元界 白皮书

修订历史

版本	描述	作者	日期	邮箱
V0.1	初稿	初夏虎	201608	eric.gu@viewfin.com
V1.2	修订	陈浩	201609	hao.chen@viewfin.com
V2.0	修订	蒋佑明	201610	youming.jiang@viewfin.com

目录

摘要 ABSTRACT **4**

元界白皮书 **5**

1 MVS 的大背景——区块链 **5**

1.1 关于区块链 5
1.2 区块链简史 5

2 为什么做元界 **7**

2.1 虚拟即现实 7

3 MVS 的经济学模型 **7**

3.1 元界的代币——ENTROPY（熵） 7
3.2 微通胀模型 9
3.3 智能资产 9
3.3.1 智能资产的注册（Registration of SmartAssets） *10*
3.4 AVATAR-数字身份 12
3.4.1 {数字身份 s.t.app}⊆{数字身份 s.t.client/address} *13*
3.4.2 保密性与信息分享 *13*
3.4.3 自由创建、自主管理数字身份的理想 *14*
3.5 ORACLE-价值中介 14
3.6 MVS 潜在的风险与考虑 15

4 MVS 的设计原则 **16**

4.1 最小化设计原则 16
4.2 演进稳定原则 16
4.3 兼容原则 17
4.4 模块化设计原则 17

5 MVS 的架构设计 **17**

5.1 基础架构 17
5.1.1 基础架构图 *17*
5.1.2 业务层级结构划分 *19*
5.2 功能迭代开发一览 21

6 MVS 的共识选型与核心功能 **21**

6.1 共识机制（CONSENSUS PROGRESS） 21
6.2 交易类型 27
6.3 账户模型 27
6.4 数字身份与 DATA-FEED 27
6.5 跨平台 28

摘要 Abstract

Metaverse Project （简称 MVS，中文名元界）。

元界是一个基于公有区块链技术体系的去中心化平台，涵盖了数字资产和数字身份。元界通过构建一个 2B2C 通用技术平台，将资产数字化（类比资产证券化），例如我们可以将珍稀物品（艺术品/古董）数字化、知识产权数字化、票据基金等收益权数字化，提升市场运作效率，通过配备智能合约和我们的数字身份，将一个一个的价值孤岛连接成价值互联网络。

MVS 希望通过紧密结合现实业务进行迭代开发，所以针对 MVS，我们在不同的版本支持不同程度的功能， MVS 的开发将根据市场的反馈进行迭代更新，所以在 MVS 的初始版本中，技术上我们仅保留公有区块链的最小化可用操作集合，即我们将以比特币为基础进行重构开发，增加数字身份和数字资产等功能。

元界最初是由维优的团队组织开发和维护，元界基于 AGPL3.0 许可协议。元界源码在上线初期开源，开源地址 GitHub： https://github.com/***

元界白皮书

1 MVS 的大背景——区块链

1.1 关于区块链

区块链技术来源于比特币系统，正是由于这项技术的去中心化、不可更改账本的特性，比特币系统才有能力解决一些问题，诸如交易造假、双花等。很多人都认为比特币系统是区块链技术的第一个应用。

比特币系统毫无疑问是一个精巧的发明，而背后神秘的创造者中本聪（Satoshi Nakamoto），曾将比特币系统定义为“一个点对点的电子现金系统”。在过去七年的潜移默化中，比特币周边的生态系统从疑云中成长起来，如今比特币的总市值已经超过了 100 亿美元。

众所周知，比特币**不仅仅**是一个新的现金系统，它同时也有区块链属性，并通过区块链技术来保障比特币的去中心化账本。更重要的事实是，比特币系统让我们确信：物理性的资产可以被，也必将被数字化。区块链作为一个去中心化的系统，以密码学的方式维护了一个不可篡改的账本，从而让多方在无需建立信任的环境中进行自由的价值互动或交易，这种模式可以给银行业、保险业、医疗业、物流业、媒体业等众多行业带来重大变革。

1.2 区块链简史

区块链技术和概念的发展伴随着对比特币系统的解构和重构。从数字加密货币到区块链概念的进程中各个重大里程碑，我们发现域名币、点点币做出了非常基础的贡献，而比特股和以太坊分别带来了两次影响更大的概念升级。

- **域名币和点点币**

域名币是首个从比特币分叉出来的应用项目，它被设计并执行的目的是在原有的电子现金系统中加入“去中心化域名”的概念（可以认为是数字身份的前身），并且采取了与比特币合并挖矿的方式保障节点网络的安全性。

如果所有的区块链都需要设计一种新 POW 机制的挖矿算法、或者需要共用一套存在挖矿中心化问题的 POW 机制、并且需要部署硬件矿机作为网络的全节点的话，那么区块链的发展将落后现在很多年。点点币系统提出了不同的共识算法概念，也就是后来非常著名的 POS 权益证明机制，在 POS 机制提出之后，关于区块链系统的新的尝试才能以低成本的方式不断涌现，共识机制的微创新也持续地在推动区块链技术的发展。

- **比特股**

比特股是站在 POS 共识机制的巨人肩膀上成长起来的项目，并在之后将共识机制改良成为 DPOS 权益代表证明。在比特股上，新的概念被不断提出来，包括更加突出数字身份的项目 Keyhotee，以及通过定义多种交易类型，可以更简便地登记、发行数字资产等。比特股主要去中心化交易所的概念，并为了实现良好的交易体验，重新改进了出快的速度，达到秒级出块，相应地也牺牲了一些系统的稳定性。

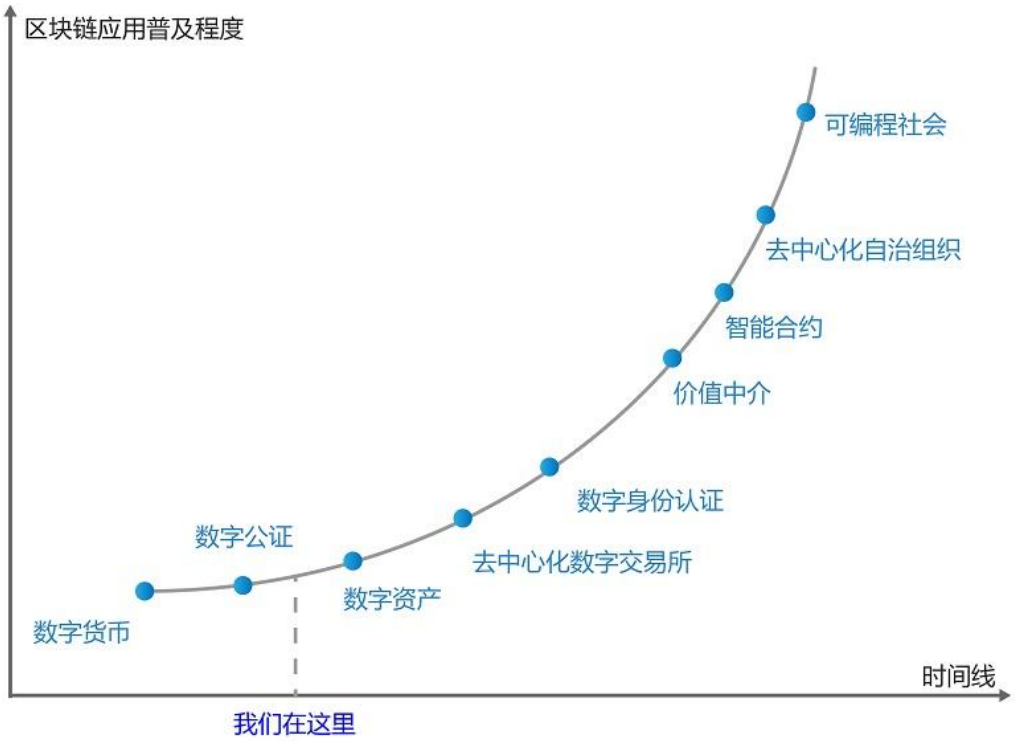
- **以太坊**

与点点币和比特股不同，以太坊项目在早期采取 POW 的共识机制保障网络不受攻击，而在近期将通过分叉的方式转变为 POS 的共识机制。这样的设计主要考虑的是初期整个系统的安全性问题。此外以太坊在实践智能合约的概念，这是以太坊除了对自身公有区块链的出块特性、奖励机制等作出改进之外，最重要的贡献，通过智能合约和专门开发的 EVM，以太坊拓展了区块链能够处理的交易类型，不过所有的交易类型都是通过合约的形式实现的。

- **公有链和许可链**

公有区块链和许可区块链的区别主要体现对待节点的态度以及信任的范围两个方面。在公有区块链上，节点接入的门槛很低，我们一般认为每个节点都是不可信的，因此需要以某种证明机制（POW,POS 或者它们的改良）来选择记账节点，而许可链只对白名单的节点准许接入，并可能会设立严格的防火墙。因此公有区块链的信任机制是面向大众的，范围很广，所有参与公有区块链记账和使用的人都在信任的范围之中，而许可链的信任范围只存在于许可的节点之间，范围相对较小。

区块链发展路径图



比特币在“数字货币”和“数字公证”处，比特股在“去中心化交易所”附近，以太坊在“去中心化组织”处。而实际上，区块链和现实的接触点，还在图示位置。所以区块链仍在成长，我们希望构建一个基础设施完善的价值传输网络，上层应用丰富的区块链生态，仍然需要付出巨大的努力。

2 为什么做元界

2.1 虚拟即现实

Metaverse 一词最早出现在 1992 年的 Neal Stephenson 的科幻小说《snow crash》(中译名《雪崩》)中，在书中描绘的世界，人们拥有自己的化身 Avatar，通过化身在一个虚拟现实的世界中互相沟通，甚至与电子代理发生关系。

现代的生活就像 Neal Stephenson 在 1992 年描述的那样，我们的工作与生活越来越倚重互联网，人们有大量的时间在线上而非线下，人与人之间的沟通方式发生了变化，频率也比以前更加频繁，在不久的将来，我们可以预见人们会经历从信息互联网到价值互联网的转变，越来越多的智能资产的转移将发生在线上，Avatar（数字身份）和中间媒介 Oracle 将成为那时候的经济主流模式。

元界项目的取名受到了 Neal Stephenson 的 Metaverse 的启发。

3 MVS 的经济学模型

3.1 元界的代币——Entropy（熵）

- **Entropy（熵）**

熵（entropy）的概念借鉴自热力学中对微观粒子混乱程度的描述，它将作为成为元界 Metaverse 的代币，缩写为 ETP。在 Metaverse 上 ETP 的 ICO 及 POW 挖矿的发行总量是 1 亿枚，ETP 的最小单位是 10^{-8}，即小数点后八位小数，类似于比特币的设计。ETP 可以在 Metaverse 上转移和交易，后期 DPOS 阶段将成为选择记账人的重要影响因子，ETP 的安全性由椭圆曲线数字签名算法保障（ECDSA）。

ETP 并不是一种新形式的数字货币，它代表 Metaverse 的股权。因此，ETP 的价格不会锚定任何法定货币或者加密货币，例如比特币，而是取决于 MVS 的生态发展以及 ETP 的市场需求。

ETP 将被用来衡量 Metaverse 上的智能资产的价值，或者作为金融交易中的一般担保物。与此同时，当使用 Metaverse 系统的过程中需要收费的时候，将是以 ETP 的形式进行收费，例如创建一种新的智能资产，注册一个 Avatar，将自己标记成为一名 Oracle，或者

在 MVS 上请专业机构对以上的资产或身份进行认证。

- **ETP 的分发机制**

（1）ICO 和社区建设

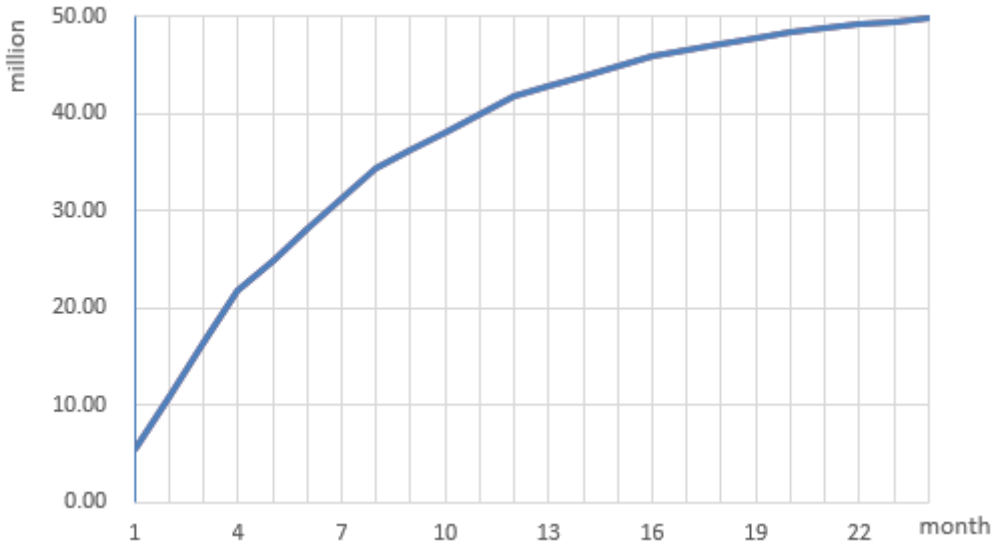
在区块链领域，ICO 的分发机制是一个代币分发的常见和默认方式。2014 年 1 月份，比特股项目开始了为期 200 天的 ICO；之后的 7 月份，以太坊项目发起了惊人的 25000 枚比特币的 ICO；之后的 2016 年有 DigixDAO 项目和 Lisk 项目也分别发起了 ICO，还有充满争议的 TheDAO 项目。国内的小蚁项目也在 2015 年 10 月和 2016 年 9 月分别成功地众筹筹集了 2100 枚和 6119 枚比特币。

Metaverse 项目的 ETP 已经通过一次 ICO，向外界分发了约 2260 万个 ETP。还有大约 2740 万 ETP 会设立元界基金会，用于跟投对元界社区有促进作用的区块链项目 ICO，以及对社区主要贡献者进行奖励。

（2）POW 机制挖矿

剩余 5000 万的 ETP 将通过 POW 机制以区块奖励的方式分发给 MVS 系统的维护者，这个过程或称为挖矿。

预计 POW 的过程将持续 24 个月，但是根据实际算力的情况，这个过程也可能会提前或者延后完成。通过 POW 发行的 ETP 累积量与时间的关系大致如下图：

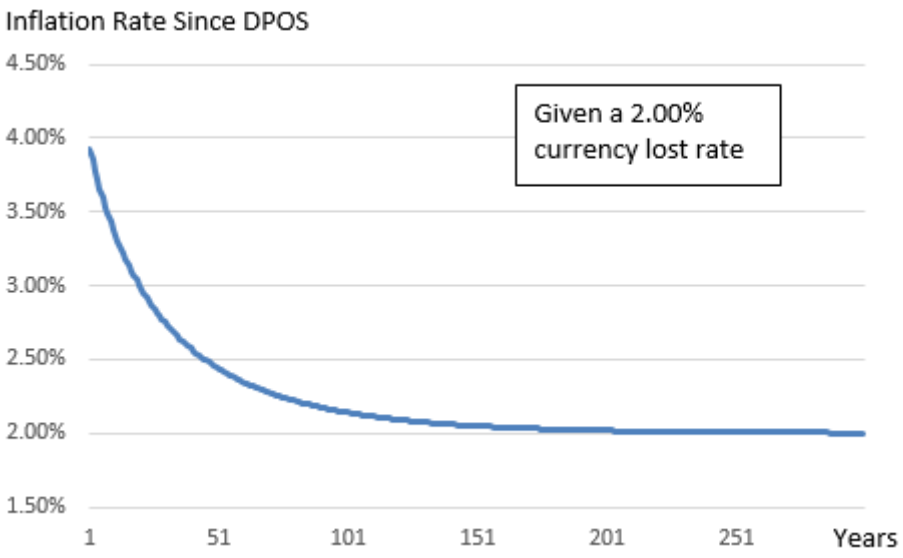


具体挖矿参数在技术细节章节有详细描述。

3.2 微通胀模型

ETP 是 Metaverse 这个 DAO（Democratic Autonomous Organization，民主自治组织）的股权代币。ETP 不是一种流通货币，因此 ETP 不应该有通胀；但是考虑到代币在使用的过程中的各种自然损耗，包括意外丢失，忘记密码，或者持有人自然死亡，这将使得 ETP 存量不足的问题日益严重。在以太坊的白皮书中，Vitalik Buterin 提出来一个代币丢失率的预测，他认为每年将有约 1%的丢失率。

考虑到 ETP 在流通过程中有部分丢失，零头损耗，以及大量质押和交易所囤积情况的可能，我们将为 ETP 设定一个微通胀率，每年将有总量为 4,000,000 个 ETP 以 DPOS 阶段区块奖励的方式流入 MVS，由于 ETP 的总量在逐年增加，年通胀率也由 DPOS 早期的约 4%降至一个固定数值，这个时机是当 ETP 的投放率等于流通损耗率（长期被囤积起来的部分 ETP，需要按一定比率计算流通折损，这样才是调整后的流通损耗率）。下图是假设这个流通损耗率为 2.00%时的情况，我们可以发现随着年份的增长，通胀率会向这个损耗率缓慢趋近，最终稳定在 2.00%上。



3.3 智能资产

比特币的维基百科词条中提到，Nick Szabo 在他 1997 年的研究中提出了“智能资产”的概念，实际上维基犯了一个错误，Szabo 只是定义了一类嵌入了智能合约来实现特定契约条件的资产。

在以太坊的项目中，智能合约的概念被过度地强调出来，数字资产必须依靠智能合约才能存在。这样的设计是有违直觉的。

在元界中，我们要重新强调数字资产的重要性，依赖性顺序是智能合约需要数字资产才能工作，而不是反过来。如果我们将面向对象的编程模式来类比就会发现，数字资产是一个面向对象的类 class，而合约是 class 类里面的方法。

与以太坊的设计不同，元界的原生数字资产 ETP 将沿用比特币系统的 UTXO 方法（未交易输出 Unspent Transaction Output），任何交易都将由一组输入和输出定义，并且带有当前 ETP 的所有者和之前交易者的私钥签名，由以上这些元素共同组成新的 UTXO。而智能资产将尝试账户模型，这样既不会过分增加系统的复杂度，也能保留 UTXO 的好处。

这样设计的结果是，元界上的数字资产将像比特币一样可以很方便地进行接收和发送，只有当更复杂的交易模式需求出现的时候，才会需要智能合约。

3.3.1 智能资产的注册（Registration of SmartAssets）

智能资产的注册要考虑以下几个问题：

（1）为什么要注册智能资产？

区块链有一种价值在于提供了一种可公开共享的数据存储：只能有序添加（append-only with timestamps），不允许对过往记录进行修改、删除的操作（注意是“不允许”，而非不可能，在实际运行中，过往记录被修改和删除的可能性来源于区块链网络的抗攻击能力，以及是否有掌握特殊权限的力量进行人为的干扰）。

这个特性满足了“注册”功能的设计需求，即公开、唯一并且可信，因此不仅是智能资产的注册有必要以区块链的形式实现，任何其他有价值的数据，都有理由寻求某种方案存储在区块链上。

（2）如何设计注册智能资产的功能？

当我们说“注册”一样事物的时候，我们其实是在尝试用数据描述这件事物；从这个角度来看，注册智能资产的第一步是找到一组数据描述一个“资产”，并且注意两个设计要点：

A.这样的一组数据描述应该能被重复使用，只能有一条记录的表设计是低效而失败的；

B.考虑到将来可能的应用场景，配套设计合适的查询、新增、计算和验证接口。

鉴于“资产”这个事物的通用属性相对简单，特殊属性各不相同，并且重要的数据产生于资产转移过程中，因此注册智能资产可被简单描述为填写一个类似下表的表单：

类别	**智能资产字段**	**解释**
通用属性	标识	唯一标识该资产的一串字符串
	总量	转账时验证资产有效性的基础属性
	最小单位	
特殊属性	描述	特殊属性存放的地点

满足了以上基本信息结构的设计之后，还要考虑这些信息将被如何使用。比特股（Bitshares）尝试过基于市场功能来发行资产（复杂的超额抵押、锚定机制、喂价机制等），实践证明局

限性比较大，在底层金融设施不完备的情况下，市场并不能在更大的资产规模下发挥其应有的作用。

同时比特股和以太坊等新生代区块链系统的设计中也探讨了资产证明（PoA，Proof of Assets）机制的可行性。在比特股上，如果能通过其他方式证明智能资产的真实性，例如在论坛发布带有私钥签名信息的帖子，或是提供资产证明证书并绑定了个人（账户）的信用等，就可以在公开市场上寻求认可该资产的人对其进行定价；不过这个过程中的问题是，要提供这样的证明，在比特股上并不方便，而且用户也没有动机在一个流动性不大的内盘市场发行他们的区块链资产。在以太坊中，智能合约似乎可以解决任何问题，其中就包括定义代币（token），一些代币其实可以被视为智能资产，因为它们可以是有价值的，也同样是可编辑的。由于在理论上智能合约支持任何狂野的商业模式，因此才会出现像 Digix 这样的项目，它们巧妙地寻求第三方（黄金交易所、会计师事务所、托管商）来提供一系列资产证明，形成市场认可的证据链。而这一切证据都记录在区块链上，使得这种资产登记变得不可篡改（当然先不考虑硬分叉的人为事件）。

第二步是注册费用做经济设计，元界做了如下考虑：

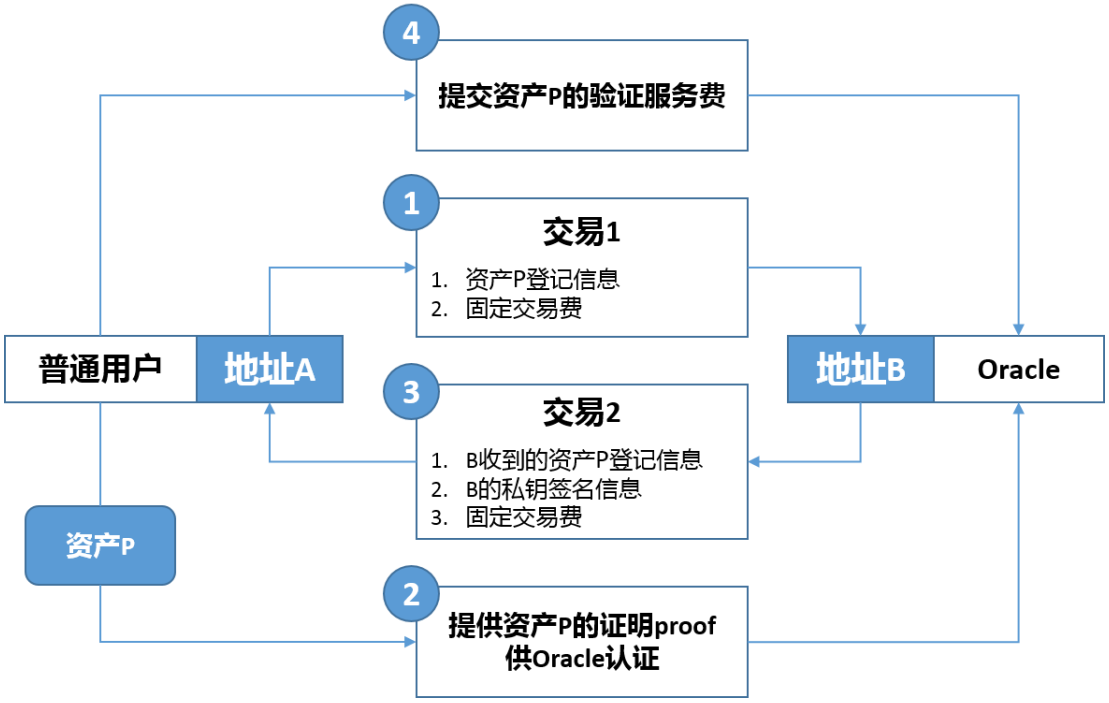
A. 注册费用的正当性和合理性。注册费用无疑是正当的，这是一种系统自我保护的机制，当注册智能资产不需要任何代价（或者代价微不足道），系统面对 DDoS 攻击时将不堪一击。不过需要确定的是，这笔费用收取多少是合适的？目前谁也说不清楚元界区块链上的一个比特价值多少钱，就设计而言，这个价值可能是变动的，因此费用模型倾向于使用一个加权计算的结果。

B. 这笔费用并非传统意义上的转账费用，因为这笔交易也不是为了转账，而是一种有特定功能的新交易类型。所有新交易类型产生的交易费，将有一部分被归集到一个特殊的系统地址，用于支持元界的开发社区，剩余的分配给出块的节点。

（3）注册智能资产之后能做什么？

智能资产在区块链上的登记并不是孤立的动作，登记之后意味着需要被其他人认可（PoA）才有资产属性，否则只是一串自定义的数据；一旦被认可了，智能资产就同时有了两重属性：价值属性和可编辑属性（或者成为“值得编辑”）。其中价值属性将依赖不断的交易和市场价格变化来体现，而可编辑属性将通过各种技术手段（基于虚拟机的智能合约或者基于业务的脚本语言等），将现实社会中对资产流转的约束条件添加到区块链中登记的智能资产中去。

元界将重点发展 PoA 模式的智能资产，因此设计中将特别关注如何帮助用户方便地提供资产证明，在以上手段之外，元界还归纳提出了：（1）价值中介（Oracle）通过他们提供的 datafeed 来作为资产价值的证据，从这个层面上看，Digix 项目中的第三方都是 Oracle 的实例；（2）一种基于区块链交易（transaction）的信用传递模式，即通过构造两笔对称的交易，实现 Oracle 对资产的认证操作，如下图：



保障普通用户和 Oracle 不会被欺诈的设计细节比较容易实现，在 Oracle 部分补充。

3.4 Avatar-数字身份

一个人无法像现实生活中持有黄金实物那样在物理上持有线上的智能资产，智能资产的所有权需要通过个人对数字身份的掌控、再由数字身份以数学上不可伪造的方式持有。Avatar 作为一个线上身份的象征，可以代表人们在区块链上持有智能资产。

创建一个 Avatar 远不止给你的公钥加上一个别名，就像身份证、手机号不是你的姓名的别名一样，其他有应用价值的信息也将依附在 Avatar 的唯一索引之下，并以密码学的方式保护信息的隐私性，除非 Avatar 的所有人授权信息的访问（例如提供私钥签名信息、发起特殊交易、或者以智能合约的方式），否则无法获取一个 Avatar 的加密或非加密信息。在这里零知识证明、同态加密等技术将发挥巨大作用，Avatar 不需要展示信息的内容就能够获得匹配验证、信用评价等服务。在比特币系统中我们通过公私钥对可以匿名持有比特币，但是在现实生活中，大多数活动需要我们提供各种程度的个人信息，例如，如果你需要加入一个女企业家的俱乐部，你需要提供年龄和性别这两个基本信息。

在 Avatar 背后，可能是一个真实的人，也可能是 AI（人工智能），或者是物联网（IOT）中的一台机器，或者是一个公司、组织。

一个 Avatar 可以拥有多种类型的智能资产，一种智能资产也可能由多个 Avatar 共同拥有，avatar 和智能资产是多对多的关系。这种关系看起来比较复杂，但是这是现实生活中真实的所有权关系，同时在元界区块链上，这些关系被确权并且得到了加密技术的保障。

构建在智能资产之上，特定的（金融）应用场景可以很丰富：交易、借贷、租赁，还有抵押等。

3.4.1 {数字身份 s.t.app}⊆{数字身份 s.t.client/address}

应用中的数字身份信息是用户端数字身份信息的子集，这意味着（1）用户端对自己身份信息有着绝对的所有权和使用权，应用端虽然短暂地获得了使用权，但是所有权仍然是归属用户端的；（2）用户端与应用端必须共享一部分数据字典，否则无法实现字段信息的对接，交集将为空。

对于（1），基本主张是保护用户端的身份信息相关的利益不受到应用端的侵犯，用户有义务在元界区块链上通过“及时创建身份”、“更新状态”、“寻求认证”等主动管理方式来宣称对数字身份的所有权；可以通过选择授权的方式换取应用端服务而不会丧失所有权。这个问题将在后面展开讨论。

对于（2），基本主张是允许用户端自己定义字段名，但是也要限制这种自由。这个问题也将在后面展开讨论。

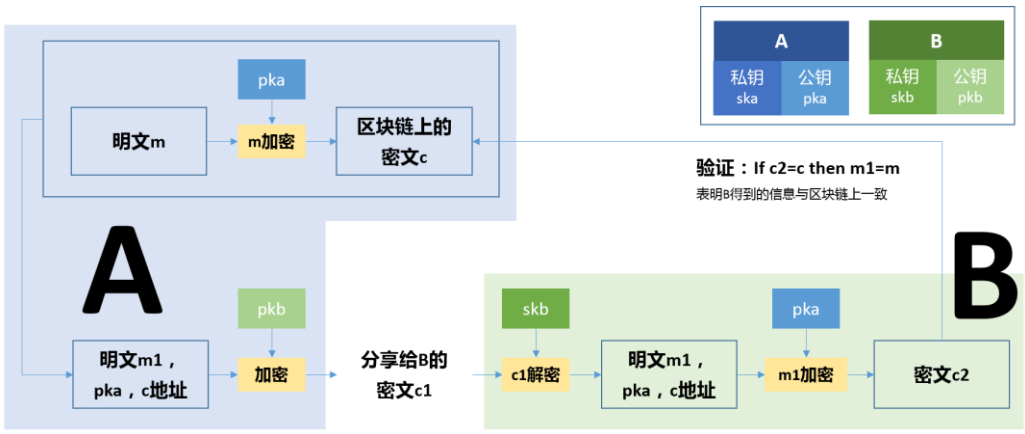
3.4.2 保密性与信息分享

众所周知，非对称加密中通过公钥加密、对应私钥解密可以实现信息的私密传输；私钥制作数字签名，对应公钥验证可以实现自证身份。通过公私钥对构造一个组合可以实现以下目标：

（1）A 可以在一开始对自己所有的数字身份信息实现加密；

（2）A 可以只透露部分数字身份信息明文给部分人，例如 B（至少在第一次是这样的），而不泄露自己的私钥；

（3）B 可以验证 A 提供的信息是否与区块链上登记的密文对应的明文一致。



不过这个构造仍然不能解决（1）-（3）之外的问题，比如 B 搜集了足够数量的信息之后对外泄露 A 的身份隐私。这个问题已经超越了区块链所能解决的范围。

另外，由于区块链上的交易自带数字签名，在一般情况下分享身份信息的交易与创建身份信息的交易同属于一个账户，因此 A 无需将数字签名包含在密文 c1 中。如果这两个交易

分别由不同的账户发起，那 A 也需要提供创建身份的交易所属账户的数字签名，以表明 A 确实拥有这个数字身份信息。

3.4.3 自由创建、自主管理数字身份的理想

我们在现实生活中其实失去了自由创建、自主管理数字身份的权利，我们的数字身份被不同的服务提供商瓜分，更不用说一旦在他们服务器建立数字身份之后的相关数据——使用权、所有权的管理和保护变得几乎不可行。

元界认为数字身份属于知识产权，应该是一类特殊的资产，虽然被看见明文就意味着知识产权被侵犯，但是“分享”的动作意味着价值将如何变化、以及各方是否受损或获利，都是随着实际情况变化不定的。

元界提供一个场所，任何人都可以在上面注册自己的个性化“简历”，只需要花费少量的信息存储费用，就可以拥有一份不可能更改的个人简历，这个简历的格式由自己定义，时间戳、公私钥加密构造等机制，将共同保障信息的所有权。当然，有的人可以霸占你的姓名、手机号等等信息，但是他们无法提供验证码、护照号码等更强的证据链，所以关于你的数字身份最早建立的、最完整的、最新的版本，将只属于你。关于数字身份的验证机制，与智能资产的类似，并且将由 Oracle 这种角色来提供服务，在 Oracle 章节进行进一步阐述。

在元界创建数字身份时，会体验如下步骤：（1）提供可以强验证的个人信息，即邮箱和手机号码；

（2）自定义其他个人信息，先填写字段名，再填写字段值，例如，“城市”，“上海”；

（3）如果不希望马上登记在区块链上，只需要填完信息后保存在本地，以后可以更改；

（4）如果希望它们成为不可篡改的记录，付出一些创建数字身份的 ETP，发出这笔交易。

在元界使用数字身份时，会体验如下步骤：

（1）应用服务商提出数据请求，按照 3.4.2 的方式对其分享信息；

（2）请求 Oracle 对自己注册的数字身份进行验证，这些 Oracle 可能是银行，公安系统，另一个已经被认证过的朋友，等等。

（3）生成个人简历的时间线，这个简单的应用如果在若干年之后使用，其效果将十分显著——原来这就是我的一生的轨迹，没有哪个无良的服务商篡改过的记录。

3.5 Oracle-价值中介

举 Alice 和 Bob 的例子说明，在一个简单的预测纽约天气合约中需要多少 Oracle 中介？答案是至少 3 个：一个天气数据输入的 Oracle，一个小组的仲裁 Oracle，以及一个起担保作用的 Oracle。

区块链技术声称要去中介化，或者叫“消灭中间人”，目前看来还只是天方夜谭。价值的中介仍然有重要作用，未来还有相当长的时间有重要作用。他们就像是虚拟和现实平行时间的虫洞，离开他们，两个世界的沟通就会出现障碍，因为就目前而言，两个世界的价值评判标准和逻辑还无法全部量化写成代码，更别谈实际应用了。

不同于“消灭中间人”的口号，元界会为价值中间人保留区块链上的位置，我们称其为 Oracle。托管 Oracle 可以保管物理形态的资产，然后在链上发行智能资产，身份认证 Oracle 可以在链上提供个人信息与 Avatar 相关性的证明，监管 Oracle（例如监管特殊交易的政府部门）可以在链上提供交易真实性、合规性证明……还有很多其他的 Oracle 可以在元界上提供这样的服务。

此外 Oracle 还有一个更宏观的作用，即丰富交易类型，提升区块链价值。

在 MVS 以 POW 方式分发 50,000,000 个 ETP 之后，DPOS 的挖矿奖励将主要来源于交易的手续费（transaction fee），MVS 为价值中介的生态设计了基于信息注册、认证等多种交易类型的原生功能，每种交易类型又能支持数字身份、智能资产等方向的不同应用，我们可以预见交易手续费的附加价值和总量都将得到提升。

我们以前总是在讨论如何降低比特币或类比特币系统作为支付网络的交易费（使用费），同时扩大区块的量和出块速度，一方面满足业务的需求，另一方面让价值源源不断注入系统，让矿工、记账节点有足够多的激励来——现在我们可以重新审视这个问题，当手续费不再只是因为转账支付，而是有为了换取更多的区块链服务（例如购买价值中介的服务，启动智能合约），那区块链的价值将不再仅仅依赖区块容量和出块速度，而可以转移到提升服务类型和品质，这将会带来新的机遇。

关于记账人的激励模型也将达到新的平衡，记账人会从利润率较高的服务费中获得更多的分成，而在以前这些服务是完全 offline 的，他们既没有用到区块链技术的价值（除了转账记录），也没有回馈给区块链系统更多（除了转账手续费）。这样的“交易”记录在区块链上有一种买椟还珠的感觉，所有的服务也会根据其稀缺性、重要性等特征，在市场上以区块链代币对这些服务进行定价。

3.6 MVS 潜在的风险与考虑

区块链技术仍在处在发展的早期，其成熟度还在持续的研究过程中。区块链技术来自比特币系统，因此它将继承比特币系统的优点，以及一些缺陷。

- **不断增长的区块体积**

比特币区块链的总数据量大约每 10 分钟增加 1MB，相当于 1GB 每周，因此运行一个全节点的成本将显著地增长。全球范围内比特币的全节点数目从 2013 年下半年的 1 万多个下降到目前 2016 年 7 月的 5500 多个。以太坊的区块数据体积大约每个月增加 2GB，增长

率还在增加。元界区块链也将面对区块上面数据不断增长的问题，这个问题可能会因为元界的设计采用了 UTXO 方法而变得更加复杂。在以太坊的白皮书中对这个问题进行了详尽的阐述，早期这个问题将有矿工来解决，因为他们挖矿需要运行全节点。

- **中心化挖矿问题**

挖矿是一把双刃剑，一方面挖矿可以保障系统受到算力的保护，另一方面由于挖矿产生了一些新的问题，比如说挖矿中心化问题和潜在的 51%算力攻击的威胁。

在比特币的行业领域，挖矿中心化是个令人十分厌恶的结果，以太坊在面对挖矿的中心化问题上也逐渐失去主动权。

元界希望通过挖矿算法的优化，虽然不能保证避免挖矿中心化的问题，但是可以缓解这个进程，直到整个系统从 POW 迁移到 HBTH-DPOS 共识算法。

- **商业成功带来的失败**

如果元界在商业上十分成功，这将带来一个新的风险。当元界上的数字资产的总价值上升到一个水平之后，破坏元界系统、并且在交易所上做空数字资产的攻击行为将变得有利可图。因此，元界上的数字资产的总价值是一个维护/攻击系统的成本的函数（在 POW 阶段特指挖矿的成本）。理想情况下，数字资产的总价值不应该超过挖矿成本的 5 倍。

4 MVS 的设计原则

4.1 最小化设计原则

在高层次设计中，以底层核心功能模块为重点，不在基础功能上作过多的复杂设计，只在必要的时候才进行扩展。

4.2 演进稳定原则

在 MVS 的演进过程中，只发生两种需要 MIP 的情况：

- 核心功能增强与拓展
- 安全缺陷修复

无论以哪种形式的 MIP，都不应当产生对底层架构产生过大的影响。

4.3 兼容原则

MVS 的版本必须向下兼容；

4.4 模块化设计原则

分层分模块，降低各模块间的耦合度，将参考 Libbitcoin 的实现方式。

5 MVS 的架构设计

在元界的发展规划中，我们将元界的发展分为两个阶段：

第一阶段 ,元界将以 POW 共识算法为基础 ,主要提供数字身份 ,数字资产登记与交易，简单内置脚本，简单 datafeed 与信用评价等功能。元界可以用于支持所有的联盟链，形成一个开放式的平台生态。

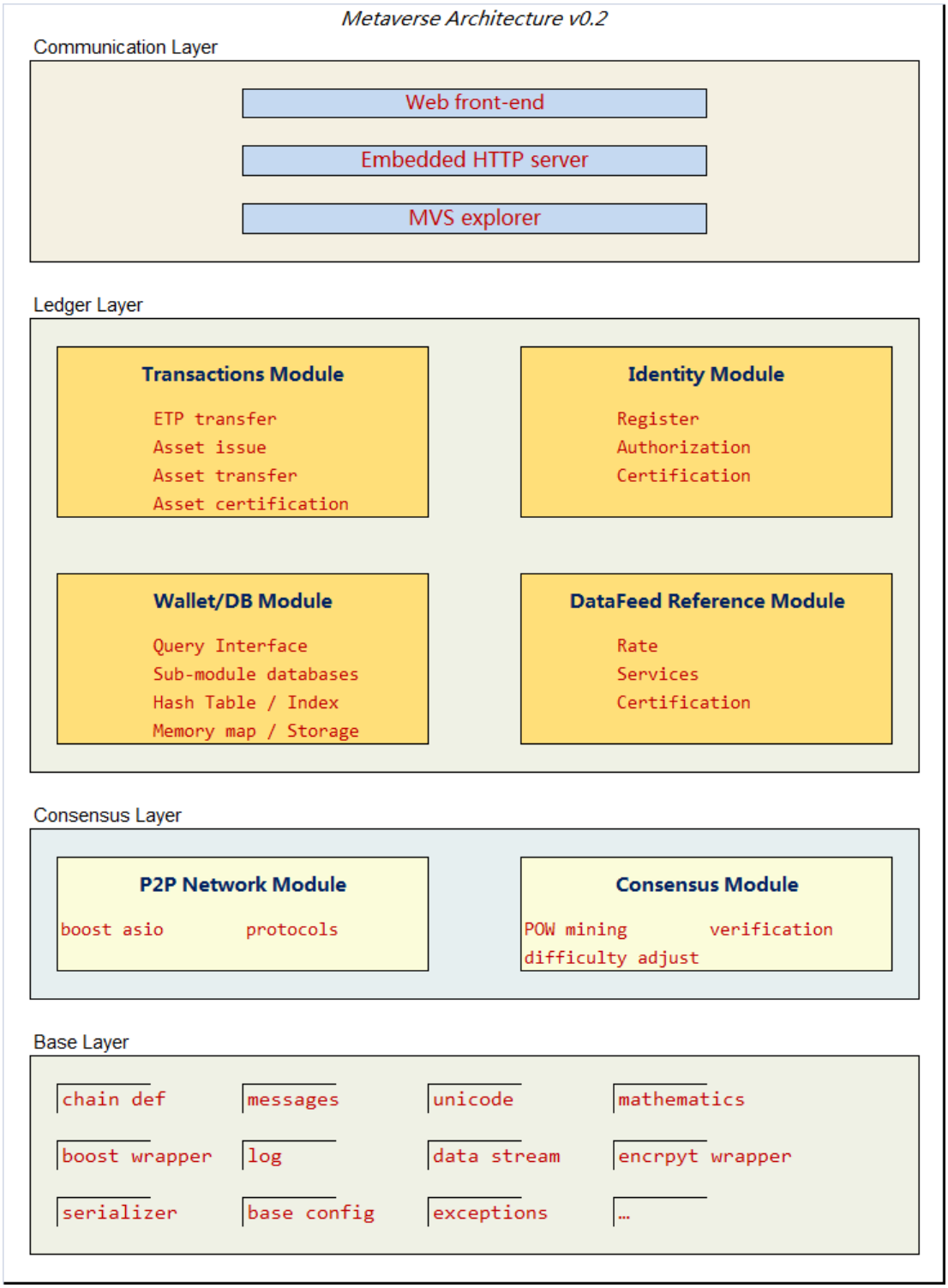
第二阶段，元界将转到以 DPOS 为基础的改进共识算法，借助第一阶段的生态积累，扩展元界的智能合约功能，提供完整的 Oracle 服务。

本节架构我们主要讨论第一阶段的元界架构。

5.1 基础架构

5.1.1 基础架构图

v0.2版架构图如下图所示：



一共分为四个层，六大模块：

1. Comunication Layer

本层主要设计了用户 Console 以及一个 Embedded HTTP server。

用户 Console(explorer)主要是 MVS 提供的交互操作集合。

Embedded HTTP server 集成了 Json-rpc 和 Restful API 的功能 以及提供简单的 WebUI

界面。

2. Ledger Layer

本层主要设计了四大模块，

基于 bitcoin 数字代币 Ledger 以及智能资产的 Ledger 扩展——Transactions Module.

基于基础 Ledger 扩展的数字身份模块——Identity Module.

MVS 的主要存储以及查询模块——Wallet/DB Module.

用于支持 Oracle 价值中介的 Data-feed —— Data-feed Reference Module.

3. Consensus Layer

本层主要设计了两大模块：

用于支持所以网络消息的 P2P 网络模块（不支持局域网穿透）;

共识模块，包含挖矿，验证，以及网络难度调整等功能。

4. Base Layer

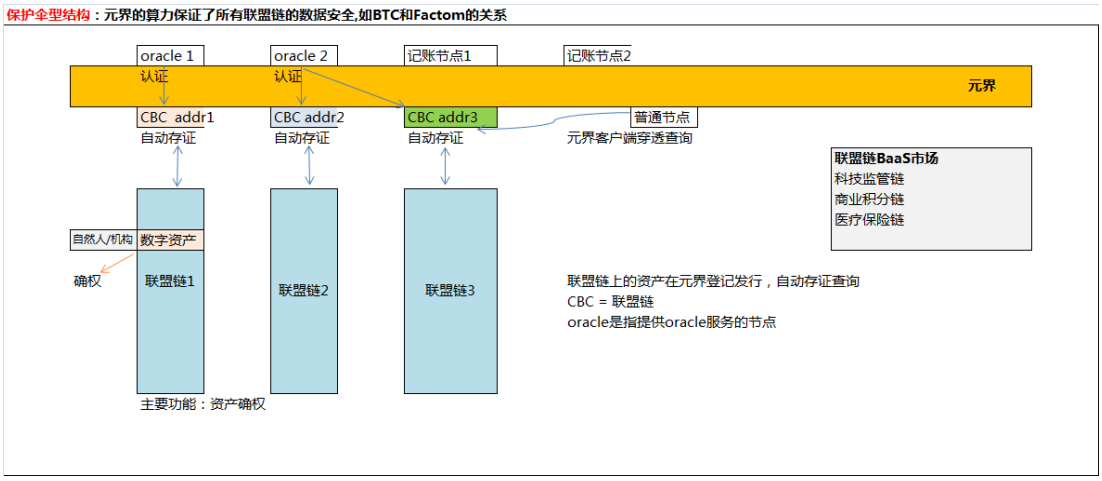
本层是一个基础库层，里面包含了一些基础类的定义，配置继承关系，数学库数据流处理库以及 log 库等通用功能。

5.1.2 业务层级结构划分

MVS 的设计宗旨是为了更好的结合现有商业应用，MVS 可以搭配联盟链而使用。

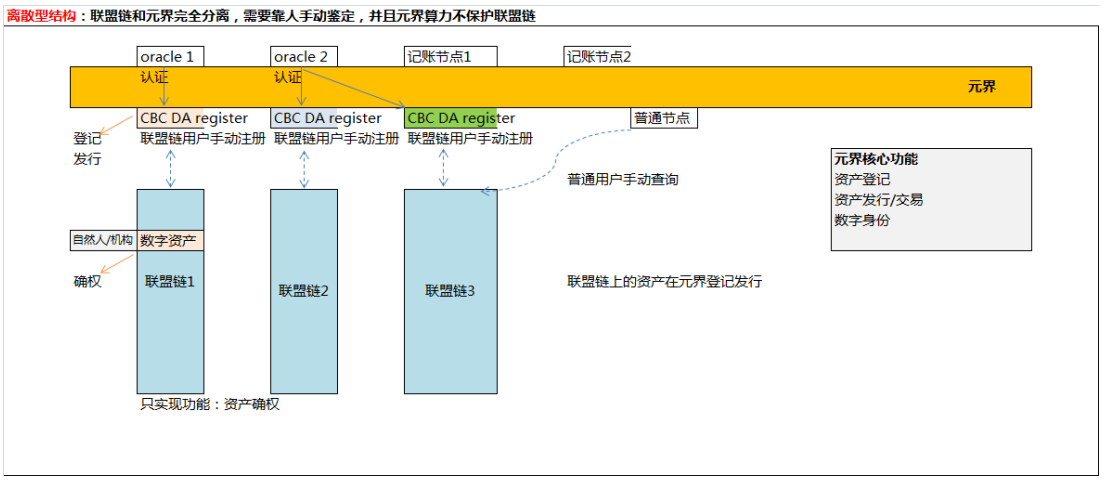
MVS 提供认证的 Oracle 身份，以及为每个人提供一个数字身份，而联盟链提供具体的 Blockchain Service。

下图是 MVS 与具体的联盟链的一些关系，我们称之保护伞结构：



在 MVS 未来发展中，我们考虑将 MVS 做成一个通用的用户端入口。

而在 MVS 初始版本，我们将提供一个更简单的方式，我们称之为离散结构，关联验证需要用户手动验证（虚线部分）或者通过 Oracle 签名（通过交易签署）的方式：



在 Oracle 手动签名的方式中，联盟链的资产确权以后，在元界上登记时，需要出示联盟链资产确权信息，而在元界上的 Oracle 可以对该签名再签名，可以公示给用户，普通用户可以直接查询公示信息。

5.2 功能迭代开发一览

O待定，√发布，X不发布

功能	一级功能	二级功能	初始版本
账户(n)	地址(n)	普通地址	√
		HD地址	√
		智能资产地址	√
	数字身份(1)	基本身份(邮箱/手机)	√
		扩展身份(其他)	○
		自定义别名	○
		认证与授权	○
		元界点数	○
	平台代币-熵(1)	ETP挖矿	√
		ETP转移	√
	资产(n)	我的资产	√
		登记资产	√
		资产转移	√
	data-feed(n)	数据录入操作	×
		feed的欧几里德引用计数	×
		信用点数评价	×
市场(1)	资产市场(n)	市场热度排序	×
		k线走势	×
		comments	×
	Oracle市场(n)	领域按数字身份的信用排序	×
		免费公共oracle	×
		收费oracle	×
		接入目标Oracle的data-feed	×
	合约市场(n)	领域按热度排序	×
		免费合约	×
		收费合约	×
		定制合约	×
智能合约			×
系统功能	系统账户	资金池查询	√
		提案查询	×

6 MVS 的共识选型与核心功能

6.1 共识机制（Consensus Progress）

所谓区块链共识过程，是指如何将全网交易数据客观记录并且不可篡改的过程。目前"三巨头"分别使用不同的共识算法（Consensus Algorithm），比特币使用工作量证明 PoW（Proof of Work），以太坊即将转换为权益证明 PoS（Proof of Stake），比特股使用授权权益证明 DPoS（Delegated Proof of Stake）。

以上这些算法我称之为“经济学”的算法，所谓经济学的算法，是指让作弊成本可

计算，且让作弊成本往往远大于作弊带来的收益，即作弊无利可图，通过这种思想构造一个用于节点之间博弈的算法，并使之趋向一个稳定的平衡。

相对应的我们还有计算机领域的分布式一致性算法，例如 Paxos、Raft，我也称之为传统分布式一致性算法。

他们之间的最大区别是：系统在拜占庭将军（Byzantine Generals Problem）情景下的可靠性，即拜占庭容错（PBFT 算法支持拜占庭容错）。然而无论是 Paxos 还是 Raft 算法，理论上都可能会进入无法表决通过的死循环(尽管这个概率其实是非常非常低的)，但是他们都是满足 safety 的，只是放松了 liveness 的要求, PBFT 也是这样。

下面是一些传统分布式一致性算法和区块链共识过程的异同点：

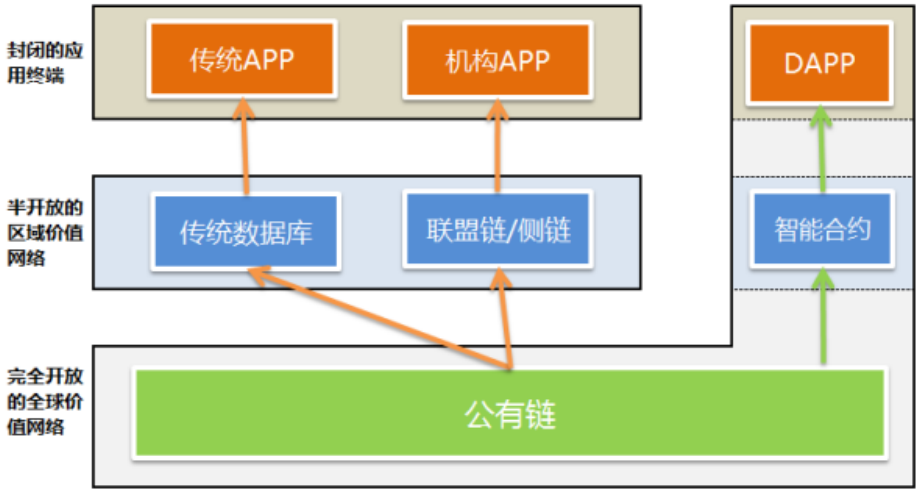
相同点：

- Append only
- 强调序列化
- 少数服从多数原则
- 分离覆盖的问题：即长链覆盖短链区块，多节点覆盖少数节点日志

不同点：

- 传统分布式一致性算法大多不考虑拜占庭容错(Byzanetine Paxos 除外)，即假设所有节点只发生宕机、网络故障等非人为问题，并不考虑恶意节点篡改数据的问题；
- 传统分布式一致性算法是面向日志（数据库）的，即更通用的情况，而区块链共识模型面向交易的，所以严格来说，传统分布式一致性算法应该处于区块链共识模型的下面一层。

下图是一张未来区块链生态示意图：



公有链提供可信可靠的价值传输网络，上面可以继续组建去中心化应用（DAPP）或者部署联盟链，甚至传统数据库都行，在上层搭建 C 端应用。

元界是一个公有区块链，公有区块链有几种杰出的共识算法设计，包括由比特币系统首创的工作量证明机制 POW（proof of work），由点点币系统首创的权益证明机制 POS（proof of stake），由比特股首创的权益代表证明机制 DPOS（delegate proof of stake），此外还有其他一些拜占庭容错的机制（BFT，拜占庭容错，Byzantine Fault Tolerance）。

大多数的加密货币都选择性忽略拜占庭容错算法，因为这个算法不解决代币分发的问题。元界的 ETP 虽然不是货币，但是作为对网络安全有贡献节点的回馈，ETP 将被分发给这些节点。

在任何区块链项目的早期，全节点的总量都是不足的，这样全网的系统安全就比较难有保障。通过引入工作量证明挖矿的机制，元界向挖矿节点分发 ETP 作为区块奖励，系统本身会获得大量矿工全节点，可以在项目早期提供足够的系统安全性。

未来随着项目的成熟度增加，用于进行挖矿奖励的 ETP 分发接近尾声，元界将切换到一种改良的 DPOS 共识算法上，这种算法将考虑“币区块高度销毁”这个重要指标设计。

第一阶段：工作量证明 POW 挖矿

在元界系统的前几年运行时间中，将会采用 GPU 挖矿的方式保障系统安全，以及一个去中心化的时间戳服务。元界的挖矿算法还在比较和研究中，不过会避免使用比特币的 SHA256 算法和莱特币的 scrypt 算法，原因是避免比特币或莱特币矿池 51%算力攻击。

第二阶段：HBTH-DPOS

虽然 POW 工作量证明机制的挖矿可以帮助元界系统在最初的几年内有系统安全的保障，但是 POW 挖矿也有它的问题，比如说能源的浪费，挖矿的中心化发展趋势等等。

由比特股首创的 DPOS 权益代表证明机制，相比 POW 和 POS 而言是一个更加健壮和更加去中心化的机制，更重要的是系统的每一个参与者都是合格的投票者。

不过 DPOS 共识算法的设计仍然有两个缺陷：首先是金融干扰问题，攻击者可以通过短期内持有大量系统代币，投票支持或者反对系统中重要的议案，操纵完这个投票议案之后再抛售代币，再从交易市场上获利。经过测算，目前在比特股系统中，要完成这样的攻击只需要约 3 百万美元价值的代币就可以操纵投票结果。

其次是投票者冷漠问题，选票持有者一般对系统的工作状况并不关心，他们中的大部分人选定自己的代表之后就不愿意再去改变，甚至当代表们作恶的时候，也动力不足。过去的三个月中仅有 1%的投票者改变了他们的代表人。

元界改进了 DPOS 共识机制，加入了币区块高度和心跳的概念，基本的模型如下：

币区块高度（TH）源于币天销毁的概念；

比特币的币天=比特币数量×上一次花费至今的天数；

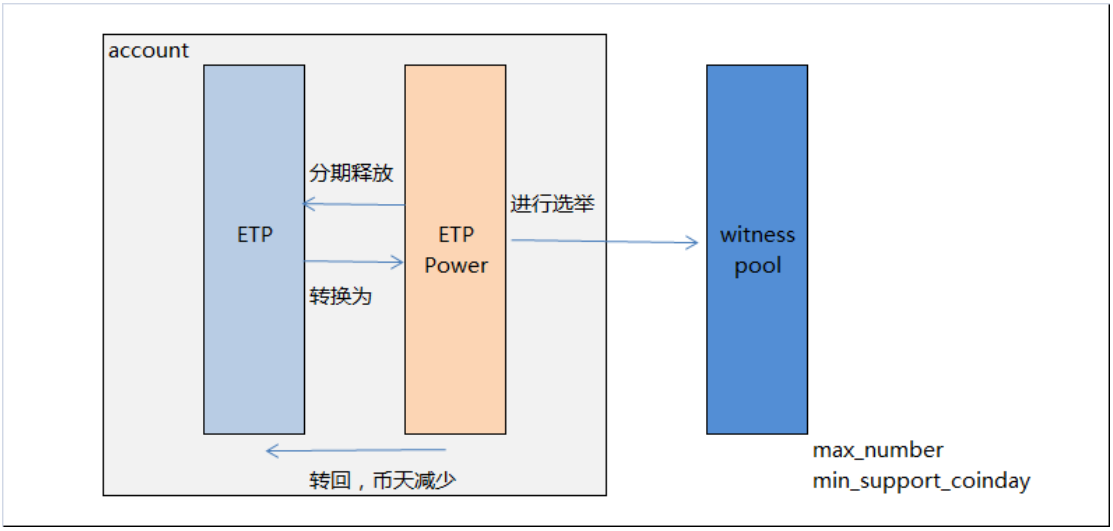
TH=ETP 的数量×上一次花费至今的区块数×元界常数。

元界将 TH 作为 DPOS 中投票的权重，目的是避免金融干扰问题，如果攻击者临时从市场获得大量的 ETP 打算对投票进行影响，那么他们的币区块高度将很小，因此投票的影响力也很弱。攻击者为了达到目的，将不得不从市场上获得更多的 ETP，或者持有 ETP 达到足够长的时间来获取币区块高度，不论是哪一种方式都将显著增加攻击者的成本。

在 DPOS 阶段，元界与其他采用 POS 共识机制的系统一样，会根据当时的权益持有情况把 ETP 分发给不同的股权持有人。不过，不同之处在于，元界系统的股权持有人将不是以被动接收代币的方式获得新的 ETP，而是需要持有人向系统发送一个“心跳”以证明该股权持有者还是活跃的。同时这个心跳相当于一个来自股权持有人私钥的数字签名，股权持有人在发送心跳的时候还要选择更换或维持自己的权益代表。

设计这个心跳的好处有两点：第一点是激励人们去检查自己的权益代表，虽然不是从根本上解决了投票者冷漠问题，但是起到了缓解作用；第二点是系统不会再把新的 ETP 分发到已经失活的股权上去，并且对失活的股权有稀释的作用。

在 DPOS 阶段，我们也将考虑使用 Power-DPOS 改进算法：



具体模型如下：

1. 将 ETP 的投票属性和交易属性进行分离，定义投票专用的内置 token 为 power。定义币龄（coinage）为有效选票的计算基础，可以预防直接从交易市场获取大量 ETP 进行选票冲击；

2. 定义币龄概念，即权益对时间的积累，是一个不可作假的“证物”，类似工作量证明。考虑到持有并锁定权益是持有人付出的代价和牺牲，正如计算机的 CPU 或 GPU 进行数学函数的验证需要矿工付出的电费和计算能力占用成本。币龄的计算公式如下：

$$Coinage = \sum_{h=h_1}^{h_2} Locked(ETP) * f(h)$$

$$f(h) = \begin{cases} \dfrac{H-h}{a}, h \le H，H = h_1 + max; \\ 0, h > H. \end{cases}$$

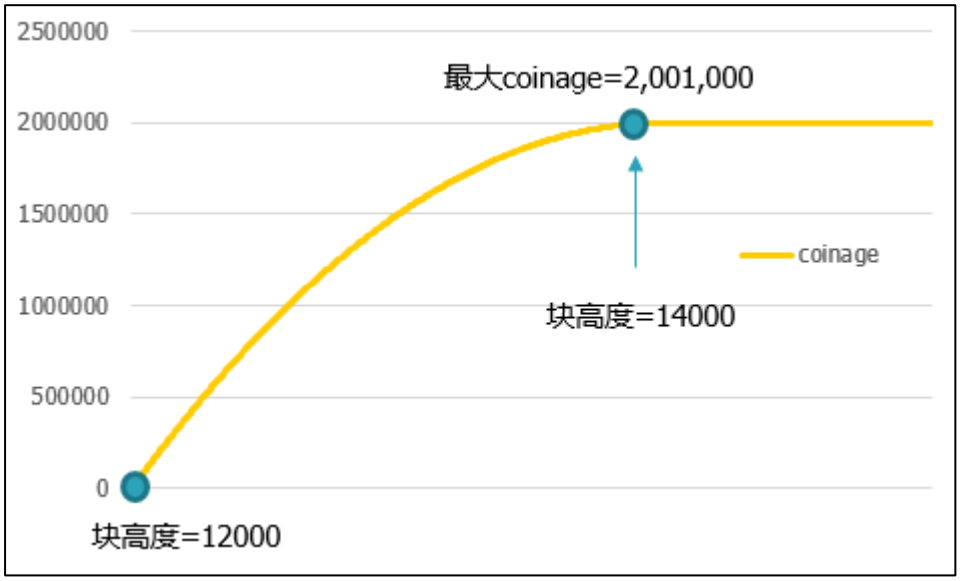
其中 coinage 即币龄；

- Locked(ETP)即投票前在特殊地址锁定的 ETP 数；
- f(h)即与高度相关的时间密度函数；
- h1 为锁定起始时的块高度，h2 为锁定解除时的块高度；
- H 为 ETP 锁定产生 coinage 的最大高度，锁定 ETP 的块高度超过 H 并没有产生新的记账 coinage；
- max 即可以产生 coinage 的块数目;
- a 为转换参数，没有特别的意义；

假设 h1=12000，当前高度 h=14500，最大高度 max=2000，转换参数 a=5000，锁定的 locked(ETP)=5000，若此时解除对 ETP 的锁定，则 h2=h=14500。但 H=h1+max=14000<h2，锁定的 ETP 能产生的 coinage：

$$Coinage = \sum_{12000}^{14000} 5000 * f(h) = 2{,}001{,}000$$

示意图如下：



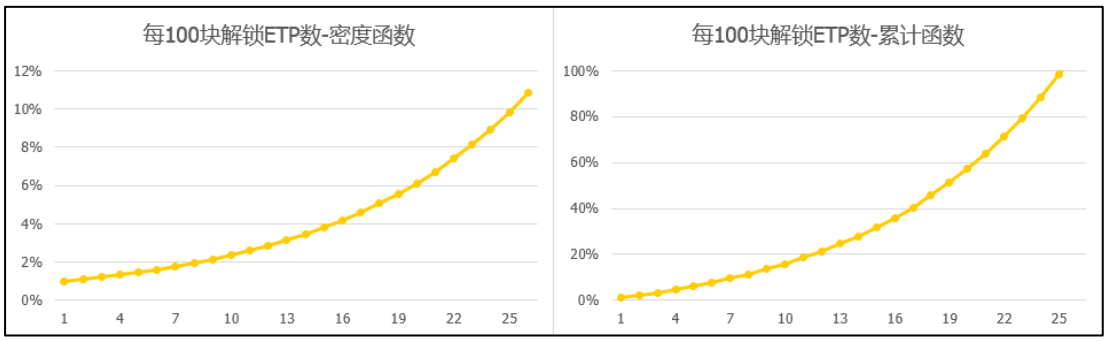
在这个案例下 ,假如新块的产生时间约为 15 秒 ,则产生 2000 个块大约需要 8.33 小时，攻击者只需要锁定 ETP 较短的时间即可获得全部的投票权重，这是有较大风险的。只需调节 max 就可以改变这个时间。

3. Coinage 与 power 的数学关系为线性函数，定义比例为 ratio(CoinageToPower)。

4. ETP 产生 power 的流程如下：

   本地客户端：普通地址(ETP for power)->本地客户端：选票地址(ETP for power)->锁定通过地址间交易完成，交易完成的瞬间发生 ETP 的锁定->解除锁定时，计算锁定(hight(unlock-lock))，计算 coinage->解除锁定，解锁是锁定的逆向交易，但这个过程不是瞬间发生的，解除锁定的条件函数是：

   第一个 100 块每个块解锁 0.01%ETP，之后每 100 个块增加 10%，即第二个百块每个块解锁 0.01%×（1+10%），以此类推直至全部解锁。则 ETP 解锁数目的密度函数和累积函数如下图：



可以发现刚开始解锁的速度较慢，后期解锁的速度较快。在这个假设条件下，需要大约

2400 个块来完成解锁，若出块速度为 15s/block，那大约需要 10 小时来完成全部 ETP 的解锁，并且前 5 个小时解锁的 ETP 仅为总量的 20%左右。如果需要调整这个总时间，则需要调整解锁数增加的高度间隔，例如调整为 200 个块，时间将增加一倍。

若要在保留曲线形状的前提下改变解锁速度，则需要调整增加比例，例如调整为 5%，则解锁速度将下降。

还可以考虑其他解锁的模型，这里使用的是最简单的等比例级数的模型。

6.2 交易类型

除了 coinbase 的交易类型之外，比特币上仅有一种交易类型，即从发送者到接收者的比特币转移。

以太坊系统中引入了另一种成为“合约”的交易类型，而合约将用于除以太币交易之外其他所有的交易类型，包括资产的发行等。以太坊的使用者需要知道一些代码才能完成这样的操作，虽然以太坊团队投入了很大精力使以太坊的代码编写起来更简便，比如说只需要几行代码就可以实现一些功能，但是写代码的方式来进行常用操作的概念还是会让很多商业的客户敬而远之。

在元界上的交易类型有很多种，交易类型的设计考虑到效率和可用性两个方面，既不会像以太坊那种通过一种合约来适应所有的交易类型，也不会像比特股那样定义很多种交易类型。智能资产的发行和数字身份的注册是除 ETP 交易之外，两类最高级别的交易类型。之后像以太坊智能合约一样的交易类型也会添加到元界系统中去。

6.3 账户模型

MVS 将混合使用比特币的 UTXO 账户模型和基于余额的模型。

- 针对 ETP，我们使用 UTXO 模型；
- 针对用户自定义的数字资产，我们使用基余额的账户模型。

有关 UTXO 模型读者可以参见比特币开发者文档。

6.4 数字身份与 Data-feed

MVS 将参考并整合由 Zcash 提出的零知识证明方案（zero-knowledge Succinct Non-interactive ARguments of Knowledge，zk-SNARKs）来保护用户数字身份的隐私性。

Data-feed 是 MVS 的另一个重要功能，不同于以太坊的构想，MVS 的 data-feed 将大部分由具有 Oracle 身份的角色来承担，他们的可信度将由两方面构成：（1）他们自己提供的有效信任证明；（2）他们在 MVS 上的记录的集合。

市场将对这个可信度进行反馈，方式是：（1）data-feed 的使用者通过消费记录对其进行“投票”，恰当的投票结果将使投票人获得奖励（类似于评价返利），关于投票行为判定规则和奖励模型的建议将在后续版本中披露；（2）不恰当的投票是由投票动机和对结果的影响来判定的，这种行为是会付出代价的，首先不论是何种投票结果，都将忠实地记录在 MVS 上，其次其他 Avatar 或者 Oracle，可以根据自身的好恶来选择如何应对有这样记录的数字身份。

之所以是规则的建议，是因为业务层次的规则不应该以硬编码的方式写进 MVS。任何区块链都不能做超过其“核心业务”（即共识）的业务设计。对于 data-feed 而言，如果有破坏性攻击行为，只会影响到 data-feed 的有效性，而不会影响 MVS 的共识，任何利用 data-feed “作恶”的行为仍然需要为 MVS 的共识付出成本，但他们的攻击行为需要在 Oracle 或者 BAPP 的层面进行防御；即便如此，MVS 的设计者还是希望能有健康的 data-feed 模式，因此会给出规则建议。

6.5 跨平台

MVS 初期将兼容 Windows/Linux/MacOS 等平台。

随着 MVS 的发展，也考虑将 MVS 移植到 ARM 等嵌入式平台，辅助物联网/能源互联网的资产数字化。

参考文献

1. Bitcoin Whitepaper ——Satoshi Nakamoto http://bitcoin.org/bitcoin.pdf

2. Namecoin: https://namecoin.org/

3. Bitshares whitepaper——Daniel Larimar http://docs.bitshares.org/bitshares/papers/index.html

4. Ethereum WhitePaper——Vitalik Buterin: https://github.com/ethereum/wiki/wiki/White-Paper

5. Smart Contract ——Nick Szabo http://szabo.best.vwh.net/idea.html

6. Smart Property —— https://en.bitcoin.it/wiki/Smart_Property

7. Blockchain— from Digital Currency to Credit Society ——ChangJia, HanFeng and etc. ISBN：9787508663449

8. Snow Crash——Neal Stephenson 1992

9. Metaverse——https://en.wikipedia.org/wiki/Metaverse

10. Tim Swanson ——http://www.coindesk.com/smart-property-colored-coins-mastercoin/

11. Coin Days Destroyed ——https://en.bitcoin.it/wiki/Bitcoin_Days_Destroyed

12. http://blockchaindev.org/article/consensus_introduction.html

13 ZeroCash——http://zerocash-project.org/paper