以太坊学习：第一天

目录

介绍：以太坊Ethereum。

区块链目前可以分为四类：公链，私链，联盟链以及侧链。

公链

- 公链是指任何人都可读取的、任何人都能发送交易且交易能获得有效确认的、任何人都能参与其中共识过程的区块链。

  公链采取了采取工作量证明机制（POW）、权益证明机制(POS)、股份授权证明机制（DPOS）等方式，并将经济奖励和加密数字验证结合了起一个原则就是每个人从中可获得的经济奖励与工作量成正比。这些区块链通常被认为是完全去中心化的。

- **特性**:

  1. 开源

  由于整个系统的运作规则公开透明，这个系统是开源系统；

  2. 保护用户免受开发者的影响

  在公有链中程序开发者无权干涉用户，所以区块链可以保护使用他们开发的程序的用户；

  3.访问门槛低

  任何拥有足够技术能力的人都可以访问，也就是说，只要有一台能够联网的计算机就能够满足访问的条件；

  4.所有数据默认公开

  尽管所有关联的参与者都隐藏自己的真实身份，这种现象十分的普遍。他们通过他们的公共性来产生自己的安全性，在这里每个参与者可以看到余额和其所有的交易活动。

  案例：公有链中有许多我们熟悉的身影：BTC, ETH, EOS, AE, ADA等

私链——权利掌握在少数人手里

- 私链是指其写入权限仅在一个组织手里的区块链。读取权限或者对外开放，或者被任意程度地进行了限制。相关的应用囊括数据库管理、审计、司，尽管在有些情况下希望它能有公共的可审计性，但在很多的情形下，公共的可读性并非是必须的。
- **特性:**

  1. 交易速度快：

  一个私链的交易速度可以比任何其他的区块
度，并不需要每个节点来验证一个交易。

2. 隐私性好：

给隐私更好的保障私有链使得在那个区块链上的数据隐私政策像在另一个数据库中似的完全一致;不用处理访问权限和使用所有的老办法，但至数据不会公开地被拥有网络连接的任何人获得。

3.交易成本低：

交易成本大幅降低甚至为零私有链上可以进行完全免费或者至少说是非常廉价的交易。如果一个实体机构控制和处理所有的交易，那么他们就不工作而收取费用。

案例：Linux基金会、R3CEV Corda平台以及Gem Health网络的超级账本项目（Hyperledger project）或在开发或在使用私链。

联盟链——部分去中心化

- 联盟链开放程度和去中心化程度是有所限制的。其参与者是被提前筛选出来或者直接指定的，数据库的读取权限可能是公开的，也可能像写入权于系统的参与者。
- **特性：**

1. 交易成本低

交易只需被几个受信的高算力节点验证就可以了，而无需全网确认；

2. 节点容易连接

若是出了问题，联盟链可以迅速通过人工干预来修复，并允许使用共识算法减少区块时间，从而更快完成交易；

3.灵活

如果需要的话，运行私有区块链的共同体或公司可以很容易地修改该区块链的规则，还原交易，修改余额等。

案例：瑞波用于日韩国际汇款及日本本国银行间汇款建立了联盟链，同时之前火过一阵子的迅雷链克也是一种半开放的联盟链。

侧链——拓展协议

- 侧链"从严格上来说，其本身并不是区块链，可以理解为区块链的一种扩展协议。早期"侧链"是为了解决比特币区块链技术的限制问题。侧链就像路，将不同的区块链互相连接在一起，以实现区块链的扩展。侧链完全独立于比特币区块链，但是这两个账本之间能够"互相操作"，实现交互。
- **特性：**

1. 独立性

侧链架构的好处是代码和数据独立，不增加主链的负担，避免数据过度膨胀。 侧链有独立的区块链，有独立的受托人或者说见证人，同时也有网络，就是说一个侧链产生的区块只会在所有安装了该侧链的节点之间进行广播。

2.灵活性

侧链所有的区块链参数是可以定制的，简单的比如区块间隔、区块奖励、交易费的去向等，高级用户还可以修改共识算法。

案例：LSK, RDN, ARDR等币种是利用的侧链技术。

参考资料

- 《精通白皮书》：https://github.com/ethereumbook/ethereumbook
- 《以太坊白皮书》:https://github.com/ethereum/wiki/wiki/White-Paper
- 以太坊官方文档：http:/www.ethdocs.org/en/latest/index.html
- Solidity官方文档：https://solidity.readthedocs.io/en/lastest/
- 《以太坊黄皮书》

以太坊的组成部分

- P2P网络：在以太坊网络运行，在TCP端口30303上寻址
- 交易
- 以太坊虚拟机（EVM）：以太坊的状态转换，由虚拟机来处理。可以参考Java的虚拟机模式
- 数据库：Blockchain作为数据库存储每一个节点，包含序列化后的交易和系统状态
- 客户端：以太坊有几种可互操作的客户端软件实现。比如Geth

以太坊中的重要概念

- **账户（account）**：包含地址、余额、随机数，以及可选的存储和代码的对象。普通账户（EOA）：存储和代码均为空；合约账户（Contract）和代码
- **地址（address）**：一般来说，这代表一个EOA或合约，它可以在区块链上接收或者发送交易。具体来说，他是ECDSA（椭圆曲线算法）公钥列的最右边的160位（就是作为地址）。
- **交易**：可以发送以太币和信息；向合约发送的交易可以调用合约代码，并以信息数据作为函数参数；向空用户发送信息，可以自动生成以信息为约用户
- **Gas**：以太坊用于执行智能合约的虚拟燃料（简单理解为手续费）。以太坊虚拟机使用核酸机制来衡量gas的消耗量并且限制计算资源的消耗

以太坊的货币

以太坊的货币单位是以太（ether），也可以表示为ETH。以太币的发型规则如下：

- 挖矿前（Pre-mine,Genesis）：以太坊一开始是一个众筹项目，最初发行了7200万以太币。每年产量基本稳定，被限制不超过7200万的25%。以发行的，不像比特币那样总数量有限制，我认为可能是因为：消耗gas，所以不断需要以太币。
- 挖矿产出（Mining）：区块奖励（block reward），叔块奖励（uncle reward），叔块引用奖励（uncle referencing reward）。所以以太坊所有源：挖矿前7200万+挖矿产出
- 以太坊出块机制从PoW转化为PoS后，以太币的发行会有什么变化尚未知道。PoS将使用一个称为Casper的协议，在这个协议下，以太币的发行大低于幽灵协议（GHOST）写一下的发行率。 如果真的转为PoS，那肯定会有人存币，然后该用户的话语权会越来越大，导致中心化的结果

以太坊的挖矿产出

- 区块奖励（Block rewards）：每产生一个新区块就会有一笔固定的奖励给矿工，一个是5个以太币，现在是3个。以太币大约是十几秒就出一个
- 叔块奖励（Uncle rewards）：有些区块被挖的稍晚一些，没有被确认上链，因此不能作为主区块链的组成部分。比特币这类区块称为“孤块”，并弃他们。但是，以太币称他们为“叔块”，并且在之后的区块中，可以引用他们。如果叔块在之后的区块链中作为叔块被引用，每个叔块回味挖矿奖励的7/8。一个区块可以指定多个叔块，也可以不指定，叔块奖励3*0.825。
- 叔块引用奖励（Uncle referencing rewards）：矿工每引用一个叔块，可以得到区块奖励的1/32作为奖励，最多引用两个叔块。
- 这样的一套基于PoW的奖励机制，被称为以太坊的“幽灵协议”。

以太坊区块收入

普通区块收入：

1. 固定奖励（挖矿奖励），每个普通区块都有
2. 区块内包含的所有程序的gas花费的总和
3. 如果普通区块引用叔块，每引用一个就可以获得固定奖励的1/32

叔块奖励：（叔块高度 + 8 - 引用叔块的区块高度） * 普通区块奖励 / 8。（可以理解为离区块越近，亲缘关系越近，收益越高）

区块链相关网站

https://etherscan.io

“幽灵”（GHOST）协议

个人理解：以太坊出币十几秒，如果A用2秒就算出来，B用4秒算出来。A算出来后就继续算下一块，而B在比如过了6秒后才从广播接收到A算的结果第10秒才开始算下一个块。由此这里，A和B在一个块中就相差了8秒，如果不断累加起来，B可能就永远追不上A，出现一家独大的风险。而在比特币在这个问题：比特币至少用十分钟才出一个块，而确认只需要十几秒，大可忽略不计，所以下一个块各个节点是同一个起跑线，保证了公平性和稳定以太坊存在的风险，以下是用“幽灵协议”来解决这个风险：

- 以太坊出块时间：时间为12秒，实际14~15秒左右。比特币的出块时间是10分钟左右，但是比特币只需要12.6秒的时间就可以把信息广播到全网
- 快速确认会带来区块的高作废率，由此链的安全性也会降低
- “幽灵”协议：Greedy Heaviest Observed SubTree, "GHOST"
  - 计算时间工作量证明时，不仅包括当前区块的祖区块，父区块，还要包括祖先块的作废的后代区块（“叔块”），将他们进行综合考虑。
  - 目前的协议要求下探到第七层（最早的简版设计是五层），也就是说，废区块只能是以叔区块的身份被其父母的第二代至第七代后辈区块引是更远关系的后辈区块。
  - 以太坊给以“叔区块”身份为新块确认作出贡献的废区块7/8的奖励，把它们纳入计算的“侄子区块”将会的区块奖励的1/32，不过，交易费用不区块。

比特币一条主链，而以太坊主链+分叉，看重量。

以太坊与“图灵完备”

以太坊能够在虚拟机中执行存储程序，同时向内存读取和写入数据，使其称为图灵完备系统，因此称为通用图灵机。简单来说，以太坊中支持循环，就可能出现死循环的风险！会消耗掉全部资源！

为了解决上面的问题，以太坊引入gas。执行程序会消耗gas，当gas不足的时候，程序会被强制停止，就解决了死循环的问题。

去中心化应用

Dapp：基于以太坊可以创建智能合约来构建去中心化应用。

以太坊的构想是成为DApps变成开发的平台。

DApp至少有以下组成：区块链上的智能合约，Web前端用户界面。

以太坊应用

- 基于以太坊创建新的加密货币（CryptoCurrency，这种能力是2017年各种ICO泛滥的技术动因）
- 基于以太坊创建域名注册系统、博彩系统、拍卖系统、投票系统
- 基于以太坊开发去中心化的游戏。比如：2017年底以太猫（CryptoKitties，最高一只猫售价80W美元）

代币

- 代币（token）也称作通证，本意为“令牌”，代表有所有权的资产、货币、权限等在区块链上的抽象。可以想象成Q币。
- 可替代性通证（fungible token）：指的是基于区块链技术发行的、可以互相代替的、可以季节无限拆分的token。每一个都是一样的，不管怎么同，比如将两个一块钱细分成若干个一分钱，每个一分钱都是一样的。
- 非同质通证（non-fungible token）：指的是基于区块链技术发行的、唯一的、不可代替的、大多数情况下不可拆分的token。如：加密猫Cryptc一个token都是唯一的不可替代的，比如加密僵尸游戏中用的。

名词解释

1. **EIP**：以太坊改进建议
2. **ERC**：以太坊征求意见。一些EIP被标记为ERC，表示试图定义以太坊使用的特定标准的提议
3. **EOA**：外部账户。由以太坊网络的人类用户创建的账户
4. **Ethash**：以太坊1.0的工作量证明算法
5. **HD钱包**：使用分层确定性密钥创建和转账协议的钱包
6. **Keccak256**：以太坊中使用的密码哈希函数。Keccak256被标准化为SHA-3
7. **Nonce**：在密码学中，属于nonce用于指代只能使用一次的值。以太坊使用两种类型的随机数，账户随机数和PoW随机数