with Non-fungible tokens, which are becoming more and more recognized in the game industry, will greatly enhance the openness and collaboration of finance and game sector.

These tokens are being connected and merged, and the ways of such connection and merger are trends to diversified as well. Such connections might be performed with smart contracts, Dapp, or appchain protocols, that lead to the formation of an open token-network. Darwinia Network powered by decentralized token bridges and decentralized backing technology, via develop infrastructure and core-applications, to support the growth of the token-network. Darwinia focuses its major application in games and de-fi sector.



Build Future Token Internet

Technical Architecture

Blockchain network is being layered and specialized, while public chains cover consensus, security and cross-chain transfer of data or tokens, second-layer networks and sidechains are now targeting specific applications.

The innovation of new technologies as Polkadot and Substrate in lines with the trends of progression. Under such circumstances, Darwinia, a cross-chain network protocol to build the internet of tokens, chooses to join these trends of ecology and technology, with layered networks, cross-chain interactions, application-oriented design, user experience, etc. conducted as our key design features and principles.

In the process of using blockchain technology to create new DAPP, we found several problems for the mass promotion and utilization of blockchain technology:

1. The current blockchain infrastructure is not yet able to meet the requirements of user experience.

At present, the user experience problem of blockchain dapps is mainly reflected in two aspects. First, crypto wallets is still not easy to use for those who have never accessed blockchain and cryptocurrency. The necessity of private key backup and the inability to retrieve tokens if the password is forgotten are still big cognitive thresholds for users. Second, low-TPS of the public chain, and the gas fee costs are also big obstacles for users that are accustomed to free services.

2. Traditional vendors lack blockchain experience

The development of blockchain dapps require certain accumulation of blockchain technology and it could be costly for traditional developers to build a complete blockchain development platform.

3. Blockchain dapps are split among different public chains

Due to the heterogeneity of public chains, blockchain dapps developers need to develop the same dapp for each public chain in order to reach multiple public chain community, and the cost is relatively high.

We hope to use the most advanced blockchain technology and framework to construct an open network and application suite to solve these problems. This network and application suite combines blockchain trusted technology with a Web3 infrastructure with the following features: layered network design, cross-chain interaction, developer-friendly, best user experience, and high concurrency and customization.

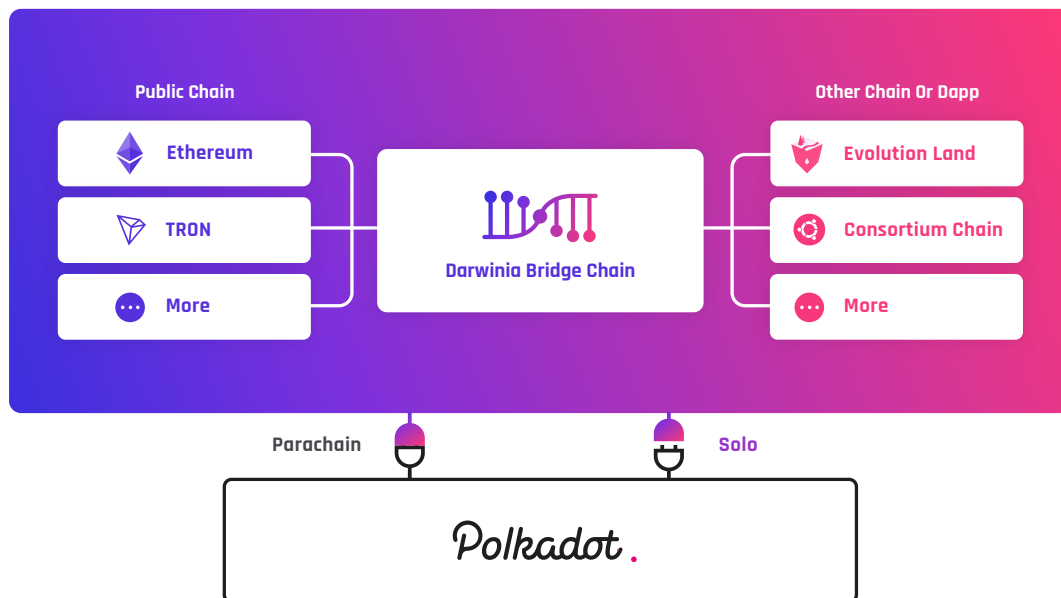
Architecture Design

Darwinia Network is a blockchain network based on Substrate[1] technology. Darwinia Network is part of the Polkadot ecosystem, and at the same time differentiated from Polkadot, Darwinia Network focuses on cross-chain token.

Blockchain Dapps can easily perform cross-chain token transactions and transfer through the Darwinia Network. For example, Cryptokitties can transform its NFT (Kitties) on the Ethereum into NFT on EOS through the Darwinia chain; players on the Ethereum and players on the EOS can play Evolution Land game simultaneously through the Darwinia Network. **At the same time, thanks to the Polkadot ecosystem, Darwinia Network can link to a wider range of games and players.**

The architecture relationship of Darwinia Network is shown as below.

ARCHITECTURE DESIGN



Darwinia Bridge Chain

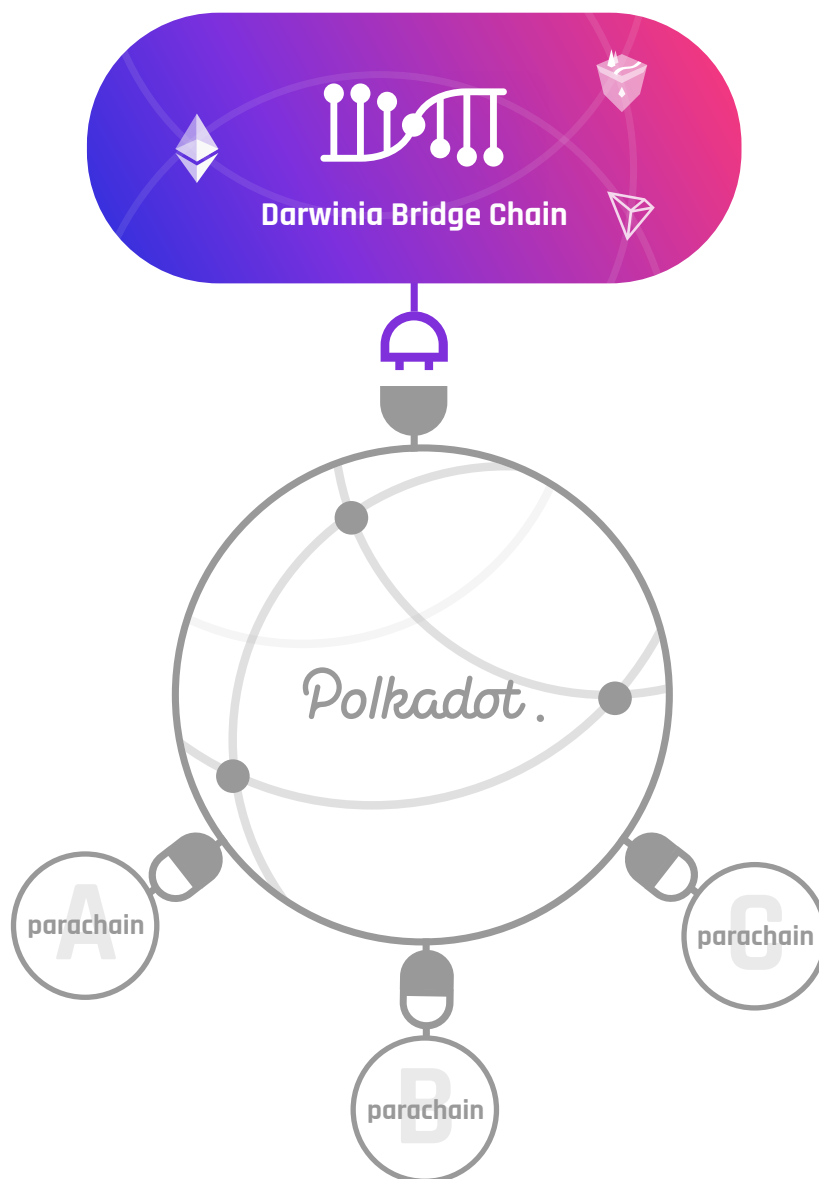
Darwinia Bridge Chain is the most important part of the Darwinia Network, it is also the bridge hub of dapps and public chains.

Darwinia Network itself can operate as a stand-alone cross-chain network, and Darwinia chain will be responsible for consensus security and cross-chain interoperability. Meanwhile, benefits from Polkadot, which provides an open parachain network access method, Darwinia Chain can also chooses to access Polkadot as a Parachain of Polkadot, then Polkadot will take over and be responsible for the security of the Darwinia chain. All of the Parachain in Darwinia Network will be able to connect to a wider external blockchain network via Polkadot.

To this end, we divided the operating mode of Darwinia chain into Solo mode and Polkadot connection mode:

Solo Mode

Darwinia Network can choose to operate as an independent public-chain network and is responsible for its own consensus security, with its core business and application services, including the cross-chain functionality of each application chain, controlled by Darwinia Network itself.

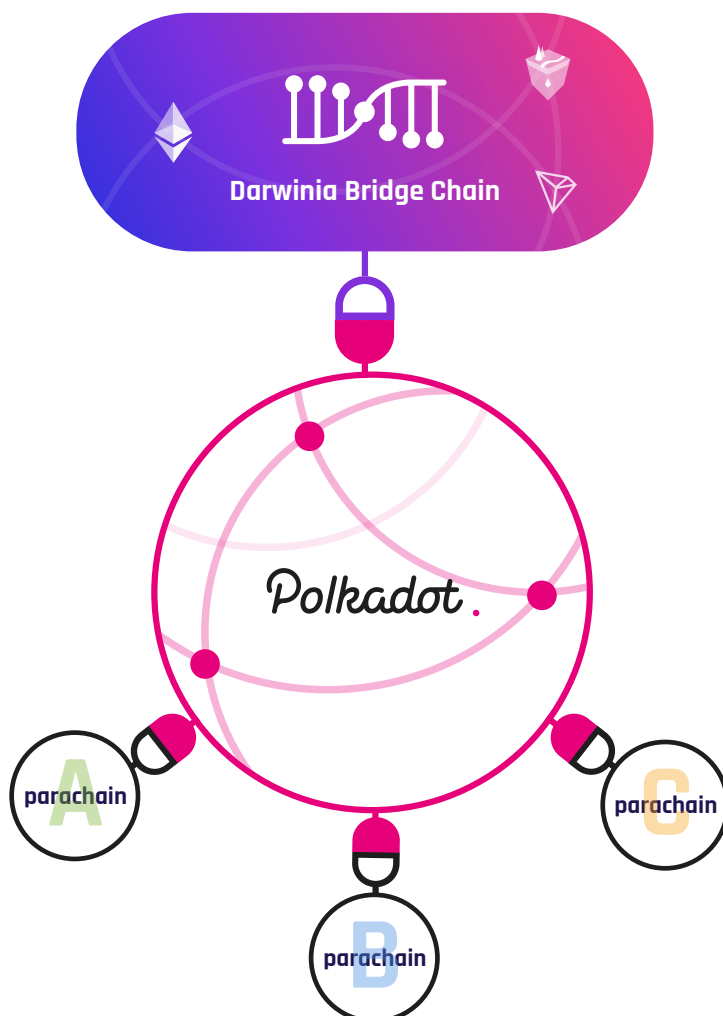




Polkadot Connection Mode

In Polkadot connection mode, Darwinia bridge chain serves as a Parachain for Polkadot.

Since Polkadot network adopts shared security model, the cross-chain security of the parachains will be guaranteed by the validators of Polkadot Relay Chain in the Polkadot connection mode. After Darwinia Network switches to the connected mode, the original validators and Staking mechanisms will be used to ensure local consensus within the Darwinia Network, which will help achieve faster block confirmation and higher TPS. This local consensus mechanism will also help Collator to determine that the block submitted to the Polkadot validators does not violate Polkadot global consensus.



Appchain SDK

In order to facilitate application developers to develop blockchain networks that meet application-level requirements, without having to deeply understand blockchain technology, the Darwinia Network team developed a framework to utilize blockchains based on Substrate and Darwinia Web Application Tools. This framework is called Appchain SDK.

Its design goal is to meet the needs of the application level, the business level, rather than the platform requirements of the public chain, so Darwinia Appchain will focus on the flexibility of the framework, the diversity of components; and the consensus algorithm, the speed of the block, and the governance model will be very different from the public chain.

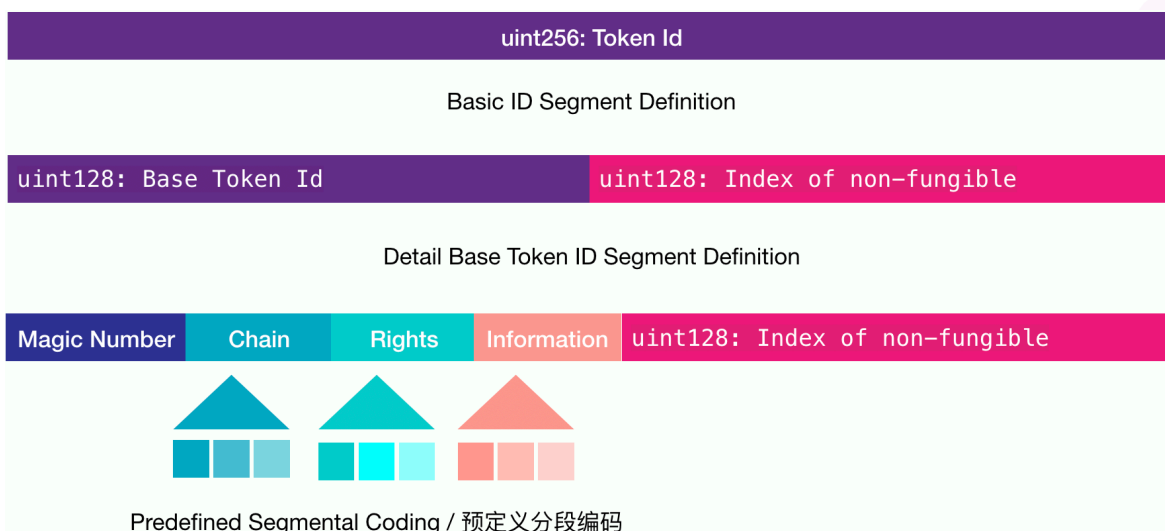
The Appchain SDK is a set of blockchain development kits that can be tailored to the needs of application developers for different blockchain networks. It can even create a blockchain with one-click, provide random number services and DKMS distributed key management services. The appchains developed based on this SDK will also use Substrate kernel, which is designed to be a sub-chain that connects to the Darwinia Network bridge chain.

Non-fungible Token Identifiability

In blockchain network, we use a single ID stand to mark different items. In the virtual realm, due to the existence of different ledger or blockchain network (domain), different items with different ID are identifiable within one domain, but the observers within one realm cannot identify item IDs from other domains.

The current design of many existing ERC721 blockchain applications is mainly for the identification of intra-domain products, and does not take into account the re-use of products from different domains, which leads to a situation that single Token ID cannot identify a unique product when re-using non-fungible products, and it also needs to carry a lot of domain information, which could be very complicated to implement.

To solve this issue, we designed an Interstellar Product Coding Standard, that enable different public chain and different products to have a single ID in the Darwinia Network, to allow easy cross-chain transfer for NFT products.



Economic Model

Total circulation	Total Remaining Issuable	Year	Issuable this year/Total remaining	Issuable this year	Development 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%

Native Token

The native token for the Darwinia Network is RING, RING can be used as gas for transactions. Gas include transaction fees, contract execution fees, network bandwidth charges, storage fees, and more.



RING's initial supply (INITIAL_SUPPLY) before Darwinia Network mainnet release is 2 billion, after which the newly issued RING will be distributed to the validators and nominators (Staking participants).

After the Darwinia Network mainnet goes live, the total cap of the block reward (MAX_BLOCK_REWARD_YEAR) is adjusted once a year. The block reward of year N is $1 - (99 / 100)^{\sqrt{N}}$ of total remaining issuable.

$$\text{Total remaining issuable RING} = \text{HARD_CAP} - \text{CURRENT_SUPPLY}$$

$$\text{Supply in the next year} = \text{supply in the previous year} + \text{total actual reward in the year}$$

The total number of HARD_CAP for RING is 10 billion.

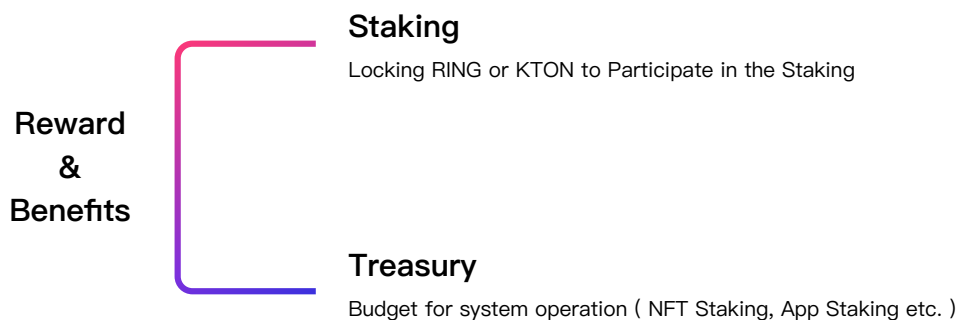
According to the annual block reward limit and the block interval (in seconds), you can calculate the block reward toplimit (MAX_BLOCK_REWARD) for each block of the year.

$$\text{Block Reward Limit for Each Block} = \frac{\text{Total Reward Limit for the Year} \times \text{Block Interval Time}}{\text{Total Number of Seconds per Year} (365 * 24 * 3600)}$$

The following table shows RING's Annual development statistics

Benefits Distribution

The benefits of Darwinia Network include block reward and transaction fees. The transaction fees include block fees, cross-chain staking fees, App-chain access fee and other related fees. (e.g from Evolution Land)



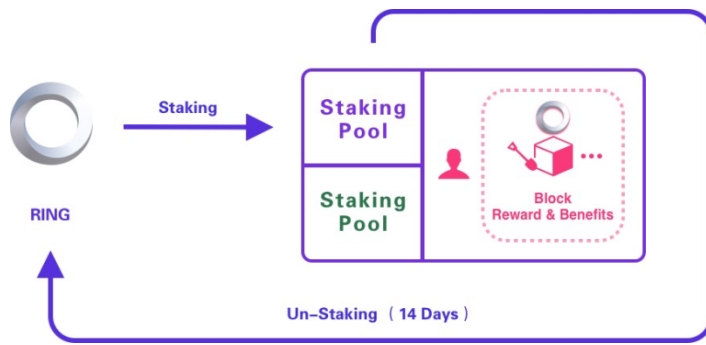
Treasury is primarily used for payment of system proposal budgets, and may include system operation proposals such as NFT mining or App mining, Polkadot slot bidding incentives, or for eco developer support.

Staking

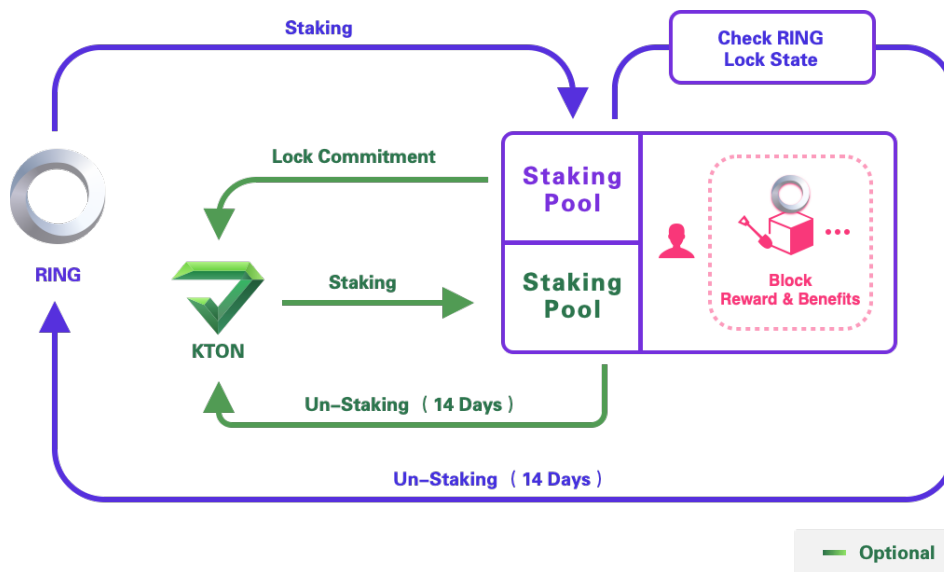
The Darwinia Network will distribute new RING generated on the blockchain as an incentive to the participants of Staking. The process of Staking can also be understood as the POS mining process, where the miner obtains Staking energy by pledging tokens for POS mining. The term POS mining refers to providing computing capability of traditional web and network service to serve the users in the Darwinia Network.

Generally speaking, users can perform POS mining by pledging the base token "RING". If users start to retrieve the RING from Staking pledge, the mining will stop, and the unpledged "RING" will take 14 days to fully arrive. Based on the role of a 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 capabilities to users in the Darwinia Network to insert and query the data on the network. The role is well documented in the section of the staking hash rate.

According to complexity, Staking can be divided into basic and professional versions



Basic Staking



Professional Staking

KTON

To encourage users to make long term commitments and pledge, users can choose to lock RING for 3 - 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 utilise triple the amount of KTON 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, yet before the Darwinia mainnet launch, some users have already started locking their RING in Evolution Land, so there will be some KTON supply at the time of mainnet launch. The earliest design to obtain the KTON by locking the RING appears in the Gringotts of Evolution Land. The related introduction can refer to the Gringotts KTON model [5].

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 Hash Rate

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

In Darwinia Network, the ability to elongate blockchain to get the token rewards is not by the computing power but by the entity having a larger amount of RING and KTON pledged. This mechanism is named as Nominated Proof-of-Stake (NPoS), it is one of the Proof-of-Stake (PoS) mechanisms. Herein, the Staking Hash Rate can be analogized to the Hash Rate in PoW and be used to represent the current contribution of Hash Rate of a certain account. The security of PoW system is provided by computing power competition, but it is wasted computing power and time-consuming. The security of PoS system 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 around 1 week will be delayed or ahead 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 in the one era.

In other words, a validator is the leader of the entity to obtain the token rewards, and a nominator can use the pledged RING and KTON to partake one or more validators to help the entity become a larger entity with more pledged RING and KTON. Therefore, there is only one validator in the entity, and a nominator can belong to one or more entities base on the pledged RING and KTON his participating. The action that a nominator decides to use his pledged RING and KTON to partake one or more validators is called voting in NPoS mechanism. After voting, the small amounts of entities with the largest number of pledged RING and KTON will be selected, and the validators of the selected entities are the elected validators. There may be some nominators belonging to one or more selected entities. Only the elected validators have the right to elongate the blockchain of Darwinia Network in the era, so the token rewards are only given to the validators and the nominators of the small amounts entities. If the elected validator is not diligent on elongating the blockchain of Darwinia Network, all pledged RING and KTON of that entity will be automatically destroyed by the system within the Darwinia Network. Besides, the validator can decide the token reward portions between the validator and the nominators before the voting. In general, the validators and nominators are service providers or manufacturers, they provide their service and use RING as a utility token to exchange their services or their products. The difference between the validators and nominators is not on the service they provide, but based on the Hash Rate they contribute to the Darwinia Network. The validators provide Hash Rate to the Darwinia Network directly, and the nominators will provide the same indirectly by voting for higher quality validators. An account that usually heavily relies on the RING to exchange his

or their services or provides services with a larger value of RING will join the Darwinia Network with better infrastructure. An account using less RING to exchange their services with can also participate with the Darwinia Network by voting better validators with good infrastructures. The business of account using RING to provide a service may change in a different time period, so the Darwinia Network allows the account to change the roles between nominators and validators easily. As mentioned before, the PoS has advanced on calculating power and time consuming than the PoW, the NPoS mechanism used in Darwinia Network comparing with the pure PoS system can be better, due to only small amounts of elected validators participating in the elongation process. On the other hand, the small amounts of elected validators can take a good balance between the robustness of the system and the efficiency.

In an era, the validators provide one or more computation nodes with network accessibility to act as a web and network service provider in order to help the users of Darwinia Network to insert and query the data in the Darwinia Network, so the benefits from this service will be given to the network users. After the era, additional RING (as token rewards) that are generated on the Platform is separated into two equal portions. One is for the nominators and the validators who pledged RING, another is for the nominators and the validators who pledged KTON. And then, each portion will send to the selected entities based on the percentage of pledged RING and the percentage of pledged KTON. And then the token rewards of each entity will be sent to the validator and the nominators in the entity 3based on the benefits portion decided before the voting. The aforementioned process is performed automatically by the Darwinia Network without operation from validators. Besides, another voting process will be performed, such that there will be newly elected validators to elongate the blockchain of Darwinia Network in the next era.

In other words, the token rewards received by an account are based on the portions, and the portion can be present as the Staking Hash Rate.

The Staking hash rate for a certain account represents the current contribution of this account.

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, corresponding hash rate provided to the Darwinia Network will vanish.

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

Staking Participants can change their voting validator without unpledging tokens.

Staking Hash Rate may play an important role in system governance. (Note 2)

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

$$\text{Staking Hash Rate} = \text{Total Staking Hash Rate (THE)} \times \text{Staking Hash Rate Percentage}$$

$$\text{Staking Hash Rate Percentage for THE account} = \frac{\text{Staking Hash Rate Percentage(RING)} + \text{Staking Hash Rate Percentage(KTON)}}{\text{Staking Hash Rate Percentage(RING)} + \text{Staking Hash Rate Percentage(KTON)}}$$

Staking benefit of THE account:

$$\text{Staking benefit of THE account} = (\text{Total number of additional RING generated on the Darwinia Network} \times Y) \times \text{Staking Hash Rate Percentage for THE account}$$

Voting weight formula for THE account:

$$\text{Voting weight} = \text{Total Voting weight} \times \text{Staking Hash Rate Percentage for THE account}$$

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

Remark 2: Because KTONs can be sold on the secondary market, it may not fully represent long term commitments. Only pledged “tokens×days” can accurately represent the commitment to Darwinia’s network.

Slash Algorithm

In order to prevent the network from validators' attacking or unstable block validation, when the attack or error occurs, the system needs to punish the validator (and the voters) by slashing its pledged tokens. The process and mechanism of the penalty is the Slash algorithm.

Since there are two different tokens (RING and KTON) existing in the Darwinia Network, supplementary explanation of Slash algorithm is required.

The punishment related parameter in Staking system are in percentage, in the occurrences of Slashing event, tokens pledged by the validator and the voters will be slashed by a certain percentage, no matter whether the tokens are RING or KTON.

In the Staking system of Darwinia Network, there are four main states for RING: account balance, in Staking, Staking lock, un-Staking, so there exists two different states for pledged RING token: in Staking and Staking lock, and the RINGs in Staking lock may have different unlock date. In the occurrences of Slashing, it is essential to confirm the sequential and priority of RINGs that is being Slashed. The Staking system will follow the order of unlocking expiration, and Slash tokens with earlier expiration dates first. The pledged tokens that are not locked will be Slashed first, and then comes the tokens that locked and with earlier expiry date.

Community Ecosystem

Protocol Researcher

The protocol and standard research'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.

Developer

Develop and improve Darwinia Network, Darwinia AppChain and related services, and develop applications and services using the Darwinia Network and the Darwinia AppChain. 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 software development for infrastructure, the developer community includes application developers, which can be divided into Dapp developers and Appchain developers, Evolution Land, and more.

Dapp Developer

Dapp developers include developers who develop applications based on the Darwinia Web Smart Contracts module, as well as developers who develop Dapp on the public chain, such as blockchain games or Defi applications on platforms such as Ethereum, TRON or EOS. For the Dapp and game inventories on the public chain, bridge parachain of Darwinia Network can be connected to the Darwinia Network for cross-chain transfer operations.

AppChain Developer

Application chain developers developing with the Darwinia Web Application Suite (Darwinia AppChain).

Ecosystem & Application

Open Gaming Application

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. Its first, second and third continents are based on Ethereum, Tron and EOS development. The way the Evolution Land connects to the Darwinia Network is as follows:

1. The first, second, and third continents, as heterogeneous other public chains, will access the Darwinia Network through bridge parachain.
2. Subsequent continents will be developed based on the AppChain SDK and can be directly bridge to the chain of Darwinia Network.

Defi Application

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

Darwinia System

A non-profit open source system established by the community to support and promote the development, construction and promotion of the early Darwinia Network. [WIP]

Polkadot Ecosystem

Under Polkadot connection mode, Darwinia Network will connect to polkadot parachain slot, so polkadot ecosystem is a vital part of Darwinia Network.

When Darwinia Network connects to the Polkadot network, according to the model of Polkadot Parachain Auction[4], Darwinia chain will need to lock enough DOTs to participate in the Parachain Slots bidding. Darwinia Network will organise a campaign to motivate Darwinia community participants to help in the Parachain Slots bidding.

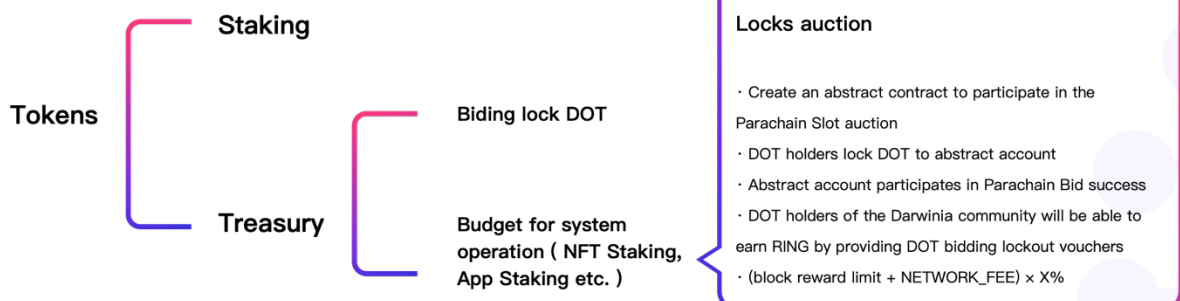
Polkadot's Parachain Slot auction allows any type of abstract account to participate in the auction, including general address accounts, smart contract accounts, and parachain accounts. This extensive abstract account support provides flexibility for participating bidders to design a variety of decentralized bidding models.

Darwinia Network will design a way for the Polkadot connection model to participate in the Parachain Slots auction. The participant does not need to transfer the DOT ownership, but will only need to lock the DOT and provide the locking credentials, and open a certain vote or bidding permissions for the Darwinia Chain. DOTs participating in bidding locks are secure because the entire process is done through smart contracts (or runtime modules) and no one can control these partially locked tokens.

Polkadot Slot Bid Incentive Proposal

In the connection mode, Darwinia Network may initial such proposal under this design, to provide benefits to participants who lock their DOT and support Darwinia to its Polkadot Parachain slot bid.

When Darwinia Network switches to polkadot connection mode, DOT owners in the Darwinia community may lock their token through bidding lock, and receive benefits from the incentive proposal.





Node and Validators

By participating in Staking as a validator to obtain the Staking benefits of the Darwinia Network by protecting the system security and validate new blocks.

Like Polkadot's participants, Darwinia Network has nominators, collators, fishermen besides validator.

User

Users of Darwinia Networks and Darwinia AppChain related products and services.

Core Team



Alex Chien

- Co-Founder of Darwinia Network
- Blockchain and smart-contract specialist. Senior Technical Advisor
- Ever since 2011, he found bitcoin and started blockchain research and development work for various open source projects
- Graduated from Shanghai Jiao Tong University



Denny Wang

- Co-Founder of Darwinia Network
- Blockchain and smart-contract specialist. Senior Technical Advisor
- One of the core developers of the BitShares 1.0 software
- Ethereum Enterprise Alliance China representative
- Graduated from Nanjing University, majoring in Mathematics

Roadmap

2019-07
Launched



Darwinia
Trilobita Testnet

2019-09



Darwinia
Crayfish Testnet

2019-11



Darwinia
Icefrog Testnet

2020-Q2



Darwinia
Crab Network

2020-Q3



Darwinia
Mainnet

2020-Q4



Ecological
Applications

Reference

- (1) <https://github.com/paritytech/substrate>
- (2) <https://polkadot.network/PolkaDotPaper.pdf>
- (3) https://github.com/darwinia-network/rfcs/tree/master/zh_CN
- (4) <https://wiki.polkadot.network/en/latest/polkadot/learn/auction/>
- (5) <https://forum.evolution.land/topics/55>
- (6) <https://research.web3.foundation/en/latest/polkadot/Token%20Economics/#treasury>

