Metaverse-whitepaper-v3.0-CN

The New Reality

Version:Gravity (v3.0)

SuperNova drives low entropy to higher entropy via gravity.

HaoChen, EricGu, YoumingJiang

May 2018

摘要Abstract

元界（Metaverse）是一个关注社会和商业需求的作为基础设施的区块链项目，目标是构建以数字资产（Metavase Smart Token）和数字身份(Avatar)为基础，围绕Oracle和资产交易的新型区块链生态，这种生态会为人类社会带来深刻的变革，最终形成The New Reality。

与其它以技术为切入点的区块链项目不同，元界从商业需求出发，总结人与人、人与资产之间的关系，把总结后的通用需求抽象成模型，然后做到区块链底层供使用者方便使用，这种方式我们叫做BISC（Built-in Smart Contract）,它可以降低商业应用在开发和使用过程中的技术风险。

通过BISC元界提供了数字资产MST、数字身份Avatar、Oracle以及资产交易的功能。数字资产MST可以让使用者享受区块链带来的点对点操作资产的优势，让人们获得等价与发行属于自己的“比特币”的能力；而数字身份Avatar则体现了人与人、人与资产之间的关系，它可以连接到MST上，通过Avatar任何人都可以成为Oracle，Oracle可以帮助人们构建不可篡改的去中心化信誉（Reputation）系统；资产交易可以为MST解决基础的流动性需求；

人们使用MST、Avatar的时候，将区块链作为基础服务植入既存IT系统中的过程叫做BaaS（Blockchain As A Service），BaaS是一种快速、方便构建区块链应用的方式。

区块链简史

区块链技术来源于比特币系统，区块链的发展伴随着对比特币系统的一次次解构和重构，其中，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。

- **比特币**

  比特币系统是一个划时代的发明，其背后神秘的创造者中本聪（Satoshi Nakamoto）将比特币系统定义为“一个点对点的电子现金系统”。比特币系统完美地融合了工作量证明机制、代币激励、密码学、点对点网络、UTXO各项技术，稳定安全运行了近十年。

  比特币也带来了一种全新的货币形式——加密货币（CryptoCurrency），数字货币近些年成为区块链领域第一大类型应用，同时数字货币的出现也驱使人们探索更多形式的区块链应用，例如彩色币（ColoredCoin），域名币（NameCoin），之后人们又提出了智能合约、侧链等形式的技术拓展。

- **域名币**

  域名币是首个从比特币分叉出来的应用项目，它的设计初衷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。

- **点点币**

  点点币提出了PoS共识机制（Proof of Stake权益证明机制）。首先如果所有的区块链都需要设计一套自己的PoW共识机制，能源浪费问题以及物理矿机部署成本，会让整个区块链的发展落后现在很多年。其次PoS共识机制被提出之后，共识算法的创新成为业界永恒的讨论主题。

- **比特股**

  比特股在PoS共识机制的基础上提出了一个高网络吞吐的共识机制——DPoS（Delegated Proof of Stake 代理权益证明），DPoS达到了秒级区块确认，极快的交易确认提供了良好的交易体验。DPoS不仅仅是一个技术层面的共识算法，它还提供社区治理机制。比特股本身也是一个“去中心化”的交易平台，在比特股上，新的

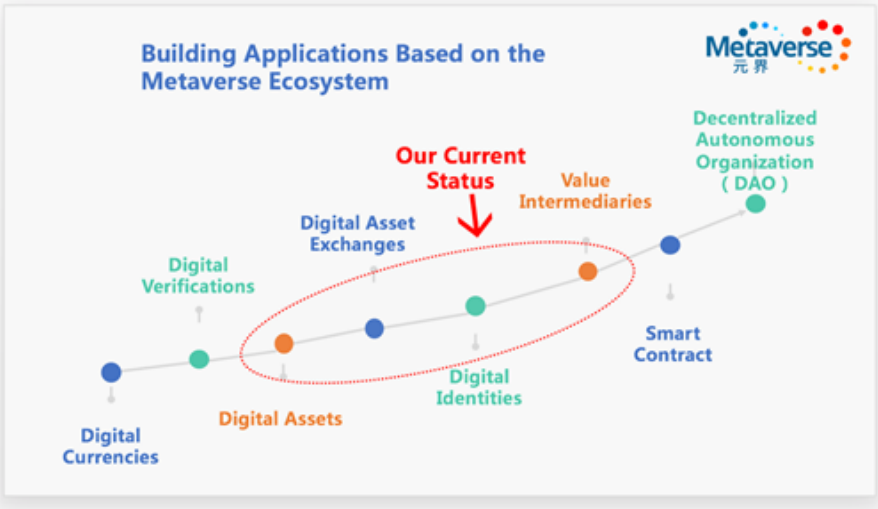
概念被不断提出来，包括更加突出数字身份的项目Keyhotee，以及通过定义多种交易类型，可以更简便地登记、发行数字资产等特性。

- **以太坊**

  以太坊的极大创新在于，它为人们提供了在区块链自定义业务逻辑的一站式工具，这些工具包括智能合约语言、智能合约虚拟机，极大地降低了人们开发区块链应用的门槛。除了智能合约以外，以太坊还实践了更为高效的P2P网络协议——KAD算法，提出叔伯块（Uncle Block）来降低矿池中心化的风险，以及Casper共识机制、ERC20代币标准等，极大推动了区块链行业的发展。

区块链发展路径图

区块链的发展是有迹可循的，譬如在90年代设计人工智能显得遥不可及，但是随着近些年互联网应用的普及以及算法和芯片的发展，一切条件水到渠成，人工智能开始真正走入人们的视野。区块链也一样，如果要一下跨入DAO，似乎缺少很多条件，我们在下图中归纳了这些条件：



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”，以太坊在“智能合约”处。而实际上，区块链和现实应用的接触点，还在图示位置，元界希望构建的，正是围绕这几个元素所打造的生态。

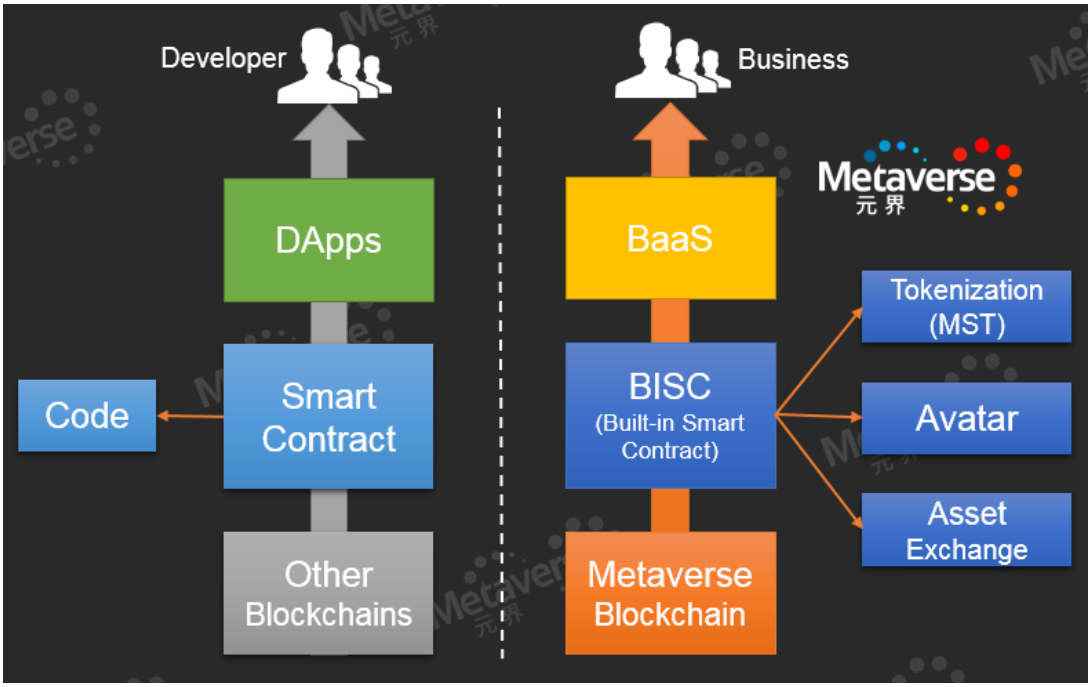
元界：The New Reality

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。元界项目的取名受到了Neal Stephenson小说中所构建Metaverse的启发。

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，越来越多的数字资产的转移将发生在链上，Avatar（数字身份）和中间媒介Oracle将成为那时候的经济主流模式。

与以技术为切入点的区块链项目不同，元界从商业需求出发，总结人与人、人与资产之间的关系，把总结后的通用需求抽象成模型，然后做到区块链底层供使用者方便使用，这种方式我们叫做BISC（Buit-in Smart Contract）,它可以降低商业应用在开发和使用过程中的技术

风险。下面这张图展示了这种关系，左侧是其他的智能合约型区块链项目，右侧是元界为人们提供的：



通过BISC元界提供了数字资产MST、数字身份Avatar、Oracle以及资产交易的功能。数字资产MST可以让使用者享受区块链带来的点对点操作资产的优势，让人们获得等价与发行属于自己的“比特币”的能力；数字身份Avatar体现了人与人、人与资产之间的关系，它可以连接到MST上，通过Avatar任何人都可以成为Oracle，Oracle可以帮助人们构建不可篡改的去中心化信誉（Reputation）系统；资产交易可以为MST解决基础的流动性需求。

BISC由元界核心开发者和社区共同打造，使用者不用关注BISC的技术细节即可安全方便地使用。BISC不仅仅可以用于构建去中心化的应用，更可以完美地融合到传统IT技术方案中，也就是上图中的BaaS（Blockchain As A Service），BISC通过BaaS这种方式为所有商业应用注入区块链的技术及其价值。

我们很难想象上述内容为我们带来的新世界，它会彻底改变我们的生活、工作、学习的方式，这种变革就是The New Reality。

熵（Entropy）ETP

熵（Entropy）

熵（Entropy）是元界的权益代币，缩写为ETP，这个概念借鉴了热力学第二定律中的概念，它描述了系统微观粒子的混乱程度。

ETP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。ETP可以在元界上转移和交易，后期PoS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，它代表元界代币持有人的权益。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，而是取决于元界的生态发展以及ETP的市场需求。

ETP可以被用来衡量元界上的数字资产（MST）的价值，或者作为金融交易中的一般担保物。当系统需要收费的时候，是以ETP的形式进行收费，例如创建一种新的数字资产，注册一个Avatar，将自己标记成为一名Oracle，或者在元界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

ETP 通过以下三种模式进行分发：

（1）ICO和社区建设

ETP将通过ICO向外界分发了2500万个ETP，余下2500万ETP用于设立元界基金会，用于支持对元界社区有促进作用的区块链项目，以及对社区主要贡献者进行奖励。

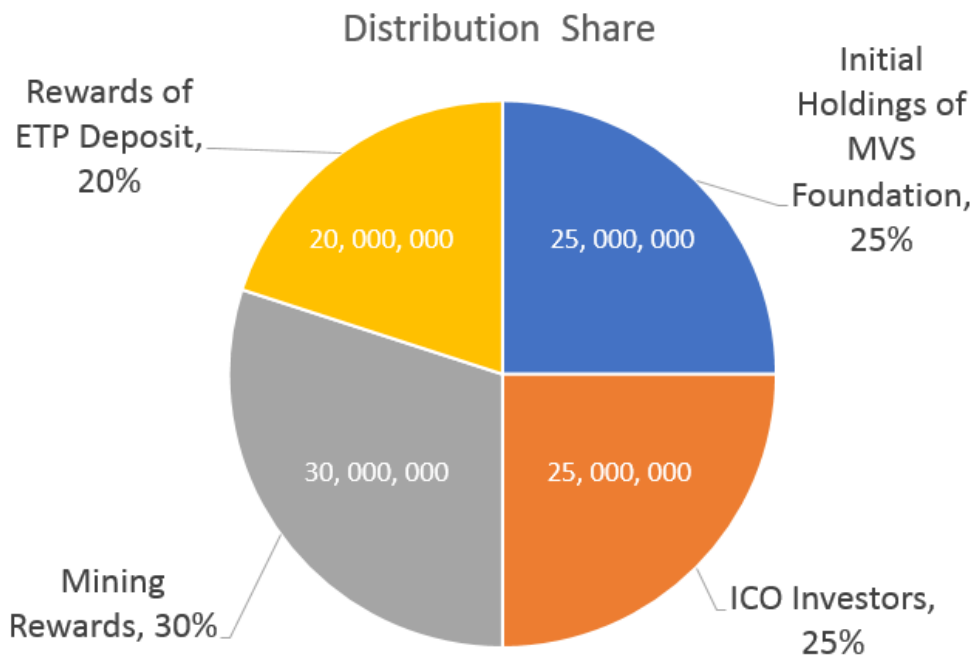
（2）PoW挖矿奖励

3000万枚ETP将通过PoW区块奖励的方式分发给元界系统的维护者，这个过程被称为挖矿。

（3）锁币（Deposit）利息奖励

用户可以自行发起锁币交易（ETP Deposit），系统会给予利息奖励，本金和利息会被当作普通交易处理发放给用户，用户可以立刻看到奖励，但是会被锁定，目前利息奖励总共是2000万。

ETP分布列表如下：

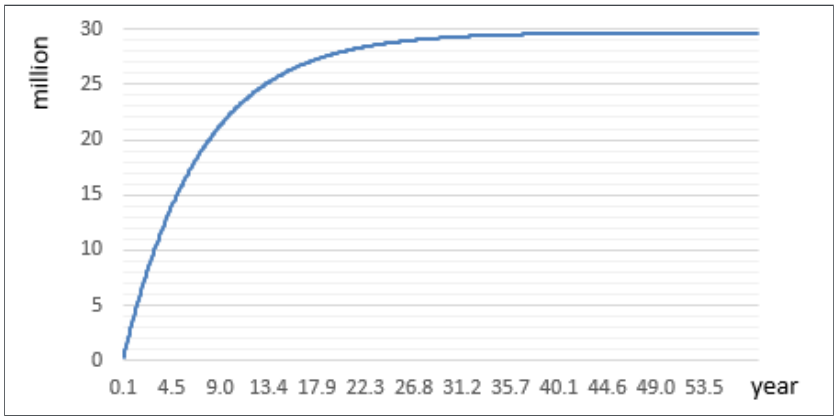


PoW机制分发

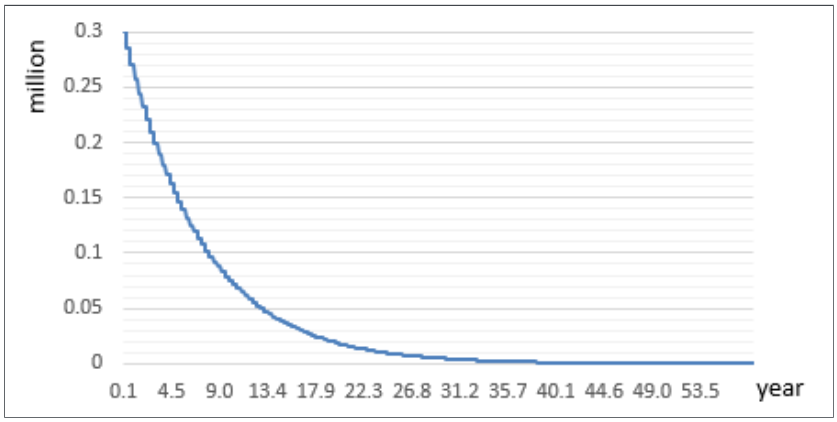
元界PoW挖矿理论出块时间是24秒，我们设定初始每块奖励是3枚ETP，每50万块为一个周期调整一次奖励，按照0.95系数每周期衰减一次。

$$TotalPoW = \lim_{n \to +\infty} \sum_{0}^{n} 0.95^n * 500000 * 3 = 3000000$$

若以此出块时间和块奖励为标准参数，可以得出通过PoW挖矿发行的ETP总量随时间变化和每十万个块总奖励的衰减曲线：



（PoW挖矿的ETP发行总量随时间变化示意图）



（每十万个块总奖励的衰减示意图）

锁币与锁币奖励分发

在ETP的经济模型中，我们加入了区块链内置的有偿锁币功能，这对区块链的经济系统来说是全新的设计，为元界未来切换到DPoS共识机制、以及由锁币衍生的金融应用做的铺垫。

用户需要主动去使用锁币功能，才能获得系统的ETP奖励，奖励会在交易确认时自动转入到用户的锁币地址上。

锁币奖励设计如下：

块个数X	25200	108000	331200	655200	1314000
奖励利率	0.10%	0.66%	3.23%	7.98%	20.00%

块个数X：假设当前块高度为H，发起锁币（Deposit）交易后，立刻获得奖励但是被冻结，用户需要等到X个块之后才能解锁ETP本金和奖励，；

奖励利率：假设用户锁定的ETP为100个，选择了20%奖励利率，那么用户最终可获得ETP数量将为100×（1+20%）=120个。

由于锁币奖励始终是有利息的，这会让ETP总量最终上限突破1亿枚，这个时间窗口在MIP-2中演算过，大约需要14年的时间，元界社区近期已有提案来终止突破1亿枚的可能性。

在区块链上锁币是一个大胆的设计，尝试产生一个区块链生态或社区原生的利率，不依赖于外部央行的现金利率。不过初版的实现方式并非特别理想，因为这一版本并没有把模型设计成动态、可调整的利率，更无法说是实现去中心化地、通过博弈方式产生市场的现金利率。

进一步，未来我们将推进ETP在中心化和去中心化交易市场的活跃度，在这些市场上的“ETP交易对”将作为ETP利率的重要数据基础，通过投票或者直接获取去中心化市场数据的方式，影响ETP的经济模型，进而调整参数。ETP在链上的转账活跃度、账户数、特殊交易数（待构建）等参数也有机会被纳入这个范畴。

微通胀模型

ETP是元界生态的权益代币，而不是一种流通货币，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，我们设计的ETP经济模型需要引入微通胀来弥补ETP流通的需求。

在ICO和元界基金会中我们一共分发了5000万ETP，在挖矿进程中我们一共会分发3000万ETP，而在锁币奖励过程中，我们将持续、有序地向系统释放少量的ETP奖励，具体的量将锁币的总量、时限来决定，同时通胀率又会作为参数，给ETP锁币奖励利率机制的调整提供参考。

这套反馈机制的系统将有经济自我调整和修复的功能（主要通过ETP锁币奖励利率作为关键工具），关于修复力度和修复周期的设计将在元界之后的版本不断升级，最终实现元界链上更为直观的经济模型以及有效的经济生态。

共识机制

元界使用的共识机制分为两个阶段，第一阶段我们采用保守安全的PoW来保证区块链生态成长。

第二阶段，随着元界生态的丰富，为了支持更高的交易吞吐量，或者用于进行挖矿奖励的ETP分发接近尾声，我们可以考虑切换到DPoS或PoS共识机制上，又或者类似ETHASH–Casper混合共识方案。

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，挖矿算法选型我们避免使用比特币的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。

考虑到ASIC带来的矿池中心化，我们选取了ETHASH算法作为元界的挖矿算法。

PoW机制将维持相当长一段时间，直到业界出现了足够稳定安全的新型共识算法，我们将切换到这种新型共识算法。并且我们也设计了一种DPoS算法的改良版本作为第二阶段的备选方案。

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。

从石墨烯（Graphene）所实践的DPoS算法提供了高性能的区块链系统，不过DPoS共识算法的设计仍然有两个缺陷：

1. 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。

2. 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；

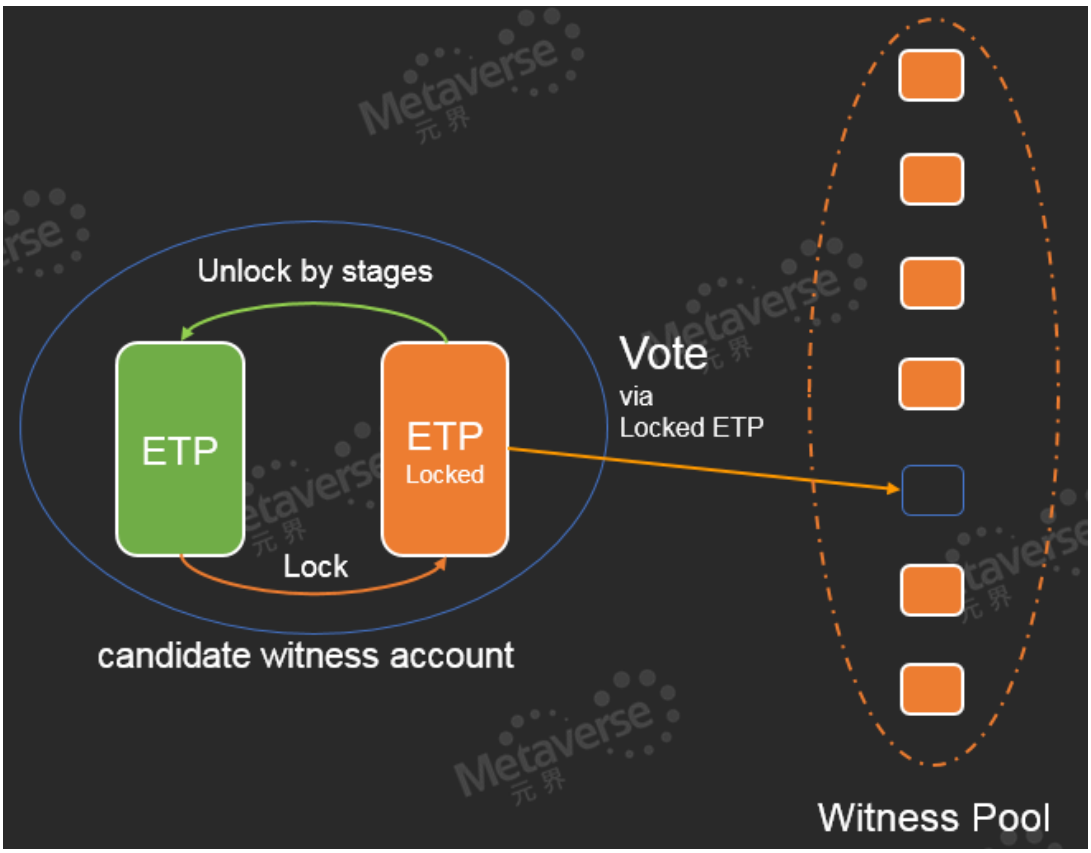
TH = ETP的数量×上一次花费至今的区块数×元界常数。

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ETP持有人。不过，不同之处在于，元界系统的ETP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ETP持有者还是活跃的。同时这个心跳相当于一个来自ETP持有人私钥的数字签名，ETP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分发到已经失活的权益持有人上去，并且对失活的权益有稀释的作用。

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：

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

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

3.

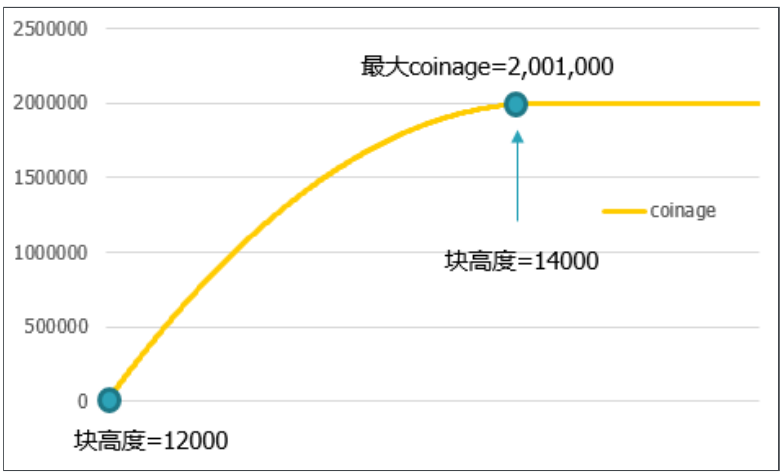
其中coinage即币龄；

- 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：

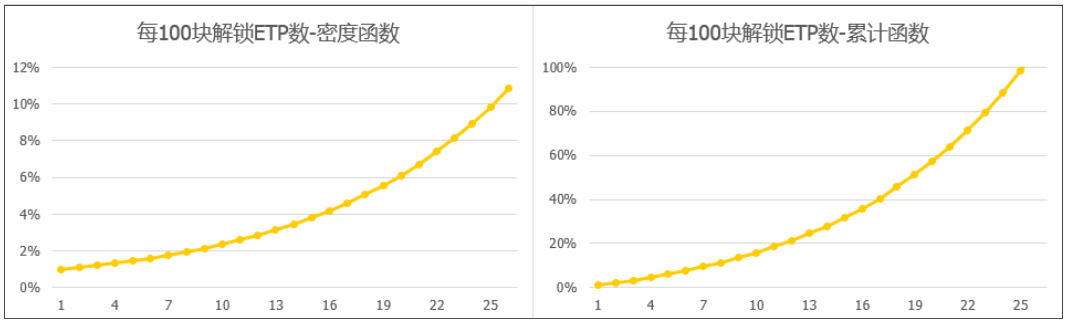


在这个案例下，假如新块的产生时间约为15秒，则产生2000个块大约需要8.33小时，攻击者只需要锁定ETP较短的时间即可获得全部的投票权重，这是有较大风险的。只需调节max就可以改变这个时间。

4. Coinage与power的数学关系为线性函数，定义比例为ratio(CoinageToPower)。
5. 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，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。

数字资产–MST

在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式智能合约来实现指定契约条件的资产。

在以太坊上，智能合约被过度地强调，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。其中的典型便是ERC20标准，虽然它为使用者提供了方便的Token转移和存储功能，然而由于以太坊合约账户是有状态的，在token转移过程如果目标账户代码不兼容ERC20标准又或者触发了异常，会导致token意外丢失，因此以太坊社区开发者提出了ERC223标准，虽然标准升级提升了数字资产的安全性，但也佐证了使用智能合约实现数字资产是一种反直觉设计。

ERC20标准的出现也规范了ICO市场，在ERC20以前的ICO由于缺乏标准，新的token上线交易平台往往需要长期的技术储备，有了ERC20以后，则仅需向支持以太坊的平台提供合约账户地址即可。

因此区块链Token的标准化是历史的必然，平台和应用都使用标准化的token将极大释放区块链的能量，带来可观的经济效率提升。

元界上的数字资产的实践形式为**Metaverse Smart Token**，缩写为MST，MST重新强调了数字资产的重要性，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。

元界现阶段在比特币UTXO模型上做了技术延伸，比特币的特性都会附加到到MST上，UTXO的优秀特性，如较好的安全性、可追溯性、ACID特性都被MST继承，MST给了所有人等价发行“比特币”的能力。MST不仅仅可以用于点对点支付，MST还支持资产增发、资产置换功能等多种金融工具。

注：元界最初版本的白皮书把数字资产称作数字资产（Smart-Property）。

如何设计MST

资产登记（发行）

设计MST的第一步是找到一组数据描述一个“资产”，例如股权登记、游戏道具登记、消费积分登记，这里的“登记”操作便是MST的第一步。

当我们说“登记”一样事物的时候，我们其实是在尝试用格式化的数据描述这个事物，它要满足两个设计要点：首先这组数据描述应该能被重复使用，不能轻易被篡改，例如发行总量必须有条件修改；其次提供方便、准确的查询、新增、和验证接口。

鉴于“资产”这个事物的通用属性相对简单，自定义属性各不相同，并且重要的数据产生于资产转移过程中，因此资产登记可被简单描述为填写一个类似下表的表单：

类别	数字资产字段	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	小数点后可自定义1~8位
	特殊权利（资产证书）	特殊权利存放的地点，例如发行权
自定义属性	自定义数据域	自定义属性存放的地点

MST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数字资产的真实性，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ERC20 token，一些代币其实可以被视为数字资产，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。

用MST可以做什么

资产登记只是开始，登记之后意味着需要被其他人认可（PoA）才有资产属性，否则只是一串无意义的数据，一旦被某个MST被市场认可了，MST所代表的数字资产就同时有了两重属性：价值属性和可操作属性。

价值属性依赖不断的交易和市场价格变化来体现，可操作属性将通过技术手段（基于虚拟机的智能合约或者基于业务的脚本语言等）实现。可操作属性可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数字资产中去。

元界将重点发展PoA模式的MST，因此设计中将特别关注如何利用元界数字身份帮助用户方便地提供资产证明，我们提出：

（1）价值中介（Oracle）可以通过他们提供的链下数据（data-feed）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）数字身份的信用可以基于区块链交易（Transaction）的进行传递，当链上的证明足够多的时候，链上的数据就可以自证明了，我们称作“证明自举”。

当我们拥有一个被认可的MST的时候，意味着我们拥有了“资产”，那么资产在区块链上的转移也就意味着资产流动性可以通过区块链保证，所以资产转移是MST的最基础的功能。

MST的转移是“寄宿”在ETP的交易之中的，所以使用ETP支付交易费变得非常自然。我们可以看成小额的ETP转移附带了MST的转移，但这里不同的是，我们并没有兼容比特币技

术标准，兼容比特币标准的token机制是彩色币（ColoredCoin），这也使得我们在扩展比特币技术栈上有更高的自由度。

支付费用（ETP）

要求使用者提供登记费用无疑是正当的，这是一种系统自我保护的机制，如果登记MST时不需要任何代价（或者代价微不足道），系统面对DDoS攻击时将不堪一击。我们规定了任意类型的MST转移都必须支付ETP作为费用

所以接下来的问题是，这笔费用收取多少是合适的？目前谁也说不清楚元界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。

就目前而言，元界上的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，用于支持元界社区的发展，剩余的奖励给矿工。

MST的基本特征

MST符号的全局唯一性

智能合约型的Token不具有全局唯一性的特点，我想这是不合适用到金融领域的。通常我们要求Token的符号具有唯一性，而不是Token的接收地址具有唯一性。如果合约的资产符号可以重复的话，欺骗者可以构造相同符号的token，使用者往往无法快速准确地通过智能合约的地址来区分Token。

所以在元界上必须构造一种全局唯一性的Token系统，这使得Token的符号具有以下两种性质:

1. 优质符号的珍稀性；
2. 先到先得，优质的Token符号需要抢注；

考虑到全局唯一的特性，为了让用户更容易区分，符号的大小写应当设置为不敏感。以上两点也会催生出Token符号的交易市场，我们可以类比域名交易。这使得MST必须具有以下特性：

1. 符号所有权可转移；
2. 符号的使用权（冠名权）可授予其他人；

MST在使用权和所有权上作了拆分，这是目前所有智能合约型的Token系统不具备的特性。

MST域名空间

我在设计Token的符号系统的时候，预留了dot(.)作为允许字符。这种特性可为资产表达一种所属关系，例如 SONY.GAME，SONY.PICTURE。这削弱了优质符号的稀缺性这一特性，例如在元界上发行BTC符号，和发行VIEWFIN.BTC，后者显得更可信一些。

由于dot的存在，符号的冠名权变得可交易，例如想使用VIEWFIN前缀，可以联系VIEWFIN的发行人进行私下购买。

MST多种操作范式

MST支持发行全局唯一的token，并且token可进行与比特币相同的支付功能。而在场景的使用上，我们发现这远远不够。这体主要现在以下几个方面：

1. 初次发行后总量不可修改，这是不合适的，增量发行的需求必然存在；

2. 在经济活动中，往往伴随资产需要冻结的情况，所以如果提供基于区块链的冻结功能，它不是面向经济模型的，仅仅作为平台工具帮助人们完成交易；
3. 冻结伴随着解锁，解锁的条件代表着智能合约的真正涵义所在，在解锁条件不满足的时候，元界将强制执行仲裁条款；
4. 置换（Swap）是单个资产的基本需求，MST必须满足；
5. 资产在特定场合需要被销毁；
6. 撮合交易（Exchange）是资产之间高级需求，MST必须满足；

基于以上6点，我们依次提出元界MST的6个功能。

- MST Secondary Issue;
- MST Lock;
- MST Conditional Unlock;
- MST Swap;
- MST Burn;
- MST Exchange;

加上issue和transfer，这8个功能会作为MST的核心功能，通过MIP进行迭代升级。

投资门槛

MST除了支持针对资产的需求，它可以被连接到元界数字身份Avatar上，这意味着Avatar的Reputation可以体现在MST上。

例如名为‘ERIC’的Avatar要参加名为’NEW-NASDAQ’项目的ICO，项目发起方可以设置Avatar的（Reputation）的准入门槛，例如ERIC的Reputation不达标的话，交易是无法在链上达成的。

挖矿糖果位（Mining Token Rewards）

PoW产出两种类型的交易，第一种是普通Coinbase；第二种是锁币产生的奖励；
对于第一种普通Coinbase我们其实可以升级成带MST的Coinbase，技术上来说只是UTXO扩展新类型。

看起来的效果是：一个矿工配置了MST挖矿位，例如目标币种为SONY.GAME，那么矿工挖出ETP的同时，也可以获得SONY.GAME作为奖励，这个奖励可以在SONY.GAME发行时进行配置。

考虑到区块容量，MST挖矿位不宜太多，建议是1~2个，需要矿工自行选定目标MST。

MST Offering Curve

挖矿糖果位的设置，会让人们获得与ETP同等能力的代币释放过程，这有助于构建MST的经济生态。但是我们发现，有时候人们并不需要挖矿产生糖果，直接规定一个代币释放曲线比糖果位更常见。所以MST必须支持以下三种时机下的曲线释放：

1. 首次发行时
2. Additional offering 时
3. Transfering 时

主网分叉升级下的MST兼容性

智能合约型的Token还面临着升级难以兼容的问题。例如从ERC20升级到ERC223标准时，智能合约必须重新部署，也意味着用户必须一比一兑换成新标准下的智能合约（e.g. 以1:1兑换的亏率，将ERC20 token兑换为ERC23 token）。

我们考虑比特币，比特币的软、硬分叉升级则没有为用户带来这样的麻烦，仅仅要求矿池和使用者升级钱包程序即可。

对于元界来说，使用比特币模式的升级是对用户友好的，这让商业需求得以继续，而不是被迫中断来处理升级技术标准。

所以元界MIP（Metaverse Improvement Proposal）可以使得MST功能迭代是向下兼容的，它不要求使用者重新部署合约以及兑换新的token。

数字身份–Avatar

一个人无法像现实生活中持有黄金实物那样在持有线上的数字资产，数字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。元界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数字资产。

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。

我们把元界上的数字身份称之为**Metaverse Avatar**。

四个核心问题

The current model of digital identity — focused on service access (eg:OAuth2.0 standard), does not provide true identities.
In fact, the Internet itself misses an adequate identity layer.Hence, companies and public institutions have implemented an ad-hoc system of workaround like internal databases— incompatible data silos in which they then manage the identities of people and things in their data ecosystem.
Currenttly, blockchain itself does not provide an identity layer either.
如果我们要构造blockchain-based identity，首先我们需要找到目前身份模型的问题：

Issue1. 身份数据所有权的问题

考虑到现实生活中的情况，无论是加入俱乐部还是在互联网上购物，我们都或多或少直接赋予了运营商过多的个人信息。换句话说，我们的身份其实一直在被别人记录，而不是我们自己，我们的身份信息被不同的服务商瓜分，更不用说 个人对身份数据的使用权、所有权的管理和保护。

从财产的角度分析，数字身份其实是一类特殊的个人资产，如果没有被授权就就进行读取，其实对个人财产的侵犯。例如，我在社交媒体上分享了一张风景照，这张照片存储在社交媒体服务商的数据库，服务商通过读取我的照片进行分析，随后向我推广附近地点的旅游信息，那么这张照片作为推荐系统的初始数据，间接地从我的照片获利了，这里的数据所有权、使用权的边界是模糊的。

于此，我们可以发现如今的身份系统，无论是基于IT技术的，还是 其他媒介的，均存在身份数据所有权、使用权边界模糊的问题。

Issue2. 维护身份数据的安全性（盗窃或丢失）

即使，我们很好地明确了数据所有权和使用权的边界，我们依然面临第二个问题，即信息盗窃或丢失的风险。只要我们的身份数据托管在中心化的服务商处， 必然会面临：

1）内部工作人员的道德风险；我们永远无法通过管理制度来避免人性恶的一面，内部员工都可以任意窥视我们的身份信息，而我们只能假设他们是没有恶意的。这种情况在中国内地更为恶劣，内部员工甚至可以通过贩卖用户个人基本信息和手机号在黑市上赚取高额利润。

2）黑客入侵导致的数据泄露；不存在没有BUG的计算机软件系统，只要存在缺陷就面临着被恶意利用的风险。这种情况自社交平台流行以来似乎就没有消停过，Facebook账户数据泄露，数字货币交易平台账户数据泄露等等。

Issue3. 重复且不兼容的身份数据

当我们打开一个新的网站，重复着注册，验证等过程的时候，其实相当于产生了大量的身份数据，我们一遍又一遍地填着年龄、出生地、教育情况。所以用户没有统一的数字身份，而是分散在不同组织中的数十或数百个身份片段，无法有效控制，更新或保护这些碎片身份。这些重复的身份数据似乎暗示了并不存在一个统一的、标准的、有效的身份系统，来帮助我们构建独立于服务商的身份系统。

我们想历史上曾经出现过类似的项目，例如cardsapce、openid等数字身份项目。但也许这不是我们所期待的。我们期待一个能帮助我们管理reputation、帮我们管理个人资产的数字身份项目，而不仅仅是一些应用数据。

Issue4. 欺诈

我想这也是为什么淘宝等电商服务平台能在中国流行的根本原因，由于互联网本身缺失有效的身份标准，所以任何互联网公司都不能唯一识别可能订购他们从未支付的商品的不良行为者，而用户可能会购买到虚假或者永远收不到的商品或服务。

最常见的案例是女巫攻击（Sybil Attack），用户可以对交易对手方发起女巫攻击，致使正常的服务被虚假身份所访问。

一些统计数据（来自Sovrin whitepaper）：

- 30–40% of contact center call volume is related to password and account recovery
- 18% of shoppers abandon their shopping cart due to username and password issues
- 82% of businesses struggle with fake users and on average 10% of a web-facing organization's user base will be fake
- The average retailer cost for each stolen record containing sensitive and confidential information is $165.
- 25 people in the US fall victim to identity theft every minute—leading to $15 billion in losses from 13.1 million consumers in 2015.

Worthy Identity Standard References

Blockchain-based digital identity will face these same problems, and as agreements become auto enforceable and entries in the database immutable, these problems may become even worse. Thus，We need to research those exsiting identity standards and projects.

There are some decentralized identity standards we can refer to:

- FIDO U2F/UAF, FIDO Alliance
- Web Authentication, W3C
- DIDs, W3C

- DKMS， W3C
- Verifiable Claims, W3C
- OAuth1.0 and OAuth2.0, IETF
- OpenID Connect, OpenID Foundation
- UMA and OTTO， Kantara Initiative
- Sovrin， Sovrin Foundation
- Facebook Connect, Facebook

我们发现有OpenID Connect和Sorvin与Metaverse Avatar比较接近，因此我们重点分析了它们。在Sovrin whitepaper提到了四种类型的身份类型，我们认为这种分类方法符合现实情况，它们分别是：

- Centralized identity
- Federated identity
- User-centric identity
- Self-sovereign identity

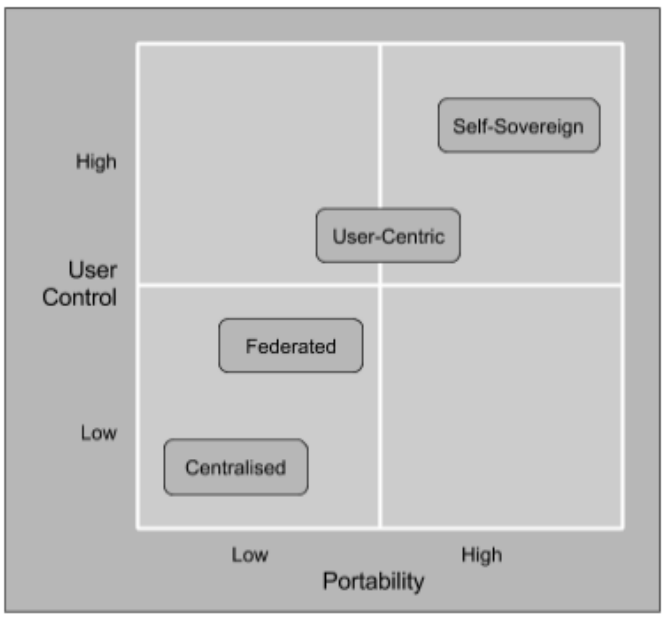


Fig 2: The four stages of online identity (from Christopher Allen #1) against at the axes of portability and control

Centralized和Federated不是我们所期待的，User-centric是目前互联网身份标准的真实处境。其中User-crentric模型下的代表是Facebook Connect，但是商业化使然，使得User-crentric仅仅在数据上实现了User-centric，自主权仍然不是用户掌握。

自我主权身份（Self-Sovereign Identity）可以说是数字身份的终极理想，自我主权身份本质上是从身份孤岛模型转变为标准层级模型，为了拥有真正的自我主权身份，我们需要身份数据和操作的权利归还给用户。

作为blockchain-based decentralized identity的一次探索，选择性地兼容已经存在的身份标准是非常必要的，毕竟完全构造属于区块链自己的数字身份标准工作量巨大，而且包含很多重复的设计工作。为了从更更好地理解这个过程，我们需要明确一下身份账本和身份终端的概念。

身份账本(Identity Ledger)与身份终端(Identity Terminal/Agent)

区块链领域有关数字身份的项目有很多，例如UPort、Shocard、Netki、Ping Identity，但人们在谈论数字身份的时候容易混淆两个概念，即身份账本与身份终端的区别。

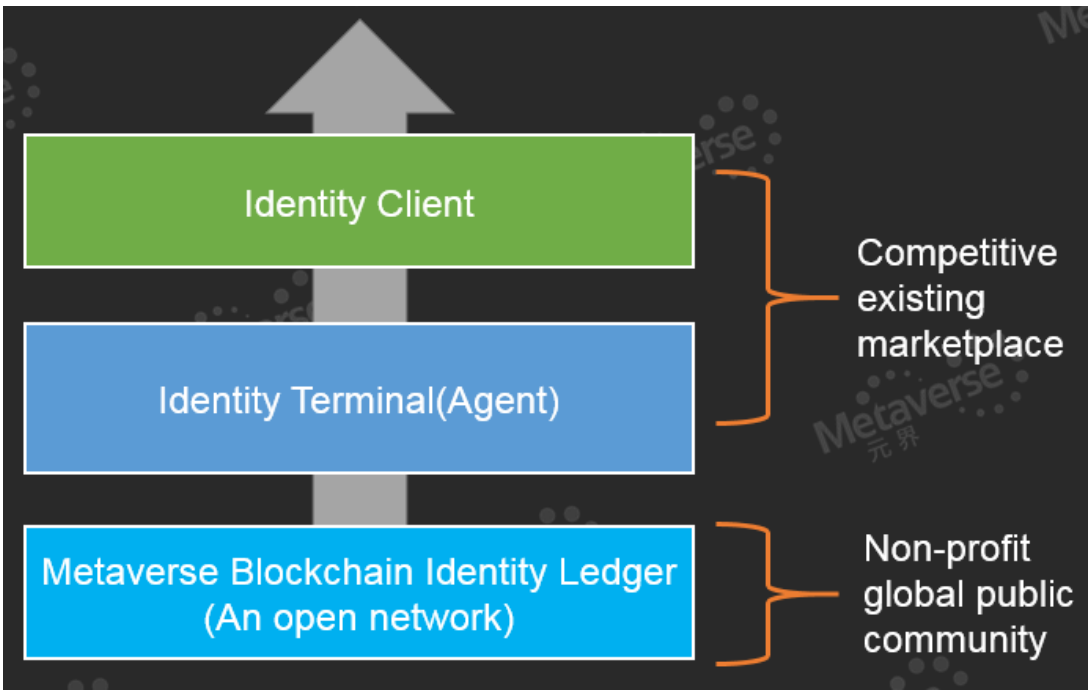
首先我们需要给身份一个定义：身份是指个体或机构在自然时间序列上的发生的一切客观有序事件集合的的统称，该事件集合具备可被验证、可授权两大特征。

我们定义身份账本：身份账本是由一条一条的记录组成，这些记录反应了一个身份所发生的客观事件。身份账本要满足两个条件，首先账本要尽可能地忠实记录客观事件，其次所记录的事件应该是我们所关注的那部分，而不是所有事件。例如Bob 1991年出生在上海，这个事件被记录在上海公安局内部的数据库中，这个数据库中有关Bob的所有记录组成了Bob的身份账本。

我们再定义身份终端：是指用户进入身份账本的代理终端，该终端支持身份验证、身份信息访问授权的功能。例如你的护照本，护照本提供了一种查询索引，在你出示护照的时候，检查人员通过读取护照本中的ID，接着到系统中（身份账本）中查询并验证你的信息是否合法。所以护照本身只是一种索引，兼具凭证功能，但它并不能代表你的真实身份，系统中的记录才 组成了你的身份。

身份终端是最贴近用户的一层，如今终端技术发展较快，从早期的磁条信息到 最近的的IC芯片，再到 现在的人脸识别和指纹验证，均属于终端上的改进。

但我们无意于革新身份终端，区块链的本职是记账，所以元界可以提供以人为中心的基于区块链的数字身份标准协议。按照这种思路，所以元界可以和各种身份终端厂商合作，构造一套 适合区块链的标准身份终端接口规范，来提升整个数字身份体系的兼容性和实用性。其次，我们可以发挥生物识别终端的优势，让硬件也可以支持元界数字身份协议，例如通过指纹识别、人脸识别、声纹识别、虹膜识别等技术来访问元界数字身份账本。



如果我们在身份终端和身份账本的概念上达成共识，我们将基于以下原则来设计元界Avatar：

（1）身份保护原则；基本主张是保护使用者的身份信息不受到侵犯，首先使用者有义务在元界区块链上通过“创建身份”、“更新身份”、“寻求认证”等主动管理方式来宣称对数字身份的所有权，其次元界区块链有义务为使用者提安全多样的接口，帮助使用者以授权访问的方式来换取其他人的服务。

（2）身份终端接口标准化；身份账本的数据格式可以自定义的，这取决于与使用者的要求，但是使用者在接口上必须是统一标准并且可扩展，否则会为身份终端的接入带来麻烦。

身份Profile与Claim

构建一套统一所有身份数据的区块链身份账本是非常困难的，但我们仔细分析就会发现，身份数据具有以下几个特征，我们只要让元界数字身份满足以下几个特性，做成开放式的标准，然后使用一些激励手段，让用户在身份账本上各取所需，这是我们应当做的。

隐私边界

任何身份产生的行为记录，对公开的敏感程度是不同的，这种敏感程度我们定义为隐私边界。

隐私边界由人的本能安全感和文化约束两部分组成。例如绝大部分人不能接受在公共场合赤身裸体，即使没有道德约束，这也是难以接受的，因为毫无庇护让我们丧失了安全感，找到安全感也是隐私的主要诉求。其次文化的约束也是不同的，例如在 欧洲文化中，对PII（Personally Identifiable Information）信息非常敏感，政府甚至要求服务商不能要求用户在线上提供PII信息。而在东方文化中，集体主义的盛行也让个体 对隐私边界比较宽容，例如父母可以 干预成年子女的婚姻、就业。

隐私边界的多样性也决定了数字身份必须是中性的，它必须提供足够的自由度，让人们可以控制自己的隐私边界。所以元界数字身份可以使用两种手段来保证隐私边界：

1. 提供匿名交易；
2. 不推荐用户PII信息登记到区块链，即使它是加密的；

声誉Reputation与简历Profile

假设我们现在已经有了元界身份账本，那么对于使用者来说，最重要的是什么呢？是Reputaion。

任意一个新数字身份或者使用频率低下的数字身份，被大众所接受的概率低，反之使用频率越高，涉及的身份记录越多，也就证明这个身份越可信。换句话说，被登记的记录越全面，被验证的次数越多， 身份的信用度高。

所以对于元界数字身份， 如何度量数字身份的置信度变得格外重要。

置信度体现在两个方面：

1） 原生链上记录；是指用户使用元界数字身份产生的记录，例如基于数字身份的转账记录，数字身份下持有的资产情况；

2）引用链下记录；是指用户可以登记任意信息的数据域data-feed。

到这里我们可以推导出元界数字身份的基本结构了。首先我们定义身份Profile，用来描述一个身份，它是身份账本的基本单位。

Profile包括上述1）和2）中的两种记录，使用者可以根据这两种记录计算出自己认可的Reputation。

1）类型的记录是由区块链的交易记录保证的，我们提供准确方便的查询接口即可。

2）类型的记录具有多种设计模式，以太坊ERC725提案描述了一种容易使用和设计的方案——Claims-based identity。

如果我们观察一些商业领域的案例，例如交易平台KYC认证体系，也是Claims-based，平台授予用户一个Claim，这个Claim表示用户通过了该平台的KYC认证。

所以data-feed的主要功能是Claims-based进行填充，一个身份理论上可以有无限多的claims，这些Claims具有以下特性：

1. 时效性；任意的Claim必须具有有效期，例如KYC认证具有有效期，而不是永久。

2. 多面性；一个自然人或者机构具有多面性，例如某人在公司是工程师，在学校则成为孩子的家长。
3. 隐私可控；

有了Profile以后，任何使用者可以基于Profile来定义Reputaion，例如我们可以要求Reputation达标的用户在可以参与ICO，而不是任何人都可以。

身份DID连接数字资产

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应该能拥有多种类型的数字资产，一种数字资产也可能由多个Avatar共同拥有，avatar和数字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。

所以即使我们有了Profile，它仍然是孤立的，它需要与数字资产联系起来。于是我们需要一个全网唯一的索引，这个索引是身份的凭证，它连接了数字资产与数字身份。

我们这里定义为：DID（Digital Identity Designation)。DID可以唯一索引到一个Profile，并且可绑定到任意元界上的地方，这带来匿名性上的好处，用户仍然可以使用基于地址的数字资产，也可以选择使用DID公开与数字资产的关系。

DID可以帮助人们操作资产，例如发行、转移、抵押、担保数字资产，而不必基于钱包地址。例如我的DID是“chenhao”，Eric支付我ETP或MST的时候不必填入元界支付地址，使用“chenhao”代替地址即可。

DID看起来仍然像是一个孤立的“域名系统DamainName Sytem”，不足以表示与MST以及Avatar之间的关系。MST与Avatar我们可以参考OOP（Object Oriented Programming），MST与Avatar以及Avatar之间至少会展现出：Has-a，Is-a，Like-a 三种关系。

为了实现以上三种关系，DID、Profile、Claim可能需要与已经存在的互联网身份发生联系，例如将OIDC中End User的Claim可以映射到DID下的Profile下的Claim上。

验证(Authenticate)与授权(Authorize)

Profile和DID只解决了数据的问题，并没有描述使用者如何操作数字身份。

数字身份上的核心操作只有两个——验证和授权，所以我们研究了有关验证和授权的既存标准协议：基于PKI体系的x.509标准、互联网标准授权协议——OAuth2.0、去中心化的身份验证协议OIDC（OpenID Connect）。

x.509

基于x.509标准的应用范围很广泛，例如TLS/SSL基于X.509标准，而TLS/SSL被众多互联网应用所引用，所以x.509是一个偏向底层的基础设施标准。

X509标准本质上是CA-based，它描述了证书的行为和格式，但x.509不满足我们所说的身份账本和身份终端的概念，它只提供了证书这一种模式，并且有以下缺陷：

- 根证书（Root CA）无法被撤销；
- using CRLs and OCSP 带来的中心化问题，降低了安全阈值；
- 复杂的结构，使用并不友好；
- 由于不同类型的Claim过度聚合，引起的隐私和维护问题；
- 对于EV（Extended Validation），DV（Domain Validation）、OV（Organization Validation）可以重复申请带来的中间人攻击（man-in-the-middle attacks）。

所以直接基于x.509构建Avatar并不是一个很好的选择，虽然可以立即支持大量应用，但是有很多额外工作需要做。

OAuth2.0

OAuth 2.0 is an open standard protocol for authorization that enables an application to access certain user information or resources from another web service, without giving the user's credentials for the web service to the web application.

Actually, OAuth2.0 has already become the standard protocol for Internet application authorization and has been used widely. Through analysis, we can find that the popularity of OAuth2.0 is based on the authorization agreement of the User-Centric mode, which also reveals that OAuth2.0 can only complete part of functions of digital identities, rather than all functions.

OAuth 2.0 is an excellent tool, but it is still oriented towards centralized services. Since there is no concept of defining digital identities, this issue will not be solved until the establishment of next standard – OIDC (OpenID Connect).

OpenID Connect

OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.

目前对这个项目起最大推动作用的，当属Google Identity Platform和Google+应用。Google作为互联网2.0时代的一个超级入口，本身存储着海量的个人身份数据，通过OIDC允许第三方应用接入和使用Google账户相关信息。

虽然Facebook、Google、腾讯、阿里、微软都使用了OIDC，但实际上平台间的个人数据依然是各自独立的，不能相互授权和验证，换句话说，身份数据在各平台内部是兼容不重复的（Issue3），但是在平台之间仍然还有兼容性问题，并且由于个人数据是托管在平台内部的，所以Issue1仍然没有解决。

可以说OIDC改进了Issue1、Issue2、Issue3的问题处境，但并没有真正解决，例如最近发生的Facebook 8700万用户数据泄密事件。

Metaverse Avatar

MAV（Metaverse Avatar）是基于区块链的开放式身份标准协议，MAV可以兼容OIDC，从技术层面来说，MAV是OIDC在区块链上的协议扩展。

这里明确的是MAV不是既存身份系统的映射，目前也无法完全达到自主身份的理想。理由如下：

由于区块链容量的限制，人们无法把海量的身份信息存储在区块链上，提升区块链性能只会加剧区块的增长，因为当区块链的尺寸被某个应用过度使用，造成每天1GB的尺寸增长，区块链就失去了作为公共资源的意义。

所以我们需要将MAV划分为两个层次来解决这个问题：第一层是OIDC，第二层是MAV MetaData。

我们推荐使用OIDC来解决海量存储的问题，OIDC我们可以选择IPFS作为存储协议，也可以选择云存储，这两种方案都可以在MBaaS中解决。

而MetaData提供区块链级别的记录，这里的MetaData是指身份的关键信息，在交易平台的KYC案例中，MetaData就是指KYC的验证结果，它可以被存储到DID下的Profile中，换句话说，MAV的Profile为MetaData提供了链上数据容器。

为了实现MAV，需要从以下两个方面考虑：

1. **Relationships Management（关系管理）：** 通过MetaData体现出来的MAV之间的关系；MAV与MST之间的关系；
2. **Permission Control of Avatar（权限控制）：** MAV对MetaData权限控制；MAV对OIDC的权限控制；

MetaData是区别身份数据是否上链的标志，对于具有自我意识的主体（通常指人类，未来也许是人工智能）来说，我们建议将PII信息驻留在OIDC，而不进入MetaData；对于各类实体的、虚拟的资产，例如私人汽车、宠物，我们可以通过Identifiable Information生成MetaData，然后把MetaData登记到链上。

MAV的验证和授权首先基于OIDC，其次也会在链上提供基于零知识证明的授权过程、或者基于同态加密的授权过程。

价值中介Oracle

某些区块链项目声称去中介化，或者叫“消灭中间人”，目前来看是不现实的。

取得链外数据，也就是可信的data-feed不是区块链本身能解决的问题，data-feed数据本身的可信与否区块链本身是无法判断的。例如某MST的合约解锁条件设置为3天后上海地区降雨量达到50毫升，区块链是无法感知现实天气状态的，那么必然会涉及到Oracle，MST合约的data-feed指向为雅虎天气作为数据源，Oracle需要为此担保，并且还有一个仲裁Oracle用于执行出现分歧时的仲裁。这里一共出现了3个Oracle，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。

所以不同于“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。提供资产托管服务的Oracle可以保管物理形态的资产，然后在链上发行数字资产；身份认证型的Oracle可以在链上提供个人信息与Avatar相关性的证明，监管型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。

Oracle是一类特殊的Avatar，Oracle也基于Avatar的认证和授权体系，这些都是元界区块链的内置功能，所以任何人都可以无条件声称自己是一名Oracle，但随之而来的问题是，如何证明这名Oracle提供的服务是忠实信任的，这取决于这名Oracle的Avatar记录是否足够丰富，Reputation是否足以支撑他说声称的服务。这会极大地扩展元界上的交易类型，每种交易类型又可以连接到数字资产MST，所以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。

两个阶段

数字身份Avatar的发展必然会经历两个阶段，我们称之为引入证明阶段和自举证明阶段。
引入证明：引入证明是指链上的数据不足以支撑一个数字身份的可信度，那么必然需要**直接**引入链外数据作为证明。例如证明你的出生年月是否真实，可能会用到你的护照作为证明。
自举证明：自举证明是只链上的数据足以支撑一个数字身份的可信度，不需要额外引入链外数据。例如你的出生年月已经被其他Oracle证实过了，验证者只需要直接引用即可。

引入证明是数字身份发展的初始阶段，随着使用者增多，诚实Oracle验证的次数足够多，那么新的应用似乎可以直接开展，而不需要再次引入证明，这里Oracle扮演了至关重要的角色。

区块链即服务BaaS

站在Oracle的角度来看，中介是必然存在的，这也使得元界不同于只提供dAPP的区块链平台。

区块链本身是去中心化的，但不意味着应用也必须是去中心化的，因为应用去中心化意味着打破了人类千百年来的文明结构：

所有的信息的流转体系中永远都会存在信息提供者和信息消费者两种角色， 这是由人类社会结构决定的，妄图消除这两种角色之间的鸿沟是非常难的。假设即使消除了信息信息不对称（实际上只能降低，无法消除），人与人之间还存在认知不对称的问题，认知不对称由于人的精力有限，无法绝对学习人类已经获得的全部知识，例如我看病的时候，我听取医生建议的前提是我信任这个医生。

如果现在存在一种新的模式，构建任意应用都无需依赖信任，那么也意味着人类的社会结构会发生巨变，例如我们不需要信任任何医生，去任何医院我都能获得有价值的建议，那么当这些医生的建议出现分歧的时候，这个无需信任的系统是否就崩坏了呢?

所以无论什么类型的应用，应用的提供方必然既是服务者又是占据信息优势的一方，用户处于消费者的角色，那么只要这两种角色存在，应用就无法去中心化，中心化代表着资源汇聚产生的优质服务，除非人工智能和代码能完全取代目前人类社会的所有服务，这显然不太可能。

例如一个智能的去中心化交易平台使用了TLS/SSL对网络通讯进行加密，再次出现类似2014年的Heart Bleeding的缺陷，导致成千上百用户的资产丢失了，谁会为此负责呢?

基于以上论述，元界认为区块链与现实最好的接触点，是成为互联网的底层基础设施之一，它并不颠覆中心化的互联网应用，恰恰相反它所带来的数字货币、数字资产将会成为互联网的补充并迅速侵袭互联网，让所有应用以几乎为零的成本享受数字金融带来的便利。

在这个过程中，Oracle可以是中心化人为控制的应用，也可以是dAPP代码，Oracle为人们提供服务，且接受人们监督，这一切发生在元界上，而不是割裂在不同的IT 系统中。

智能合约与BISC（Built-in Smart Contract）

如果把区块链技术的发展比作计算机技术的发展，例如比特币是汇编语言，它靠这套语言实现了基本的支付功能，那么可以认为以太坊等众多智能合约平台提供了高级编程语言。

但如果说计算机技术的发展方向是编程语言的发展，我相信大部分技术人员都不会同意的。技术包罗万象，编程语言只是其中一个工具集，况且一种编程语言的流行程度背后其实是这门编程语言背后框架所能支持的应用生态的多样性决定的，与其说编程语言是发展方向，不如说这些编程语言的一些通用库、框架是发展方向，例如Javascript的Vue.js、C++的Boost库、深度学习框架Tensorflow、大数据处理框架ApacheHadoop等。

那么什么是区块链领域的Vue.js？答案是ERC20、ERC725等一系列能帮助现实世界建模的通用智能合约标准（模板）。ERC20的流行是由于它提供了Tokenization的能力，所以并没有多少人了解ERC55标准是什么。

那么什么是区块链领域的Tensorflow呢？答案是按照体系构建的数字资产和数字身份带来的基础框架，而不是个别模板组成的功能单一的基础设施。

我们进一步分析可以发现，比特币极力避免使用图灵完备的智能合约语言，因为在比特币看来，完成稳定、高效、安全的支付的是第一位的，比特币脚本其实是一套轻量级的智能合约模板，例如P2SH脚本可以提供多重签名支付，这对于比特币支付已经足够。激进的可编程智能合约往往带来潜在的安全性问题，我想这也是比特币核心开发者不想看到的，对于比特币的支付安全来说，加入图灵完备并且可编程不是必需的。

遵循比特币思路，元界应当为人们提供稳定并且安全的有关数字资产的智能合约标准模板，也就是MST，提供有关数字身份的智能合约标准模板，也就是元界数字身份，这些智能合约标准模板我们内置到元界底层，我们统一命名这些模板为**BISC（Built-in Smart Contract）**。

BISC可以是比特币脚本实现的，也可以是基于EVM又或者是WASM的。

在编程领域，我们有两种常见模式，第一种是OOP（Object-Oriented Programming）和OOD（Object-Oriented Design），第二种是函数式编程（Functional Programming）。

现在考虑账户模型，基于账户模型的智能合约更适合OOP，而UTXO模式比较适合FP。考虑到构造的BISC的安全性，ETP和数字资产本身可能更适合UTXO+FP模式，基于这两者去构建更复杂的行为，需要吸取OOD的经验。

基于以上思路，BISC首先需要generalization standard templates for digital assets (MST) and digital identities (Avatar)，他可能是基于UTXO+FP的，rather than redefine their own applications with OOD（realization、dependency、association、aggregation、composition and inheritance）.

我们可以考虑在区块链上提供经过安全代码审计的BISC区块，开发者可以直接调用BISC或者运行一个BISC的实例（instance）。看起来的效果可能是这样的：

```
import MST
import Avatar

myAsset = MST.connect("ERIC.BTC")
myAvatar = Avatar.connect("CHENHAO")
if myAvatar.reputation.get() > MST.threshold.reputation.get():
   myAsset.swap(myAvatar.etp, 10)
```

代码展示了使用10个ETP购买ERIC.BTC的过程，这里的MST、Avatar都是元界区块链的BISC，这中间还判断了名为CHENHAO的Avatar的reputation是否达标。

这段代码可以部署在区块链上，也可以是普通的python脚本，视场景而定，实际上我们推荐人们使用侧链或者传统应用的方式使用BISC，这就是我们接下来会讨论的BaaS。

区块链即服务

如果我们要定义BaaS，首先我们需要找到BaaS与PaaS的联系。

PaaS提供了有用的基础业务组件（Component），例如AWS的Amazon Translate服务，Aliyun的短信服务，这些服务不是单纯的技术框架，而是已经能够提供特定功能的服务。

我们接下来考虑比特币，比特币提供了全球支付的功能，那么这种功能是否可以植入到云服务中呢？答案是肯定的。对于诸多有支付需求的应用来说，自己搭建比特币节点，并且结构化区块到数据库中是非常痛苦的过程，毕竟比特币全节点提供的API有限，而我们的查询需求可能细致到交易输出和脚本签名。

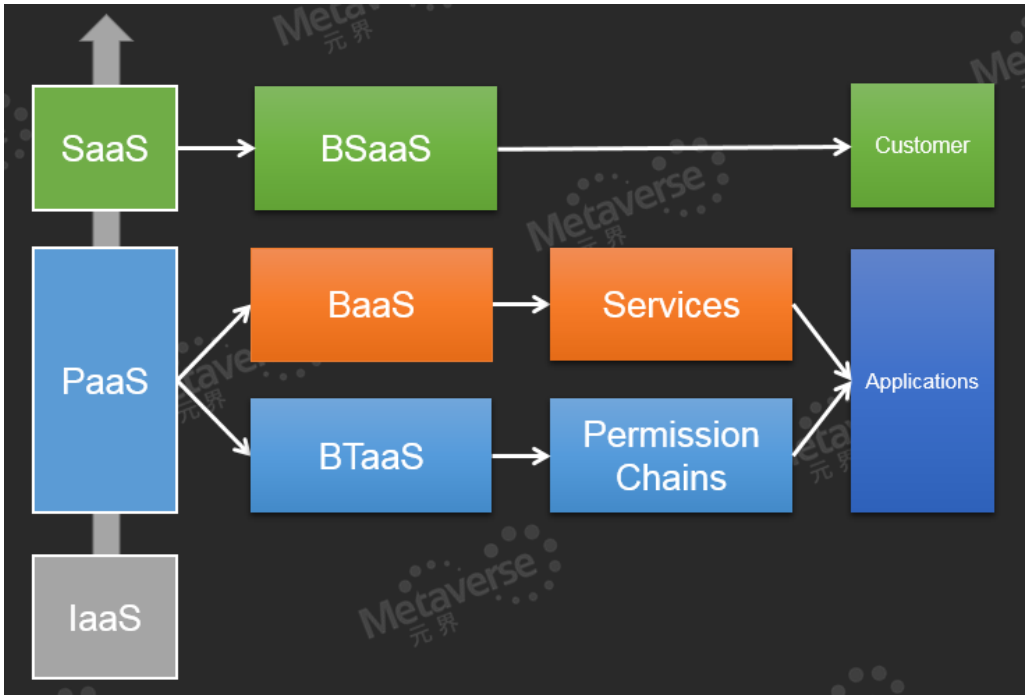
据此我们可以发现，比特币等诸多数字货币都可以做成基础PaaS服务提供给用户。于是我们可以给出区块链即服务的定义：

区块链即服务是指提供多种方式的查询、交易广播、交易验证，使得公有区块链的服务可以植入到传统IT架构或互联网架构中，这些服务包括Tokenazation（资产数字化），数字身份Avatar服务、Oracle服务，这些服务以前是割裂的，现在BaaS定义了标准规范。

目前区块浏览器、数字货币交易平台多数架设在公有云服务之上的，进而他们必须搭建属于自己的数字资产管理和验证服务，实际上这是非常通用的基础功能，云服务厂商完全可以提供通用的基础框架，就像Amazon Translate服务一样，所以我们可以得到基于区块链的PaaS衍生版本——即BaaS。

接下来我们考虑SaaS，SaaS最好的例子是Google Docs，按需按时间付费使用厂商的应用是SaaS的显著特征。实际上比特币本身也是一种SaaS，只不过比特币并没有特定的云服务提供商，但是如果我们把比特币的网络看成是一种开放式的云，它可以提供公证公告的功能，并且交易费用按size收费，那么比特币是SaaS似乎可以说得通，例如blockchain.info。

我想这张图可以很好地解释这些的概念：



- BaaS——PaaS的变种——**BaaS (Blockchain As A Service)**
- BTaaS——PaaS的变种——**BTaaS (Blockchain Technology As A Service)**
- BSaaS——SaaS的变种——**BSaaS (Blockchain Software As A Service)**

BSaaS要求用户可以直接使用的区块链快速构建服务，构建过程可能是图形化的，目前BSaaS尚不成熟，更没有成熟的应用，也许以太猫算是。

IBM和微软曾经提出过BaaS的概念，它对标PaaS，但我们在这里将BaaS概念作了拆分，拆成了BTaaS和BaaS。

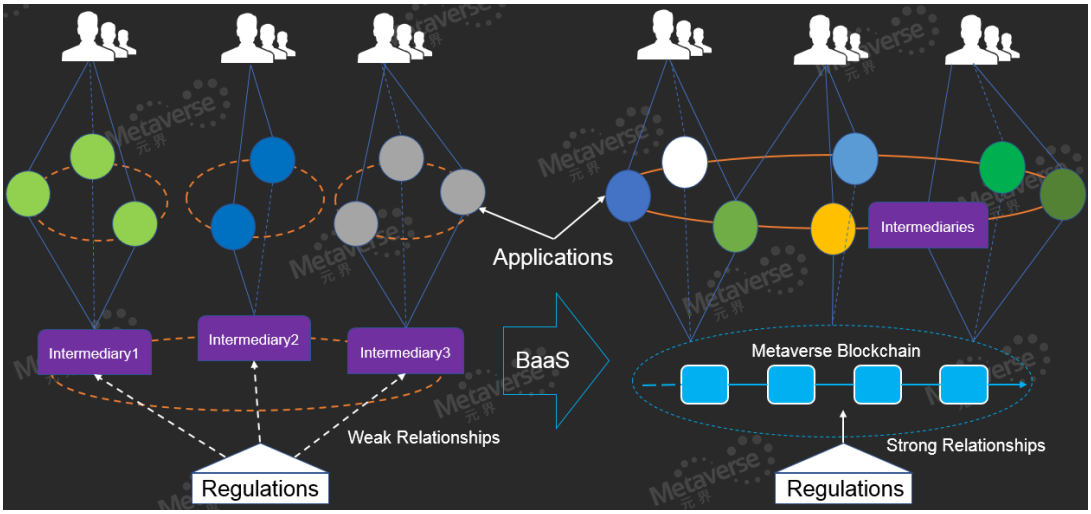
这里的区别在于使用区块链技术框架构建属于自己的许可链，还是使用公链上的服务。前者也就是IBM和微软提的BaaS的概念，这里我们更名为BTaaS。BTaaS也可以通过传统IT方案解决，例如使用SOA架构的软件替代区块链去构建复杂的企业内部应用。

许可链，是少数节点之间的活动，它往往退化成微观经济中的博弈，所以利用许可链构建少数节点之间的协作系统不是一个技术问题，而变成了如何构造一个稳定的微观经济模型使得协作者可以达成帕累托改进，在这里技术是次要的。

公链提供的服务往往会比许可链丰富，如果公链具有匿名性和权限管理机制，则完全可以替代许可链。

BSaaS和BTaaS都不是元界所关注的类型，BaaS才是元界首先关注的。

BaaS意味着将公链提供的服务方便地集成到既存的系统中，例如比特币提供的支付功能。这里元界提供的是Avatar和MST，例如电商可以为所有店家提供MST登记服务，那么店家就可以基于元界发行自己的积分系统，这些积分具有区块链带来的优势——点对点，不可篡改，无界流通的优势。

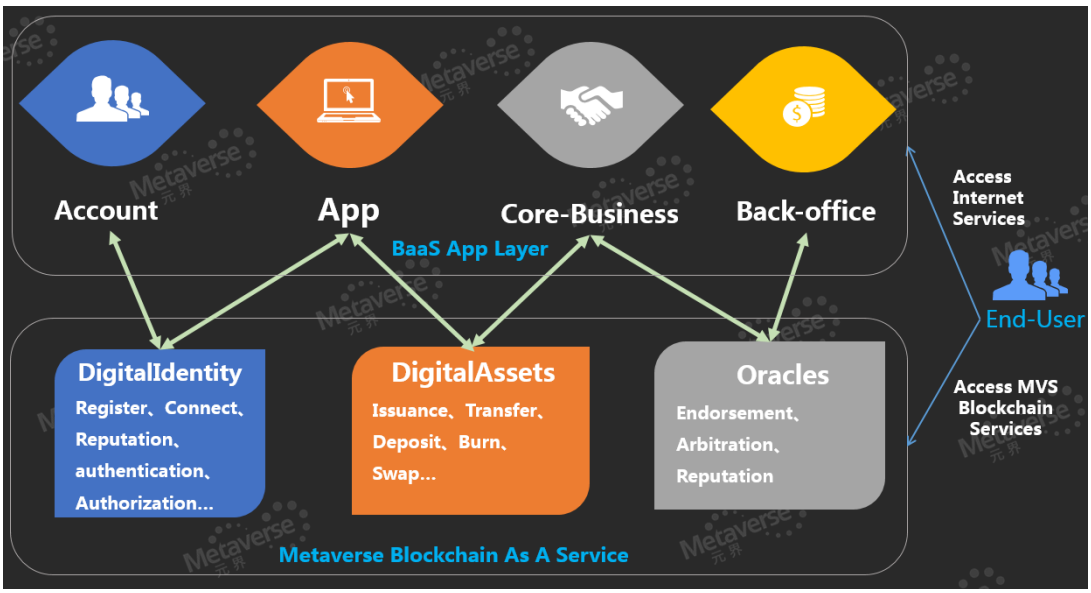


最终，BISC可以成为Oracle和项目开发者的有利武器，他们的实践形式就是BaaS，项目方可以使用BISC开发多样性的中心化应用，Oracle可以利用自己的数字身份BISC对其进行背书，使用者可以通过BISC监督项目方，三者可以组成链上闭环。

元界公链即服务MBaaS（Metaverse Blockchain As A Service）

数字货币的基本功能是支付，所以集成数字货币的支付服务是非常简单的，考虑将比特币定义为支付网关，那么在架构上的位置就很清晰了，可以被纳入到资金管理模块当中。

考虑到元界的MST，以及数字身份，那么元界区块链可以在常见的IT系统中扮演如下角色。



我们假设所有系统具备自己的账户系统、登录系统、业务系统、后台管理系统。那么数字身份可以用于支持既存系统中的账户系统；数字资产MST可以带给你的产品资产数字化的能力，而不必构造自己的区块链技术体系；Oracle可以增强你的系统业业务抗风险能力。

以上服务我们统称为MBaaS，MBaaS可以为任何既存的IT系统、互联网应用甚是物联网设备提供基础设施服务，这些服务以数字身份作为主要的切入点，为人们提供方便简单的资产数字化能力。

区块链应用开发过于复杂，如何降低技术的集成难度，这样可以让业务更聚焦在创新上，而不是区块链的底层技术。BaaS本质提供了一种集成思路，目前亟需解决以下两个问题：

1. **集成问题：典型稳定的技术框架，用于集成BaaS和既存的IT系统；**
2. **数字资产管理问题：面向企业的数字资产管理工具，提供安全访问的私钥管理机制；**

MBaaS也面临上述问题，而我们的思路是：

1. 对钱包功能进行解耦，提供隔离运行的独立模块程序，全节点钱包和轻钱包属于粗粒度的划分，不足以满足架构的多样性需求。
2. 基于HD(Hierarchical Deterministic)的私钥管理体系，提供多重签名（Multi-signature）。

HD和多重签名是比较成熟的技术了，那么考虑 Aggregation将是MBaaS面临的首要问题。

MBaaS与架构模式聚合(Aggregation)

架构模式有很多种，我们仅讨论单点应用、分层架构模式、事件驱动的架构模式和微服务架构模式。我们将讨论MBaaS应当处在这些架构模式的什么位置。

MBaaS与钱包的关系

首先MBaaS是一类服务的集合，在系统中的表现形式是一类服务进程，它们通常是由钱包程序运行而产生的。

目前我们有两种模式可以可以操作：

1. **钱包程序分离模式**：从钱包程序分离出功能，做成多进程模式，每个进程提供了轻量级的MBaaS；
2. **钱包程序统一模式**：钱包程序提供有所MBaaS，但是可以形成主从关系，做成内部分布式网络，而不是连接到公网。统一模式对钱包的优化和稳定性提出了更高的要求。

分离模式

元界至少提供以下基本模块分离：

- P2P网络
- 交易验证和解析
- 私钥管理
- 区块持久化存储

轻钱包是分离模式的第一个案例，从全节点钱包。

统一模式

钱包程序至少提供内部高速同步的功能，内部节点从最终一致性转变为强一致性，要求当区块链分叉时，支持内部节点可以达成强一致。

分离模式和统一模式并不是绝对的，在实际场景中可能存在混合用。我们接下来根据架构模式进行探讨。

单体应用（Monolith Appicatlions）

单点应用分为客户端单点应用和服务端单点应用。

服务端单点应用例如wordpress，如果我们想让wordpress支持MST，最快速的方法是在wordpress的后端同时搭建元界钱包，然后修改后端代码去调用MST相关的API，最终界面显示MST的token即可。这种情况适合统一模式，快速部署。

单点应用比较常见地是使用微内核架构（Microkernel Architecture）模式。例如在Eclipse IDE中植入Metaverse Avatar，这就要求元界轻量级钱包作为插件植入到Eclipse中。这种情况适合分离模式，例如轻钱包。

分层架构模式（Layered Architecture）

分层架构既适合分离模式，也适合统一模式，取决于这个分层架构的规模大小。分离模式适合大规模的分层架构，例如一个SOA架构中，统一模式显然胜任不了。

考虑分离模式，分离模式下的MBaaS适合放在分层模式的业务层，成为一个个普通组件，它只要求钱包的API与业务层的其他模块尽可能兼容。如果存在持久层，可能需要区块链结构化存储，否则可以直接使用钱包本身替代区块存储的功能。

考虑统一模式，统一模式下的MBaaS适合小规模的应用，MBaaS的搭建可以参考服务端单点应用。

事件驱动的架构模式（Event-driven Architecture）

事件驱动的架构模式适合分离模式。

事件驱动的架构模式关注的是对事件的分发和处理，如果我们分析区块链的逻辑，我们可以发现区块链都是基于交易的，交易本身就是一个事件，所以在事件驱动的架构模式中，分离模式是最适合的。

在Mediator模式中，交易类型与交易数据需要被解析再分发，所以Mediator必须具有解析交易的能力。如果是账户状态模型，还需要具备读取账户状态的能力；在Broker模式中，每个Processor具有解析和判断交易的能力即可，不涉及Broker的变更。

上面的流程作为事件输入的，而需要交易输出的时候，我们可以可以把钱包看成一个processor，只处理和区块链相关的业务，但这里可能会遇到这个processor演变成中央processor的问题，因为在任意一个核心业务流的最终目的都是支付，钱包processor会成为验证、签名、广播交易的集合体，会遇到明显的性能瓶颈。

所以分离模式下的网络模块、交易验证模块可以设置为水平扩展的。分离模式要求元界提供比较完备的SDK来支持事件分发和处理。

微服务架构模式（Micro-services Architecture）

微服务架构既适合统一模式，也适用于分离模式。

考虑统一模式，让钱包成为微服务组件，只要求钱包功能足够内聚。例如钱包可在组件A中扮演支付的角色，在组件B中扮演交易验证的角色。这就要求钱包的行为尽可能地贴合微服务架构中微服务，并且提供足够丰富的查询和验证API。

考虑分离模式，分离模式似乎与微服务的架构思路非常契合，那么提供标准化的元界微服务组件就成了我们首先要考虑的，这似乎不是很难。

MST链上可交易（Exchange）

链上可交易是MST的高级需求，主要出于可扩展性（scalability）的考虑。

方案一：石墨烯（Graphane）

目前比较成熟的技术是石墨烯（Graphane），为了可以支持链上交易，元界考虑集成Graphane，面临了以下技术挑战：

1. MST的向下兼容性；
2. Avatar与DPoS算法的兼容性；
3. UTXO模型与Graphane账户模型的兼容性；
4. Transaction本身的兼容性；
5. 加密模块的兼容性；
6. 撮合模块的可控性；

方案二：链上结算、链下撮合的0x协议
比特币隔离见证（SegWit）和闪电网络(Lighting Network)提供了良好的scalability，升级到隔离见证以后，元界可以建立类似0x Project的链上结算协议，利用激励措施让众多交易平台的订单和行情数据互通。

潜在的风险与考虑

区块链技术仍在处在快速发展阶段，其成熟度还在持续的研究过程中，元界来自比特币系统，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，如果不考虑去中心化的原则，UTXO模型可以支持区块截断，截断位置可以从最老的一笔UTXO所在的区块开始。从这个位置开始定义为“Milestone”区块，它的意义接近于创世区块。

- **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。

如果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五倍。

参考文献

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

2. Namecoin: https://namecoin.org/
3. Bitshares whitepaper: http://docs.bitshares.org/bitshares/papers/index.html
4. Ethereum WhitePaper: 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. Tim Swanson ——http://www.coindesk.com/smart-property-colored-coins-mastercoin
10. https://en.bitcoin.it/wiki/Script
11. https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper
14. https://en.wikipedia.org/wiki/Claims-based_identity
15. https://en.wikipedia.org/wiki/Digital_identity
16. https://en.wikipedia.org/wiki/X.509
17. https://en.wikipedia.org/wiki/Personally_identifiable_information
18. Shocard whitepaper – https://shocard.com/wp-content/uploads/2016/11/travel-identity-of-the-future.pdf
19. https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf
20. ERC725 – https://github.com/ethereum/EIPs/issues/725
21. The Construction of Reputation in a Negotiation – Carl-Erik Torgersen
22. Digital Identity Interoperability and eInnovation – Berkman Publication Series
23. Software Architecture Patterns —— Mark Richards
24. https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki
25. https://blockchainhub.net/blog/blog/decentralized-identity-blockchain/
26. https://sovrin.org/wp-content/uploads/2017/07/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf