第24课：公有链...

大家好，我是丹华。本节是区块链全景课第三篇——应用篇的第一课，主要介绍目前关注度较高的11个公有链项目。

包括：

- 比特币
- 以太坊
- 比特现金
- 莱特币
- 瑞波币
- EOS
- NEO
- ZCash
- IOTA
- IPFS
- Bancor

1.比特币

比特币（BitCoin，简称 BTC）的概念最初由匿名人士中本聪在2009年提出，是成立最早、市值最大、影响最大的数字货币。它由一个开源软件、内生代币比特币、区块链结构、以及一个 P2P 网络组成，实现了一个去中心化的支付系统。

比特币不依靠特定货币机构发行，它依据特定算法，通过大量的计算产生，众多节点通过共识机制来确认并记录所有的交易，使用密码学确保安全性。比特币总数量非常有限，2100万枚，具有极强的稀缺性。更多介绍见第2课：比特币。

相关资源一览

比特币官网 bitcoin.org/
比特币白皮书英文
https://bitcoin.org/bitcoin.pdf
白皮书中文 satoshinakamoto.me/zh-cn/bitcoin.pdf
Bitcoin Core 网站 bitcoincore.org
Github 主页
https://github.com/bitcoin/bitcoin
Bitcoin wiki
https://en.wikipedia.org/wiki/Bitcoin
浏览器 https://blockchain.info/
资讯、统计、浏览器、钱包 btc.com
区块网浏览器 qukuai.com/search/
比特币 BBS bitcointalk.org/
比特币 reddit 主页 reddit.com/r/Bitcoin/
书籍：Mastering Bitcoin: Programming the Open Blockchain（2ed） Jul 1, 2017，by Andreas M. Antonopoulos
比特币期货 http://cfe.cboe.com/cfe-products/xbt-cboe-bitcoin-futures
比特币期货2 https://www.cmegroup.com/trading/bitcoin-futures.html
闪电网络官网 https://lightning.network
闪电网络白皮书https://lightning.network/lightning-network-paper.pdf

2.以太坊

以太坊（Ethereum）是一个开源的有智能合约功能的公有区块链平台，一个支持去中心化应用的通用的世界计算机。通过内生数字货币以太币（Ether，简称 ETH，或以太币）提供去中心化的虚拟机（Ethereum Virtual Machine，EVM）来处理点对点合约。目前，以太币是市值第二高的数字货币，市值仅次于比特币。更多介绍见第3课：以太坊。

相关资源一览

以太坊官 https://www.ethereum.org/
区块链浏览器 https://etherscan.io/
以太坊中文论坛 https://ethfans.org/
以太坊 wiki 主页https://en.wikipedia.org/wiki/Ethereum
Github 主页
https://github.com/ethereum
以太坊白皮书
https://github.com/ethereum/wiki/wiki/White-Paper
以太坊黄皮书
https://ethereum.github.io/yellowpaper/paper.pdf
以太坊 Reddit 主页https://www.reddit.com/r/ethereum/
创始人 Vitalik Butterin 个人网站https://vitalik.ca/
联合创始人 Gavin Wood 个人网站http://gavwood.com/
以太坊书籍：Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners by Chris Dannen，Mar 18, 2017

3.比特现金

比特现金是比特币的分叉币 Bitcoin Cash（简称 BCH），其客户端软件 Bitcoin abc 是对 Bitcoin core 0.14 在区块高度#478559进行硬分叉（Hard Fork）得来的版本，将区块大小调整到了 8M，并且移除了隔离见证（SegWit）。2018年8月1号 UTC 时间12:37，比特币区块高度478558正式开始分叉，BCH 由此而来，可将其视作比特币（BTC）的分叉币或竞争币。Bitcoin cash 不存在一个"官方"的参考实现（reference implementation），而是有多个版本都支持比特现金，如 Bitcoin ABC，Bitcoin Unlimited 等。

另外，由于比特现金和比特币的"近亲"关系，两者在技术上极为相似，因此大多数支持 Bitcoin 的应用（如交易所、钱包、浏览器等），也都支持 Bitcoin Cash。

相关资源一览

比特现金官网 bitcoincash.org/
比特现金 Wiki 页面
https://en.wikipedia.org/wiki/Bitcoin_Cash
比特现金 Github 页面
https://github.com/zquestz/bitcoincash
Bitcoin ABC 的 Github 页面
https://github.com/Bitcoin-ABC/bitcoin-abc

4.莱特币

莱特币（Litecoin，简称 LTC）是最成功的模仿比特币的山寨币，创始人为李启威（Charlie Lee），基本技术、架构和发行机制都与比特币非常相似，工作量证明使用 scrypt 加密算法。莱特币发行总量为8400万枚，每2.5分钟产生一个区块（因此交易确认更快），区块奖励每四年减半。因此社区有“比特是金，莱特是银”的说法。

相关资源一览

莱特币官网 https://www.litecoin.com/
莱特币 wiki：https://en.wikipedia.org/wiki/Litecoin
莱特币 Github 主页
https://github.com/litecoin-project/litecoin
莱特币 reddit 主页 https://www.reddit.com/r/litecoin/
莱特币浏览器：http://www.qukuai.com/search/ltc
莱特币中国社区：http://www.ltchome.cn

5.Ripple

瑞波币是 Ripple 网络的基础货币，简称为 XRP，总数量为1000亿，它可以在整个 Ripple 网络中流通，并且随着交易的增多而逐渐减少。瑞波币的运营公司为 Ripple Labs。Ripple 网络的基本功能是实现了基于网关的任意货币跨境转账，其愿景是成为世界范围内各大银行通用的标准交易协议，使货币转账像发电子邮件那样成本低廉、方便快捷。

瑞波（Ripple）系统的转账模式有两种：一种是以网关或瑞波币 XRP 为桥梁，用户甲将任意类别的货币或虚拟货币兑换为瑞波币 XRP，然后发送给其它任何地区的用户乙，用户乙可将收到的资金兑换成自己需要的任意货币币种；还有另一种模式，用户甲将在资金存放在乙信任的网关，经过网关转给乙。

相关资源一览

Ripple 官网 https://ripple.com/
Ripple wiki
https://en.wikipedia.org/wiki/Ripple(*payment*protocol)
Ripple 的 reddit 主页https://www.reddit.com/r/Ripple
Ripple 的 Github 主页
https://github.com/ripple

6.EOS

全称为 Enterprise Operation System，简称 EOS，2017年兴起的新兴项目，愿景是成为商用分布式应用（Dapp）设计的一款区块链操作系统。EOS 是一种新的区块链架构，旨在实现分布式应用的性能扩展，以支撑工业级的 Dapp 开发，号称将免除交易费用，实现百万级的 TPS（transactions per second）。此点主要针对以太坊的高交易费用和缓慢的交易处理速度，使得 EOS 成为以太坊的一个潜在竞争对手。EOS 采用 DPOS（delegated Proof-of-stake）共识机制，出块时间0.5秒，目前流通量8.9亿枚。核心程序由 C++ 写成。其背后是一家公司 Block.one，CEO 是 Brendan Blumer，CTO 是 Dan Larimer，即所谓 BM。

相关资源一览

EOS 官网 https://www.eos.io
EOS 在 Github 的主页 https://github.com/EOSIO
EOS 网络浏览器 http://eosnetworkmonitor.io/
EOS 的 wiki 主页https://en.wikipedia.org/wiki/EOS.IO
项目方主页 https://block.one/
EOS 白皮书
https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md

7.NEO

国内最知名的公有链项目，NEO 是一个非盈利的社区化的区块链项目，愿景是利用区块链技术和数字身份进行资产数字化，利用智能合约对数字资产进行自动化管理，实现“智能经济”的一种分布式网络。NEO 于2014年正式立项，2015年6月在 Github 上实时开源，共识机制是 DBFT。

NEO 的生态中包含三个元素，数字资产、数字身份和智能合约。

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。用区块链技术实现资产数字化有去中心、去中介、免信任、可追溯、高度透明等特点。NEO 在底层支持多数字资产，用户可在 NEO 上自行注册登记资产，自由交易和流转，并且通过数字身份解决与实体资产的映射关系。用户通过合规的数字身份所注册登记的资产受到法律的保护。NEO 中有两种形式的数字资产：全局资产和合约资产。全局资产能够被记录在系统空间，可以被所有智能合约和客户端所识别；合约资产被记录在智能合约的私有存储区中，需要兼容该智能合约的客户端才能识别。合约资产可以参照某种约定的标准，从而实现与多数客户端的兼容。

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。目前较为成熟的数字身份体系是基于 PKI（Public Key Infrastructure）的 X.509 标准。在 NEO 中，将实现一套兼容 X.509 的数字身份标准。这套数字身份标准，除了兼容 X.509 的层级式的证书签发模式，还将支持 Web Of Trust 式的点对点的证书签发模式。并通过人脸、指纹、语音、短信等多因素认证实现签发阶段和使用阶段的真实身份比对。同时，还将使用区块链取代 OCSP 协议来管理、记录 X.509 的吊销证书列表 CRL。

智能合约

NEO 具备独立的智能合约体系：NeoContract。其最大特点是无缝对接现有的开发者生态。开发者无需学习新的编程语言，就能用 C#、Java 等主流编程语言在熟悉的 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 NeoVM 具有高确定性、高并发性、高扩展性等优点。NeoContract 智能合约体系让全球百万级的开发者能够快速进行智能合约的开发。

相关资源一览

NEO 官网 https://neo.org/
NEO 在 Github 主页
https://github.com/neo-project
NEO 白皮书 http://docs.neo.org/zh-cn/index.html

8.ZCash

Zcash（简称 ZEC），前身是 Zerocoin 项目， 采用 POW（Proof of Work）共识机制，创世块诞生于2016年10月28日。Zcash 总量为2100万枚，2.5min一个块，前20000个块奖励线性递增，之后每四年减半，前四年区块奖励20%归零币公司。采用了 zk-SNARK 零知识证明技术，工作量证明算法采用 Equihash。与比特币相比，Zcash 的最大特点就是匿名性，可以实现绝对的匿名。交易可自动隐藏区块链交易双方及金额，仅仅持有密钥者可看到具体交易信息。
Zcash 交易的元数据是加密的，而不是公开地展示交易参与方和交易数额当然，用户可自行选择哪些人拥有该权限。该技术允许网络在不公开交易参与方或者交易数额的情况下维护一个安全的账户余额账本。

相关资源一览

Zcash 官网 https://z.cash/
Zcash 在 Github 的主页
https://github.com/zcash/zcash
技术与白皮书
https://z.cash/technology/index.html

9.IOTA

IOTA 是为物联网（IoT）而设计的一个革命性的新型交易结算和数据转移层。它基于新型的分布式账本——Tangle（缠结）。Tangle 能够克服现有区块链设计中的低效性，并为去中心化 P2P 系统共识的达成创造了一种新方法。愿景：通过真相验证和交易结算来激励设备，将所有设备连接起来，以实时使用其数据和属性。这将诞生全新的通用的应用和价值链。

通过 IOTA 进行转账不需要支付手续费，这是首例。这也就意味着，无论是多小额的支付都能通过 IOTA 完成。目前 IOTA 可以很好的做两件事：交易结算（尤其是微支付）和数据完整性。随着 Tangle 的不断发展，越来越多的参与者都将发起交易，确认时间会缩短，整个系统也会变得越来越安全和快速。

相关资源一览

IOTA 官网 https://www.iota.org/
白皮书与研究https://www.iota.org/research/academic-papers
IOTA 在 Github 的主页https://github.com/IOTAledger
Tangle 浏览器 https://thetangle.org/
另一浏览器 https://iotasear.ch/

10.IPFS

星际文件存储系统（InterPlanetary File System，IPFS）是一个去中心化的文件共享系统。IPFS 使用，分布式哈希表和 Merkle 有向无环图数据结构，将文件分割称很多小块来实现 P2P 的存储，拥有一个类似 Git 的文件版本管理系统。其内部货币是文档币（Filecoin），网络中的节点通过出租自己的磁盘空间、存储加密文档而赚取文档币，用户存储/检索文件时，需要花费文档币。IPFS 和文档币使用区块链数据结构和数据可检索证明（Proof of Retrievability，POR）共识协议。

相关资源一览

官网 https://ipfs.io/
Wiki 主页
https://en.wikipedia.org/wiki/InterPlanetary*File*System

11.Bancor

一个分层货币系统和去中心化交易所，建立在以太坊区块链上，内生代币 BNT（Bancor Network Token），为体系内的任何代币提供连续的、链上的流动性，任意兑换，没有对手方，自动计算价格。

相关资源一览

官网 https://www.bancor.network/
白皮书https://storage.googleapis.com/website-bancor/2018/04/01ba8253-bancor*protocol*whitepaper_en.pdf

下一节，我们将介绍主要的联盟链项目。