元界白皮书

穿越智能资产，数字身份和价值中介

来到虚拟现实世界

摘 要

摘要

元界是基于公有区块链技术开发的去中心化的平台，涵盖了数字资产和数字身份。元界最初是由维优的团队组织开发和维护的，是在 MIT 许可协议之内进行开发的项目。当元界项目达到一定的成熟度，其代码将被开源公布在 GitHub 上，地址是：
https://github.com/ViewFin/Metaverse

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、物流业等众多行业带来重大变革。

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。细数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

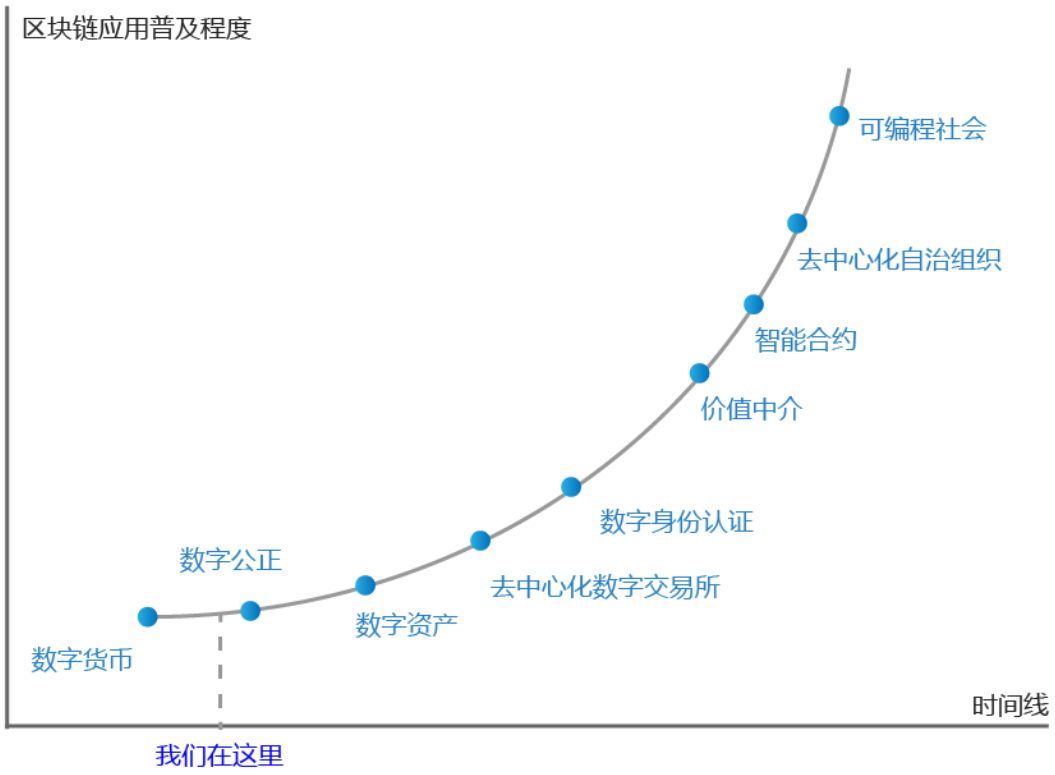
比特股是站在 POS 共识机制的巨人肩膀上成长起来的项目，并在之后将共识机制改良成为 DPOS 权益代表证明。在比特股上，新的概念被不断提出来，包括更加突出数字身份的项目 Keyhotee，以及通过定义多种交易类型，可以更简便地登记、发行数字资产等。比特股主要去中心化交易所的概念，并为了实现良好的交易体验，重新改进了出快的速度，达到秒级出块，相应地也牺牲了一些系统的稳定性。

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

元界 Metaverse

虚拟即现实

Metaverse 一词最早出现在 Neal Stephenson 的科幻小说《snow crash 雪崩》中（1992 年），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。

Entropy（熵）-元界的代币

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，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。

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，或者申请成为一名 Oracle。

ETP 的分发机制

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 月成功地众筹筹集了 2100 枚比特币。

Metaverse 项目的 ETP 将会通过两次 ICO，向外界分发 1 亿枚总量的 50%～60%。其中 2016 年 8 月的首次 ICO 会分发 20%～30%，而第二次 ICO 将在 Metaverse 的客户端（钱包）和区块链底层完成之后启动，第二次 ICO 也将分发 1 亿枚总量的 20%～30%，预计时间是在 2016 年的十月。

剩余总量 40%～50%的 ETP 将通过 POW 机制以区块奖励的方式分发给系统安全的维护者，这个过程或称为挖矿。

微通胀

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。为了保障系统代币具有足够的流动性，并且让 Metaverse 能够容纳更多的数字资产，我们设计了一个线性微通胀的经济模型。在 POW 阶段结束之后，每年将由系统发行 4 百万 ETP 投入到系统中进行流通，并且不难预见的是，最初几年的通胀率约为 4%，然后这个通胀率将越来越小，等到达与 Vitalik 预测的 1%年损耗相等时，将保持动态平衡。

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，元界的数字资产将沿用比特币系统的 UTXO 方法（未交易输出 Unspent Transaction Output），数字资产将保留一个域空间和一个地址/数字 ID 身份。任何交易都将由一组输入和输出定义，并且带有当前数字资产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。

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。

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集成在 Avatar 中，并以密码学的方式保护起来。这些信息将可以通过零知识证明的技术向其他人展示需要透露的部分，并且要经过 Avatar 所有者同意（私钥签名）。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。

在智能资产之上，特定的（金融）应用场景可以起舞：交易、借贷、租赁，还有抵押等。

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。

技术部分

共识算法

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。

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。

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。

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。

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。

跨链虚拟机

以太坊的智能合约代码是通过 EVM 虚拟机来执行的。元界与此不同，将把研究力量放在跨链交易的虚拟机（CCVM，Cross Chain Virtual Machine）的研发上，实现不同公有区块链之间的价值交换。

潜在的风险和考虑

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。

结论

与比特股和以太坊相似的，元界是从比特币系统中受到启发，使用区块链技术解决比电子现金系统更多、更复杂的问题；比特股解决的是去中心化交易平台的问题，以太坊解决的是智能合约和去中心化应用平台的问题。元界通过对数字资产、数字身份的清晰的定义，还有对区块链上价值中介 Oracle 的重要性的突出，保障了数字资产的确权，并且定义了未来数字金融的基础。

在元界中，通过价值中介起到的作用，智能资产可以在不同的数字身份中进行各种安全的转移。得益于区块链技术，元界天生继承了其不可篡改的账本，以及不可双花的优点，元界将在数字资产和可数字化资产的海洋徜徉。

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