# DP Coin 技术白皮书

语言版本：简体中文
翻译人员：帕萨卡尔彼

目录

# 1.DP 项目介绍

## 1.1 关于 DP Coin 项目

DP Coin 项目是由 DP 社区团队研发的的区块链技术公链，是一个去中心化、 支持 Pos 挖矿，可实现 DAPP 在技术层面上的应用扩展的系统，本质上等同于平行扩展的传统区块链系统，但是能够无限的扩展，在项目使用的技术上领先 ETH，在系统安全性上较比特币更胜一筹，私钥长度将达到 2 的 64 次方长度。 基于 DP Coin 所建立的平台可以将区块链技术服务于去中心化金融 Defi，去中心化交易所，去中心化社交，私密通讯，游戏支付等产品。通过区块链网络连接全球服务商与用户，以去中心化金融 Defi 和社交娱乐为切入口构建基于可信任并且安全的区块链生态。未来的 DP Coin 平台是一个资金流、信息流、价值流多重平台，在 DP Coin 平台上构建的信任价值体系中，各式各样的人或物将自我价值通过区块链网络进行传递，形成丰富的价值互联网络生态，这最终将极大地提升社会生产效率。

## 1.2 项目概览

区块链系统发展到如今，交易速度成为了区块链产业化如 DAPP、物链网、可信任数据交换等进一步发展的瓶颈。BTC/BCH 等纯粹通过增大区块大小而达到扩展目标，此方法手段不可取。另外通过 BTC/ETH 子网络的方式如闪电网络，跨链等技术其实是在牺牲安全性的前提下提高 TPS，同时必须具备更多的附带条件（如交易双方必须同时在线，需要抵押等）才能交易。因此我们需要一条全新的链来解决上述问题，只有通过 DP Chain 所打造的全新公链，才能在保证系统安全性的同时，提高 TPS，并保证区块的大小不至于超越系统的边界，降低系统基本功能实现时需要解耦的附带条件。

从最早的 IOTA 至今，DP Chain 有一个自己的原创性，具备创新性且全新的数据分块式中心一体化的结构性算法---区块融合算法，可以在保证高 TPS 的同时，解决链上拥挤的问题，促进项目的应用落地实施，而跟目前主流 BTC/BCH， Ethereum 等主流 PoW 币区块必须同一时间 Pending 住交易然后挨个打包，不同节点打包交易区块互斥（虽然 Ethereum 有 GHOST 和 Uncle Block 机制，但远远不够）所有不同。 相当于高速公路只有一条出口，不管道路有多少条，行驶车辆有多少，最终只有一条出 口。

而出口速度决定了车流量，后面只能排队。通过 Epoch 周期产生一个稳定主单元 MC，通过 DP Chain 独有的算法将其链接在一起，从主单元角度形成类似比特币链式结构。系统中每个组成部分都可以分成独立 Partition，互不干扰产生交易而后进行交易块融合，能够实现扩展性能的基本条件。在这个结构中，双花检测迟早能成功，在全局角度算法是稳定一致的。一旦一个节点可以看到某个 Epoch 的全局数据，加上一个稳定一致排序算法那么双花检测就会成功。

## 1.3 系统结构

DP 系统在计算机领域的算法研究中，又有 DP 算法一称，而 DP Coin 及其附带的 DP Chain, 其中所采用的算法, 我们将会全部使用 DP 算法实现。在区块链领域，后一个生成的区块是基于前一个区块以及当前链上数据的状态产生的，因此我们通过 DP 算法，控制一定的区块生成规律，那么就可以通过高速的算法控制来实现块的高速生成以及链上交易处理时的验证和签名，这对于系统本身来说是及其具备代表性意义的。而我们对于 DP 的严格定义为：如果给定某一阶段的状态，则在这一阶段以后过程的发展不受这阶段以前各段状态的影响。

我们认为以 Luna 为代表的算法稳定币是极其失败的。算法本身的作用不在与实现货币价格的锚定和稳定机制，算法应当是深入区块链底层设计，融合系统架构及其设计思路，通过算法实现优秀的货币及其链上数据处理能力的综合提升，这对于代币质量有着至关重要的帮助。

从数学角度来看，对于动态规划问题而言，f(n)的定义就已经蕴含了“最优”。利用 f(n)的最优解，我们即可算出 f(n+1)的最优解。大问题的最优解可以由小问题的最优解推出，这个性质叫做“最优子结构性质”。

我们的系统结构需要满足最优子结构的性质，因此，系统需要在底层实现彻底的重构。

无论是 DP 算法还是其他算法，我们实现的目的都是在可能解的空间寻找最优解，同样的，对于传统加密技术而言，无论是对称加密算法还是非对称加密算法，在量子技术到来的未来，都将面临毁灭性的打击，而通过算法实现安全性保证的区块链技术将会在这种暴力打击中得到生存的空间。

虚拟货币具备的虚拟特性需要通过算法来保障这个特性的实现，而密码学不过是计算机科学中的一部分，无法完全通过密码学来保障一个信息系统的绝对安全。

我们需要更多可能的途径。

## 1.4 节点验证和确认

DP Chain 的网络是一个高吞吐量、低延迟、可配置的拜占庭容错弹性区块链网络，该网络最初的应用场景会作为波场链区块链的侧链。在这种情境下，它可被称为“弹性侧链网络”。 网络中的侧链由一组从网络节点集合中选出的虚拟子节点所运作，同时它们占据每个节点计算与存储资源的 全部或一部分（多租户）。每一个侧链都是高度可配置的，用户可自由选择侧链的规格、共识协议、虚拟机、 母链以及额外的安全措施（例如，虚拟子节点的轮换频率）。

DP Coin 通证是一种实用型与功能性通证。为获得在网络中工作的权力，节点必须通过一系列智能合约（也被 称作 DP 管理员）来运行 DP Coin 的后台程序。一旦某个节点被网络承认以后，就会随机选出 24 个对等节点来审查它的运行时间与延迟——这些指标会被定期提交给 DP 管理员，进而影响节点参与网络的奖励。

创建一个弹性侧链时，用户会指定他们所需要的区块链配置，并根据他们计划租用运行区块链所需网络资源的租期支付费用。如果网络有足够的带宽，满足区块链指定配置计算与存储要求的节点就会作为虚拟子节点参与网络。 弹性侧链的虚拟机的兼容性可以让用户在侧链上直接部署他们现有的、基于波场链的智能合约。

为了成为系统的一个节点，潜在节点必须运行 DP 系统的后台程序，这会评估该潜在节点，以确保它满足网络硬件要求 。如果潜在节点通过了此验证步骤，后台程序会允许它向 DP 系统管理员提交加入网络的申请。

申请会包括所需的网络保证金以及由后台程序收集的节点元数据（如 IP 地址、端口、公钥等）。申请提交至主链后，潜在节点会加入到系统中，成为“全节点”或“轻节点” 。全节点会为某一个弹性侧链提供其所有资源，而轻 4 节点则会参与到多个弹性侧链中（多租户），主系统再在每个网络周期，一次性把这些指标提交给 DP 系统管理员，这些指标决定了节点的奖励。

这里的链在未来将会全部由 DP Chain 链取代。

当节点退出网络时，它必须首先广播它们退出的消息，再等待一个终止期 。终止期结束后，节点处于闲置状态，并可从网络中取回其最初质押的保证金。 如果用户无法等待终止期结束，而立刻从网络中退出，它会被 DP

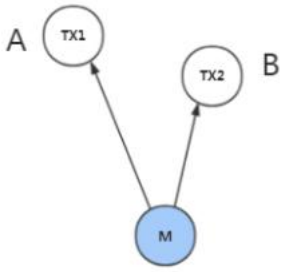
虚拟子节点划分为不良（死的）节点，那么该节点无法获得奖励，并且随后会被移出区块链。

基于上述节点的节点描述，资产划分也同样满足上述规律。

# 2.DP Chain 的介绍

## 2.1 简单区块结构

主块 M 引用了两笔交易 TX1 和 TX2，并且经过 PoS 节点 A，B，C，D 签名确认。




如果我们使用 Json 格式来描述一个简单主块引用且经过了 PoS 节点签名的结构则：

```
{
    "block":{
          "hash": "HASHINFO",
        "time": "TIMESTAMP",
          "type": "1",
        "diff": "THIS diff",
        "owner": "OWNER ADR OR PUBKEY",
          "nonce": "NONCE INFO"
    }
    "Signers": ["A"],
    "Signinfo": "SIGN CONTENT",
    "sign":"SIGN"
}
```

## 2.2 用户账号模型

跟传统交易系统一样，DP 系统使用余额账户模型。每一个 DP Chain 的生命周期和共识周期处理发现某个 TXBlock 之 OUTPUT 账户不存在，则全网创建此账户。并将 INPUT 的 Amount 转 入此账户中，而 INPUT 需存在且余额足够。 每个账户余额由交易单元 INPUT 和 OUTPUT 之差决定。在某个生命周期中，从创世块至该时刻，账户余额 Balance = All(INPUT) − All(OUTPUT。每个交易单元由 INPUT 方用 ECDSA 私钥签名，用 INPUT 公钥进行验证块合法性。

系统保证每笔 Transcation（后面称 TX）经状态机处理为幂等性，即交易 TX 执行一 次和执行多次最后结果都为一样。

修改余额时需并发加锁，系统每个过程和函数都需具备可重入性。于是乎，账户余额修改跟状态机一样，不管流入多少笔交易，又或者多少 次重复交易，其最终结果都为一致。判断是否为重复交易即根据交易 TX 之随机数 Nonce 值，除了 Nonce 一样，整包 hash 值一样称之为重入成功，反之称为重入失败，系统对这两种情况分别处理。

同时账户表中，每个账户会有一个 Nonce 字段，用于检测每个转出交易的重复交 易，但如果重复交易在不同池子中，经过稳定排序，优先高的块先执行，优先低的块不 存储实际块，只存储哈希。 后续更新块时，先更新优先级高的块，只有哈希没有实际块的交易，之前一定会存在重复交易，要检查这种情况。

用户在每次交易中，将会产生一个完全随机的哈希值信息，这个哈希值信息就是交易哈希信息，交易哈希信息在传统以太坊和波场链中都会存在，并以 transhx 的形式存在。

用户在 DP 系统中注册的账号将会当 DP Chain 系统正式网上线运行时，通过 DP 网络投入使用，DP 网络会为系统中的每个用户分配地址信息和私钥信息，这个信息都是基于 DP Chain 产生的，因此具备 DP Chain 的安全属性。

## 2.3 DP Chain 的应用

应用层作为最终呈现给用户的部分，主要作用是调用智能合约层 的接口，适配区块链的各类应用场景，为用户提供各种服务和应用。

数字货币分散了货币发行和存储的权力，智能合约分散了代码执行与验证的权力，数字签名确保了用户资产所有权， 基于此，开放金融雏形逐步

显现。

开放金融基于用户对网络和数字签名的信任构建而成，资产所有权被遍布在全球各地的节点和网络守护，资产确权的过程被简化为机器算法。用户能够在无中介的情况下通过与智能合约交互，进行资产操作与交换，极大的提高了金融服务效率。

如果说以太坊整合了 DeFi 模块，让金融应用像积木一样在原有的基础之上持续构建创新，应用链则是将应用和产品剥离打散，分散到不同的链载体之上。

以太坊就像一台互联网大型机，集中解决了底层的共识、初始用户、数据和代码，但日渐臃肿。

应用链则更加分散，产品与产品之间相对割裂，需要依赖标准来完成服务与服务的组合。

同样，全栈应用链作为新的方案并非完美，仍然需要解决很多实际的问题，新项目和应用链的融资面临较多问困难，生态中基础服务与配套工具不完善，初始用户进入门槛和以太坊用户的迁移成本较高，早期代币流动性不足，共识网络难以形成等等，都制约了应用链的普及和跨链生态的发展，开放金融基础设施的迭代和构建并非一帆风顺。

而 DP Chain 尝试在集中的大型计算机与独立全栈应用链之间寻找一种平衡，解决现有区块链应用底层设施的问题。

从经济层面考虑，降低成本，是区块链技术的一个重要的设计思想。在区块链体系中，参与者可以不需要了 解对方基本信息的情况进行交易，实现了“无需信任的信任”，改变了传统模式中以第三方为 中心的信任模式。这种设计模式有许多创新性，其中两项值得关注：第一，交易信任由机器和算法确定。区块链通过构建一个依赖于机器和算法信任的交易体 系，解决在匿名交易过程中的相互信任问题。所有参与者将在无须建立信任关系的环境中，通 过密码学原理确定身份，依靠共识机制实现相互间的信任。 第二，交易过程可以由程序自动执行。区块链通过可编程的智能合约，自动执行双方所达 成的契约，排除了人为的干扰因素，从制度上防止任何一方的抵赖。从而推动经济社会进入一 种智能的状态，实现当前经济交易系统的质的飞跃。 基于区块链技术的“弱中心化”特性，现有的经济体系可以脱离当前通过制度约束或第三 方机构背书，双方直接实现价值交付。这种“弱中心化”特性可以有效降低交易成本，提高交 易效率，减少因交易一致性所引发的摩擦。

通俗的说，区块链可以看成是一套由多方参与的、可靠的分布式数据存储系统，其独特之 处在于：一是记录行为的多方参与，即各方可参与记录；二是数据存储的多方参与、共同维护， 即各方均参与数据的存储和维护；三是通过链式存储数据与合约，并且只能读取和写入，不可 篡改。 在应用实践中，这种系统能够实现所有参与者信息共享、共识、共担，可以成为各种商业 行为和组织机构的基础技术架构。

## 2.4 DP Chain 的核心技术

区块链技术不是一个单项的技术，而是一个集成了多方面研究成果基础之上的综合性技术 系统。我们认为，其中有三项必不可缺的核心技术，分别是：共识机制、密码学原理和分布式 数据存储。

第一，共识机制

所谓共识，是指多方参与的节点在预设规则下，通过多个节点交互对某些数据、行为或流 程达成一致的过程。共识机制是指定义共识过程的算法、协议和规则。 区块链的共识机制具备“少数服从多数”以及“人人平等”的特点，其中“少数服从多数” 并不完全指节点个数，也可以是计算能力、股权数或者其他的计算机可以比较的特征量。“人 人平等”是当节点满足条件时，所有节点都有权优先提出共识结果、直接被其他节点认同后并 最后有可能成为最终共识结果。

第二、密码学原理

在区块链中，信息的传播按照公钥、私钥这种非对称数字加密技术实现交易双方的互相信 任。在具体实现过程中，通过公、私密钥对中的一个密钥对信息加密后，只有用另一个密钥才 能解开的过程。并且将其中一个秘钥公开后（即为公开的公钥），根据公开的公钥无法测算出 另一个不公开的密钥（即为私钥）。

第三、分布式存储

区块链中的分布式存储是参与的节点各自都有独立的、完整的数据存储。 跟传统的分布式存储有所不同，区块链的分布式存储的独特性主要体现在两个方面：

一是 区块链每个节点都按照块链式结构存储完整的数据，传统分布式存储一般是将数据按照一定的 规则分成多份进行存储。

二是区块链每个节点存储都是独立的、地位等同的，依靠共识机制保证存储的一致性，而传统分布式存储一般是通过中心节点往其他备份节点同步数据。数据节点 可以是不同的物理机器，也可以是云端不同的实例。

## 2.5 DP Chain 的发展趋势

区块链将对现有的经济社会产生巨大的影响，有望重塑人类互联网活动形态。

对于区块链近期的发展趋势主要有以下几个方面：

第一、应用模式升级。

鉴于公有链的安全性及交易量与日俱增对现网容量之间的平衡问题，未来区块链的应用领域将以联盟链、私有链或混合链为主。比特币模式增加了区块链网络的维 护成本，对于低价值、低风险的交易来说并非完全适用。考虑到效率及安全的提升，未来将是 以联盟链、私有链、或由联盟链和私有链组成的混合链组成。

第二，多中心化。

未来区块链系统架构将是构建可信任的多中心体系，将分散独立的各自 单中心，提升为多方参与的统一多中心，从而提高信任传递效率，降低交易成本。即在信息不 对称、不确定的环境下，建立满足各种活动赖以发生、发展的“信任”生态体系。

第三，从金融创新带动其他行业应用突破。

区块链的应用领域将先从对交易各方有相互建 立信任的需求，但又不容易建立信任关系的领域切入，如金融、证券、保险等领域。随着应用 普及和社会认知度的提高，区块链将逐渐向社会各领域渗透。比如区块链已经初步的应用于政 治选举、企业股东投票、博彩、预测市场等领域。

第四，智能合约的社会化。

未来，所有的契约型的约定都实现智能化，利用智能合约可以 保障所有约定的可靠执行，避免篡改、抵赖和违约。除了将社会中的有形资产转变为数字智能 资产进行确权、授权和实时监控外，区块链还可应用于社会中的无形资产管理，如知识产权保护、域名管理、积分管理等领域。

# 3.DP Coin 介绍

## 3.1 整体经济规模及趋势

当前，区块链经济处于爆发期前夜。

金融行业应用已经相对广泛，其他行业的应用情况也进入了探索研发阶段。就这种新型经济形态未来体量，有测算如下：

据达沃斯论坛创始人克劳斯·施瓦布（Klaus Schwab）认为，区块链作为继蒸汽机、电气 化、计算机之后的第四次工业革命的重要成果，预计到 2025 年之前，全球 GDP 总量的 10% 将利用区块链技术储存。

根据市场研究机构 Gartner 预测，2020 年，基于区块链的业务将达到 1000 亿美元，除 金融业外，制造业和供应链管理行业将为区块链带来万亿美元级别的潜在市场。

研究咨询公司 MarketsandMarkets 在专题调研报告 1 中预测，2016 年至 2021 年之间， 全球区块链市场应用和方案供应商的复合年均增长值将达到最高。

这类供应商的业务包括支付、文件证明、交易和其它用于提高企业运作效率的方案。 在区块链技术所涉及的行业中，银行、证券业和保险业所占市场份额最高。未来，区块链 技术主导下的娱乐和媒体行业发展速度将持续加快，医疗健康、物联网、供应链等行业应用则紧随其后。

因此，DP Coin 需要通过这次产业变革，抓住时代机遇，来打造一款跨时代的经济体系，成为时代的产物。

## 3.2 DP Coin 代币规模及其分配

· 总量：10 亿

· 40% 社区空投和邀请奖励

· 20% 质押挖矿和节点奖励

· 5% 早期生态建设

· 5% 项目储备金（锁定）

· 15% 社区开发人员

· 10% 项目组成员

· 5% 社区活动和项目活动保留

## 3.3 DP Coin 价格建设方案和预测

· 2023 Q1-Q2 DP 系统开发和搭建。

· 2023 Q3 DP 系统正式投入使用，开始 DP Coin 空投行动和 DP 系统性活动。

· 2023 Q4 预测用户量突破 100 万，启动邮箱账号验证程序和质押挖矿系统。

· 2024 Q1 开放 DP 系统转账功能和系统回收功能，官方回收价格预测将会持续保持为 1USDT:1 DP Coin。

· 2024 Q2 通过投资商和用户群体，进入全球前十大交易所，并逐渐提高项目组回收价格，同时保证不低于 0.3 USDT，实现价格硬锚定。

· 2024 Q3 DP Chain 主网正式运行并开源，开放投票系统。

· 2024 Q4 DP 项目进行去中心化管理，由社区接管。