

# 基于区块链的分布式超级计算项目 （分布式渲染等）

技术白皮书以及商业路线图

（2018.4.2）

版本 3.0

## 1.写在前面的话

如果比特币能把算力大部分输送到有效的运算里面，少部分算力用于区块生成，大部分算力做商业运算，这将是一个多么美好的事情，当时为此，我在 boinc 论坛看了很多技术方面的帖子，我意识到，在那个时候想要开发这么一套系统，将是一件多么难的事情，你需要有自己的钱包，有自己的公链，需要开发一套分布式计算的中间件，还需要在中间件基础上开发应用层的应用软件，这是一件多么大的工程。但是社区 没有停止这方面的探索，这几年，我们可以看到，在基于区块链的分布式计算领域，涌现出了不少项目，他们各自有各自的 idea 从 girdcoin 到 GNT SONM 还有 IEX.EC 下面，我将在我个人的理解范围内，与大家一起分析探讨基于区块链的分布式计算项目，未来可能应该要走的路

## 2. 分析现有的典型的区块链分布式计算项目

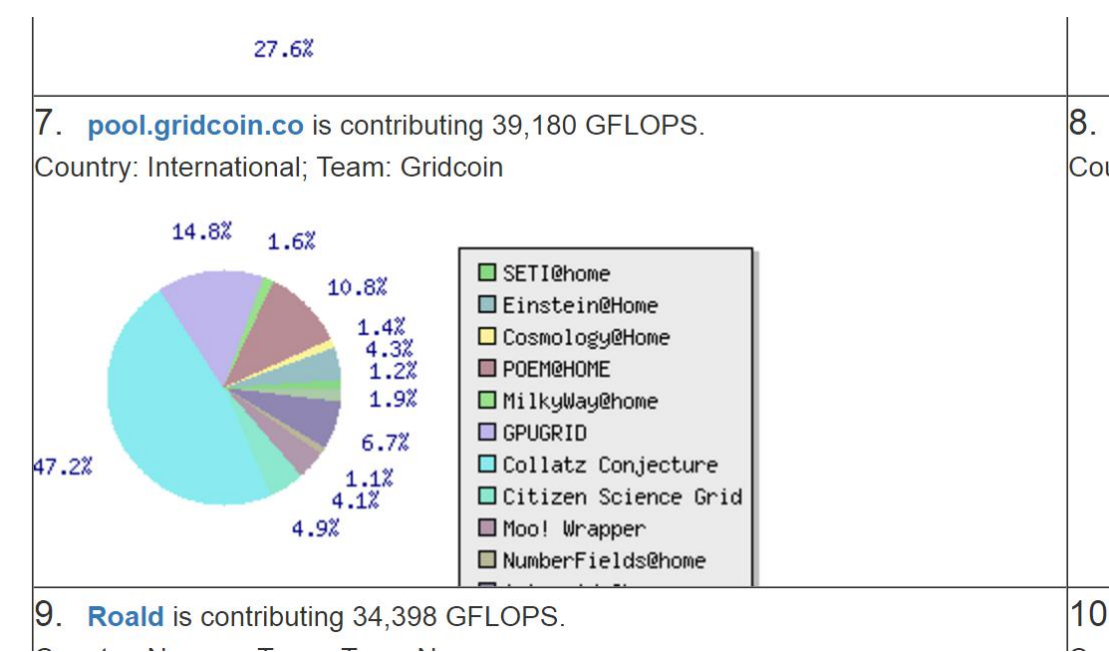
Gridcoin

Gridcoin 应该是 13 14 年那一波山寨币泡沫中幸存的代表。那时候基

于比特币钱包改的山寨币也不会比现在的 ico 项目少多少，从技术上来讲，gridcoin 目前大概只能将全网算力的 50~60%输送到 boinc 项目里面去做有效的运算，剩下的算力还是老传统的显卡挖矿，也就是说，从利用效率来讲，他的利用度不高。我们再来分析一组数据，从 boinc 官网我们可以看到 <http://boinc.berkeley.edu/>

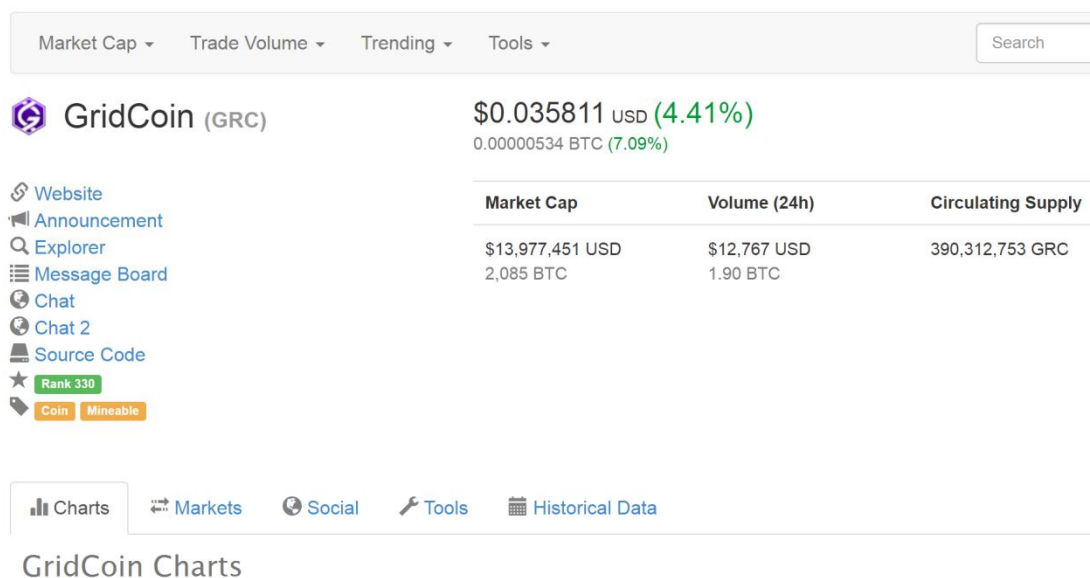


有几个数据我们需要记录下来，24 小时平均算力 2.2384 万万亿次浮点运算能力 837754 台计算机，170907 志愿者 平均每个志愿者贡献 5 台计算机。我们再通过这个地址 志愿者排名前 100 名的地址 [http://boinc.berkeley.edu/chart\\_list.php](http://boinc.berkeley.edu/chart_list.php) 我们可以看到



我们可以看到 gridcoin 矿池贡献了 39180GFLOPS 的算力 排名第七名，那么，39180GFLOPS 是多大的算力？giga floating-point operations per second 每秒十亿次浮点运算数，十亿次浮点运算/秒 gridcoin 贡

献的算力就应该是 391800 亿次浮点运算数/秒。占 BOINC 总共算力的比例是  $391800/223840000=0.0017503573981415$  这个比例真的很小。不过排名第一名的贡献算力也跟 gridcoin 差不多。我们可以换算出 gridcoin 上面运行的计算机数量是  $1466*2=3000$  台计算机。Gridcoin 差不多是一半的算力输入到 boinc 一半的算力进行区块生成。我们再看看 coinmarketcap 上 gridcoin 的市值。



Gridcoin 目前市值 1400W 美金。3000 个节点 平均每个节点价值 4600 美金。这反应出了社区对区块链的分布式计算有很高的期望。

Gridcoin 因为架构古老，目前算法只能输送 50~60%到 BOINC 项目里面，而 BOINC 属于公益性的分布式计算，而 we 希望能探索基于区块链的商业化分布式计算框架，所以很明显，gridcoin 难堪重任。

## GNT SNM RLC

把这 3 个放一起，是因为这 3 个项目均属于以太坊上面的项目。只是各自的侧重点不一样，在我个人的理解范畴里面，他们还算不上真正

的基于区块链的分布式计算项目，他们只是在支付手段上使用了有智能合约的 ERC20 代币。他们最大的风险在于，支付代币是运行在以太坊上面的，如果项目发展很好，以太坊扩容不够，那么转账速度很难保证，然后因为项目是运行在以太坊上面，没有自己的主链，ERC20 代币仅仅只是项目的支付手段，实际上，我个人的理解，这 3 个项目其实也可以不用以太坊智能合约代币来运行的，他们完全可以自己做个网站，用美元支付也好，欧元支付也好，本质上，不会有太大的区别。反而使用智能合约，在一对一的使用场景中，增加了处理欺诈作弊交易的难度。

### Supercomputing

我们可以叫它超算链。在超算链的技术架构蓝图中，我们使用一项名称有效的工作证明机制，让极少部分矿工挖矿，大部分将算力输送到链上的付费需求中去，超算链从底层设计上就是要付费使用的，哪怕是每次使用付费一分钱，也是需要的。自有主链设计未来可以扩展更多的功能，将算力的需求者与算力的提供者从古老又简单的一对一的买卖关系，改造成链上付费进区块见证，链下计算积分评论的模式，也就是说，收入统筹，分配按劳分配，这是设计的基础共识，在这种设计场景里面，欺诈作弊已经没有任何意义。

### 3 我们的愿景

构建一个基于区块链的分布式计算平台

Supercomputing 超算链会有一个属于自己的主链，2.5 分钟出块，少部分矿工维护出块，大部分矿工通过 dapp 将计算机资源输入到需求者手里，输送的资源不仅仅是 CPU GPU 的计算能力，还可以是存储空间，上传带宽，IP 资源，因为采用链上付费见证，链下计算，链上评分的机制，我们会成立一个非盈利性基金会，用于推广，维护主链代码更新，制定一套 dapp 开发收录标准，运营 dapp stone。我们还需要成立一家以创始人 共同创始人 早期投资人 非盈利性基金会共同控股的 dapp 软件开发公司，开发基于分布式计算平台开发能与传统企业竞争的有商业价值的大型 app，在拥有足够节点的情况下，还可以为有需求的企业单位开发定制的分布式计算软件，因为节点都是闲置的手机计算机资源，只要开发的软件使用性不比传统模式开发的软件差，由于巨大的成本优势，商业公司会取得合同，获得利润，而非盈利性基金会代表的是所有贡献资源节点的利益，我们可以决定利润是用来继续开发适合一些垂直行业使用的 app，还是按照持股比例返回给股东，而非盈利性基金会将资金在二级市场回购代币，通过查询计算每个节点的有效工作证明的积分比例，用代币的形式给节点返回分成。

这些都是记录在区块链上面，每个人应分比例都是显而易见的。

#### 4 大致技术细节思路

先讲核心的开发思路，我们使用现有的技术，在现有的技术基础上做微创新，从而实现主链需要实现的功能，这样防止主链开发陷入到一个无法预估风险的场景里面去，我们认为这样的项目，最核心的一个

是要有足够的节点，一个是要有能与传统企业竞争的应用软件，app 软件是不需要开源的，这个是真正的竞争壁垒。减少主链的开发难度，从而可以将大部分的资金投入到 dapp 的开发进程中，大型的应用软件不是个人能够开发的，属于软件工程，也是行业壁垒所在。

区块链的解释不多说，我们这里提及几个新名字 主块 附属块 主链 虚拟链

主块既传统意义上的区块

附属块依附在主块上面,生成主块的时候伴生附属块,比如在创世区块 0 生成的时候，伴生 0a 0b 0c 0d 等等这样的附属块，主块 0 里面记录代币转账记录，附属块 0a，0b，0c，0d 通过共识规则，我们可以定义不同的数据进入不同的附属块，从而实现不同的功能。

主链 由主区块链接起来的 最终可以查询到不同地址的最终代币数量

虚拟链 由主区块伴生的附属块链接起来，因为他不同于区块链有一个继承的关系，而是依存在主区块而存在的一个虚拟的区块链，不同的虚拟链 最终在数据表现上可以实现我们需要实现的不同功能。

依据这样的技术构架 目前我们可以实现的基础功能如下

- 1，代币的转账支付功能 基本的
- 2，虚拟链实现有效的积分证明，节点做了多少有效的贡献我们可以记录在一条虚拟链里面 比如 0a 1a 2a 3a 4a 5a 这样的数据结构 最终可以查询到每个节点的贡献比例
- 3，虚拟链实现类似论坛买卖区这样的功能，目前设计是一个区块只

能打包一条交易信息，竞价法则，付费高的优先打包进区块，从而所有钱包上都可以看到这一则广告信息。

4，钱包地址对钱包地址的短信功能，之所以设计这个功能，考虑到直接钱包上看到交易信息，可能信息发布者与需求者直接交流不会通畅，比如有些通讯软件有防火墙封锁，新上手一款通讯软件需要时间适应，简单的，直接钱包上看到交易信息，直接钱包上地址与地址短信联系，我们可以通过另外一条虚拟链实现这个功能。

5，UTXO 汇总功能 简单就是每个地址最终余额情况，比特币全钱包体积太大了，实际上运行全钱包时间长了都有这个问题，我们设计一个共识，在一条虚拟链上面，比如设计区块高度每增加 100000 个区块的时候，在虚拟链 10000c 这个附属块里面记录上 0~99999 个区块的所有 UTXO 汇总。这个是软件设计共识，这个新区块会被所有节点验证，不生成这个附属块的区块也不被全网节点接受，那么，我们增加一个新用户，假如他是在区块高度 108974 下载全钱包的，那么 he 可以从区块 100000 开始下载数据，区块 100000 里面的附属块 100000c 里面的 utxo 汇总是被所有节点验证认可的，新用户不需要太多的数据，整个区块链可以实现自我减肥的功能。

基于钱包的基本功能开发这些也是够用了，在钱包的基本功能之上，我们需要开发分布式计算平台的基础底层框架。如 GNT SONM RLC 之

类，因为他们没有自己的主链，所以底层框架开发必须基于 p2p 通讯原理 幸好，我们有自己的主链，我们主链有虚拟链，本质上，区块链就是个分布式的数据库，每个节点的数据库都是一样的，基于此，我们在开发分布式 dapp 运行的中间层，难度就小多了，完全可以抛开 p2p 的通讯原理进行简单开发。

我们先按照使用场景来看，算力需求者，需要节点来领任务，计算完毕之后节点返回结果给算力需求者。这个使用场景完全是在链下进行的，我们如何将这个使用场景与区块链无缝的有机结合起来呢？

我们有自己的主链，这是我们的武器，这也是我们不同于目前其他基于区块链分布式计算项目的地方，算力需求者需要节点为他工作，那么，他需要先付费，他可以根据目前网络节点的繁忙情况，其他算力需求者的出价情况，决定他出什么价钱，算力需求出价是一个自由竞价的市场，当然，为了保护节点的权益，我们会设置一个最低出价，低于最低出价的，节点不予处理。算力需求者出价，费用直接打包进区块，注意，GNT SONM RLC 是直接算力需求者与出租者沟通价格，直接一对一的付费使用关系，我们不同，算力需求者付费进区块，这个叫付费见证，因为需求者付费了，所以进区块打包的信息，我们可以把这个信息打包进附属块，比如区块高度 455 的时候，算力需求者发布一个任务，付费 3456 个代币直接进区块，这个是区块收益，因为付费，按照共识法则，矿工会在打包这个区块的时候，将算力需求者的需求信息打包进 455d 我们可以把这个虚拟链叫工作链，所有需求信息都打包进这个虚拟链里面，所有进工作链的信息，应该在同区



块高度的主链里面，有个付费见证，直接代币进区块的特殊付费模式。

在工作链里面，可以记录算力需求者需要什么 dapp 解决什么问题需求者的 IP 端口是多少。当然 很多需求者是内网 IP 后面我们会详细解说，为什么第一个开发的 dapp 应该是内网穿透器 以及这个内网穿透器在整个体系里面，扮演了多么重要的角色。继续接上面的讲，节点在更新区块之后，有了算力需求者的付费信息，需求者需要什么 dapp 需求者的软件 IP 地址。那么 节点将按照工作链里面的信息，与算力需求者取得联系，算力需求者将数据包发给节点，节点处理完之后发给需求者，需求者在任务完成之后，给节点打分，打分数据将记录在虚拟链上的积分链上面 这也是各个节点以后分享区块收益的唯一依据。节点只需要把自己的钱包地址告知算力需求者。任务完成之后算力需求者发布一个任务完成报告，写入区块，区块上面的节点看到任务完成报告，将会在任务列表中将任务删除。任务处理法则按照竞价排名，任务含金量越高的优先级越高。

也就是说，整个体系的设计，如果你将他比喻成一个公司来说，公司赚了多少钱，账目是公开可查的，每个员工做了多少有效贡献，是由公司客户打分评级的，这个也是公开可查的，那么，按照共识的分配法则，每个区块的收益，区块打包交易的矿工应该分多少比例，非盈利性的基金会应该分多少比例，dapp 软件开发应该分多少比例，剩下的每个提供算力的节点应该的分配比例，都是可以计算出来的，矿工诚实的按照共识规则给大家分配代币，那么他打包的区块就会得到全网节点的认可，矿工打包的时候如果想把区块收益全部分配给自

己，那么按照共识规则，他的区块不会得到大家的承认。他也得不到任何的代币奖励。

## 内网穿透器

内网穿透器很重要，我个人认为，内网穿透器这个 dapp 应该属于灵魂 dapp，通过内网穿透器，内网节点能与内网节点畅通链接，在有足够的内网穿透器集群基础上，我们还可以在这些集群基础上开发更多好用的功能。限于技术保密的需要，技术细节不做太多的阐述，具有负载均衡的内网穿透器集群将会显著的简化我们整体的开发难度。

## 5, 我们能开发一些什么有用的 dapp 软件 能让用户舍得花钱的 哪怕是一分钱？

这是重点，没有使用价值的 dapp，再炫的技术也是垃圾，衡量使用价值最好的标尺就是用户是否愿意花钱，愿意花多少钱，目前有一些构思 在此大致阐述一下。

### 1, 具有负载均衡的内网穿透器 dapp 。

这很重要，这是超算链的重要组成部分，有了它，有了足够的公网 IP 做节点，基金会可以将大部分需要租用服务器的费用花费在链上，节省了服务器开支，还属于内生经济的代表。内网穿透器除了第一版的内网穿透功能之外，未来还可以集成消息转发，内容分发的功能。基于公钥 私钥的验证体系，我们真的可以解决很多问题。

### 2, 下载加速器 dapp

基于 BT 原理，使用场景，比如公司有个软件包要发布，软件包有 1G，属于临时发布，下载的人数前期会比较多，直接租用服务器发布，在下载人数比较多的情况下，带宽支出也不少，那么他可以使用我们的下载加速器 dapp 原理就是他本机发布端做种子，节点完整下载也作为种子做文件的分发着，基于 bt 协议，最终软件完整发布给节点，节点之间互相传达到完整度 100%，发布者只需要生成一个磁力链接，下载者在下载文件的时候，会有上千上万的节点做种子给他下载加速。当然，发布是需要付费的，属于竞价付费，文件保存也是有时间的，比如 30 天，节点在保存这个文件 30 天之后，自动删除这个文件，为其他的文件加速腾出空间。发布者想继续加速只需要在文件到期之前再次付费一次就可以了。

### 3， 网页加速器 dapp

这个很好理解了，我有一个网站打开速度不理想，通过付费挑选一个速度好的节点给我做加速服务。

### 4， 分布式渲染 dapp

动画渲染特别适合分布式计算，电影的本质就是一副一副的图画，通过特殊的算法再把一副一副图画再分割成更小的数据包给节点去运算，节点运算完毕返回给渲染需求者。

### 5， 分布式深度训练 dapp

这一块目前值得关注，变化太快，不值得目前投入。

### 6， 部分垂直领域，计算任务可以分解，子任务之间相对松耦合，相

互之间不需要进行大量的数据交互，大量的实时性交互任务只能靠超算中心完成，符合这种计算特征的都可以用来定制开发 dapp 闲置资源节点做计算任务可以极大的降低计算成本。

## 6 可展望的商业计划

因为挖矿属于计算机 闲置手机挖矿，通过有效的工作证明这个虚拟链我们可以在共识里面控制矿工的人数，绝大部分计算资源都是在等待有价值的计算任务，显而易见，一头我们通过挖矿这个模式调动闲置资源挖矿的热情，从而筹备初始算力，一头我们通过开发有商业价值的 dapp，能为使用者降低使用成本，从而整个系统将会变得很有价值，因为我们有极地的挖矿门槛，你只需要有台电脑，限制手机也行，你就可以分享区块收益，不需要花大价钱购买专门的矿机，全球的电脑以及二手手机将是一个天文数字，dapp 的开发是重中之重，开发出来之后还要进行免费的推广使用，这是一个巨大的市场，dapp 不需要开源，更可以申请软件知识产权，这也是未来的门槛所在。因为极低的挖矿门槛，软件自带交易信息功能以及钱包地址对地址的短信功能，我想钱包应该不仅仅是一个钱包，在未来，如果我们的分布式渲染 app 开发很顺利，渲染水平能与国际上的大公司竞争，加上我们极低的算力持有成本，我想，有 2 个可展望的商业计划是值得探索的。

A 因为挖矿人人有电脑有手机都可挖矿，我想我们的钱包 pc 端 手机端会有一个不错的安装量，钱包有买卖交易的功能，还有钱包地址对地址的短信功能，我们钱包的使用黏性肯定比其他的钱包要高，在此基础上，

钱包上可以增加一个区块链资讯的频道，除了可以增加广告收入之外，因为有自己的媒体频道，还可以与业内其他同类媒体互推软文，降低推广成本

**B** 在分布式渲染 **dapp** 开发不错的情况下，理论上开发资金到位，不会有太大的技术难度，我们的软件会在全球动画设计圈里面 有一批数量庞大的使用者，只要效果差不多，极低的渲染成本将会是设计师的首选，在此基础上，我们可以开辟原创动画频道，通过扶持优秀的个人，小的动画开发设计室，我们的动画频道会首发一些优秀的原创动画作品，这将会继续增加我们软件的使用黏性，增加广告收入，反过来可以继续反哺优秀的设计师，展望未来，我们是有可能成立子公司，利用自己的渲染平台，以及汇聚在平台上面的各种设计师，孵化优秀的数字电影 IP，出品自己的数字电影。

## **7 超算链的可行性以及风险分析**

技术可行性，目前设计的技术都是在现有已有的技术上做微创新，通过排列组合不同的技术实现要求的功能，所以主链上面的开发难度并不大。难点在部分 **dapp** 的开发进度上，这也是不可预知的风险，部分 **dapp** 想要开发到能与传统企业竞争的水平上，需要特定行业的优秀开发人员，开发难度以及所需的开发资金也是很大的。当然，顺利开发成功，配合成本极低的闲置计算资源，这将是一个巨大的商业机会，风险总是与机遇并存的

## **8 暂定的计划路线**

目前项目处于早期白皮书阶段，我们希望对这个项目有能力又有兴趣的开发人员，对这个项目的有兴趣的早期投资者，能与我们取得联系，共同推动项目的落地发展。早期融资金额不超过 **50W** 美元，主要用于技术团队的组建以及早期 **demo** 版本的开发，宣传等。

## 9 代币的发行 分配 回收

区块 **2.5** 分钟一个块 创世块生成 **1** 亿 每区块固定生成 **1** 个，固定生成 **1** 个是为了防止部分钱包私钥丢失造成代币总数减少，从而能稳定保持在一亿的水平。每区块固定生成一个，一年固定生成 **21W** 的水平，对比总发行 **1** 亿的数量，膨胀率才千分之 **2** 的水平，加上可能的丢币状况，膨胀率应该很低很低的。

**3000** 万将用来十年时间内分配的算力提供着，也就是节点，基金会通过每天发布任务，按照有效的积分证明链上按劳分配。

**3000** 万用于推广 **dapp**，每当推出一款好用的 **dapp** 的时候，我们将在全球范围内开展免费试用，你使用，我买单的模式做全球推广。

**2500** 万用于 **ICO**，**ICO** 筹备的资金大部分将用于大型 **dapp** 的开发

**1500** 万分配给创始人 联合创始人 创始团队人员 早期投资者

## 区块收益的分配

区块收益为：固定的区块奖励 **1**+手续费+算力需求者付费使用进入区块的费用

区块的收益是不固定的 可能这个区块收益最低只有 **1** 下一个区块因为打包进去了一个很大的算力需求，需求者付费 **10000** 个币 加上

手续费，这个区块会有 **10000** 多个币的收益，所以，我们在设计上，用闲置资源挖矿变成了一个很有趣的行为。

具体分配：

**10%** 区块收益奖励给矿工

**10%** 区块收益为非盈利性基金会所有

**20%** 给 **dapp** 发展委员会，按照区块上面 **dapp** 的付费使用占比，**dapp** 的开发者获得代币收益，开发者开发的软件越好，愿意使用的人越多，开发者获得的代币收益越高

**60%** 按照有效的积分证明链上面的每个节点的积分情况，按比例直接在区块上分发给贡献算力的节点，当然，获得 **10%**区块奖励的矿工只要他在周期内也参与了有效的算力输出，他也是能获得他应该获得的那一部分的。

代币回收

**10%** 分配给非盈利性基金会的代币，如果在一个分配周期内代币没有使用完毕，剩下代币将存入一个多重签名的地址，仅用于大型 **dapp** 开发过程中资金缺乏的时候使用。

## **10 超算链的组织架构体系**

我们不强调我们是一个完全去中心的区块链项目，我们会是一个弱中心化的开放式的区块链项目，人人都可以参与，矿工节点也没有完全固定的节点，我们不是私有链，犹如一家开放式的公司，人人都可以参与进来做工作，做的工作越多，权重越高，就能参与更机密的

比如区块打包的业务，分配按照共识，工作积分权重完全记录在链上，公开透明。如果不成立一家强有力的软件开发公司，分布式计算的软件全靠个人软件开发者的话，很难与传统大型企业在计算领域展开有效的竞争。

a, 非盈利性基金会 非盈利性基金会维护更新区块链代码，全球范围内推广我们的项目，维护运营 dappstone

b, 大型 dapp 开发公司 使命是开发适合超算链使用的，在传统领域有广泛使用需求的应用软件，这是项目的核心，公司由创始人 联合创始人 投资机构 非盈利性基金会联合控股成立。

如果你对此项目有兴趣 我的联系方式是

**QQ                361024260**

**Webchat        361024260**

**Email           xoxbox@foxmail.com**