

全球最快落地的可信商业生态

BBR（商基链） 白皮书

WhitePaper

版本 1.0

2019 年 10 月 1 日

1. 概述
2. 当前商业生态
3. 商业社会信用的痛点
4. 区块链改变商业社会信用共识
5. BBR 的定位和愿景
6. BBR 促进商业生态发展
7. 生态应用
 - 7.1 工业大麻全生态应用
 - 7.2 可信任的游戏应用
 - 7.3 可信电商行业
 - 7.4 去中心化金融服务
 - 7.5 服务实体经济
8. 技术架构和关键技术
 - 8.1 多层可插拔架构
 - 8.2 Byzantine Fault Tolerance 共识算法
 - 8.3 模糊数据混合存储
 - 8.4 基于 cosmos 的 Flight 跨链架构
 - 8.5 Super BBR Protocol 超协议
9. 商业应用逻辑
 - 9.1 商业生态
 - 9.2 去中心化商业信用评价体系
 - 9.3 电商平台商信评分体系（举例）

10. 社群生态

11. 代币发行方案

12. 风险提示

12.1 司法监管相关的风险

12.2 BBR 技术应用风险

12.3 BBR 应用缺少关注度的风险

12.4 黑客或盗窃的风险

12.5 漏洞或密码学科突飞猛进发展的风险

12.6 缺少维护或使用的风险

12.7 未保险损失的风险

12.8 应用存在的故障风险

12.9 无法预料的其它风险

1. 概述

信用是市场经济发展的基石。经济的飞速发展是以社会诚信作为依托，社会信用体系是维持市场经济秩序，保障商业社会可持续发展的关键。从日常购物，娱乐消费，理财投资，到法律规章，信用两字渗透到生活的方方面面。然而，由于信息不对称，人为违约等行为，造成了信用崩塌事件，造成经济上千亿级的亏损，最为典型的的就是 P2P 等持续崩盘事件。整个社会对信用生态的渴望达到了极端迫切的地步。但是，依赖“人治”确定“信任”并非长久之计，有必要依托于去中心化的技术，对人群的行为进行更为精准的评估和约束。

区块链是信任的机器。非对称密码、哈希算法、去中心化、共识机制融合下的区块链技术具有数据不可篡改、安全可靠特性，能够彻底实现信任机制，催生更多的组织生态、商业生态变革。

BBR (Business Block Reveal, 中文名：商基链) 旨在打造一个基于区块链技术的商业生态公链，通过可以度量的信用因数，实现商业生态的资产化，实现商业所有权与使用权的分离，依托人工智能、大数据分析、匿名隐私保护技术，打通商业孤岛，降低交易成本，构建平台、商家、消费者共赢的生态圈，达到商业组织重构。同时，BBR 通过 SDK 接口、零知识身份认证接口、基于 Cosmos 的 Flight 混合跨链技术提供区块链标准化服务，打造一站式商业生态接入方案，支持对接多商业超级结点，支持去中心化身份认证，打造全流程商业联盟，打破“信息孤岛”，实现商业实体链改。

我们欣喜的宣布，BBR 已经和加拿大合法工业大麻 Articles of Incorporation 和全球网红游戏开心豆游戏取得合作，Articles of Incorporation 和开心红豆游戏作为 BBR 第一批商业应用场。

当 Articles of Incorporation 纳入 BBR 生态后，将实现大麻商品的溯源，确保商品的真实性，保障用户的利益，系统对接完成后预计直接带来百万级优质用户流量。比如用户通过 BBR 系统将能直接使用虚拟化产品，从种子到种植、到销售全程可溯源，直接共享大麻的财富密码。

未来，BBR 将打造成全球最可靠的可信商用服务平台，帮助各大商家平台、移动商场、实体商店实现链改，覆盖电商平台、区块链手机、去中心化综合征信体系、去中心金融等更多应用场景，共享区块链技术，一站式解决企业“信任度低、粘性差、留存率与复购率低”等运营难题。

2. 当前商业生态

随着市场经济的蓬勃发展，为了提升商业资本循环的效率，个人的商业信用往往被企业和机构当作一个提供产品或服务的重要考量。信用卡就是一个充分利用信用的典型案例，根据个人的消费记录、还款情况，银行或信用卡公司提供额度贷款。这里，我们看到，商业信

用在整合个人或企业的资金管理，提高资金利用管理，节约成本，加速商品流通方面发挥着巨大的作用。

在信用管理方面，从银行信贷到电商平台，从工业大麻、从游戏平台、从移动支付到共享经济，信用作为个人的资产，在消费领域起着关键的作用。随着认知和科技的进步，通过进一步挖掘包括行为在内的商业信用价值，才有可能激励个人和企业的守信之举。

个人凭借自己的良好的信用，可以获得生活的诸多便利，比如利用支付宝的芝麻信用积分免抵押租借单车，充电宝，也可以用京东白条进行借款用作资金周转。作为个人，逐渐意识到守信带来的好处，而公司和机构，也将个人信用作为提供服务的重要审核要素。然而，传统的信用评价体系，只存在钱的标准，例如还款记录等作为信用评价维度过于单一，机构和企业逐渐考虑以个人综合记录作为更为广泛的数据源，丰富的使用场景，高频的行为记录，能有效而全面地反应个人的信用情况，有助于提供服务的企业和机构作出合理的决策。然而，对于庞大的个人消费数据的记录，存储和分析，对数据真实性的保障，要求强大的技术平台作为支撑。

3. 商业社会信用的痛点

通过推动商业社会信用，能提升商业运作的精准度，简化沟通流程，在极大程度上，降低企业运作的风险和成本，有助于提升利润和规模，也能够为个人提供良好的生活和工作体验。但商业信用体系，面临着以下几个主要难点：

一是中心化的网络结构下，难以保障个人信息的安全。个人信息散落在商业流通的各个环节。二是数据共享。各大企业和机构出于利益考量，以及保护用户隐私的考虑，并不乐意分享用户数据。三是信用系统重复建设，各个系统各自为政。四是欧盟 GDPR 隐私保护给区块链系统带来挑战。我们以具体的案例来说明商业信用的这些痛点。五是通过商业行为数据来更好的保护知识产权的利益，让价值获取的过程也融入综合信用体系，提升全面的评判标准。

比如大麻相关产业的监管是一项较为复杂的行为，其通常涉及多个部门的联合执法，以美国联邦层面的大麻的监管为例，其通常涉及以下三个部门：

- 联邦药品执法局（Federal Drug Enforcement Administration, 下简称 DEA ）
- 农业部（Department of Agriculture, 下简称 DoA ）
- 美国食品药品监督管理局（U.S. Food and Drug Administration, 下简称 F.D.A. ）

当前每个执法部门都耗费大量的精力来处理流程问题，但是工作量巨大，效果不佳。

此外，受高利润驱使，非法大麻交易行业一直有增无减，每年在美墨边境缉获 1000 多吨非法大麻，市场上大部分的大麻交易都没有从源头到顾客的适当追踪数据，这也限制了相关产业的合理发展。

4. 区块链改变商业社会信用共识

区块链主要是解决信息不对称的问题，降低信任成本，提高交易效率，是一个改善生产关系的工具，而生产关系又是反作用于生产力的。区块链与实体经济结合，会为社会带来庞大经济效益，产生颠覆性的改变。各大企业和机构纷纷采用区块链技术，采集信用相关的数据，做到个人信用数据确权。在得到用户的授权后，机构或企业可以进行加密分享，促进个人信息在各渠道和平台之间的流通，以最大化其商业价值。

以上的案例表明，用区块链技术来解决商业信用问题已成为共识。未来在大厂的全力布局推动下，区块链技术潮流已不可逆转，区块链技术一定能够颠覆世界，未来全球每个人都将受益于分布式点对点、不可篡改、智能合约技术，未来哪个行业将诞生落地大应用，解决商业信用问题，将万众瞩目。

5. BBR 的定位和愿景

BBR (Business Block Reveal) 旨在打造最快落地的全球可信商业生态体系，建立经济领域里去中心化的自治管理和发展组织结构。充分利用区块链技术的去中心化、不可篡改及公平公正，重塑用户价值体系，再造领域的新业态价值。

BBR 团队认为，区块链是未来的大趋势，但是在通往未来的道理上，仍然有很多问题亟待突破，由于缺乏群众基础，成本过高、技术扩展性不足等诸多原因，区块链技术在全民推广还存在一定的困难。

因此，应该从日常、高频的生活场景入手，打造最快落地的可信商业生态。

基于如上判断，BBR 团队认为区块链技术发展应该是循序渐进，迭代发展的。为此，BBR 制定了两个 3 年发展愿景。

（1）2019 年至 2021 年，BBR 打造优先接入与普通民众息息相关的应用场景。

BBR 认为区块链应该首先在普通民众推广，让更多的人认识享受区块链、大数据分析、机器学习、万物互联时代带来的红利，因此在第一个三年计划中，BBR 将优先布局以下高流量用户领域：

- 自主的区块链游戏平台，如红色小豆、特种植物资产；
- 区块链特种植物产品可追溯供应链和金融服务平台；
- 可信商业平台，如“豆在” (DOUZAI) 未来商业平台；
- 去中心化社区，如全球的城市合伙人，品牌加盟商；
- 个性化营销平台，如基于用户端的广告共享模式；

上述应用场景能够带来较大的用户流量，同时上述应用场景的商业模式对信用高度依赖，因此 BBR 优先在这些市场布局有利于快速占领市场，带来庞大的流量市场，为 BBR 的技术架构提供技术验证，也有利于 BBR 技术的迭代发展。

（2）2022 年到 2024 年，建设下一代新零售诚信体系。

在越来越多的应用成熟后，BBR 将以区块链 BaaS 云平台、大数据行为分析、机器学习为依托，建成面向用户、面向服务的普惠链态生态圈，任何企业、商家、开发者都能以零编程、可插拔、可配置的

方式，通过简单的参数配置即能实现业务链改，共享上品生态服务，从而实现共享、共治、共献普惠链态目标。

BBR 具体方案如下：

2022-2023 年，“豆在” (DOUZAI) 商业平台 APP 3. x 版本上线，线上平台引入 AR+MR 虚拟现实场景，启动 BBR 积分诚信体系计划，启动独立公链，确立技术标准及发行计划；

2023-2024 年，全面开放线上商业运营品类及产品，建立独立完整的区块链底层技术研发机构或公司，完善基于 aboo 商业的 BBR 积分诚信评价体系，建立以商业及服务业为主体结构的代币交易中心，形成完整生态体系。适机上线孵化更多的独立跨链公链生态，完成商业闭环。

6. BBR 促进商业生态发展

BBR 利用区块链的技术挖掘个人信用商业领域的价值，实现个人信用的数字化，进行个人数据的确权和分权，打通了商业数据的孤岛，降低交易和沟通成本，构建了全新的零售诚信体系。

BBR 以其在性能、吞吐率、安全性、扩展性、易用性等方面的卓越表现，为个人信用领域数据的采集和流通提供了有力的基础设施技术支持，可以应用在生活的各个领域。

（1）商业信用链改的一站式解决方案。

通过提供高性能的基础公链，快速提供链改支持，让现有的商场和店家快速接入服务。BBR 通过记录和分析用户的日常消费和娱乐习

惯，多维度量化用户消费需求和信用，共享给所有接入 BBR 的平台、商家，打破了渠道间的隔阂。

各平台和商家无需耗费精力重新开发，即可共享区块链技术，通过商业信用体系，解决信用度低，用户粘性差，留存率低，复购率低的问题，充分了解用户需求，调整供应链各个环节，多样化营销手段，从而取得规模和利润的较大增速。

（2）用户的数据隐私和安全保障。

不同于现有互联网盗取用户信息的劣迹，BBR 采用零知识加密算法、格量子密码，生成密钥保证数据加密过程的安全性，有效进行隐私信息的隔离。在去中心化网络结构下，BBR 可以有效地增强和抵御黑客的攻击，最大程度保护商户和用户信息。

由于区块链去中心化的属性，商户的信息和用户的信息均真实可信，不可篡改，商户和用户行为更加透明化。比如，商户的采购信息完全记录在链，未来还包括引用北斗卫星定位的唯一性地理数据记录，避免“假冒伪劣”产品混充其中，商品的物流信息全部上链，可以避免快递诈骗事件产生，避免用户的经济损失。

（3）安全可靠的新零售诚信体系。

在 BBR 出现之前，各个游戏平台，电商平台，金融机构均各自为阵，碍于技术和利益的原因，掌握用户的部分数据却不愿共享，甚至相互设置流通障碍，造成了诸多信息不对称的情况出现，影响商家正常运转，有悖于互联网的商业本质。

BBR 的出现，以强大的区块链技术作为支持，保护了各参与方的数据存储，确保了数据的真实性，在获得授权的情况下，能保证数据的流通，形成了全面，完善的消费信用的生态。商家和个人的信用，真正地被当作资产，投入流通并使用，特别是包含不可篡改的商业行为数据记录，这对整个消费领域，特别是金融消费领域，有着不可估量的作用。

7. 生态应用

7.1 工业大麻全生态应用

在传统概念中，大麻是违禁药物，让人避之不及。然而，事实并非如此，随着近几年，工业大麻的价值被逐步挖掘，该行业得到该有的“正视”。中国的古人对其早有发掘应用，称“汉麻”。

工业大麻提取物大麻二酚（CBD）有显著的药用价值，在医学上可以用来辅助治疗某些疾病或晚期绝症（癌症、艾滋病），用以增进食欲、减轻疼痛等；工业大麻还有巨大的经济价值，其茎皮纤维长而坚韧，可用以纺线织麻布制作成纺织品，编制绳索，在制造业得以广泛应用。随着大麻二酚（CBD）在食品、化妆品、医疗多个领域的价值被挖掘，越来越多国家宣布工业大麻合法。截至 2019 年 1 月，全球有 41 个国家宣布医疗用大麻合法。合法化进程、大麻素应用的拓宽促进行业高速增长。根据相关数据显示，2018 年全球大麻合法市场约 120 亿美元；至 2025 年，合法产品市场规模将达到 1660 亿美元。大麻素 CBD 需求提升，未来两年增速有望接近 80%。

2019 年，在工业大麻合法化下的巨大市场规模推动下，工业大麻概念股一路暴涨，可见市场对其市场前景的看好。BBR 紧抓工业大麻的风口，积极开展工业大麻的线下种植。2019 年 5 月，BBR 线下种植基地开始建立，在中国山东及湖北两地共开发 1660 亩种植园区，种植包括特种粮油类、食药类等高价值，长期收益的作物，并积极展开与中国一流药用科学研究学院及国家重点生物研究实体战略合作关系，共同建设位于中国云南省腾冲市占地面积 95 亩的生物科研生产基地，还有千亩的药用植物种植园区，2020 年 3 月前生产研发主体园区的落成，5 月份完成设备生产运行，主要生产与 5 大类高附加值食药用途植物中相关有效成分的提取，并制造系列产品。

受限政策、地域、技术限制，普通投资者无法直接参与工业大麻的行业中，必然错过行业财富机遇。然而，BBR 借力于区块链技术，让普通投资者可以参与工业大麻等相关高级药用植物的种植和商用财富分享中去，享受由特殊高附加值行业带来的巨额收益。

除了以上工业大麻（CBD）的提取物及相关产品，我们的生物领域产品还包括：

- 东革阿里提取物，宽缨酮（Eurycomanone），提高自身免疫力，增强综合体质，避免人体自我生长激素流失；
- 红豆杉提取物，紫杉醇（Taxol），抵抗癌细胞，祛除带病毒素；
- 银杏叶提取物，银杏内脂（GBE），预防治疗中风，增强循环系统活力，治疗肺虚咳喘，高脂血症；
- 白藜芦醇（Res），抗氧化，增加心血管活力，延长寿命；

- 腊梅提取物，芳香精油 (Ethereal oils)，纯天然香味剂，高级化妆品必要成份；

投资者使用 BBR 投资特种食药产业的财富机遇中，将有以下几点优势：

- 1) BBR 具有区块链溯源的特性，投资者能够追溯产品诞生的全过程，实时透明地了解的生产状态；
- 2) 投资者可以通过 BBR 进行智能结算，排除人为干预，获得相应的投资回报；
- 3) 投资者隐私得到全方位保护。BBR 采用专业加密算法，生成密钥保证数据加密过程的安全性，有效进行隐私信息的隔离；
- 4) BBR 独一无二地域优势和行业紧密的合作关系，例如能够确保并提升工业大麻相关产品的直接产能。

BBR 作为一个平台，将实体经济与数字经济完美融合，达到了服务所有普通投资者和消费者的目的，充分利用各地资源优势和技术优势，打造出全新的生产，零售一体化的平台，大有颠覆现有电商之势。BBR 以工业大麻为突破口，吸引全球有识之士，汇聚 BBR 平台，创造惊人财富。

7.2 可信任的游戏应用

BBR 是以开心红小豆的游戏为切入点，借助其现成的流量，在欢乐有趣的氛围中，向年轻并乐于接受新事物的用户，传播和推

广新型的商业模式，用户将种植过程满足碎片时间的粘性。BBR 利用区块链技术打造全新的商业模式，相比传统的游戏，规则更为公开、透明，游戏更为有趣、有利，营销推广更为丰富、有效。BBR 的这种新型的游戏商业模式，具有极强的可复制性，可以从开心红小豆，拓展至更大的游戏生态中去。

通过将农场+商城+娱乐+文化的界面功能组合，BBR 将建立一个完整的初级生态，满足更多人对于生活=收获=欢乐的理想生存预期。每个人都能有自己的土地，每个人都希望土地更能体现充分的个性化，独特的商业化。未来可以更多的选择自己土地上的展示内容，包括视觉内容、商业内容、文化内容等，可以将自己所擅长的生活方式和经营方式都在此处逐步实现。

眼下，全球有超过 10 亿的基于手机端的网络游戏玩家，仅国内的有效数量就超过 4 亿，而最热门的区块链项目仅几百万，游戏领域显然是个巨大的流量池。对于游戏用户而言，其迫切需要一个以新技术为基础，保障个人隐私和权益，有情节体验，有价值收益，更有公平的原则，包含着社交和商业基因的新平台。然而，传统的游戏行业，抽水，舞弊的丑闻不断，打击了普通玩家的信心，而 BBR 平台在保护玩家隐私和权益的同时，满足其日益升级的娱乐需求，并且能给予其相应的游戏收益，对玩家而言，无疑是一个极具吸引力的平台。

让游戏和区块链项目之间产生碰撞，是最有可能出现从量变到质变的价值跃升，BBR 充分利用这两个行业的同向性和平行性

的特征关系，利用游戏大众性，娱乐性，门槛低，附加值高等特性，作为用户进入全新零售信用体系的入口，休闲类游戏是再明智不过的选择。

在游戏中，BBR 可以多维度评估用户个人偏好和消费数据，充分发挥通过社交基因而形成的数据潜力，还可以形成以下的产品反馈及功能：

- 在社交网络中针对社区圈子的识别；
- 基于好友关系为用户推荐商品或内容；
- 社交网络中个体人物影响力的计算；
- 热点信息在社交网络上的传播模型；
- 针对虚假信息和机器人账号的识别；
- 基于社交网络信息对于币值的预测；
- 借鉴互联网金融行业中的反欺诈模型。

玩家们不仅在游戏中得到愉悦，还可以参与到游戏的分发和推广中，从而获得 BBR 奖励。游戏项目方也可以在 BBR 平台上，进行宣发，如举办游戏大赛，或购买广告位等吸引新玩家。得益于 BBR 的区块链技术，游戏和推广数据不可篡改，智能结算，保障了商家和玩家的权益，重新定义了游戏行业的商业模式，BBR 帮助游戏行业打造了新型的信用体系，有助于良性游戏生态的建成。

7.3 可信的新电商模式

以开心红小豆的游戏为流量入口，BBR 已经上线了 aboo 自有品牌商城，打造包括线上电子商城和数字货币支付于一体的综合性平台。aboo 是利用区块链技术链接实体行业的电商品牌，以消费者信用为基础，形成良性的信用商业体系。

在 aboo 品牌的系列产品中，BBR 针对电商模式进行了以下调整：

- 数据上链：BBR 将所有商品数据上链，使 aboo 的商品具有数字资产属性，使所有数据真实可追溯，有效存储不篡改；
- 供应链管理：建立在 BBR 上的线上商城，将可以实现所有商品的溯源，确保产品的真实性，保障用户的利益，如果 aboo 出现产品问题，通过 BBR 浏览器可以在几秒内查询跟踪到问题所在，未来还将增加基于北斗地理信息系统功能的机制；
- 广告分成：如今互联网广告打开率非常极低，不少事以影响消费者的体验作为代价，BBR 会采用精准的数据分析方式，将更有针对性的数据结果反馈给各类商家和用户，进行有效的广告推送，而消费者可以用过点击广告获得激励，从而形成积极的观看体验。这样一来，商家可以降低传播成本的同时，可以大幅降低广告传播的有效性成本、最大化的满足真实性；
- 去中心化信用：通过记录和分析用户的日常消费行为，为用户建立商业信用体系。购物信用良好的用户，可以受到更高效的服务，更多的福利和权益。由于用户所有的消费都记录在链，可以防止违规刷单交易虚假排名，以及恶意差评人员讹诈行为，从而减少商家的损失，维护商家的正当权益。

目前，aboo 品牌商城已上线健食类，饮品类，粮油类和医药类等自有品牌产品，据悉，在 2019 年 12 月前，aboo 品牌即将上线更完整的应用，用全新的零售体验让大众用户得到全新的消费体验，并上线基于平台的商业共享广告产品，同样服务于广大的商户、品牌和消费者。未来商家可以通过持有相应的 BBR 入驻平台进行产品销售，未来消费者也可以将自身的信用变成有效资产，获得 BBR 奖励等，为逐步建立全球可信的商业生态提供落地案例。

7.4 去中心化金融服务

因为 BBR 收集了海量消费者的数据，建立了更趋于完善的信用评估体系，金融机构也可以通过接入平台，获得有价值的信息。

通过接入 BBR 平台，各银行或信贷机构可以把各自用户的数据保存在各自的数据库，把部分摘要提交区块链保存，又查询需求可以追溯到原始提供方，以此保护了自己用户的核心数据，又可分享外部用户的海量数据。

比如，银行可以通过 BBR，查看经营者和借贷人的商业信用积分，更有效评估借贷人的行为本质和还款能力，或是了解借贷人在其他银行的借贷情况，评估借贷人的风险指数，提供贷款方案。BBR 的存在有效避免信贷用户多头负债的情况，降低了其中数据交易成本，组织协作成本和行业监督成本。对于保护知识产权和发展良性商业价值更起到了原有网络信用体系所无法满足的需求。

7.5 服务实体经济

通过接入 BBR，企业和机构可以了解到个人的信用评级，并且通过评级了解个人的信用水平，这些信息同样可以应用于实体经济，如二手房市场的买卖。在二手房市场，通过评估买卖双方的信用，可以降低交易的风险，降低交易成本，也可以链上查询房产信息，了解房产购买历史，避免交易雷区和陷阱。

比如，BBR 记录房产信息，可以做到房产确权，在交易的过程中，若经过身份验证的卖家一旦付款，网络进行多节点确认，房屋产权进行自动移交，不由第三方的意志进行篡改。这样可以有效避免除产权人意外的个人，无论是进行房屋售卖还是租赁，都可以避免一套房产进行重复交易，包括根除黑中介，消除欺诈行为。

在经济和数据全球化的今天，如果大数据只存在大企业手中，那么全球市场的信用体系建立是并不能去中心化的，因为互联网公司形成了内在的价值转移闭环，而区块链的出现，可以让所有加密数据可以直接链上交易。BBR 还可以打破行业龙头垄断用户数据的情况，打破企业之间的壁垒，将用户数据分享给小微企业和相关行业参考使用，有助于商业生态更为蓬勃的发展，有助于旅行社，共享服务类公司，小微金融机构等快速壮大。

8. 技术架构和关键技术

8.1 多层可插拔架构

BBR 系统架构采用分层设计，分为协议层、交易层、AI 层、接口层和应用层，层与层之间有严格的逻辑接口，保证了调用安全性。其中智能合约、共识机制和 **Byzantine Fault Tolerance** 加密算法属于区块链底层协议；交易撮合等属于交易层；AI 层提供深度学习、学习预测模型；用户层面向用户，提供电商、内容、游戏、社交等各管理模块；接口层提供标准化、参数化的 SDK 接口。

8.2 Byzantine Fault Tolerance 共识算法

区块链核心块链层最重要的是共识算法。针对大流量、物联网和大数据的特性，BBR 采用拜占庭容错（Byzantine Fault Tolerance，简称 BFT）和 PoS 结合的共识机制。BBR 面向未来科技的应用，需要融合人工智能、大数据等先进技术，其对系统的可靠性要求极高，因此 BBR 选择了容错性较好的 BTF 算法。

BFT 容错能给分布式网络带来了较好的可靠性，能够提升交易速度，缩短区块验证速度，避免区块链分叉问题，并带来一定程度的交易的最终确定性，间接的提高了性能。如果说纯 PoS 比起纯 PoW，仅仅是解决了能源消耗，那么 BFT + PoS 比起纯 PoS，那就是除了解决能源消耗外，还解决了 PoW 的交易确认，交易分叉，性能较低等问题，带来质的变化。

为了更好的解释块生产的算法，我们假设有 3 个块生产者，A，B 和 C，这是因为我们的共识算法需要 $2/3 + 1$ 的投票来解决所有情况，这个简化模型将假设块生产者 C 为打破平局的那个生产者。在现实世

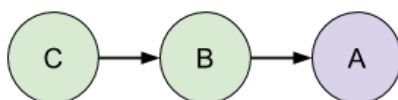
界中，将有 21 个或更多块生产者。就像 POW 算法一样，我们定义共识算法的两个规则：

规则 1：块生产者的数量 N 为奇数

规则 2：最长链为有效链

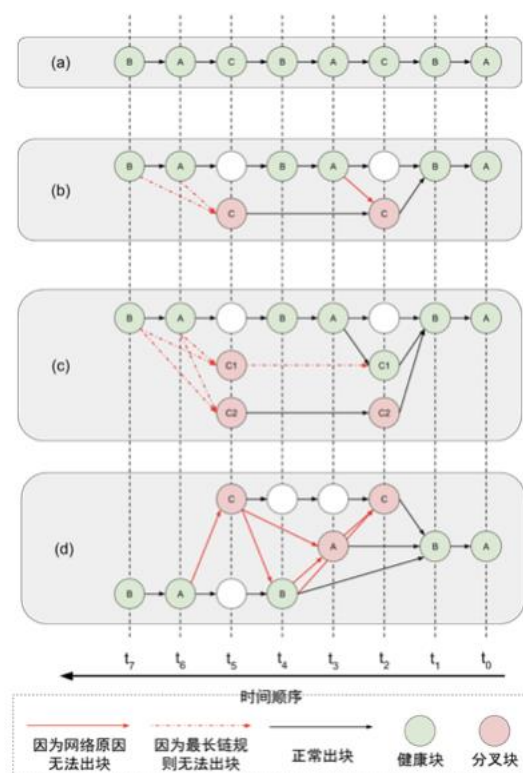
即，当一个正常运行的块生产者发现一个有效的更长的链，它就会认为当前链为分叉链，接着从当前的分叉链切换到该更长的链上。我们将通过下图展示 DPOS 如何在各种网络条件下运行，逐渐阐述共识算法的规则，并证明 DPOS 的强大和难以破解的特性。

在网络分区的情况下，多个链分叉的情况可能会持续很长时间。但从长时间来看，最长的链将获胜，但我们需要一种方法来确定在哪个时刻一个区块绝对是增长最快的链的一部分，即被确认。这可以通过查询连续 $2/3 + 1$ 的块生产者的确认来确定。



图：A 区块被 B 和 C 区块连续确认

在上图中，A 区块已连续被 B 和 C 确认，因此我们可以推断，如果 2/3 的生产者是诚实可信的，那么不可能存在其他更长的分叉，即 A 区块被确认。



8.3 模糊数据混合存储

随着 5G 普及而进入万物互联时代，海量数据存储需求是 BBR 必需满足的基础。BBR 使用的是 IPFS 技术，但是 IPFS 在隐私保护、支持海量并发存储和可靠性方面仍有提高地方。为此，BBR 专门设计了存储层，负责统一处理 IPFS 与应用层的交互。

存储层除了满足对 IPFS 请求外，还增加了自主研发的加密去重、存储缓存等功能。BBR 利用非对称加密和零知识证明技术，研发了一套文件加密去重技术。利用零知识验证方法，基于多次哈希运算，实

现了密钥与分片文件分离、完整性验证、不使用第三方传递密钥等功能，解决了 收敛加密对重复数据的加密开销等问题。即使是不同的用户同时存储相同文件，整个网络也只需要保存一份加密后的内容拷贝，而不用担心内容和隐私泄露，从而提升整个网络的存储效率。

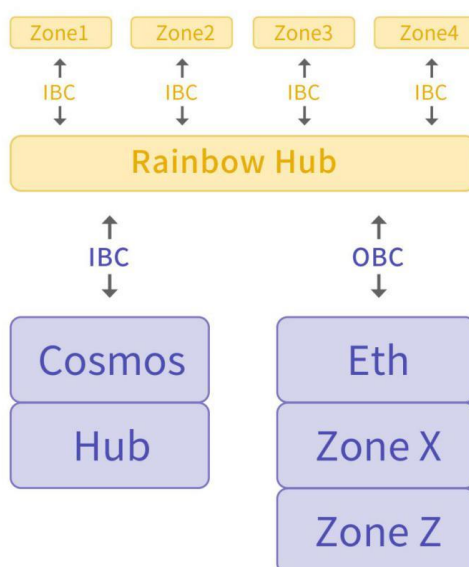
BBR 对待存储数据进行预处理，即将数据文件分割成多个碎片，并将其存放在不同的节点上。每个节点只需处理一小部分传入的交易，并且通过与网络上的其他节点并行处理，就能完成大量的验证工作。

在 BBR 网络中，分块技术具有多层含义：在超级节点网络中，利用分片技术提升 TPS 和智能合约执行速度；在边缘节点网络中，通过将计算密集型和存储密集型任务进行分片，提高整个网络的计算能力和存储能力。

具体步骤为：

- 1) BBR 使用一致性 HASH 技术将数据文件分片备份在 20 到 40 个不同的节点处；
- 2) 当客户端发现某个种子节点离线，客户端会将此切片复制到新的种子节点上，从而确保数据不会丢失；

3) BBR 还使用非对称和哈希函数来保护在线文件，文件存储前被划分为 64M、32M 或 8M 大小的数据分片，经加密后在网络上进行分散存储；



这种分片并分散的存储方式，在重组后可以更快地获得下载文件，但是第三方无法获取整个文件，从而确保了文件的隐私保密。

8.4 基于 cmosmos 的 Flight 跨链架构

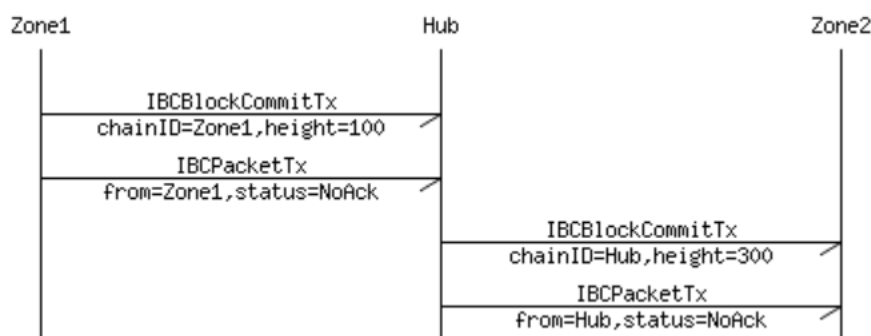
从跨链的核心架构来看，BBR Flight 使用了 Cmosmos 一样的跨链架构，BBR HUB 管理着特定的区块链 Zone，比如大麻供应链 Zone、溯源 Zone、红豆游戏 Zone、去中心化交易所 Zone。区块链 Zone 和 hub 之间通过 IBC 协议进行，通过发布 Merkle-proofs 作为信息被发送和接收的证据，将信息包从一个区域传送到另一个区域。这种机制称为区块链间通信，简称 IBC。

按照 Cosmos 架构，Hub 是一个区块链，它托管一个多资产分布式分类帐本，其中代币可以由个人用户或区域本身持有。Zone 是一个独立的区块链，可以与 Hub 交换 IBC 消息。从 Hub 的角度来看，区域是一个多资产动态成员的多签名账户，可以使用 IBC 数据包发送和接收令牌。与加密货币账户一样，它不能传输比它更多的令牌，但可以从拥有它们的其他人那里获得令牌。可以被指定为一个或多个令牌类型的“源”，从而赋予它扩充该令牌供应的能力。

8.5. Inter-blockchain Communication (IBC)

BBR Zone 的区块间通信，一般情况下采用 cosmos 一样的 IBC。IBC 协议使用两种类型的事务来定义：一个 `IBCBlockCommitTx` 事务，它允许区块链向任何观察者证明其最近的块哈希，以及一个 `IBCPacketTx` 事务，它允许区块链向任何观察者证明给定的数据包确实由发件人的应用程序通过 Merkle-proof 发布到最近的块哈希。

通过将 IBC 机制分成两个独立的事务，我们允许接收链的本地费用市场机制确定哪些数据包被提交（即确认），同时允许发送链完全自由地允许有多少出站数据包。



注：更多的细节请查阅 Cosmos 白皮书。

8.6 Super BBR Protocol 超协议

SuperBBR 是 BBR 中间平台层的核心程序，在形式上提供各种 SDK 供应用调用，为上层应用提供各类存储服务，包括至关重要的加密去重技术，去中心化静态持久存储、缓存服务、存储管理、跨链调度等管理功能，还包括账号管理、密钥管理等数据安全机制。

由于当前存在多种异构存储结构需求，有来自传统的存储系统，还有来自区块链的存储系统，SuperBBR 需要为各种存储系统提供 SDK 接口，比如我们会把 IPFS 集合进来，提供以下的接口层服务。

- 1) 作为一个挂载的全局文件系统，挂载在 /SuperBBR 和 /ipns 下；
- 2) 作为一个挂载的个人同步文件夹，自动的进行版本管理，发布，以及备份任何的写入。也即是说个人电脑出现了 C、E 盘符后，还会出现 SuperBBR 盘符；
- 3) 作为一个加密的文件或者数据共享系统；
- 4) 作为所有软件版本包管理者；
- 5) 作为虚拟机器的根文件系统；
- 6) 作为 VM 的启动文件系统（在管理程序下）；

- 7) 作为一个数据库：应用可以直接将数据写入 Merkle DAG 数据模型中，获取所有的版本，缓冲，以及 IPFS 提供的分配；
- 8) 作为一个 linked（和加密的）通信平台；
- 9) 作为一个为大文件的完整性检查 CDN（不使用 SSL 的情况下）；
- 10) 作为一个加密的 CDN；

通过 BBR 的 SuperBBR 协议，在总体设计框架中，我们还将实现传统云存储的管理支持。目前随着云计算的发展，云存储越来越受到很多区块链厂商的喜好和支持，一方面，云存储能够提供海量、安全、低成本的云存储服务，提供 99.999999999% 的数据可靠性。另一方面，云存储一般使用 RESTful API，可以在互联网任何位置存储和访问，容量和处理能力弹性扩展，多种存储类型供选择全面优化存储成本。

为了便于 SuperBBR 节点维护者方便进行存储数据的维护，SuperBBR 提供了基于云计算的存储服务，用户可以按量存储，弹性伸缩存储大小，降低维护成本与运维难度，也能够保证数据存储的安全性与稳定性。

9. 商业应用逻辑

9.1 商业生态

BBR 利用区块链技术建立完善的个人信用评分体系。其信任评分由去中心化的信任评分节点来计算，打造一个安全，透明的商业生态体系。BBR 根据不同的应用场景而具有不同的角色，以下以 aboo 商城为例，介绍其生态。

在 aboo 电商购物平台中，商业信用生态圈包括平台方、商家、用户、持币用户，而支付网络中所有的主体，都有信用评分。

平台方即拥有海量用户信用数据的公链 BBR，其将用户信用数字化，资产化，从而提供多种服务，例如：

- 1) 提供链改支持，上链服务，对接各大商场系统；
- 2) 提供通证支持；
- 3) 提供交易所、钱包、等服务；
- 4) 提供去中心化的社群等。

商家：可以接入 BBR 平台，共享区块链技术，完成币改链改，上链，实现商品溯源，了解用户消费习惯和信用等；

用户：正面的商业行为均可积分，用以换取更优质的服务，和更丰富的权益，比如高信用者可以参与团购等，可以票选优秀供应商等；

开发者：基于 BBR 开发去中心化的 SDK，并获得代币奖励；

整个完整的商业流程：用户注册之后，BBR 会根据用户的行为进行评分，确保参与者的真实性和可信度；其次，信用分值越高的用户，交易确认的速度会越快，享受的折扣会更高；信用分值高的用户可以成为生态内的仲裁员，对商家的决策进行建议，从而优化商家的服务，达到双赢的目的。信任体系可以充分激励商家和用户之间诚实沟通和交易，并对负面行为进行惩戒，让交易过程变得更为透明直观。如此融洽的交易氛围促使更多的商家和用户涌入，从而丰富了BBR 整体生态。

9.2 去中心化商业信用评价体系

为了更好得约束和激励生态系统中的各参与方（平台、商家和用户），系统设计了商业信用评价体系。在这个体系下，我们将设定不同的指标，并配给不同的权重，最终经过累计加权得到商信评分。

去中心化商信评分基本公式为：

$$\mathbf{H} = \sum_{k=0}^n \mathbf{h}_k \times \mathbf{r}_k$$

H 为商信评分，H_k 是各项一级指标所占的权重，R_k 是各项一级指标平均分。H 是与具体的应用相关的，其指标可以自定义，接入应用时需由运营人员通过 BAAS 进行参数配置，主要配置 H_k 和 R_k，两者可以进行调整变更，以便更好的评价消费者的品质需求。

9.3 电商平台商信评分体系（举例）

在电商平台应用中，权重包括代币余额、评论、交易笔数、交易累计金额、在线时间、赞赏、邀请注册等指标，指标和权重通过参数化分数进行配置。

所有指标和权重都通过节点共识，存储在商信主链上，永远不可篡改，并通过 BBR 上的浏览器可以全程跟踪，具备完全的去中心化。电商平台应用中，商信评分用户越高，其权限、挖矿收益越高，还可以分享分红、决策权、手续费减免等权益。

各参与方还可以通过以下方式获得去中心化信用分：

用户：对商品或者服务进行投票，同时评价网上商城的质量；

商家：为用户提供高品质的商品及服务；

商家平台：确保商城商品的质量符合国家要求甚至更高；

参与方的等级或者积分越高，其所占投票权重越大。商家平台或者商家销售的商品不达标，其积分将会减少。如果商家平台或者商家的信用分数小于 0，系统将自动终止其买卖商品的权利。

10. 社群生态

BBR 希望通过区块链技术和经济激励模型设计，建立一系列公开正的规则，让商业活动可以在无人干预和管理的情况下自主运行的 DAC 组织机构。

BBR基金会：负责资金募集，运营团队组建，负责资金管理、资金分配等，负责重大事务决策，负责社区生态建设；

运营团队：负责BBR技术系统的建设，负责日常运营，负责社区用户日常维护，负责主要业务的运营开展；

决策顾问委员会：基金会负责招募金融、技术、运营、国家政策、业务应用各个方面的专家，由其对基金会以及运营团队做出指导和建议；

社区代表委员会：设计章程规则，进行社区代表选举，对社区运营民主采集意见和建议，对重大方向性事务，进行民主表决。

11. 代币发行方案

BBR 作为流通于全球可信商业生态的代币，基于 ERC20, 总量恒定为 25 亿枚的 BBR。具体分配方案如下：

- 1) 分配 60%，计 15.0 亿枚用于挖矿、平台应用场景长期分配；
- 2) 分配 10%，计 2.5 亿枚用于私募及宣传推广成本；
- 3) 分配 10%，计 2.5 亿枚用于未来产品预留分配；
- 4) 分配 10%，计 2.5 亿枚用于加盟商户保证金沉淀；
- 5) 分配 10%，计 2.5 亿枚用于创始人团队奖励池；

BBR 有非常丰富的应用场景，对于消费者而言，可以用作购买商品，购买服务，理财投资等，对于商家而言，可以用做店铺入驻，商品溯源，分销推广，信用认证等，是促成全球可信商业生态体系建立

不可或缺的一部分，其价值会随着 BBR 生态的壮大得到进一步的体现。

12. 风险提示

12.1 司法监管相关的风险

区块链技术已经成为世界上各个主要国家的监管主要对象，如果监管主体施加影响则 BBR 可能受到其影响，例如法令限制使用，销售，电子通证诸如 BBR 有可能受到限制，阻碍甚至直接终止 BBR 应用的发展；

12.2 BBR 技术应用风险

目前来看，白皮书的应用还停留在概念验证阶段，实际 BBR 在开发和应用的过程中，可能会到技术的制约，比如 Cosmos 技术发展制约，甚至可能需要重新设计风险；

12.3 BBR 应用缺少关注度的风险

BBR 应用存在没有被大量个人或组织使用的可能性，这意味着公众没有足够的兴趣去开发和发展这些相关分布式应用，这样一种缺少兴趣的现象可能对 BBR 应用造成负面影响；

12.4 黑客或盗窃的风险

黑客或其它组织或国家均有以任何方法试图打断 BBR 功能的可能性，包括服务攻击，Sybil 攻击，游袭，恶意软件攻击或一致性攻击等；

12.5 漏洞风险或密码学科突飞猛进发展的风险

密码学的飞速发展或者科技的发展诸如量子计算机的发展，或将破解的风险带给加密通证和 BBR 平台，这可能导致 BBR 的丢失；

12.6 缺少维护或使用的风险

首先 BBR 不应该被当作一种投资，虽然 BBR 在一定的时间后可能会有一定的价值，但如果 BBR 缺少维护或使用的话，这种价值可能非常小。如果这种情况发生，则可能没有这个平台就没有后续的跟进者或少有跟进者，显然，这对 BBR 是非常不利的；

12.7 未保险损失的风险

不像银行账户或其它金融机构的账户，存储在 BBR 账户或以太坊网络上通常没有保险保障，任何情况下的损失，将不会有任何公开的个体组织为你的损失承保，但诸如 FDIC 或私人保险公司将会为购买者提供保障；

12.8 应用存在的故障风险

BBR 平台可能因各方面的原因故障，无法正常提供服务，严重时可能导致用户 BBR 链的丢失；

12.9 无法预料的其它风险

密码学通证是一种全新且未经测试的技术，除了本募集说明书内提及的风险外，此外还存在着一些 BBR 团队尚未提及或尚未预料到的风险，此外，其它风险也有可能突然出现或者以多种已经提及的风险的组合的方式出现。