以太坊常用术语

王文刚

2018.7.10

工欲善其事、必先利其器

- 实战以太坊区块链，先背诵20个术语，然后理解其概念，这样看书、看源码，才会豁然开朗，嗯，达成共识了：你和区块链之间。

- 教是最好的学：写博客、写总结、上课、分享、实践。。。

比特币-区块链-以太坊概念术语

- 比特币：2008年发行，最近
- 区块链：比特币的底层技术，最近几年突然火起来的。
- 以太坊：2015.7公网。前比特币程序员，以太坊创始人Vitalik Buterin 发起。
- 白皮书：内有关于以太坊平台的概述，并包括平台发布
- 黄皮书：内有关于以太坊技术的实现规范
- 创世块：区块链初始化配置文件，定义的0块。
- 以太坊基金会：瑞士

备注：

- 区块链技术网络tps低，数据冗余度超级高。n万节点，人人都有一份全账本。上百G数据—交易。
- 开源
- 社区方式运作—社群
- 中本聪原本打算让个人都台式电脑来挖矿，从而形成高度分散的共识和平等分配方案。但是，今天，挖矿是一个高度集中的行业。尤其是5大矿池形成垄断。

以太坊客户端：兼容以太坊协议的客户端

- 功能（协议）： 账户管理、转账、合约管理、太坊虚拟机（EVM）、P2P等功能。
- 客户端：轻型客户端、全节点，如以太坊的100G+ ， 全节点可以挖矿 。

1. Geth: go语言编写。 CLI。
2. Parity：C++语言编写。 ？
3. Mist：GUI界面，Windows、Mac都有客户端。

其他： Java、 Python、C#、 Objective C和node.js等等。

- 以太坊是一个生态，尤其是ERC20协议，发币、Token，运算存储都要交费—比Apple Store模式更酷炫、比Azure.cn更酷炫的**商用模式**。
- 谁是最大玩家？
- 开发一个系统：透明、公开，被人用，很幸福。但是，系统干啥？
- 交易，才有价值。 **所以Token数字通证更有趣。**

备注：搭建私链，就是在网络中，自己一个networkID，3~4台服务器，搭建以太坊网络。Geth有5个程序在run。。。

数字货币—代币—燃料术语

- 钱包：在加密货币平台最基本的一个应用是钱包，模拟模仿银行式的保护措施—自己掌控！ Dapp应用一种。
- 法币：美元、人民币。国家信用背书。问题，人民币谁在发行？
- 账本：过去企业的命脉。 电子化后，税务局直接网上查账本。
- 锚定：黄金是货币的锚定物，不过目前各国货币，近似于随意印发。10年前，4万亿货币，导致10年经济…

- 以太币（Ether）是以太坊内部的主要加密燃料，用于支付交易费用。
- 这种商用设计，非常巧妙。Gas。
- Token：数字货币、代币。

GAS 计价策略

指令计价类型

- 单一计价:按照操作次数计价
  - SLOAD/SSTORE
  - ADD/MUL
  - CALL
- 按照数据长度计价
  - SHA3, 每一个WORD 6 Gas
  - Logdata, 每个字节8 Gas
  - 更多的临时存储,每个字节 3 Gas
- 返还类型
  - 永久存储清零 返还15000
  - 删除合约返还 24000
- 创建账号 32000 GAS
  - 如果加入代码32200
- 将永久存储值由零改为非零值 20000 GAS
- 创建合约 32000 GAS
- 每个交易的起价 是 21000 GAS
- 消息调用传入非零参数 9000 GAS
- 增加存储负担就贵
- 反之就便宜

钱包术语

- 私钥：不能对外公开。
- 公钥：？
- 钱包地址：银行账号，可以公开。

- EOA： Externally Owned Account。个人账号。由用户私钥所控制,可以发起/签名交易, 可以创建合约.地址长度为公钥的Keccak256散列值LSB20Bytes
- CA： Contract Account。合约账号一经创建, 存在于区块链中,一旦接收到消息,其包含的代码被激活开始运行, 它修改全局状态或者向其它合约继续发送消息. **函数的指针**。 全局静态函数？

坑爹的：

1. 钱包地址，不能通用。我有3个钱包APP，各自账号独立。
2. 不要发送到无效地址！否则对方收不到钱，你的钱就没有了。
3. 专有的销毁以太币地址： 0xdead

几个日常现象：

- ATM机有时会和银行主机房失联，问题是，在失联状态如果有用户等待吐钱取款，它到底吐不吐钱出来呢？
- 你的钱在银卡里面，还是在银行数据库里面？

- 你的钱在公交卡里面，还是在公交数据库里面？
- 你用公交卡刷卡，怎么实现扣费？　NFC充值呢？

- 我爸爸，60岁+，现在依然不相信银行卡，而是相信存折！

共识术语

- 什么是共识：哪个节点有记账权、交易的顺序

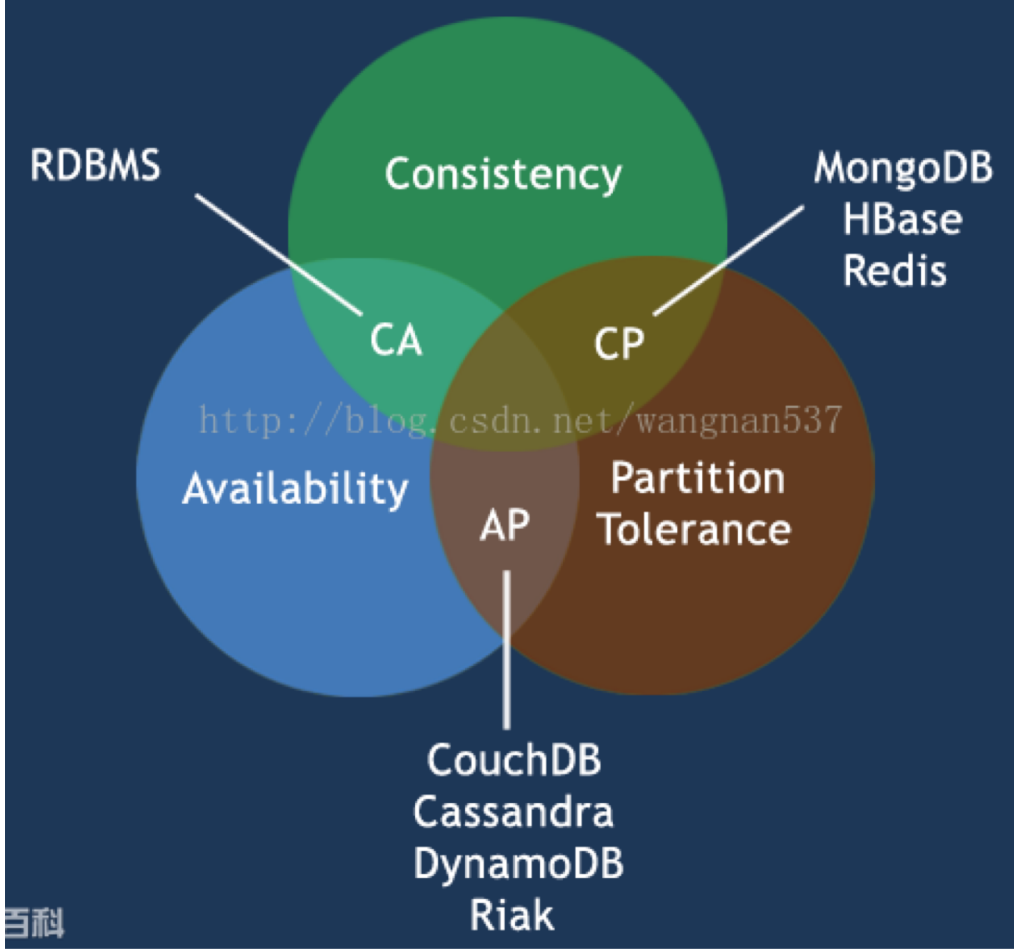
Hash Cash 简介：主要设计思想 就是通过暴力搜索, 找到一种Block 头部组合(调整nonce)使得嵌套的SHA256 单向散列值转
===》计算密集型算法, 一开始从CPU挖矿,转而为GPU, 转而为FPGA, 转而为ASIC. 从而使得算力变得非常集中.
俗称：挖矿。

- 拜占庭： PBFT是Practical Byzantine Fault Tolerance的缩写
- POW： Proof Of Work
- POA：
- POS：
- Dpos：
- 网络从工作量证明（POW）转换到权益证明（POS）将需要一个实质性的转换

- 好消息：2017.12 POS上线以太坊公链。

CAP原则

- CAP原则又称CAP定理，指的是在一个分布式系统中，Consistency（一致性）、 Availability（可用性）、Partition tolerance（分区容错性），三者不可得兼。
- CAP原则是NOSQL数据库基石。
- ● 一致性（C）：在分布式系统中的所有数据备份，在同一时刻是否同样的值。（等同于所有节点访问同一份最新的数据副本）
- ● 可用性（A）：在集群中一部分节点故障后，集群整体是否还能响应客户端的读写请求。（对数据更新具备高可用性）
- ● 分区容错性（P）：以实际效果而言，分区相当于对通信的时限要求。系统如果不能在时限内达成数据一致性，就意味着发生了分区的情况，必须就当前操作在C和A之间做出选择。



交易所术语：交易市场

- 场外交易：私下交易，不需要手续费，不安全。
- 场内交易：交易所内，需要交手续费，安全。
- ICO： Initial Coin Offering。源自股票市场的首次公开发行（IPO）概念。
- 糖果—空投
- 现在的私募普通个人是无法参加的，基本由资金雄厚的币圈大佬和投资机构组团承包了，往往二三十家就能把价值上亿的私募额度分光。然后他们再等着代币登上交易所，利用二级市场的差价，赚取投资利润。

Jd、淘宝、房屋中介？

区中心应用-DApp

- EVM技术：以太坊虚拟机，类似C#的VM。类似Java的JVM。
- C++的程序，是二进制的，其VM集成到了Windows、Mac中。

DAPP 适用场景

DAPP 定义

- DAPP 是一种根植于区块链的应用程序
- 最大的特点是需要与区块链进行交互
- 最核心的状态信息需要存储在区块链中
- 最核心的逻辑功能要用智能合约实现
- 其它静态数据可以保存在一个中心式服务器或者一个分布式的存储服务中 Swarm/IPFS

适用场景

- 对等的多方参与的有交易行为的场景
- 各方之间信任建立在算法/协议之上, 信息高度透明,可重复独立的验证结果
- 历史记录一旦形成就不可更改
- 具有高可用性/鲁棒性, 单点故障不影响整个系统运作

DAPP 例子

ICO类

- ERC 20 Token. 数以千计
- EOS.io
- Lamden
- https://eidoo.io/erc20-tokens-list/

游戏类

- ERC 721 Token
- Cryptokitties
- Ethergoo
- Decentraland

收藏/拍卖类

- ERC 721 Token
- 收藏/拍卖 字画, 珠宝
- 房产拍卖

博彩类

- 可验证伪随机数
- Crypto-lottery

https://www.stateofthedapps.com/ https://dappradar.com/

DAPP 例子

交易所/侧链类

- Hawala
- Raiden
- Plasma

其它治理类

- 电子投票
- 非营利组织管理

DAO

- DAO
  - venture capital 管理
  - 由一组 Smart Contracts
  - 代表长期的发展方向

广告媒体类

- Basic Attention Token
  - 用户被动接受,无收益
  - 广告从投放到发布中间环节太多
  - 用户隐私得不到很好的保护

https://www.stateofthedapps.com/ https://dappradar.com/

区块链派系：币圈、链圈

- 发行Token，目前是区块链唯一可行的创业项目。
- 核心：数字货币，记账思维，说破天就是超级积分—会员卡。

- 其他落地的Dapp，成本太高，而且，相当不实用。

后记—常用网站

- https://etherscan.io/ 以太坊浏览器
- https://www.stateofthedapps.com/ DAPP雷达
- https://dappradar.com/ DAPP雷达
- https://ethstats.net/ 以太坊网络监控
  https://www.bitansuo.com/calendar/waiting/ ICO发行日历
- http://tokenwallet.cc/ 钱包排行榜