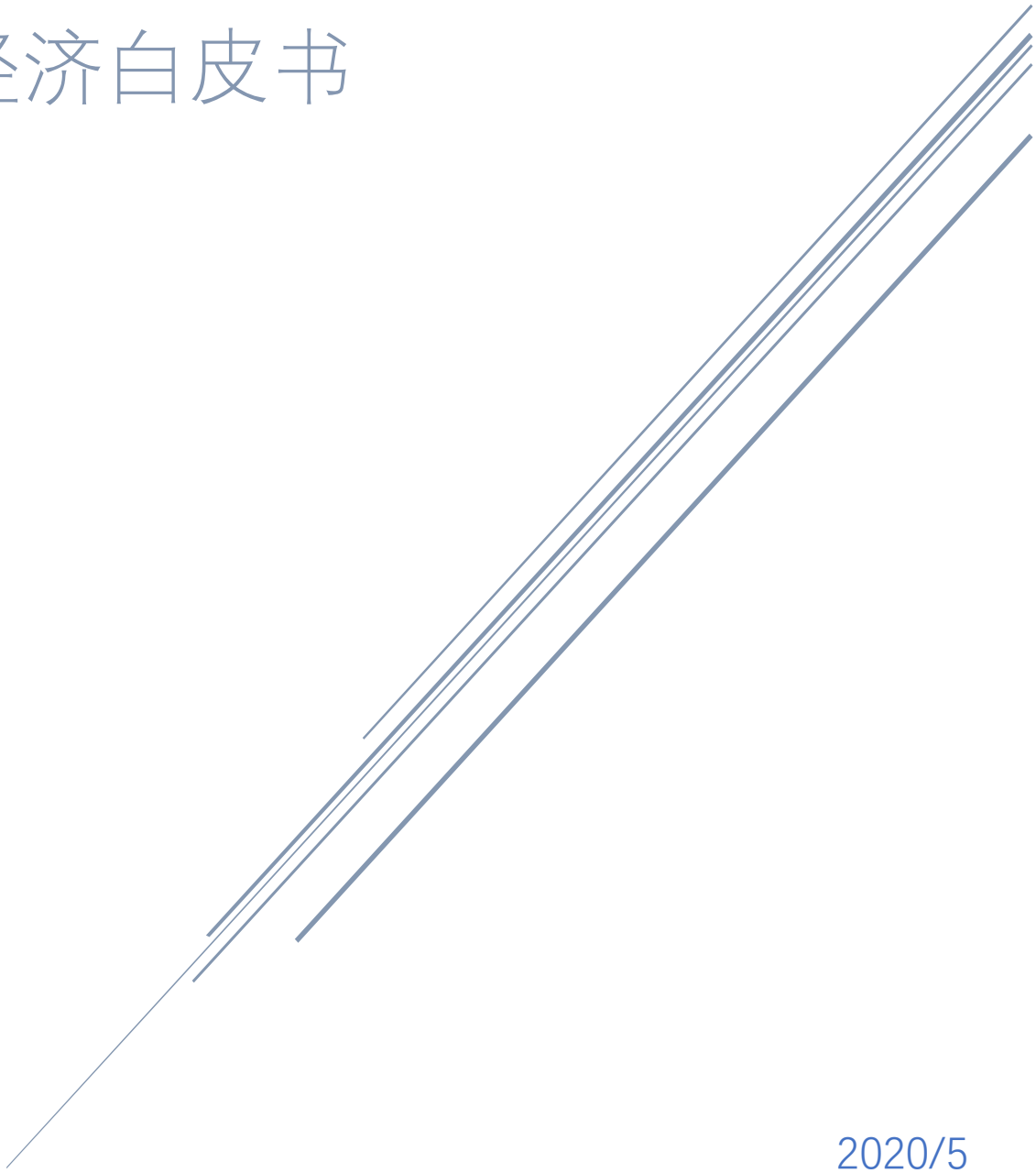
ECOMONY

经济白皮书



2020/5

Crust 经济模型和资产体系草案

1. 概述

Crust 作为一个去中心化的云系统是公有开放给所有人自由参与的分布式网络。这个系统由基金会孵化，在渡过它的成长期后最终会由社区自治。在这个系统中，无论是云服务的提供方、需求方还是维持系统的各个利益方都可在遵循系统协议的前提下自由进入和退出。Crust 的经济模型维持着各个参与方的利益，并保障整个 Crust 系统的发展。

2.经济设计目标

Crust 经济设计的目标是要将各方参与者的利益与 Crust 系统的价值增长保持同一个方向， 一方面要保障各方参与者利益，另一方面也维持 Crust 系统的稳定。即各个参与方在追求自身利益的同时也对 Crust 系统做出贡献。

为了达到我们的经济设计目标，我们要从几个方面思考：

如何保证 Crust 协议的安全性

如何维持 Crust 系统的可持续发展

如何保障参与方的利益

如何维持参与方利益与 Crust 系统价值在同一个方向

在设计 Crust 经济模型之前，我们先分析一下现有分布式系统的模型：

比特币作为最早的区块链协议，使用了原生的通证来激励节点验证交易，并使用 PoW 共识来协调节点之间的竞争。在比特币的经济模型中，早期区块奖励是维持节点利益的主要方式，在后期区块奖励减少后，手续费收入成为维持节点利益的主要方式。比特币普遍被认同的功能有两个：价值存储与流通支付。价值存储用户期望持有通证保值或者增值，他们关注比特币网络协议的安全、货币通缩政策；流通支付用户使用比特币网络的点对点价值传输功能，类似法币支付功能，他们关注比特币的交易费用和价值波动性。在不改变现有比特币经济模型的前提下，价值存储用户的利益得以保障，这类用户主导的网络里，不会产生许多的交易，从而长期来看手续费难以维持节点并保障网络安全性。这将影响到整个系统的可持续发展。

以太坊是最大的智能合约平台，原生的通证用于支付计算服务，和比特币类似，区块奖励减少后，服务费用可能成为维持节点利益的主要方式。不一样的是在以太坊网络里交易为主的流通支付用户更多，而且它的货币政策没固定，现在是一种通胀政策。规划中的 ETH2.0 系统将以太坊的共识更改为 PoS，设计成通过永续的通胀保障节点的利益，通胀会让通证的价值受到贬值影响。其经济模型将尽可能平衡这种关系。

Crust 在学习了其它分布式项目的模型后，根据自身项目的特点，提出了 Crust 经济模型和资产体系。

3.Crust 系统的参与方

在整个 Crust 系统里有多个参与方，它们各自有不同的需求，按照每个角色参与的方式，我们将它们分为：验证人、候选人、担保人、用户，在此文中提到的用户，主要指存储和计算资源用户。在 Layer2 层面还会有其它不同的用户角色，比如通证做市商。

3.1 验证人

验证人是 Crust 网络中打包并生成区块的节点，维护着整个区块链网络。同时根据 Crust 网络的 GPoS（Guaranteed Proof of Stake）共识，验证人节点需要有存储资源作为担保，才可以 Staking 相应额度的 CRU 通证（Crust 网络中的原生通证，在下一章节详细介绍），且需要保持在线。所以验证人节点也是一个提供存储资源的节点。参与到网络中的

验证人节点可以获得单独给予打包区块的奖励和区块链每个周期的奖励分成，且要承担被罚没资产风险。验证人也可以通过存储交易市场出让存储资源获得收益。

3.2 候选人

候选人是 Crust 网络中参与竞争成为验证人，但没有获得验证资格的节点。和验证人节点一样，候选人节点也需要有存储资源作为担保，才可以 Staking 相应额度的 CRU 通证，且需要保持在线。和验证人节点的区别是，候选人节点不参与生成区块，不能获得单独给予生成区块节点的奖励。候选人节点可以获得区块链每个周期的奖励分成，同时也可以通过存储交易市场出让存储资源获得收益。候选人和验证人并不是固定的，每一个周期它们的身份可能产生变化，主要依据每个周期末节点 staking 的通证数量决定。

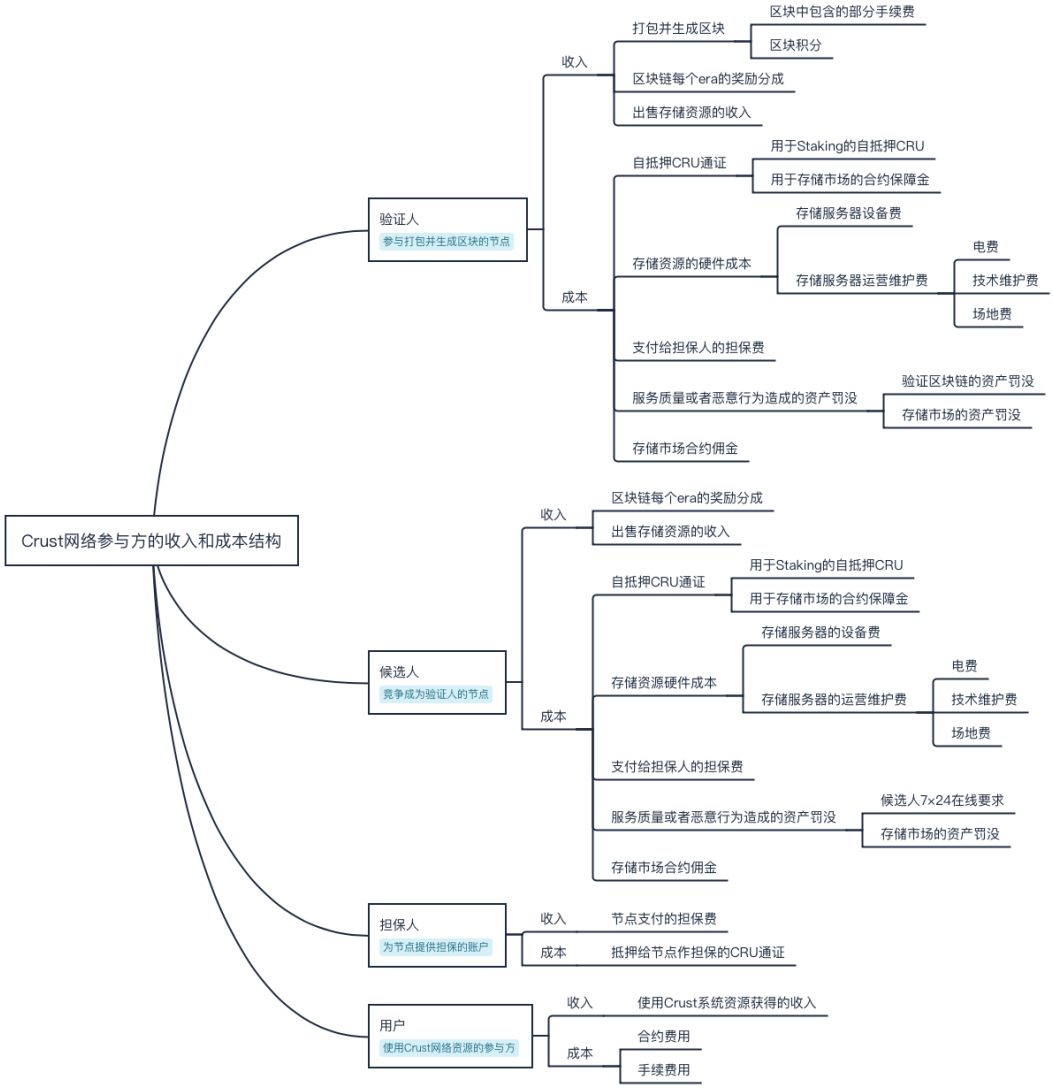
3.3 担保人

担保人是 Crust 网络中为任意一个或者多个节点提供担保的账户。拥有 CRU 通证的账户都可以成为担保人，可将其 CRU 作为担保资产。担保人为节点提供担保可以获得担保收入，同时也按比例承担节点被处罚风险。

3.4 用户

用户是指使用 Crust 网络资源的参与方，主要指存储和计算资源用户。会使用 CRU 通证或者 Crust 网络中支持的其它通证资产购买资源服务。

各参与方的收入成本结构如下图：



4.通证

Crust 网络中的原生通证 CRU 是实现整个网络价值的功能性通证。类似以太坊网络中的 ETH 或者波卡网络中的 DOT。

4.1 通证的功能

在 Crust 网络中，CRU 通证主要有以下几个功能：

1. Staking 维护 Crust 网络的 GPoS 共识

2.用于担保所选的节点

3.作为提供资源服务的合约保障金和佣金

4.作为使用网络的交易费

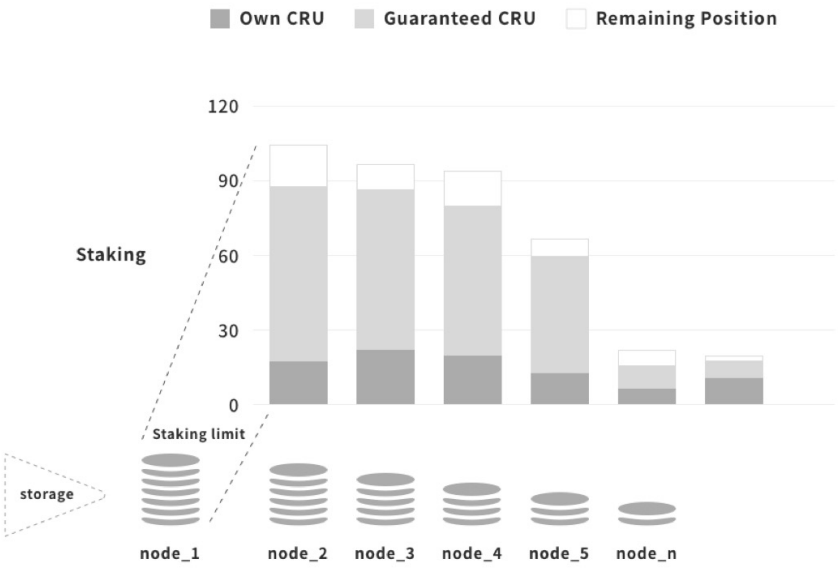
5.可用于购买资源服务

6.可用于链上治理机制的竞选和投票，并对提案进行表决

Crust 网络中的区块链共识是 GPoS（Guaranteed Proof of Stake）共识，称为有担保的权益证明。GPoS 是一种混合了 PoW 的 PoS 共识，机制上结合了 PoW 的资源公平性和 PoS 链的高性能。和现有的 PoS 项目类似，节点需要将 CRU 通证 Stake 来竞争生成区块的权利，不一样的是节点还需要有存储资源作为担保，有了担保额度才可以 Stake 相应数量的 CRU。在这个机制下需要有存储资源和 CRU 通证两类资产才可以成为节点，将资源型（如比特币）和通证型（如 Cosmos）共识机制的优点结合起来，更有效的保证网络安全性。如果想从共识上攻击 Crust 网络，除了需要拥有大比例的 CRU 通证，还需要能控制足量的存储资源，这样的设计会让攻击难度变得非常高。

节点在拥有存储资源担保的前提下，还可以寻求担保人使用 CRU 为其担保。即节点 Stake 的 CRU 可以是自有的也可以是来自担保人。当担保人用 CRU 为一个节点做担保时，其担保的 CRU 数量和节点自已 Staking 的 CRU 数量将合并计算成为节点 Staking 的总量。节点为了吸引担保人为其担保，需要支付担保费用，担保费率由节点自行设定，担保人选择自己愿意接受的担保收入去为节点担保。担保人选择为节点担保也需要承担节点被处罚的风险。如果节点因为触发了处罚机制被系统罚没资产，担保人也要按所担保比例被罚没。在这个机制下，担保人会倾向选择诚信的、服务质量好的节点而为其担保，在担保收入和处罚风险之间由市场决定出一个平衡。

GPoS 共识的运行如下图所示：



作为一个底层数据存储的网络协议，Crust 提供了存储资源交易的功能，CRU 通证在这个交易市场中作为交易合约的保障金来保障交易市场次序。

和其它区块链项目类似，CRU 通证还会作为使用网络的交易费，类似以太坊中的 Gas。它也可以直接用于购买网络中的资源服务。

Crust 系统的治理机制会使用 CRU 通证进行链上的议会竞选和投票，并对提案进行表决。

4.2 通证的产生与销毁

CRU 通证的产生方式有两种：一种是主网启动时一次性产生；另一种是随着区块的生成而产生。

Crust 主网启动时产生的通证数量为：20,000,000 CRU

主要用于以下几个方面：

7,000,000 CRU 有成本的投放给社区发展**#包括 Lockdrop、Worklock 等

1,000,000 CRU 用于 Crust 生态建设

4,000,000 CRU 转让给专业投资机构**

4,000,000 CRU 给予技术团队奖励

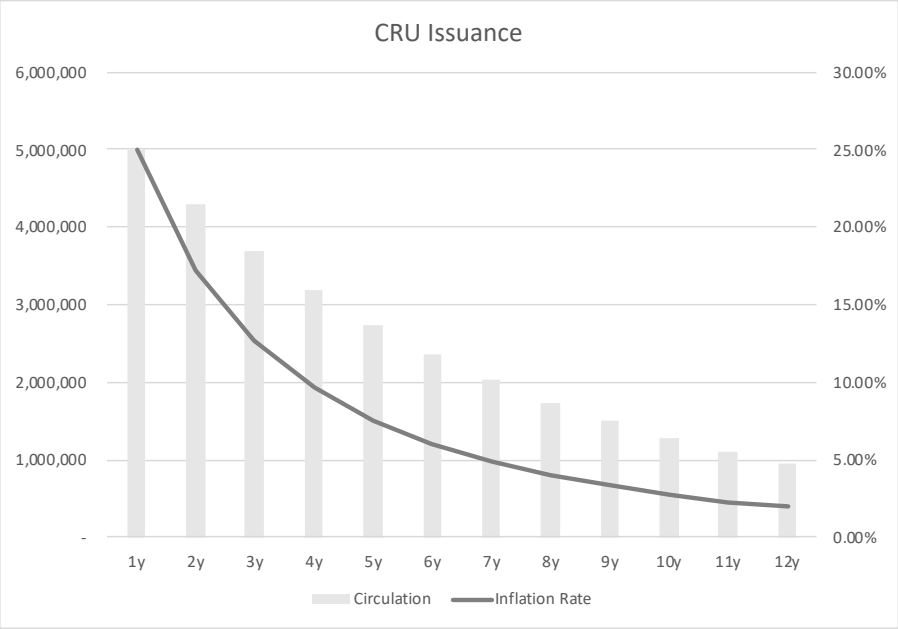
4,000,000 CRU Crust 基金会预留

随着区块生成的通证有每个周期的奖励和积分兑换奖励，主要是奖励给参与网络中的节点，维持网络协议的安全性，并在早期激励各个参与方参与到网络中来。总发行方式如下：

第一年 5,000,000 CRU

从第二年开始每年发行总量为上一年的 86%，直到全网通胀率达到 1.8%时不再减少。具体数据如下图表：

时间	发行量	通胀率
1y	5,000,000	25.00%
2y	4,300,000	17.20%
3y	3,698,000	12.62%
4y	3,180,280	9.64%
5y	2,735,041	7.56%
6y	2,352,135	6.04%
7y	2,022,836	4.90%
8y	1,739,639	4.02%
9y	1,496,090	3.32%
10y	1,286,637	2.77%
11y	1,106,508	2.31%
12y	951,597	1.95%



节点如果服务质量不稳定或者被发现有作恶行为可能会面临 CRU 通证的罚没，被罚没的通证有一部分会直接销毁，有部分被放入 Treasury 账户作为储备。网络中由于交易产生的费用，有一部分基本费用会直接销毁，剩余部分分配给生成区块的节点。

4.3 通证的价值

CRU 是 Crust 网络的功能性通证，其价值依赖 Crust 网络。它的价值和 Crust 网络的规模正相关，当 Crust 网络被大量的用户使用时，CRU 的需求相应的会上涨。CRU 通证捕捉网络价值的方式主要有两类，一类是当被使用时在网络中锁定或者占用从而减少了流通的总量。比如存储和检索服务的保障金、购买存储服务的付费、链上治理的投票、共识机制中的 Staking 等等；另一类是当被使用时会销毁从而减少了通证的总量，比如一部分交易手续费。

5. 经济模型

Crust 经济模型主要解决的问题是在保证网络协议的安全性前提下，合理的分配各个参与方的利益。经济模型能激励各个参与方加入到网络的同时，也能使系统变得更强壮、更加安全、更加有价值，并使用 CRU 通证作为价值承载和价值流转维持系统的可持续发展。

5.1 GPoS 共识的设计

GPoS 的设计除了要维护网络的安全，还追求尽量优化 PoW 下的工作量匹配实际市场对工作量的需求，使得工作量是有意义的（Meaningful Proof of Work）。CRU 被用作 Staking 来维护 Crust 网络的 GPoS 共识时，节点需要有存储资源担保才会拥有可 Stake 的额度，其存储资源和 CRU 额度之间有换算比率 X，即一个单位的存储资源可产生多少单位的 CRU 额度。X 在系统中的设计为：

$$X = \mathrm{R} \times (1 + Y \times Z \times M) \times \frac{Amount_{cru}}{\mathrm{Storage}}$$

*X:存储资源和 CRU 额度的换算率

*M:有效存储比，即节点的有意义存储数据量和自身提供的总容量比

*Amout_cru: 全网总的 CRU 通证数量

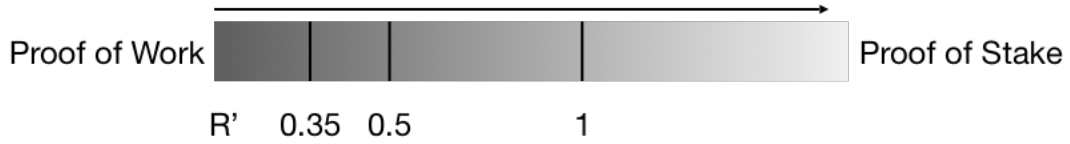
*Storage: 全网的总存储资源量

*R：换算系数

*Y：有效存储系数

*Z：有效用户指标系数

有意义的存储数据是指用户在存储市场中通过签订存储合约后上传给节点的数据。在这个设计中，我们定义 R'=R×（1+Y×Z×M），R' 系数设定了系统里可以质押的 CRU 上限。当系数设计较低时 GPoS 共识的经济特性会更接近于 PoW 共识，这时网络的安全性主要由存储资源保障，利益分配会流向资源节点；当 R'系数的设计较高时 GPoS 共识的经济特性趋近于 PoS，网络的安全性主要由 Staking 在网络中的 CRU 通证来保障，利益的大比例将分配给持 CRU 的账户。则如下图：



我们将 R=0.4，同时 Y=0.25，Z=1（当有效用户数>=30；如果有效用户数<30，则 Z=0），因此得出：

$$X = 0.4 \times (1 + 0.25 \times 1 \times M) \times \frac{Amount_{cru}}{\mathrm{Storage}}$$

其中，有效用户是指和节点签定合约并且合约在有效期内的用户。这样设定下，当存储节点都是空盘情况下，总的可 Stake 额度占全网流通 CRU 的 40%，如果硬盘使用空间存

满有效文件后，可 Stake 额度占全网的 50%。对于节点来说，提高有效数据存储比增加存储资源更经济，会激励节点尽可能的将存储变成有意义存储。

在分析了现有的 PoS 项目的通证 Staking 比率后，普遍被认同的安全比率约为 0.35~0.66，也就是 PoS 系统中被锁定的通证占总量的 35%~66%。而实际项目中，Staking 比率区间可为 0.15~0.85，具体的原因是项目所在的阶段和 Staking 收益率决定。下表是 cosmos 和 tezos 项目的 Staking 情况：

项目	staking 比率	通胀率	共识
cosmos	73%	7%	BPoS
tezos	78%	5%	LPoS

设定换算系数，只是规定了全网能 Stake 多少 CRU，具体实际上会有多少 CRU 参与 Staking 和参与的收益率相关。从上表中 Cosmos 和 Tezos 项目的数据可看出，在项目早期，通证的功能性没有发挥出来时，用户比较倾向将通证质押在系统里赚取分红收益，在收益率为 6%~8%时 Staking 比率可占 75%左右。在 Crust 系统里，当通证的价格较低时，节点不会盲目扩张存储资源，这和所有 PoW 项目类似；当通证价值被认可后，会带来价格上涨，Staking 比率会相应下降，节点扩张存储资源来增加 CRU 抵押额度也并不会直接带来收益，会减弱节点扩张的意愿。如果通证的价值是由于存储市场的发展带来的，节点在存储市场的收益才会驱动它增加存储资源。这样的设计让资源供应更根据市场需求来变化，而非单纯的依赖通证价格上涨。

在渡过了区块奖励期以后，Crust 网络中的通证通胀率会维持在比较稳定的比例，通胀率会影响全网 Staking 比率。具体的设计如下：

永续通胀率：1.8%

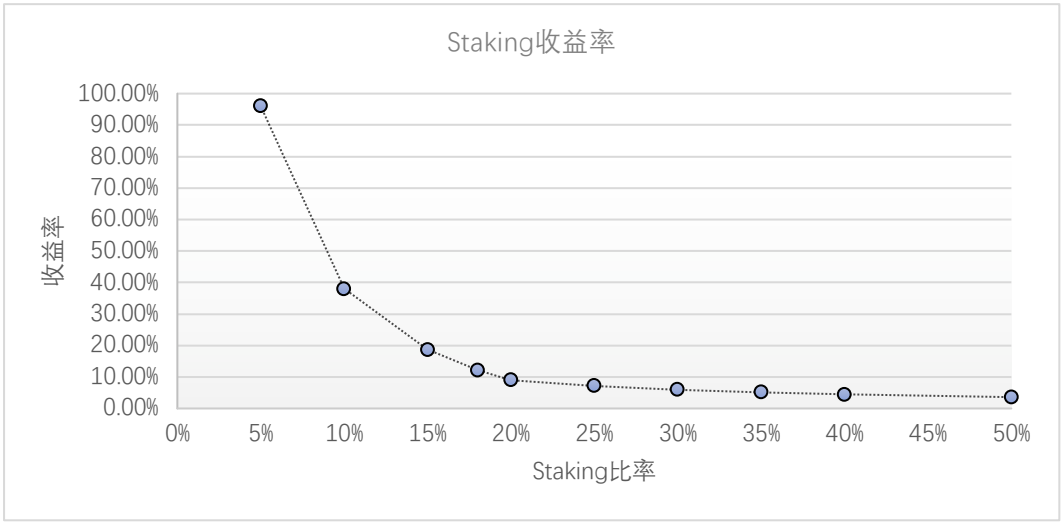
当 staking 比率低于 20%时通胀率：$1.8\% + \left(1 - \frac{\text{staking\_rate}}{0.2}\right) \times 0.04$

对于 Staking 比率，我们预期的短期目标为 50%，中期大约 35%，长期在 20% ~ 35%之间。因为低于 20%后，网络安全性会快速下降，所以在全网 Staking 比率低于 20%时我们设计了收益补偿。

全网的 Staking 平均收益率 r 为：

$$r = \frac{0.018 + \left(1 - \frac{\text{stakin\_rate}}{0.2}\right) \times 0.04}{\text{staking\_rate}}$$

其收益率曲线如下图：



Crust 系统里，节点 staking 的 CRU 可以来自节点自有也可由担保人为其担保。我们进一步分析作为节点或者担保人参与网络的投资回报：

我们定义验证节点的 ROI（Return On Investment）为：

$$ROI = \frac{Rv + Re + Rs - Fg - Fs}{C\_node + Cm + Vcru}$$

*C_node：为节点参与网络投入的硬件成本

*C_m：为节点硬件维护成本

*V_cru：为节点自有 Staking 的 CRU 价值

*R_v：为区块链的区块生成奖励（其包括区块中包含的交易手续费和区块积分）

*R_e：为区块链每个周期的奖励分配

*R_s：为存储市场收入

*F_g：为节点支付给担保人的担保费

*F_s：为节点被罚没的费用

候选人节点相比验证人节点少了生成区块的工作，不用承担生成区块的处罚风险，也不享有 R_v 收益。节点投入的资产成本类别有硬件设备、电力费用、人工费用、场地费用、CRU 通证资产，收入有 CRU 通证以及交易市场可自主决定的资产类别，主要分为以法币计价资产和 CRU 通证资产。由于存储资源有独立的交易市场，其 ROI 可单独列算为：

$$ROI = \frac{Rs}{C_{node} + Cm}$$

存储资源的 ROI 和现有的云存储厂商类比，最终会由市场化决定收益率。考虑到在系统的早期存储市场的不完善，R_s 应该较小，Crust 系统设计了较高的 R_e 来保障节点的收益，并随着系统的成长 R_e 会逐渐减少。在 R_e 减少到稳定比例后，节点通过 Staking 的 CRU 通证有独立的 ROI 计算，其中验证节点为：

$$ROI = \frac{Rv + Re - Fg - Fs}{Vg + Vcru}$$

*V_g：为担保人为节点担保的 CRU 价值

候选人节点 ROI 为：

$$ROI = \frac{Re - Fg}{Vg + Vcru}$$

验证人节点和候选节点 Staking 的 ROI 和全网的 Staking 平均收益率 r 有很大关系。因为系统的通胀占节点收益的比较大比例。当手续费和交易市场佣金收入占比提高后能显著提高 ROI。

在不考虑节点罚没的情况下，担保人的 ROI 为：

$$ROI = \frac{Fg}{Vg}$$

担保人的投入资产为 CRU 通证，收入也为 CRU 通证。资产类别相同的情况下，以 CRU 币本位计量投资收益率。其收益率会由市场化决定，其值可参考 Cosmos 和 Tezos 项目中的委托投票人收益率。

5.2 交易费用组成

在区块链网络中，典型的资源和相应的费用设计方式如下：

有限的区块大小，通过计算每笔交易占用的字节数来收取交易费；

有限的区块生成时间，通过计算或者性能测试得出不同交易所消耗的时间；

链上状态的存储资源，通常方式有一次性付费和租赁两种模式。一次性付费发生在交易处理过程中，在开发时对此费用评估。租赁模式还会考虑某个交易占据链上状态的时长，超时之后对相应状态进行清除。

Crust 系统设计里，交易费用由以下几部分组成：

总费用=基本费用+（字节费用+权重费用）×（1+动态调节费率）+小费

基本费用是每笔交易都需要支付的费用，字节费用=每字节费用×字节数。系统会给一个初始的费用配置，并可以随着升级进行更新。动态调节费率是一个会根据区块资源使用比例进行调节的费率，当网络资源使用率较高时会增加交易费；当网络资源使用率较低时会减少交易费。小费是由交易发送者自行决定的费用，当网络特别拥堵时可增加小费提高交易被打包的优先权。

基本费用会直接销毁，其它费用会支付给打包区块的节点。销毁的基本费用让系统中的通证通缩。

5.3 罚没机制（后续更新）**

6. 交易市场

Crust 第一阶段会完成存储资源的交易市场，让存储资源提供方和存储资源用户可以在这个市场中交易，在未来会进一步引入计算资源市场。

6.1 存储资源交易市场

在存储资源交易市场中，提供的服务主要包括两种类型：文件存储服务和文件检索服务。存储资源提供方为 Crust 网络中的节点，包括验证节点和候选节点；存储资源用户为有数据存储和检索需求的用户，包括 Web2 中心化云存储用户、Web3 生态中有大数据存储需求的去中心化用户。

为了满足存储市场服务需求，资源提供方需要做到 7×24 小时在线，我们在对验证节点和候选节点的入网协议中设计了相应的机制，在交易市场中对节点在线提出了进一步要求。不同于在 GPoS 共识中对节点提出的在线要求（具体可参考 GPoS 共识介绍），存储服务响应和区块链验证是分开工作的，所以节点需要有额外的抵押来保障存储服务，我们称这个抵押资产为保障金 G，系统规定最低的保障金 G 为 10 CRU。用户方则不需要有在线要求。

6.1.1 文件存储服务

在一笔典型的文件存储交易中，用户一般会租用一段时长的存储空间，从而为对应的空间和时长付费。这笔费用 P 在交易合约生效时会锁定在网络中，随着时间分批解锁付给提供存储空间的节点。为了保障在这一段时间中出让空间的节点能保证服务质量，系统会要求提供存储空间的节点质押一定的 CRU 通证资产作为合约保障金 G，直到服务终止这笔保障金 G 才可以解质押。保障金 G 只可以使用 Crust 原生通证 CRU，费用 P 可以是节点愿意接受的资产，可以是 CRU、稳定币或者其它通证资产，但需要在通证交易市场中与 CRU 可交换。在合约存续期，用户不可以取消定单合约，存储节点可以申请终止合约，但需要扣除相应比例的保障金。Crust 网络中初始设定：

$$\boldsymbol{Vg} \geq \sum Vp$$

*Vp:用户付费 P 的市场价值

*Vg:节点保障金 G 的总市场价值

即在交易合同生效时，按通证交易市场中的价格，存储节点的保障金 G 需要在交易市场的价值大于费用 P 可以等价交换到 CRU（不计手续费），最低保障金为 10 cru。合约生成时，会从保障金中提取合约价格的 0.5%作为合约佣金进入到区块链下一个周期的奖励分配池，合约佣金的最小值为生成链上交易合约的手续费。如果存储节点提前申请终止合约，剩余的费用 P 会退还给用户，而保障金的一部分比例会被系统罚没。（##关于存储市场罚没机制，设计待完善）

6.1.2 文件检索服务

和文件存储服务类似，用户可以对某个节点上的文件发起检索服务请求，并为这项服务支付费用 **Pr**，从而会生成一份检索合约。节点在完成了用户的检索服务后可以收到这笔费用 Pr。同样地，会从保障金中提取合约价格的 0.5%作为合约佣金进入到区块链下一个周期的奖励分配池，合约佣金的最小值为生成链上检索合约的手续费。和存储合约不同的是，检索合约的支付费用 **Pr** 中的一部分比例会被发送到特定的账户 **A**，如果用户将检索收到的文件发送验证报告到链上，它可以收回被发送到特定的账户 **A** 的资产。这样做的目的是为了鼓励用户验证收到的检索文件。

6.1.3 钓鱼任务

Crust 网络中设计了一个钓鱼任务机制来检查节点是否提供了文件检索服务。通过 VRF（可检查的随机函数）挑选出的用户可接受这个随机任务，当它完成了这项任务检索任务后它可以从特殊账户 **A** 中分到一部分奖励。

6.2 计算资源交易市场

Crust 网络未来将会支持去中心化的云计算，与存储市场不同的是，计算资源服务一般不会为时长质押资产，而是用户直接以手续费的方式支付计算服务。这个交易市场的设计在后续的版本中更新。

6.3 通证交易市场

为了服务 Crust 网络中的各方参与者，Crust 网络中提供了一个去中心化的通证交易市场。在这个通证交易市场中，多类通证可以与 CRU 进行交换。由于 Crust 是基于 Polkadot 生态的 Substrate 框架开发，并且将会以平行链接入 Polkadot 网络，可以方便的接受生态内各类其它通证与 CRU 的交换。

在上文中我们提到存储市场的参与用户包括 Web2 中心化云存储用户、Web3 生态中有大数据存储需求的去中心化用户，传统的 Web2 用户作为消费者会偏好于使用价值稳定的货币来购买存储服务，比如稳定币；Web3 生态的用户也可以很方便的使用自身项目的通证来购买存储服务。提供存储资源的节点也可以选择自己愿意接受的资产来给服务定价，当用户支付的资产与节点接受的资产不同时，通证交易市场可以提供实时通证交易，只需要支付一定手续费。

7.链上治理

Crust 使用 Substrate 技术搭建了链上治理机制，和经济相关的主要作用是针对于 Treasury 账户资金的处理，以及未来可能出现的对系统改进的提案。在网络运行时，节点因为一些原因被罚没资产，这个操作有可能因为网络不完善而错判，我们希望通过一个渠道纠正这样的错误。链上治理的投票功能可以让 CRU 通证的持有人参与网络的建设。链上治理机制仍然在开发中。

8.参考文献

[1] Satoshi Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
[2] Ethereum “A Next-Generation Smart Contract and Decentralized Application Platform” 2014
[3] Polkadot: Vision for A Heterogeneous Multi-Chain Framework 2017
[4] Cosmos: A Network of Distributed Ledgers 2016
[5] John Maynard Keynes “The General Theory of Employment, Interest and Money” 1936
[6] What is Tezos https://tezos.com/get-started
[7] Filecoin: A Decentralized Storage Network 2017
[8] More