

Delos 白皮书

DELOS WHITE PAPER

2017 年 8 月

目录

链上可信生态世界	1
1 实施内容	2
1.1 核心内容	2
1.2 概念产品	4
1.3 术语	6
2 价值模型	6
2.1 原生资产	6
2.1.1 初始发行模型	7
2.1.2 通胀发行模型	7
2.1.3 开户保证价值模型	7
2.1.4 基金会价值模型	8
2.2 发行资产	8
3 技术模型	9
3.1 技术架构	9
3.2 账户模型	9
3.3 关键技术	10
4 商业模式	12
4.1 NGO	12
4.2 智能投顾	13
4.3 中小企业	14
4.4 精准扶贫	15

5	路线图.....	17
---	----------	----

链上可信生态世界

未来企业的成功之道，是聚集一群聪明的创意精英，营造合适的氛围和支持环境，充分发挥他们的创造力，快速感知客户的需求，愉快的创造相应的产品和服务。

从互联网到移动互联网，再到物联网，从云计算到大数据，未来商业的一个基本特征已经非常清楚，那就是基于机器学习的人工智能将成为未来商业的基础。

From 《重新定义公司》

互联网技术的出现变革了社会协作关系，“世界变成平的”，世界范围的大协作空前高涨。移动互联网技术的出现更加拉近了人与人之间的社会协作关系，“世界变成了空心球”，全球范围内任意两人之间都能快速构建协作关系（ C_N^2 关系）。区块链技术以其密码学、P2P 网络、共识防篡改等特性，使世界范围内实体与实体之间的社会协作关系更加可信。

随着社会协作关系被不断的迭代再造，专业化分工更加精细，人与人的距离更加临近，关系越来越多，短小精干、虚拟化和分布式自律的组织必将是未来组织形态的一种关键形式。

基于区块链技术的基础协议已经得到了时间的验证，初步证实其是解决“不可信网络下可信协作”的一种关键解决方案。Delos 区块链基础协议的实施，初衷是将赋能型组织提升到区块链网络中，解决实体（人、组织和物）间的可信协作问题，构建高效和可信的分布式自律组织。

未来已经到来。世界分成了实体世界、联网世界和链上世界。能够优化或者变革社会协作关系的技术必将引领下一个时代的潮流，Delos 将与其他优秀区块链技术实现一道，构筑更加高效、更加透明和更加规范的分布式自律组织协作网络，共同铸造链上可信生态世界。

1 实施内容

短小精干、虚拟化和分布式自律等组织，一方面在于组织自身的自律，另一方面在于组织间的协作，并接受外部的监督。

Delos 的实施将使用区块链技术和分布式账本技术实现上述两方面内容。

使用区块链价值交换网络，实现组织中的财和物等资产在组织内部及外部交换全程可信、可追溯。

使用精简数据存储分布式账本持久化、防篡改地存储组织决策关联数据，实现组织的决策和执行高度确权，并可控制限度访问，接受外部组织或者人进行监督。

使用智能分析关键服务，基于链上和链下的数据，对组织进行同标准动态评级。

Delos 实施的内容主要包括了以下几个方面。

1.1 核心内容

(1) 搭建区块链价值交换网络

Delos 采用 Account 模型进行属性信息组织，任何一个人、组织和物都可以抽象为账户，每个账户类似一个神经元，之间的混沌协作，构建区块链价值交换网络。

Delos 采用两种智能合约实现。一方面，为了降低操作性风险，通过“时间事件+权限阈值+多签名”方式（非图灵完备智能合约）处理组织决策和执行过程，降低发生类似以太坊 DAO 事件的可能性；另一方面，通过图灵完备的智能合约处理逻辑复杂的契约关系。

Delos 多签名决策投票。支持资产数量阈值与多签名相结合的决策投票机制。

Delos 采用部分拜占庭共识机制。全网拜占庭共识机制增加整个网络的协作负担，降低网络的执行效率。部分拜占庭共识机制，一方面，在网络搭建初

期实现“安全性高于活性”的原则，另一方面，可以提高整个网络的执行效率，关账时间将<5S。

Delos 密码学将采用模块化方式处理。支持主流的非对称、对称和 Hash 等密码学标准或者算法，同时，支持本地化密码学算法（例如 SM2、SM3 和 SM4）。加密和解密非区块链技术的关键模块，而 Delos 网络由于自身的特性（下文描述）将原生支持加密和解密模块。

Delos 采用 P2P 网络模型。由于国际网络的延时等问题，在区块链网络实践过程通常是采用大洲或者国家进行连接，避免洲际光缆的延时和可靠性问题。一方面，Delos 会构建全球范围的区块链基础网络，另一方面，鼓励各个组织进行适应性改造，构建自己的联盟链或者专有链。

Delos 多节点模式。Delos 支持全节点、验证节点、同步节点、智能计算节点、账本节点等节点模式，适应不同用户的不同硬件资源。

Delos 账户连续性关联模型。一个分布式自律组织对应着多个账户，账户间、契约间、账户与契约间必将存在关联关系，Delos 将强化这种关系，构建类似神经网络的协作网络。

Delos 资产发行模型。在 Delos 中包括原生资产和发行资产两种资产模式。原生资产在网络启动时进行自动化的发行，发行资产可以映射为显示世界的物资、股票、数字化资产等等。每个账户可以自由发放一种或者多种发行资产，“账户 ID+资产代码”将唯一确定一种发行资产。由于发行资产需要发行账户进行信用背书，针对特定账户需要持有发行账户的发行资产，Delos 支持“申请+批准”模式，强化发行资产的账户管理。

Delos 支持分布式交易。分布式交易模块作为可选模块，可以在构建网络时灵活配置，支持异构交易。

Delos 支持跨链锁定。当前已经存在优秀的区块链基础协议，Delos 采用 Hash 签名方式支持与其他区块链基础协议的跨链交易。

网络健壮性。Delos 针对账户的开设采用保证金模式，防止大量无效账户挤进网络中，提高网络的整体自防御能力。

（2）搭建精简数据存储分布式账本

组织全生命周期决策和执行过程必将有关联数据进行确权固化，由于区块链技术特性，当前区块链技术不适应大量精简数据的快速存取，Delos 将构建针对结构化数据和小文件数据存储的分布式账本。

分布式账本存储。数据终将海量，Delos 支持“各取所需”模式，只需要同步自己的和自己想关注的的数据。

数据限度访问。区块链技术本身是一个大的非对称密钥库，原生支持数据的精细化控制，支持对数据进行限时、限次和限账户控制。

数据确权追溯。Delos 在支持数据确权、数据防篡改的基础上，支持数据关联关系锁定，从技术上控制组织的操作性风险。

网络健壮性。Delos 数据存储分布式账本对存入的数据进行原生资产锚定（数据保证金），防止大量无效的数据挤进网络中。

数据归档。Delos 支持非活跃数据自动归档，动态判断网络中数据的访问活性进行自动归档判断。

（3）搭建智能分析关键服务

基于链上不断增加的关联数据和原生神经网络结构数据，Delos 支持链上数据和链下数据的智能分析。

组织动态自动评估。根据链上数据进行模型自适应学习智能演进。Delos 原生支持组织动态自动评估，根据组织关联数据自动训练初始化模型，按照既定的频率进行自动化训练，并记录模型的各个中间版本，区块链节点可以根据自身的需求灵活配置选择信任的评估模型版本。

网络负载动态调整。根据网络中提交事务的数量，动态调配账本（或区块）大小，动态调整关账时间，以符合前端应用用户体验的需要。

链外数据智能分析。Delos 支持链接链外数据，并锁定模型的演化版本，支持模型采用图灵完备的智能合约进行形式化，同时支持锁定特定形式化模型（但无法链上自动执行）。

多方混合验证。Delos 支持智能模型的多方参与验证。

1.2 概念产品

Delos 基金会将为社区提供关键技术和基础产品服务，关键业务操作下沉到区块链成为区块链原生操作，方便快捷集成到各类已有应用。

Delos 基础协议采用 Apache2.0 开源协议，开源所有代码，并鼓励开源社区共同参与实施。同时，Delos 将提供原生的各类概念产品，并将采用 Apache2.0 开源协议，方便用户使用。

随着 Delos 各个阶段的逐步实施，共识节点部署、原生资产发行等关键事件采用去中心化策略，构建开放平等的 Delos 社区。

自包含特性。Delos 基金会自身作为一种组织，将使用 Delos 自身进行决策和执行。

(1) 分布式自律组织管理器

方便用户不做任何开发工作，快捷访问 Delos 网络进行业务操作。包括了以下功能：

组织管理。提供常规组织管理过程使用的契约模板，支持组织决策和执行操作。

资产管理。支持原生资产和原生资产的收发；账户资产发行；发行资产控制管理。

账本浏览器。支持区块链价值交换网络和精简数据存储分布式账本数据浏览。

(2) 开放中间件

Delos 中的特性提供相应的 API，支持集成到现有已有的应用场景。中间件将提供以下功能：

SDK。支持常用开发平台的开发工具包及单元测试用例。

高可靠特性。支持事务报文重发和缓存。

高性能特性。支持关联外部缓存及消息队列服务，支持事务排序机制。

(3) 桥接服务

Delos 支持与现有系统的集成能力。

客户化标识映射服务。将区块链账户标识与客户化标识进行映射。

风控系统映射服务。Delos 支持各个业务领域已有的风控规则进行对接。

审计系统映射服务。Delos 支持为现有审计系统进行数据清洗。

(4) 网络监视器

运行情况监视。监控网络当前资产、节点、账本情况的图形化监视器。

数据统计。支持当前网络中各个维度的数据统计，并提供开放 API 方便集成到已有的系统中。

1.3 术语

(1) Delos

区块链基础协议，在实现了区块链基本功能的基础上，提供了更加方便可靠的组织协作能力。

(2) 原生资产 (XDE)

原生资产是在 Delos 网络启动后，按照既定规则进行自动发行的资产，无发行账户，代号为 XDE。其中 delos 是 XDE 的最小计量单位，如下所示。

$1\text{XDE}=10,000,000\text{delos}$

(3) 发行资产

在 Delos 网络中进行自由发行的数字资产，发行账户地址与发行资产代码唯一确定一种发行资产。

(4) 事务 (Transaction)

对 Delos 网络进行数据写的动作。

(5) 动作 (Action)

对 Delos 网络进行数据写的原子操作，一个事务可以包含多个动作。

2 价值模型

2.1 原生资产

原生资产是使用 Delos 网络或者服务的商圈资产，用于兑换 Delos 生态中的产品和服务。

2.1.1 初始发行模型

原生资产的初始发行 1000 亿 XDE，按照“锚定价值”的原则，将采用如下的发行模式。针对任何人要获取原生资产，必须使用其他的资产或者价值进行兑换获取。

2.1.2 通胀发行模型

Delos 网络原生资产在初始发行后，按照每年通胀 1% 的策略进行发行，鼓励更多的组织使用 Delos 网络，通过 Delos 网络实现应用产品。

具体的通胀发行模型如下图所示。

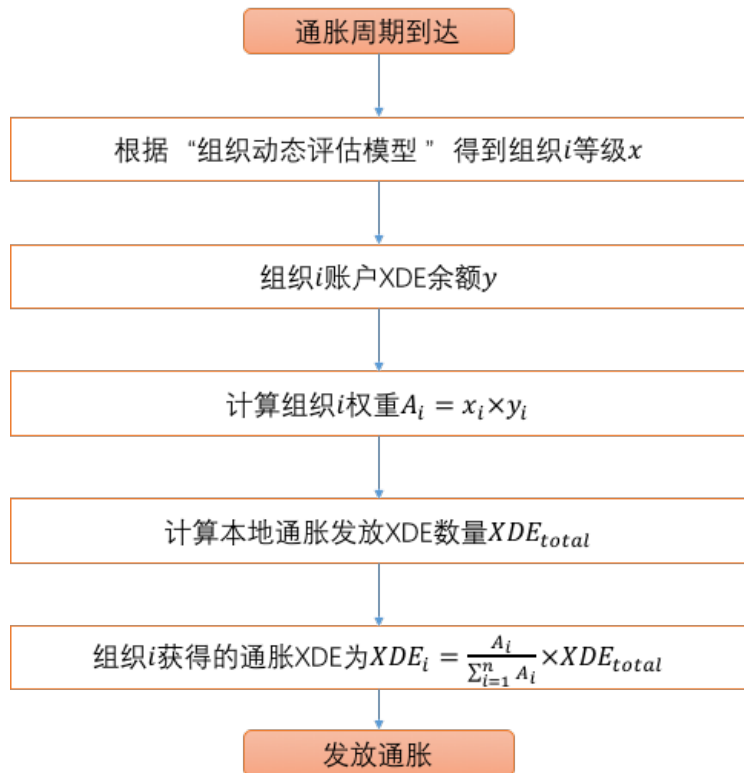


图1 通胀发行模型

Delos 通胀发放周期为每周，按照既定的发行模型进行自动发放。

2.1.3 开户保证价值模型

新用户加入 Delos 网络中时，需要使用 100XDE 保证价值来激活账户。

2.1.4 基金会价值模型

为了激发 Delos 基金会长期活力，同时，为了提高 Delos 网络自免疫能力，Delos 网络中每个事务需要一定数量的 delos 作为交易费，此部分费用会自动计入 Delos 基金会账户，用于社区维护日常各种费用。

事务费用计算公式如下所示：

$$\text{Fee} = (\text{Number}_{\text{action}} \times 100) (\text{delos})$$

2.2 发行资产

在 Delos 网络中的账户可以发行一种资产，该资产需要发行方进行信用背书。发行账户地址和发行资产代码唯一确定一种发行资产。

3 技术模型

3.1 技术架构

Delos 采用“核心+扩展+中间件+应用”的模块化设计思路，其技术架构大图如下图所示。

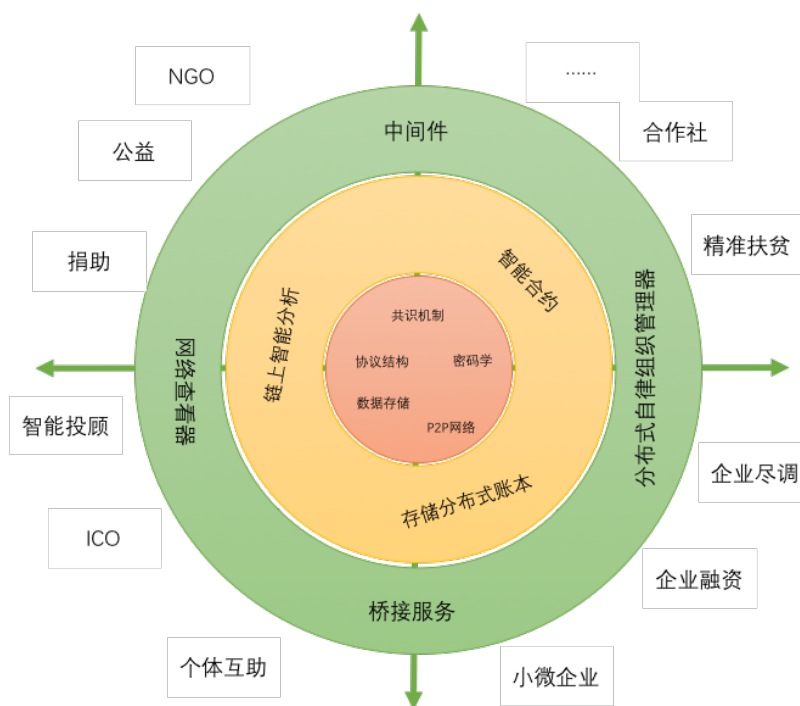


图2 Delos 技术架构大图

3.2 账户模型

账户模型重点描述在 Delos 中的主要实体关系，其实体关系图如下图所示。

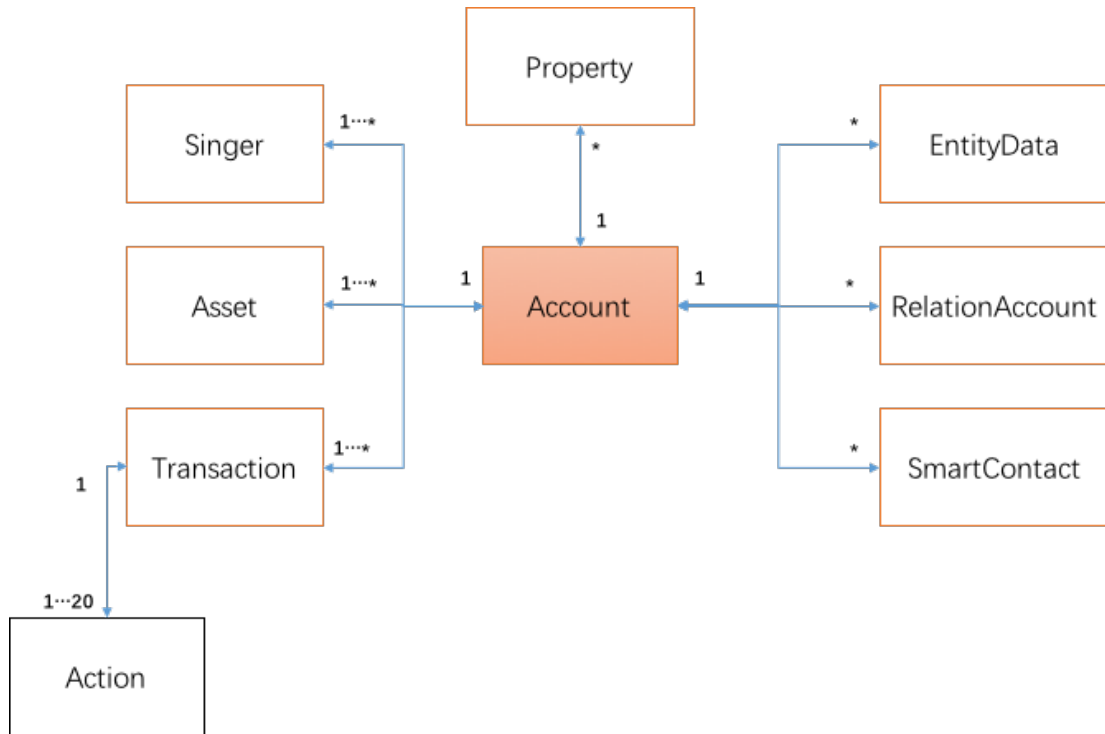


图3 账户实体关系图

3.3 关键技术

(1) 多签名及多层签名

Delos 事务操作是区块链数据写的唯一操作，其中包含动作，将各类动作权限分为高、中、低三类，针对不同的权限设置不同阈值。每个账户可以设置多个签名者和其权重，以控制账户的各类动作。

与此同时，Delos 提供最大三层的多层签名，如下图所示。

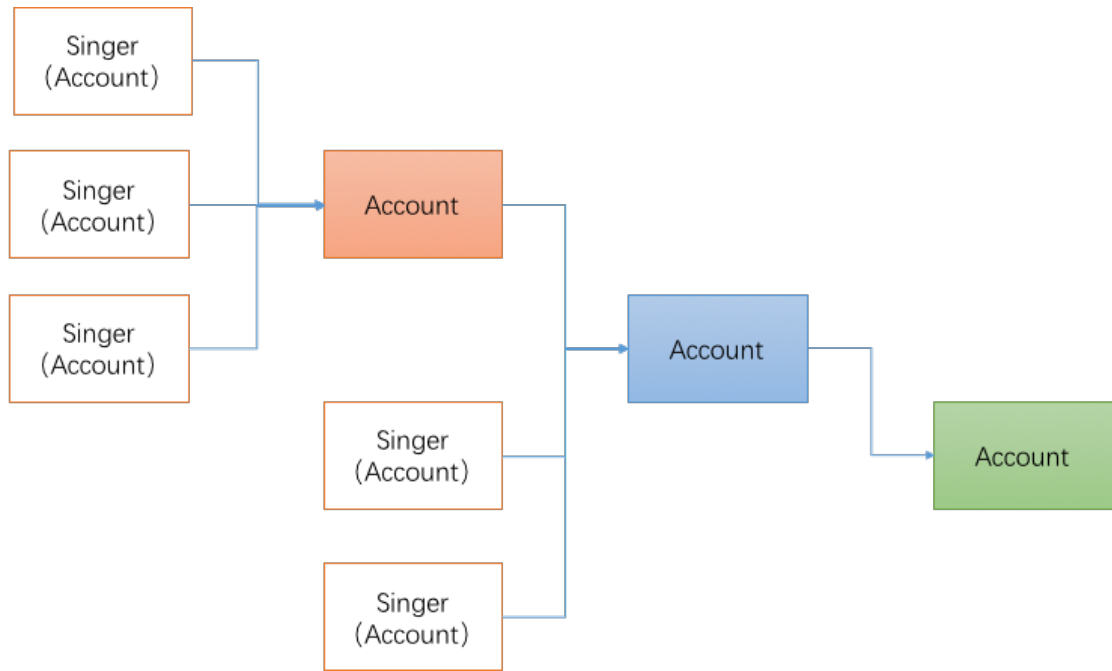


图4 多签名及多层签名关系图

（2）跨链资产锚定

Delos 将通过密码学特性，控制其他区块链网络中或者链下的数字资产，实现其他数字资产的有效管控。

（3）交易事务性

由于区块链技术的特性，账户资产一旦转出则无法回滚，为了应对此类需求场景，Delos 采用“事务+动作”的处理方式，一个事务可以包含多个动作，动作具有原子性，事务具有数据事务性。

（4）数据限度访问

Delos 网络提供存储分布式账本技术，针对数据可以进行限次、限额、限时和限用户等细粒度控制，在用户数据确权的基础上，充分保证数据的安全性。

4 商业模式

4.1 NGO

NGO 常具备如下特征：组织性、民间性、公益非营利性、自治性和志愿性，其涉及的领域包括环境保护、社会救济、医疗卫生、教育、文化等。此类组织多为致力于社会公益事业，提供公共物品，并无偿或低偿地服务在社会公众的生活中，但这些组织本身的资金能力有限，而往往需要各种社会力量在财力与道义上的积极支持和参与。

随着社会财富的累积，公众对于公益服务事业的参与积极性有愿意地显著提高，但社会组织的服务透明性还存在着一些问题，诸如：资金流向不透明，数据不公开，风险把控可能存在人为破坏因素，而致使组织可信度下降，社会各力量的参与度不高。

通过在 Delos 网络中实现 NGO 的信息披露可以很好地解决上述问题，本应用场景提出一种通用的关系账户架构如下图所示。

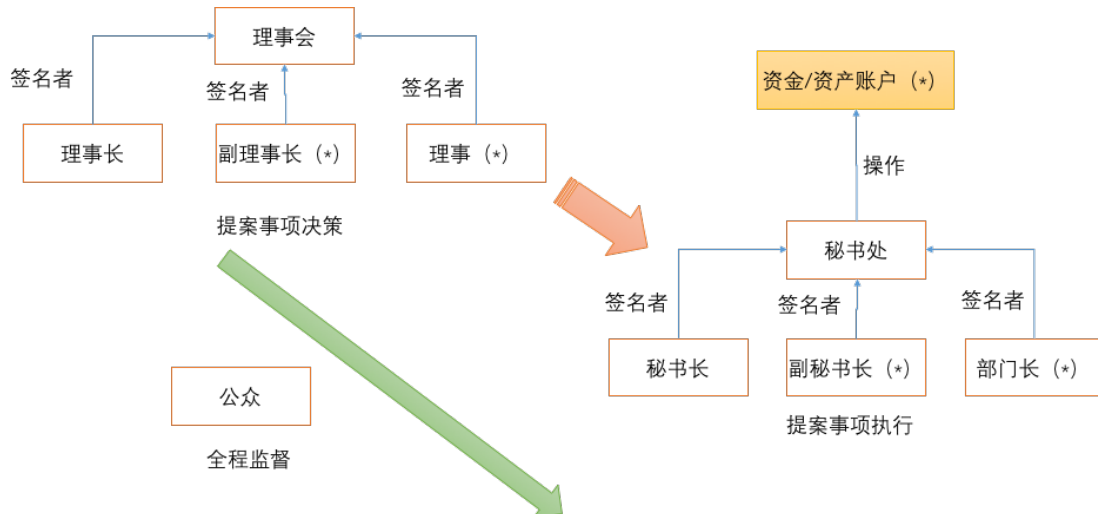


图5 NGO 关系账户架构图

如上图所示，理事会账户由理事长账户、多个副理事长账户、多个理事账户进行多签名操作控制，秘书处账户由秘书长账户、多个副秘书长账户、多个

部门长账户进行多签名操作控制，资金/资产账户是链下资金或者资产（物）进行映射的链上账户，由秘书处账户进行多层签名操作控制。

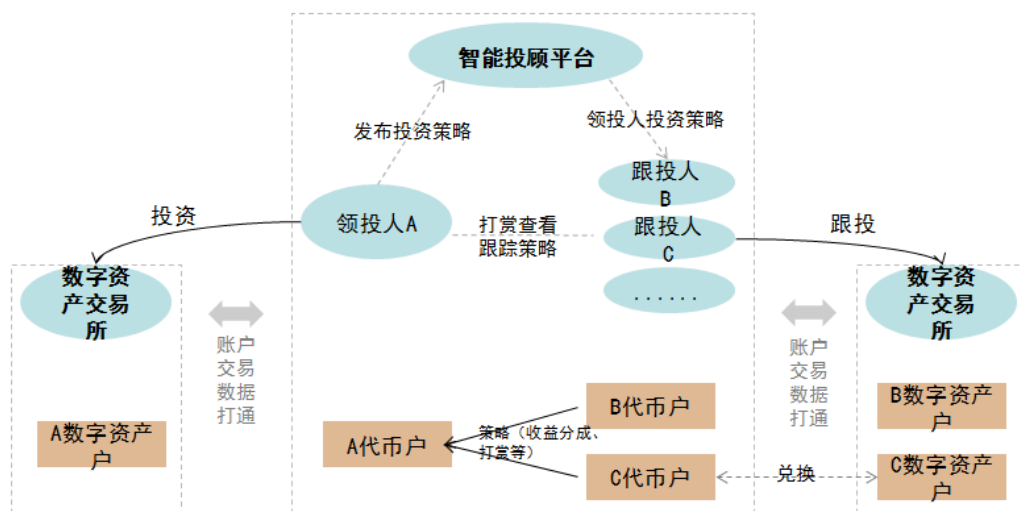
针对资金的筹措、使用决策由理事会进行多签名提案事项决策，理事会对资金/资产账户无操作权限，由秘书处进行多签名提案事项执行，提案事项决策与提案事项执行分别对应链上事务操作，同时，链上事务操作之间存在勾连关联关系，保证，公众账户可以对提案事项决策和提案事项执行进行全程跟踪。

4.2 智能投顾

眼前正在蓬勃发展的区块链市场也是如此，一大批早期进入市场的投资者已经享受到了市场高速发展带来的红利，然而更多投资者还在门外徘徊。越早进入区块链投资市场的投资者，收获就越大。数字货币的火热，让很多别有用心的的人，利用大部分投资者看不懂数字货币的情况下，将“数字货币”的概念与传销结合起来，形成“传销式数字货币”。由于传统的投资策略属于卖方市场，容易形成不负责任的一锤子买卖，各种“信口开河”和“事后诸葛”的投资策略充斥着投资市场，投资者对投资策略缺乏有效的信任，同时投资策略提供者也对投资者存在不信任，提供策略信息拿不到回报。普通用户理解门槛偏高，对数字货币投资能力有限。因此，我们尝试从智能投顾的切入点进行数字货币资产的投资。

基于长期的市场实践，以及技术积累，我们尝试结合智能投顾的专业投资能力，和区块链技术的去中心化、去中介化、不可篡改、加密安全性等特性，打造数字货币投资领域的智能投顾平台，希望能够推进市场发展中存在问题的解决。

- 1、投资者教育
- 2、孵化、优化投资策略
- 3、降低投资门槛，更加普惠



注：代币支付用于策略查看、跟踪、收益分成、投顾费用等

图6 智能投顾平台应用场景机制说明

保证交易记录真实有效有历史留存，包括孵化策略、连接投资人与交易所、详细公正的记录策略收益、交易记录、结果反馈等信息，平台不碰资产，陌生人通过投资社区之间的交流成为熟人，熟人跟投更符合用户心理。

领投人将在第三方平台的投资策略（或者人工智能投资策略）放到链上，供其他投资人查看或者跟投。跟投人跟投每笔交易后，所得收益与领投人通过智能合约进行分成，分成通过平台代币形式展开。发行币跟主流数字货币挂钩，在平台以奖励、打赏等形式获取流转。

4.3 中小企业

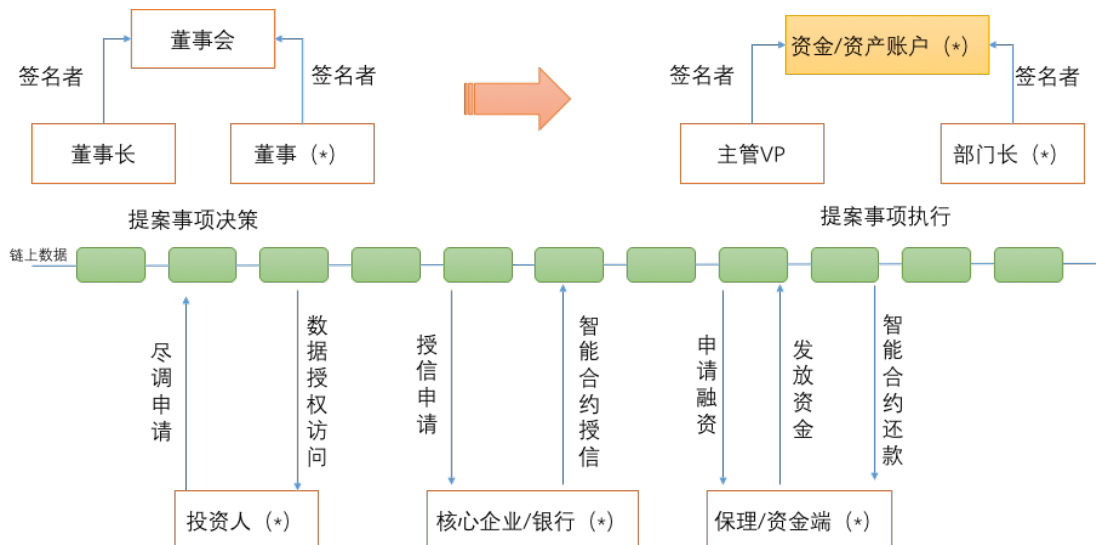
根据《中国中小商业企业协会》的数据显示，截至 2016 年底，中国的中小企业数量超过了四千万家，占据了中国企业总数 99.7%。中小企业的发展对于一个国家尤其是发展中国家的经济实力来说具有极大的影响，当前中小企业征信问题是解决中小企业融资的关键问题。

中小企业本小利薄，从而注定了它们无充足资金、无良好资产、无强大信誉的特质。无充足资金让中小企业长期面临着资金流不足的重压；无良好资产让中小企业难以通过金融机构的抵押信贷进行融资；无强大信誉将中小企业信用融资困难。

通过在 Delos 网络中实现中小企业的信息披露，首先，对于中小企业可以规范管理过程；其次，对于投资方可以随时进行尽调（数据限度访问）；最

后，对于企业产品用户来说更加清晰产品质量保证过程。通过 Delos 网络可以实现股权确权、股权转让、投资和融资等各类精细化场景。

场景应用的一种简化关系账户架构如下图所示。



如上图所示，董事会账户由董事长账户、多个董事账户进行多签名操作控制，资金/资产账户是链下资金或者资产（物）进行映射的链上账户，由主管 VPI 账户、部门长账户进行多签名操作控制。

董事会进行多签名提案事项决策，主管 VP 和部门长对资金/资产账户进行多签名提案事项执行。与此同时，投资人账户可以申请尽调，董事会授权其数据访问权限（数据限度访问）；董事会可以向核心企业/银行提出授权申请，核心企业/银行按照历史决策事项记录进行授信；保理/资金端根据历史决策事项、授信记录等信息对企业发放融资款项。

4.4 精准扶贫

是指针对不同贫困区域的环境，不同贫困农户状况，运用科学有效程序对扶贫对象实施精确识别、精确帮扶、精确管理的治贫方式。一般来说，精准扶贫主要是就贫困居民而言的，谁贫困就扶持谁。

长期来，由于贫困居民数据来自抽样调查后的逐级往下分解，扶贫中的低质、低效问题普遍存在，如：贫困居民底数不清，扶贫对象常由基层干部“推估”（推测估算），扶贫资金“天女散花”，以致“年年扶贫年年贫”；重点

县舍不得“脱贫摘帽”，数字弄虚作假，挤占浪费国家扶贫资源；人情扶贫、关系扶贫，造成应扶未扶、扶富不扶穷等社会不公。

利用 Delos 平台全程记录、顺序时间戳、不可篡改、可追溯、防伪造等特性，首先可以将扶贫模式由“自顶向下”转变为“自底向上”，明确贫困户，量化贫困的资产；其次，明晰扶贫重点，精细化扶贫，资产收益转化，提高贫困户自身造血功能；最后，贫困户脱贫前，政府等部门就可以精准支持，脱贫后，根据积累的信用，可以获得信用贷款支持，持续扩大收益规模。

场景应用的一种简化关系账户架构如下图所示。

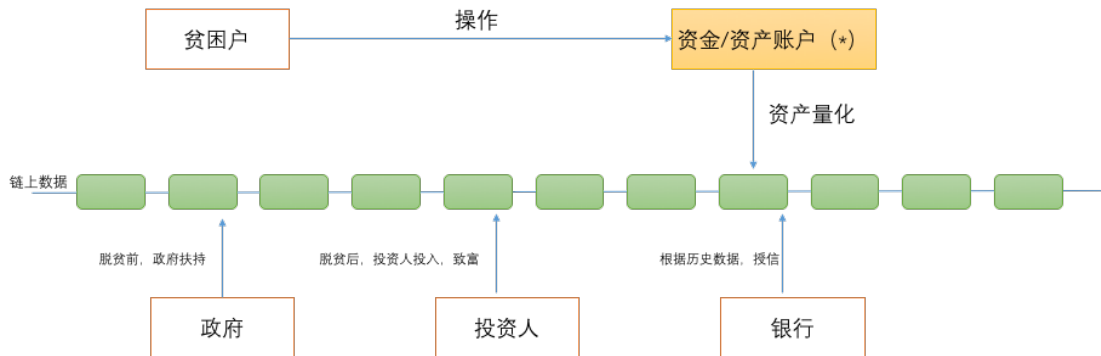


图8 精准扶贫关系账户架构

贫困户将自身拥有的能力或者资源进行资产量化，根据量化结果，在脱贫前，政府提供针对性的帮扶资金，将贫困户资产收益化，随着贫困户收益的增加，链上历史记录的增多，贫困户逐步转变成脱贫户，根据历史的记录，银行可以进行专项的授信，投资人可以进行针对性的投资，帮助贫困户彻底致富。

5 路线图

第一阶段：规划设计阶段

（2017 年 Q3）此阶段进行 Delos 规划设计工作，形成各类白皮书，同时进行详细技术设计与验证。

第二阶段：测试验证阶段

（2017 年 Q4）此阶段搭建完成测试网络，并提交开源 Delos 核心代码及关键概念产品，重点开展网络功能和性能的验证工作，开始开放社区的搭建工作。

第三阶段：生产运行阶段

（2018 年 Q1）此阶段搭建完成生产网络，重点完成去中心化相关工作，同时，NGO、智能投顾、精准扶贫、共享出行等关键种子应用上线。

第四阶段：发展推广阶段

（长期）此阶段进行功能和性能上迭代，并扩大社区影响力，在逐步加大应用接入的同时，重点推进 Delos 企业联盟（Delos Enterprise Alliance），鼓励企业广泛采用 Delos 作为区块链底层进行产品应用开发。