卡路里链白皮书

CC，to be the BTC3.0

全球通用，人人共建——大道至简，回归人体

第Ⅱ版

作者：龙杰

2018 年 7 月 24 日

目录

摘要：经过近 10 年的考验和发展，比特币不断壮大并声名远播，但也出现了几个一直难以根治的现实问题，包括“算力中心化”、“挖矿高能耗”、“机会不平等”、“交易高成本”等，已明显违背“去中心化”，全网随时可能遭受算力攻击，中本聪的初衷——建立“一种点对点的电子现金系统”，将变得不再安全。随着时间的推移，比特币的价值也将因此而大打折扣。为此，我们希望继承和发展中本聪对比特币的愿景，改进比特币在早期制度设计上的不足，根本性的解决比特币目前面临的多重问题，创造性的提出了 POC 共识机制，将打造 BTC3.0 版本。

一、简介

本文针对以比特币为代表的区块链项目，由于共识机制设计缺陷所导致的“算力中心化”、“挖矿高能耗”、“机会不平等”、“交易高成本”等现实问题，创造性提出 POC（Proof of Calorie）共识机制，即用人体运动产生的热量替代计算机算力，作为工作量证明。

基于 POC 共识机制，开发一种类似比特币的卡路里币（CC, Calorie Coin），在卡路里主链（Calorie Chain）上运行。卡路里币将继承比特币的去中心化等优秀理念，以及闪电支

付等创新技术，运用石墨烯技术及超级站点中继方法提高转账速度，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，使卡路里币真正继承比特币初衷，并融合最新的区块链技术，成为一种永久去中心化、安全可靠、更加公平、流通高效、环保节能的点对点电子现金系统。

二、设计原理与框架

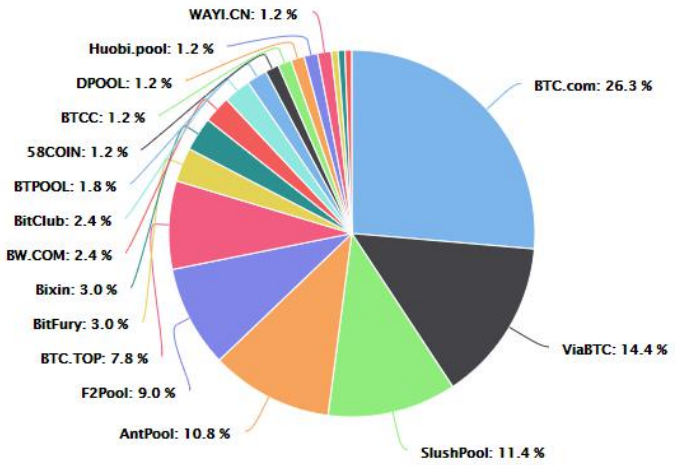
1. 行业背景

人类的商品经济活动中，一直在探索一种可靠的信任模式来开展交易，例如基于权威机构、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 11 月 1 日，中本聪的比特币白皮书发布，到 2009 年 1 月 3 日比特币第一个区块开始运行，标志着以比特币代表的区块链项目的诞生，为人类史建立一种全新的“免信任”模式，这种信任不需要国家等“权威机构”或“第三方机构”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，形成免信任价值流通，人为因素下降为零。基于这种免信任，比特币成为一种可靠的点对点支付数字货币。

但由于早期机制设计的不足，导致 10 年后许多问题凸

显，2009 年 1 月发展至今也在一直针对部分问题迭代更新，包括闪电支付、拓展区块大小等，但许多源于 POW 共识机制的系列问题一直没有得到很好的解决。换句话说，包括 POS、DPOS 等新的共识机制在内，没有一种比 POW 等适合的共识机制，以确保完成 POW 的任务同时，能解决 POW 带来的问题。目前比特币明显伴随至少以下 4 个问题。

(1) 算力中心化。根据 btc.com 网站数据显示，目前全球前 4 大矿池算力已超过 60%，这对比特币已经构成了 51%潜在算力攻击危机。究其根源不在于 POW 挖矿模式的原理和初衷问题，而是利益驱动市场把矿机做向专业化，所以算力中心化的本质是矿机的中心化。从中本聪最初设想的“一 CPU 一票”原则，CPU 已经转化为 GPU、ASIC 等专业矿机，继而形成了算力中心化的结果，完全违背“去中心化”理念。长此以往，比特币的中心化趋势必将更加强化，不诚实的算力攻击危机随时可能暴发。



2018 年 7 月 18 日 BTC.com 统计的比特币挖矿算力分布

(2) 算力高耗能。根据中国新华网道：能源价格比较服务网站 PowerCompare.co.uk 研究显示，2017 年用在比特币“挖矿”上的电量超过 29.05 太瓦时（1 太瓦时为 1 亿度电），超过了全球 159 个国家的年均用电量，而爱尔兰全国（477 万人口）一年的用电量也只有 25 太瓦时的电力。以比特币为代表的 POW 共识机制伴随的高耗能问题，已成为环保的痛点，遭到许多人指责，成为圈内诟病。

(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（更多的资本购买或生产算力），谁就会获得更多的挖矿激励；POS 共识机制会导致的局面是：谁在早期拥有更多的代币，只要存着，在后期就可以免费获得更多的代币。这两种模式都会导致“富者越富，后来者很难获得”的结果，形成分配机会过度不公平问题，从而导致大量的币集中于少数人手中的现象，长此以往，必然导致用户数量持续下降，进一步导致币的流通性下降，继而导致币的价值持续下降。比特币最终可能成为只具有收藏价值的币。

(4) 交易高成本。作为一种“点对点电子现金系统”想要实现的初衷就是免去第三方保障的信任，实现点对点的免信任支付功能。但是，比特币总量 2100 万个，如果按照全球 70 亿人口折算，人均持有仅 3‰个，数量少限制了比特币的流通；近一年币价在 6000 美元至 2 万美元波动，单价太

高，限制了比特币的价值交换属性；2018 年 7 月，支付一个比特币的手续费约 20 美元，高昂的手续费限制了比特币的流通。其中交易手续费过高的原因之一，就是 POW 共识机制导致了过高的记账成本。

2. 设计原因

比特币逐渐被更多人所认可，主要在于它以区块链为基础，实现了公开透明、难以篡改、不依赖中介机构的特点，安全、高效、低成本（早期）的价值传输。反思比特币目前存在的问题，我们认为一个能够被人们普遍接受、长期有效流通的全球通用加密数字货币应该至少具备以下 4 个特点：

1、“算力去中心化趋势”。制度设计应使项目朝长期着“去中心化趋势”方向发展，趋势不可逆，从而保障代币长期不被 51%算力攻击而威胁系统安全。

2、“人人挖矿机会平等”。全球每个人都能以极低，而不是高昂的挖矿成本获取该数字代币，实现人人机会平等；卡路里币本身没有价值，是使用的人多了才产生价值。

3、“挖矿模式健康环保”。挖矿模式符合人类健康、环保的共同价值理念，而不能高能耗，浪费能源。

4、“高效流通支付便捷”。在早期制度设计和完善时，应尽可能减少各种可能影响流通效率、支付便捷性的阻碍，只有流通高效、支付便捷的功能，才能充分实现数字代币内

在的价值交换属性。

基于这样的考虑，我们想从改变 POW 共识机制角度出发，探寻一种既能完成 POW 机制的任务，又能规避 POW 机制问题的新的共识机制。于是我们从传统货币的价值存储和价值交换的两个本质属性，以及货币与价值之间的关系出发，基于人类一直在探索一种最优的“按劳分配”制度事实，我们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。以人的运动量大小，而不是以 CPU 计算速度为算力，并以卡路里（Calorie）为计算量纲，得出了 POC（Proof of Calorie）共识机制。

从理论角度，POC 共识机制至少可以解决 POW 共识机制面临的“算力中心化”、“挖矿高能耗”、“机会不平等”、“交易高成本”等 4 个问题。因为市场可以创造更高算力的 CPU 用于一个人或一个组织挖矿，却难以创造出更多的人用于一个人或一个组织挖矿，算力中心化趋势难以形成；不会消耗大量电力等能源，反而有益身体健康，既环保又不会导致过高的交易成本；老少皆宜，人人都能以极低成本平等的挖矿，机会更公平。

从实践角度，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。

3. 设计原则

为长期维持卡路里币的初衷，我们确定了以下 6 条基本设计原则。

（1）**去中心化方向。**首先要确保机制设计是朝着去中心化的方向，尽量考虑未来可能的技术革新带来的冲击，“去中心化”是卡路里币能成为“免信任”点对点支付现金系统的基础，如果违背了“去中心化”，卡路里币也将失去生存土壤。比特币在初期就是没有考虑到专业矿机的大量出现，从而导致了算力中心化，这一点卡路里币将借以为戒。

（2）**数据采集防伪。**卡路里币的算力是来源于用户移动终端的运动数据，确保运动数据是诚实而不是伪造的，是 POC 共识机制正常运行的关键。所以在移动采集终端将构建一套数据防伪验证模型，包括识别人运动时的心跳、体温、呼吸频率等人体指标，GPS、海拔高度、温度、湿度等环境指标，运动距离、运动速度、步频变化、休息时间等具体运动状态指标，以验证运动量数据的真实性。对此，我们考虑了以下 2 种可能的伪造行为及防御措施：

- 用机器等设备替代人体运动：如将手机放在秋千等设备上，其 GPS 变化将会很小，会被证伪。如将手机放在汽车上，其运动速度将超过一般人跑步速度，会被证伪。如果后期要求用智能手环等终端，能够监测心跳频率等指标时，所有的物理设备都将被证伪。

- 用其他动物替代人体运动：如将移动终端与狗、猫等动物绑定，其运动轨迹、体温、心跳频率等指标会与人体有明显不同，容易被证伪。同时，如果识别出存在某次造假行为，将有一定的惩罚。

综上所述，防伪机制只要在实际中不断优化，就可以确保终端数据采集的真实性，具体举措将在开发过程中由开发团队共同研讨商定。

（3）**安全可靠，支付便捷。**使用最先进的区块链加密技术等最先进的安全措施，并融入抗量子加密特性等新兴技术，确保卡路里币安全可靠。同时，在保障安全的基础上，确保快捷、便利的支付体验，确保卡路里币能够高效的流通。

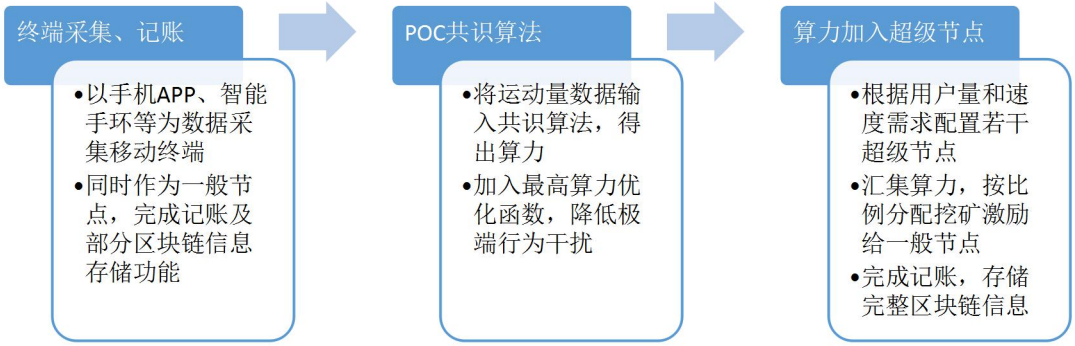
（4）**公开透明，不可篡改。**用独立的区块链浏览器+分布式账本，总量恒定，不可篡改，匿名交易，但所有交易信息公开透明、追溯可查，包括项目基金等。

（5）**可拓展性，与时俱进。**任何项目要保持长期的运行，都离不开与时俱进的自我革新。卡路里链也将如此，在早期设计时，将加入可拓展性功能，保持与时俱进的设计原则，让卡路里链在以后的变化中，能够更容易的自我革新。

（6）**卡路里链建设激励机制。**除了挖矿和交易费激励外，还将建立一套卡路里链生态建设激励机制，对在主链建设、技术维护、项目推广、社区建设等方面有贡献的人，给予卡路里币激励，具体激励机制由项目团队共同商定。

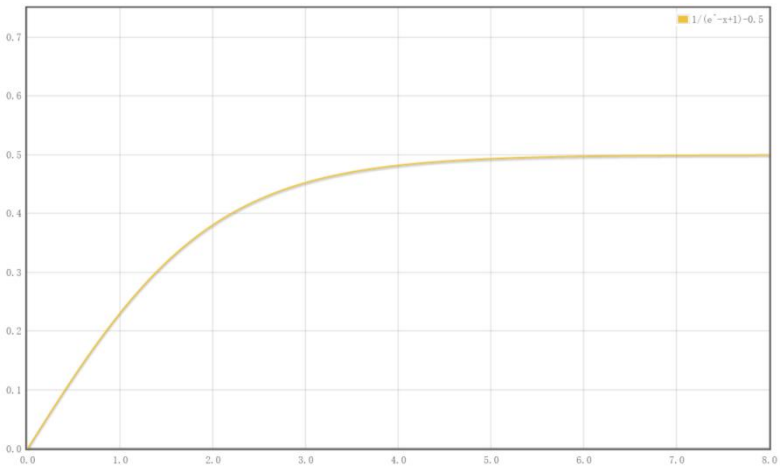
4. 产品框架

产品整体框架如下：



（1）**终端采集、记账。**在智能手机上安装一个运动量数据采集终端，可以是手机 APP、智能手环等移动设备，实现运动数据采集、验证、统计及记账功能。这一步有两个关键，一是保证采集数据的准确、真实，能防止伪造；二是集成区块链记账功能，完成部分链的存储功能，因为完整链可以由超级节点存储，移动终端不必存储完整链，以提高运行速度。

（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，加入一个“厂”字形曲线的优化函数，如函数图（y=1/(e^-x+1)-0.5），以限制过度运动量等极端行为的影响。



（3）**算力加入超级节点。**考虑到移动终端运算速度的限制，有必要增加超级节点，用于汇总各数据终端算力，完成记账功能，记录完整的区块链交易信息，并分配挖矿激励。超级节点数量、产生、要求等具体内容由项目团队共同商定。

5. 项目特征

卡路里链项目将会具备以下 10 大显著特征：

(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，无论男女老少、长幼尊卑，上下班、散步、遛狗都可以，能够真正形

成“人人挖矿”的氛围，接地气，用户量具有无限的可能。

(2) **千年币。**公元 1023 年诞生于中国成都的世上最早“正式”发行的纸币——交子，距今已经 995 年，5 年后就是 1000 年。作为一个理念诞生于成都，有理想有远景的卡路里链项目，初定卡路里币的 POC 挖矿机制也将持续 1000 年。

(3) **早期双重共识机制。**POC 共识机制将维持 1000 年，同时为提高项目初期的用户忠诚度，在项目最初的 10 年还将同时支持 POS 共识机制，即前 10 年是 POC+POS 双重共识机制，这同时也是考虑到项目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。

(4) **POC 挖矿年产量不变。**不同于比特币每 4 年产量减半，考虑到时间越久，用户量越大，挖矿难度自然会增大，价值自然随着时间而上升，因此卡路里币每年产量保持不变，共持续 1000 年，这样后来矿工不会因此感觉明显减少而造成不公平感。

(5) **总量恒定，预分配公开。**卡路里币总量恒定，永不增发，1000 年总发行量为 15960.82 亿个，其中 POC 挖矿占比达 98.79%；前 10 年总发行量 350 亿个，其中 POC+POS+The Dao 占比 57%，余下的预分配为二次分配帐户、基金会、开发团队等 7 个部分，具体内容见“Token 与公募”板块内容。

(6) **永久的去中心化。**为确保永久的去中心化，将分配98.79%的币用于 POC 挖矿，其中前 10 年 POC 挖矿占比 45%；考虑到“算力去中心化趋势”的设计，及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，时间越久，去中心化程度将越高，遭受 51%算力攻击的可能性就越渺茫。

(7) **安全、快捷、实用的支付功能。**卡路里币将会以安全、快捷、实用为特征设计，可以用于及时支付和价值存储，使卡路里币在生态系统中高效运转。

(8) **建立二次分配帐户**。团队早期将建立一个二次分配帐户，主要用于分配给一些领域因认识不足等原因，而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，二次分配帐户体现卡路里币促进分配公平和慈善的价值理念。帐户资金主要来源于预分配和用户捐赠。

(9) **个人运动私链。**后期根据主链情况，将拓展智能合约功能，结合 IPFS 等项目，可以让用户发布运动私链，将照片、视频、文字等信息与私链结合，形成个人运动记录，永久载入人类运动史册。

(10) **与时俱进。**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，保持与时俱进，适应社会需求。

6. 技术创新

本项目最大的技术创新就是 POC 共识机制，它近乎完美的解决了“算力中心化”、“挖矿高能耗”的问题，很大程度上减轻了“分配不公平”、“交易高成本”的问题。具体原理前文已经说明，此处不再赘述。

POC 共识机制运动热量计算的参考方法：

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）

实际计算方法由项目早期团队共同商定。

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、身份认证、去中心化的分布式设计、传输安全性 HTTP+SSL 等。

三、项目实施方案

1. 项目路线图

项目落地时间路线图大致如下：

1、**募集团队和资金**，2018 年 11 月 1 日前。我们希望用

2 个月左右的时间，**在比特币白皮书发布 10 周年时**，完成我们的 BTC3.0 早期团队和种子资金的募集，将 BTC3.0 项目开发框架定型。希望有兴趣的技术人才或投资者加入我们，文章尾部附联系群。

2、**发行代币，**初定团队确定后用 1 个月时间，基于以太坊 ERC2.0 发行代币，做好早期分配。

3、**数据采集终端开发**，初定 3 个月，具体由项目团队中的 APP 开发组确定。早期以智能手机 APP 终端和智能手环为主，做好数据防伪等功能。

4、**上线主链**，初定 6 个月，争取 2 个月（2019 年 1 月 3 日前，比特币诞生 10 周年时），具体由项目团队中的主链开发组确定。包括早期集成 POC+POS 共识机制，安全及性能测试，及集成其它优秀功能。

5、**生态建设，**长期，包括上线交易平台；加强与运动团体组织、商家、其它项目深入合作，持续拓展卡路里币的用户数和应用场景。

2. Token 与众筹

Token 总量：根据对人走路、跑步产生能量的估计，得出每秒生成 50 个币比较适合 POC 挖矿，以此计算，每年将挖矿生成 15.768 亿个币（365*24*60*60*50），POC 挖矿 1000

年，将总计生成 1.5768 万亿个币。

前 10 年是卡路里主链生成及完善、应用成熟的最重要时段，我们以前 10 年的 POC 挖矿数量为基数，计算出早期币的分配。前 10 年 Token 初步如下：

分配	CC	POC	POS	The Dao	二次分配	基金会	开发团队	私募	公募	2 年公募	空投
占比	100%	45%	6%	6%	5%	10%	10%	2%	5%	10%	1%
总量（亿）	350	157.68	21.16	21.16	17.5	35	35	7	17.5	35	3.5
锁仓时间			10 年	1000 年		10 年	10 年	5 年	5 年	5 年	

- POC 45%，每年 POC 挖矿生成 15.768 亿币，10 年共生成 157.68 亿，占前 10 年总数量的 45%。
- POS 6%，10 年均匀分配，激励早期期投资者忠诚度。
- The Dao 6%，1000 年，用于维护卡路里链的原始初衷，避免因币集中于少数人手中而恶意串改主链共识；1000 年后将自动销毁。
- 二次分配 5%，用于二次分配、支持运动和健康等相关主题的行业发展、慈善捐赠等，拓展卡路里链的公平、慈善、健康、共赢的价值理念。
- 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。
- 开发团队 10%，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及新加入成员。

- 私募 2%，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。
- 公募 5%，公募时间持续 1-6 个月，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。
- 2 年长期公募 10%，公募时间持续 24 个月，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。
- 空投 1%，空投交易所或 BTC 等持有用户，用于拓展早期用户和实现顺利上交易所。

据此计算，10 年后每年通过 POC 挖矿产生的卡路里币 15.768 亿个，如果平均到 84 亿人口上，每人平均获得 0.2 个币；如果全世界有 1%的人挖矿，矿工将平均获得 20 个币。1000 年挖矿完成后，卡路里链币的总量将是 1.5768 万亿+192.82 亿=15960.82 亿个，即约 1.6 万亿个，其中前 10 年 POC 挖矿占比 45%，POC 挖矿总占比达 98.79%。

具体配置以团队共同商定为准。

四、结论

我们首先从实际出发，讨论了比特币存在的 4 个现实问题，并针对性的提出了全球通用加密数字货币应该至少具备 4 个特点，据此依托 POC 共识机制创新提出卡路里币，打造 BTC3.0，并从理论和实际 2 个角度论证了其可行

性，接着明确了本项目具有的 10 大特征，本文也包含了项目框架、路线图、Token 分配等全部内容。但仍然还有许多细节需要项目团队共同讨论商定，在此再次号召有志向、有兴趣的朋友加入我们。

人类第一张正式发行的纸币诞生距今近 1000 年，逐步的替代了金、银、铜等金属币形式，但也因为主权国家可以任意控制发行，通货膨胀随时都在，纸币大幅贬值也偶有发生，主权纸币的弊端因此而极为明显。

比特币诞生距今近 10 年，它的理念和价值逐渐被认可，同时因为早期设计的缺陷，问题也凸显，纵然如今有 1600 多种代币，但鱼龙混杂，炒作为主，没有一种代币能很好的解决比特币的问题，并很好继承比特币理念。

量子学派基于区块链技术，提出未来“人即货币”的设想，但当下如何很好的用区块链技术与现实结合起来？卡路里币的 POC 共识理念，以人体运动量为算力，实现人人挖矿的氛围，是否与之有所契合？卡路里币将来能否成功上线并获得社会的认可？等等诸多问题，不是白皮书作者目前能够回答的。我们期待有更多人对这份白皮书提出的内容进行探讨、翻译，有更多的技术团队、技术人才、投资人加入，一起建设卡路里链，朝着共同的理想。

五、参考文献

[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf, 2008

[2] QQagent，“比特币白皮书：一种点对点的电子现金系统”，http://www.8btc.com/wiki/bitcoin-a-peer-to-peer-electronic-cash-system

[3] 新华网，“比特币'挖矿'： 能耗黑洞！”，http://www.xinhuanet.com/info/2018-02/28/c_137005191.htm，2018

[4] 勋爵，“[区块链] 共识算法之争（PBFT，Raft，PoW，PoS，DPoS，Ripple）”，https://www.cnblogs.com/X-knight/p/9157814.html，2018

[5] block.one，“EOS.IO Technical White Paper v2”，https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md，2018

[6] 维基百科，“交子”，https://zh.wikipedia.org/wiki/%E4%BA%A4%E5%AD%90，2018

[7] CoinMarketCap，https://coinmarketcap.com

[8] IPFS，https://ipfs.io

[9] 罗金海，“人即货币”，https://mp.weixin.qq.com/s/pwYEW_V5eDqG8OHi9rVmOw，2018

卡路里链(CC)白皮书研讨联系方式

联系方式	备注	二维码
CC 项目研讨微信群	7.30 前有效	
CC 微信客服	微信号：JackDragon2008	
CC 项目研讨电报群	加入网址：https://t.me/CalorieChain	

我们同时在招募团队，您若有意愿成为我们项目投资人、开发者、宣传及社区建设者，请联系：

微信：JackDragon2008

邮箱：TheBTC3.0@gmail.com