



# DIPPER

# 白皮书



重定义交易服务与资产管理的全球第一 DAM 平台



# 摘要

## 》》一个完备的去中心化金融生态公链

一些观点认为 2018 年是区块链落地元年，2020年是区块链商用元年：事实证明这些看法忽略了技术发展事实，以及应用落地的难度。虽然今年整个行业在应用和场景层面，并没有出现“爆款”，但不可否认的是，DeFi无疑是2020年区块链技术在应用领域的最大亮点。

区块链技术天然更适合应用在数字化等线上虚拟场景，并且经过多年的发展，无疑金融相关的应用生态是最繁荣和旺盛的。但是，由于数字货币炒作、ICO、 以及一些低质项目的操作，导致用户对“区块链+金融”与数字货币、ICO、“割韭菜”等划上了等号。这无疑是不利于技术发展和应用探索的。DeFi 的出现，适时的将一些正向的、有价值的“区块链+金融”应用和探索，从传统概念中剥离出来，同时与一些糟粕划清界限。通过概念普及和应用推进，DeFi将逐渐成为利用区块链实现普惠金融、新型金融、数字化金融的正确方向，并最终达到造福社会和人类的作用。

The Decentralized Asset management Plaform (以下简称DIPPER) ， DIPPER是DEFI领域全球第一个DAM平台，重新定义开放式金融时代下的交易服务与资产管理，通过资金托管去中心化、标的交易去中心化、策略收益与回撤数据预言机验证、交易信号实时存证上链等技术手段，真正实现去中心化的开放式资产管理平台。

DIPP是开放式资管平台DIPPER的唯一平台通证，总发行量仅1000万枚，通证经济模型领先有效，将成功打造开放式资管与交易服务新生态。



目前，DIPPER平台上已成功构建智能交易应用：神器开阳MIZAR，利用策略智能筛选标的，并实时提示现货/期货在不同周期的买卖价位，自动跟踪趋势，并提供其他快捷交易服务，如矿场套期保值、网格套利、跨期套利等等，支付DIPP通证即可使用神器开阳所有功能服务。

目前，DIPPER平台已发行加密货币市场第一支DAO形式的量化策略基金：摇光基金ALKAID，是现货投资组合管理+去中心化资金托管为一体的去中心化资管基金，所有交易标的皆由神器开阳应用智能筛选，跟踪大趋势，获取长期利润回报。买入DIPP通证即拥有摇光基金的基金份额，并可在二级市场自由流转。

DIPPER为新时代的消费者提供了一个更公平、更高效、更全面的金融服务市场。分布式数据协作协议允许参与者提高数据质量，降低数据获取成本，扩大数据覆盖范围，最终通过人工智能创建更好的信用评分模型。

未来将有更多优秀的智能交易策略、DAO形式的量化基金在DIPPERP平台发布，敬请期待。



通过建立在Defi协议之上的DIPPER生态系统，我们可以看到能够大幅改善多个金融服务垂直领域的巨大潜力，包括：

- 通过普惠金融，推动社会公平和经济发展。世界银行认为，改善信贷获取渠道促进了社会公平，是推动经济发展和减轻贫困的最佳做法之一。
- DIPPER致力于为用户提供安全、高效、快速的数字资产撮合平台，定位于“全球首家金融级数字货币及衍生品交易平台”，数字货币交易采用全球领先的技术架构，技术方案基于 Jelurida 与 TenX，有效防止 DDoS 等攻击，支持动态与静态数据分离，支持热点数据缓存，支持异地容灾，支持平行扩展，并通过一系列地检测和优化，有效避免常见的错误和漏洞，以金融级的安全技术标准，保障用户交易。
- 通过扩大信贷市场和消费市场的份额，向大众提供信贷覆盖可以创造非常大的利润价值。这样的增长刺激可以激励更高质量的借贷、支出和投资。

DIPPER优化提升区块链技术在各个层面的协议和机制，实现价值传输网络各层次的支撑协议，作为真正的区块链 4.0 金融基础设施，为各类价值传输应用提供基础设施，为各类 DApp 开发提供底层开发平台，为构建全球价值互联网提供现实可行的技术途径。

# CATALOG

## 01. 背景综述.....07

- 1.1 DeFi 的时代机遇
- 1.2 新金融新机遇
- 1.3 金融服务下沉需求强烈
- 1.4 去中心化由试验到生产
- 1.5 持续面临的挑战

## 02. 项目介绍.....15

- 2.1 项目简介
- 2.2 解决方案

## 03. DIPPER 创新实现方案.....20

- 3.1 连续型随机取样替代传统离散型共识算法
  - 3.1.1 连续型和离散型数据的定义方式
  - 3.1.2 描述离散趋势的统计量
  - 3.1.3 四分位区间距
  - 3.1.4 平均差
  - 3.1.5 方差与标准差
- 3.2 异步排序技术将共识转化
- 3.3 多语言的开发编程
- 3.4 实现数据迁移

## 04. DIPPER 底层构架方案.....31

4.1 DIPPER 整体架构

4.2 存储证明

    4.2.1 Proof-of-Storage via Merkle Audits

    4.2.2 Proof-of-Storage via Pre-generated Audits

4.3 冗余证明

4.4 DIPPER 账户

    4.4.1 外部帐户

    4.4.2 合约账户

4.5 分布式控制结构

4.6 数据区块结构

4.7 去中心化算力集群

4.8 安全加密算法

4.9 P2P 协议

4.10 DIPPER 恶意攻击防范与惩罚机制

4.11 弹性共识机制

4.12 预言机是链内与链外万物相连的桥梁

## **05. DIPPER 生态体系.....52**

- 5.1 孵化中心
- 5.2 Staking 中心
- 5.3 流动性挖矿
- 5.4 DIPPER 预言机验证
- 5.5 DIPPER 金融神器
- 5.6 摆光基金

## **06. DIPPER-Token 数字化凭证.....58**

- 6.1 介绍
- 6.2 分配机制
- 6.3 通证模型
- 6.4 销毁机制

## **07. 团队介绍.....61**

## **08. 风险控制&免责声明.....64**

- 8.1 风险控制
- 8.2 免责声明



01

# 背景概述

## 1.1

### DeFi 的时代机遇

我们认为，不论是现有金融服务和业务，还是未来将发展壮大的数字化金融服务，随着数字化生活以及数字经济浪潮的发展，他们的业务形态、服务方式、面对的用户需求等，都将发生缓慢但巨大的变化。甚至比电子化、信息化浪潮时金融发生的變化更加深刻。

DeFi 由于其去中心化的底层技术以及其倡导的开放包容的技术理念，在透明公开、审查、以及一些场景下的效率提升和成本降低方面，相比传统模式有鲜明的优势。我们认为 DeFi 在未来的主要机遇在于两方面：

1) 已有金融业务或服务的分布式化改进和升级。 随着社会的发展，一些现有金融服务和业务会催生出升级和改造需求，而某些情况下，利用区块链技术进行赋能，通过利用其共建信任、透明公开、不可篡改等特性，相比利用传统中心化技术更容易满足升级要求。

2) 成为新兴的金融场景和需求下的分布式基础支撑。 数字化进程的深化必然会创造众多全新的需求和应用场景，他们对金融服务和功能的需求，将迫切但不同。区块链技术具备天然契合数字化场景的优势，基于区块链技术的DeFi 完全有能力成为数字化和物联网时代底层的金融基础设施。

## 新金融新机遇

毫无疑问，此时我们正处于一个变革的时间区间，互联网、云计算、大数据、人工智能信息技术的发展，让信息化、数字化能够触达到社会的方方面面。现实世界的数字化、数字化虚拟场景的增加，也不断催生新形势的金融需求，我们可以统称为“新金融场景和需求”。新金融场景和需求具有以下特征：

### 1) 围绕用户而非机构

与传统金融业务通常围绕机构、在金融机构间开展不同，新金融场景下，主角由机构迁移到终端用户。所有金融行为的发起、参与以及主导作用，皆转移到普通用户。新金融场景下，机构作用仍然非常重要，但是场景的整个中心已经无疑转移到用户。不严谨的说，新金融时代得用户者得天下。

### 2) 线上行为远多于线下行为

传统场景围绕线下营业厅、客户经理等金融机构业务人员、线下支付等展开，只是通过网络和计算进行数据信息化和数据传递与存储，整体流程主干仍是线下为主。而新金融场景下，主干流程已经基本线上化，场景的金融行为触发、流转交互等。

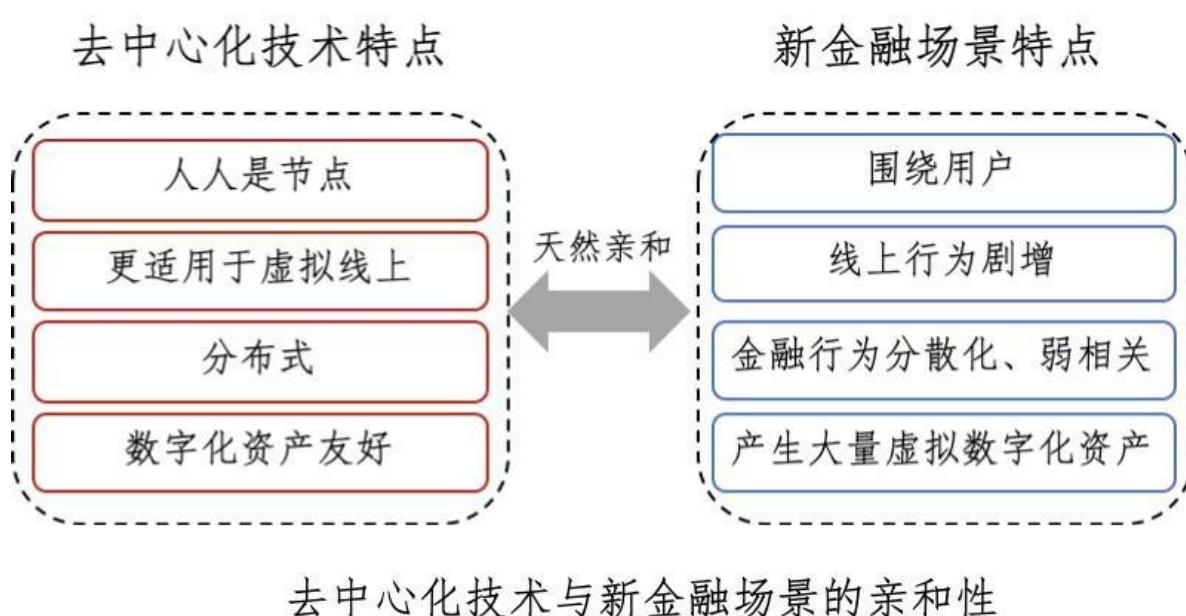
### 3) 金融行为参与方呈分散化、弱关联化

金融行为的线上化，带来的另一个特点是，金融场景的参与方已经打破了传统金融场景地域的限制，涉及的参与方越来越分散、陌生化；首次或低频的发生金融行为关联的情况占比越来越高。这种由传统金融场景中大部分参与方是强关联的情形不同，呈越来越弱关联化的新金融场景，为业务协同、联合风控等带来了更大的挑战。



#### 4) 数字化资产参与越来越多

虚拟权益(会员、付费阅读与观看等)购买、数字化资产(文章、图片、视频等)价值保护与流转、甚至数字化货币的参与，在新金融场景里越来越多，未来大部分场景也将围绕数字化资产展开。基于区块链技术的分布式金融，其底层技术和适用场景恰好契合新金融场景：去中心化技术与用户为中心的应用契合、基于去信任假设的理念与弱关联的参与方特性契合、天然更适合线上数字化虚拟场景、支持数字化资产相关应用……正因如此，正在展开的新金融时代对 DeFi 而言是一个巨大的机会。





## 1.3

### 金融服务下沉需求强烈

在当前移动互联网时代，用户涉及的一些金融行为通常由用户主动发起：支付交易、消费信贷、理财投顾等，并且通常用户每天的金融行为次数可能在数十次到最多几十次之间。但是在新金融时代，金融行为和服务需求将变得越来越频繁，也将逐渐下沉为更加基础层面的需求。

首先，数据将不仅仅是信息的数字化表示，将逐渐资产化。而用户已有的大量存量数据，以及每天新生产的数据，其价值将越来越被行业和用户所重视。将海量有价值的数据资产进行保管、流通和利用，将是未来几乎所有场景将有的基础层面的需求。而这过程中对金融服务而言，则是非常高频、小量交易结算和分散的金融行为支撑需求。

其次，从用户感知角度，未来金融需要“由重变轻”。当前金融服务通过各种技术和风控手段的应用，已经在往“轻量级”方向演进：网上开户、人脸验证、大数据风控等等。但是仍然不够快、不够轻。将复杂的金融规则、流程和服务下沉并成为坚实的基础设施，让用户安全、便捷的使用金融服务的同时，又能实现低成本和对业务的低侵入。

第三，用户和系统对降低金融摩擦和消耗成本的需求愈发强烈。这里的摩擦和成本，除了系统和业务间手续费和协调成本，还包括过于复杂和不匹配的流程带来的额外开销，不够智能和自动的流程和服务带来的高额成本等。综合起来，未来金融服务特别是直接面向消费者的金融服务，需要成为如同水电煤一样的基础又坚实的服务。而 DeFi 基于区块链技术在面向大量用户、基于非完全信任模型构建金融服务上有着更加明显的优势，并且基于数学和密码学构建而成，理论上具备坚实的基础。因此这种新形势的需求对 DeFi 反而是一个巨大机会。

## 1.4

### 去中心化由试验到生产

我们认为以区块链为代表的去中心化技术仍然处于初级阶段，未达到成熟应用特别是成熟商用的程度。但是近几年来，技术发展速度加快、应用场景探索不断增多。预测在未来3-5年左右时间，去中心化技术将走完试验探索阶段，出现被广泛认可的生产及应用。从几个方面我们能够看到去中心化技术在逐渐走向成熟：

#### 1) 基础设施能力缓慢完善

联盟链和公有链的核心技术在逐渐得到完善，共识与一致性、性能与去中心的平衡、合约语言与合约虚拟机等都取得可见的进展；同时，围绕核心技术的基础设施能力也不断丰富，例如细分标准的探讨、评估benchmark、评估方法、环境和安全扫描等。

#### 2) 服务能力不断在细分业务领域增强

虽然去中心化技术暂时还不能如同云计算一样提供标准和能力统一的服务，但是近年来在一些细分业务领域，比如数字货币相关、溯源、存证、数据协同、baas服务等，出现了一些完备且具备迁移能力的区块链服务。而就在前几年这块还是行业空白。

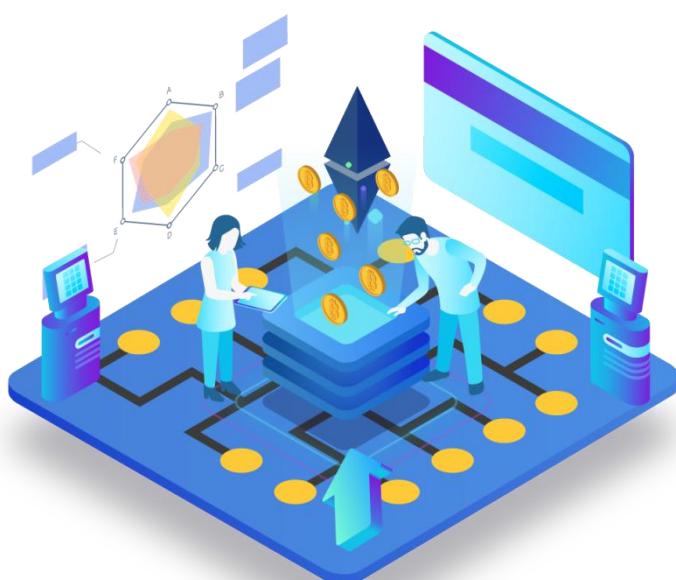
#### 3) 更多应用探索往业务痛点方向推进

我们看到，现在与区块链和去中心化技术发展初期不同，越来越多的应用尝试通过区块链解决用户和业务的现实痛点。虽然这些尝试可能不够深入，或者逻辑推演还存在漏洞，但是这是区块链技术走向应用成熟必要的阶段。而在去中心化技术走向成熟的过程中，DeFi将是推动去中心化技术从试验到生产的重要力量。去中心化技术是最有可能在金融相关领域实现场景和应用的突破，因此DeFi天然占据了先机。

## 1.5

### 持续面临的挑战

机遇和挑战始终是并存的。更加客观的看待 DeFi 的当前和未来，能够让我们做出更加正确的策略和行动。将时间拉长来看，DeFi 要真正走向繁荣和并得到深入应用，DeFi 本身模式和技术以及底层的区块链技术，还有很多问题需要解决：技术上的根本性制约、业务上较大的约束和转变成本、整体区块链行业的协同推进问题以及无法忽视的监管等。



DIPPER

风口已至  
资本涌入





02

# 项目介绍



## 项目简介

科技赋予金融新的生命力，金融与互联网结合产生了 Fintech 概念。通过大数据、人工智能等科技，可以帮助传统金融公司更好地做用户的识别和产品的匹配，提供个性化服务，降低服务成本，提升服务效率。Fintech 概念植根于传统金融系统和它长久以来的信任机制，是对金融的升级。金融与区块链结合则产生了更接近未来的新物种 DeFi(Decentralized Finance) 去中心化金融。

加密支付、去中心化交易、加密借贷、预测市场及衍生品交易、基金管理等均在 DeFi 范畴之内，更多的形式正在不断开拓，任何技术上可行的理念都可以被建造为现实。广义上讲，DeFi 属于 Fintech 范畴之内，但 DeFi 与 Fintech 有着本质的区别，DeFi 是对于金融的改造而不是升级，这个体系的核心是去中心化金融。现行金融体系下金融资源的不公平分配这一桎梏，开放金融领域正在试图打破。探索更高效的技  
术和更适用的商业模式，以使所有人都有机会享受到平等的金融服务，普通投资者有机会也能享受到高净值人群的服务，有机会参与到优质的机构级金融产品，实现平等的财富增长，实现更深刻、更广阔的去中心化金融生态。

基于此，DIPPER 开放式金融生态系统，旨在开发一个完备的去中心化金融生态系统，是能够去打造借贷、融资、交易、预言游戏等功能为一体的跨链的金融科技服务生态，可以让全球用户 365 天 24 小时无门槛地使用该金融生态系统，实现加密世界货币的价值最大化，定义数字金融的未来。并推出全球性的国际通用的数字资产与法币汇兑的支付通道，最终形成聚合型 DeFi 金融平台，帮助用户实现真正意义上的便捷高效低成本的去中心化金融服务。

## 2.2

### 解决方案

可以看到，针对数字化、资产化和新金融带来的变革，现有金融基础设施和服务难以满足，需要一套从理念到设计到实现都适配的金融技术和服务方案。DIPPER认为基于区块链的分布式金融技术和服务是这方面的最佳选择：

#### 1)DIPPER去中心化的理念非常契合以用户为中心的新金融行为。

通过去中心技术，能够很好支持金融行为从以机构为中心向以用户为中心的思路的转变；同时能够从底层机制上保证用户对自我数据资产和金融行为的掌控，这在虚拟的数字化场景尤为重要。

#### 2)DIPPER能够自底向上构建更加坚实的信任。

在数字化场景，很多控制金融风险的手段面临失效或不适用，金融的核心信任基石受到威胁。而 DeFi 利用区块链技术，依托数据和密码学等，在最少信任假设的前提下，自底向上建立了更加健壮的信任，奠定了更加坚实的金融基石。

#### 3)DIPPER去中心化网络天然更加契合海量用户的海量金融行为。

大量用户产生的分散、弱关联的金融行为，只需要交易双方在分布式网络达成，相关节点鉴证和监督即可。在不依赖绝对中心的情况下，大量的交易并行进行，随着交易、用户、节点的增多，没有中心节点成为制约整体网络发展的瓶颈。用户控制自己的节点，控制交易的发起、参与行为以及记账。



#### 4)无障碍资金跨境流通：

DIPPER建立新的货币金融体系，为资金流转提供便捷通道。通过通证即可实现价值转移，不仅突破了地域性监管限制，而且略过昂贵的中转机构，有效降低了资金跨境流通的成本。

#### 5)DIPPER信用体系基石更加可靠

DIPPER的整个信用体系基石是基于去中心化技术保证的数据，经过共识机制达成广泛共识，从源头上保证生成的信用结果可靠。同时由于去中心化技术以及监督和多副本的存在，使得篡改基础数据几乎不可能，因此传统场景涉及修改信用结果的一些不可控情况，在DIPPER架构下几乎不可能发生。

#### 6)DIPPER对金融业务友好易用

DIPPER不是将信用体系建设为独立于架构外的服务，而是直接内置了关于信用体系的信用模型、数据计算、评估方法等功能，业务只需简单配置即可拥有自己领域的信用构建体系。同时整个信用结果提供了完整的使用和交互机制，以及相应的 API 接口，使内外部对信用结果的使用成本更低。

#### 7)DIPPER完备的基础设施能力

DIPPER具备包括底层基础能力)、分布式核心协议、网关、客户端在内分布式基础能力，这些能力使在去中心的基础上，保证了数据的一致、网络的稳定、共识的可靠、服务的可用。同时，这些基础能力通过完备的 OpenAPI 进行暴露，使得跟其他金融组件和业务很好的融合，进而更好支撑分布式金融场景的构建。

科技  
智能  
引领  
未来



03

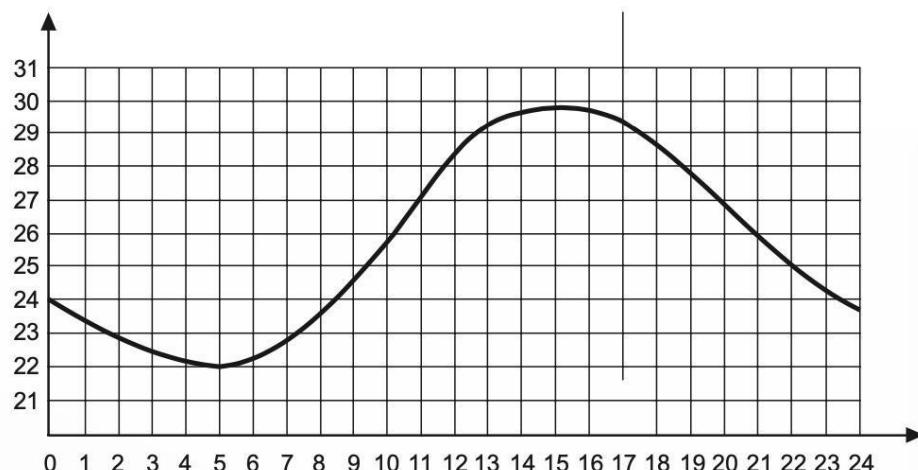
# DIPPER 公链的创 新实现方案

### 3.1

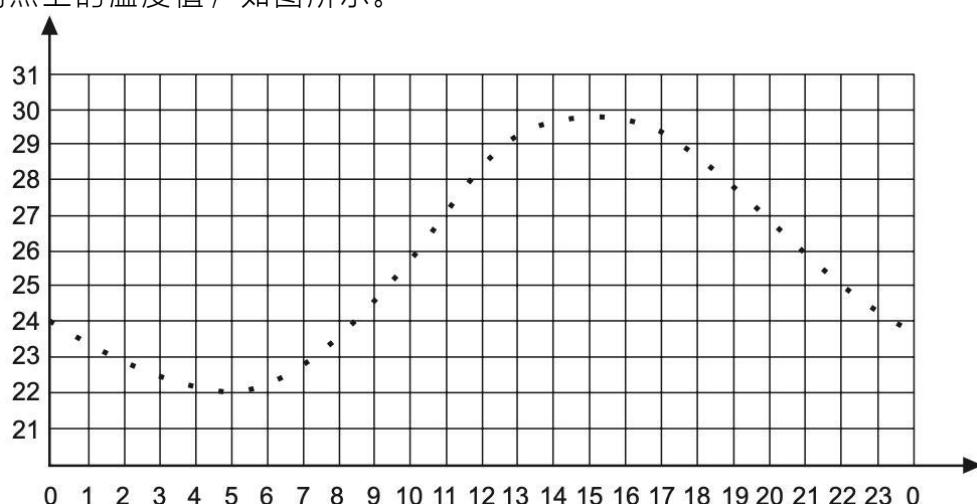
### DIPPER 整体架构

#### » 3.1.1 连续型和离散型数据的定义方式

连续量通常称做模拟量，它在时间上和数量上是连续的物理量。如温度计用水银长度来表示 温度高低。其特点是数值由连续量表示，其运算过程也是连续的。温度变化的连续量曲线图如图所示。



离散量又称数字量，它是将模拟量离散化之后得到的物理量。即任何仪器设备对于模拟量都 不可能有完全精确的表示，因为它们都有一个采样周期，在该采样周期内，其物理量的数值都是 不变的，而实际上的模拟量则是变化的。这样就将模拟量离散化，从而成为离散量。如一天中以 每小时为单位测量一次温度的值，则得到24h内离散的时间点上的温度值，如图所示。





### »» 3.1.2 描述离散趋势的统计量

尽管集中量可以很好地描述一组数据的特征，但仅用这些统计量还是不够的。还需要考虑数据的分散情况。有时，两组数据的平均数和中位数可能完全相同，但这两组数据之间会存在着很大的区别。请看下面两组数据：A组：79 79 79 80 81 81 81、B组：50 60 70 80 90 100 100。这两组数据的平均数和中位数均为80，但不能据此就简单认为这两组学生的水平是一样的。A组数据与B组数据之间显然是有区别的。首先，A组中的数据相对比较集中，每个数据的值与平均数80相差无几；而B组中的数据相对分散一些，参差不齐，它反映了数据分布的另一个重要特征——变异性(variability)。描述数据离散趋势的统计量称为离散量(measures of dispersion)，或称差异量。

集中量描述了一组数据的典型情况，离散量则反映了数据的特殊情况。在研究一组数据的特征时，不但要了解其典型情况，而且还要了解其特殊情况，前面的例子中A组数据和B组数据的集中量相同，但其离散量肯定是不同的，只有同时了解了这两组数据的集中量和离散量，才能更为透彻地了解这两组数据之间的差别。常用的表示数据离散趋势的统计指标有全距、四分位区间距、平均差、方差和标准差。全距是说明数据离散程度的最简单的统计量。把一组数据按从小到大的顺序排列，用最高分减去最低分，所得的值就是全距，即最高分和最低分之间的距离。上面A组数据的全距为 $81-79=2$ ，B组数据的全距为 $100-50=50$ 。全距小，说明数据的分布相对集中；全距大，说明数据的分布较为分散。全距的优点是计算方法简单，而且也容易理解。缺点是由于它只考虑到两端的数值，没有考虑中间数值的差异情况，描述数据时不太稳定。



### »» 3.1.3 四分位区间距

中位数可以用来表示一组数据分布的集中趋势。中位数正好把一组数据一分为二。如果把中位数左侧和右侧的分布再各分成两个部分，得到的是四个相等的分位。这组数据的第一个四分位：

$$81 - 79 = 2$$

B组数据的四分位区间距为

$$100 - 60 = 40$$

除了四分位区间距，统计学上还有十分位区间距和百分位区间距，它们的区分方法相同，十 分位则将数据由大到小或由小到大排序后，用9个点将全部数据分为十等份，与9个点位置上相对应的变量称为十分位数(deciles)，分别记为 D<sub>1</sub>, D<sub>2</sub>, …, D<sub>9</sub> 表示 10% 的数据落在 D<sub>1</sub> 下，20% 的数据落在 D<sub>2</sub> 下……100% 的数据落在 D<sub>9</sub> 下。百分位区间距与十 分位区间距同例，只是将数据分成 100 等份，于 99 个分割点位置上相对应的变量称为百分位数 (Percentiles)，分 别 记 为 P<sub>1</sub>, P<sub>2</sub>, …, P<sub>99</sub>，表 示 1% 的 数 据 落 在 P<sub>1</sub> 下 … … 99% 的 数 据 落 在 P<sub>99</sub> 下。

### »» 3.1.4 平均差

与全距相比，四分位区间距在表述数据的离散情况时稍微好一些，但由于它没有把所有的数据都考虑在内，其稳定性会差一些。比如说，我们得到两组数据，这两组数据的值并不完全一样，但最后得到的四分位区间距的值则可能完全一致，这便是用四分位区间距来表示数据分布的不足之处。理想的办法是把全部数据都考虑在内来计算分布程度。理由很简单：平均数代表一组数据的集中趋势，我们把一组数据中的每个



数据与平均数相比较就可以得知每个数据与平均数偏离的程度，或者说与平均数差异的情况。如果把这组数据中每个数据与平均数差异的情况相加起来，那么所有数据的差异情况便一目了然。把这个值除以数据的个数，所得的值叫做平均差。公式为：

$$\frac{\sum |X - \bar{X}|}{N}$$

其中，

**X**

=每个数据的值；

**$\bar{X}$**

=总体平均数；

**N**

=观测的数据个数。

从上式可知，平均差是数据分布中所有原始数据与平均数距离的绝对值的平均。用绝对值是为了不出现负数。由于平均差是根据分布中每一个观测值计算求得的，它较好地代表了数据分布的离散程度。然而，由于平均差的计算要求绝对值，不利于进一步的统计分析，故在统计实践中平均差不常使用。

### »» 3.1.5 方差与标准差

根据上面的公式，如果不求每个原始数据与平均数之差的绝对平均值，而是求它们之间的平方，这样就不会有负数出现了。然后再把每个原始数据与平均数之差的平方的值加起来，得到的是每个原始数据与平均数之差的平方和：



$$\sum (X - \bar{X})^2$$

用这个平方和再除以所观测到的数据的个数，得到的值被称作方差。用公式表示为：

$$S^2 = \frac{\sum (X - \bar{X})^2}{N}$$

标准差与方差的概念易于理解，它们实际上都是一个差异量数：标准差的平方就是方差，或 方差的平方根就等于标准差，二者都反映了一组数据围绕平均数分布的情况。标准差的值越大， 表明这组数据的离散程度也越大，即数据越参差不齐，分布范围越广；标准差的值越小， 表明这组数据的离散程度越小。即数据越集中、整齐，分布范围越小。当数据完全没有差异时，所有数值都与平均数相等，这时标准差或方差等于零。

可以证明，在公式中用N作为除数时(尤其是当N很小时)，所得出的作为总体标准差估计值的样本标准差是有偏差的，而N-1 作除数时，所得标准差则是无偏差的。因此，比较稳妥的做法是用 N-1作除数，所得结果差别不大 。

离散转连续由传统离散型共识算法投票确认，升级成了连续型随机取样，只选取所有节点中的一部分来获得一个结果，往复多轮取样，实现全覆盖。并行共识提升异步系统的运行效率，配合异步系统多节点设计，进一步提升系统的并发性能。不需在共识过程中与大多数节点连接，并获取投票，节省系统数据传输，使用随机可计算函数，用户根据计算得知其是否被选择中，并将结果反馈和广播给其它用户。线性扩展性，即性能随节点规模增大而线性加速，节点规模越大收敛越快，性能越好。



### 3.2

### 异步排序技术将共识转化

独创异步排序技术,将共识转化为处理对异步系统大规模并发请求,以及数据的排序问题。优于网络的整体连通性,在非全连通网络的环境下,甚至网络连接比例<50%的系统中也能够正常运行。

多隐层网络,用一个隐层网络来逼近任何连续函数。架构由深层网络代替单隐层,在拟合过程中可以更快地收敛归一结果。反向传播算法、多层次分区、雾算法、在弱中心化和去中心化之间切换网络拓扑结构。超级节点和监督节点相结合的方式。异步通讯策略在并行处理技术中,任务之间的信息通讯通常采用2种策略,异步通讯策略和同步通讯策略,由此引出了异步并行算法和同步并行算法。所谓同步并行算法就是在执行过程中的数个任务然而区块链环境仅支持同步通讯机制,同一通道连接的2个节点进程(任务)只有当分别处于输入/输出准备就绪状态时才能发生通讯,否则已经处于就绪状态的进程(任务)(不管是输入进程还是输出进程)将一直处于等待通讯状态。具体地说,由于分配到各处理机上的任务总归有不平衡的情形,因而可能会发生:1任务了'x'输出相延迟太久才响应任务'x'的输入相的输入数据请求;2任务'x'输出相请求发送数据等待任务'x'输入相的响应过久,以致数据可能会丢。进一步说,由于通讯等待,致使任务'x'不能进入下一步递归运算。为此,考虑设计一种通讯策略,使Trasnputer—OCCAM多处理器机系统实现异步通讯的数据交换策略是非常必要,而且是必须在这里考虑增加一个起缓存作用的OCCAM进程C氏(CommuniCationprOCessing),使它并发执行。内存变量中,1自己进入下一次递推运算;2当任务'x',输入相请求数据输入时,将内存变量暂存的数据转赋给任务'x';3当1和2同时发生时,将CP勺中内存变量1存的数据转赋给任务'x',与此同时,将'x'新送来的数据存入内存变量2中;1当无请求时,CP将不起作用。



### 3.3

### 多语言的开发编程

如果你是个开发者，想用区块链实现某一个应用场景，则可按照如下步骤使用DIPPER公有链开发该应用，以下的步骤在DIPPER公有链开发平台操作：

(1) 注册成为开发者：得到APP的 ID 和 KEY，这是基于DIPPER公有链的区块链应用必须具备的两个参数。

(2) 参数设置：

A. 异步调用：有些API函数不能实时返回，需要一定时间(几秒)后才能回复最终结果，等待时间过长，用户体验不佳。我们可以设定调用API后不等待结果立即返回，我们称之为异步调用(例如支付宝、微信支付等的异步机制)。

B. 设置回调 URL：在异步调用情况下，有必要设定一个回调 URL，DIPPER公有链在该交易被确认后，将API调用的最终结果通知到该 URL(如果开发者确定不需要回调，则本步骤可以省略)。开发者指定的 URL 需要有处理结果通知的程序逻辑。设置区块链：开发者可设置默认区块链，API 接口在没有指定区块链类型情况下，使用默认区块链。

(3) 熟悉 API、SDK：DIPPER公有链将提供详细的 API 接口说明、SDK 源代码。开发者参考API和SDK可以很容易上手开发区块链应用，大大简化了入门过程。

(4) 开发区块链应用：开发者选取应用场景，开发自己的区块链应用，呈现界面可以是网页、桌面客户端、手机 APP 等。

### 3.4

### 实现数据迁移

这里用一个场景来阐述:某开发者开发了一个区块链应用，使用 B 管理了 1000个用户，发行了 10 种资产。某天该开发者想把该应用切换到 E,问题是:原先在 B 上的用户和资产数据 该如何处理? DIPPER公有链系统支持异构区块链的切换，开发者可以在开发者管理平台上手动切换该如何处理? DIPPER公有链系统支持异构区块链的切换，开发者可以在开发者管理平台上手动切换默认区块链，并且进行数据迁移。数据迁移的规则:对于用户和资产数据，DIPPER公有链保存其最终状态;当切换到其他区块链时，DIPPER公有链把用户和资产的最终状态还原到新的区块链上，但不还原历史交易。状态还原过程包括在新区块链上注册用户、向该用户发行所拥有的资产类型和数量等操作。

数据迁移的时间视用户和资产数据大小而定，从联盟链或私有链迁移至公有链如 B、E 时，以加密货币形式支付发送交易所需的交易费。开发者自行上传的智能合约因区块链智能合约体系不同，没法从源区块链迁移至目标区块链，智能合约中的开发者自定义数据也一样。但是 DIPPER公有链提供了同时访问多个区块链的能力，开发者可在目标区块链中部署新编写的智能合约，再从源区块链的智能合约中提取出自定义数据，存放到目标区块链的智能合约中，完成数据迁移过程。

### 3.5

### 模拟 Neuron 神经元系统，合力决策

人工神经网络(Artificial Neural Networks，简写为ANNs)也简称为神经网络(NNs)或称作连接模型(Connect是一种模仿动物神经网络行为特征，进行分布式并行信息处理的算法数学模型。这种网络依靠系统的复杂程度，通过调整内部大量节点之间相互连接的关系，从而达到处理信息的目的。

神经网络是通过对人脑的基本单元——神经元的建模和联接，探索模拟人脑神经系统功能的模型，并研制一种具有学习、联想、记忆和模式识别等智能信息处理功能的人工系统。神经网络的一个重要特性是它能够从环境中学习，并把学习的结果分布存储于网络的突触连接中。神经网络的学习是一个过程，在其所处环境的激励下，相继给网络输入一些样本模式，并按照一定的规则(学习算法)调整网络各层的权值矩阵，待网络各层权值都收敛到一定值，学习过程结束。然后我们就可以用生成的神经网络来对真实数据做分类。DIPPER公有链将率先人工智能Neuron网络神经元系统结合在了主链中，合理决策，判断拥挤达成平衡，数据价值分享决策。无数独立决策个体组成传导结构模拟Neuron，合力决策。

# DIPPER

THE FUTURE HAS TO

交互体验

智能思维

精准定位

真实触感

数据  
存储

数据  
分析

加密  
算法

精准  
定位

远程  
分析

点点  
传输

共识  
机制

精准  
定位





04

DIPPER

底层构架方案

## 4.1

### DIPPER 整体架构

DIPPER是一条基于智能合约开发的主链，合约共识，多链并行，多原混合共识机制及跨链原子操作构建高速跨链资产流通公路，共识机制方面集成了 NDPOS、DPOS、POS、POST、POC、POW、PDIPPERT的优势，通过算法反推共识将共识机制打散且通过异步排序及离散转连续的方式进行择优选取，不需在共识过程中与大多数节点连接，并获取投票，节省系统数据传输，降低节点对网体依赖，节点随机选择，使用随机可计算函数，用户根据计算得知其是否被选择中，并将结果反馈和广播给其它用户，多原混合机制(Multiple Hybrid Consensus Mechanism)从共识层面将优势放大提高TPS的速度，我们团队进行研发的时候发现，单单的通过传统的共识层面去提高TPS，都是受限制的，传统的共识机制不管是POW/POS/DPOS/NDPOS以及PDIPPERT单一的共识机制经过多次运算都无法实现质的突破，所以我们通过算法反推并运用独创技术将共识打散并择取优势部分，从而使 TPS进行了质的突破。有人说 TPS不能作为区块链发展的唯一命题，但是我们DIPPER团队坚信区块链作为一种技术必须还是要落实到实际应用中，那这其中就包含了大量的商业应用，作为商业层面的应用，无论是溯源还是物流追踪还是支付，对TPS都有或多或少的要求，起码TPS理论也要在5000以上，而现有的共识机制不论是 POW(TPS停留在个位数只能挖矿)还是POS(只能做简单的钱包和应用开发)乃至是DPOS其实真正的做到TPS的突破都是不现实的，因为无法满足在高并发时的并发问题，从而使得在多用户多节点的时候出现TPS无法支撑的情况，即便是满足图灵完备的PDIPPERT容错率高达33%所出现的 TPS值也远远无法达到商业级别的应用，与传统VISA的TPS值相差甚远。综上所述，DIPPER团队跳



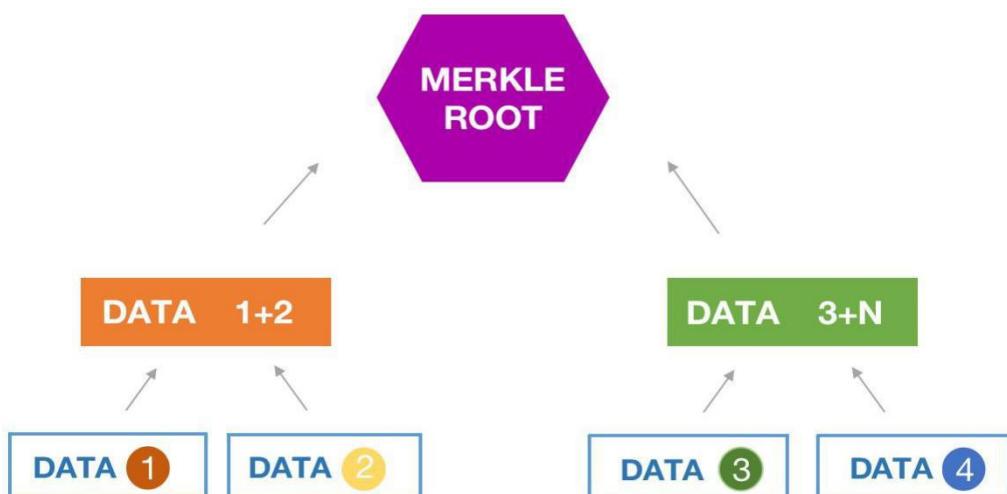
出了传统的区块链思维，我们突破了传统的共识机制思维，传统思维是共识机制决定TPS从而决定 Performance, DIPPER在底层的突破打破了传统思维，以算法为核心突破口，而用共识机制做 相应的配合，从而达到了显著的效果和TPS的实测数据，所以我们DIPPER的重点是在于运算算法的核心部分。

在这一层面，我们做了大量的工作和创新并取得了显著的成绩，通过多次运算及权威的超算中心测试，我们的TPS值实测突破了千万级别，这对于传统高性能开发平台开发不论是基于共识机制还是DAG都是极其深远的影响，极其方便的打造友好世界级区块链基础设施。同时，在DIPPER上，共链共享统一的用户系统上用户共享打通区块链世界大用户生态，交易时间、隐私保护、渐进节点共识，以及提高信任的效率，在并发响应方面也同时做了大量的突破。

DIPPER必须解决的另一个问题是，存储空间的提供者必须能够加密地证明他拥有这个碎片，并且没有以任何形式修改过。为此，DIPPER设计了如下的技术体系：

### »»4.2.1 Proof-of-Storage via Merkle Audits

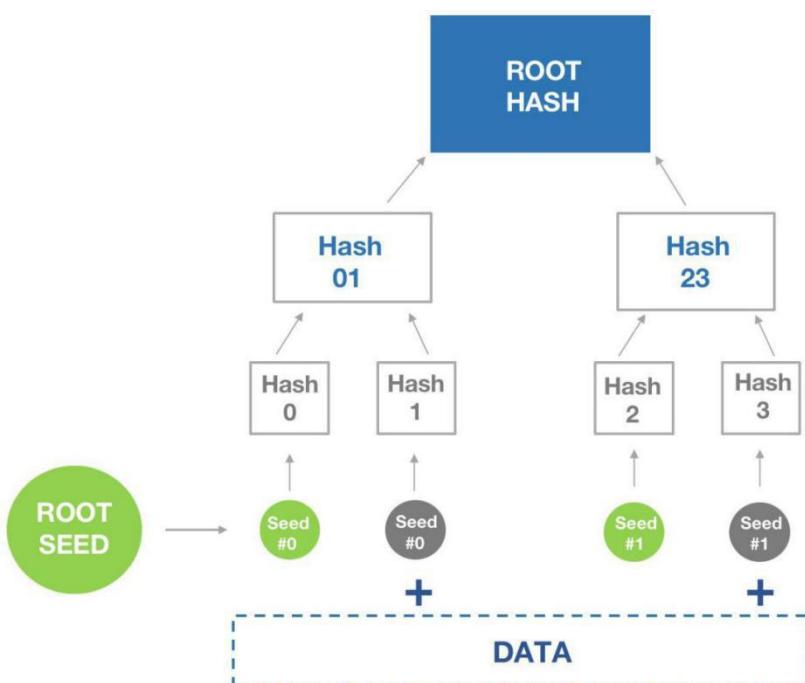
为了实现一个去信任的数据存储网络，DIPPER必须给客户提供一个审计方法，证明他或她存储在网络上的数据可用并且没有被修改。DIPPER通过使用Merkle树和Merkle证明来做到这一点。DIPPER采集数据的集合并生成Merkle树：



树的叶子应该是 256 字节碎片或更小。理想情况下，树应该比数据大，因此树应该在生成而不是存储。对远程位置上的数据的审计仅由特定索引和由位于该索引处的子分片加上 Merkle 树 SPV 证明的响应组成。该算法已被进一步描述在秘密共享和擦除编码。

## » 4.2.2 Proof-of-Storage via Pre-generated Audits

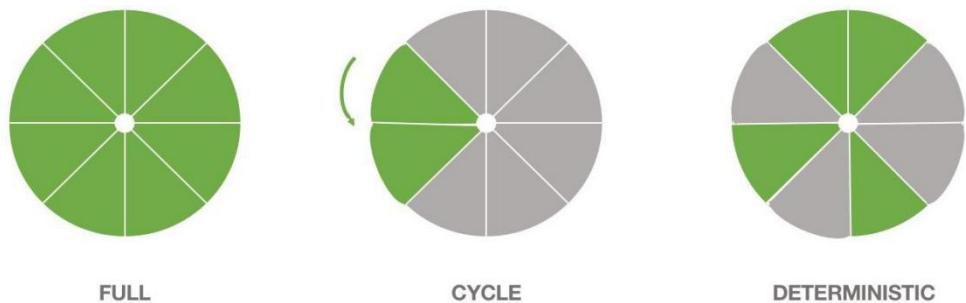
DIPPER 提出了一个替代的审计方法，这需要更多的成本，但可能比之前的方法有一定的优势。DIPPER 通过哈希挑战（质询算法）来做到这一点，在客户端产生一系列种子（由根种子确定），可以添加到文件并且进行哈希，产生唯一的哈希值。DIPPER 把这个过程称为心跳。客户端产生这些哈希挑战（质询算法），建立一颗 merkle 树并且把 merkle 根加入到中本聪类型的区块链中。然后把除去叶子节点的 merkle 树发送给存储空间提供方。客户端可以定期的发送种子给它托管数据的存储空间提供方，检查存储空间提供方的返回结果是否能和它产生的哈希值匹配，通过验证存储空间提供方返回的值与 merkle 树中的值。（客户端自己有完整的 merkle 树，所有节点都在，存储空间提供方只存储了某一个碎片，给它发送种子，它会返回一个哈希值，检查这个哈希值是否在我的 merkle 树中就可以了）。



存储空间提供方不能修改或者删除文件，因为他或她进行哈希挑战（质询算法）时会失败。通过加密和哈希的前提，这些心跳不能蛮力强迫。它是加入到区块链中的。

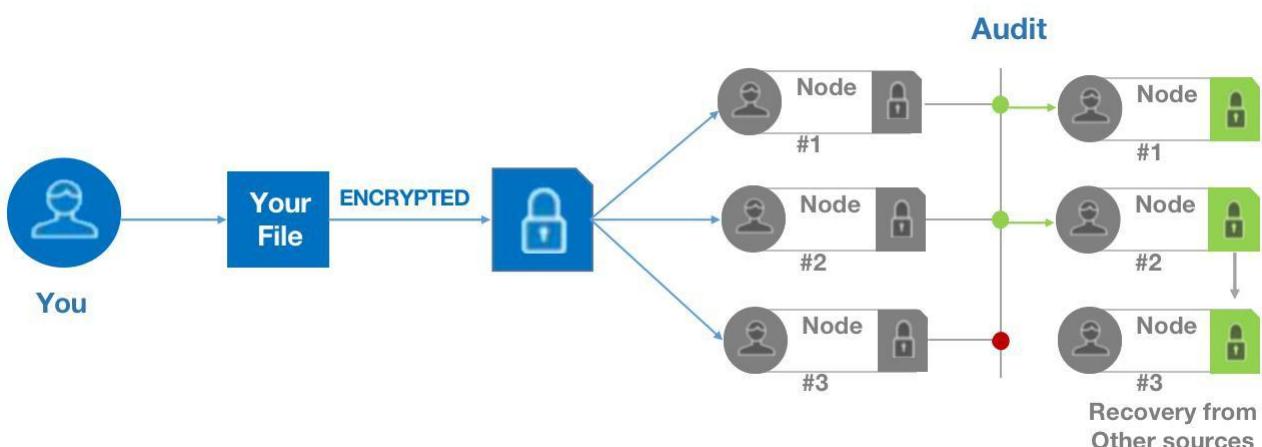


这样，DIPPER 用区块链给存在证明背书，以使各个部分都是诚实的。DIPPER 采用 3 种不同的机制产生挑战：



### 4.3 冗余证明

传统云存储公司拥有或者租借服务器存储他们客户的文件。他们使用 RAID 方案或者多个数据中心的方法从物理或者网络故障中保护文件。DIPPER 没有中心服务器。文件存在于一个分布式的、虚拟的、去中心化的网络中。DIPPER 不像传统云存储公司那样依赖于一个存储空间提供方雇佣相同的安全措施防止数据丢失。鉴于此，DIPPER 通过在多个存储空间提供方上使用 K-M 纠删码技术存储碎片保证冗余。更具体地说，DIPPER 考虑到在网络层上的冗余，而不是物理层。DIPPER 还必须解决存储空间提供方干脆关掉电脑的可能，从而从网络中删除一个碎片的可用性。





如果一个节点审计失败或者不可到达，DIPPER 就发起一个网络复制过程，通过把网络上一个现有的副本转移到一个新的节点上。因此，网络就能在每次审计之后恢复正常。每个碎片都是唯一加密的。这意味着，当恶意存储空间提供方只有一个文件副本时，不能假装拥有多个冗余副本。

DIPPER 可以通过在集中加密碎片时，加入确定性的混淆值来完成。即使解密密钥是一个已知的特定文件，恶意存储空间提供方也不能完成他们没有被分配到的碎片的审核。

这样，DIPPER 可以证明一个特定的碎片的冗余，因为每一个冗余副本是独一无二的。DIPPER 使用 K-M 纠删码技术确保文件碎片是有效的。客户端可以选择 K 和 M 达到文件鲁棒性和花费代价的平衡。在计算章节更是统计性地描述了文件的鲁棒性。纠删码技术也对攻击章节提到的 hostage 字节和修改字节提供了一种保护。

最终，用户和应用都被 K-M 纠删码技术的参数和分布式的冗余控制。对于简单的数据存储，用户可能选择推荐的设置，把他们的数据平均分配在 3 到 4 个存储空间提供方上。这对简单容错已经足够。如果数据特别重要，用户可能把数据分散到 500 个存储空间提供方中，这能保护数据免受世界末日和上帝的破坏。K-M 纠删码技术也能影响数据的鲁棒性。



## 4.4

## DIPPER 账户

### »» 4.4.1 外部帐户

DIPPER 外部账户 (EOA)

- 有以太币余额
- 可以发送交易 (以太币交易或引发合约代码)
- 由私钥控制
- 没有相关代码

### »» 4.4.2 合约账户

DIPPER 合约账户

- 有以太币余额
- 有相关代码
- 代码执行由从其他合约接收的交易或消息 (调用) 触发
- 执行的时候—执行任意复杂的操作 (图灵完备的)—操控它自己的永久存储，例如，可以有自己的持久状态—可以调用其他合约 DIPPER 区块链上的所有行为都由外部账户引发的交易调动。每次合约账户接收到交易时，它的代码都按照输入参数的指示执行，作为交易的一部分发送。合约代码由参与到网络的每个节点上的以太坊虚拟机执行，作为验证新区块的一部分。这个执行需要是完全确定性的，它唯一的语境是 DIPPER 区块链上区块的位置和所有可见的数据。DIPPER 区块链上的区块代表时间单位，DIPPER 区块链本身是时间维度，代表在链上区块指定的离散的时间点上状态的整个历史。



## 4.5

### 分布式控制结构

DIPPER 的数字加密根据系统确定的开源的、去中心化的协议，构建了一个分布式的结构体系，让价值交换的信息通过分布式传播发送给全网，通过分布式记账确定信息数据内容，盖上时间戳后生成区块数据，再通过分布式传播发送给各个节点，实现分布式存储。具体来说，分布式结构体现在 3 个方面：

#### 1、分布式记账

平台上用户行为轨迹以及交易数据由多个节点进行记账，并且会验证其合法性，合法性的交易会被记录到所有用户的账本中，最大限度地避免了道德风险，并且不容易出现错误。

#### 2、分布式传播

数字加密中每一笔新交易的传播都采用分布式的结构，根据 P2P 网络层协议，消息由耽搁节点被直接发送给全网其他所有的节点。

#### 3、分布式存储

让数据库中的所有数据均存储于系统所有的电脑节点中，并实时更新。完全去中心化的结构设置使数据能实时记录，并在每一个参与数据存储的网络节点中更新，这就极大的提高了数据库的安全性。

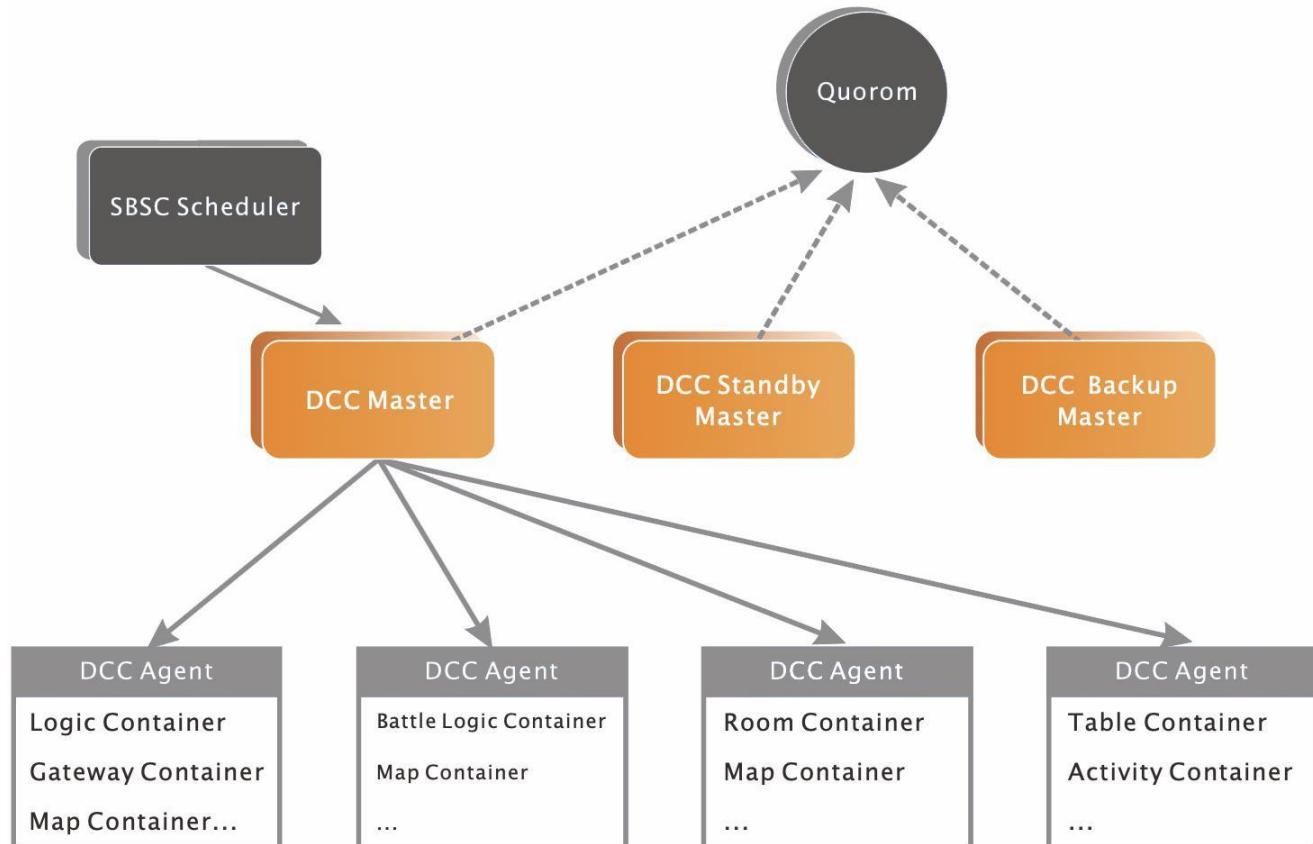
综上，通过分布式记账、分布式传播、分布式存储这三大技术模块，系统内的数据存储、交易验证、信息传输过程全部都是去中心化的。使用分布式交易所的方式进行撮合支付，买方挂单和卖方挂单缓存在数字加密中。当共识节点记账时，自动触发买卖挂单，将账单分布式传播到网络中，在 51%以上的节点验证通过后，完成交易。分布式撮合交易支付的好处是每一笔交易都有据可查，每一笔交易都得到了最广泛节点的确认，在提高交易记录安全性的同时增加了黑客操纵交易盘的难度。

## 4.6

### 数据区块结构

数字加密就是区块以计算机底层的方式组合在一起，数字加密是系统内所有节点共享的交易数据库，这些节点基于价值交换协议参与到数字加密的网络中来。每一个区块的块头都包含了前一个区块的交易信息压缩值，这就使得从创世块（第一个区块）到当前区块连接在一起形成了一条长链。由于如果不知道前一区块的 HASH 函数值，就没有办法生成当前区块，因此每个区块必定按时间顺序跟随在前一个区块之后。这种所有区块包含前一个区块引用的结构让现存的区块集合形成了一条数据长链。





现在行业内出块速度受共识协议的制约相对较大，DIPPER 在共识优化后，通过 SH-DPoS 共识能够做到秒级出块，通过技术驱动，走到了整个行业的最前端。而对于第一梯队的算力所需的交互效率，依旧是远远不够的。DIPPER 在继续优化共识算法的同时，还开发出一套 DCC+RDIPPERN 为核心驱动的，毫秒级响应数据交互与处理系统，能够在现有技术可达到的情况下，满足运行链上大型算力所需的速度/效率需求。

为解决目前区块链算力行业痛点——速度瓶颈，建立起行业标准，实现毫秒级数据处理响应，保证所有高并发类型生态的链化。DIPPER 技术团队经过深度研究，采用 DECENTRALIZED COMPUTING CLUSTER(简称 DCC)，即以去中心化分布式算力集



群的形式，高效率完成云储存运行中的逻辑计算与交互服务，突破现有的区块链公链，尚无法支撑云储存中高频率数据交互的瓶颈(包括算力/状态存储/持久存储等)。现有的云资源服务，虽然能够在一定程度上满足中高频的数据交互需求，但依旧面临着中心化程度高、稳定性与安全性无法得到保障的问题。而通过 DIPPER 所提供的搭载 Quorom Protocol 的节点程序客户端，能够在将云算力资源高效调配起来的同时，将原本中心化的服务以分布式算力集群所代替，以去中心化资源协同的方式保证效率与安全的共存。Quorom Protocol 以双层结构完成去中心化生态网络运行。该结构中，以 Master Standby 及 Backup Master 组成的 Master 节点矩阵保证调度资源节点的高可用性。Agent 节点矩阵接入的带宽资源、算力等，完成不同资源类型的逻辑服务。为保证算力集群的高效运作，确保各资源节点的优质与稳定，所有节点必须达到生态准入标准并获得授权 Admition Certification 才可并入 DIPPER 生态网络。

### »» Step1: 标准入网许可

资源节点不仅必须满足特定的内存空间、带宽空间、CPU 性能、地域等要求，还需缴纳一定量 DIPPER 作为保证金，节点方可上线提供服务并获取收益。在遇到节点无法提供稳定资源或是直接进行恶意行为等，对整个构架产生负面影响的情况下，会自动扣除节点所预存的保证金，并将其作为对消除负面影响而做出贡献行为的正直节点的奖励，以增加各节点的自律性；

### »» Step2: 极简式节点并入

去中心化算力集群生态网络在 Quorom Protocol(基于去中心化算力集群的智能合约)的运行下，满足准入标准并获得 Admition Certification 的资源节点将被并入 E 交易所去中心化算力集群生态网络中。为了完成技术层面上的“极简式”并入，DIPPER 将



为各节点提供专用 BPP 程序端口，运行该程序端口后全球各分布式节点服务器即可一键式并入去中心化算力集群生态调度网络。在成功并入参与算力调度后将通过自动化奖励机制获得 DIPPER 收益；

### »» Step3: 去中心化自治经济体系运作

为保证去中心化算力集群生态中资源的有效利用。我们并没有采用传统固定超级节点+备用节点数量的模式。考虑到 DIPPER 国际站发展的扩容性与整个去中心化算力集群网络的适配性，去中心化算力集群以去中心化自治经济体系运行，以自动化奖励机制，通过市场经济模型自发调控的方式，做到在去中心化，无人为干预的情况下，使得算力资源节点能够通过 CRME 模型，自动进行供需关系的调配与控制，调节并入网络的节点数量，实现整个生态中资源调配、资源利用及奖励的自治生态体系，做到资源的最优分布与运用，同时保证了节点资源提供者的积极性与稳定性，确保算力的永久在线，与高频数据的高效率交互达到云储存所需毫秒级的处理需求。在实际的运行过程中，去中心化算力集群通过 Performance Evaluation，会对需响应的算力需求进行评估，确定所需的算力资源量，然后通过 Matrix SchDIPPERler，动态调度与需求相匹配的内存、带宽、算力等节点资源，做到高效与稳定兼得;调配到所需资源后，去中心化算力集将从 RDIPPERN 中获取到相应的服务数据包，并形成单个服务的 Isolation Container，为需运行的服务程序划出专属算力区间，并产生服务程序的冗余镜像副本，实现全球多节点资源备份，以供交叉效验。这样不仅保障服务所需的算力稳定以及不受干扰，同时也能验证主节点的运行情况，如算力确认、防止数据篡改等行为，为数据的安全可靠做出多重防护与验证。

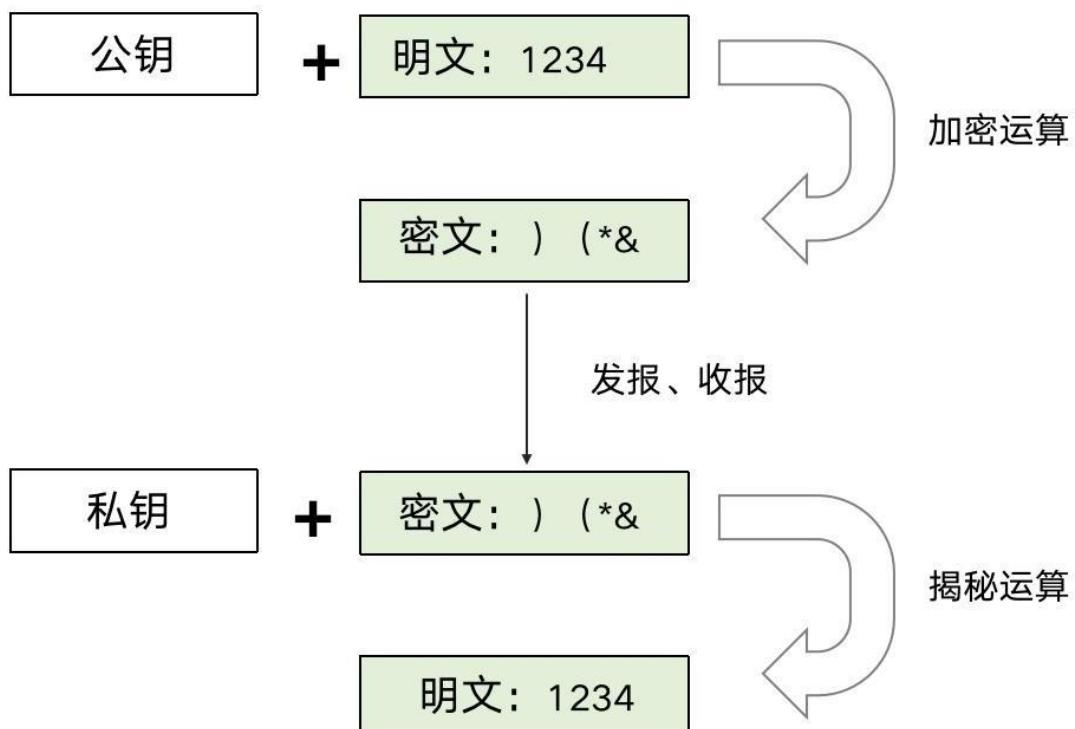
DIPPER 选择符合国内和国际标准的加密机制，对行业各项数据进行加密，用户间的交易数据和交易信息仅交易双方和有相应权限的用户可以查看。

### 1、私钥 (privatekey)

非公开，是一个 256 位的随机数，由用户保管且不对外开放。私钥通常是由系统随机生成，是用户账户使用权及账户内资产所有权的唯一证明，其有效位长足够大，因此不可能被攻破，无安全隐患。

### 2、公钥 (publickey)

可公开，每一个私钥都有一个与之相匹配的公钥。ECC 公钥可以由私钥通过单向的、确定性的算法生成，目前常用的方案包括：secp256r1（国际通用标准）和 secp256k1（比特币标准）。DIPPER 控制链与初始数据链选择 secp256r1 作为密钥方案。





### 3、加密

DIPPER通过非对称加密的数字签名的技术，做到了业务请求在传输过程中不被篡改，并且通过共识机制保证各节点的数据一致。对于已经存储的数据记录则通过节点内的自校验系统和准实时多节点系统来校验，以保证已经存储的数据记录同样无法篡改。

节点的自校验性是指 DIPPER 采用块链结构存储数据记录，其中篡改数据会破坏块链结构的完整性，系统可以快速校验出来并从其他节点将数据恢复。另外 DIPPER 每个记账节点都有自己的私钥，每个区块中记录了本节点私钥的签名，区块内数据的修改都可以通过签名校验出来。

准时多节点的数据校验：当节点的私钥被盗取，恶意用户是存在修改账本链上所有数据的可能性的，DIPPER 数字加密提供了准时多节点的数据对比机制，可以及时发现某个节点账本数据被篡改的情况。





## 4.9

## P2P 协议

DIPPER 上，每个节点（客户端）均采用 P2P 协议进行消息广播交互。对于 DIPPER 的数据区块，采用的 P2P 协议是标准的加密货币协议，该协议的核心特点是引入“幽灵”协议。而 DIPPER 的控制区块则采用标准的 P2P 协议，不支持“幽灵”协议。客户端通常工作于守护状态。该状态下，客户端执行的工作包括：

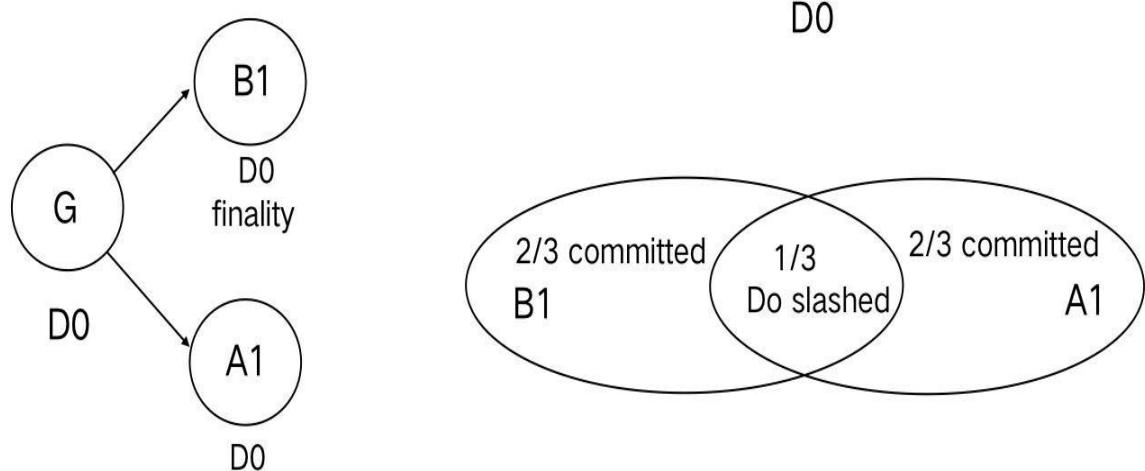
(1) 调用网络守护进程维护连接及定期发送消息； (2) 获取当前区块信息以及关联区块信息； (3) 获取工业制造参数，并对工业制造参数按照标准模型分析，确定是否提交更新的参数。

## 4.10

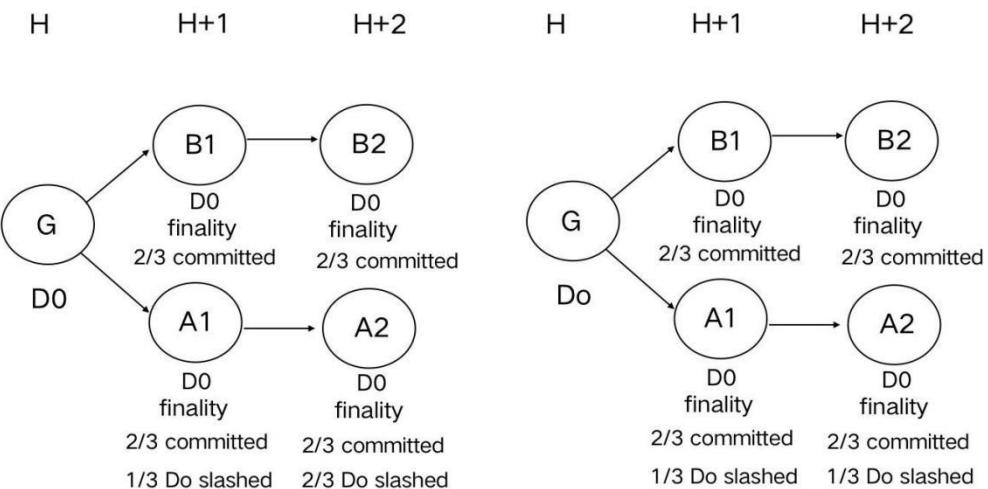
## DIPPER 恶意攻击防范与惩罚机制

PoD 中的每个高度上的区块都有共识有效期，如果某个高度距离最新高度超过 100 时，该高度的所有区块在共识过程中将被视为过期，那么这些区块上的所有新的共识活动将会被直接忽略。因此要在 PoD 中完成长程攻击(long-rangeattack)几乎不可能，但是在有效期内依旧存在发起短程攻击的可能性。短程攻击者 Attacker 试图在高度  $H+1$  的区块还没有过期的情况下，伪造 A 链来替代 B 链成为权威链，Attacker 需要让区块 A1 的得分比 B1 更高。由于多投会被严惩，所以 Attacker 将不可避免地要贿赂验证者，否则无法完成短程攻击。为了展现 PoD 共识算法的安全性，下面分别分析使不同数量的区块失效时，Attacker 需要付出的代价。如果 Attacker 想要使 B1 失效，最小代价的情况如图，就相当一次双重支付攻击，Attacker 幸运地成为了  $H+1$  高度的区块提议者，那么至少需要贿赂朝代 D0 中  $1/3$  的验证者多投使 A1 达到 finality，最小代价为所有押金的  $1/3$ 。

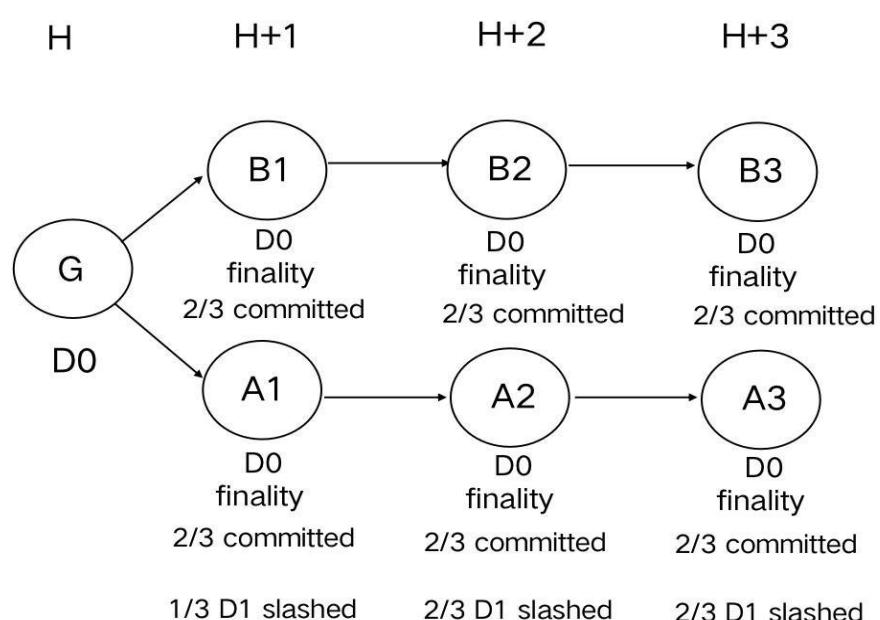
H H+1



如果 Attacker 想要使 B1-B2 失效，假设 B1 和 B2 都已到达 finality，块中交易都已生效，为了让这些交易失效，这里考虑两种情况。第一种如下图所示，高度 H+1 和 H+2 在同一个 Epoch 中，朝代相同，那么 Attacker 首先需要贿赂 D0 中 1/3 的验证者使 A1 达到 finality，此时这 1/3 的验证者将会被惩罚，押金被罚完。在 A2 的验证中整体押金总和只有 A1 中的 2/3，此时 Attacker 想要让 A2 到达和 B2 同价值的 committ 票，需要贿赂剩下所有没有作弊的验证者，合起来至少需要损失总押金的 3/3，即使如此也不能保证 A1 得分比 B1 高，攻击失败风险高。第二种情况如下图所示，高度 H+1 和 H+2 正好在不同的 Epoch 中，且朝代不相同，那么此时 Attacker 需要贿赂 D0 中的 1/3 来让 A1 到达 finality，然后贿赂 D1 中的 1/3 来让 A2 到达 finality，完成一次这样的攻击至少需要损失总押金的 2/3。综上，想要发起短程攻击导致两个 finality 区块失效，至少需要花费总押金 2/3 的代价。



如果 Attacker 想要使 B1-B3 失效，如下图所示，Attacker 首先需要贿赂 D0 中 1/3 的人完成 A1 的 finality，然后贿赂 D1 中 1/3 的人完成 A2 的 finality，最后需要贿赂 D1 中剩下 2/3 中的所有人来完成 A3 的 finality，综上至少要损失总押金的 4/3。要完成这些攻击准备将会十分困难，而且即使有幸做到了，也不一定能保证 A1 的得分比 B1 高，攻击也可能会失败。





## 4.11

### 弹性共识机制

一个稳定有效的区块生成机制是 DIPPER 区块链生态的基石，DIPPER 主链采用全新的 IPOS 共识机制来保证高频、稳定地生成区块，以提升用户体验。不同的领域及行业需要不同的网络运行机制，DIPPER 配置了不同的共识算法来满足不同的使用要求。DIPPER 协议下的共识采用可插入式算法，用户可以根据自己的需求自行选择共识算法。

## 4.12

### 预言机是链内与链外万物相连的桥梁

在古代，由于人们对于世界的认知处于初级阶段，相关知识累积的不足，对于超出他们认知范围内的事物无法找到合理的解释。有一个神谕出现，能够将无法理解的外界事物与现象，转换为自己所能够理解的信息，用以指导自身的实际判断与行为。同样，在区块链的世界里，由于去中心化的特征，每条链本身其实是与外界隔绝的。因此当外界信息需要与区块链发生交互时，区块链本身并没有直接的途径，可以随时获取并理解链外的信息。尤其是在智能合约的编写中，往往回遇到链下外界的限定条件无法被准确定义，或者在需要判定外部限定条件时，由于实际情况的复杂多变性，链上无法获取准确且明确的判定条件信息，导致智能合约无法正确执行。

DIPPER 的生态体系中，基于各种生态在 DIPPER 公链上自主性运行，云储存服务中的部分环节根据技术的发展进度，以及外部大环境等因素，在一定时间内，无法或者不需要完全地去中心化(例如法币支付、跨平台跨算力交互等)。而这些环节所产生的外部数据，需要与 DIPPER 上的智能合约进行交互，继而参与到 DIPPER 去中心化进程体系中。

# 智能 雲耕 DIPPER

全新模式

DeFi 之王



05

DIPPER

生态体系



## 5.1

### DIPPER 公链孵化中心

DIPPER 公链交易所设置有专属的项目孵化中心，帮助优质项目可以更快的获得融资以及技术支持，用户持有 DIPPER 可以享受各种优质项目的 IEO 空投，此外私人产品软件定制、一站式项目孵化等技术性输出都将通过 DIPPER 通证进行收费，部分收益平台将会进行销毁通缩。

## 5.2

### Staking 中心

DIPPER 公链交易所设置 Staking 中心 7 Staking 即 POS (或类 POS 机如 DPOS.LPOS.BPOS.HPOS 等)机制下的“抵押挖矿”，这是采用 POS 共识机制的区块链网络所独有的，也就是权益质押，通过对加密资产的通胀模型设计，任何人都可以通过加密资产抵押锁仓参与 Staking 保本“赚币”，实现加密资产的增发奖励，抵押的加密资产越多，收益越多。



## 5.3

### 流动性挖矿

为了满足 DIPPER 用户使用的数字资产流动性与深度，DIPPER 设有锁仓挖矿形式，俗称流动性挖矿，用户可以通过质押如 BTC、ETH、LTC、USDT 等主流数字资产，获取抵押算力获取利息。而用户用 DIPPER 平台生态子币和 UST 进行 1:1 质押到交易所，流动性挖矿为 DIPPER 在 Uniswap 贡献 ETH 对 DIPPER 流动性奖励权重 50%。发行总量 1000 万枚，零投资，零私募投资，零预挖，零团队预留，完全依靠社区与开源智能合约，同时 DIPPER 会拿出交易所手续费的 80% 用来回购销毁。

## 5.4

### DIPPER 预言机验证

DIPPER 将会发展预言机验证功能，通过去中心化激励方案解决价格数据上链的问题，具体是通过矿工双边报价的方式来生成价格，然后验证者如果觉得报价与市场价格之间有偏差，那就可以吃单套利，然后在链上直接生成价格。以 Chainlink 为代表的其他预言机，是通过分布式节点向链上合约填补数据的方式形成预言机数据，通常来讲就是由节点（也即矿工）把数据上传到链上。而 DIPPER 的价格比较能够代表市场公允价格，而不是依赖于节点的判定，但这在某种程度上也是 DIPPER 未来可能面临的瓶颈，即团队影响力被弱化。

除了上述使用外，未来 DIPPER 通证还会有更多应用场景，如算力合约云挖矿、合约系统、DAPP 研发投资等，其中获取的 80% 利润都将回馈给 DIPPER 通证持有者。

## 5.5

## Mizar 神器开阳

Mizar 神器开阳是自主研发的金融市场交易神器，主要有以下功能：

- (1)跨市套利：多个交易所，相同交易对之间的无风险套利；
- (2)单市场套利：同一个交易所，不同交易对之间的无风险套利；
- (3)策略回测：为历史数据提供多维度的分析报告；
- (4)趋势交易：不同 K 线条件下的趋势分析和全自动交易；
- (5)交易监控：为投资者提供实时的交易报单与信号提醒；
- (6)大数据分析：对交易数据进行分析，制定更优策略，获取更丰厚收益；
- (7)实时监控预警：7\*24 小时监控，实时推送，100% 及时送达消息；
- (8)会员服务：使用 DIPPERT 即可付费订阅，即可立刻享受私人投资顾问服务、私人投资教练服务、定期加密货币市场投研分析服务、结构化理财与对冲产品定制服务等。



## 5.6

### 摇光基金

目前，DIPPER 平台已发行加密货币市场第一支 DAO 形式的量化策略基金：摇光基金 ALKAID，是现货投资组合管理+去中心化资金托管为一体的去中心化资管基金，所有交易标的皆由神器开阳应用智能筛选，跟踪大趋势，获取长期利润回报。买入 DIPP 通证即拥有摇光基金的基金份额，并可在二级市场自由流转！

摇光基金同时提供股票金融证券、股票基金的投资教育与知识传播，为投资者普及证券期货投资常识，分享交易心得，传授证券期货交易技术，为多家私募基金提供研究报告、购买意见 以及高净值人群股票账户代资产管理，管理资产规模超过 3000 万美元，未来拥有 DIPP 通证即可享受资产“增值”！



正如人类对未知的探索

百闻不

如一见

下一个未知 又将为谁引领



06

DIPPER-Token

数字化凭证



## 6.1

### 介绍

DIPPER-Token (简称 DIPP) 是基于以太坊 ERC20 协议发行的可流通的全球数字加密货币，发行总量 1000 万枚！

DIPP 是开放式资管平台 DIPPER 的唯一平台通证，连接全生态体系，是社区治理的基石，支撑生态体系的重要枢纽。

DIPPER 重新定义开放式金融时代下的交易服务与资产管理，通过资金托管去中心化、标的交易去中心化、策略收益与回撤数据预言机验证、交易信号实时存证上链等技术手段，真正实现去中心化的开放式资产管理平台。

## 6.2

### 分配机制

1、发行总数：1000 万枚

2、分配计划

(1)DIPPER 基金会：500 万枚

(2)市场推广：100 万枚

(3)团队员工：50 万枚

(4)其他外部优秀社区贡献者：100 万枚

(5)DIPPER 节点：250 万枚，25 个创世节点



## 6.3

### 通证模型

- 1、DIPP 是开放式资管平台 DIPPER 的唯一平台通证；
- 2、使用 DIPPERT 支付神器开阳 MIZAR 付费产品；
- 3、DIPP 本身具备摇光基金市场份额，享受红利增值；
- 4、更多的策略/去中心化基金将会在 DIPPER 上发行。

## 6.4

### 销毁机制

DIPPER 基金会采取锁仓机制、通缩机制与线性解锁，三管齐下共同压制泡沫的形成。

员工 DIPP 前 3 年进行稳定锁仓，不允许流入市场，提供用户对于项目的忠诚度。

3 年后根据社区线性解锁逐渐释放。

DIPP 神器开阳每年收入的 80% 用于永久销毁，会导致 DIPP 总量越来越少，进而使剩余 DIPP 的价值越来越高。而造成这一趋势的原因，则是由于市场对 DIPP 的需求并未减少，稀缺性使得 DIPP 的价值将会越来越高。这也就间接导致了用户手中的 DIPP 升值，从而使用户所获得的利益增加，且摇光基金为 DIPP 提供基本面的支撑与保证，使得 DIPP 可以持续增长，同时 DIPP 节点持有者也可享受达基金会年度分红权益。



07

团队介绍



Prescott

英国大学金融管理学硕士， 曾就职于摩根士丹利投资银行，在交易支付领域有自己独特的见解， 2017年初开始系统研究区块链技术与加密数字资产ICO，对区块链产业潜力和未来方向有独到见解。他曾先后投资了 EOS、Filecoin、Cybermiles 等优质项目，观察并参与多个加密数字资产项目的社区建设与运营，拥有丰富的社区组织运作经验。在 DIPPER 牵头运营媒体宣传和战略研究。



Worthington

曾为谷歌、亚马逊等多家知名企业进行过顶层架构设计和诊断梳理的顶级企业架构大师，擅长为企业改造弱点，是激发团队精神的核心导师，也是帮助企业开启高速发展模式的品牌军师，曾用一年时间帮助某知名销售团队创造一亿美金的销售额，被无数团队视为最能赢得并洞彻人心的灵魂架构大师。



Garfield

DIPPER 大数据平台核心开发成员，牵头负责 ETL 核心指标计算、任务监控、任务调度、任务优化，并参与反作弊及推荐算法研究。作为区块链技术早期关注者，对比特币、以太坊、EOS 源码有深入研究，并为多个开源项目贡献代码、提交安全漏洞补丁。在 DIPPER 牵头产品开发、区块链技术实现。



Garfield

曾为谷歌、亚马逊等多家知名企业提供过顶层架构设计和诊断梳理的顶级企业架构大师，擅长为企业改造弱点，是激发团队精神的核心导师，也是帮助企业开启高速发展模式的品牌军师，曾用一年时间帮助某知名销售团队创造一亿美金的销售额，被无数团队视为最能赢得并洞彻人心的灵魂架构大师。



08

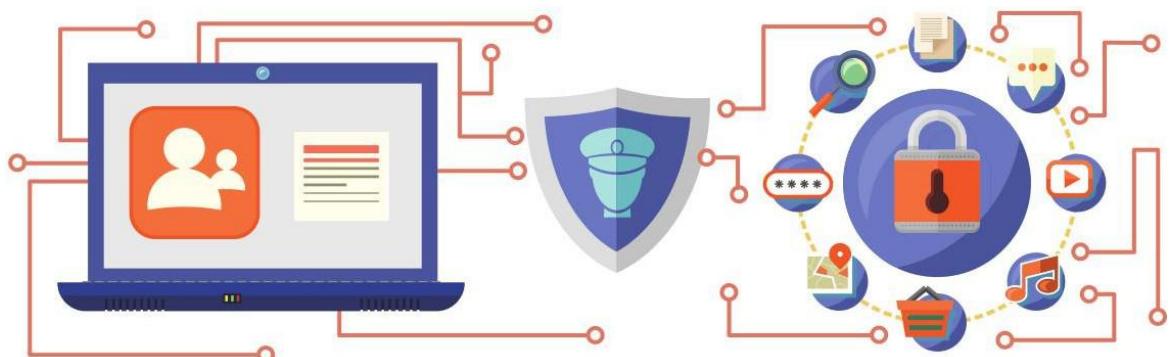
风险控制

免责声明

## 8.1

### 风险控制

DIPPER 基于本身生态发展的最大利益，会毫不犹豫地去惩罚生态系统的破坏者，其次，所有生态内的研发者、创新者、服务者，都会自发进入系统，针对性提供免费或收费的服务或工具，或自动请求代表用户发起群体诉讼，配合 DIPPER 快速来解决问题或降低风险。



## 8.2

### 负责声明

- ① 本白皮书仅作为一份概念性文件，用于描述 DIPPER 以太坊智能合约项目，并不构成招股说明书、要约文件、证券要约或出售任何产品和资产的要约。基金会和 DIPPER 公链团队无法保证白皮书信息的准确性和完整性，您应该在参与本白皮书中所述任何活动之前咨询自己的法律，财务，税务或其他专业顾问。
- ② 所有 DIPPER 公链项目的支持者，应当仔细阅读白皮书和官方网站的相关说明，全面理解区块链技术，明确了解项目的风险。
- ③ DIPPER 仅作为 DIPPER 公链平台的使用 Token，并不代表分红、增值、股权、证券及其衍生品的收益许诺，项目方不提供任何回售渠道，持有人获取后有权自主决定使用。
- ④ DIPPER 公链团队将不遗余力实现白皮书中提出的目标，并积极探索项目更长远的发展空间，然而由于外部环境和内部资源的不确定性，我们将保留对白皮书描述内容进行调整的权利，白皮书内容的所有变更我们并无主动告知义务，请参与者通过相关渠道及时了解更新，区块链技术仍然是一项非常早期的技术，DIPPER 公链团队不能完全确保所有技术的顺利落地。
- ⑤ 所有的技术类项目都具有被黑客攻击或代码漏洞造成用户损失的可能，我们不承担程序所出现的任何损失。DIPPER Token 目前通过智能合约发布，由于智能合约同样是一个比较早期的技术，DIPPER 公链团队不保证 DIPPER 公链 的合约完全没有安全问题，我们不承担智能合约安全问题造成的任何 DIPPER 公链的损失。

# DIPPER

## 公平 公开 透明

