BITCONCH 贝克链

基于创新性PoR信誉共识的分布式协议

A Newly Distributed Web Protocol Based on an Innovative Proof of Reputation (PoR) Consensus Algorithm

www. bitconch.io

目　录

摘要 1

第一章 背景及行业痛点 2

1.1 公链之争 2

1.2 公链的基础——高性能 2

1.3 公链的痛点——生态和流量 3

第二章 创新的 POR 共识协议 4

2.1 创新的 Bit-R 信誉量化体系 5

2.2 PBFT 实用性拜占庭容错 8

2.3 创新的 BLAZE 并行处理技术 10

2.4 SHARDING 数据分片技术 12

2.5 系统架构图及其他相关技术 12

2.6 安全性分析 15

2.7 有效抗中心化 16

2.8 制衡哲学打破三角困境 17

第三章 流量交互平台及生态共建体系 18

3.1 区块链世界的信誉体系 18

3.2 用户激励及社群治理 19

3.3 流量交互平台 20

3.4 落地应用场景及布局 22

第四章 技术团队及顾问团队 23

第五章 技术线路图 25

第六章 经济模型 26

6.1 运行通证 BUS 设计 26

6.2 通证的作用与职能 27

6.3 经济模型分析 27

6.4 融资计划及资金用途 28

第七章 免责声明 30

附录：参考文献 31

摘　　要

贝克链是十万级 TPS 并兼容以太坊智能合约的高速公链。于 2018 年 10 月 3 日向全球发布 MVP 测试结果，在五个不同国家的分布式节点公网环境下，峰值速度达到 120,000TPS，是目前全球已知的同等运行条件下速度最快的基础公链。

在性能方面，贝克链提出了创新的 PoR（Proof of Reputation）信誉共识算法，通过 Bit-R 信誉值（Bitconch Reputation）选择诚信节点来有效抗中心化，通过 PBFT 实用性拜占庭容错提高共识效率，通过创新的 BLAZE 技术提高并行处理效率，通过 Sharding 分片技术实现多节点协作。

在安全性方面，POR 共识算法和 Bit-R 信誉体系使系统拥有良好的容错性能、抗双花攻击和抗女巫攻击性能。为了有效抗击中心化，预防少数节点联合作恶，贝克链通过扩大候选池、提高作恶成本、基于交易历史的信誉无法合并等方式，更公平的让更多高用户参与和获得系统权益。

Bit-R 信誉体系是贝克链的另一项重要创新，代表用户在区块链世界的可信度、贡献度和活跃度，由用户行为、时间（币龄）、算力贡献三个维度构成。Bit-R，可以在满足用户隐私保护的前提下为开发者提供精准的用户行为画像。同时，也为开发者在启动闪电网络（高频离线交易）提供了执行标准。Bit-R 信誉在用户激励、节点激励、社群治理和生态可持续发展方面具有重要意义。

在吸引和帮助开发者方面，除了上述所介绍的基于 Bit-R 信誉值的各种开发工具之外，贝克链还兼容以太坊的 Solidity，golang 等多种语言的智能合约。

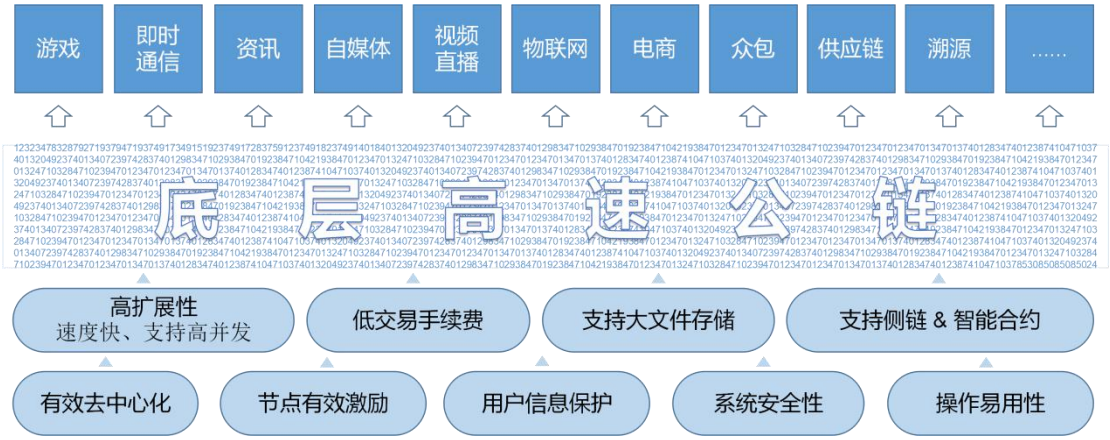
在生态建设方面，贝克链通过经济学模型构建了一个流量交互平台。自带流量的开发者和社群领袖将成为参与共识的诚信节点，通过贡献流量获得系统奖励。没有初始流量的开发者可以凭借优秀的产品获得更多用户试用机会，因为用户为了增加社交活跃度有动力、有积极性去尝试各种 DAPP 应用。因此，贝克链以 Bit-R 信誉激励为核心，形成开发者、社群、广大用户之间的共建合力，使贝克链生态在未来可以实现可持续发展。

第一章 背景及行业痛点

1.1 公链之争

公链，在性能上可以粗略分为高额低频交易和高频小微交易两大类。两者对于可扩展性、安全性和分散性的技术需求不同，可以服务的落地应用场景也不同，与之匹配的经济模型和商业模式也不同，特别是在节点共识、流量激励、社群治理等方面。高频小微交易的公链开发难度最大，但适用范围也最广泛，应用场景及底层技术需求如图1所示。

图 1. 支持高频交易的公链应用场景及技术需求



1.2 公链的基础——高性能

公链，作为各种DAPP应用的底层基础设施。只有搭建高速、稳定的基础公链，才能使各种落地应用的侧链和智能合约有底层操作系统可用，才是孕育杀手级应用的土壤和基石。

速度，是公链的基础，特别是当千万级应用运行时，高通量、高并发性、稳定性、安全性是决定用户体验的重要因素。目前，大部分主流公链的速度在几十至几千TPS（Transaction per second，每秒传输速度）之间，难以满足大规模落地应用对速度和并发性的技术需求。例如：

- 以太坊：15~20 TPS
- Cardano：≈ 300 TPS

- IOTA：≈ 800 TPS
- NEO/小蚁：1,000 TPS
- EOS：≈ 3,900 TPS

纵观一些中心化的应用，交易速度至少应满足几万TPS。例如：

- Visa/万事达卡：24,000 TPS
- Facebook脸书：52,000 TPS
- 股票市场：100,000 TPS
- 支付宝：250,000 TPS

1.3 公链的痛点——生态和流量

目前区块链领域缺乏杀手级应用，已成为限制区块链发展的主要因素之一。全球存量用户预计约 2,000 万左右。以太坊上现存的 DAPP 中最活跃的应用是 Etheremon，以 2018 年 10 月 17 日的数据为例，24 小时内的活跃人数只有 496 人。增量用户的导入需要杀手级应用作为媒介，通过产品体验逐步完成用户对区块链的教育和转化。

一个自带流量的开发者为何要将自己的杀手级应用运行在这条公链上？这个问题成为所有公链面临的极大挑战。在区块链这个开源的世界里，复制和抄袭是常态化的。技术的先发优势会随着项目的开源被其他项目快速借鉴使用，甚至站在前人肩膀上加以优化并超越。若要成为全球第一梯队的主流公链，不仅需要底层技术在性能上具有核心竞争力，更需要经济模型和商业模式上能够支持可持续的生态建设，吸引并奖励自带流量的开发者来参与生态建设，孕育出更多杀手级应用。能否快速形成流量汇集和孕育出杀手级应用才是一条公链能否成功与否的关键。

商业竞争的本质是流量竞争，在技术壁垒不高的前提下，比拼的是经济模型能否有助于运行通证的价值提升，商业模式能否吸引开发者和激励流量汇集，以及社群治理效率。

第二章 创新的 POR 信誉共识协议

贝克链已于2018年10月3日向全球发布MVP测试报告[1]，在五个分布式节点（分别位于纽约、阿姆斯特丹、法兰克福、新加坡、北京）公网环境下，峰值速度超过12万TPS，是目前已知的同等运行条件下速度最快的基础公链。此次MVP测试目的是为了证明并展示贝克链提出的创新的PoR共识算法可以顺利实现，可以达到十万级TPS的高性能既定目标。MVP是贝克链技术研发过程中的一个重要里程碑。此次MVP展示了PoR信誉共识中PBFT和BLAZE两个核心算法的协同效果。Sharding技术将在未来版本中逐步实现，将会进一步增加系统性能。

贝克链的高性能得益于由贝克链团队自主研发的具有突破性创新的PoR信誉共识协议，该算法在结构上包括四个部分：

- 创新的Bit-R信誉量化体系：用于选诚信节点，并有效抗中心化
- 基于PBFT的拜占庭容错过程：提高共识效率
- 创新的BLAZE技术：提高并行处理效率
- SHARDING数据分片技术：实现多节点协作

图2. PoR信誉共识协议架构图

2.1 Bit-R信誉量化体系

区块链技术的核心是共识算法，共识算法的本质是在分布式网络中，各节点互不信任的条件下，通过举证稀缺资源的方式，形成了纳什均衡的博弈场，赢得各方的信任，快速在各个节点之间达成一致，并同步的完成任务。

PoW，Proof of Work/工作量证明，举证的是矿工的时间和电力；PoS，Proof of Stake/权益证明，举证的是权益，用持币数量或币龄计算。共识就是能够举证某项稀缺资源，因而被信任，可以参与共识，贡献算力，获得奖励。贝克链提出通过举证信誉的方式，来获得共识的达成。

2.1.1 交易数据模型与社交图谱建立

贝克链提出的 Bit-R 信誉体系（Bitconch Reputation System）是基于有向无环图的 DAG 交易数据模型和 Social Graph 社交图谱模型建立的区块链世界的信誉和声望量化体系。

图 3（a）和（b）展示了交易数据结构和社交图谱之间的互动关系。15 个用户产生了从 Tx0，Tx1 到 Tx13 的 14 笔交易，构建了如（b）所示的社交关系。随着交易 Tx 的增多，社交图谱中各个节点之间会有越来越多的边，社交网络趋向成熟。

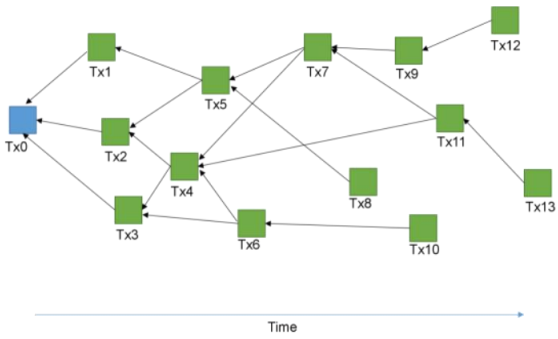


图3（a）交易数据的DAG数型结构

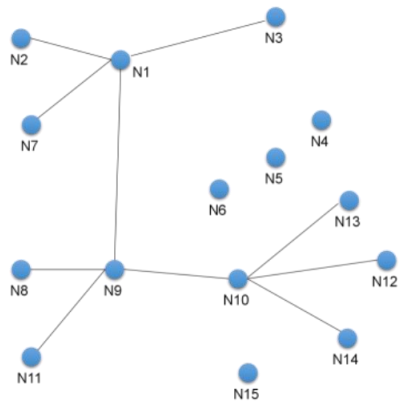


图3（b）社交图谱

如图 4（a）和（b）所示，当新交易 Tx14 和 Tx15 生成时，其中 Tx14 表示用户 N1 向 N4 转账 m 个 BUS，Tx15 表示 N5 向 N1 转账 n 个 BUS，如果 m>n，对于 N1 的信用贡献，Tx14 大于 Tx15 的权重。除了交易额对信誉贡献的影响之外，用

户 N14 和 N15 本身信誉值的越高，这笔交易的信誉贡献权重越大。随着交易的不断增多，社交图谱中各个节点之间的联系不断增加，提供更多的社交数据喂养信誉值。

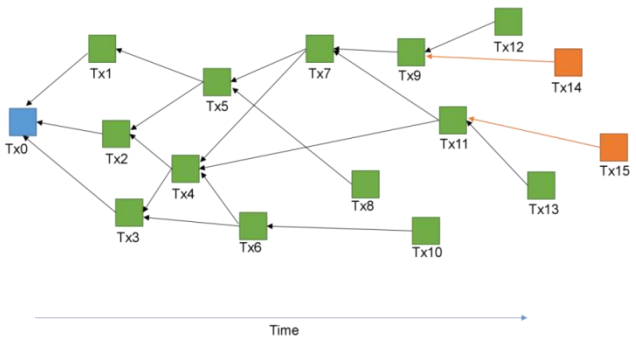


图4（a）新交易产生及验证

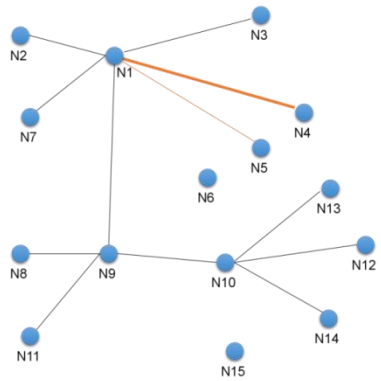


图4（b）新交易对社交图谱的影响

2.1.2 信誉模型和数学抽象

通过对用户社交、持币时间、算力贡献三个维度的活跃度进行数学建模，描绘了用户在区块链世界中的行为习惯和活跃程度，以及作为节点参与共识和记账的可信程度和算力贡献程度，如图 5 所示。

在区块链网络中，贝克链将信誉 Bit-R 由三个维度构建：社交活跃度 D、时间活跃度 T 和贡献活跃度 C。公式分别如下:

$$\mathcal{R}(\alpha，\beta，t) = \omega_1\mathcal{D}(E,t) + \omega_2\mathcal{T}(S,t) + \omega_3\mathcal{C}(N,t) \tag{1}$$

$$\mathcal{R}_n = \mathcal{R}_0 e^{\mu t} \tag{2}$$

$$\mathcal{D}(E,t) = \sum_{i=1}^{k} \alpha E_i^{\beta \log (D_r)} \tag{3}$$

$$\mathcal{T}(S,t) = \beta + \alpha \log (St) \tag{4}$$

$$\mathcal{C}(N,t) = \sum \alpha \mathrm{N}_{file} + \beta \log \mathrm{N}_{Rnd} \tag{5}$$

其中 ω_n为权重，在某个时间t内，D(α,t)为节点的社交活跃度，T(β,t)为每个节点的时间活跃度，C(γ,t)为贡献活跃度。为了能让用户有持续不断的活跃

度，同时也为了让后来者能更加公平的参与系统运行，避免先行者优势（FMA）带来的马太效应，我们规定Bit-R随着时间而进行衰减，如公式（2）所示。

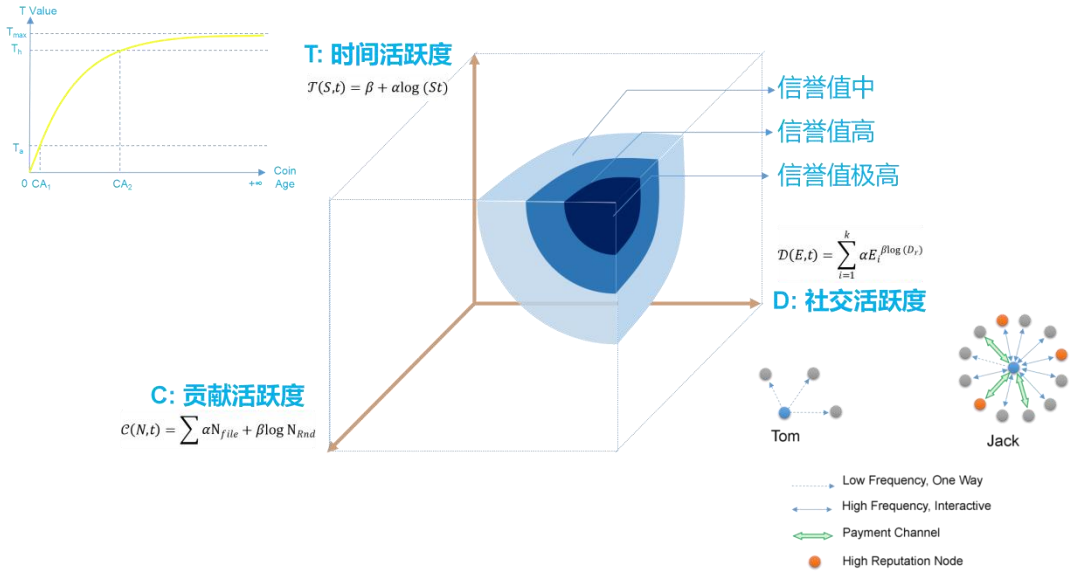


图 5. Bit-R 量化信誉演示图

社交活跃度 D：见公式（3）。由一个节点在应用社交网络中朋友的数量、与朋友互动的频率（即热度）、朋友的信誉值和交易额大小等多种因素决定。如图 5 所示，Tom 只有少数几个朋友低频次单向交流。而 Jack 有很多朋友，与朋友之间也是频繁互动的，有的朋友是高信誉用户，与有的朋友之间互为可信节点，适用于“交易通道”的高频离线交易。则 Jack 的 D 值远远高于 Tom 的 D 值。在对社交活跃度进行数学抽象时已经充分考虑女巫攻击的可能性，详见 2.6 章节。

时间活跃度 T：见公式（4）。该指标主要由用户持有 BUS 的币龄决定，我们认为通证的长期持有者比非持有者更可信，作恶动机更小。但与 PoS 共识中 Stake 权益不同，财富并非衡量节点是否可信的唯一标准。如图所示，T(β,t)的对数公式为广大的中产阶级用户提供获得高信誉机会。

贡献活跃度 C：见公式（5）。该指标描述节点用户对于系统的贡献度 C(γ,t)，表示在时间为 t 时，节点对于系统做了多少的贡献，N 是系统 Account Nonce 值，用于记录用户对于系统贡献的频率（分享文件和参与记账）。系统将会按定时任务对文件状态进行检查。

2.2 PBFT实用性拜占庭容错

实用性拜占庭容错过程包括两个部分：

（一）定义可信节点列表

（二）一个基于 PBFT 的拜占庭容错过程

2.2.1 诚信节点的定义和选择

定义诚信节点（Transaction Validator），在区块链网络中，有用户数为 N，每个用户都有 Bit-R 信誉值，根据每个节点的信誉值筛选出前 5%的高 Bit－R 信誉值的节点进入“节点候选池（Candidates Pool）”，标记为列表 𝕃，相当于节点社群中的“优秀公民”。

候选名单采用季度竞选制度，每季度更新一次。由于竞选节点数量的不确定性，为了保障有效去中心化同时兼顾系统效率，候选节点池设上限为 500 个，下限为 30 个。

即：

当 $N>10,000$ 时，$\mathbb{L}=500$

当 $N<600$ 时，$\mathbb{L}=30$

$30 \leq \mathbb{L} \leq 500$

诚信节点列表 𝕃 中的节点，系统每回合从候选名单 𝕃 中随机选择 M 个节点轮流参与验证共识，通过拜占庭容错过程，验证网络中的新交易。验证成功的交易被记录到系统的分布式账本之中，同时增加相应节点的信誉值。拜占庭容错过程，可以在有限作恶节点存在时，仍然为系统提供安全性和活性的保证。作恶的节点的信誉分数将被减少或扣除，并被取消共识和记账权益。

由于Bit-R信誉分数的差异主要来自于社交活跃度而非时间活跃度，所以诚信节点可能主要来自于贝克链生态中的商业开发者或社群组织，是生态中流量的主要贡献者。

2.2.2 拜占庭容错过程

在获得$\mathbb{L}$之后，信誉证明通过一个基于PBFT的拜占庭容错过程验证交易的正确性并更新账本。为了清晰的说明过程，我们做出如下定义：

系统中存在两种节点：非故障节点和故障节点。

非故障节点：

系统中运行正常，遵守规则并且无错误的节点。

故障节点：

出现错误的节点，包括超时、数据损坏和恶意行为（拜占庭错误）等。

我们做出如下规定：

- 节点验证交易，只会输出两种状态：0为验证成功，1为验证失败。
- 所有的诚信节点会在有限时间内做出决策。
- 所有的诚信节点会做出相同决策。

POR将共识分为若干个任期，每一任期都会从所有节点中，选择信誉值最高的5%的节点组成候选人池（Candidate Pool），每个任期包含若干回合，每个回合会处理若干交易数据，因此可定义$\mathbb{L}(k)$为第k周期的诚信节点列表。$\mathbb{L}(k)$中含有M个节点，是从所有节点中信誉值最高的百分之五所选择出来的。

达成共识流程：

- 使用分布式随机数生成算法，$\mathbb{L}(k-1)$中节点生成一个随机字符串$\mathrm{Str}(k)$
- $\mathrm{Str}(k)$在M中所有节点中被广播，上一个回合结束。
- 根据$\mathrm{Str}(k)$，从$\mathbb{L}(k)$随机选择出一个Leader节点，和相应的投票节点（Voting Node）。
- Leader节点负责交易的广播。投票节点验证交易，并投票。
- Leader节点负责通过哈希函数，在各个节点之间同步周期和回合数。
- 有若干未验证交易Tx0。
- 本回合又有若干新交易生成Tx1。
- 未验证交易Tx0和新生成Tx1，汇聚到Leader节点，组合成待验证交易列表Tx。

- Tx会在$\mathbb{L}(k)$中广播，$\mathbb{L}(k)$中的投票节点会验证交易，并进行投票，若交易获得足够多的投票，则该交易会被确认，并被更新到账本中。
- $\mathbb{L}(k)$中的节点会分为Leader节点和Voter节点。$\mathbb{L}(k)$的作恶节点小于m/3，即投票数>2m/3，则该回合定义为成功。$\mathbb{L}(k)$中节点的贡献活跃度增加，相应节点的交易活跃度增加。

2.3 创新的 BLAZE 并行架构

为了进一步提高系统并行处理效率，提高运算速度，贝克链团队首次提出 BLAZE（Bitconch Ledger Access Zero-delay Extension）贝克链零延迟账本访问技术，简称 BLAZE 并行处理技术。

BLAZE 的架构设计受到了 Classic RISC pipeline（经典精简指令集流水线）的启发，如图 6 和 7 所示。将区块链验证中的数据 Fetch、解码 Decode、哈希运算 Hash、状态变更 State、写数据 Write 的五个步骤，在操作期间，每个流水线阶段一次处理一个指令。这些阶段中的每一个都包括一组初始指令，这些指令对进入的交易的输出进行操作。

图 6. 创新的贝克链零延迟账本访问技术

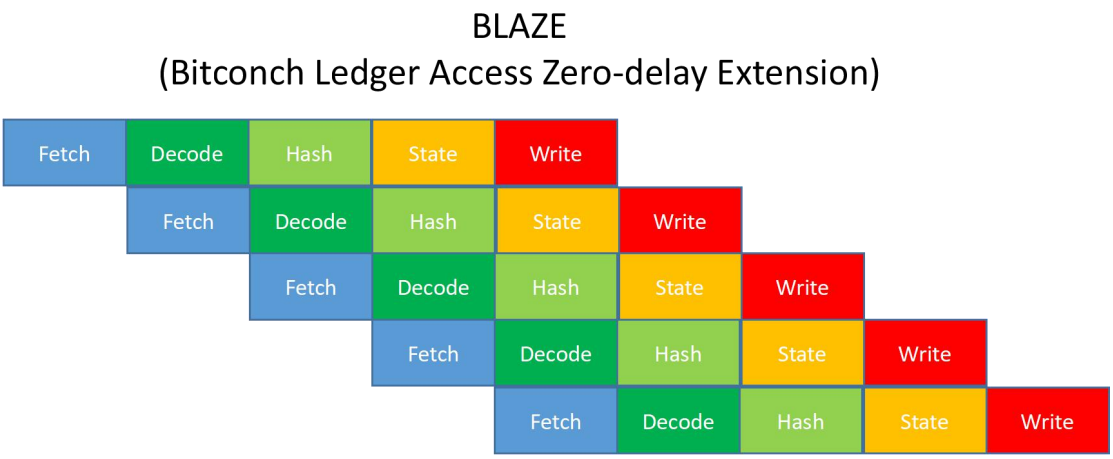
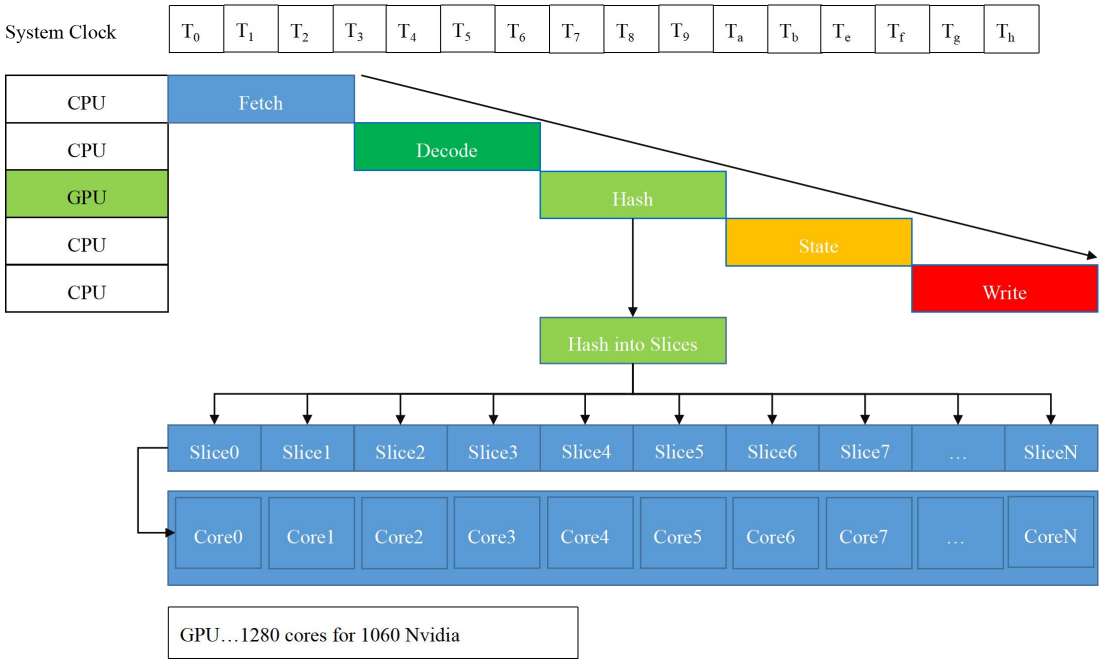


图 7. BLAZE 架构图



Finality Time（终态确定时间）

终态确定时间是确认区块链上的数据最终状态所需要的时间。提高区块链的速度，就是要减少终态确定时间。POR 算法通过 Reputation 定义了诚信节点，缩小了确认终态的节点数量，从而减少了确定时间。但是要达到亚秒级的速度，还需要快速的验证大量的交易块（本地），同时快速的在网络各个节点之间快速的广播（网络）。对于交易验证来说，签名验证是最需要消耗时间的部分（瓶颈），此外还有诸多如网络驱动、数据依赖性的管理等诸多部分都需要消耗时间（瓶颈）。我们需要定义一个可以让所有的硬件的等待时间最少的架构，因此贝克链借鉴了 CPU 设计中的经典精简指令集流水线设计思想，将多核处理（CPU 和 GPU）和五步流水线结合起来，可以达到验证交易速度的大量提升。

2.4 SHARDING数据分片技术

POR 支持通过分片技术（Sharding）提高吞吐量。分片技术借鉴于经典数据库中的分区技术，当数据吞吐量很大的时候，一个数据库的读写会需要很长的时间，因此可以通过将数据分别存储在不同的数据库的不同的表中，提供高速访问数据的能力。在 POR 中，我们从高信誉节点中选择 N 个节点，作为 Sharding 节点，Sharding 节点通过和 leader 节点保持同步，每个 Sharding 节点打包处理自己所关心的数据，通过上一层的 Leader 节点再一次将每个 Sharding 节点打包的交易进行确认。

首先在所有的记账节点中，定义一组 Sharding 节点和 Leader 节点。在这里我们使用分布式随机数生成算法，选择 Sharding 节点和 Leader 节点。Sharding 节点负责分流汇聚到 Leader 节点的 Tx，通过系统时钟，Sharding 节点和 Leader 节点保持同步，并且可以同步验证交易的正确性，系统时钟在这里充当了一个信息通道的作用，保证 Leader 节点和 Sharding 节点之间的一致性。每一个 Sharding 节点给自己处理的交易，加上一个标记序列（Sharding ID），Leader 节点和投票节点可以通过校验 ShardingID，从而对于交易进行确认。

2.5 系统架构图及其他相关技术

2.5.1 BVM虚拟机并兼容以太坊智能合约

贝克链通过提供多种工具支持开发者打造属于自己的分布式应用，丰富贝克链的生态系统。贝克链提供了基于 Solidity 的编程语言 BO 和相对应的虚拟机 BVM，如图所示。在贝克链上，开发者通过编程语言将商业逻辑转化为智能合约，智能合约通过虚拟机（Virtual Machine），将编程语言编程成机器可以运行的字节码。

BVM 相对于 EVM 有三大优势：

第一、更容易开发强大功能的智能合约

相比较以太坊的 65 个 opcodes，贝克链为了方便开发者能开发更优质的 DAPP，会提供更多可选的 opcodes 和标准库，扩展更多的社交和落地应用的功能。因为智能合约中通常都有大量的代币存在，一旦出现错误将对开发者和用户

造成巨大损失，因此 BVM 将会提供智能工具，检测交易顺序、时间戳、意外处理和可重入漏洞（Reentrancy Vulnerability）等常见 Bug。为了提升开发速度，让开发者更容易编写智能合约，BVM 将是一个基于寄存器的虚拟机。

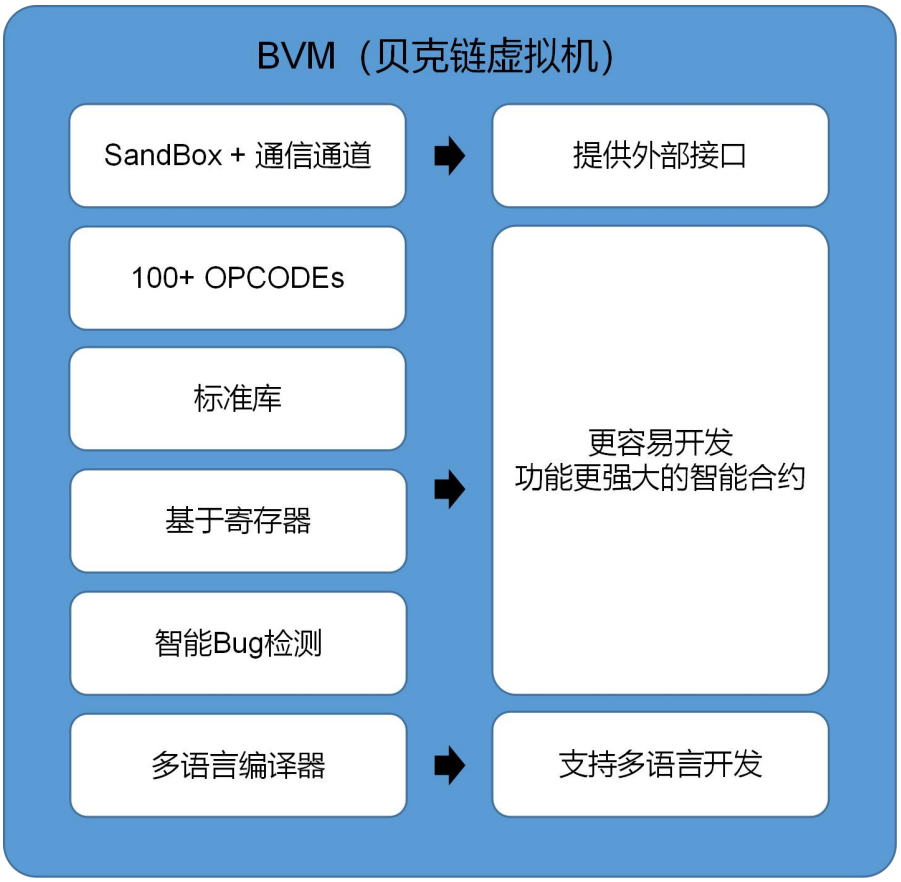
第二、提供接口，使智能合约和外部进行通信

相对于 EVM 和外部世界隔离（无法使用网络、文件或者其他进程的权限）的沙箱环境，BVM 通过数字签名建立传输通道，解决智能合约和外部世界的通信问题。

第三、支持多语言开发

为了能让更多的开发者加入贝克链社区，BVM 未来将支持 Python，Java，C++ 等多种开发语言。

图 7. BVM 虚拟机架构图



2.5.2 系统架构图

贝克链通过零知识验证将交易详情进行加密，从而保护用户的隐私。为了应对将来量子计算机时代的到来，贝克链将采用抗量子攻击的密码学算法。贝克链提供套件可以让用户生成可修改的智能合约模板。用户根据贝克链提供的模板和规则，可以开发出易于升级和管理的智能合约。贝克链支持不同的挂钩机制（Two-way Peg/双向锚地）实现主链和侧链的结合，并将为开发者提供侧链开发模板。在未来的应用场景中，贝克链作为主链将主要提供可信记账和信誉管理，更丰富的商业功能将开放并支持侧链进行实施。例如：贝克链将提供分布式存储功能，开发者可以在自己的侧链上实现文件存储、多媒体等功能。

图 8. 贝克链系统架构图

注：▲项为采用了当前最先进的技术或算法；

★项为贝克链具有自主知识创新和核心竞争力的技术或算法

2.6 安全性分析

2.6.1 女巫攻击

用户发动女巫攻击的目的是希望通过低成本的创建多个虚假账户来获取系统信誉奖励。由于每个用户的 Bit-R 信誉值是由持币数量和时间、历史交易、算力贡献值构成，如果大量的假账号没有持币和算力贡献值，这就使虚假账号缺乏 1~2 个维度的信誉分数，仅仅依靠交易数来积累 Bit-R 信誉值是有上限的，难以像绝大多数的真实用户一样通过三个维度获得更高信誉分数。

由社交活跃度计算公式可知，其中E_i为每次交易的权重函数，E_i与交易金额正相关，D_r是交易对象，$\log(D_r)$为关于D_r信誉值的对数函数，用于控制当D_r过小时，即一个节点和一个或者多个低信誉度交易，并不能显著提高自己的 $\mathcal{D}$ 值，这有效规避了试图通过增加虚假用户恶意提升信誉的可能。在社交活跃度计算时，不仅取决于交易数量，还取决于好友本身的信誉值，与一群虚假的没有信誉的账号互刷交易，信誉分数的增长也是有限的。而交易本身需要在机器上运行，需要电费和时间，假账号需要大量的时间来积累 Bit-R 值，成本非常高，根据朴素的经济学原理，是非常不划算的。

2.6.2 双花攻击

由于 POR 信誉共识算法采用的是确定性模型。若系统出现双花交易，由于拜占庭容错过程的确定性特质，即使两笔交易被同时确认，当其中的一个被更新到账本上后，另一个由于余额不足就会被自动舍弃，从而避免了双花攻击的出现。

作恶的节点将被追溯并受到惩罚，信誉值降低，失去参选信任节点的资格。由于节点的作恶成本远高于作恶可能带来的收益，所以作恶动机极低。

2.6.3 Runtime失败和超时失败

当 Leade 节点出现硬件故障、断电、Bug 时，其余的 Validator 节点可以触发选举，重新选择下一个 Leader 节点。这个时间段内的所有交易将不会被确认，会在新的 Leader 节点出现并开始工作之后，重新确认。

如果出现网络超时，系统也会重新触发选择新的 Leader。

2.6.4 拜占庭容错性

POR 信誉共识算法中采用了 PBFT 实用性拜占庭容错算法，具有 2/3 的拜占庭容错性。

2.7 有效抗中心化

贝克链采用两种方式来有效抗击中心化，预防节点之间联合作恶：

（一）扩大诚信候选节点范围至所有节点的 5%，从候选池中按照时间任务随机选择共识和记账节点。参与共识的节点范围越大，联合作恶的可能性越小。

（二）基于 Bit-R 信誉值来选节点。Bit-R 信誉值是每个用户和节点行为画像和历史交易记录，不能像代币一样合并和转移，所以节点之间联合作恶可行性小。

PoR诚信节点 vs DPOS超级节点

贝克链基于Bit-R信誉值选超级节点比DPOS基于持币量选超级节点更能够有效抗击中心化，防止节点作恶。

贿选，是DPOS算法在竞选超级节点过程中被广为诟病的弊端之一，因为用代币（钱）来选节点很容易导致参选节点之间为了谋取利益最大化而组织起来，贿选往往是难以避免的，取证过程也非常困难，因此难以通过社群治理来杜绝和惩戒。

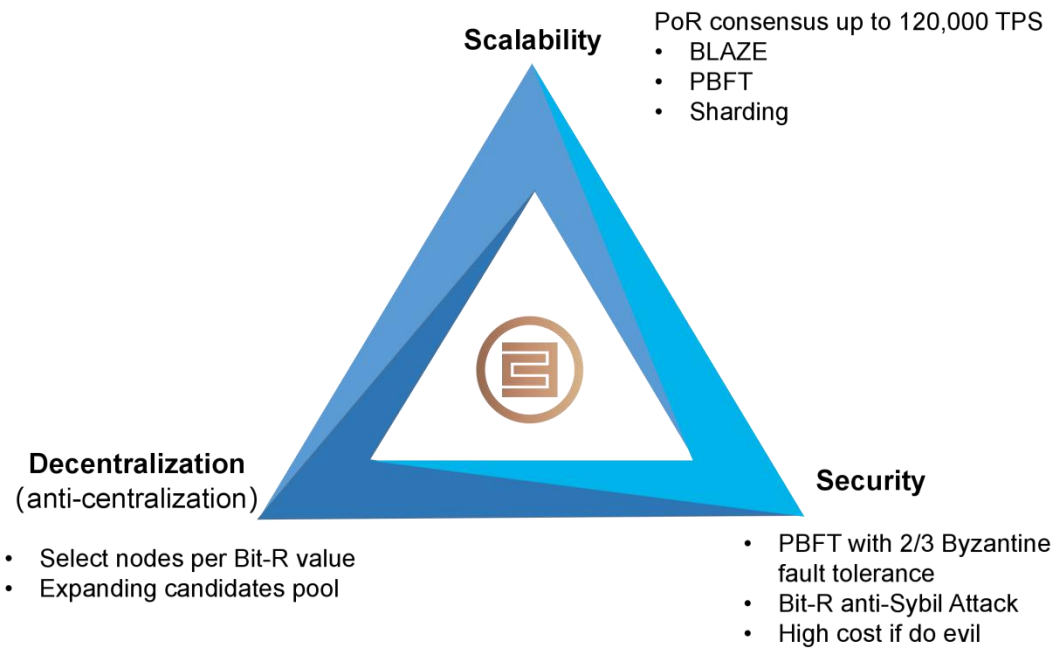
贝克链采用的PoR共识算法是基于Bit-R信誉值来选节点，每个节点信誉分数由社交活跃度（DAPP应用项目的用户量、普通用户的其朋好友数量、交易历史）、时间和算力贡献活跃度等决定，是经过时间积淀的。钱的合并是非常容易操作的，但信誉的合并是非常困难的，两个开发者不可能把流量合并在一起，即便合并，用户也未必愿意使用新的产品；两个社群即便要合并在一起，曾经的交易记录也无法复制，需要重新再来。因此，Bit-R信誉解决了DPOS在竞选超级节点过程中可能出现的“贿选”弊端，能够更加有效的抗击中心化，超级节点在参与共识的博弈中作恶成本更高。

2.8 制衡哲学打破区块链的三角困境

可扩展性、安全性和去中心化被认为是区块链的“三角悖论”，又称“不可能三角”。贝克链通过技术创新和制衡哲学实现了区块链的扩展性、安全性和有效去中心化。如图9.所示，通过PoR信誉共识等底层算法优化使贝克链实现了高可扩展性和安全性，贝克链创新的POR共识算法是以实用性拜占庭容错算法为基础，增加BLAZE架构和Sharding技术进一步提升系统可扩展性，但这种算法本身无法做到狭义的“完全去中心化”，而是巧妙的采用信誉值来提高可信节点的作恶成本，减少联合作恶的可能性。

前5%高信誉用户进入候选池，使更多的诚信节点可以参与共识，候选池中的节点再按时间任务选出有限的节点（专业设备、时时在线）参与共识，保障贝克链具有高性能，交易被快速度确认，并保持全网一致性。由于信誉的累计需要付出很高的时间成本。所以，贝克链通过信誉制衡机制达到有效抗击中心化。

图9. 贝克链的三角平衡图



第三章 流量交互平台及生态共建体系

3.1 区块链世界的信誉体系

传统的商业社会信誉体系已经有 150 年的历史，三大信誉机构为全美国人民提供了信誉画像。同时，美国的信誉体系又深刻的影响了欧洲、日本、澳洲和中国的信誉体系。传统的商业信誉描绘了精准的借贷关系，被广泛用于银行、租赁等需要评估用户借贷行为的相关行业和领域。例如：高信誉用户可以获得更高额度的银行贷款并享有更低的利率和更有低的首付。在享受租房、租车等服务时无需支付押金。

表1. 传统商业信用和区块链信誉Bit-R体系的对比

	传统的商业信用 Credit	区块链的信誉 Bit-R
历史	150+ 年	0 年
关系	借贷	活跃度和节点的信誉价值
目的	把钱借给谁?	选谁做可信节点?
收益	贷款额度更高， 利率更低 头款更低 租房无押金	被选为可信节点几率高 交易成本更低（甚至免费） 闪电网络无需押金
数据提供者	银行； 贷款机构； 讨债公司	区块链世界的所有应用
评价机构	中心化	去中心化

Bit-R是由贝克链提出并建立的区块链世界的量化信誉体系。Bit-R借鉴了传统商业信誉的治理和激励体系，区别在于Bit-R构建的是去中心化的区块链世界中，各个节点的活跃度和行为画像而非借贷关系，即：Bit-R解决哪个节点可以被信任，不作恶，可以成为可信节点参与共识或记账，获得相应的算力收益的问题，不解决银行贷款和按时还款的问题。Bit-R信誉越高，被选为可信节点的几率越高，交易成本越低（甚至免费），在运行闪电网络时无需押金。如表1所示。

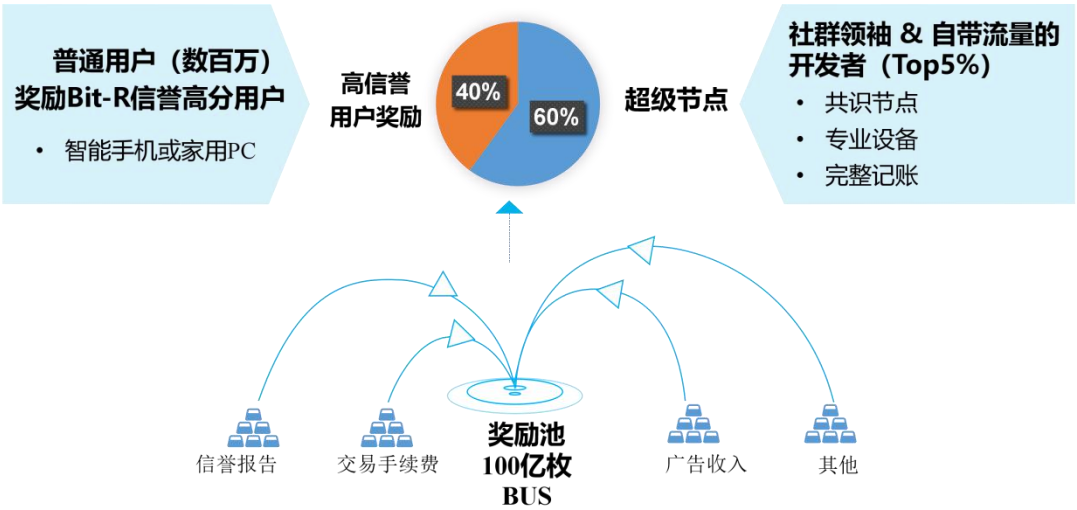
以美国三大信誉机构为例：2017 年，Equifax 销售额 33.62 亿美金，利润 5.87 亿美金；Experian 销售额 43.35 亿美金，利润 8.65 亿美金；Trans Union 销售额 19.3 亿美金，利润 1.2 亿美金。传统商业信用是中心化的，每年数十亿美元的丰厚收益归这三家公司及少数的股东所有。但在区块链去中心化的世界中，代码即法律，所有收益将归于社群共享，高信誉用户通过提供算力和存储等资源获得相应的奖励。

3.2 用户激励及社群治理

在Bit-R信誉量化模型中，分数的差距主要来自于社交活跃度，即：与本节点密切往来交易的节点数量越多、交易越频繁及这些往来节点本身的信誉分数越高，社交活跃度得分越高。由于时间活跃度中对币时的计算采用了对数函数，即持有一定数量的BUS就可以达到这一维度上很高的分数，各节点之间无法通过持币数量来获得明显优势。

社群领袖和商业应用开发者由于本身具有更多元的社交图谱和频繁交易，往往可以凭借流量优势累积更高的信誉值，被选为“诚信节点”的概率也越高，获得的系统奖励也越多。信誉奖励机制如图10所示。20%的BUS将投入系统的信誉奖励池，其中60%给诚信节点，40%给高信誉分用户。

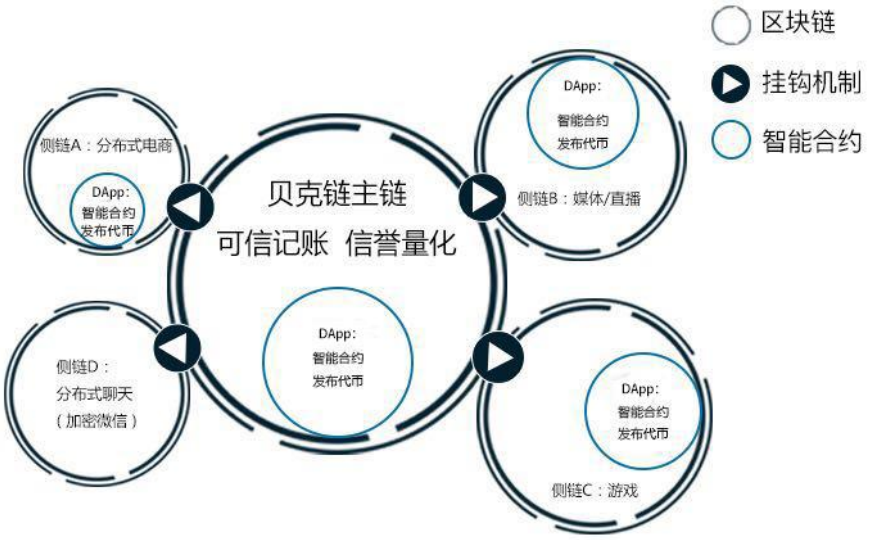
图 10. Bit-R 信誉激励制度



3.3 流量交互平台

Bit-R 的用户数据不仅仅来自于贝克链运行的智能合约或侧链形式的应用，还将通过跨链合作的方式对接各种运行在其他公链上的应用。因此，贝克链既是一个支持各种应用的底层基础公链，又是一个通过社交图谱和 Bit-R 信誉激励体系构建的流量交互平台。贝克链主网与侧链的交互关系如图 11 所示，大部分的商业应用可能会通过侧链运行，交易信息被记录在主网上，同时为主网提供信誉数据喂养。各个应用产品自带流量的同时，用户之间不可避免的存在交互共享（见图 12（a&b）），勾勒了更加丰富的社交图谱和生态系统。

图 11. 贝克链主链与侧链的交互关系图



社群领袖和开发者通过流量贡献将获得高信誉值，可以参选超级节点，并获得丰厚的Bit-R信誉奖励。自带流量的开发者可以凭借产品的流量优势成为贝克链BUS通证的持有者，与建设者和投资人一起共享权益。

即：

流量贡献 = 高信誉分数 = 诚信节点 = 贝克权益

广大的普通用户为了提升自己Bit-R信誉分数，特别是在社交活跃度中的分数，有动力和积极性去尝试使用各种需要的DAPP应用产品。因此，需要流量的

开发者可以通过不断打磨和提升自己产品的用户体验来赢得流量。随着流量的增加，Bit-R信誉值提高，可以获得信誉奖励。

即：

优秀产品 = 赢得流量 = 信誉分提高 = 成长为新的诚信节点

图12（a）. 各种应用之间可能存在的流量交互共享

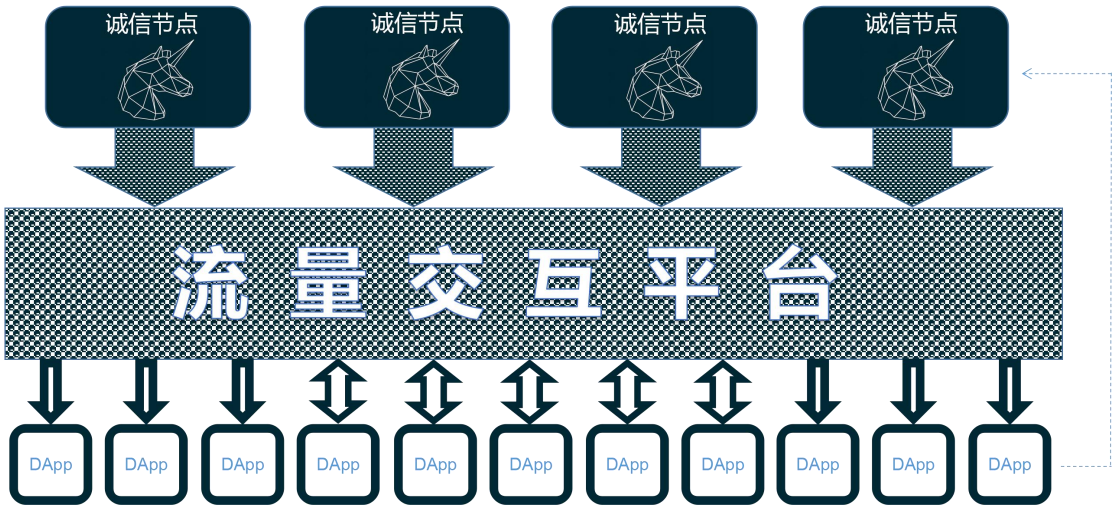
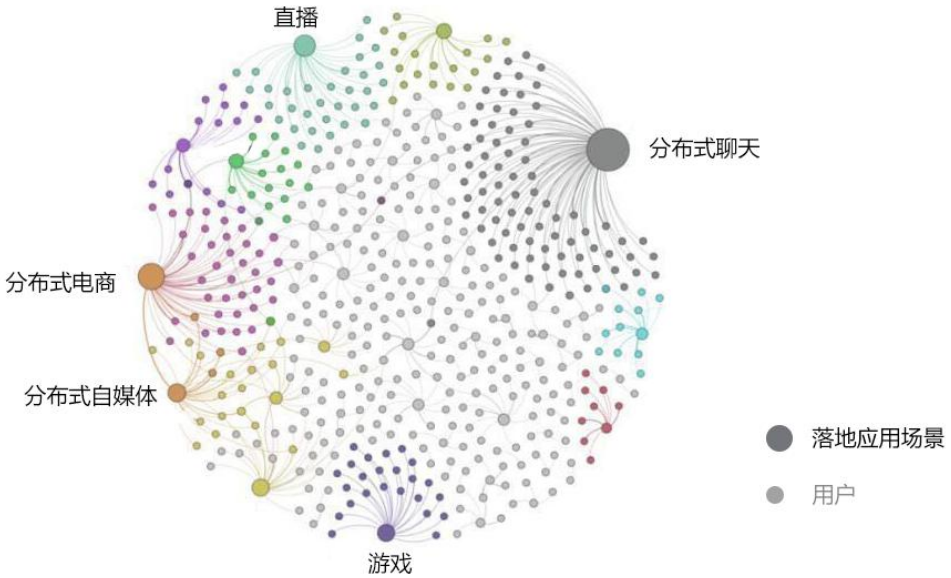


图12（b）. 各种应用之间可能存在的流量交互共享



3.4 正在进行的生态建设和应用孵化

创始团队基于自身在传统投行和传统商业的资源，孵化了多个自带流量的应用，累积覆盖用户超过1亿人，这些用户的转化是贝克链社区的非币圈增量用户。目前，孵化中的应用涵盖：游戏、智能自动售货柜（物联网）、供应链、产品溯源、通用积分异业联盟、分布式电商、分布式订票系统等。关于每个项目的详细情况将在各自的白皮书中发布。

第四章 技术团队及顾问团队

TECHNICAL TEAM

Joseph Sadove
CEO

Served IBM, Oracle, Goldman Sachs, UBS, Industrial Bank, Merrill Lynch, TD Securities

Bob Bergman
Chief Scientist

Raduated and taught at MIT, served and led Intel Corporation for 28 years, known for its technology vision and strategy

Neo LIU
CTO

Served as technical director of Vipshop, and technical executive in several listed companies, cloud computing, Internet of things and other technical fields

Caesar Chad
Technical Director

Served in Google and IBM Yitaifang code contributor, participated in the development of IBM distributed books and Artetoken core personnel of block chain project

Leon LIU
CIO

Served as IT executives in Former Deutsche Telekom, Danaher, Samsung, BMW and US General Electric IT .etc, graduated from RPI.

Sunmeet Singh
Architect

Technical Director at a number of companies including Skyhi, HSAglobal

John Y. Ten
Technical Director

Graduated from Texas Tech University, USA, previously working for IBM and Cisco's US headquarters.

G.F. Wu
Senior Engineer

Worked for huawei and several government agencies in software development

Y.K. Lee
Senior Engineer

Release a number of open source of IOS software. Participate in R&D and design of IOS system of several cross-company at home and abroad.

X.D. Wang
Senior Engineer

Graduated from Arizona State University and worked for companies such as MWA Intelligence.

C.Y. Xie
Senior Engineer

Worked for several listed companies such as iSoftStone, Bank of China, Beijing Capital Online, etc.

H.M. LU
Senior Engineer

Graduated from Fudan University and worked for several software companies.

CONSULTANT TEAM

Qingzhu DAI

One of the founders of Sesame credit(A subsidiary of alibaba), founding partner and COO of Bitcoin China. has rich experience in traditional finance and blockchain industry.

Jianjun YANG

Professor, department of computer science, university of north Georgia, USA. Chief academic tutor. American Distinguished Professor/Researcher

Pablo Oriando

Graduated from Harvard Business School and Stanford University. Worked in Ubanx , Avenida.com, G20 Foundation, Bluesmart, Inipop, GoodPeople.com

Jacopo Visetti

Graduated from Harvard University and Università Cattolica del Sacro Cuore. Worked in EFFORCE, AitherCO2 S.p.A, iStarter, Pragma Wealth Management Ltd etc.

OPERATION TEAM

Lilly MU

COO

Doctor of Biology.As marketing or R&D senior executives worked in NBTY and Isagenix.

Jack Sek

Finance Director

Years of experience in the financial industry, proficient in accounting, financial management.

Yong LIU

BD Director

Master of Internet Technology. Years of experience in the Internet business development.

Steven REN

Marketing Director

Continuous enterpreneurs in the Internet industry. Rich expericence in marketing planning and management.

Kira LIU

Design Director

Years of branding, visual design work experience in Australia. Korean GK media former design director.

第五章 技术路线图及执行进度

项目执行进度：MVP已完成，并向全球发布【1】。

Youtube：https://youtu.be/e3SXoLPPpI8

优酷视频：https://m.youku.com/video/id_XMzg0OTA0ODE1Mg==.html

下一个节点：

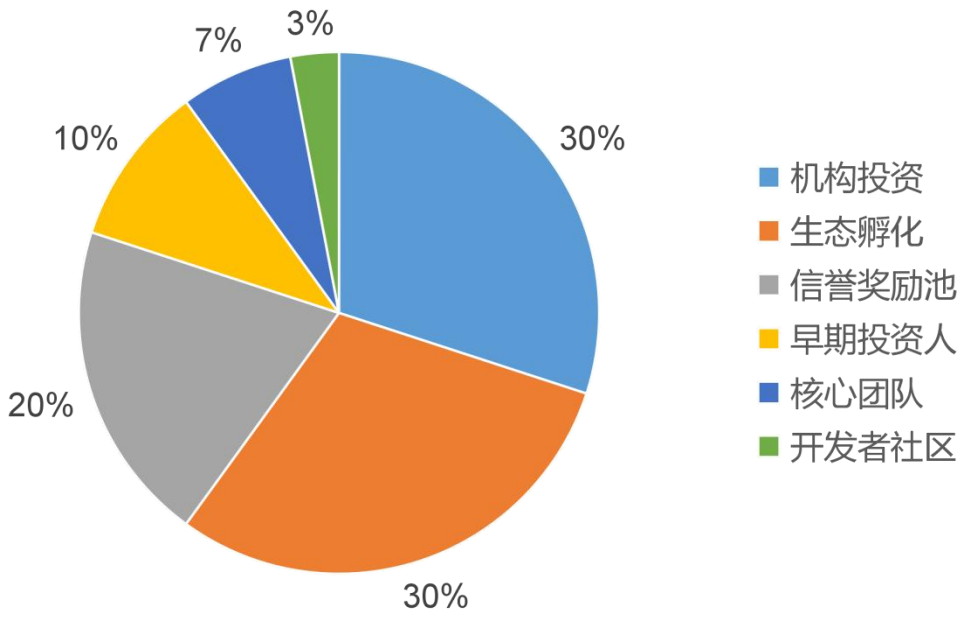
兼容以太坊智能合约Demo测试

第六章 经济模型

6.1 通证设计

贝克链主网运行的通证命名为BUS，寓意为像公共汽车一样可承载高通量的基础设施，表达了贝克链作为基础公链的社会责任感。贝克链共发行500亿枚BUS，并永不增发。在主网上线之前，将分配给投资者ERC20代币，并使用ERC20代币登录交易所。当主网上线时，将按1:1的比例映射成主网代币。

图13. Token分布图



- 30%：面向机构公开募资，首轮将释放一半，即总代币的15%。锁仓24个月，每月平均线性释放。
- 30%：用于社群建设和生态孵化。
- 20%：用于Bit-R高信誉用户奖励，其中60%给超级节点、40%高信誉用户。每年释放10%，逐年递减。
- 10%：早期（种子轮）投资人。锁仓4年，从第13个月至第48个月开始逐月线性释放
- 7%：奖励核心团队，锁仓4年，从第13个月至第48个月开始逐月线性释放
- 3%：奖励全球开发者社区

6.2 BUS通证的作用与职能

获得BUS通证的渠道主要由三种：（1）投资人购买，只针对机构；（2）二级市场购买；（3）高信誉用户参与记账及社区奖励。

BUS是贝克链运行过程中的重要通证，是Bit-R信誉体系的主要构成部分之一，承担系统激励和社群治理的重要作用。主要包括以下四种职能：

(1) 构建Bit-R贝克信誉。用户持有适量通证是构成Bit-R信誉值的一个维度，即：时间活跃度。即：持有适量BUS来提高信誉，高信誉获得算力收益。

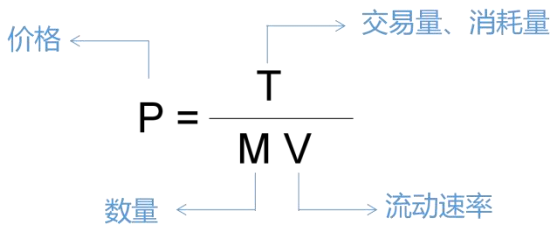
(2) 社群激励和开发者激励：高信誉用户被选为可信节点，通过贡献算力获得BUS通证奖励。

(3) 交易手续费。

(4) 开发者消耗。开发者将需要一定数量的BUS通证作为燃料，用于发布产品、运算、分布式应用等。

6.3 经济学模型

采用经典通证经济学模型，即以太坊创始人Vitalik Buterin根据区块链经济学优化过的费雪方程式进行BUS通证模型的分析和论证。



T：总交易量，总消耗量。T值越大，价格P越高。生态建设就是为了扩大BUS的使用场景，激发使用需求。海量的落地应用是促进BUS消耗和流通的终极动力。

M：通证数量。流通的通证数量减少，价格升高。

V：通证流动速率。流动速率越低，价格越高。

在贝克链的Bit-R信誉构建过程中，币时（Coinage）是构建时间活跃度的主要因素，用户需要持有一定时间的代币来构建或增加在该维度上的分数。因此，BUS的流通数量降低，流动速率V降低，有助于价格P升高。

对于BUS流动性分析：

中短期：用户购买BUS有明确的刚性需求，保有量高，流通量少。用户需要购买一定量的BUS并持有一段时间（币时）来获得Bit-R高信誉值，从而获得更多的系统奖励。高信誉用户拥有更多的权益，例如：低手续费、闪电网络无押金、被选为记账节点概率增加等。Bit-R贝克信誉的时间活跃度采用对数形式的币时参数，早期持币用户通过时间积累可以逐步释放部分BUS而同样保持较高的信誉分数，使新增用户可以有机会购买到逐步释放出的BUS。

中长期：大量的落地应用是促进BUS交易量和消耗量的终极动力。随着公链性能的不断完善和生态建设的不断推进，例如：当有1,000个DAPP运行在贝克链上时，开发者发布一个DAPP的费用是1,000BUS，则发布过程总共需要消耗100万BUS。

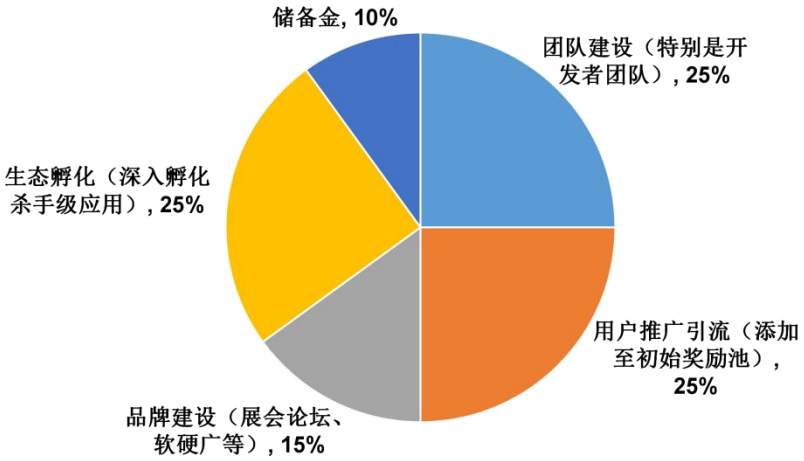
例如：平均一个应用日活人数为1,000人，每人每日平均需要使用100BUS，这些BUS可能用于用户交易量（用于支付、购物等）、DAPP运行费用、交易手续费、新增用户购币持有构建信誉等，则仅应用部分每年需要：1,000个应用×365天×1000人×100BUS=385亿BUS，占总代币数量的77%。此时，整个网络的日均活跃人数为50万，而一个杀手级应用的日均活跃人数通常在百万至上千万级。随着全网用户数的增加至数千万用户，甚至上亿用户时，BUS的流通量也将迅速增加。

6.4 融资计划

天使轮：0.01美元/BUS，拟募资7,500万美元，占总代币的15%。锁仓期为24个月，每月平均线性释放。

资金用途见图14.

图14. 资金用途



25% 用于团队建设，特别是开发者团队建设

25% 用于社群推广，例如增加至初始奖励池，强化早期的高信誉用户激励，促进快速形成社群共识。即：高信誉用户不仅可以获得BUS通证奖励，还可以获得额外的现金奖励（例如BTC、ETH、USDT等）

25% 用于生态孵化

15% 用于品牌建设

10% 作为储备金

第七章 免责声明

除非您本人已了解并认可贝克链项目的技术路线和应用场景，以及明白区块链行业的相关风险，否则不建议您参与公开兑换。数字货币是一类早期并且有风险的项目，参与兑换需要谨慎小心。一旦用BTC或ETH等参与兑换BUS，您原有的BTC或ETH等将不再退回！募集来的资金使用由贝克链团队决定。本项目有可能因政策、市场需求、技术或者其他不可控因素导致项目开发、推广或落地场景等环节失败，项目失败的最差后果可能导致投入的BTC或ETH无法收回，且BUS的收益或亏损都由兑换者自行承担。

附录：参考文献

1. Nick Szabo. Formalizing and securing relationships on public networks. First Monday, 2(9), 1997
2. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf. 2002
3. Vitalik Buterin. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. 2013
4. Gavin Wood. Ethereum: A Secure Decentralized Generalised Transaction Ledger. 2018
5. W. Dai, "b-money," http://www.weidai.com/bmoney.txt. 1998
6. Andreas Antonopoulos : Mastering Bitcoin: Unlocking Digital Cryptocurrencies. 2014
7. Sheldon M. Ross. A First Course in Probability. 2009
8. Nash John. "Non-Cooperative Games" The Annals of Mathematics. 1951
9. Schlegel, H.: Reputation Currencies. Institute of Customer Experience.
10. Marko Vukolić: The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. 2016
11. Adam Back, Matt Corallo : Enabling blockchain innovations with pegged sidechains
12. Vitalik Buterin : Zk-SNARKs: Under the Hood
13. Eli Ben-Sasson : Zerocash: Decentralized Anonymous Payments from Bitcoin
14. Petar Maymounkov : Kademlia: A Peer-to-Peer Information System Based on the XOR Metric
15. Everett Hildenbrandt : VM: A Complete Semantics of the Ethereum Virtual Machine
16. L. LamPoRt, Constructing digital signatures from a one-way function, Technical RePoRt SRI-CSL-98, SRI International Computer Science Laboratory, Oct. 1979.
17. "Winternitz one-time signature scheme" https://gist.github.com/karlgluck/8412807#comment-1258433

[Social Media]

Web: www.bitconch.io
Twitter: https://twitter.com/bitconch
Telegram: https://t.me/bitconchbustoken
Facebook: https://www.facebook.com/BitConchofficial
Reddit: https://www.reddit.com/r/BitConch/
Slack: https://bitconch.slack.com/messages
Github: github.com/bitconch/bus
Medium: medium.com/bitconch

[12万 TPS – MVP DEMO]

扫码即可观看视频