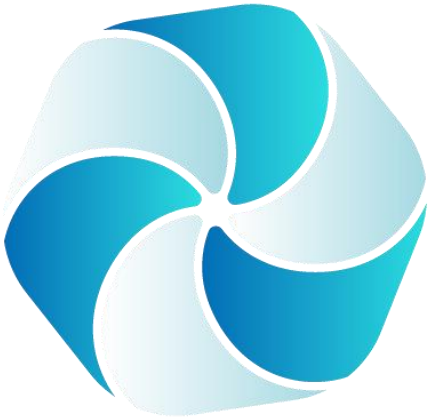


HPB 白皮书

HPB™ (High-performance Blockchain) White Paper

目录

1.项目背景

区块链技术经过几年的发展，逐步展现出其潜力，开始在一些领域落地。但是，作为一项新兴技术，仍存在诸多技术瓶颈。其中，易用性和 TPS(Transactions per Second)是制约目前区块链应用落地的重要原因。易用性制约了企业的开发进度，导致仍然没有一款杀手级的区块链应用出现。而对于需要高并发的业务，目前也没有区块链技术解决方案来满足。

社区的一些优秀代表都在积极推动区块链技术的发展，在各自领域深耕细作，取得了长足的进步。但受限于当前技术的发展状况，TPS 成为各个平台都面临的难题，TPS 3000 成为行业的共同的瓶颈，使得区块链在高价值的高并发业务领域无法落地。

综上所述，行业急需一个支撑 BAT 用户级别的海量高并发运用场景的区块链底层平台。HPB 应运而生，旨在解决这个行业瓶颈。HPB 将提供高频率访问需求的智能合约业务。它除了能够实现中心化服务器的用户体验，还会支持中心化服务器无法承载的千亿级终端的超大规模物联网场景。

HPB 希望能改变区块链无杀手级运用的尴尬境地，开创一个全新的区块链新生态，培育出真正能改变现实世界的区块链应用，成为真实商业区块链世界的基础设施。

2.设计理念

HPB 是一种全新的区块链体系架构，定位为易用的高性能区块链平台，旨在实现分布式应用的性能扩展，以满足现实世界的真实商业需求。这是通过创建一个可以构建应用程序的类似操作系统的架构来实现的。该体系架构提供帐户、身份与授权管理、策略管理、数据库、异步通信以及在数以千计的 CPU、FPGA 或群集上的程序调度。该区块链为一个全新的体系架构，通过低延时高并发硬件加速技术，可实现每秒支持数百万个交易，且达到秒级确认。

如图所示该体系架构定义包含两部分，硬件体系架构及与之配合的软件体系架构，是一个融合 HPC（High Performance Computing）及云计算概念的高性能区块链架构，硬件体系由具有 HPC 硬件支撑的分布式核心节点、通用通讯网络及具有 HPC 硬件支撑的云终端构成。

除了标准区块链软件体系架构下的核心节点上支持的网络管理、共识算法以及区块链任务处理功能，核心节点引入了与加速硬件匹配的软件加速引擎，通过 TOE 技术、共识算法加速、数据压缩、数据加密等技术实现支持每秒百万级用户接入。 该架构下的云终端可以是传统的 PC、智能终端等，同时可以是具备硬件加速特性的终端设备。

3.技术架构

3.1 技术特性

要成为一个成功的区块链高性能区块链平台，需要满足以下几个特性。

3.1.1 开源

从软件产业的发展历史看，成功的大型软件基本都采取开源模式。开源能吸引更多优秀的开发者加入，促进软件快速的升级迭代。从商业上来讲，用户不必为了使用软件而付出费用，免费使用的软件自然可能会得到更多的关注和使用度。对使用软件的公司来讲，开源降低成本，把有限资源投入到服务用户上，有了足够的用户规模,开发者和企业可以创建对应的盈利模式，公司的成功会有更多资源来提升开源软件的性能。

3.1.2 支持亿级日活用户

如 Google、Uber、Facebook、BAT 这样的应用，需要能够处理数亿日活跃用户的区块链技术，因此可以处理大量用户数据的平台至关重要。

3.1.3 低延迟

秒级的确认时间。及时的反馈是良好用户体验的基础。延迟时间如果超过了几秒钟,会大大影响用户体验，甚至压根无法胜任商业需求,严重降低应用的竞争力。

3.1.4 高吞吐、高并发

由于像交易所应用程序场景无法并行而只能串行执行，HPB 需要提供强大的串行能力。

对于其他场景，我们将提供强大的并行处理能力，将大部分任务并行化，通过软硬件结合的架构，让区块链的 TPS 提升 2 个以上数量级。

HPB 采用 TOE 技术，该技术旨在通过专用网卡上专用处理器来完成一些或所有数据包的处理任务。也就是说，通过采用配有 TOE 芯片的专用网卡，包括 TCP 在内的四层处理请示都可以从主机处理器转移到硬件加速卡上，其最终的结果就是在加速网络响应、并发能力增强同时降低服务器复杂度，提高节点处理性能。

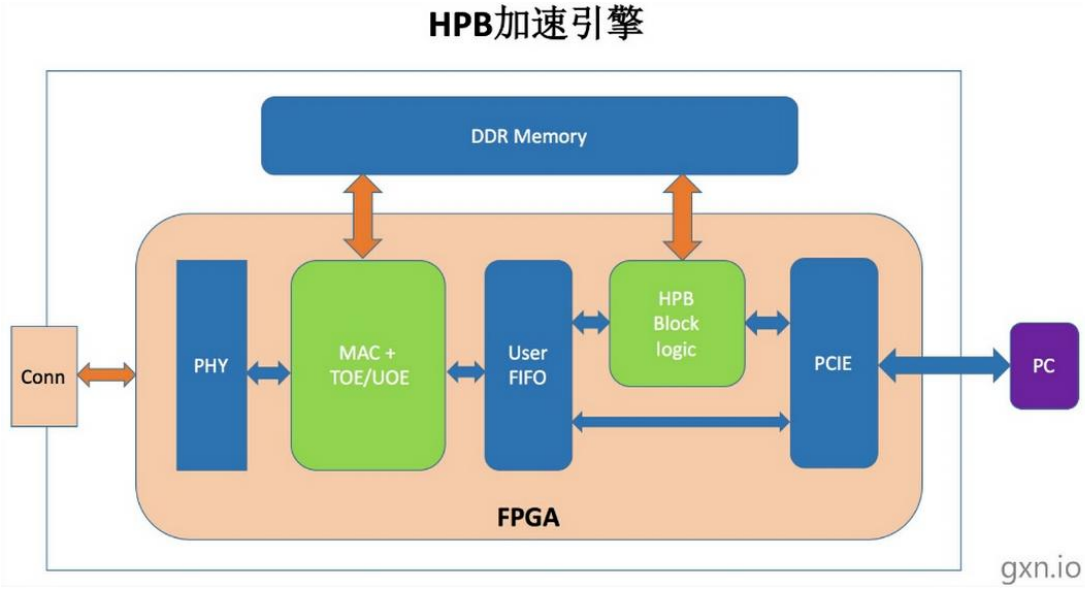
3.1.5 HPB 加速引擎

传统区块链的节点，交易任务、交易确认等功能均基于软件层面来实现，无论是在任务广播，还是交易确认，确认信息发布，每个节点之间的数据连接均是串行处理，导致了网络层次结构复杂、延迟时间长、串行处理性能低等用户体验的问题。

因此 HPB 设计了专用的区块链硬件加速单元(包括加速硬件及加速硬件固件)以及与之匹配的软件引擎（硬件加速系统层驱动以及上层软件接口 API），可以通过结合 CPU 串行能力和 FPGA、GPU、ASIC 等芯片的并行处理能力，实现高性能和高并发计算加速。

硬件加速引擎可实现大并发连接，并同时维持支持超过 10000 条 TCP 会话，可并行处理 10000 条会话，大大降低了网络层级数，专用并行处理硬件将接管由传统软件串行处理功能,例如交易数据广播、未验证 Block 全网广播、交易确认广播等。其对会话的响应速度以及会话维护数量均是普通 PC 节点处理性能的 100 倍以上。

HPB 硬件加速引擎系统架构和流程描述如下：



1、系统初始化，硬件系统获取全网配置表项，建立会话，并维持会话可靠。

2、任意节点用户端软件发起交易请求，通过加速硬件向全网并行广播发送附有签名的信息，同时开始监控全网确认状况。

3、随机指定节点（通过 DPOS 算法选举出来的区块生成者）收到带有签名信息的交易后，打包形成未确认 Block,通过加速硬件全网广播。

4、全网各节点 HPB 硬件进行 Block 确认，并广播确认结果。

5、任意节点收到约定的 k 个 Block 确认消息。

6、达成共识并发布完整 Block。全网广播完整 Block，各节点更新各自账本。

HPB 硬件加速引擎，因为可以与很多节点维持大量会话，因此可以不用等到完整 Block 发布，即可通过自行统计交易确认数，从而提前向用户反馈交易确认信息，改善用户体验。

3.2 共识算法(DPOS)

HPB 架构中采用目前为止唯一能够符合上述性能要求的区块链共识算法(DPOS)。根据这种算法,全网持有代币的人可以通过投票系统来选择区块生产者,一旦当选任何人都可以参与区块的生产。

HPB 里预计每 3 秒生产一个区块。任何时刻,只有一个生产者被授权产生区块。如果在某个时间内没有成功出块,则跳过该块。

在正常情况下,DPOS 区块不会经历任何分叉,因为区块生产者合作生产区块而不是竞争。如果有区块分叉,共识将自动切换到最长的链条。具有更多生产者的区块链长度将比具有较少生产者的区块链增长速度更快。此外,没有区块生产者应该同时在两个区块链分叉上生产块。如果一个区块生产者发现这么做了,就可能被投票出局。

3.2.1 交易确认

由 DPOS 共识算法维护的区块链出块者都是 100%在线的。这就是说一个交易平均 1.5 秒后,会被写入区块链中,同时被所有出块节点知晓这笔交易。这就意味着只需要 1.5 秒,一笔交易可以认定为 99.9%被区块链接收了。

3.2.2 可插拔的共识算法模块

DPOS 共识算法可以广泛支持公有链、联盟链与私有链的场景,如果有业务场景需要用到满足特定业务需求或目的的共识算法,HPB 的可插拔共识算法模块可以灵活支持不同共识算法的集成切换,

并且对 POS 类的算法提供通用的共识步骤接口。

3.3 身份与授权管理

身份认证与授权是企业级应用的重要基础性模块，HPB 框架服务层设计多层次的参与者与相关资源的认证和授权体系。

HPB 允许使用唯一的长度为 3 到 32 个字符的可读的名称来实现对帐户的引用。该名称由帐户的创建者自行选择。所有帐户必须在创建时必须充入最小的帐户余额以支付存储帐户数据的费用。

3.3.1 基于角色的权限管理

权限管理主要涉及明确特定的消息是否被正确授权。权限管理的最简单形式是检查事务是否具有所需的签名,但这隐含着所需的签名是已知的。通常权力是与可以分类的个人或个人群组绑定在一起的。HPB 供了一个声明式权限管理系统,可以让帐户细粒度和高级别地控制谁在何时能够做什么。

至关重要的是,身份认证和权限管理被标准化实现,并与应用程序的业务逻辑分离。这使得开发某种工具以通用方式管理权限成为可能,并为性能优化供了巨大的空间。

每个帐户都可以通过其他帐户和私钥的任何加权组合来控制。这种机制创建了一个能够真实反映权限在现实中的组织情况的层次化权限结构,并使得多用户对资金的控制比以往任何时候都更容易。多用户控制是提升安全性的最重要因素,如果能正确地使用,可以极

大地消除黑客盗窃的风险。

3.4 状态通道

HPB 不应把智能合约部署在区块链上，而是通过利用状态通道上的智能合约来提高区块链的速度、可靠性和可扩展性。在当前实际的应用中，区块链系统不可能完全替代已有的系统，也多多少少需要传统中心化模块的引入。状态通道的引入，为封闭的区块链系统架构做出了一个极其有意义的尝试。

3.5 应用服务

3.5.1 区块链应用程序接口 (APIs)

在区块链基础层，设计提供一系列的区块链数据访问和交互接口，采用 JSON-RPC 和 RESTful API 支持各类应用和开发语言。支持多维度的区块链数据查询和交易提交等区块链交互操作，在不同的业务场景，交互访问接口可以进一步和权限控制体系集成。

3.5.2 应用开发包 (Application SDKs)

应用程序开发包（Application Software Development Kit）是基于不同开发语言对区块链操作和功能的综合性服务包，提供加密、数据签名、交易生成等综合性服务功能接口，可以扩展集成特定业务逻辑功能，无缝支持各类语言业务系统的集成与功能扩展。将支持 Java、JavaScript、.NET、Ruby、Python 等多种语言 SDK。

3.6 智能合约体系

3.6.1 智能合约生命周期管理

对于每一项智能合约，作为一项链上资产进行全生命周期管理，对智能合约的提交、部署、使用、注销进行完整可控的流程管理，并集成权限管理机制对智能合约操作的各项机制进行综合性安全管理。

3.6.2 智能合约审计

对智能合约进行自动化工具审计与专业人员代码审计结合的保护性审计，进一步集成代码审查和形式化验证的自动化工具，集成单元测试覆盖率的审查工具。

3.6.3 智能合约模版

根据不同业务领域的通用性业务模型与流程，逐步形成通用的智能合约模版，可以支持各类通用业务场景中的灵活配置使用。

3.7 通用虚拟机机制

HPB 的目的是可以支持多种虚拟机,同时可以随着时间推移持续按需求增加新的虚拟机。

HPB 会实现轻量化的智能合约虚拟机，支持多层次的智能合约虚拟机体系，底层的虚拟机与上层高级程序语言解析转换相结合，

灵活支持虚拟机的基础应用。通过定制化的 API 操作实现虚拟机的外置接口，可以灵活地与账本数据以及外部数据进行交互操作。这一机制实现了智能合约运行时达到原生代码执行的高性能。同时也实现了支持不同区块链的通用虚拟机机制。

3.7.1 以太虚拟机(EVM)

这个虚拟机已经被用于大多数现有的智能合约,并且可以在 HPB 系统区块链上使用。可以想象,在 HPB 操作系统区块链上,EVM 合约可以在内部沙箱中运行，只需要少量适配就可以与其他 HPB 应用程序交互。

3.7.2 小蚁虚拟机(NeoVM)

这个虚拟机已经被用于金融等各行业,并且可以在 HPB 系统区块链上使用。希望未来使用 NeoVM 的客户需要高性能场景时，只需要少量适配就可以与其他 HPB 应用程序交互。

3.8 系统管理

3.8.1 系统配置

在分布式账本的区块链体系的应用中，会涉及系列的运行机制，如区块生成时间、区块容量、参与节点限制等，系统配置可以对系统运行中的各参数在特定范围内进行灵活配置,系统可以基于不同参数运行。

3.8.2 系统监控

对区块链体系、网络、节点进行可视化应用和日志系统的综合监控，各类异常的实时报警与通知，并支持特定情况的远程故障恢复，网络系统重启等服务。支持根据不同业务领域需求进行综合监控扩展。

4.治理架构

4.1HPB 代币介绍（GXN）

HPB 网络代币（GXN）是一种用来为 HPB 网络提供支持的实用代币，包括去中心化的社交媒体协作，金融大数据的分发和交换，电商流程跟踪和信誉评价，以及可信搜索网络和广告系统。

4.2 代币细节

代币分两个阶段：

第一阶段：开始日期：2017 年 6 月 28 日，预售（presale）阶段，时间为三天。一个以太币可兑换 1300 个 GXN，总额为 8000 个以太币。

第二阶段：开始日期：计划 2017 年 8 月 23 日 。ICO 阶段，时间为三周。其中，第一周 ETH 与 GXN 的兑换比例为 1200 个；第二周为 1100 个；第三周为 1000 个。

ICO 将在达到本次募集以太上限（22000）或者三周后结束，以

提前达到条件为准。

- **代币分配：**

众筹参与者 36%，ICO 公开售卖，ICO 募集所得资金将用于 HPB 项目的设计研发和市场运营。

早期参与者 10%，分发给项目早期的社区成员、贡献者及早期投资人。

创始团队和基石投资者 20%，锁定期为一年，此后两年每半年释放一次 ，每次释放 5%。

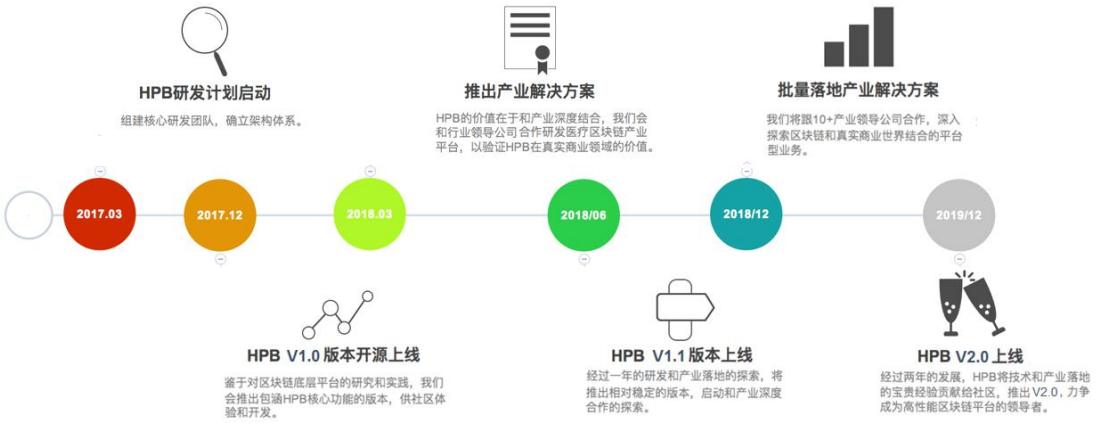
19%为储备金，锁定期两年，此后视社区发展情况决定，可能会销毁。

15%为团队新进入者及程序贡献者奖励金，围绕 HPB 基础服务，壮大发展社区。

- **资金分配：**

资金分配：核心开发 50%、硬件 5%、安全相关 10%、运营 10%、市场营销 10%、法律 5%，与高校与研究机构组建联合实验室 10%。

5.发展路线图



6.应用场景与经济模式

6.1 共享医疗经济

HPB 可用于去中心化的医疗经济，服务国家的健康医疗事业。目前医疗行业存在很多问题和痛点，例如：

(1) 数据信息孤岛，机构素质层次不齐，信息无法共享。

(2) 传统医疗业务流程繁殖，诊疗挂号，候诊，缴费问题突出。

(3) 患者信息不透明，医患矛盾突出，患者交易成本很高。

(4) 现有医疗机构无法满足特定层次人群高需求

中共中央、国务院于 2016 年 10 月 25 日印发并要求实施《“健康中国 2030”规划纲要》。纲要是为推进健康中国建设，提高人民健康水平，根据党的十八届五中全会战略部署制定。纲要内容提到： 共建共享是建设健康中国的基本路径。从供给侧和需求侧两端发力，统筹社会、行业和个人三个层面，形成维护和促进健康

的强大合力。

HPB 响应国家的号召，并预测这是一个巨大的蓝海市场，通过 HPB 自身具有的特性能解决未来医疗机构的数据，信息共享，交易数据落地。并且把服务面向 B 端和 C 端。B 端接入需要提供接入的 HPB 代币当做交易费用，C 端即提供数据使用许可也会请求数据（例如不同医院病历查看）可以进行收取 HPB 代币作为交易费用。同时保证了交易数据的合法性，并且通过 HPB 的高性能特性高实用性，实现了全行业的数据共享，数据分析，节省了资源，并且为国家的医疗健康管理，预测会发挥巨大的作用。

6.2 普惠金融

目前国内的金融行业都是采用的传统金融架构，每个金融机构都是自己孤立的信息系统。未来的去中心化的趋势是不可避免的，这是一片待开发的处女地，里面都是保守的企业和客户，但是区块链的潮流是不可阻挡的。同时传统金融行业的观望也是很有道理的，比如金融行业里最关注的安全性，高并发，高性能，异地灾备要求，是目前区块链技术中需要提高的，或者遇到瓶颈无法解决的，的比如 TPS3000 的瓶颈，所以推动起来非常困难。

HPB 的出现将会推动这个行业的蓬勃发展，本身符合国家要求去 IOE 化的政策，HPB 的高性能高并发解决了交易性能的问题，区块链自身先天性的数据加密安全，分布式去中心数据存储，可以去满足金融客户的高性能，高并发，高安全，高灾备需求。HPB 通过

软硬结合，未来把这些机构接入 HPB 的公有链，通过对接入公有链的金融机构收调试，运行费用，构造整个 HPB 的高性能底层的完美生态圈。

HPB 团队正在研发的区块链融资供应链系统，就是以普惠金融为目标，对 HPB 公有链的积极探索和尝试，将会整合行业内的资源，例如对汽车制造的模具使用场景进行研发，预计将在 2017 年年底第一个版本会上线运行验证。（注，汽车制造模具供应链是一个很巨大的市场，一个车型的模具定型后的使用量折合价值至少 10 亿人民币以上，而且是最普通的车型）。

名词解释：

- 去 IOE 化：它是阿里巴巴造出的概念。其本意是，在阿里巴巴的 IT 架构中，去掉 IBM 的小型机、Oracle 数据库、EMC 存储设备，代之以自己在开源软件基础上开发的系统。目前央行也发文要求国有化的银行金融机构为了安全考虑，逐步进行去 IOE 化。

- 汽车模具：是指为了批量生成一辆定型的汽车，要去制造的模具，其中钢材是其中使用最多的成分。一个汽车模具大约有 3 万个零件，一个最普通的汽车模具的研发，使用费用大约在 10 亿人民币以上。

6.3 智慧大数据

大数据目前仍属于万众注目的行业，但是基于数据获取的廉价性以及侵犯隐私性，在国内有其先天的原罪。都是基于政府政策作为导向，目前随着国家政策不断完善，从最近国家查出了 50 多家违法的大数据公司，风口已经变了。

只有打造围绕普惠金融的生态圈，结合 HPB 软硬件能力，并通过智能合约，对数据的采集，使用，授权，都进行了智能处理，保证了数据的纯净性，才能让大数据真正的成长起来。通过 HPB 营造一个良好的生态圈，通过智慧大数据来利用区块链的数据，未来将会大大的提高数据的安全，授权，隐私性，和可用性，挖掘区块链智慧大数据的蓝海。同时对公有链上数据的授权传输，以及使用，查询交易费用可以通过收 HPB 取代币方式解决。

6.4 区块链积分系统

区块链积分系统是作为普惠金融的一部分，这里单独拎出来是因为 HPB 目前已经在和一家商业银行合作，正在实施区块链积分系统，目前已经进入到中后期测试待投产阶段。

通过区块链积分系统的建设，探索行业联盟链的实现机制，并为未来 HPB 公有链上推行积分系统进行最佳的实践并积累经验。