

先行链白皮书2022（V1.01）

1. 背景

汉全科技是一家原生区块链技术公司，从2017年初进入区块链行业，五年来见证了区块链行业的发展，跟数百个企业和组织一起探讨过区块链解决方案，参与了数十个区块链项目的开发。

我们发现，虽然参与者对产业区块链热情高涨，但是由于区块链技术发展处于早期阶段，基础设施还不成熟，可参考的行业案例少，参与者又对区块链技术了解不多，解决方案难以落地。

如果能提供较低准入门槛和投入成本，相信会吸引更多的参与者加入进来。

我们结合了数十家客户应用区块链的经验，推出了先行链区块链网络，先行链是开放平台，专注于产业区块链，可自由加入或者退出，平台涵盖了区块链五大要素：分布式、加密、不可篡改、通证化和去中心化，是完备的区块链解决方案，加入先行链，即可以实现快速建链、上链和用链。

2. 区块链的五大核心要素

区块链是一种用于创建分布式数字账簿的数字机制。借助这种账簿，点对点网络中的两个以上参与者可以直接交换信息或资产，而不需要可靠的中介结构。

区块链整合了现有的技术，形成了包含五大要素的创新体系结构。

2.1 分布式

区块链的参与者在现实世界中是相互独立的个体，但在区块链中则通过网络联系在一起。每个管理完整节点的参与者都需要维护账簿的完整副本，该副本会在有新交易发生时进行更新。更具体地说，节点是参与者拥有或使用的计算机，可以运行共识算法。所有参与者都可以查看账簿的全部内容，但无权更改，除非遵循预先制定的规则。

2.2 加密

区块链采用公钥和私钥等技术，以安全、半匿名的方式记录区块中的数据。参与者掌控着自己的个人身份和其它信息，在交易中只共享必要的信息。

2.3 不可篡改

交易完成后的记录会经过加密签名，加盖时间戳，并按时间顺序添加至账簿。通过 SCPOS（见4.4 共识机制）和拜占庭容错算法（见4.5 拜占庭容错算法），来防止网络攻击，防止节点作恶。

2.4 通证化

区块链的运行依托于每一个成员的共同维护，通证化是将通证作为燃料用来代表社区治理权限，通过质押燃料获取投票权来确定出块节点和进行社区治理，保证区块链的去中心化。同时任何交易都会消耗链资源，如果有人恶意执行大量交易，那么将占用大量链资源，破坏链的稳定运行，为了避免此类攻击，保证链能更稳定的运行，我们通过使用燃料来量化链上资源，每次执行交易时消耗对应量的燃料。

先行链通证只用于燃料、投票等合规合法用途，不用于交易炒作。

2.5 去中心化

维护网络信息和网络运行规则的是分布式网络中的多台计算机，或者称为多个节点。在具体的实践中，去中心化意味着不存在单个实体控制所有计算机和信息，或单个实体制定规则。每个节点维护相同的加密副本，并保存网络中的记录。由所有完整节点运行的共识机制负责交易的验证和审批。这种去中心化的、共识驱动的系统架构意味着，由中央权威机构进行治理已不再是必需的，同时还可以防止欺诈和恶意交易。

区块链的五大要素结合在一起，就可以支持两个以上互不相识的参与者在数字环境中安全地交互。这五大要素缺一不可，如果缺少其中一个或几个要素，区块链的价值就会受限，甚者被破坏。

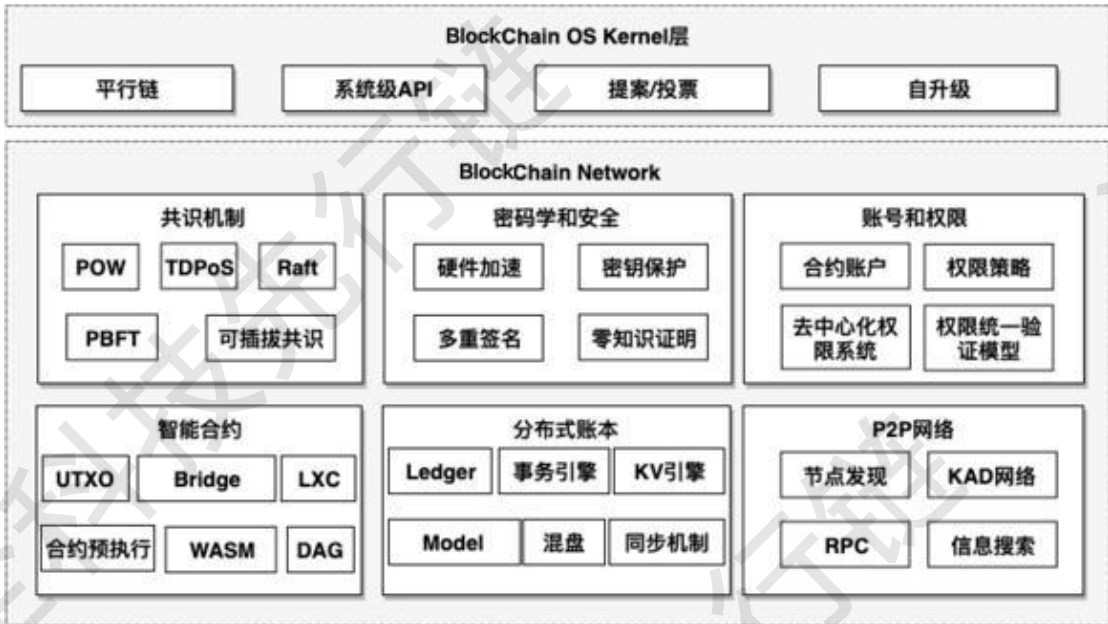
3. 先行链定位

区块链未来发展，将经历创新、完备、增强三个阶段。先行链从开始就定位区块链完备解决方案，通过部署分布式、加密、不可篡改、通证化和去中心化这五大要素，为参与者提供区块链完备解决方案。

目前市场上产业区块链平台几乎都没有完整用到区块链的五大要素，其中最难以实施的是通证化和去中心化，只有做到这两点，才能发挥区块链最大价值。

要适合商业应用，性能是核心，先行链采用主链+平行链架构，主链确保去中心化，共享安全，平行链用于联盟或者项目，数据权限自由控制。

4. 先行链系统架构



4.1 主链

主要特点是高性能，真正实现了智能合约的并行执行和验证。

在架构方面，其可插拔、插件化的设计，使得用户可以方便选择适合自己业务场景的解决方案。

在网络能力方面，具备全球化部署能力，支持广域网超大规模节点，SCPoS算法确保了大规模节点下的快速共识。

在账号安全方面，内置了多私钥保护的账号体系，支持权重累计、集合运算等灵活的策略。

4.2 平行链

在先行链的立体网络里面，有大量的区块链存在。这些链通过主链管理起来，这些链就是平行链，从而形成一个真实、独立存在的区块链体系。我们把这个网络叫做立体网络。立体网络上通过主链创建的平行链，可以选择是公开链，也可选择是联盟链（仅成员可见）。

平行链内交易不消耗主链燃料。

4.3 共识机制

基于POS基础上衍生出了很多改进算法，先行链也自主研发实现了一套POS共识，我们称之为SCPoS（超级共识权益证明）。依据这种算法，全网持有燃料的人都可以给候选人投票，产生验证人节点进行区块的生产。

SCPoS的参数包括每轮的节点个数、出块间隔、节点每轮出块个数等，在创建链的时候可以指定，也可以通过提案机制升级。例如，如果配置的参数为每轮10个节点、出块间隔为6s、每个节点每轮出块个数为60个，则每轮的时间为60分钟。

共识机制有三种角色：验证人、候选验证人、提名人。

验证人：出块和交易验证，需要部署服务器和运行客户端，由提名人在候选验证人中投票选出。

候选验证人：符合条件的人可以通过抵押一定数量的燃料申请成为候选验证人；成为候选验证人后可以接受提名人的投票，票数达到前10则可成为验证人；为了约束候选验证人池子，抵押的燃料一般不少于系统总燃料的十万分之一。

提名人：燃料持有者，可以抵押后获取投票权，投票给验证人，一个燃料可获取一个投票权，且采用一票一投的方式进行投票。提名人可根据投票的票数按加权平均分享验证节点奖励。

4.4 跨链

由于区块链行业还处于早期发展阶段，因此产生了很多的区块链框架，例如有Fabric、FiscoBcos、XuperChain、BTC、Ethereum、Cosmos、Polkadot等。

这些框架底层协议各不相同，由此形成了新的数据孤岛。无论这些孤岛是基于相同的底层系统还是不同的底层系统，其数据互通都非常困难。因此，迫切需要一个解决方案能够系统地解决多链数据融合的问题，从而实现不同链之间的价值互通。

跨链（Cross-Chain），简单来说就是通过一定的技术措施实现相对独立的不同区块链系统之间数据和资产的链接互通。可以将跨链理解为在不同的信息孤岛间搭建起一座座桥梁，使得信息能够便捷的流动，为价值互联网奠定基础。常见的跨链解决方案一般是针对资产类，实现不同链之间任意数据的跨链互通难度会更高。

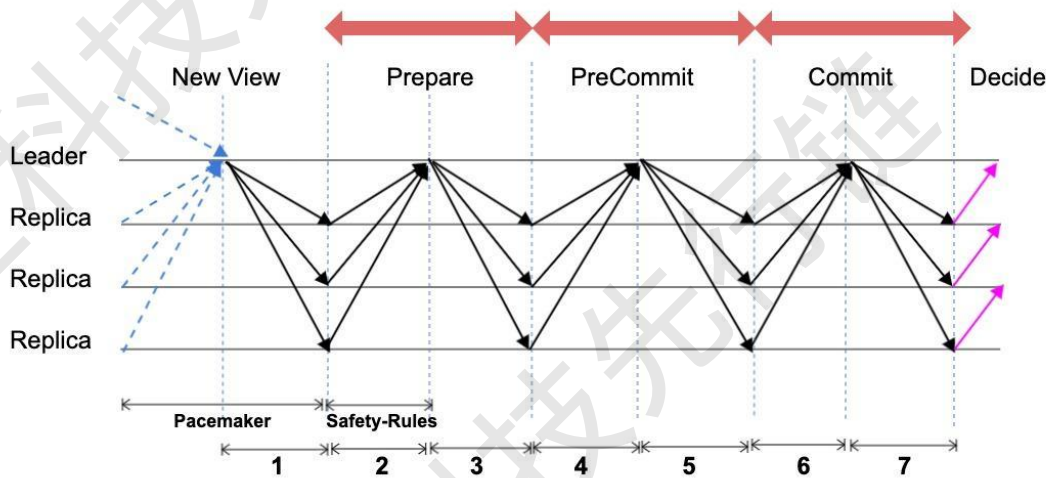
4.5 实用拜占庭容错算法（Practical Byzantine Fault Tolerance，简称PBFT）

PBFT是一种状态机副本复制算法，即服务作为状态机进行建模，状态机在分布式系统的不同节点进行副本复制。每个状态机的副本都保存了服务的状态，同时也实现了服务的操作。所有的副本在一个被称为视图的轮换过程中运作。在某个视图中，一个副本作为主节点，

其它的副本节点作为备份节点。主节点通过SCP0S算法选出，用来负责打包交易出块。主节点选出后，将交易进行校验并打包，然后发送预准备消息给所有的副本节点。

每一个副本节点在收到来自主节点的预准备消息之后，都要检查消息的正确性，然后发送准备消息给除了自己以外的其他所有副本节点。同时它也会收到其他副本节点发来的准备消息。在收到消息后，副本节点对其他节点的准备消息进行验证，如果正确就将准备消息写入消息日志，集齐规定数量的准备消息之后，它就进入准备状态。

副本节点进入准备状态后，在全网范围内广播commit消息，当副本节点集齐规定数量个验证过的commit消息后，就表示请求处理完毕，当前网络中的大部分节点已经达成共识，于是发送处理结果给客户端，运行客户端的请求。



5. 惩罚机制

节点成为超级节点后，每漏一个块，扣除0.01%的保证金，并没收该块的奖励；在5个出块轮次中，漏块个数超过应出块数的10%，则额外扣除1%保证金；当连续漏块超过10个或在最近5个出块轮次内漏块个数超过应出块数的30%，则认定该节点宕机或系统不稳定，将额外扣除10%的保证金，并将该节点剔除当前超级节点列表中，新的超级节点在候选验证人节点中顺号补位；当最近10个出块轮次内漏块个数超过应出块数45%，则认定该节点为恶意节点，将额外扣除15%的保证金，并将该节点剔除候选验证节点列表中，且接下来20个出块轮次内不可再次申请成为候选验证节点；另外，当超级节点被惩罚时，该节点的提名人将被扣除相同比例的保证金，即提名人给该节点的投票票数×惩罚比例；惩罚时扣除的通证将全部销毁。

6. 先行链产品架构



7. 先行链治理模式

- 计划用两年时间，从许可制向去中心化方向演进。
- 决策：通过提案投票，参与者允许在没有中央权威机构的情况下，在区块链上记录和执行决策。
- 参与：只要具备适当的基础设施并同意遵守运营条款，任何人或物都可以充当完整节点。燃料持有者通过提名验证人获得奖励。

8. 开发者服务

主链采用开源的方式，将为开发者提供常用开发语言的SDK和API。开发者可根据先行链API文档搭建自己的应用或者工具；先行链发起方也将率先提供各类基础设施和应用，既便于普通的用户参与到先行链中来，也便于开发者基于先行链开发生态应用，这将极大的丰富先行链的生态建设，使得更广泛的成员能够加入到先行链中来。

9. 先行链基础设施

9.1 客户端

采用自动化部署功能实现一键部署节点，可快速加入主网；并提供节点管理、查询节点运行状态、提交节点信息等功能。一键部署节点的功能将大大降低普通人的参与成本，使得不懂代码的用户也能快速便捷地搭建起区块链节点，并参与到社区建设和治理。这样做将使得先行链能拥有更广泛的用户基础，能让人加入到先行链中来成为先行链的节点，而当节点越多，先行链也将趋于更稳定、更安全。

9.2 先行链通

创建先行链通账户，参与链上治理。包括安全验证、出块节点评选、社区决策投票等，保证区块链安全、公平、公正地运行。

9.3 BaaS平台

BaaS平台主要用于创建和管理联盟链，采用自动化部署功能，一键部署BaaS系统，可快速搭建联盟链，支持配制主流的共识机制、共识参数、联盟链的其他参数，BaaS还提供了一系列的配套功能，用于管理和监控联盟链、管理成员、部署和管理智能合约等；BaaS工具的搭建，降低了开发者参与区块链应用建设的成本，开发者无需重新开发区块链底层，无需深入学习区块链的技术，也可快熟的搭建自己的联盟链；这使得开发者能够专注于业务的开发，这将大大提高成员的参与度，丰富先行链的生态应用。

BaaS平台主要功能：

- (1) 区块链配置管理：负责对新建区块链节点进行快速配置以及初始化等操作；
- (2) 智能合约管理：对智能合约的上传、发布、审核、安装、初始化、权限设置、升级等功能的管理；
- (3) 动态联盟管理：联盟管理包括，联盟链的创建，联盟链新成员的加入、联盟链已有成员的退出、联盟链的投票策略设置等功能；
- (4) 区块链模版管理：针对一些典型的区块链应用场景，预选制定相应的区块链模版，配置好缺省参数；
- (5) 区块链监控：负责对区块链网络和节点的运行状况进行监控报警，包括但不限于网络连通性监控、计算资源使用情况监控以及节点服务状态监控；
- (6) 区块链浏览：平行链浏览器，查询区块链高度、交易数量、网络拓扑、安装的智能合约列表、具体交易情况等区块链细节信息；
- (7) 用户日志：记录用户在平台执行的各项操作，比如创建和删除区块链、增加和删除节点、安装智能合约等；

(8) 数据统计：用于统计区块链服务平台自身运行状况，比如用户操作的相应时间、区块链创建时间、在线用户数等指标。

9.4 区块浏览器

浏览器用于查询主链或平行链的区块链高度、交易数量、网络拓扑、安装的智能合约列表、具体交易情况等区块链细节信息。浏览器对于平行链的兼容性方便用户查询主链和平行链的信息，也使得平行链的开发者开发成本减低，无需重复开发多套浏览器。

10. 先行链应用生态

我们希望和每个参与者一起共建生态，共同打造应用市场，丰富先行链生态，为开发者提供可信数据服务、存证溯源、数字营销、供应链等解决方案。

11. 节点

超级节点：即验证人节点，早期数量10个，随着网络参与者增多，超级节点数量可以增加。

轻节点：非验证人节点，数量没有限制。

12. 开发线路

- 2022.1：客户端、先行链通、浏览器、BaaS系统开发完成，主网启动。
- 2022.2：可信数据服务平台、区块链+商品溯源系统上线。
- 2022.6：深度支持NFT应用。
- 2022.10：提案投票功能上线。
- 2022.12：去中心化治理组织成立。

13. 团队介绍

先行链发起方广州汉全信息科技股份有限公司（简称：汉全科技），成立于2015年，是国内优秀的区块链综合解决方案提供商，团队核心已从事区块链研发5年以上，参与数十个区块链项目，是区块链资深从业者。

14. 免责声明

本文档仅作为传达信息之用，文档内容仅供参考。

本文档不构成在及其相关公司中出售股票或证券的任何买卖建议、教唆或邀约。本文档不组成也不理解为提供任何买卖行为，也不是任何形式上的合约或者承诺。鉴于不可预知的情况，本白皮书列出的目标可能发生变化。虽然团队会尽力实现本白皮书的所有目标，所有拥有燃料的个人和团体将自担风险。文档内容可能随着项目的进展在新版白皮书中进行相应调整，团队将通过在网站上发布公告或新版白皮书等方式，将更新内容公布于众。本文档供主动要求了解项目信息的特定对象传达信息使用，并不构成未来任何投资指导意见，也不是任何形式上的合约或承诺。

15. 结语

新兴技术的飞速发展，正在加速全球化信息化的浪潮，全球范围内的资源分配、跨组织协作，深刻影响着我们的生产生活，这就要求我们以全球视野、开放精神面对日益激烈的市场竞争。区块链作为一项新兴技术，其技术生态、场景应用和监管制度尚有诸多待设计、待开拓、待完善的工作，呼唤广大技术研发企业、行业应用企业和监督管理部门参与，共创、共建、共享一个由区块链技术参与构筑的，更加开放透明、高效协同、风险可控的信用社会。这也是先行链将继续和长期坚持区块链技术实践的根本原因。

区块链技术实践不是封闭的、孤立的、短暂的原型验证，而是开放的、共享的、长期的生态建设，我们欢迎志同道合的区块链技术企业、独立开发者、科研机构、应用企业、监管部门等所有关注区块链发展的同仁们加入到先行链开源社区建设和应用生态打造的过程中来，围绕价值共创，携手开拓未来！