卡路里链白皮书

作者：龙杰

2018 年 3 月 18 日

目录

一、简介

本文针对比特币、以太坊等区块链项目共识机制导致的“高能耗”、“不公平”、“算力中心化趋势”的痛点，创造性提出 POC（Proof of Calorie）共识机制，基于 POC 共识机制开发一种类似比特币，主打支付功能的卡路里币（CC, Calorie Coin），卡路里币基于卡里路链（Calorie Chain）运行。卡路里币将继承比特币的去中心化等优秀的传统价值、闪电支付等创新价值，融入目前市场中存在的匿名交易、零知识签名、抗量子加密等区块链项目应用功能，并通过独创的 POC 共识机制，确保成为永久去中心化、简单可依赖、更加公平的点对点支付数字货币。

卡路里链（Calorie Chain）是基于 POC 共识机制的卡路里币主链，卡路里链的目标是成为全球第一大安全、隐私、开放、自由的区块链公有链，数字货币领域优秀功能的集大成者，从支付安全性、用户体验度、平台灵活性、应用多元化等方面打造亿级用户群。

二、设计原理与理念

1. 行业背景

有史以来，人类社会活动都在探索一种可靠的信任模式，

例如通过合同、权威机构、第三方担保、个人信用记录等，但这些信任模式的背后都带有人为主观因素，也就会天生带有不确定性风险。2008 年，以比特币代表的区块链应用项目的诞生，为人类史建立一种全新的“信任”模式，这种信任不需要国家等“权威机构”背书等作为信用基石，而是以分布式记账和密码学原理为基础，形成前所未有的可靠信任，其人为因素下降为零。基于这种可靠的信任，比特币成为一种可靠的点对点支付数字货币。但由于设计较早，许多区块链项目自身有许多的内在缺点，2008 年发展至今也在一直迭代更新，包括闪电支付、拓展区块大小等，但一直没有出现一种比 POW、POS、DPOS 等更优秀的共识机制。现存的共识机制会明显的伴随以下 3 个问题。

(1) 算力高耗能。以比特币、以太坊为代表 POW 共识机制伴随的高耗能问题，成为环保的痛点，遭到许多人指责，成为圈内的诟病。

(2) 算力中心化趋势。由于 POW 挖矿对算力的要求越来越高，对计算机的性能要求也就越来越高，从而导致算力集中在极少部分的人手中，甚至有爆料说比特大陆作为比特币矿机最大生产商，已经控制了全网 53%的算力，这对比特币已经构成了 51%算力攻击危机。究其根源不在于 POW 挖矿模式的原理和初衷问题，而是其带来的算力源——矿机的中心化问题，所以 POW 共识机制将难以长久持续维持去中

心化。只有调整共识机制才能解决这个问题。

(3) 分配不公平。POW 共识机制会导致的局面是：谁有更多的算力（更多的钱购买算力），谁就会获得更多的 Token；POS 共识机制会导致的局面是：谁在早期拥有更多的 Token，在后期就可以免费获得更多的 Token。这两种模式都会导致“富者越富，后来者很难获得”的结果，从而形成大量的币集中于少数人手中的现象，长此以往，必然导致用户数量下降，进一步导致流通性下降，流通性下降必然导致币的价值持续下降。比特币可能最终成为具有收藏价值的币，而其它类似的币也因为失去流通性，而失去价值。究其根源就在于，虽然 POW 共识机制早期实现了人人都可以挖矿的机会平等，但是，长期发展会因为算例中心化趋势导致“机会不再平等”，进而导致分配不公平，所以 POW 和 POS 共识机制最后必然导致使用他的数字货币很难持续发展和长久生存。

2. 设计原因

POW、POS 等共识机制，运行时间越久将导致的问题将越严重，会阻碍区块链的长期发展。高能耗，导致反对压力越来越大，特别是来自政策和环保意识的压力；算力中心化趋势，最终导致“去中心化”走向“中心化”，进而失去信任基础；分配不公，导致后期加入并使用比特币等数字货币的人越来越少。这个三个痛点，只有改变共识机制才能解决，

这种共识机制应该至少能够具备“低能耗”、“算力永久去中心化”、“低门槛获取”等特征，进而能让 Token 有不断增长的用户，能永久的良性循环流通，持续保值或不断增值。

POC 共识机制的思路起源：为寻找这样一种共识机制，我从传统货币的本质和劳动价值两个角度出发，来思考探索。货币（特别是以国家信用为基础的纸币）本身没有价值，它价值的产生是因为流通而传递了劳动价值；而劳动价值是源于人的劳动，劳动是人类社会持续发展的核心动力。所以“按劳分配”才能最大限度的体现了“公平”，但“劳”是难以量化的，特别是脑力劳动更不能量化，所以按劳分配在各国制度中始终是理想而难以实现，现实总用二次分配等多种制度来调和。依据这样的事实，为了从币的分配层面尽可能实现“公平”，我想到了最接近的一个量化指标——“体能”，即人通过运动产生的热量，用卡路里（Calorie）为计算量纲，以运动量大小作为算力的依据，而不是以计算 hash 值的能力为算力。

根据现在的技术，人体运动热量可以比较准确的计算出来，这为我们的共识机制产生奠定了现实技术基础。POC 共识机制，以运动量为算力，不会消耗电力等能源，反而有益身体健康，具有“低能耗”特征；每个人的体能都是有限的，而且不会相差太远，这就确保了“算力永久去中心化”；绝大部分正常人都可以适量的运动，产生热量，而且几乎是“零

成本”，老少皆宜，人人挖矿，确保了“低门槛获取”特征。POC 共识机制可以同时具备这三大特征，这是一大创造性共识机制。

3. 设计原则

（1）**简单、精简、可靠。**用最简单的理念、最精简的技术、做最可靠的数字货币，才能促进最广泛的共识，吸引最多的用户。

（2）**去中心化，去信任。**这是比特币等点对点支付区块链项目的基本要求，卡路里币也必须具备。

（3）**加密、隐私、安全。**这是主打支付功能的数值货币的基本要求。

（4）**开放透明，不可篡改。**用独立的区块链浏览器+分布式账本，确保所有交易信息可查，特别是项目基金等，确保开放透明，不可篡改，这也是去中心化模式上的信任基石。

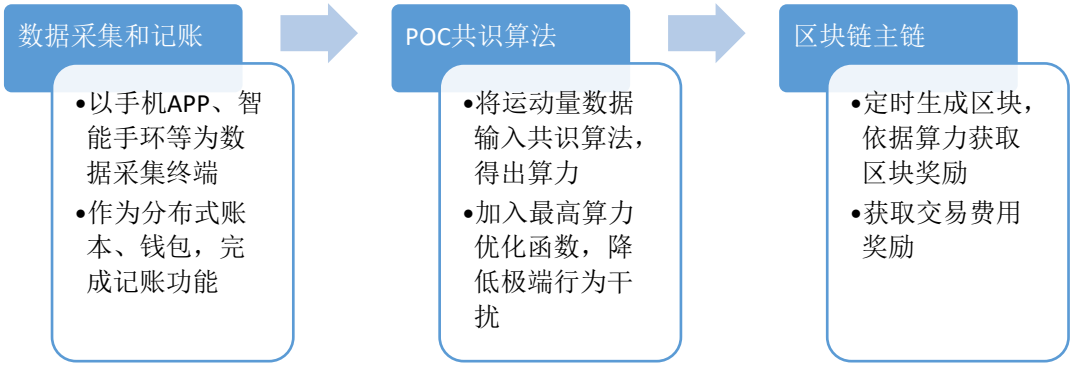
（5）**数据采集准确、真实，防伪。**数据的准确、真实是算力准确、可靠，卡路里币的分配准确、可靠的前提，也是 POC 共识机制的核心，这一点必须保障。如果存在造假，还要有适当的惩罚机制。

（6）**集体维护，建立维护基金和激励机制。**项目能长期稳定运行，离不开持续的技术维护和稳定的社区推广，因此建立维护基金和激励机制，提高集体维护的积极性，是保

障卡路里主链持续稳定运行的基本保障。如设立按代码贡献度奖励、按推广用户数奖励等机制。

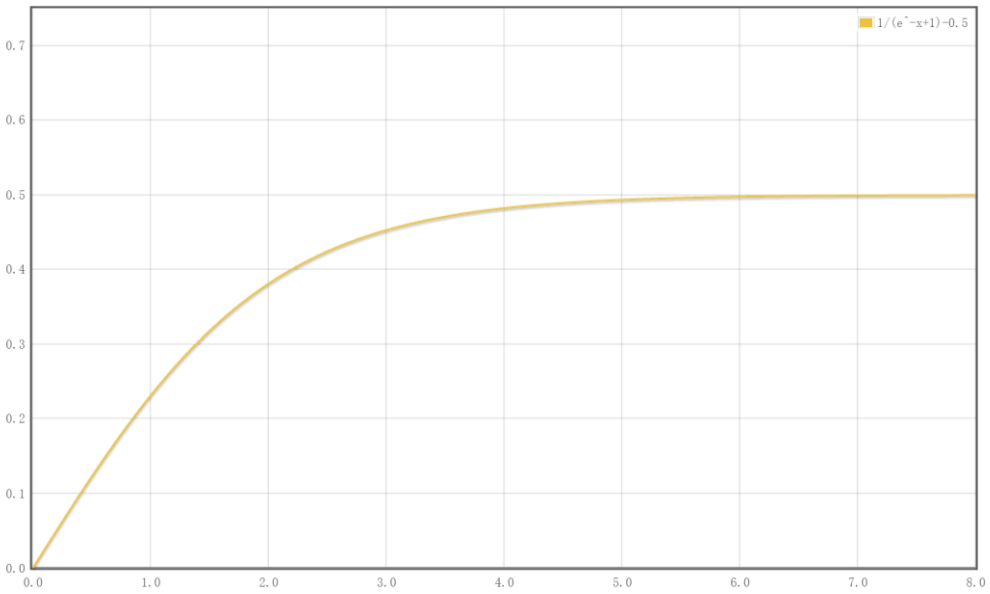
4. 产品框架

产品整体框架如下：



（1）**数据采集终端和记账。**在智能手机上安装一个运动量数据采集终端，类似微信里的计步功能、跑步软件的运动数据统计。这一步有两个关键，一是保证数据的正确、真实，能防止造假；二是集成区块链记账功能

（2）**POC 共识算法。**将终端采集的运动量数据输入共识算法，得出运动量数据，即算力，作为“挖矿”的依据。同时考虑到一些职业运动者的特殊优势和一些极端行为，为进一步促进公平，应设定一个类似“厂”字曲线函数的一个优化函数，如一下函数图（y=1/(e^-x+1)-0.5），以限制极端行为的影响。



（3）**主链区块链。**继承比特币主链的优质特性和其它区块项目的优秀功能，定时生成区块，依据算力分配区块奖励；分配交易费用奖励。

5. 项目特征

本项目将会具备的特性有：

(1) **最接地气的挖矿模式。**POC 挖矿模式，允许矿工以走路、跑步、登山、自行车等多种运动方式挖矿，以运动产生的卡路里数量作为挖矿的工作量证明，均分每个区块等量的币，因此可以形成“人人挖矿”的一种区块链项目，男女老少皆宜，用户数有无限可能。

(2) **早期多重共识机制。**POC 共识机制将维持 100 年，同时，为提高项目初期的忠诚度，在项目最初的 5 年，还将有少量的币用于支持 POS 和 POW 共识机制，这主要是考虑

到运行初期的不确定性，提高用户的忠诚度和项目稳定性，及反馈早期投资者。

(3) **最大限度的促进公平。**一方面，从空间角度看，POC 共识机制可以让任何人在任何时候都可以近乎“零成本”的参与挖矿，这可以确保每个人在空间上有平等的挖矿机会，使挖矿更加普惠化。另一方面，从时间角度看，卡路里币每年产量一样，共持续 100 年，不会如比特币一样每 4 年减半，这样后来挖矿的人不会因此感觉明显减少而造成不公平。

(4) **总量恒定，预分配公开。**卡路里币的定位是全人类共有的，依据 2017 年世界总人口数据约 75 亿，考虑上涨趋势，将未来人口估计为 84 亿人，按每人 10 个币计算，卡路里币拟发行总量为 840 亿个，总量恒定。其中 75%用于 POC 挖矿。这些基础数据会在主链上设置好，做到预分配公开，用区块链不可修改的特点确保其稳定、可验证。

(5) **永久的去中心化。**为确保永久的去中心化，将分配 80%的币用于 POC 挖矿；考虑每个人的运动量有限和大量的用户数，可以完全的避免算力中心化趋势，用户越多，算力将越是去中心化，充分稀释卡路里币的持有集中度，确保永久的去中心化。

(6) **安全、快捷、实用的支付功能。**卡路里币主打支付功能，所以建立的钱包将会以安全、快捷、实用为特征设计，可以用于购买商品及时支付，在生态系统中高效运转。

(7) **建立二次分配机制和慈善账户**。建立一个二次分配帐户，主要用于分配给一些劳动领域不易获得卡路里币的人群，如工人、农民等其它领域的劳动者，这些人群的特点是早期不易获得卡路里币，但又创造了劳动价值。同时，还将设立一个公益帐户用于接受捐赠，用于慈善，这也是二次分配的另一种形式。

(8) **个人运动私链。**后期将运用智能合约功能，可以让用户发布私链，运用区块链存储功能，将照片、视频、文字等信息与私链结合，形成个人不可篡改的记录，形成个人运动私链，永久载入人类运动史册。

(9) **与时俱进融入新技术。**保持卡路里链的自我革新，不断学习和融入区块链新技术，例如现有的闪电支付、抗量子加密、零知识证明等功能，与时俱进，适应需求。

6. 技术创新

本项目最大的技术创新就是 POC 共识算法，它近乎完美的解决了“算力高能耗”、“算力中心化趋势”和“分配不公平”的问题。

POC（Proof of Calorie）共识机制就是以人通过跑步、走路、登山等运动产生的身体热量计算出来的卡路里数据为基础，作为获得区块记账权限的证明，即类似于 POW 挖矿中的算力。这种方法不会消耗电力等任何社会能源，反而可以

增加“矿工”的体能，促进健康。这种方法的挖矿门槛近乎为零，只需要在个人手机中安装一个专门的 APP 即可，任何人在任何时候都可以挖，包括老人、小孩，因为至少他们能走路，这就从根本上让挖矿具有普惠性，极大的解决了算力中心化趋势和“不公平”问题。

热量的简单计算方法：

热量（kcal）＝体重（kg）×运动时间（小时）×指数 K

其中，指数 K＝30÷速度（分钟 400 米）

为了确保公式中运动数据（体重、运动时间、运动速度等）的真实、可靠，将采集人的心跳、体温、呼吸频率、运动路线作为参考指标，以验证真伪。例如：如果一个人是在秋千上摇摆，虽然有速度，但距离不会有大幅的移动，这种运动将被证伪；如果是将设备绑定在狗狗、牛、羊等其它动物身上，其体温、心跳、运动频率等将有明显的不同，也将被证伪。

7. 安全策略

卡路里链的安全策略将充分借鉴比特币及其它区块链项目的安全策略，包括 Hash 唯一性、非对称加密、设分认证、去中心化的分布式设计、传输安全性 HTTP+SSL 等。

三、项目的具体实施方案

1. 共识机制

卡路里链主链上线的前 5 年，将采用 POC+POW+POS 的组合共识机制，从第 6 年以后将采用纯 POC 共识机制。

2. 项目落地

项目落地时间路线图大致如下：

1、**募集团队**，3 至 6 个月。考虑到项目的难度，早期将招募一批认可卡里路链项目价值的技术开发团队、项目推广团队、项目顾问团队、早期私募投资者等。

2、**数据采集终端开发**，3 至 6 个月。早期以智能手机 APP 终端和智能手环为主，确保采集的数据真实、可靠，作为区块链节点占用空间小。

3、**上线主链**，3 至 9 个月。包括集成 POC+POW+POS 共识机制，安全及性能测试，及集成其它优秀功能。

4、**推广合作，长期**。上线交易平台；与一些商家、项目深入合作，提高卡路里币的用户数和应用场景，包括网店、大小实体商户、代码贡献奖励、论坛发帖奖励、其它运动领域等。

5、**生态建设，长期。**以优秀、简单、可依赖的支付功能，累计用户群。有庞大的用户群就会有丰富的生态可以建

设。就如 QQ 累计用户群一样，坚持以扩大用户群为导向，用稳定良好的性能保持卡路里币的内在价值、用简单可依赖的用户体验留住老用户、用低门槛的挖矿吸引新用户。

3. 生态激励机制

基本的激励机制与比特币一样，一是记账激励（挖矿奖励），每个区块产生时奖励预先设计好的卡路里币给矿工。二是交易费奖励。三是建立激励基金，用于奖励其它领域的贡献，如代码贡献，宣传贡献，论坛发帖贡献等。

4. Token 与众筹

Token 总量：卡路里链是全球的，我们依据 2017 年的世界人口统计约 75 亿人口，考虑到人口的上涨趋势，我们将未来人口上浮到 84 亿，按每人 10 个币的数量计算，拟发行总量为 840 亿。

Token 初步分配如下：

类型	POC	POW	POS	基金会	开发团队	私募
占比	75%	2.5%	2.5%	10%	5%	5%
时间（年）	100	5	5	10	10	5

- POC 75%，100 年。
- POW 2.5%，5 年，用其成熟优势，确保早期稳定运行。

- POS 2.5%，5 年，激励早期期投资者忠诚度。
- 基金会 10%，限售，每年解禁总量的 10%，10 年解禁完成；属于用于项目开发、维护，包括商业、应用等拓展。
- 初期开发团队 5%，限售，每年解禁总量的 10%，10 年解禁完成；属于团队成员个人私有。期间若有队员退出，未解禁部分将分配给后期加入的成员。
- 私募 5%，限售，每年解禁总量的 20%，5 年解禁完成；用于早期建站等运营发展。

四、项目前景展望

1、**人人挖矿，实现分布式记账。**试想每个人只要在手机上安装一个 APP 或戴一个智能手环，通过日常走路、跑步等就可以“挖矿”，锻炼身体的同时获得可以信任的数字货币，提高用户吸引力，必然有更多的用户乐意加入。如此用户在获得收益的同时，完成了记账，实现了区块链的分布式记账功能，记账节点将非常的多。

2、**主链运行，卡路里币有价值。**实现了分布式记账，就能保障卡路里主链分布式的良性运行，从而区块链+分布式记账就保障了卡路里币的基本价值。

3、**不断拓展，丰富支付应用场景。**虽然目前主打支付功能的很多币种都首先跟银行合作，但这种方式有违背去中心化的初衷。所以，卡路里币选择的是另一条路——“散户

包围大户”，早期不会跟银行合作，而是与广大的大小商家实体商家合作，包括网店、便利店、超市等，用丰富便利的应用场景与广大的用户数对口，提高用户粘性，同时实现卡路里币的高效流通，不断提高币的流通价值。

4、良性循环，卡路里币价值提升。随着用户的持续增加，应用场景的不断丰富，卡路里币的价值就自然持续提高。如果这套简单可依赖的良性循环系统建立起来，卡路里币未来的价值不可估量，系统生态拓展价值不可估量！