BDC

虚拟现实生态网络

(BDC)项目白皮书

目录

摘要

区块链技术被认为是继蒸汽机、电力、信息和互联网科技之后，目前最有潜力触发第五轮颠覆性革命浪潮的核心技术。可以说区块链极有可能在未来的 5-10 年内颠覆很多行业，区块链这项未来最重要的底层技术，与数据这项未来最重要的社会资源结合在一起，能够释放出极大的商业价值、社会价值。

现代的生活越倚重互联网，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。

宝岛链的定位，是基于区块链建立一个可信任的虚拟现实生态网络，让各个领域的数据都可以非常自由、相互信任、极度高效的共享交换，让数据逐渐远离垄断，信息不再有孤岛，让数据为商业和我们的生活提供更高的价值。

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。

区块链技术存在的主要问题

以比特币[1]为代表的基于 UTXO 的区块链和以以太坊[2]为代表的基于账户的区块链向我们打开了新世界的大门。比特币和以太坊的成功，证明了区块链技术的价值和未来的巨大潜力，同时在这个过程中我们也看到了区块链技术在一些方面存在的先天不足。

可扩展性

为构建通证（价值）流动的去信任的分布式网络，比特币和以太坊均采用了全网共识的

方式来保障每笔交易信息的准确性：即为对某个状态形成共识，所有的节点都必须运行同样的程序。比特币网络每秒只能处理 7 笔交易，2017 年 12 月，热门应用加密猫（CryptoKitties）一经出现便造成以太坊网络的极度拥堵，也同时使得交易费大大增加。这些现象都将矛头指向了现有区块链网络中的全网共识问题。

互操作性

如今的区块链，如比特币、以太坊等，都是由完整节点组成的强信任机器。这些节点验证各自链上的交易，但是对链外一无所知。

由于每个链都是独立的、垂直的封闭体系，这些区块链逐渐变成孤岛，使得他们越来越像当今的“内联网”。

宝岛链

宝岛链基础介绍

宝岛链是中华区块链团队打造的一条在公网（开放式互联网）上运行的联盟许可链（有一定的准入门槛）。同时，通过整合分布式多维实体认证体系及各类不同区块链体系，纳入多源身份认证和多源信息交换协议，实现分布式 P2P 的信任体系，从而让基于信任的价值在不同的区块链系统中自由流通。通过在宝岛链上开发应用，不仅可以利用区块链的技术特性，还可以获得各行业多维度大数据的支持，做出非常落地于民生的有价值应用，从而形成一个**非常自由、相互信任的虚拟现实生态网络。**

宝岛链架构

宝岛链技术架构如下图所示：

BDC – 宝岛链的代币

在宝岛链上 BDC 的发行总量是 6000 万，BDC 的最小单位是小数点后八位小数，类似于比特币的设计。BDC 可以在宝岛链上转移和交易，安全性由椭圆曲线数字签名算法保障（ECDSA）。

BDC 将被用来衡量宝岛链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，当使用宝岛链系统的过程中需要收费的时候，将是以 BDC 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。

BDC 的分发机制

宝岛链将通过早期投资者(Pre-Sale)进行分发并回收，计划于 2018.4.8 分发总量 1200 万(20%) -（每轮 10 天）：

- A 轮 300
- B 轮 400
- C 轮 500

注：3 轮分发完毕将于 6 天内统一按 A 轮双倍价格进行回收，持有者统一注册宝岛链生态网络的数字身份，拥有对应的算力，算力可以进行数据挖矿，从而获得数字资产的奖励，算力越高，奖励也越多。

- ✓ 开发团队 300 万(5%)
- ✓ DPoS 产出 4200(70%)作为数据挖矿的奖励。
- ✓ Pool 产出 300 万(5%)将作为参与宝岛链生态网络的奖励免费分发

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。 在宝岛链中，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，宝岛链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，宝岛链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，同时在宝岛链区块链上，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，宝岛链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 可以在宝岛链上提供这样的服务。

技术部分

宝岛链的共识机制

宝岛链使用 DPoS 和 POOL 来实现区块链记账和数据交换的共识机制。

DPoS(Delegated Proof of Stake)机制，源自于 Graphene，中文名叫做股份授权证明机制（又称受托人机制），它的原理是让每一个持有代币的人进行投票，由此产生 101 位代表 ，我们可以将其理解为 101 个(可无限扩展)超级节点或者矿池，而这 101 个超级节点彼此的权利是完全相等的。从某种角度来看，DPOS 有点像是议会制度或人民代表大会制度。如果代表不能履行他们的职责（当轮到他们时，没能生成区块），他们会被除名，网络会选出新的超级节点来取代他们。

POOL 验证池机制，基于传统的分布式一致性技术，加上数据验证机制。优点：不需要代币也可以工作，在成熟的分布式一致性算法（Pasox、Raft）基础上，实现秒级共识验证。

为什么选择 DPoS 共识机制

现有区块链项目的主要共识机制为 PoW 和 PoS，少部分项目采用修改后的 BFT（拜占庭容错）的共识机制，BTC 就是 PoW 机制下最成功的加密货币。PoW 机制虽然已经成功证明了其长期稳定和相对公平，但在现有框架下，采用 PoW 的“挖矿”形式，将消耗大量的能源。其消耗的能源只是不停的去做 SHA256 的运算来保证工作量公平，并没有其他的存在意义。而目前 BTC 所能达到的交易效率为约 5TPS（5 笔/秒），以太坊目前受到单区块 GAS 总额的上限，所能达到的交易频率大约是 25TPS，与平均千次每秒、峰值能达到万次每秒处理效率的 VISA 和 MASTERCARD 相差甚远。

PoS 机制下较为成熟的数字货币是 Peercoin（点点币）和 NXT（未来币），相比于 PoW，PoS 机制节省了能源，引入了“币天”这个概念来参与随机运算。PoS 机制能够让更多的持币人参与到记账这个工作中去，而不需要额外购买设备（矿机、显卡等）。每个单位代币的运算能力与其持有的时间长成正相关，即持有人持有的代币数量越多、时间越长，其所能签署、生产下一个区块的概率越大。一旦其签署了下一个区块，持币人持有的币天即清零，重新进入新的循环。在 PoS 机制下，因为区块的签署人由随机产生，则一些持币人会长期、大额持有代币以获得更大概率地产生区块，尽可能多的去清零他的“币天”。因此整个网络中的流通代币会减少，从而不利于代币在链上的流通，价格也更易受到波动。由于可能会存在少量大户持有整个网络中大多数代币的情况，整个网络有可能会随着运行时间的增长而越来越趋向于中心化。相对于 PoW 而言，PoS 机制下作恶的成本很低，因此对于分叉或是双重支付的攻击，需要更多的机制来保证共识。稳定情况下，每秒大约能产生 12 笔交易，但因为网络延迟及共识问题，需要约 60 秒才能完整广播共识区块。长期来看，生成区块（即清零“币天”）的速度远低于网络传播和广播的速度，因此在 PoS 机制下需要对生成区块进行“限速”，来保证主网的稳定运行。

为了让处理效率能有质的突破，DPoS 机制应声而出。DPoS 机制要求在产生下一个区块之前，必须验证上一个区块已经被受信任节点所签署。相比于 PoS 的“全民挖矿”，DPoS 则是利用类似“代表大会”的制度来直接选取可信任节点，由这些可信任节点（即见证人）来代替其他持币人行使权力，见证人节点要求长期在线，从而解决了因为 PoS 签署区块人不是经常在线而可能导致的产块延误等一系列问题。DPoS 机制通常能达到万次每秒的交易速度，在网络延迟低的情况下可以达到十万秒级别，非常适合企业级的应用。因为公信宝数据交易所对于数据交易频率要求高，更要求长期稳定性，因此 DPoS 是非常不错的选择。

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。宝岛链与此不同，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。

路线图

对于宝岛链的整个发展而言，是一个短期建设与长期完善相混合的发展过程，并随着区块链和智能合约技术的成熟与普及，逐步完善下述战略步骤。此处战略规划只描述关键性节点，而不涉及详细的开发计划：

团队简介

Matthew Charles

BDC 联合创始人
IBM 公司 商业策划。
获得美国德克萨斯州大学奥斯汀分校硕士学位。

Kevin John

20 余年 web 开发、线上市场推广及商务解决方案的工作经验，获得美国宾夕法尼亚大学商业硕士学位。

陈旭博士
BDC 团队专家
1999 年获得美国南卡罗来纳大学数学博士，随后担任美国 Summus Inc 的研究科学家，主要为美国国防研究部门，如 ONR、Sandia National Labs 等开发图像处理和模式识别方面的算法及软件。

田毅
BDC 架构师
数据库专家，《SQL Server 数据库技术大全》作者，长期从事数据库应用、数据仓库、大数据和区块链应用开发和研究。拥有 Fabric 开发经验

项目风险与优势

政策性风险

目前虽然多数政府对区块链相关产业态度明朗并持积极鼓励政策，但公有区块链天生的去中心化属性在与现有的中心化政府的法律法规下依然面临政府政策层面的很多不缺定性。

针对政策性风险宝岛链团队将会采取如下措施：

- 在团队单独设立公共关系部门，积极与政府以及业内从业人员保持沟通协作，在法律框架下设计数字资产发行／交易／区块链金融／区块链应用等方面业务。
- 宝岛链项目运营不涉及法定货币交易，但并不干涉第三方交易所开展宝岛链兑法币交易业务，宝岛链团队只专注技术。

市场风险

宝岛链的终极目标是要实现价值在区块链系统中的去中心化自由流动，然而区块链产业刚刚兴起，项目的未来会面临各种各样的市场考验。

针对市场风险运营团队采取的应对方式为：

- 宝岛链运营团队将定期的参与业内会议，并定期或不定期举行项目进展与发布会，与相关开发者沟通与交流目前的市场需求与前景预测，确保项目能够回应社区与市场的声音。

结论

与比特股和以太坊相似的，宝岛链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。宝岛链通过对数字资产、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。 在宝岛链中，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，宝岛链天生继承了其不可篡改的账本，以及不可双花的优点，宝岛链将在数字资产和可数字化资产的海洋徜徉，为宗旨实现链上信任生态，应用于各级应用场景中。从而实现整个生态的成功构建.

参考文献

1. Bitcoin Whitepaper ——Satoshi Nakamoto http://bitcoin.org/bitcoin.pdf
2. Namecoin: https://namecoin.org/
3.Bitshareswhitepaper——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