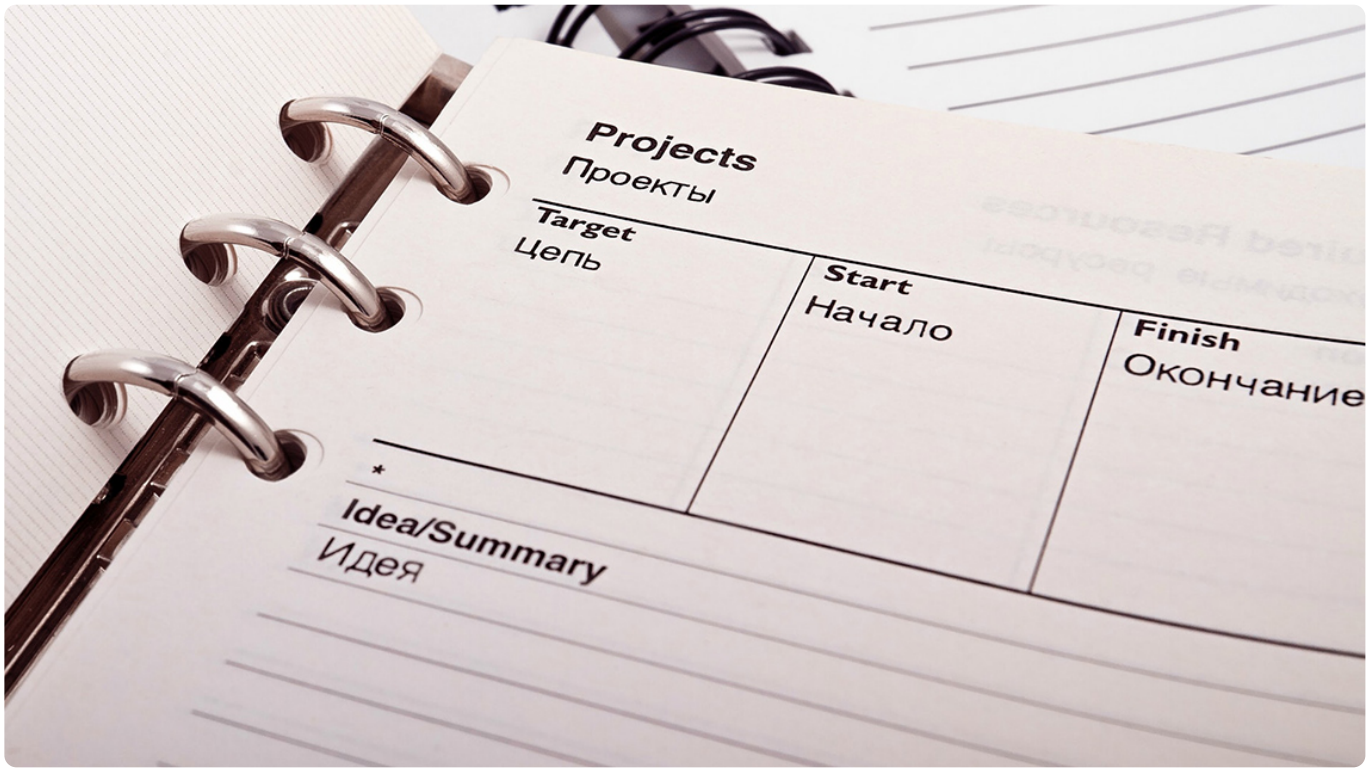
第22讲 | 国内区块链项目技术一览

2018-05-14 陈浩

深入浅出区块链

进入课程 >



讲述：黄洲君

时长 11:55　大小 5.46M

区块链的深入技术篇写到了现在，我们已经一起看过了很多国外区块链项目的技术逻辑。实际上，国内的优质区块链项目其实也不少，并且势头很足，不容小觑。

我在前面的文章中介绍过国内的几个区块链项目，不过仅从发展的角度做了一个简要概述，并没有进行深入探讨，今天我们就重点来看一看这些项目的设计思路与技术特点。

小蚁 NEO

1. 简介

我们以前讲到过，NEO 的前身是小蚁，小蚁最早在 2015 年发起，它在 2017 年□中正式更名为 NEO。

NEO 项目一共经历过两次 ICO，第一次 ICO 是项目创立，第二次 ICO 是项目更名后的品牌升级。可以说通过 NEO 项目的起起落落□见证了整个国内区块链项目的发展。

在重做了市值管理和社区建设后，NEO 成为了市值 TOP10 区块链项目之一。

2. 设计思路

NEO 是一个开放式智能经济平台，它提供了数字身份、数字资产、智能合约三种核心元素用来支持 NEO 智能经济生态。

数字资产：数字资产是以电子数据的形式存在的可编程控制的资产，NEO 在底层也直接支持类似 ERC20 的 Token 机制，所以用户可以在 NEO 上自行注册登记资产、交易和流转。□它也通过数字身份解决与实体资产的映射关系，用户通过正规的数字身份所注册登记的资产受到法律的保护。

数字身份：数字身份是指以电子数据形式存在的个人、组织、事物的身份信息，NEO 将实现一套兼容 X.509 的数字身份标准以及支持 Web Of Trust 式的点对点的证书签发模式。

智能合约：NEO 上的智能合约与以太坊不同，叫做 NeoContract。这套智能合约体系的最大特点是直接支持 C#、Java 等主流编程语言，所以开发者可以在熟悉的 IDE 环境（Visual Studio、Eclipse 等）中进行智能合约的开发、调试、编译。

NEO 的通用轻量级虚拟机 Neo VM 具有高确定性、高并发性、高扩展性等优点。

3. 技术特点

NEO 采用了 PBFT 类的共识算法。NEO 的修改版为 dBFT 共识算法，这里 d 为 Delegated，就是代理人的意思。所有的 PBFT 类算法都有个特性，就是通信复杂度是节点数量的平方次，例如 7 个节点出一次块至少通信 72 次，对网络带宽要求很高。所以记账节点一般不会很多，它带来的优势就是 TPS 较高，并且不会分叉。

自成一派的智能合约体系。这里降低了智能合约开发者的局限性，不必使用 Solidity 语言开发。

C# 技术生态。NEO 的主要实现都是 C# 语言编写的，得益于.Net Core 的开源，NEO 的技术生态也在一直扩张。

Token 体系。提供了等价于以太坊 ERC20 的 NEP-5 Token 体系。

元界 Metaverse

1. 简介

元界是我所主导的一个开源区块链项目，项目于 2016 年 8 月发起，经过了 5 个月开发和测试，于 2017 年 2 月份上线。

元界是一个关注社会和商业需求的区块链项目，目标是构建以数字资产（Metavase Smart Token）和数字身份 (Avatar) 为基础新型区块链生态，这种生态会为人类社会带来深刻的变革。

除了数字资产和数字身份两个概念，我们还提出了 BISC 内置智能合约和 BaaS 区块链即服务的概念，并把数字身份作了延伸，提出了 Oracle 价值中介（此 Oracle 非彼 Oracle）。

总体思路是总结人与人、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）内置智能合约，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，这一切都是围绕资产和人来展开的。

数字资产 MST 可以让□人们□获得区块链带来的点对点操作资产的优势，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系统，资产交易可以为 MST 解决基础的流动性需求。

人们将区块链作为基础服务植入 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。

2. 技术特点

延续并扩展了 UTXO 模型，一切皆 UTXO 为资产和身份带来了良好的安全性。

内置 BISC，没有为用户提供自己编写智能合约的功能，提高了安全性，降低了多样性□。

PoW 挖矿，与以太坊的 PoW 挖矿算法兼容。

内置了数字身份，提供了基于数字身份的域名系统，可以连接到数字资产上。

默认提供 HD 类型的主私钥账户体系。

□块上限是 1MB，但出块速度是 33 秒，所以 TPS 大约是比特币的 18 倍。

提供等价于 ERC20 的 MST Token 体系。

量子链 QTUM

1. 简介

量子链致力于开发比特币和以太坊之外的新型区块链生态，它的目标是通过自行设计，让比特币和以太坊完美地融合在一起，并通过智能合约为人们提供 Dapp 平台。

除此之外，量子链还提出了移动端 Dapp 策略，通过引入身份机制和 Data-feed 链外数据达到合规性要求，最终通过推动 Dapp 的普及，让传统互联网企业可以将量子链作为一个新的应用平台进行尝试。

量子链关注利用区块链技术进行价值传输，首次提出了 VTP——Value Transfering Protocal，价值传输协议的概念。这里的价值传输协议是对标 HTTP、SMTP、POP3、SSH 等协议的。

量子链认为，在比特币之前人们一直无法在不借助第三方的情况下进行较好的点对点价值转移，比特币是运行在互联网上的一个 VTP 协议，随着区块链技术的发展，人与人、人与信息的交互更加多样化，未来会有更多的实体会被数字化（Tokenization）。

这里所说的就是资产登记，被登记完之后，肯定还会面临价值流转的问题。量子链从技术出发，提供了第一个结合比特币 UTXO 和以太坊 EVM 的区块链技术生态区来解决上述问题。

2. 技术特点

基础代币 QTM 与比特币脚本高度兼容，兼具 UTXO 和账户模型的优点。

与以太坊智能合约体系高度兼容的技术栈。

共识算法使用了 PoS3.0 算法，属于经典 PoS 算法。

提出了主控智能合约和普通智能合约的概念，通过主控合约可以引入链外数据 Data-feed。

通过主控合约可以提供合规性需求。

提供了等价于以太坊 ERC20 的 QRC20 Token 体系。

比原链 Bytom

1. 简介

比原链是一种多元的资产交互协议。简单来理解也是做数字资产的，不过换了种说法，理念稍不同。比原链认为在区块链上存在两种不同形态资产。

比特资产：是指区块链上原生的数字货币、数字资产，例如比特币、以太币；

原子资产：对应到现实世界的资产，例如权证、权益、股息、债券、情报资讯、预测信息等。

人们可以通过比原链进行对上述两种资产进行登记、交换、对赌、甚至基于合约的更具复杂性的交互操作。目的是连通原子世界与比特世界，促进资产在两个世界间的交互和流转。

比原链采用三层架构。

1. 应用层对移动终端等多终端友好，方便开发者便捷开发出资产管理应用；
2. 合约层采用创世合约和控制合约进行资产的发行和管理，在底层支持扩展的 UTXO 模型 BUTXO， 对虚拟机做了优化，采用自省机制以防止图灵完备中的死状态；
3. 数据层使用分布式账本技术，实现资产的发行、花费、交换等操作。

2. 技术特点

共识算法是 PoW，属于忠实的比特币 PoW 党。

挖矿算法采用对人工智能 ASIC 芯片友好型算法，在哈希过程中引入矩阵和卷积计算，使得矿机在闲置或被淘汰后，可用于 AI 硬件加速服务，从而产生额外的社会效益。

兼容比特币 UTXO 模型。

默认提供了基于 HD 的主私钥账户体系。

加密模块提供了基于国密 SM2、SM3 标准算法。

植入了隔离见证设计。

本体网络 Ontology Network

1. 简介

本体网络是原 NEO 项目组成员李俊创立的，不过与 NEO 是完全独立的项目，随着技术大咖季宙栋的加入，市值跃入 TOP20。

本体网络是一个主打构建分布式信任体系的区块链项目，支持多链、多系统融合的协议网络，不同的链和不同的系统都可以通过本体的信任协议进行协作。

本体包含独立的分布式账本、P2P 网络协议、模块化的共识协议组，模块化的智能合约机制几个主要模块。

本体的产品形式是 ONTO，ONTO 是基于本体的综合客户端产品、区块链搜索引擎和区块链体系的入口。

ONTO 将帮助用户实现包括数字身份管理、数字资产管理、分布式数据交换等综合性功能，ONTO 可以将数字身份与现实身份进行映射关联，用户可以利用这款产品建立自己的数字身份和多维的身份画像，通过密码学算法实现隐私保护。

本体主要提供了以下三种协议。

1. 提供分布式身份管理框架 （ONT ID），一个基于 W3C 的 DID 规范构建的去中心化的身份标识协议。
2. 提供分布式数据交易协议 （ONT DATA），用于构建去中心化数据交易应用框架。
3. 提供了信用评分协议（ONT Scores)，支持建立开发不同的声誉评价逻辑，提供评级授权与审计功能。

支撑这些协议的是 ONT 公链，以及 ONT 区块链高性能可定制化框架。

2. 技术特点

基于账户模型，并保留 UTXO 模型。

共识算法采用 VBFT，它是结合 PoS、VRF(Verifiable Random Function) 和 BFT 的全新共识算法。

模块化的智能合约，提供 WASM 和 NEO VM 两种。

通过 FPGA 加速计算密集型的业务模块。

多层跨链的结构设计。

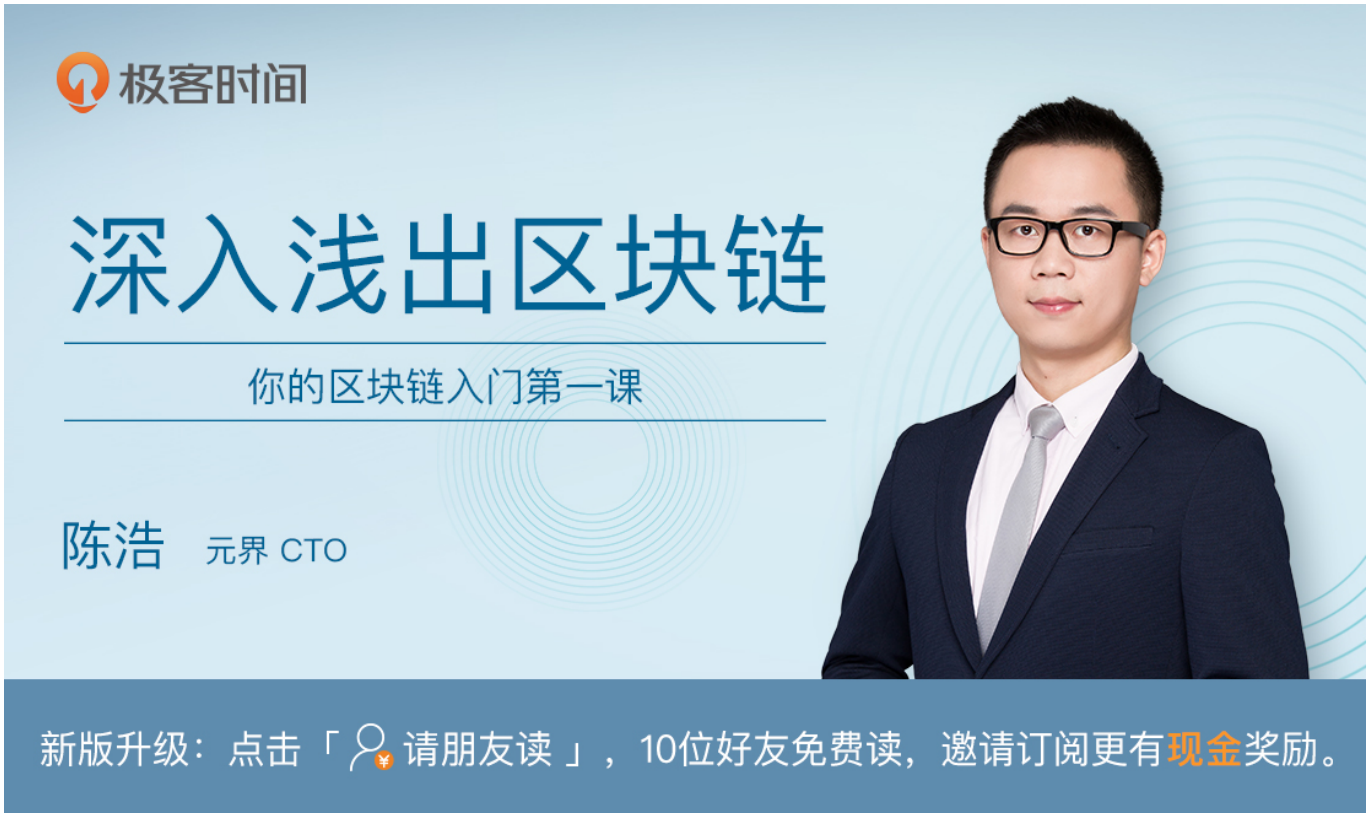
提供链上搜索引擎。

总结

今天带你了解了一些从国内发起的比较知名的区块链项目，其实还有不少区块链项目，例如公信宝、YoYow 等，今天就介绍到这里，你可以进入这些项目的社区寻求更详细的资料。

好了，今天的问题是，你觉得做公链最大的挑战是什么？你可以给我留言，我们一起讨论。

参考引用： https://info.ont.io/view-point/V0019/zh



© 版权归极客邦科技所有，未经许可不得传播售卖。 页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

上一篇 第21讲 | 引人瞩目的区块链项目：EOS、IOTA、Cardano

下一篇 第23讲 | 联盟链和它的困境

精选留言 (11)

写留言

Hansen
2018-05-14

5

最大的挑战应该是安全性问题吧，具体业务场景跟业务逻辑的多样性决定了安全性；还有就是普通民众对待各项目的看法，虽然现在有很多针对性很强的技术项目，但还是感觉总体拉力不够，这个东西的未来发展，在国内来说，还是取决于政府的政策跟态度。

作者回复: 感谢分享。赞同安全性的观点，安全也分用户端安全和主网安全，用户端主要是钱包，交易所资产托管的地方，主网安全主要是怕被攻击。

阿痕
2018-05-25

2

我觉得当前公有链最大的问题除了安全外，应该是使用场景有限，很难有实际落地的应用。

作者回复: 观点一致。技术上还有可扩展性和tps

悟空来 |...
2018-05-26

1

公链的三大件数字身份，数字资产，智能合约。其实映生产资料，价值，生产关系。通过生产关系进行生产资料的重组与搭配，创造价值。

作者回复: 有道理~

Peter zh...
2018-05-14

1

不管是哪一个公链、能落地应用 并且能经得起并发的挑战 应该算是 离成功近了一步吧.

作者回复: 并不是哦，还要有强大的社区共识。

吹牛老爹
2018-06-28

pbft中的节点如何防止参与pbft共识的节点列表被暴露，然后所有的节点被攻击，毕竟节点少嘛

jaryoung
2018-06-06

作者知道了解布比区块链不?

展开

作者回复: 你好，了解一点点，也是联盟链业务为主

vincent
2018-05-24

技术壁垒吧，还有生态的设计

展开

作者回复: 对，生态发展很重要，具有马太效应。

Sean
2018-05-22

陈老师看过xdag吗

展开

有风的林子
2018-05-16

公链最重要的，是作为基础设施存在。开放可协作和自由，最好逻辑简单。

展开

作者回复: 赞同。

陈南平

2018-05-15

陈老师，我想问一下，如果要做区块链架构师，您认为最少需要知道什么？或者说做什么？

作者回复: 你好，金融和技术都需要了解哦

青梅煮酒

2018-05-14

老师您好，我想请教一个以太坊和约部署问题，我一次写了多个合约，怎么部署了，我只会一个合约的部署方式

作者回复: 你说的是批量部署合约吗?