基于讯链的数字资产翻新方案

讯链基金会

2017-6-30

目录

1 数字资产翻新方案摘要

1.1 背景简介

针对比特时代发布的《关于时代平台对部分缺乏维护的数字资产翻新招标公告》，讯链运营团队希望通过自身的技术投入，以及基于流量比运营团队现有的资源，和比特时代、币久网协商，在比特时代、币久网选择多种缺乏团队维护运营的数字资产，建立以讯链为主体的资产官网，注册相应的独立域名，建立相关的开源代码库，提供讯链区块链代码和客户端（PC 端）下载，并且未来会开发手机版（ios 端与 Android 端）。同时，讯链运营团队在讯链钱包和比特时代、币久网交易平台，提供针对国内话费充值、流量充值、国际通信服务等多种全球通信应用保障。

讯链运营团队希望通过全球通信服务这个跨国界的，全球性的刚性服务，为虚拟数字资产，提供一个应用背书，不仅在技术开发创新上，而且能在应用扩展上做前瞻性的，试探性的探索，从而为一些沉淀的数字资产从应用角度上召集新的力量，为行业的进一步发展做成贡献。

1.2 运营团队

讯链核心运营团队包括如下核心人员：

彭波先生，互联网、通信和信息安全方面独立天使投资人和创业

者。曾任中国密码学会芯片分委会委员，国家发改委高新技术产业示

范项目技术负责人，科技部科技支撑计划项目负责人，多项国家“863”计划课题技术负责人。曾担任国家密码局可信计算、电子交易、数字电视等多个密码应用技术专项组成员，曾获得 2006 年国家密码科学技术进步二等奖，多项信息安全和通信领域专利发明人。 在讯链运营团队中，彭波先生將负责整体团队的召集组建和相关资源的筹措。

2 方案介绍

讯链英文名为 InfChain，讯链中的虚拟资产名为讯链（简称 INF），总量 10 亿，通过 POW 的方式全部产出，其中 9.5 亿枚 INF 会按照市值分发给翻新币持币用户，0.5 亿枚归研发团队所有（在达到项目预

期后激活）。INF 发布后，将会转为 POS 机制，POS 年膨胀率为 3%。完整代码将会在 github 上开源，并保持实时更新。

2.1 讯链发行总量测算

讯链的发行，其核心应用就是在讯链的钱包和交易平台，针对讯链提供针对国内话费充值、流量充值、国际通信服务等多种全球通信应用保障。因此讯链的很大一个实际应用场景，就是扮演通信应用保障中流量交易的虚拟货币角色。讯链的总额以及挖矿算法的难度需要我们根据现实世界流量交易的经济模型所设定，数据与实体经济相结合，从而对讯链的总额和挖矿算法难度做一个合理的设定。

下列数据均来源于世界知名企业的年度分析报告。

爱立信 2016.6 移动市场报告：

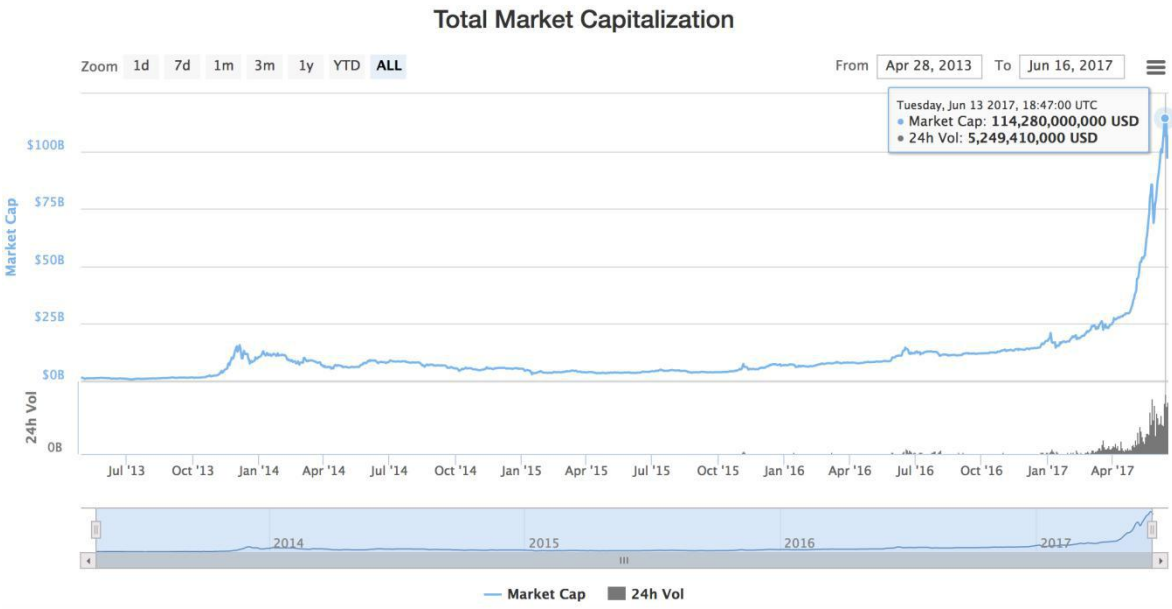
全球流量总额及发展趋势

地区	2016 年	2021 年	增长
中东和非洲	7.3EB	88.4EB	12 倍
亚太区	37.3EB	274.2EB	7 倍
拉丁美洲	5.4EB	34.8EB	6 倍
中欧和东欧	11.1EB	63.0EB	6 倍
西欧	8.8EB	50.3EB	6 倍
北美洲	16.9EB	76.8EB	5 倍

如上图表格所示，2016 年全球移动数据流量总计约为 86.9EB，

到 2021 年全球移动数据流量将达到每月 49 EB 或每年 587 EB。世界银行报告，2015 年世界总 GDP 约为 74 万亿美元。暂不考虑未来增值情况，针对于近两年的各项数据而言，全球 4G 网络平均费用为 4.86

美元/GB。2016 仅就 4G 网络而言，总消费已达 933 亿*4.86 美元，占全球 GDP 比重约为 0.5% 。



截止至 2017 年 6 月 16 日，虚拟货币市场总市值最高已达 1142.8 亿美元。拟定讯链市值在虚拟货币市场中市值比重等同于全球移动数据流量产生费用占全球 GDP 比重，即可基本计算出 2017 年期望讯链市值。讯链市值 = 0.5% * 1142.8 亿美元 = 5.7 亿美元。（注：该市值为模型测算，不代表投资建议，实际项目运行存在推广失败、技术竞争及运营不善等多重风险，请读者务必独立思考）

上述流量数据表格所示，2021 年数据流量达 587EB。虚拟货币市场市值涨幅在过去一年中超 800% 。增值速度难以精确评估，预计涨幅远超 2016-2021 数据流量使用增幅。

2.2 讯链技术架构

讯链主要技术架构分为协议层、扩展层与应用层

协议层可分为网络层与存储层。网络层方面，前期使用 POW 挖矿、之后转为 POS 挖矿、投票。数据存储方面，使用的是谷歌的 LevelDB，拥有良好的读写性能。

共识机制：

前期采用工作量证明（POW）机制，从而生成区块，一个符合要求的 Block Hash 由 N 个前导零构成，零的个数取决于网络的难度值。要得到合理的 Block Hash 需要经过大量尝试计算，计算时间取决于机器的哈希运算速度。当某个节点提供出一个合理的 Block Hash 值，说明该节点确实经过了大量的尝试计算，当然，并不能得出计算次数的绝对值，因为寻找合理 hash 是一个概率事件。当节点拥有占全网 n%的算力时，该节点即有 n/100 的概率找到 Block Hash。

讯链的应用场景之一是可以兑换流量，这对于流量运营商而言，虚拟资产的总量需要把控一定数额，且交易速度需要一定保障。POW 机制下交易速度无法过快否则会导致网络不安全，而 POS 则可以完美解决这个问题。POS 币的分发本身类似于运营商对于流量的分发，只需总量设置合理则 POS 机制运营会相对稳定，根据对于讯链总量的演算可得 POS 机制更加适合我们币种。故 POW 结束后将转为 POS 机制。

转为 POS 机制后，交易的低延迟可以极大改善用户的体验。POS 的主要思想是节点记账权的获得难度与节点持有的权益成反比，相对于 PoW，一定程度减少了数学运算带来的资源消耗，性能也得到了相应的

提升，但依然是基于哈希运算竞争获取记账权的方式，可监管性弱。该共识机制容错性和 PoW 相同。它是 Pow 的一种升级共识机制，

根据每个节点所占虚拟资产的比例和时间，等比例的降低挖矿难度，从而加快找随机数的速度。

交易速度：

出块方面每 1 分钟出一个块，每个区块最大大小为 1MB，需要 6 个节点确认，平均每笔交易（区块打包时间+处理区块+节点确认）只需 2 分钟左右即可完成。

安全性：

讯链的 PoS 机制能够有效地防止 51%攻击。在 PoS 体系中，即使你拥有了全球 51%的算力，也不能进行 51%攻击，因为，货币并不是挖矿产生的，而是由利息产生(利息存放在 PoS 区块中)，这要求攻击者还需要持有超过总量 51%的讯链资产，这大大提高了 51%攻击的难度。而且，如果自身拥有 51%资产量而发动 51%攻击，必然会导致自身资产的大量损失。所以纯 PoS 机制有效的消除了 51%威胁。

去中心化的区块生成和广播：

即不断摒弃挖矿后，去中心化的网络需要一种新的方法来就下一步添加什么区块来达成共识。在一个成熟的网络中，交易可以以每秒 12 次的速度产生，而网络的传播可能会延迟 60 多秒。这意味着，销毁更多币天数的新区块，其产生速度要超过其传播速度。如果没有挖矿，就没有抽签机制来每 10 分钟选择一个节点，该节点被赋予包括（或不包括）该区块交易的权力。

网络必须要有一种方法来调节交易和区块的产生速度。参照比特币调整难度的方式来调整每个区块的最低费用就可以实现这一点。这些费用会将交易量降低到所需要的数率，而且延迟建立第一候选区块的时间，但是，一旦第一候选区块构建成功，额外的候选区块仍会以比第一区块传播速度更快的速度产生。交易的速度可能会维持在每秒 12 个，随着输入数量的增加，一个区块中的新个体输入能够比其他所有输入销毁更多币天数的频率会越来越低。这提供了一个自然而独特的选择节点来签署区块的方式。考虑到交易额的大小，他们在所赚取的费用和交易验证中有既得利益。事实上，如果他们不签署该区块，而且也没有更大的输入，那么这个交易就会被强制从区块中移除，这样第二大输入就可以成为最大输入并签署区块。实际上，这个机制上创建了产生一个区块的时间上限，而交易费用则设置了一个下限。

POS3.0:

A.将币龄从等式中拿掉

运行一套 PoS 系统最安全的方法是将尽可能多的节点纳入网络，越多节点在线进行权利累积，系统遭受安全问题（例如 51%攻击）的可能性就越低，通过节点确认的交易确认速度也越快。

因此，拿掉币龄就需要所有节点必须更多的保持在线以进行权益累积。积攒币龄的方法在新系统里将不再可能，新系统采用以下公式计算权益累积的机会：proof < 币数 • 目标

需要注意的是该公式的系统不会改变实际的权益奖励值

B.改变权益修正因子

为了降低预先计算攻击的可能性，权重修正因子在每一次修正因子间歇时都会改变，以便对将要用来下一个权益累积证明的时间戳的计算结果进行更好的模糊处理。

C.时间戳规则

我们对区块时间戳做了适当的改变，使其在 PoS 机制下更有效的工作。预计区块时间将在原本的 60 秒的基础上有所增加，以匹配粒度。需要注意，假设节点有外部时间来源，并且节点的内部时间与全网整体时间之间的差异太大，则此节点产生的区块将很可能成为孤块。对区块时间戳规则的修改为：粒度 16 秒，预计的区块时间 64 秒。

应用层中，讯链的钱包除了应有的发送、接受、地址簿、币种的信息展示、查询交易 ID 功能之外，未来將为用户开发用于落地应用场景的功能。用户登记个人手机号，可在每个月固定日期领取手机流量，此功能将会接入钱包客户端当中，前期以交易所领取为准。我们还将会推出轻量级手机钱包，一键对接手机领取流量，为用户做到极致的体验。在区块链市场扩张迅猛之时，真正做到一款体验良好的产品。未来会开发更多的实用性功能，包括但不仅限于上述产品功能。

钱包大小方面，截止至 2017.6 月，比特币网络的区块总大小约为 128G，自创世块 2009.1.3 日以来，已经运行了 8 年零 5 个月，而

讯链的 pos 模式已经经过市场验证的机制，平均每年增长 1GB，占用硬盘大小非常低。

API 调用方面与 bitcoin 一致。

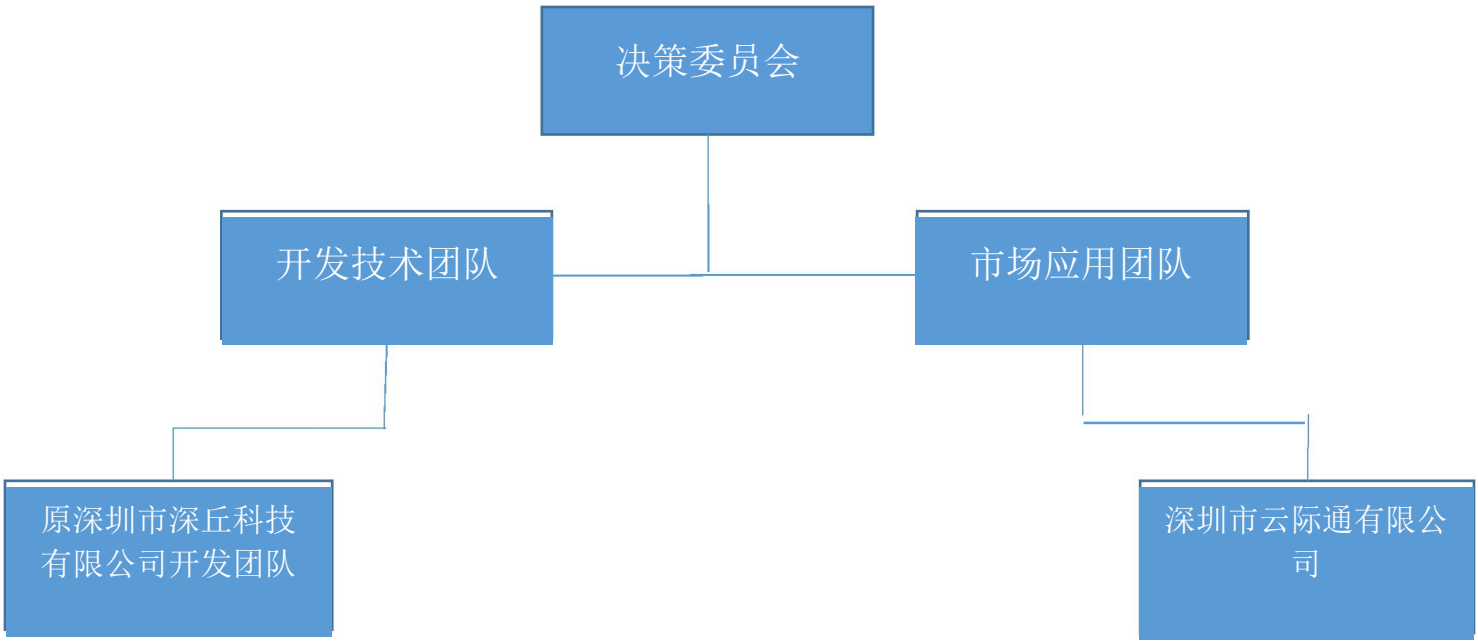
扩展层中，智能合约将是讯链的一个重要方式，讯链的数据代表着用户的可兑换流量数额，未来可通过侧链与智能合约等调取数据以及通过 API 接口的方式达到自动兑换流量的目的。讯链将会保持关注侧链技术与智能合约的发展，一旦技术成熟与测试通过，将会保持更新为用户带来更好的体验。

2.3 讯链基金会运作简介

讯链基金会（以下简称“基金会”）是非营利性组织。基金会致力于讯链的开发建设和治理透明度倡导及推进工作，促进开源生态社会的安全、和谐发展。基金会将通过制定良好的治理结构，帮助管理开源社区项目的一般轶事和特权事项。

基金会治理结构的设计目标主要考虑开源社区项目的可持续性、管理有效性及募集资金的安全性。基金会由团队人员组成，组织架构主要由决策委员会、开发技术团队、市场应用团队组成。基金会成立初期，决策委员会由基金会主席、团队核心人员和私募成员组成，每期任期为二年。

基金会结构图



基金会设立决策委员会，其职能包括聘任或解聘执行负责人以及各职能委员会责人、制定重要决策、召开紧急会议等。决策委员会成员和基金会主席任期为两年。

决策委员会任期期满后由社区根据讯链资产数和币龄计算权重进行投票选出 10 名社区代表，再进行投票选出 3 位决策委员会的核心人员，被选出的核心人员将代表讯链基金会做重要和紧急决策，并需在任职期间接受授信调查，并公开薪酬情况。凡下列事项，需经过决策委员会以记名的投票方式进行表决，每名决策委员会成员有一票投票权，基金会主席有两票投票权。决策委员会做出决议，必须获得全体在任委员会成员的过半数通过：

- 修改基金会治理架构；

- 任免执行负责人及各职能委员会负责人；
- 制定重要决策；
- 决策委员会成员在任期内的任免，如成员违反职能范围、法律、行政法规、主动辞职等
- 紧急事件，如影响整个社区的事件、软件安全、讯链系统升级等

此外，当有下列情况之一时，执行负责人应在 5 个工作日之内召集决策委员会举行临时会议：

- 基金会主席认为必要时；
- 三分之一以上决策委员会成员联合提议时；

执行负责人提议时决策委员会会议应由委员会成员本人出席。因故不能出席的，可以书面委托委员会其他委员代表出席。未委托代表的，视为放弃在该次会议上的投票权。

执行负责人由决策委员会选举产生，负责基金会的日常运营管理、各下属委员会的工作协调、主持决策委员会会议等。执行负责人定期向决策委员会汇报工作情况。

应用团队会负责筛选适合的行业，将讯链技术应用到行业中，从而实现商业落地。

代码审核委员会由讯链开发团队中的核心开发人员组成，负责底层技术开发、开放端口开发和审核、各产品开发和审核等。此外，

各产品的开发人员每周召开项目追踪会议，沟通项目进展及需求。代码委员会成员每日了解社区动态和热点，在社区中与 讯链持有者进行沟通交流，并且不定期举办技术交流会。

财务及人事管理委员会负责项目募集资金的运用和审核、开发人员薪酬管理、日常运营费用审核等。

2.4 讯链全球运营

（1）讯链节点部署

讯链是全球运营的虚拟资产，初始节点将会部署在全球多个地点，使得全球各地的节点加入初始同步及区块广播有一定的速度保证，分别是：纽约、东京、悉尼、香港、杭州、深圳、伦敦、莫斯科、柏林 。

（2）讯链国际网站

讯链作为国际运营团队，将会面向全球开发和运营多语言官方网站，第一版为英文，之后将会加入多语言支持。网站将会介绍讯

链团队、基金会以及运营模式。之后将会对接流量兑换接口，方便用户更轻便地兑换全球流量。

预计 2017 年 10 月实现国内流量及话费兑换，2017 年 12 月实现全球 5 个不同国家和地区流量及话费兑换，2018 年 6 月实现全球 20 个不同国家和地区的流量及话费兑换，2018 年 12 月实现全球主要国家和地区的流量及话费兑换。

3 讯链翻新方案实施过程

讯链对平台现有数字资产的具体翻新过程描述如下：

3.1 公告日确定(7 月 28 日前)

具体日期请参见比特时代、币久网公告。

3.2 上线筹备期(7 月 28 日-8 月 4 日)

在上线筹备期，讯链运营团队需要准备如下工作：

- 在现有的产品基础上，根据最终方案调整相关产品和算法，并且按照约定完成初始资产数量的挖掘工作。
- 在平台进行讯链交易内测和钱包交易内测。
- 提供相关的开源代码库，讯链区块链代码和钱包下载。
- 完成在比特时代、币久网平台上正式上线交易上线准备工作。
- 和平台一起，进行相关翻新方案的宣传工作。进行相关公告，启动相应客服工作。
- 对所有持有待翻新币的用户以短信和邮件的方式发出通知，通知用户可以在 7 月 28 日+7 日内将待翻新币币按照固定比例和讯链进行兑换。
- 初始官网和钱包仅提供中英文版本。其他版本的开放进度根据具体运营情况而定。
- 讯链官方 QQ 群：659393167 640767013

3.3 上线初始期(8 月 4 日 - 9 月 15 日)

应用方面，讯链的区块链浏览器将在 9 月 15 日开放。8 月 30 日前启动讯链钱包和平台的讯链兑换流量服务，微信公众号的流量兑换功能同步上线。9 月 30 日前开放针对全球客户，提供全球上网流量实体卡的兑换服务。后期根据需求的具体情况，在应用扩展上，团队将开放针对全球客户的包括中国在内的流量充值服务。在技术开发创新上，将实现基于智能合约的流量交易。

3.4 正常运营期(9 月 15 日以后)

讯链进入到正常运营期。讯链的运营管理规则按照讯链基金会的章程正常运作。

讯链的手机客户端（android+ios）将会在 10 月 30 日前推出。后续将会在手机客户端中加入流量兑换功能，具体时间视团队运营情况与应用开发周期而定。