链上价值流通网络生态系统

免责声明

这是一份概念性文件（「白皮书」），用来说明我们所提出的 IPFST-Chain。这份文件可能会随时受到修改或置换。然而，我们没有义务更新此份白皮书，或提供读者任何额外信息的管道。

读者请注意下列事项：

并非开放给所有人：IPFST-Chain 并非开放给所有人。参与可能需要完成一系列的步骤，其中包括提供特定信息与文件。

在任何司法管辖区内不提供受管制产品：IPFST-Chain（如本白皮书所述）无意构成任何司法管辖区内的证券或任何其他受管制产品。本白皮书不构成招股说明书或任何形式的要约文件，也无意构成任何司法管辖区内的证券或任何受管制产品的要约或招揽。本白皮书并未经过任何司法管辖区的监管机构审查。

不提供任何建议：本白皮书并不构成关于您是否应参与 IPFST-Chain 或购买任何 IPFST 通证的建议，也不应作为任何合约或购买决定的依据。

无任何声明或保证：对本文件中描述的讯息、声明、意见或其他事项的准确性或完整性，或以其他方式传达与计划相关的讯息，我们不给予任何声明或保证。在没有限制的情况下，我们不对任何前瞻性或概念性陈述的成就或合理性给予任何声明或保证。本文件中的任何内容，均不得作为对未来的承诺或陈述之依据。在适用法律所允许的最大范围内，尽管有任何疏忽、违约或缺乏关注，任何因本白皮书的任何相关人员或任何方面而产生或与之有关的任何损失（无论是否可预见），其所有责任均免除。可能受限但无法完全免除的责任范围，仅限于适用法律所允许的最大限度。

您必须听取一切必要的专业建议，包括税务和会计处理相关事务。我们希望 IPFST-Chain 计划能够非常成功。 但我们并不能保证成功，且数字资产和平台都涉及风险。 您必须评估风险以及您的承担能力。

摘要

现有网络协议中存在的缺陷使网络安全难以得到保障，也让价值流通无法快速高效的进行。IPFST-Chain 是一个蕴含多重激励机制的完全去中心化的创新型区块链架构，其致力于打造新一代的以技术驱动型为基础，以应用落地为切入点的去中心化全球价值流通网络生态 平台。IPFST-Chain 是从通用型区块链到专业型区块链技术的升级， 目前针对区块链生态系

统各环节链接、流通打造一套完整的，行之有效的链上价值流通网络生态系统。

IPFST-Chain 为了更好的构建一个链上价值流通网络生态系统，整合基于区块链技术的 平台或基于区块链技术的业务合作， 鼓励更多人参与到 IPFST-Chain 建设当中；首先 IPFST-Chain 在传统 Tendermint 公链 POS+BFT 共识机制的基础上进行优化改造，创造了全 新的共识机制——POF Proof of faith（信仰证明机制）让 IPFST-Chain 网络能超高速运转，避免区块网络拥堵，安全高效的交易确认；;同时在合约层以及大数据协议层中，做到兼容 以太坊 Solidity 和 IPFS 星际文件协议；并建立基于公开、透明原则的多重激励机制——共 识激励、智能算力 POS 激励、数据存储激励等机制；最终以开放的态度链接所有现实行业，让价值不断循环发展。

目录

一、区块链发展现状

比特币由 Satoshi Nakamoto 于 2009 年创建，是世界上第一个区块链技术应用。比特币网络是由互联网连接的全球计算机网络，每台计算设备都称为节点。当有人发送一些 BTC 时，交易将被广播到所有节点，每个节点可以独立地验证交易的真实性。比特币系统将每隔几分钟发生的所有事务都打包在一起为一个区块，为了完全处理事务区块并将其添加到所有历史有效事务的区块链或公共分类帐中，节点间需要竞争解决困难的数学问题，率先完成正确解的幸运节点首先获得新比特币的奖励，并且该题被添加到区块中的过程称为区块链。

从货币角度来讲，比特币是目前为止规模最大的数字货币，它是区块链 1.0 时代的一个重要应用，是区块链的首次应用：比特币在去中心化的前提下，实现了数字货币在发行、支付、流通等阶段的职能，这是一种全新的支付手段。从区块链角度来讲，随着比特币的关注度逐渐增大，区块链作为它的底层技术也越来越被大众所熟知，区块链开始逐渐脱离数字货币，渗透到许多商业领域，不同行业都希望能够将比特币这个技术应用到我们的现实生活中去，通过各式各样的应用场景，让我们获得更好的体验。

Satoshi Nakamoto 对比特币的愿景是允许跨境点对点支付和创建世界上第一个真正去中心化的价值转移网络，这无疑是革命性的。同时比特币的底层区块链技术直接导致许多去中心化网络的建立，如 ETH、EOS 等，这些网络允许智能合约，身份保护，知识产权管理，供应链管理以及众多其他前所未有的创新。

区块链带来信息互联网生产关系和价值体系变革

人对于客观世界的认识分为两大类：一是关于客观世界各种事物的属性与本质及运动规律的认识；二是关于客观世界各种事物对于人类的生存与发展的意义（即价值）的认识。马克思价值理论突破了从成本或从需求两个角度说明价值的思路，而是从人与人的关系角度说明价值问题。劳动价值论最终要说明的问题是人与人之间的关系。从原始社会到共产主义社会的变迁表现为经济的量的提高，制度的变迁，本质却是人与人之间关系的变迁。

信息互联网时代用户大数据成为了重要的生产资料，大数据涵盖两个关键技术，大数据和云计算，也就是强大的计算能力和放在云端随时可以取用的数据。第一次技术革命，煤炭是主要生产资料，第二次技术革命石油和电是主要生产资料，这一次技术革命数据将会是重要的生产资料。大数据是生产资料，云计算是生产力，互联网是生产关系，但是在传统的信息互联网生产关系里，用户并不能获得自身行为数据的实际价值。

区块链技术的诞生，为互联网行为数据信息提供了一种更为公平的价值交易模式，价值互联网由此诞生。区块链的分布式网络结合智能合约，能够解决许多信息网络的短板。区块

链技术的普及应用，将会解决信用问题、价值传递问题和价值储存问题，也可以解决个人互联网行为数据的采集、储存问题。不仅如此，区块链还蕴含着巨大的经济意义，甚至可以说，市场和时代呼唤了区块链的诞生。

区块链的出现将建立全新的互联网生产关系和价值体系，新的价值互联网将通过区块链通证经济模式把收益分配给所有的用户，用户可以在新的价值流通网络中通过个人使用行为获得奖励。用户可以在生产 “数据”的过程中处于一种自发主动的状态，同样接收 “数据”的一方会根据提供的 “数据”给予相应的回报，双方的交易信息在一种透明、不可更改的环境下运行，这样就会出现一种较为良性的循环，这将是区块链时代下新的价值互联网的主要模式。

价值互联网让每一个人的行为更有价

事实上，支撑当下互联网巨头万亿市值的核心就是高频用户行为展示和巨量用户带来的数据价值。区块链的意义恰好在于能够变革现有的用户数据价值体系，让数据所有权实现重新分配，让真正拥有数据的用户在保证隐私的同时，从分享数据中获得奖励。 互联网早期，谷歌、脸书、亚马逊、微软等互联网巨头建立了信息互联网时代，主要加速了信息流通效率，解决了信息不对称的问题；随着区块链发展，比特币和以太坊等技术实现了价值的数字通证化，但用户行为数据所有权和权益确权问题并没有得到解决。如今，Facebook 牵头成立了一家由 28 家合作伙伴成立的管理发行机构——Libra 协会，通过发布加密数字货币 Libra，建立一套简单的、无国界的货币和为数十亿人服务的金融基础设施。它认为，每个人都享有控制自己合法劳动成果的固有权利，开放、即时和低成本的全球性货币流动将为世界创造巨大的经济机遇和商业价值。

Facebook 数字货币 Libra 的发布，将对全球经济格局产生深远的影响，同时这也预示着，“通证化”成为一个全球性的变革愿景与趋势，区块链将不再相对局限于技术领域，它将更好的惠及我们每一个互联网参与者。

因此，IPFST-Chain 致力于建立新一代的以技术驱动型为基础，以应用落地为切入点的去中心化价值流通网络生态平台。通过区块链技术、云计算、 5G 技术等匹配现实互联网，

实现现实世界人类行为与虚拟世界价值流转的链接。

IPFST-Chain 会将用户产生的互联网行为记录在区块链上，保证信息的真实性和安全性，用户贡献的个人互联网行为越多，单位时间内获取数字资产的数量就越多，以此激发用户不

断地去贡献个人的互联网行为，以获得更多的行为奖励。未来将是个人价值体系越来越健全的时代，通过 IPFST-Chain，个体将真正成为价值的创造者和拥有者。

二、IPFST-Chain 设计理念

什么是 IPFST-Chain

IPFST-Chain 项目在设计之初即聚焦于现有区块链系统存在的许多局限性，IPFST-Chain 参考 DPOS+BTF 共识机制的优点，独创了 POF Proof of faith（信仰证明机制）让 IPFST-Chain网络能超高速运转，避免区块网络拥堵，安全 高效的交易确认；此外，IPFST-Chain 还通过兼容以太坊智能合约 Solidity 以及 IPFS 星际文件协议，来实现稳定，更具可扩展性以及更开放的区块链应用系统构建。

IPFST-Chain 致力于打造基于区块链技术的价值流通网络生态，提供兼具灵活性、易用性、高效性、安全性的价值流通解决方案；基于 IPFST 底层公链、IPFST 多层激励机制以及 IPFST SDK,构建开放式链上价值流通网络生态，实现整个生态链接价值，以支付，社交，信任网络，人工智能，AI，金融，大数据，农业，传统资产等点对点的价值链接，转移，提升生态资产的流通效率以及降低流通成本。

IPFST-Chain 的魅力

IPFST-Chain 链上价值流通网络生态系统的魅力所在，就是链接全球商业万物的“区块链”生态系统。通过 IPFST-Chain “区块链＋”生态系统可以把全球多元化应用连接起来，并通过 IPFST 数字通证在整个生态系统应用中的循环，不断提升 IPFST 数字通证资产价值。随着 IPFST 数字通证资产价值的倍增，IPFST-Chain 价值流通网络的运营速度也会更快。从而不断倍增循环，打造属

于全球的 IPFST 价值流通网络生态圈。

IPFST-Chain 的未来

IPFST-Chain 致力于建立新一代的以技术驱动型为基础，以应用落地为切入点的链上价 值流通网络生态平台，旨在建立全球 “区块链＋”的多元化应用商业模式。IPFST-Chain 始 终坚持 “自主代码＋开源路线”的技术战略，力争成为世界级区块链底层技术开发的商业性公链。

IPFST-Chain 目标是：融合最前沿区块链、分布式账本等技术发展，密切结合各行业业

务发展，形成创新开源的技术体系和开放的合作机制，为各行业机构与业务模式提供完整、健壮、灵活的商业级区块链技术价值流通网络生态平台。

三、IPFST-Chain 链上价值流通网络生态系统

IPFST-Chain 的应用程序预计将成为率先运用 IPFST-Chain 区块链网络的商业应用之一。在本节中，我们将讨论由我们提出的去中心化 IPFST-Chain 区块链解决方案所将实现的具体 应用情境和功能，并将其与传统的集中式市场进行对比。IPFST-Chain 区块链协议拥有一种 内建机制，能够透过其代币来帮助非合作的网络参与者达到纳什均衡共识。

构建永不停息的数字资产交易所

去中心化网络的主要优点之一为网络服务的高可用性。这个特性能够防止资料中心故障。只要仍然有网络节点在运行，网络服务就能继续运作——尽管服务量或频宽可能会有所波动。

传统的数字资产交易市场应用程序强烈依赖集中式服务器和 IT 部门的后端服务。如果资料中心失灵，市场将停止运作。在 IPFST-Chain 的交易网络中，运算能力和商业服务都可以由社群成员提供，这使得网络服务面对故障时有更高的恢复能力。同时 IPFST 交易所引入的经济激励措施，为以社群为基础的 IPFST 交易所冲突解决提供了一种方式。这将能为 IPFST 交易所省下雇用和营运客服团队以解决买卖双方之间潜在冲突的成本。根据适当的管理控制，IPFST 交易所社群内的志愿者现在可以成为仲裁者，并且能够运用记录在区块链中的透明交 易资料来作出判断。

间。

构建统一跨平台的游戏生态圈

在整个 IPFST-Chain 生态中，全球的游戏开发者与玩家，能够让自己所产出的价值转化 为自身的收益，并以 IPFST 通证的形式在生态里流通，用于权利赋能，奖励结算，交易记录，商业运营等场景。

上世纪 70 年代，游戏《Pong》及家用游戏主机 “米罗华奥德赛”的推出，标志着电子游戏的诞生。至 2007 年，全球游戏市场花费了超过 35 年的时间，增长至 350 亿美元的市场规模。而今年，预计该市场将创造 1379 亿美元的收入——从 2007 年到 2018 年，在短短的 11 年中，我们就创造了惊人的 1000 亿美元的市场附加值。

在如此巨大的市场容量下，全球众多地区和国家的游戏产业却面临着游戏形式有限，游戏支付受限、文化壁垒 、运营、融资困难等各种问题，让本身无限可能的众多地方市场在多重阻碍下，艰难发展。

IPFST-Chain 认为，任何地区的游戏市场，都可以通过区块链技术实现快速化、多元化、

广泛化的发展，依托于 IPFST-Chain，将区块链与游戏结合，IPFST-Chain 将能够改变游戏生态社区机制，打造出一个基于区块链的游戏发行与研发生态的平台。

IPFST-Chain 去中心化游戏平台将会为游戏带来一下改变：

游戏资产的所有权和流通性

在区块链上，玩家可以拥有游戏内的资产，而这些资产则有更广泛意义上的流通性。传统游戏中的积分、道具、武器、角色往往全部归开发商所有，也回此中心化的开发商有更大的权力对这些资产进行大刀阔斧的改动，甚至随意处置。游戏内的资产往往只能局限于这一个游戏内部进行流通，出了游戏之外，似乎毫无复用的价值，也从科技层面很难被再次赋予应用场景。

资产随时随地交易

大量的游戏是不具备道具交易功能的，当然这么设计很多时候的初衷是为了避免游戏内经济机制的混乱、延长用户游戏时间、新增开发商的收入。假设以上并不是开发者所担心的问题，那么 “道具上链+移动钱包”可以实现两个用户随时随地在线上线下进行。你跟好友在吃饭时聊到最近的一个 PC 端游戏，打开手机钱包，看看彼此有什么样的武器装备，完成一笔交易的体验就像一次微信扫码支付一样简单，晚上回到家，打开 PC 登入游戏，交易完成的道具早已躺在了你的装备栏里。

游戏资产复用

资产上链后因为挂在每一个玩家的地址下，对于开发商来说可以轻松的复用其他游戏的资产进行二次改造或者实现跨游戏复用。

新的用户获取管道

传统游戏下，新的游戏往往需要重新获取用户，或者用老游戏给新游戏导流。区块链可以打破这种管道，降低获客成本，比如 CryptoCuddles，所有 CryptoKitties 的用户都是

潜在可以直接转换过来的游戏玩家。如果直接复用资产涉及到 IP 问题，开发商也可以这样设计，只要在 CryptoKitties拥有猫咪的用户，可以直接在这个游戏中直接获取一定的奖励，可以是角色、宝箱、道具等等，验证管道只需要用地址登入读取一下链上数据即可。

游戏开发商与玩家之间共赢

在大部分时候，游戏玩家和开发商往往是站在对立面的，一方想寻找游戏的不平衡性赚取游戏中的声望和获得游戏中的快感，另一方则通过修改游戏机制调整参数不停一遍又一遍洗用户，榨取用户的价值。而区块链则改变了生产关系，在游戏中，开发商与玩家的关系将发生本质的改变。传统游戏运行在中心化服务器上，开发商指定规则，玩家尝试突破规则。如果游戏运行在多个节点上，而部分节点由玩家运行并给与一定激励

透明公平游戏机制

当游戏的核心机制上链之后，玩家们可以查看过去只隐藏在中心化服务器中的游戏规则，这给开发商和玩家之间建立了更强的信任纽带。在游戏机制透明的逻辑下，玩家可以清楚的知道并相信某个宝箱的开宝概率，某个稀有武器是不是真正稀有，开发商所承诺的是否真正兑现。在传统游戏原始程序码黑箱的情况下，这些完全可以由游戏运营方随意调节。 “全服绝世柳丁武”可能在游戏下一个版本中跌下神坛人手一把，这种情况在传统游戏中再常见不过了。但在区块链游戏的世界中，就不是这么回事了。公平公正的机制，和由社区达成共识的游戏更新，给玩家带来的是更纯粹的体验。

去中心化社交支付

在社交支付领域中，全球互联网用户普遍都存在着隐私泄露的致命问题，但是互联网发展下并没有采取任何技术方式从根本上杜绝用户的信息不受侵犯。举例来说，用户经常遇到的刚刚浏览完某个购物网站，接着会在其他社交平台上收到类似的广告弹窗，并且是接二连

三的弹出，严重的时候还会发广告信息到用户的手机。这些都是因为中心化的互联网时代，全球用户数据隐私被垄断的大数据平台进行了可耻的贩卖，使全球用户的隐私受到严重侵犯，甚至用户隐私落到不法商贩中，还会造成用户个人严重的财产损失。

为了还全球用户一个 “干干净净”的社交支付体验，让全球用户的隐私得到保护，财产得到保障，IPFST-Chain 以区块链技术为支撑，从根本上把全球用户社交支付网络的控制权 从中心化的公司平台转向每个对应的去中心化的数据点当中，彻底实现区块链自带的中心化向去中心化的改变，让全球用户的所有数据控制权牢牢掌握在用户自己手里。让全球社交支付变得更纯粹更透明。

解决传统文化娱乐产业价值分配

随着知识经济的兴起，知识产权已成为市场竞争力的核心要素。互联网应是知识产权保护的前沿阵地，但当下的互联网生态里知识产权侵权现象严重，网络著作权官司纠纷频发，侵蚀原创精神、行政保护力度较弱、举证困难、维权成本过高等问题成为内容产业的尖锐痛

点。文化娱乐是文化产业的重要组成部分，包括数字音乐、数字图书、数字视频、数字游戏等。文化娱乐产品涉及生产 、复制、流通和传播等主要环节。随着 “互联网+”时代的到来，文化娱乐将迎来新的发展机遇，随着知识经济的兴起，知识产权已成为市场竞争力的核心要素。

IPFST-Chain 链上价值流通网络生态系统可以通过时间戳、哈希算法对作品进行确权， 证明一段文字、视频、音频等存在性、真实性和唯一性。一旦在区块链上被确权，作品的后续交易都会被实时记录，文化娱乐业的全生命周期可追溯、可追踪，这为司法取证提供了一
种强大的技术保障和结论性证据。

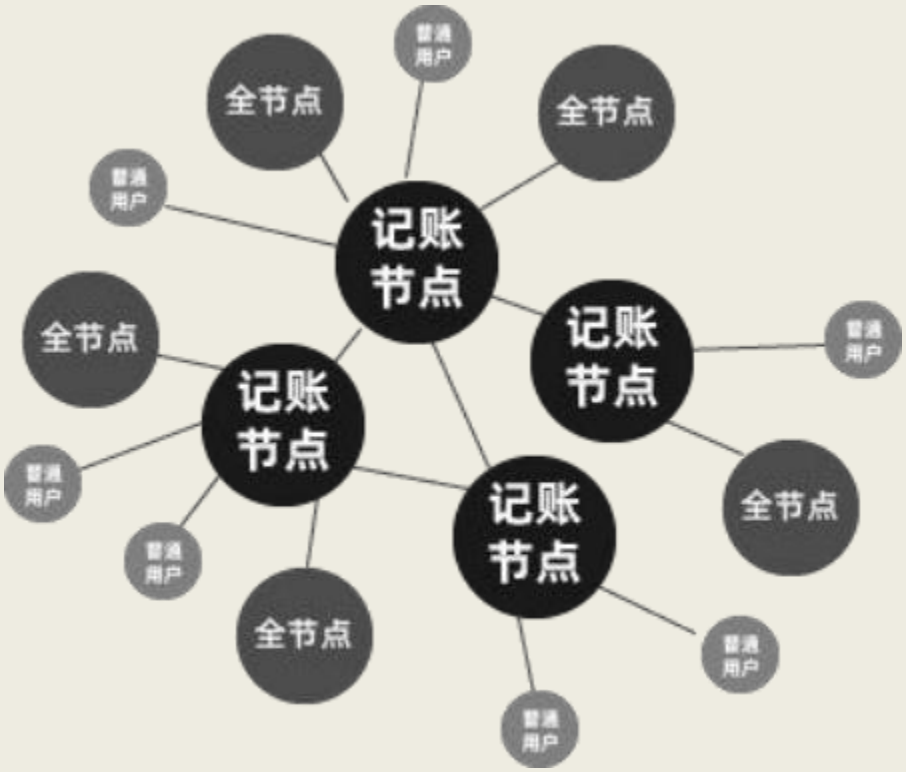
据调查， 目前全球影视行业可发展空间不断提高，为了使 IPFST-Chain 链上价值流通网络生态系统产生更广的资产价值，IPFST-Chain 会加速在全球影视行业的应用发展，通过其 生态钱包所打造的影视文化行业应用，基于区块链节点的不可复制性，保证版权交易不会被伪造，从而保障内容不被盗版侵害，中间平台无法通过伪造购买数据减少内容创作者的收入——交易都是公开透明的，创作者可以轻而易举地得知自己的点击量 、购买量，从而得知 自己应得的收入，不被中间平台欺骗。IPFST-Chain 可以从根本上让全球影视文化行业内容 更真实，规则更透明，并可以实现 IPFST 通证数字内容的价值转移，让全球影视行业利益收入分配更均匀。

四、IPFST-Chain 架构

IPFST-Chain 是由 IPFST 开发团队完全自研的一条高性能公有链，兼容以太坊 Solidity 智能合约编程语言以及 IPFS 星际文件协议，使用多层链构，由主链和子链组成，

主链主要负责子链数据同步和 IPFST 通证的交易等，子链便于 Dapp 或企业基于 IPFST-Chain 开发自己

不同的节点应用选择有不同的存储策略：



记账节点：IPFST-Chain链上价值流通网络生态系统的核心角色,受 IPFST 通证持有人的委托负责参与共识机制、制造区块。

全节点：负责保存完整数据,但不参与共识,侦听并转播交易。

普通用户直接通过接口或客户端访问,不保存数据，多层次节点系统的好处在于,IPFST-Chain 链上价值流通网络生态系统并不希望有节点都参与记账(挖矿)存储完整数据、转播交易。 因为并不是所有节点都有共同的述求,都希望保存完整数据，IPFST-Chain 链上价值流通网络生态系统设计让整个系统有清晰的角色分工，专业的节点做专业的事情，既节约能源又提高了整个系统的效率。

互联网络层

P2P 协议(P2 P Protocol)支持区块链网络中各节点的数据传输和信令交换,是数据分发或共识机制达成的重要通信保障。IPFST-Chain 链上价值流通网络生态系统设计中支持多种

P2P 协议、通信机制与序列化机制的配置,根据不同的场景需要进行灵活的协议使用,在通信安全方面,可以灵活支持 Https.TS.WSS(SecureWebsockets)等安全通信协议,在需建立平台应用对外服务接口上,可以扩展支持 OAuth 的认证集成。

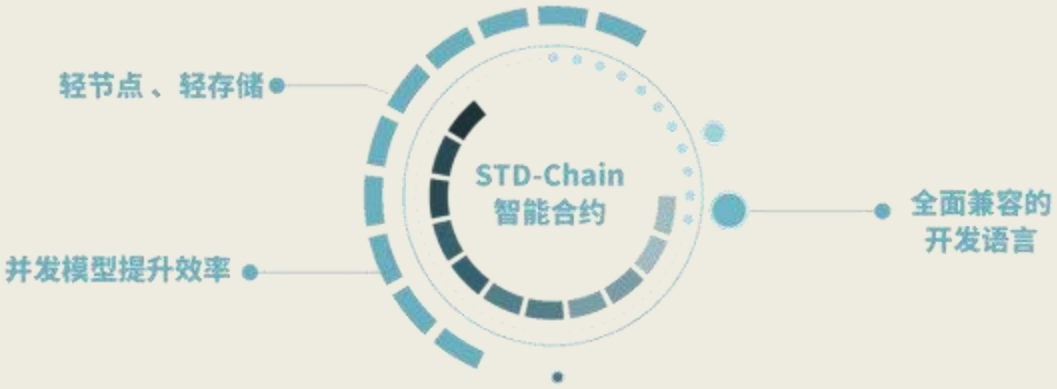
智能合约层

IPFST-Chain链上价值流通网络生态系统通过 IPFST-Chain链上图灵完备的智能合约帮助用户实现复杂的跨链交易、资产通证化，为开发者提供 DAPP 开发的便捷支持，为实现跨

链分布式商业应用打下基础。

为了能吸引更多的生态建设者到 IPFST-Chain 上开发 DAPP，共同建设 IPFST 生态，IPFST-Chain 链上价值流通网络生态系统致力于运用区块链技术为搭建去中心化应用提供基 础架构，通过针对各类开发语言的兼容引入，使得各种技术栈的开发者都可以迅速对接，便

捷高效地开发 DAPP。



全面兼容的开发语言

- IPFST-Chain 使用一种图灵完备并为区块链智能合约定制设计的字节码规范作为智能合约虚拟机的实现规范。提供静态类型的高级编程语言比如 C#，Java, TypeScript 等的

编译器实现从高级语言生成智能合约字节码，同时 IPFST-Chain 也将对以太坊 Solidity 进行

兼容，让更多区块链从业者更简单、便捷的将以太坊合约应用移植到 IPFST-Chain 上。

- IPFST-Chain 也将不断丰富各种语言的 SDK 方便开发者移植到不同的平台，从而不断吸引各行各业的 DAPP 开发者。

- 通过完善的 API 的设计和丰富的原生智能合约，简化开发者的准备工作，使开发者可以快速上手相应的开发工作。

- IPFST-Chain 提供一些常用数值操作，字符串操作等的基本库，以及一些链上查询，交易等的内置函数库，在智能合约中可以调用内置库。

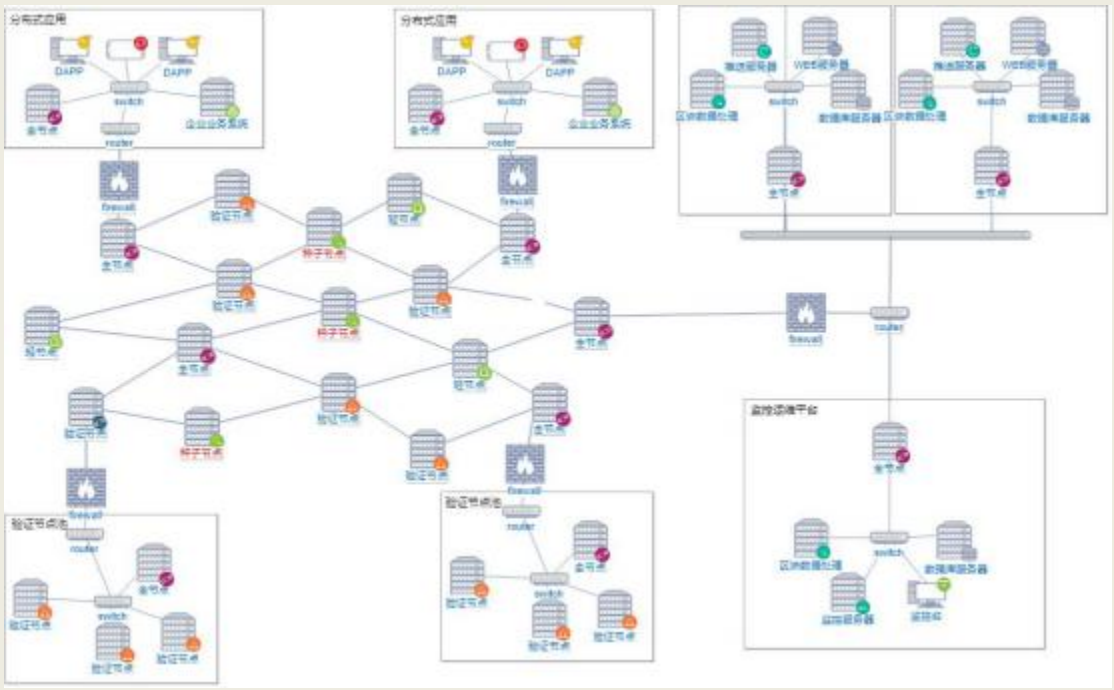
- 智能合约部署到链上后，除了可以被用户直接调用或者存取资产，还可以调用其他智能合约/内置原生合约，或被其他智能合约调用。

- 面向不同行业的 DAPP 应用，拥有不同的技术需求和侧重点。例如去中心化的社交、去中心化的存储和去中心化的游戏、去中心化的金融服务等，所需要的技术侧重点会有所不同。我们通过图灵完备 The New Standard of Value HCASH Foundation 2018 的智能合约，对行业 DAPP 深入探索后，慢慢会形成适用于该行业的 DAPP 标准，IPFST-Chain会不断将这些标准收录变为原生智能合约，方便开发者更加快速地迭代 DAPP。随着DAPP的产品化进程不断推进，我们希望普通互联网用户也可以真正进入区块链应用并感受到区块
链技术带来的价值。

- 后续 IPFST-Chain 将推出专属的带调试功能的 IDE，使得开发者既可以享受 IDE 带来的便捷，也可以在调试错误时更快地定位问题，从而大大提高 DAPP 的开发效率。

轻节点 、轻存储

目前主流主链在接入智能合约时，一个明显的弊端就是无法很好地做到资源隔离，随着生态的不断扩大，将不可避免地造成拥堵，例如以太坊就出现某个热门众筹导致整个系统拥堵的现象。



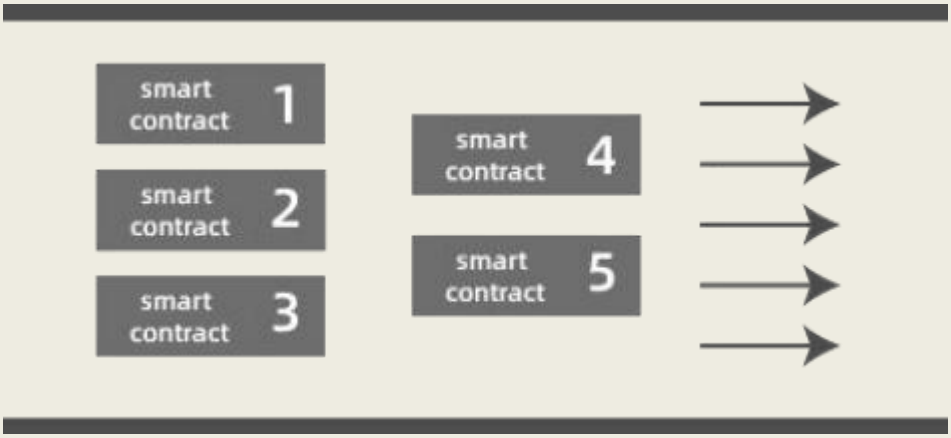
IPFST-Chain 链上每次调用执行智能合约时，都会先初始化一个独立的轻量级执行环：仅需要在链上查找到合约字节码，然后执行合约字节码；需要访问链上数据时，通过 native API 来调用，即不需要调用所有数据。在后续的开发中，IPFST-Chain 将继续完善相关技术，最终实现各 DAPP 的运行环境独立，互不影响。

每个智能合约有各自的独立状态存储区，称作 storage。合约交易的执行导致某个智能合约的状态存储区发生数据变化时（storage 改变），不会保留所有历史的 storage 的全量备份，而是只保存 storage 的当前状态和 storage 每次变化的变化量。

通过这样的设置，用户想要得到智能合约的执行结果时，可以很轻易地获取 storage 的当前值，而无需读取所有的数据，这样大大降低用户的工作量，也减少了节点的数据存储要求，节省了系统资源，提升了系统的处理效 The New Standard of Value HCASH Foundation 2018 率，还方便按 storage 的实际变化按需计算 gas。同时，用户也可以通过历史变化量还原或者回滚得到 storage 的每次历史的值。

并发模型提升效率

IPFST-Chain 通过把智能合约交易派发到并行的执行管道同时执行，能够提高大量合约交易并发执行的能力，缩短整体交易执行时间。



- 把一个出块时间内需要执行的智能合约，划分为到不同管道中执行。管道这里特指合约处理器，意味着不同的管道可以在不同的线程中同时进行合约执行。
- 管道分为串行管道和并行管道，不同并行管道可以并行执行，串行管道不能和其他管道并行执行，最多只有一个串行管道。
- 一个管道启动后，其中的智能合约交易串行执行。
- 先执行串行管道中的智能合约，再并行执行多个并行管道中的智能合约。
- 读取或者修改的账户或合约地址列表称作本交易的依赖地址列表。智能合约交易可以在客户端预先执行获取依赖地址列表。普通交易也有依赖地址列表。依赖地址列表有冲突的交易不能放入不同的管道。
- 交易中不预先附加依赖地址列表的交易，进入串行管道，但是提高手续费。
- 合约声明的依赖地址列表和实际执行的依赖地址列表有冲突时，执行失败，惩罚性收手续费并打包空白交易。
- 通过管道的并行执行，可以大幅提高（最少提高 4 倍）大部分场景下的合约交易 TPS。

POF 共识算法

在设计共识协议时，IPFST-Chain 链上价值流通网络生态系统充分考虑了以下因素：

- **性能**：IPFST-Chain 的首要设计目标是快速，为确保系统具有高吞吐、低延迟的性能表现，我们需要采用具有更高收敛速度的共识算法。
- **扩展性**：IPFST-Chain 是一个公共平台，向所有去中心化应用开放，因此，扩展性也是一个重要的考量因素。
- **安全性**：虽然 IPFST-Chain 的设计理念不是追求极致的安全性，但仍然需要确保足够的安全性底线，有效防范各类攻击。

对比现存的一些共识算法，POW 的安全性更好，在恶意节点的算力低于 50% 的情况下可以确保达成共识。但 POW 的收敛速度较慢，无法满足性能要求；POS 及其变种算法去掉了求解数学难题的步骤，提高了收敛速度和单次攻击成本，降低了能源消耗。但 POS 的扩展性仍然较差，而且 Nothing at Stake 问题较难解决；BFT 系列算法在安全性和性能方面有较好表现，但其扩展性是一个问题，通常比较适合于私有链或联盟链；DPOS 系列算法通过限制生成区块的权限，有效降低了伪分叉率，在性能和扩展性方面表现良好。相应的，DPOS 在安全性方面稍有牺牲，需要保证恶意节点数不超过 1/3。

综合来看，DPOS 算法在性能、扩展性方面有比较明显的优势，而 BFT 在安全性和性能方面有较好表现，因此，我们借鉴了 Tendermint 在 POS+BFT 混合共识机制上的思路，并在此基础上引入了更加高效、更具扩展性的 DPOS，形成新型区块链共识引擎 POF（Proof of faith）信仰证明机制，进一步提升 IPFST-Chain 网络的高速运转效率。POF 共识层具有高性能、高安全、高拓展、高并发、高一致性的特点。

多重激励层

一个强大的加密货币协议应该努力提供一个更合理的激励结构，在这个结构下维护系统中不同参与者的利益，以维持系统健康运行。

传统的点对点通讯网络将焦点关注于信息传输，有点像互联网 1.0 时代的应用用，一切都是公开和共享的，而其并没有达到区块链技术所达到的震动效应，一方面是因为缺少有效的共识机制将分散的节点协同参与工作（仅限于点和点的共识），而更重要的是因为一切人人类的行为都是需要背后的经济逻辑驱动的，在缺乏有效的经济规范趋势下人类的行为只能受到社会规范约束（即出于公益性质的精神激励的驱动下的工作），这对于大部分需要共同完成的目标而言对个体是缺乏约束力的。

比特币网络通过 POW（工作量证明）共识机制，并以贡献算力获得记账权从而获得比特币奖励的方式激励节点参与共识，无疑是一项了不起的设计，我们认为 Token经济模型是区块链价值的核心也不为过。

然而问题在于同一种 token是否能解决所有共识协同行为的激励问题？我们认为答案显然是 No。现今我们发现市场上有各种流通的 Token，背后的经济模型五花八门，但是缺乏统一的标准将其共识的成本与产生的共识价值关联起来，因此整个加密货币的二级市场流通规则显得相当脆弱。

以太坊基于同一种底层共识机制，允许智能合约开发者发行自己的 Token，并且使用 ETH 作为 GAS 费用用支支付共识成本，既统一了共识成本的计量量单位，又允许在相同的共识成本下，能够根据 Token所用于的生态获得不同的价值输出，使用者至少能够计算最佳的投入入与回报的平衡点，如今许多人诟病在以太坊上发行 ERC20 的代币太过容易导致鱼目混珠，却很少有人意识到以太坊在这个设计初衷的重要意义。

我们在设计整个 IPFST-Chain 时也同样延用了以太坊的这个功能，可以想像，通过链上完成基于共识的交易，首先我们需要降低 GAS 消耗，以降低链上交易性价比的硬门槛，为

此我们设计了新的多重激励机制。

假设在共识成本即 GAS 消耗可以忽略不计的情形下，任何一种 Token 的价值取决于链上交易的其他成本，这些成本受到数字资产的集中化程度、市场供需关系等影响，这和现实世界的货币并无不同，加密货币同样是用来衡量商品、服务或权益的价值的，因此我们认为开发者发行 Token可以有自己的经济模型。

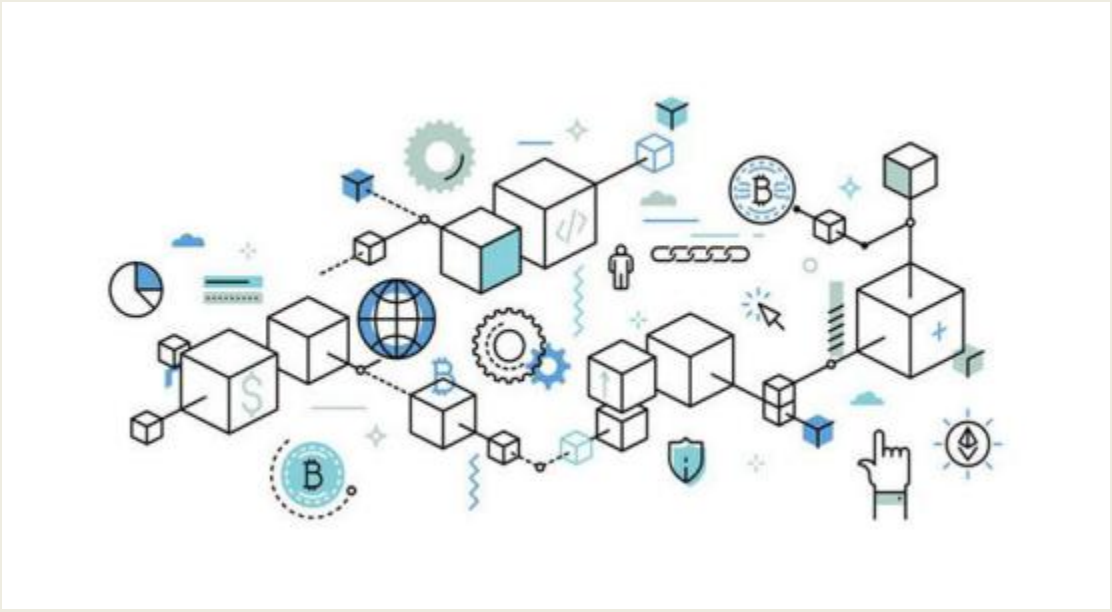
站在 IPFST-Chain 生态的角度，所有的商品、服务的价值都有一个源头，由于区块链平

台本质是一个公平的价值流通市场，因此所有的经济行为的成本底层在于交易成本，IPFST就是交易成本的载体，站在这个角度，IPFST 将用于以下激励用途：

- 记账奖励；
- 数据存储层奖励；
- 算力贡献奖励；
- 其它角色包括算法提供者（通过发布智能合约的形式）的运行激励；
- IPFST-Chain生态的开发者会因其开发应用的实际产生价值而获得 IPFST 的 Token奖励，这种奖励往往用于实际补贴其共识记账或算力支付开销的成本方式给出；
- 用户也可以将 IPFST 的 Token用于其 DApp 或 IPFST-Chain 相关的生态系统中的各种目的。

IPFST-Chain 超级账本

分布式超级账本技术是建立在一系列让参与者能够以高效的、安全的方式创建、传播和存储信息的数据库网络。通过该网络，任何参与方不需要各方皆知并信任的中心节点或中心管理人就可以顺畅、安全的进行上述操作。并且可以对整个信息变更历史进行审计和检查。此外，任何人在未经授权的情况下，改变信息及其变更历史，基本上是不可能的。换句话说，超级账本技术操作在设计上要求通过网络存储和传递的信息具有高度的可信赖性，并且网络中的每个参与者可以同时访问公用信息。



IPFST-Chain 超级账本是构筑各行业区块链的基础设施。可以类比 mysql、oracle、db2等，他们本身不是数据库，而是数据库管理系统（dbms）。用户在 dbms 之上可以通过 简单的操作，快速构造出符合自己商业应用需求的关系型数据库。相同的，通过 IPFST-Chain超级账本，人们可以非常方便的编写智能合约，快速定制出符合行业规格需求的区块链应用系统。它的优点在于非常方便搭建超级账本云。在单个超级账本网络环境下，也可以支持海量区块，促使众多中小企业一键链改成为可能。

IPFST-Chain 跨链协议

IPFST-Chain 的跨链协议突破了传统跨链只能进行资产转移的思维定式，将重要个人身份相关的行为数据也进行跨链同步与迁移，通过同态加密进行安全保护与使用。

根据不同需求，IPFST-Chain 采用同构与异构两套跨链方案，以应对不同架构下性能和成本的平衡：

o 同构跨链：IPFST-Chain 主链与子链之间通过轻量化同构跨链协议相互连接，用户可以通过钱包即时看到不同跨链平台之间的状态变化。

o 异构跨链：分布式私钥控制技术将 IPFST-Chain 体系之外的链甚至传统平台跨链连接

到 IPFST-Chain 生态中，达成安全的异构跨链，将数据协议的应用范围拓展到多种平台。

基于同构与异构两种跨链技术，将处于不同 DApp 的 Token和数据均通过跨链技术集成在主账户中，形成一个多层次、立体化的用户数据列表。

除此之外，IPFST-Chain 也在考虑将合作伙伴的用户行为也进行数据化，在跨域要求的 安全性控制条件下将数据扩展到各个不同的系统，使数据走出区块链的范围，形成广域数据生态。

分布式私钥控制

分布式私钥控制通过去中心化技术，将跨链资产用多个私钥加以控制，原持有者仍然拥有所有权，只是其单一私钥不能取出资产而已。想要回归资产，需要向对应链加以申请获得足够私钥。

举例，用户 Alice希望能够将 1 个原链币转成另一链币。跨链的若干节点（分片/超级代表委员会都可以）在原链上维护一个多签账户，将私钥分割且分别控制，任何单一节点不能取得这 1 个原链币，只有获得足够的私钥才能获得 1 个原链币的控制权。

当 Alice将 1 个原链币打到跨链掌控的多签账户时，在跨链相应的同步放出等同于 1

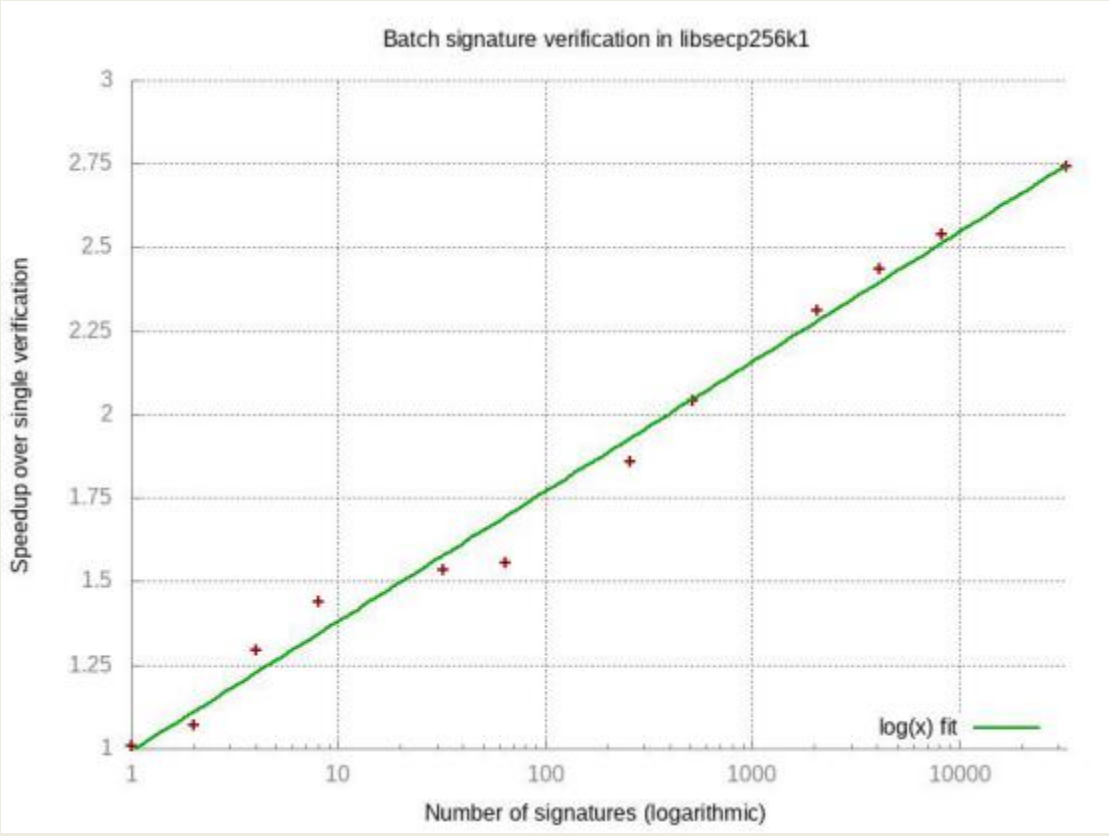
个原链币的跨链币，再和持有已将另一链币转化等价跨链币的节点进行交易。当 Alice需要将跨链币重新转回到原链时，需要先将跨链上的资产锁定，然后再原链中将同等数量的原链币释放。分布式私钥控制过程安全性较好，同时因为在跨链上放出代币，所以支持智能合约特别是多币种复杂合约，不受原链本身是否能进行智能合约影响。

IPFST-Chain **隐私保护设计**

Schnorr 多重签名

IPFST-Chain 引入了基于多重签名的 PBFT 机制。传统 PBFT 协议需要参与者将信息的签名传给 Leader，然后 Leader 将这些签名放进区块头。但存储多个签名将增加区块头的大小，影响网络传输效率。IPFST-Chain 使用了基于 Secp256k1 椭圆曲线的 Schnorr 多签名算法，明显提升了区块链效率。

BIP-Schnorr 签名中对 Schnorr 签名性能的测试结果如下：



不同于其他签名形式，Schnorr 多重签名最终只产生一个签名，大大减小了签名的长度，从而减小了区块头大小，减轻了存储开销和网络传输开销。

另外，当未来需要增强隐私性交易需求时，除了环签名之外，Schnorr 签名亦可提高隐私性。

同态加密与隐私保护

IPFST-Chain 链的运行过程中，必然会遇到将信息传递给第三方的情况——如内部的智 能管道和外部的数据共享。在这些过程中，有可能会出现用户隐私在环节内被泄露等情况，不利于用户的 ID 安全。为此，IPFST-Chain 采用同态加密的方式，在用户认定为隐私的信 息进行数据处理中， 保护数据本身的隐私安全。

同态加密使用的 Paillier 算法 12，即基于二次整数群的 n 次剩余类方法进行加密。

对于原始信息 m∈(0,n),选择随机数 r∈(0,n),根据生成的密钥对：公钥(n,g)私钥(λ,u),进行加密，C=gmrn modn2 得到密文 C。

密文 C 满足加密同态和混合乘法同态性，即：

o 加法同态性

D(E(m ,r)E(m ,r) mod n2)=m +m mod n D(E(m ,r)gm2 mod n2)=m +m mod n

o 混合乘法同态性

D(E(m ,r)m2 mod n2)=m m mod n

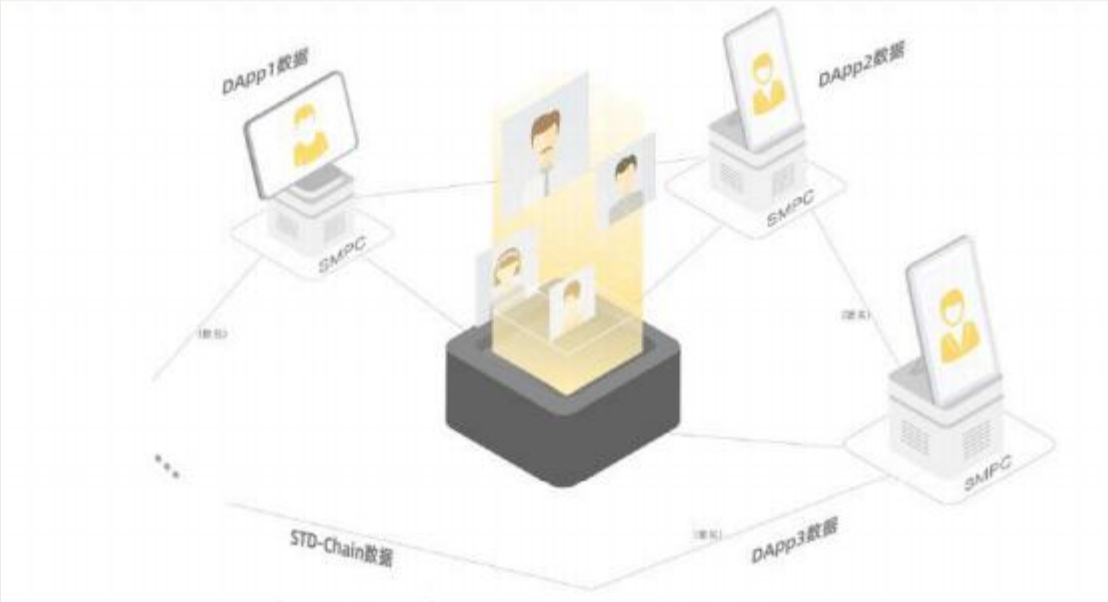
从而在加密后可以进行多种数据处理，将处理结果返回给用户，用户用私钥解密就能得到与明文数据处理相同的结果，而不存在数据泄露的可能。

在此之上，还可以进行同态加密签名，在内容中加入同态签名，在数据处理过程中得到是否发生误处理及欺骗等行为，确保自身数据得到正确的处理。

安全多方计算

在分布式私钥控制与环签名等涉及多人共同分享秘密的过程中，需要遵循尽可能不出现完整秘密的原则，故 IPFST-Chain 选择安全多方计算以保护数据安全，仅当用到时出现完整信息。

安全多方计算解决的是以下问题： n 个人分别持有隐私 x1，x2……xn，共同计算特定函数 y=f(x1,x2,……xn)，同时 n 个人无法得知其他人的隐私。考虑到现实中存在恶意节点会竭尽所能获取其他参与方的隐私信息。安全多方计算协议要求不论参与者是否有恶意，所有参与方都无法获得输出结果以外任何的附加信息。



IPFST-Chain 考虑通过同态加密、bulletproof14 等措施进行安全多方计算，以数据计算为例。IPFST-Chain 使用安全多方计算对各个 DApp 及 IPFST-Chain 中的重要数据进行加 密，即使传输中的数据被泄露，用户的原始数据也是安全的。安全多方计算也保证了传输数 据的双方能安全的加密和解密数据。同时在 IPFST-Chain 上，用户在每个 DApp 上的公钥，地址及数据都是相互独立且不可见的。

五、IPFST-Chain 经济模型

一个理想自由市场金融体系应当允许参与各方在最小化风险和成本的前提下，对价值进行存储、交易和转让。在基于比特币首次所提出具有开创性的开源协议之上，我们进行了改进和扩展，重新定义了一个新的名为 IPFST 的数字通证，以用来实现一个理想自由市场金融 体系。

IPFST 总发行数量是 1 0 0 亿 枚，IPFST 的运作方式类似于比特币，但是一些优化和新的规则能够让 IPFST-Chain 来支撑其价值。

IPFST-Chain 除了拥有比特币的所有特性以外，还提供了一些新的特性使得持有 IPFST 玩家可以获取一定数量的红利，这些红利来自于挖矿奖励和交易费用的一部分，会奖励给每个区块，并且以一种不增加网络负担的方式分发。

IPFST 价值基础

IPFST 是 IPFST-Chain 上的原生资产，IPFST 的价值起源是其能够方便地表征和度量 IPFST-Chain 上数字化经济活动。IPFST 的价值基于两点：一是使用 IPFST-Chain 上的应用需要消耗一定量的 IPFST 作为燃料；二是持有 IPFST，能够参与到比原链治理。

六、团队介绍

Goh Kheng Hee，Dani el 创始人

新加坡南洋理工大计算机系毕业，5 年区块链开源项目经验， 具有区块链思维，熟悉区块链产品设计及研发流程；熟悉 适用场景，熟悉区块链的底层运作机制和实现原理；熟悉 跨平台开发管理工作，精通 C++语言，熟悉 QT，对共识机制，P2P 通信，密码 学等相关技术有着深入的研究；具有良好的项目管理能力、组织协调能力和沟通 能力；具备全面的市场营销、客户管理、风险管理、团队建设等领域知识；

Pavel Bains 首席执行官/联合创始人

负责整体项目发展与规划，拥有超过 10 年的团队管理经验，以及超过 6 年的创业团队管理经验。精通区块链金融，金融科技、互联网金融等新兴产业，具有完备的业务规划和投资管理能力。曾就任于世界 500 强科技公司 IBM；2013 年涉足区块链领域创业，先后领导 3 家区块链领域公司成功上市；曾在 Kochava, Inc 担任 SVP，负责公司区块链布局。

Neeraj Murarka 首席技术官/联合创始人

Neeraj 负责项目的区块链结构设计，精通各类主流共识算 法；熟练掌握区块链系统开发语言，是具有 20 多年经验的工程师 和计算机系统架构师，对区块链技术有着丰富的技术运营经验。从 2012 年起多次进行区块链技术创业，先后参与 2 家交易所上市和 1 家数字钱包项目上市。他曾在 Google、IBM、Hewlett Packard、Lufthansa、Thales Avionics 等工作。

首席运营官/联合创始人:РУСЛАН ВЯЧЕСЛАВОВИЧ

负责项目全球营销策略,洞察全球市场机会，制定营销策略，带动项目及品牌影响力。拥有 12 年以上的 500 强公司营销管理经验，曾帮助多家创业公司成功完成品牌形象转 38 型。精通互联网、 电商以及金融科技领域品牌管理。曾在 USWeb 等创新性互联网公 司工作，具备丰富实战经验，多次成功塑造品牌影响力。

核心技术开发人员:РУСЛАН ВЯЧЕСЛАВОВИЧ

具有丰富的开发和管理经验，他在不同的初创公司到大型公司从事过高级开发者到研究部门总监，他工作过的公司包括 Captaris，Teamplate，Vertical Technologies 他具有十多年的开发经验，涵盖了各种各样的技术，包括前端 UI、后端服务、复杂的多层系统以及单个用户应用程序。他一直十分重视创新和新技术的采用，特别是推动数据可视化、建模和模拟的技术，作为帮助用户理解他们与之交互的系统的工具。他拥有新斯科舍技术大学的计算机科学学士学位 。

核心技术开发人员:АЛЕКСАНДР АНАТОЛьЕВИЧ

一名 Linux 开放源代码和加密货币爱好者，拥有巴尔的摩大学（University of Baltimore）的金融学位。 Synereo核心团队的成员，从事的工作有系统管理，市场营销，网站开发和托管。他曾担任 AEGON 和 Kroll 的微软系统工程师（MCSE），Fortress Technologies（现为通用动力公司）计算机安全专家。

七、风险提示

您承认并同意购买 IPFST，持有 IPFST 以及使用 IPFST 参与 IPFST-Chain 网络存在不可预知的风险。在最坏的情况下，这可能会导致购买的全部或部分 IPFST 的损失。

不确定的法规和执法行为

许多司法管辖区的 IPFST 和分布式账本技术的监管状况尚不清楚或未得到解决。虚拟货 币的监管已成为世界所有主要国家监管的主要目标。无法预测监管机构如何，何时或是否应 用现有法规或制定有关此类技术及其应用（包括 IPFST 和 IPFST-Chain 网络）的新规定。监 管行为可能会以各种方式对 IPFST 和 IPFST-Chain 网络产生负面影响。如果监管行为或法律法 规的变化使其在此类司法管辖区内运营非法，或在商业上不希望获得运营所需的监管批准， 基金会（或其附属机构）可能会停止在某一辖区的运营。在这样的管辖权。在咨询了广泛的 法律顾问并持续分析虚拟货币的发展和法律结构之后，IPFST-Chain 团队将对销售 IPFST 采取 谨慎的态度。 因此，为了销售令牌，IPFST-Chain 团队可以不断调整销售策略，尽可能避免 相关的法律风险。对于数字通证销售，IPFST-Chain 团队正与国际相关律师事务所合作。

信息披露不充分

截至目前，IPFST-Chain 网络仍处于开发阶段，其设计理念，共识机制，算法，代码及其他技术细节和参数可能会不断更新并经常更新和更改。虽然本白皮书包含了与 IPFST-Chain 网络有关的最新信息，但它并不完全完整，可能仍会由 IPFST-Chain 团队不时调整和更新。

IPFST-Chain 团队没有能力也没有义务向 IPFST 的持有人通报关于开发 IPFST-Chain 网络项目的每个细节（包括开发进度和预期里程碑），因此信息披露不足是不可避免的和合理的。

竞争对手

各种分散应用程序迅速崛起，行业竞争日益激烈。有可能建立替代网络，利用 IPFST 和/或 IPFST-Chain 网络的相同或相似的代码和协议，并尝试重新创建类似的设施。IPFST -Chain网络可能需要与这些替代网络竞争，这可能对 IPFST 和/或 IPFST-Chain 网络产生负面影响。

人才流失

IPFST-Chain 网络的发展取决于现有技术团队和专家顾问的持续合作，他们在各自的领 域都非常有知识和经验。任何成员的损失都可能对 IPFST-Chain 网络或其未来发展产生不利影响。此外，团队内部的稳定性和凝聚力对 IPFST-Chain 网络的整体发展至关重要。团队内部的冲突和/或核心人员的离开可能会发生，从而对未来的项目产生负面影响。

未能发展

IPFST-Chain 网络的开发将不会执行或实施按计划出于各种原因，包括但不限于任何数字资产，虚拟货币或 IPFST 价格下跌，不可预见的技术困难以及活动开发资金短缺。

安全漏洞

黑客或其他恶意团体或组织可能会尝试以各种方式干扰 IPFST-Chain 和/或 IPFST 网络， 包括但不限于恶意软件攻击，拒绝服务攻击，基于共识的攻击，Sybil 攻击，smurfing 和 欺骗。此外，第三方或 IPFST-Chain 会员或其分支机构有可能有意或无意地将弱点引入 IPFST或 IPFST-Chain 网络的核心基础设施，这可能会对 IPFST 或 IPFST-Chain 网络产生负面影响。 此外，密码学和安全创新的未来是高度不可预测的，密码学或技术进步（包括但不限于量子计算的发展）的进步可能会给 IPFST 和 IPFST-Chain 网络带来无效的密码共识机制，支撑该区块链协议。

其他风险

上面简要提及的潜在风险并非详尽无遗，并且与您购买，持有和使用 IPFST 相关的其他 风险（如条款和条件中更加具体的规定），包括那些 IPFST-Chain 无法预料。这些风险可能

会进一步实现为意料之外的变化或上述风险的组合。您应该对 IPFST-Chain 数，其分支机构和 IPFST-Chain 团队进行全面的尽职调查，并在购买 IPFST 之前了解 IPFST-Chain 网络的总体框架，使命和愿景。