DARWINIA

GENEPAPER

预览版本 v0.7

前言

区块链网络正在分层化和专用化，基础的公链网络负责共识安全性和跨链，第二层网络和侧链则正在往特定应用领域发展。

类似波卡网络和Substrate这样的新技术发展，符合了这样的业态发展趋势，在这种背景下，达尔文网络(简称 Darwinia)，一个专注于游戏和应用领域的跨链和应用链网络，选择加入这个生态和技术趋势，将分层网络、跨链交互、面向应用设计、用户体验等作为我们的关键设计特性和原则。

达尔文网络致力于成为未来游戏世界的区块链基础设施和网络。

行业背景

世界正在被区块链化，除了金融行业之外，最有可能带来变革的是游戏行业，区块链将极大的提升游戏世界的开放性和协作性。

在使用区块链技术打造新型开放游戏的过程中，我们发现游戏和区块链结合存在几个问题：

1.当前的区块链基础设施还无法满足游戏的用户体验需求

目前区块链游戏的用户体验问题主要体现在两个方面，一是数字钱包的使用上手困难，助记词需要备份和忘记密码无法找回资产对于用户来说还是很大的认知门槛和使用门槛。二是由于目前公链的低TPS，以及燃料费付费习惯对于互联网免费用户来说也是比较大的障碍。

2.传统游戏厂商缺乏区块链经验

区块链游戏的开发需要一定的区块链技术积累，传统游戏搭建一套完备的区块链游戏开发平台成本较高。

3.不同公链之间的区块链游戏是割裂的

由于公链的异构，区块链游戏开发者为了触及多个公链的用户，需要为每一个公链重复开发同一款游戏，成本比较高。

我们希望使用目前最先进的区块链技术和框架来构造一个开放的网络和应用套件来解决这些问题。这个网络和应用套件将区块链可信技术和Web3基础设施，同时又具备以下特性，即分层网络设计，支持跨链交互，开发者友好，最佳用户体验，高并发可定制。

这个网络就是达尔文网络，这个应用套件就是达尔文应用链。

DARWINIA

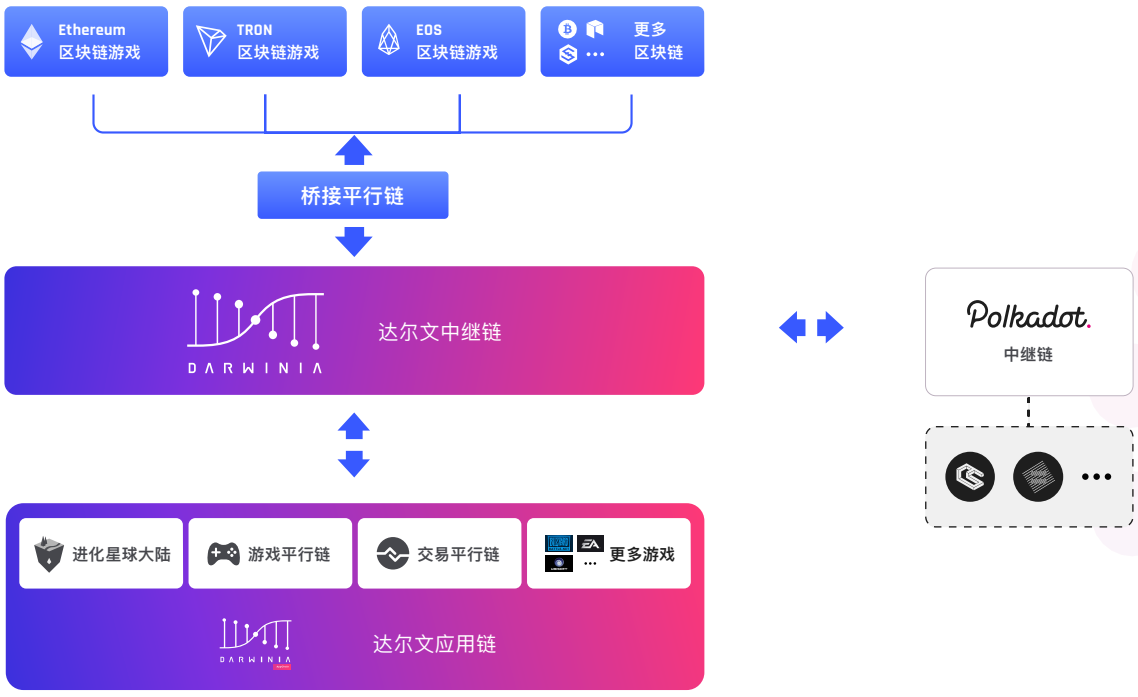
达尔文网络

达尔文网络是基于Substrate[1]技术构建的区块链网络，在架构设计上参考Polkadot[2]的跨链网络框架，包括中继链，平行链，转接桥等设计。达尔文网络作为Polkadot生态的一员，同时又区分于Polkadot的是，达尔文网络主要专注于游戏和应用方向的跨链和应用链业务。

通过达尔文网络，区块链游戏或者Dapp 可以通过达尔文网络方便的进行游戏资产和游戏操作的跨链交互，比如，以太坊上的迷恋猫（Cryptokitties）游戏可以通过达尔文链把以太坊上的 NFT ：迷恋猫转变成EOS上的迷恋猫；以太坊上的玩家和 EOS 上的玩家可以通过达尔文网络同时玩进化星球游戏。同时得益于Polkadot生态，达尔文网络可以链接更广泛的游戏和玩家。

架构设计

达尔文中继链，达尔文应用链，Polkadot 中继链等的架构关系如下图所示



DARWINIA

达尔文中继链

达尔文中继链是达尔文网络中最重要的角色，也是各个应用并行链的枢纽。

达尔文网络自身可以作为一个独立的跨链网络运行，达尔文中继链将负责共识安全和跨链互操作。同时，得益于Polkadot提供了一套开放的异构网络接入方式，达尔文中继链也可以选择接入Polkadot作为平行链运行，Polkadot将接管并负责达尔文中继链的安全，这样，达尔文网络中的所有应用链将可以通过Polkadot连接至外部更广泛的区块链网路。

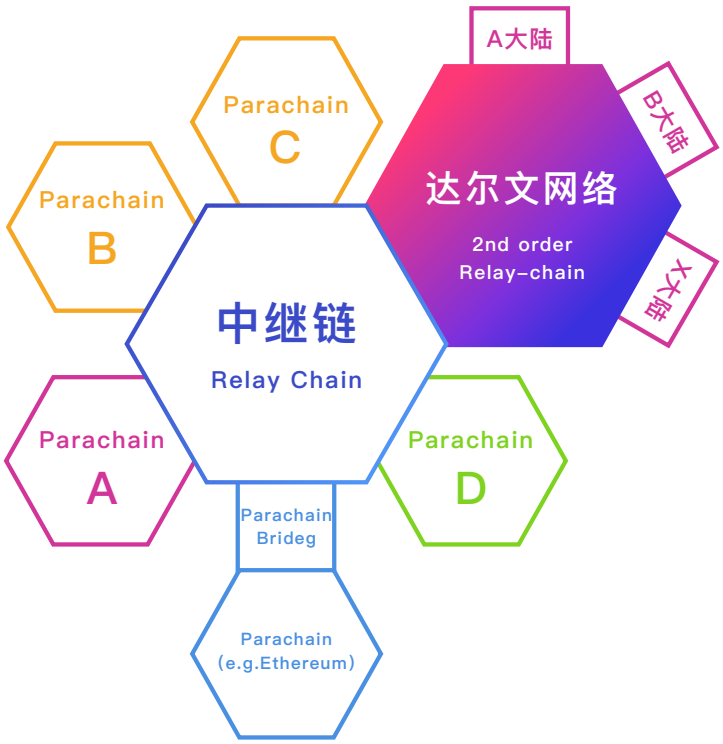
为此，我们将达尔文中继链的运行模式分成了Solo模式和Polkadot模式：

Solo模式

达尔文网络可以选择作为一个独立的公链网络运行，并负责自己的共识安全，其核心业务和应用业务，包括各个应用链的跨链功能不受影响。

Polkadot模式

在Polkadot模式下，达尔文中继链除了可以作为达尔文网络的中继链运行之外，还将作为Polkadot的平行链。



原生资产

RING是达尔文网络的原生资产。RING可以作为交易的燃料费，可以通过锁定获得KTON。燃料费包括交易费用，合约执行费用，网络带宽费用，存储费用等等。

通过锁定RING获得的KTON是达尔文网络的Staking和治理凭证。氪石持有者和氪石Staking锁定者将可以获得网络收入和Staking收益。氪石只能通过锁定RING获得，最早通过锁定RING获得氪石的设计出现在进化星球古灵阁银行，相关的介绍可以参考古灵阁氪石模型[5]。

RING在达尔文网路主网上线时的初始供应量(INITIAL_SUPPLY)为20亿，之后将会通过出块奖励将新发行的RING分发给出块验证人和Nominator(Staking参与者)。

在达尔文主网上线后，该年的出块奖励总上限(MAX_BLOCK_REWARD_YEAR)调整一次，每年的块奖励最大上限为剩余可发行供应量的20%，实际的通胀率将会跟RING和KTON的锁定率挂钩，将会远远小于20%，预期为剩余可发行供应量的4%-10%。

剩余可发行总量 = 硬顶总量(HARD_CAP) - 当前供应量(CURRENT_SUPPLY)
该年出块奖励总上限 = 剩余可发行总量 ×1/5
下一年的供应量 = 上一年的供应量 + 该年实际出块奖励总和

RING的硬顶总量为100亿。

根据每年的出块奖励上限，和出块间隔时间(单位：秒)，可以算出这一年的每个块的出块奖励上线(MAX_BLOCK_REWARD)

每个块的块奖励上限 = 该年出块奖励总上限 × 出块间隔时间 ÷ 每年总秒数(即365乘24乘3600)

最终每个块的出块奖励实际数量跟RING锁定率和氪石锁定率有线性比例关系：

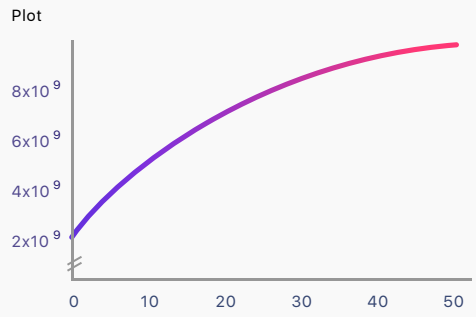
RING锁定率 = 当前未到期且锁定状态的RING总和 ÷ RING当前总量
氪石锁定率 = 当前质押锁定状态的KTON总和 ÷ KTON当前总量

在Solo模式下(区别于Polkadot连接模式下，见Staking章节)，每个块的实际出块奖励为(X, Y为系统参数，X+Y <= 100)：

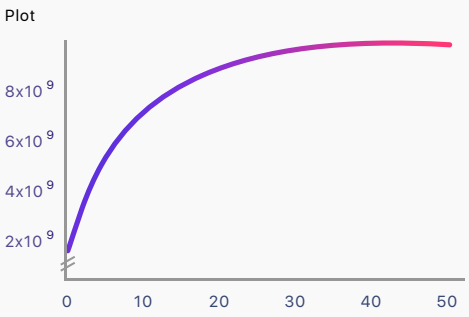
每个块的实际块奖励 = 块奖励上限 × (X% ×F(氪石锁定率) + Y% × F(RING锁定率) + (100-X-Y)%)

备注: X, Y为系统参数，满足X+Y <= 100。X%，Y%和 (100-X-Y)%的意义分别表示分配给验证人，氪石持有者，Treasury的奖励比例，其中验证人的部分已包含Nominator和Collator。F(锁定率)表示与锁定率线性的相关的函数，具体尚在研究之中，简化情况下可以理解为"F(锁定率)=锁定率"。

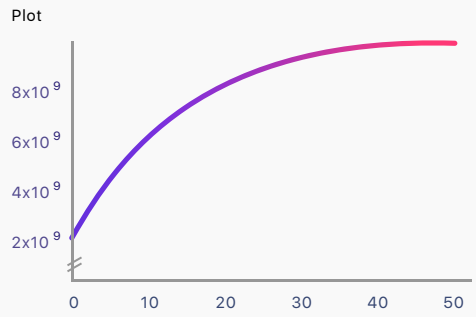
实际网络运行过程中，锁定率是不断变化的，这里我们举几个简化且理想化的情况举例子，例如锁定率都为20%，35，50%，65%时，相应供应量的增长曲线为：



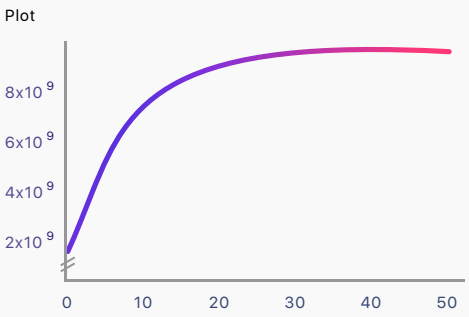
预期锁定率为20%时的供应量曲线



预期锁定率为50%时的供应量曲线



预期锁定率为35%时的供应量曲线



预期锁定率为65%时的供应量曲线

Staking

达尔文网络将会把全部收入作为激励分发给Staking的参与者。

达尔文网络的收入来源大体分为两种：

1. 出块奖励(BLOCK_REWARD)，每年的块奖励上限随时间会减少，通胀率将会随着时间快速收缩和降低。

2. 达尔文网络交易手续费(NETWORK_FEE)，包括开发者使用达尔文网络的跨链服务，达尔文网络平行链的接入费用，以及相关应用比如进化星球自主选择分配给达尔文网络的收入。

因为Polkadot网络采用共享池安全的模型，所以处于Polkadot 连接模式时，平行链的安全性将由由中继链的验证人来保证，达尔文网络在此情况下不需要负责验证，只需要负责Collator即可。

因此，达尔文网络的 Staking 在这两种模式下的安全激励也会有很大不同，具体如下。

Solo 模式收入分配

验证人和 KTON 持有者将会按照一个比例来分享进化星球的收入， KTON 持有者可以同时把自己的 KTON 投票给验证人，获取验证人部分的 Staking 激励。(Y为系统参数，将会通过KTON投票的治理机制来设定)

（锁定 KTON，全部 KTON, Treasury）=
[(块奖励上限 ×氪石锁定率 + NETWORK_FEE)×X% ，(块奖励上限 ×RING锁定率 + NETWORK_FEE)×Y%), (块奖励上限 + NETWORK_FEE) × (100-X-Y)%]

Polkadot 连接模式收入分配

当达尔文网络打算连接至Polkadot网络时，根据Polkadot Parachain Auction[4]的模型，达尔文中继链将需要锁定足够多的DOTs来参与Parachain Slots竞价，是否胜出只与锁定的DOTs多少有关，取决于当时的市场情况。为了获得足够的竞争力，达尔文网络将设计一种众筹锁定竞价机制，以激励达尔文社区参与者帮助竞价。

众筹锁定竞价

Polkadot的Parachain Slot拍卖竞价允许任何类型的抽象账户参与竞价，包括普通地址账户，智能合约账户，平行链账户。这种广泛的抽象账户支持为参与竞价者提供了灵活性，可以设计各种去中心化的竞价模型。达尔文网络将为Polka连接模式设计一种通过众筹锁定DOT来参与Parachain Slots竞价的方式，众筹者不需要将DOT所有权进行转移，只需要将DOT锁定并提供锁定凭证，同时开放一定的投票或者竞价权

限供达尔文中继链使用。参与竞价锁定的DOTs是安全的，因为整个过程是通过智能合约(或中继链)完成的，没有任何人可以控制这部分锁定的资产。

当达尔文网络切换至Polkadot连接模式时，达尔文网络不再需要自己的验证人，原来用来激励KTON锁定者Staking的部分将会被用来奖励那些帮助达尔文网络进行DOT锁定竞价的参与者，也就是说，达尔文社区的DOT持有者将可以通过提供DOT竞价锁定凭证，获得RING网络收入奖励。

（达尔文竞价锁定DOT，全部 KTON, Treasury）=
[(块奖励上限 + NETWORK_FEE) × X% ，(块奖励上限 × RING锁定率 + NETWORK_FEE) × Y% , (块奖励上限 + NETWORK_FEE) ×(100-X-Y)%)]

DARWINIA

达尔文应用链

为了方便游戏开发商和其他应用开发者在不需要懂得太多区块链知识的基础上开发满足应用层面需求的区块链网络，达尔文网络基于 Substrate 和达尔文网络区块链内核 (Darwinia Kernel) 设计开发一套应用区块链的框架，被称为达尔文应用链 (Darwinia AppChain)。

达尔文应用链是一组区块链开发套件，可以满足应用开发者不同区块链定制需求，甚至一键发链。

达尔文应用链的设计目标是为了满足应用层面，甚至是业务层面的需求，而不是公链的平台需求，所以达尔文应用链将侧重于框架的灵活性，组件的多样性，在共识算法，出块速度，治理模式上与公链也会非常不同。

达尔文应用链同样基于 Substrate 框架，使用与达尔文中继链同样的内核，所以达尔文应用链可以作为平行链直接连接至达尔文网络。

DARWINIA

星际资产编码标准

对于不同的物品，我们会用一个唯一的标识来标记它。在虚拟资产世界，因为存在不同的账本或称区块链网络(简称域)，不同的物品在同一个域里面因为有不同的标识，所以可以区分，但是该域里面的观察者无法识别来自外部域的物品标识。

目前现有的很多ERC721的区块链应用所做的设计，都主要是针对域内资产进行标识设计，没有将不同域内的资产复用考虑进来，这样导致在对非同质资产进行复用时，单独的Token ID无法标识唯一的资产，还需要带上很多域信息，实现起来十分复杂。

为了解决这个问题，**我们设计了一个星际资产编码标准，让不同公链，不同游戏的资产在达尔文网络可以得到唯一标识，让游戏资产可以方便的跨链转移。**

社区生态

协议研究者

协议和标准研究工作分成两个部分。第一个部分来自于社区，达尔文网络接受来自社区的任何RFC提交申请，包括协议新增，改进和修改建议，这些RFC将会开放给社区，并经过充分的讨论和研究以达成共识。第二个部分是核心研究团队，负责整理RFC，组织RFC同行审计和安全审计，利用达尔文网络治理模型和工具进行协议治理和投票，并形成最终的协议设计稿，以交付给协议开发团队进行实现。

目前RFC文档的提交和管理在Github [3]上进行，感兴趣的话可以访问。

开发者

开发完善达尔文网络，达尔文应用链及相关服务，使用达尔文网络以及达尔文应用链开发应用层的产品和服务。社区早期的开源软件开发，特别是重要的基础设施软件开发(包括网络协议设计，协议实现，节点软件，钱包，浏览器等等)，将会得到达尔文网络基金的赞助和支持，**目前主要的达尔文网路开源软件开发商是 Itering Tech。**

除了基础设施的软件开发之外，开发者社区还包括应用开发商，具体可以分为Dapp开发者和应用链开发者，进化星球等等。

进化星球

我们以进化星球为例来讨论达尔文网络的连接方式，进化星球是一款基于跨链和自治生态的虚拟经营类区块链游戏，它的第一，第二，第三大陆分别基于以太坊，波场和EOS开发。进化星球连接达尔文网络的方式如下：

1.第一，第二，第三大陆作为异构的其他公链，将通过桥接的方式接入达尔文网络。

2.后续的大陆将会基于达尔文应用链开发，可以直接和达尔文网络中继链连接。

Dapp开发者

Dapp开发者包括基于达尔文网络智能合约模块进行应用开发的开发者，也包括在公链上进行Dapp开发的开发者，例如以太坊、波场或EOS等平台上的区块链游戏或者Defi应用。对于公链上的Dapp和游戏资产，将可以通过达尔文网络跨链桥平行链连接至达尔文网络，进行跨链转移等操作。

应用链开发者

采用达尔文网络应用套件进行开发的应用链开发者。

达尔文网络基金

社区成立的非盈利性开源基金，用于支持和推动早期达尔文网路的开发建设和推广。[WIP]

中继链验证人

通过锁定 KTON 参与竞选成为验证人，验证人将负责达尔文网络交易的记账和出块以及节点的维护，验证人将获得达尔文网络收入的分成。跟Polkdot的参与者一样，达尔文网络跟验证人类似的角色还有Nominators, Collaters, Fishermen等。

KTON持有者

KTON 是对 RING 长期持有者的一种奖励，持有 KTON 将会获得达尔文网络收入的分成，同时，KTON 持有者可以将 KTON 锁定后投票给潜在验证人以帮助其竞选，如果竞选成功，锁定的 KTON 可以等到验证人收入的分成。

锁定竞价DOT持有者

参考Polkadot连接模式下的众筹锁定竞价章节。

用户

达尔文网络和达尔文应用链相关产品和服务的用户。

路线图

Darwinia Network
Testnet

Darwinia Network
Mainnet

Darwinia AppChain
Testnet

Darwinia AppChain
Mainnet

参考资料

(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