



DARWINIA

GENEPAPER

预览版本 v0.9.1

架构设计	6
达尔文桥接链	8
Solo模式	9
Polkadot模式	10
应用链SDK	11
NFT 可识别性	12
原生产资产	13
奖励分配	15
Staking	16
氦石(KTON)	18
Staking 算力	18
Slash 算法	22
协议研究者	23
开发者	23
Dapp 开发者	24
应用链开发者	24
生态应用	24
开放游戏应用	24
开放金融(Defi)应用	24
达尔文网络基金	25
波卡生态	25
Polkadot槽位竞价激励提案	26
节点和验证人	26
用户	26
核心团队	27

商业背景

世界正在被区块链化和通证化，通证不仅包括在开放金融领域广泛应用的同质通证(代币)，也包括正在游戏行业被越来越多使用的非同质通证(NFT)，区块链将极大的提升游戏和金融世界的开放性和协作性。

这些通证正在以可信的方式互相连接融合，融合的方式也正在变得多样化，可能是以智能合约 **Dapp** 的形式，也有可能是以构建应用链协议的方式，一个开放的通证互联网正在慢慢形成，达尔文网络以去中心化桥接和去中心化背书技术为基础，通过构建基础设施和核心应用，支持通证互联网发展壮大，主要的应用领域包括开放游戏和开放金融等。



Build Future Token Internet

技术架构

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数据,资产的跨链，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(Darwinia Network)，一个专注于资产互联网络的跨链网络，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。

在使用区块链技术打造新型区块链应用的过程中，我们发现区块链技术的大规模推广还存在几个问题：

1. 当前的区块链基础设施还无法满足用户体验

目前区块链应用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IT和互联网公司缺乏区块链应用开发工具和方法

区块链应用的开发需要一定的区块链技术积累，传统应用开发者搭建一套完备的区块链开发平台成本较高。

3. 不同公链之间的区块链应用是割裂的

由于公链的异构，区块链应用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应用，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。

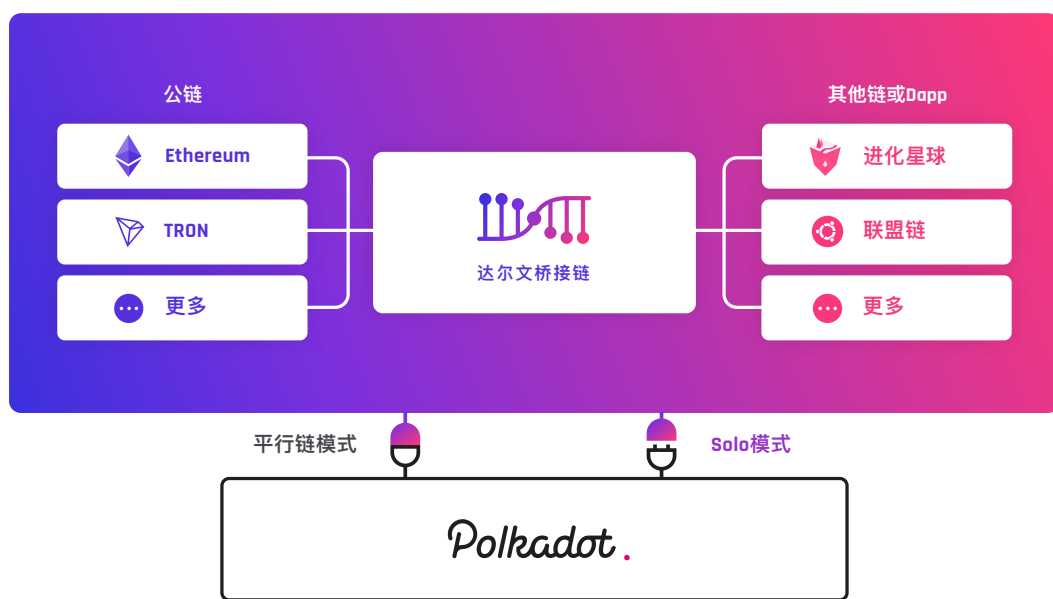
架构设计

达尔文网络是基于Substrate[1]技术构建的区块链网络，作为Polkadot生态的一员，同时又区分于Polkadot的是，**达尔文网络是一个桥接网络，并且主要专注于资产兑换协议方向的跨链业务。**

通过达尔文网络，区块链应用可以通过达尔文网络方便的进行资产的跨链交互和交易，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。**

达尔文网络的架构关系如下图所示

技术架构



达尔文桥接链

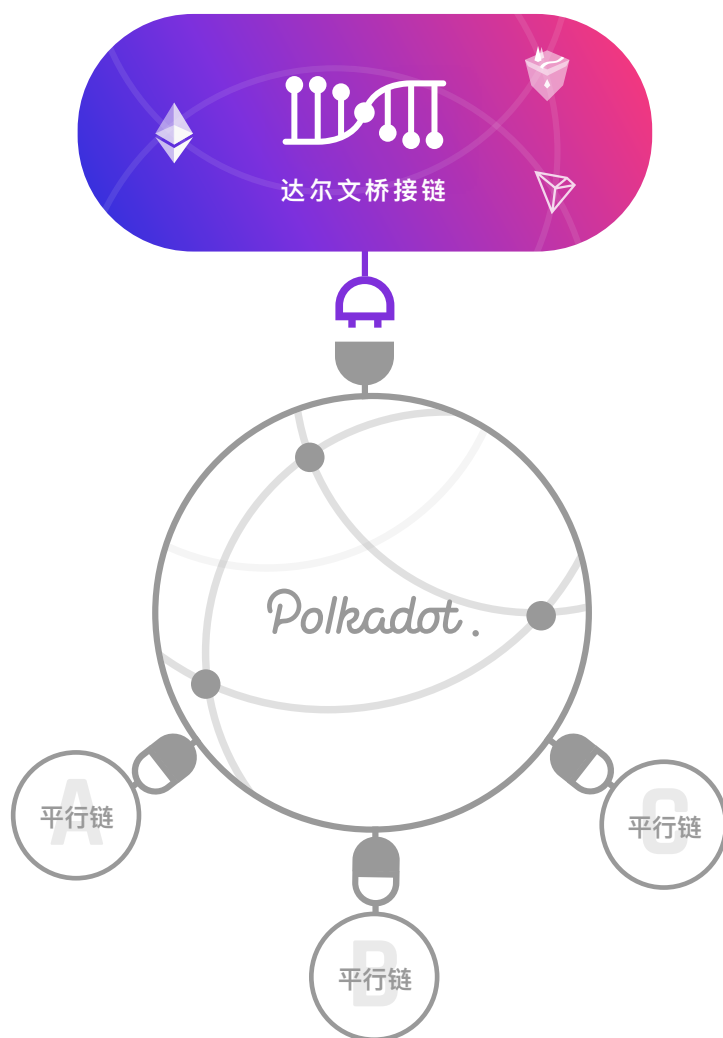
达尔文桥接链是达尔文网络中最重要的部分，也是各个应用子链和公链的桥接枢纽。

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提供了一套开放的平行链接入方式，达尔文链也可以选择接入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络。

为此，我们将达尔文链的运行模式分成了**Solo**模式和**Polkadot**模式：

Solo模式

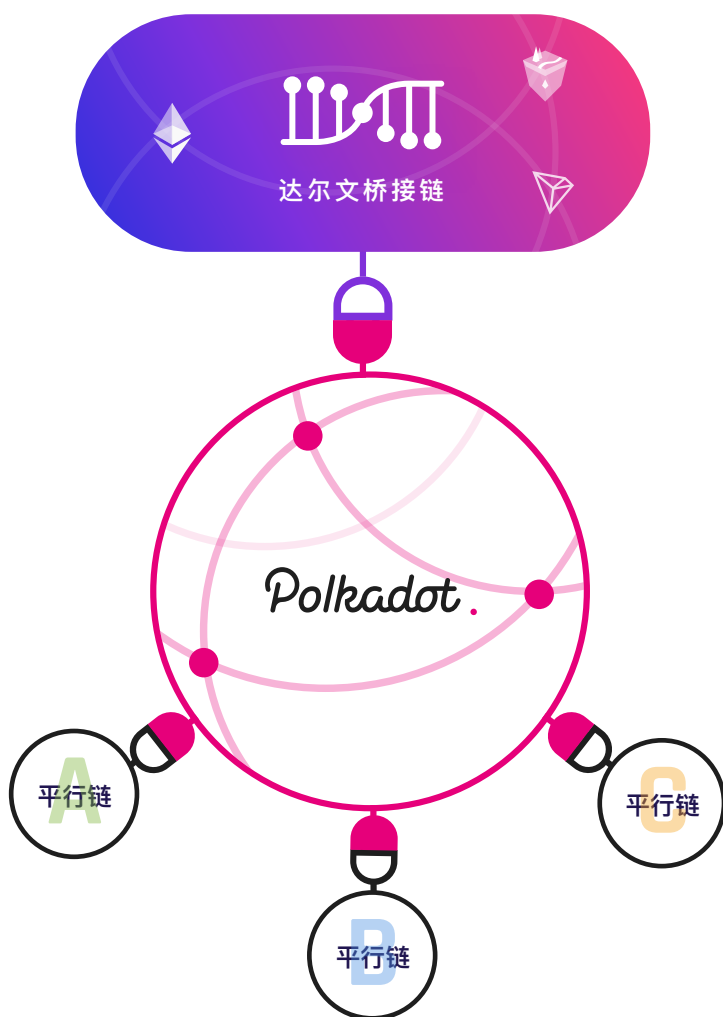
达尔文网络可以选择作为一个独立的公链网络运行，并负责自己的共识安全，其核心业务和应用业务，包括各个应用链的跨链功能不受影响。



Polkadot模式

在 **Polkadot** 模式下，达尔文桥接链将作为 **Polkadot** 的平行链。

因为 Polkadot 网络采用共享安全的模型，所以处于 Polkadot 连接模式时，平行链的跨链安全性将由 Polkadot 中继链的验证人来保证，达尔文网络在切换至连接模式后，原先的验证人和 Staking 机制将用于保证达尔文网络内部的局部共识，这样有助于帮助实现更快的块确认和更高的 TPS。这套局部共识机制也将帮助 Collator 来确定提交给 Polkadot 验证人的区块不会违反 Polkadot 全局共识。



应用链SDK

为了方便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 和达尔文网络应用工具集设计开发一套应用区块链的框架，被称为应用链 SDK。其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。

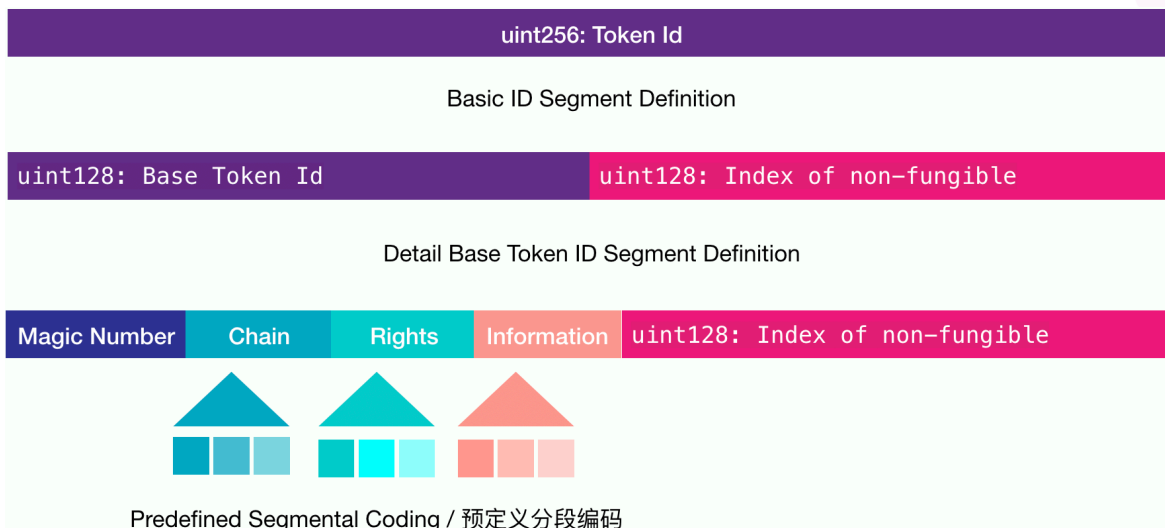
应用链 SDK 是一组区块链开发套件，可以满足应用开发者不同区块链定制需求，甚至一键发链，包括随机数服务和 DKMS 分布式密钥管理服务。基于这套 SDK 开发的应用链也将使用 Substrate 内核，将被设计成可以作为子链桥接至达尔文桥接链。

NFT 可识别性

对于不同的物品，我们会用一个唯一的标识来标记它。在虚拟领域，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。



经济模型

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。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。

RING在达尔文网络主网上线时的供应量为20亿，之后将会通过出块奖励将新发行的RING分发Staking系统和Treasury。

在达尔文主网上线后，该年的出块奖励每年调整一次，第N年的块奖励为剩余可发行供应量的 $1 - (99 / 100)^{\sqrt{N}}$ 。

剩余可发行总量 = 硬顶总量 - 当前供应量

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，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。

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

下面是预估的每年通胀率统计表

供应量	剩余可发行总量	年	当年发行占剩余 可发行总量 $(1-(1-1/100)^{\sqrt{x}})$	当年发行总量	通胀率
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%

奖励分配

达尔网络总包括出块奖励和达尔文网络交易手续费。达尔文网络交易手续费包括网络手续费，跨链服务质押费用，应用链链的接入费用，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。



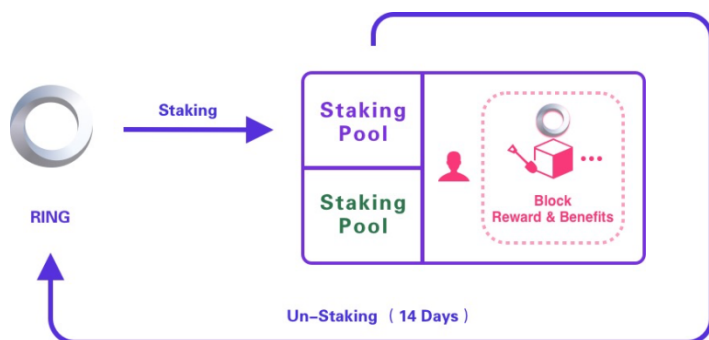
Treasury主要用于支付系统提案预算，可能包括NFT挖矿或App挖矿等系统运营提案，Polkadot槽位竞价激励，或者用于生态开发者支持。

Staking

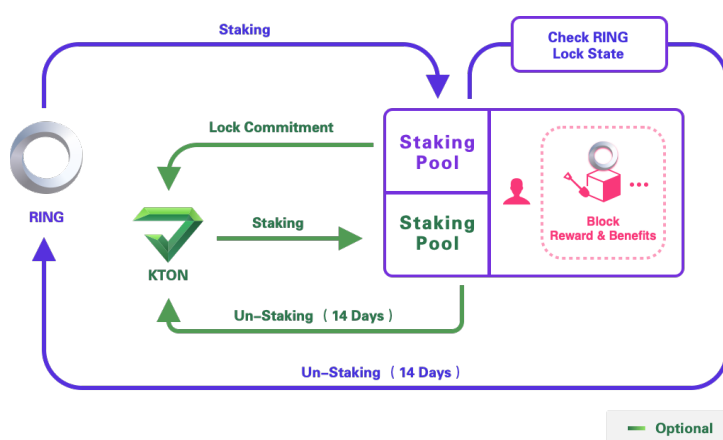
达尔文网络将会把主要收入作为激励分发给Staking的参与者。Staking的过程也可以理解为PoS挖矿过程，挖矿者通过质押资产来获得Staking能量来进行PoS挖矿。

一般来说，用户可以通过质押基础资产RING来进行PoS挖矿，如果用户开始取回Staking质押的RING，那么挖矿将停止，解除质押的RING将需要14天时间可以完全到账。并且基于参与者的角色，参与者可能会或可能不会提供基本的计算能力和网络带宽。只有充当验证人的用户提供服务，帮助达尔文网络中的用户在其中插入和查询数据。该作用在Staking算力部分中得到了很好的证明。

Staking按照简单和复杂程度，可以分为基础版和专业版。



基础版 Staking



专业版 Staking

氦石(KTON)

为了鼓励用户进行长期锁定和承诺投入，用户在**Staking RING**的过程中，可以**承诺锁定RING 3 - 36个月**，系统会给参与Staking的用户一个氦石的通证进行奖励，但在承诺锁定期间无法进行解锁RING操作(除非缴纳3倍的氦石罚金)。

因此，用户在使用RING进行Staking过程中，可以选择承诺锁定RING一段时间来获得氦石。氦石的初始供应量为零，但主网上线前进化星球应用已经开始锁定RING获得氦石，因此主网上线时将会存在一定的氦石供应量。最早通过锁定RING获得氦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氦石模型[5]。

氦石可以用于质押获得**Staking**能量，所以同样也可以参与**PoS挖矿**。用户通过质押氦石进行Staking，如果用户开始取回Staking质押的氦石，那么挖矿将停止，解除质押的氦石将需要14天时间可以完全到账。

Staking 算力

算力用于工作量证明（PoW）区块链挖矿模式中，例如比特币，算力的值代表该帐户提供的计算能力。PoW模式中帐户的奖励是基于算力的。

在达尔文网络中，挖矿的奖励不是由计算机算力决定的，而是由质押的RING和氦石的数量决定的，这样的机制叫做提名权益证明机制（NPoS），也属于权益证明的一种。Staking算力可以类比为PoW中的算力，某账户的Staking算力代表此账户当前时间对Staking的贡献值大小，PoW系统的安全性，是通过计算机算力的竞争来保证的，但是耗时巨大，造成巨

大的算力浪费，PoS系统的安全性是通过达尔文网络的产品，服务供应商大量的，高频率地使用实用型代币来保证的。

具体来说，在NPoS机制中，有两种角色，验证人和提名人，NPoS机制完成过程的时间是一个era（一段时间）。验证人可以在一个era内持有实体，提名人可以参与其中。根据参与者的网络 and 计算环境的不同，一个era大约是1周左右的时间，会因为计算机和网络环境延迟或提前。参与达尔文网络的帐户可以自由选择担任验证人或提名人，但在一个era中只能扮演一个角色。

换句话说，验证人是实体的领导者以获得奖励，提名人可以使用已质押的RING和氦石让一个或多个验证人参与，以帮助实体成为更大的实体，又有更多质押的RING和氦石。因此，实体中只有一个验证人，提名人可以依据质押的RING和氦石属于一个或多个实体。投票之后，拥有最多质押RING和氦石的实体的验证人成为被选出的验证人，有一些提名人会属于一个或多个被选出的实体。奖励只给予少量实体的验证人和提名人。

提名人决定用他质押的RING和氦石来让更多验证人参与的过程就叫做提名奖励机制（NPoS）中的投票。

在一个era中，只有当选的验证人才有权延长达尔文网络的区块链，因此如果当选的验证人不努力延长达尔文网络的区块链，则该实体的所有已质押的RING和氦石将被达尔文网络内的系统自动销毁。此外，验证人可以在投票之前确定验证人与提名人之间的Token奖励部分。通常，验证人和提名人是服务供应商或制造商，他们提供服务并使用RING作为实用型代币来交换其服务或产品。验证人和提名人之间的区别不在于他们提供的服务，而是基于他们对达尔文网络贡献的算力。验证人直接将算力提供给达尔文网络，提名人将通过投票给

更高质量的验证人来间接提供相同的算力。通常非常依赖RING来交换或提供服务，或者用大量的RING来提供服务的账户，将以更好的基础设施加入达尔文网络。使用较少的RING来交换服务的账户也可以通过投票出拥有更好良好基础设施的验证人来参与Darwinia网络。使用RING提供服务的账户业务可能会在不同的时间段内发生变化，因此Darwinia Network允许账户轻松更改提名人和验证人之间的角色。如前所述，PoS在计算能力和耗时方面均比PoW先进，与纯PoS系统相比，达尔文网络中使用的NPoS机制可能更好，这是因为只有少量的选定验证人参与了延伸过程。另一方面，少量的选定验证人可以在系统的强大和效率之间取得良好的平衡。

在一个era中，验证人为一个或多个计算节点提供网络可访问性，以充当网络服务的供应商，以帮助达尔文网络的用户在达尔文中插入和查询数据，因此从该服务中获得的奖励将赋予网络用户。在这个时代之后，平台上生成的额外的RING（作为Token奖励）被分为两个相等的部分。

一部分是给予质押RING的验证人和提名人，另一部分是给予质押氩石的验证人和提名人，然后，每个部分将根据已质押的RING百分比和已质押的氩石百分比发送给选定的实体。然后，根据投票之前确定的奖励分配比例，将每个实体的Token奖励发送给实体3中的验证人和提名人。前述过程由达尔文网络自动执行，而无需验证人的操作。此外，将执行另一个投票程序，以便将有新当选的验证人在下一个era拉长达尔文网络的区块链。

换句话说，账户得到的Token奖励由奖励分配比例决定，分配比例则由Staking算力呈现。

Staking算力可以类比为PoW中的算力，某账户的Staking算力代表此账户当前时间对Staking的贡献值大小，每个账户的算力值由该账户中质押的RING和氩石资产来决定，一旦解除质押，相应的算力也将消失。

账户的Staking算力比随其质押的资产多少不断变化，不能转移或者转账。Staking参与者可以通过修改投票支持的验证人，在不需要解锁质押的情况下，更改投票支持的验证人。

算力值有可能还将在系统的治理和升级中扮演重要角色。(备注2)

算力值占总算力值的比例称作算力占比。

$$\text{算力} = \text{总算力值} \times \text{算力占比}$$

$$\text{该账户算力占比} = \text{算力占比(RING部分)} + \text{算力占比(氩石部分)}$$

该账户的Staking奖励公式如下：

$$\text{账户Staking奖励} = (\text{达尔网络总收入} \times Y) \times \text{账户算力占比}$$

该账户的投票权重公式如下：

$$\text{账户投票权重} = \text{总投票权重} \times \text{账户算力占比}$$

备注1: RING算力贡献比例默认为0.5。

备注2: 因为氩石可以转售给其他人，所以流动性的氩石可能无法完全代表长期承诺投入，只有承诺锁定和质押的“资产×天数”才能准确代表对达尔文网络的承诺投入。

Slash 算法

为了防止验证人进行攻击，或者出块不稳定，当攻击或者错误发生的时候，系统需要对验证人(包括投票人)质押的资产进行惩罚，惩罚的过程和机制就是Slash算法。

因为达尔文网络中实际存在RING和氦石两种质押资产，因此需要对Slash的算法进行一些补充说明。

Staking系统中惩罚相关的参数将以百分比为单位，当Slash发生后，验证人或用户质押的资产将按照该百分比比例进行惩罚，无论其质押的资产是RING还是氦石。

另外，在达尔文网络质押系统中，RING存在四种主要状态，账户余额、Staking中、锁定Staking中、解除质押中。因此存在两种质押状态的RING资产，即Staking中和锁定Staking中，并且锁定Staking状态的RING有可能存在不同的解锁到期时间。因此在Slash发生时，需要确定不同RING质押资产被Slash的先后顺序和优先级。Staking系统将按照解锁到期的时间先后顺序，优先Slash那些较早到期的质押资产，也就是先Slash不在锁定状态的质押资产，然后Slash那些解锁时间先到期的质押资产。

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络开源软件开发商是 [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。

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。

生态应用

开放游戏应用

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应用链SDK开发，可以直接和达尔文网络链桥接。

开放金融(Defi)应用

在加密资产越来越多的情况下，与其相关的支付、借贷、质押、杠杆租赁和其他各种衍生资产的需求越来越多。除了目

前主要集中的Defi应用之外，游戏NFT和Defi的结合也有很多实际的需求，例如NFT的二手交易市场，NFT的抵押和借贷等等都会是比较落地的需求。

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络的开发建设和推广。[WIP]

波卡生态

在达尔文网络连接模式下，达尔网络将会作为波卡的平行链接入波卡中继链，因此波卡生态是达尔文网络十分重要的组成部分。

当达尔文网络打算连接至Polkadot网络时，根据Polkadot Parachain Auction[4]的模型，达尔文链将需要锁定足够多的DOTs来参与Parachain Slots竞价。为了获得足够的竞争力，达尔文网络将组织一系列活动，以激励达尔文社区参与推进平行链槽位竞价。

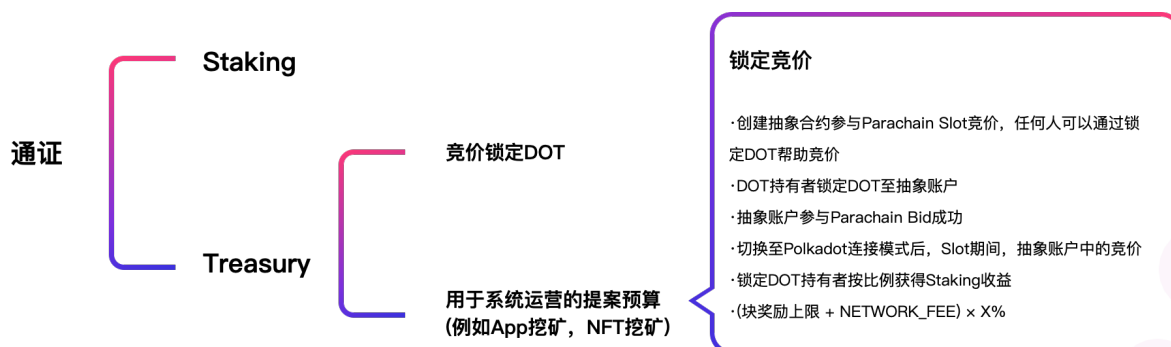
Polkadot的Parachain Slot拍卖竞价允许任何类型的抽象账户参与竞价，包括普通地址账户，智能合约账户，平行链账户。这种广泛的抽象账户支持为参与竞价者提供了灵活性，可以设计各种去中心化的竞价模型。

达尔文网络将为波卡连接模式设计参与Parachain Slots竞价的方式参与者不需要将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(或运行时模块)完成的，没有任何人可以控制这部分锁定的资产。

Polkadot槽位竞价激励提案

在连接模式下，达尔文网络可以基于这种设计发起提案，将提供一部分奖励，用于支持哪些帮助达尔文网络进行DOT锁定竞价的参与。

当达尔文网络切换至Polkadot连接模式时，达尔文社区的DOT持有者将可以通过提供DOT竞价锁定凭证，获得达尔文网络的提案奖励。



节点和验证人

通过参与 Staking 成为验证人，验证人通过保护系统安全、帮助系统出块记账，可以获得达尔文网络的 Staking 奖励。

跟 Polkadot 的参与者一样，跟验证人相关的还有一些其他的角色，例如 Nominators, Collaters, Fishermen 等。

用户

达尔文网络和达尔文应用链相关产品和服务的用户。

核心团队



钱晓栋

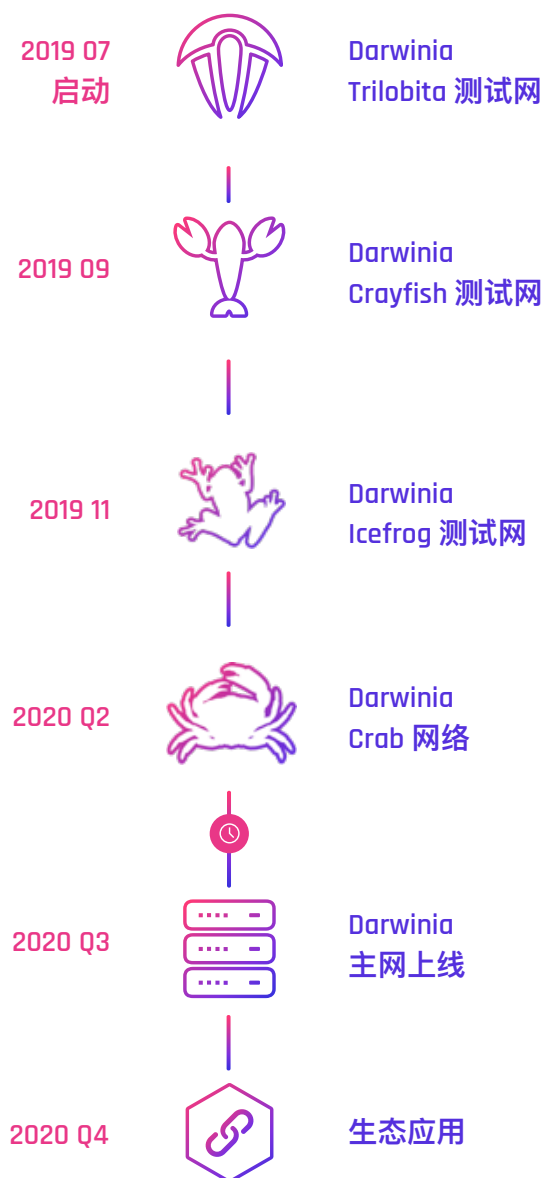
- 达尔文网络联合创始人
- 区块链及智能合约专家，高级技术顾问
- 于2011年投入比特币及区块链领域的技术工作，参与多个开源项目的技术开发
- 毕业于上海交通大学



王晓寅

- 达尔文网络联合创始人
- 区块链及智能合约专家，高级技术顾问
- BitShares 1.0 核心开发者
- 企业以太坊联盟中国代表
- 毕业于南京大学

路线图



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>

