去中心化与区块链使用场景

货币发展历史

1. 物物交换：1头牛 = 6只羊 1只羊 = 9只鸡.
2. 实物货币：贝壳、盐、金银. (具备稀缺、易分割).
3. 纸币进行支付 (信用背书，战乱、通货膨胀), 在津巴布韦人人都是亿万富翁.
4. 记账货币：银行卡、信用卡 (银行拥有记账权) , 2008年金融危机,美国政府增发美元,人们财富缩水.
5. 数字货币：分布式记账、货币不能超发、记账过程完全透明

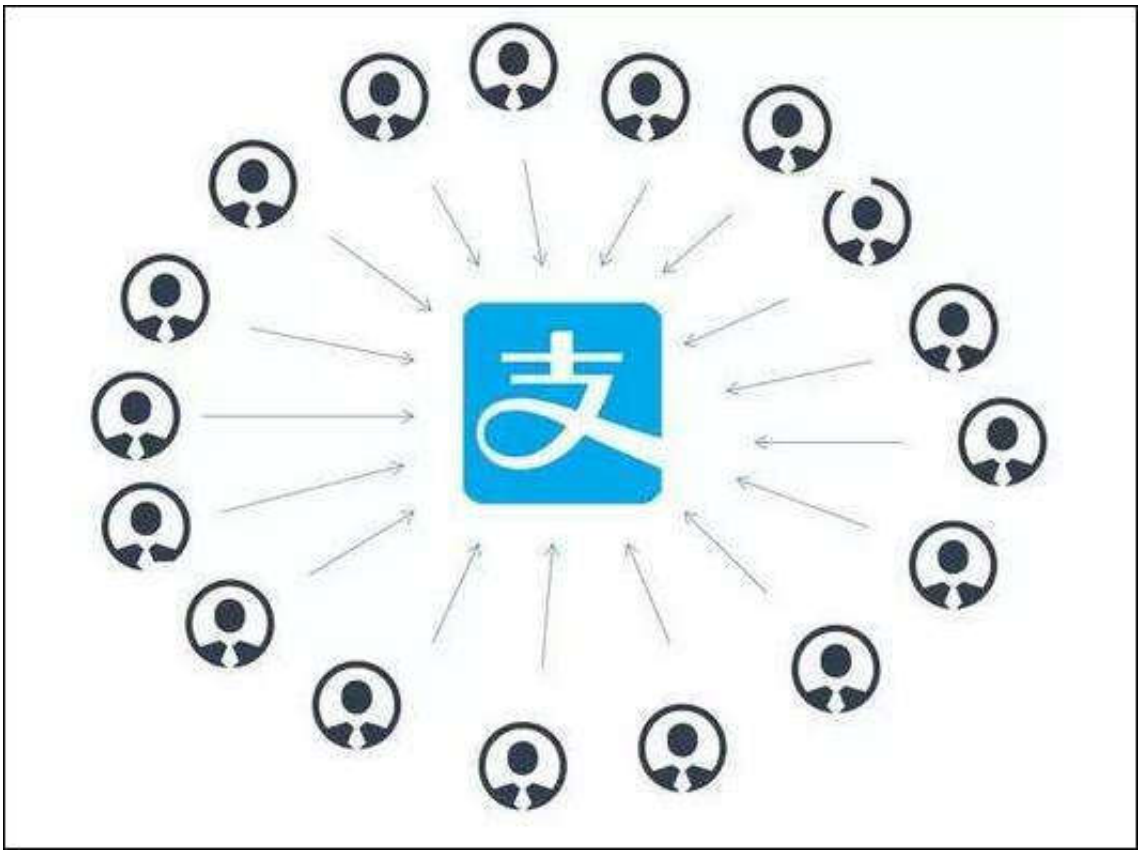
BTC特性使它天然称为金融货币

1. 比特币上限2100万枚
2. 通过挖矿(参与记账的过程)来实现货币发行与货币的分配.
3. 可分割性 1BTC = 10^18 聪
4. 交易不可伪造、不可篡改性
5. 不可重复花费,解决了双花问题.

中心化淘宝购物分析

1. 买家转款到支付宝
2. 支付宝通知卖家发货
3. 卖家发货

4. 买家确认收货
5. 支付宝货款打给卖家



中心化架构的缺点

1. 用户信息容易被泄露
2. 数据容易丢失，容易篡改
3. 中心化并不能从根本解决信用 (百度排名、刷单)
4. 郭美美与红十字会事件

去中心化实现

> 简单了解比特币实现机制：https://btc.com/

去中心化优点

1. 去中心化系统杜绝了中心结点的腐败,我们无需担忧一个中心节点出错，会导致全盘皆输的局面
2. 去中心化系统规则往往要很简单,没有中心的介入,往往更高效
3. 去中心化系统具有无限可能性。就像生物的进化一样，发展出多样性的生态

去中心化缺点

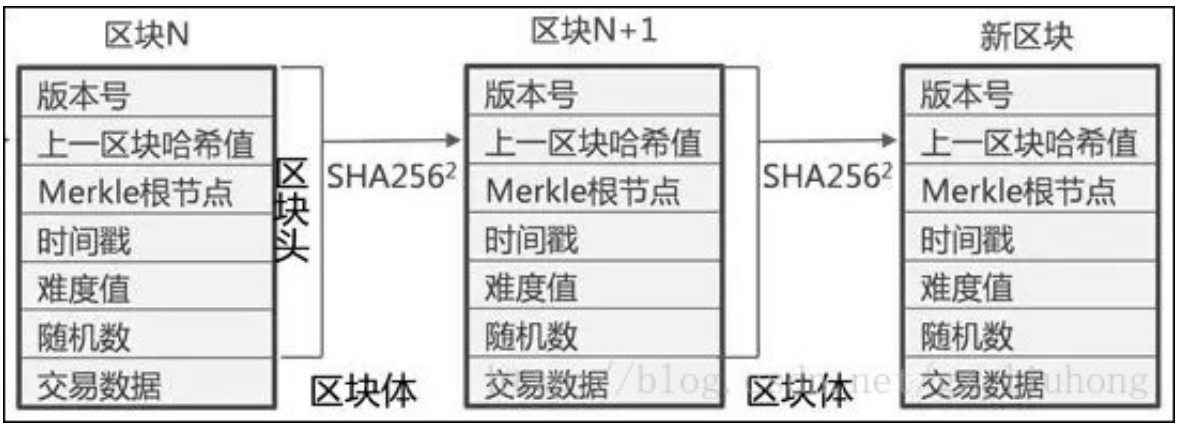
1. 去中心化系统交易存储代码非常昂贵
2. 去中心化系统不可控、不可预制、没有责任人
3. 去中心化系统意味着进化和优化效率低下

区块链概念介绍

> 区块链（BlockChain），是区块（Block）和链（Chain）的直译, 每个区块存储规定时间内的交易数据.并通过密码学的方式.形成一个不可篡改、全员共有的分布式账本

区块链的体系结构

区块概念演示：https://anders.com/blockchain/



哈希散列

> 一种保证原始数据不被篡改的二进制算法

1. 相同数据生成Hash不变
2. 加密算法不可逆

区块

> 区块链中承载交易的数据包

挖矿

> 不断计算Nonce使得生成Hash值满足给定难度的过程

挖矿伪代码演示

> 所谓的挖矿就是计算Nonce的过程,让Nonce匹配给定的Hash值,Hash值前面的0越多,则说明难度越大

- 判断生成的Hash值是否符合难度

```
function isValidHashDifficulty(hash, difficulty) {
  for (var i = 0, b = hash.length; i < b; i ++) {
      if (hash[i] !== '0') {
          break;
      }
  }
  return i >= difficulty;
}
```

- 通过不断测试nonce来找到符合条件的Hash值

```
let nonce = 0;
let hash;
let input;
while(!isValidHashDifficulty(hash)) {
  nonce = nonce + 1;
  input = index + previousHash + timestamp + data + nonce;
  hash = CryptoJS.SHA256(input)
}
```

矿工/矿机

> 打包区块的人称为矿工,运算Nonce机器称为矿机

难度目标

> 打包区块的难度,例如在比特币体系中通过调整难度目标,使得大约每10分钟左右生成一个区块

工作证明（POW Proof of work）

> 简单理解就是一份证明，用来确认你做过一定量的工作,例如：期末获得了优秀员工,就是你努力工作的证明.

工作证明的设计原理

1. 取一些公开的数据（在比特币中取区块头的数据）
2. 给这个公开数据添加一个计数器,计数器默认从0开始(在区块链中计数器就是nonce)
3. 将 data(数据) 和 counter(计数器) 组合到一起,获得一个哈希检查哈希是否符合一定的条件
4. 如果符合条件，结束如果不符合,增加计数器,重复步骤:3-4.

股权证明 (POS Proof of stake)

1. 在POS模式下,有一个名词叫币龄,每个币每天会产生1币龄.(100个币,共持了30天,那么币龄就是3000)
2. POS也需要挖矿,但是币龄越多的人挖矿越容易,如果发现了一个区块,则获得奖励,但之前的币龄就会被清空
3. POW中决定谁更能挖到矿的是算力.而POS不同.决定谁更可能挖到币的是"币数量" + "币龄"
4. POW导致了算力的浪费,而POS则慢慢会导致贫富差距扩大

DPOS (委托权益证明)

1. 类似人大代表制度,理解为N个节点,N个超级节点彼此的权利是完全等同的.
2. 不挖矿,采用超级节点方式来记账,靠数字货币增发来奖励超级节点
3. 当前EOS采用此模式,此方式也称为半去中心化.

比特币概念介绍

比特币概念

> 比特币,既然称为比特,是数字字节(Byte)的译音.则一定和数字化相关. 币:一定和钱有关.比特币就是一种数字货币.

比特币特点：

1. 完全去中心化,比特币发行不依赖国家、银行或者企业
2. 总量一定：2100万枚
3. 匿名记账：通过一个34位的钱包地址来进行交易

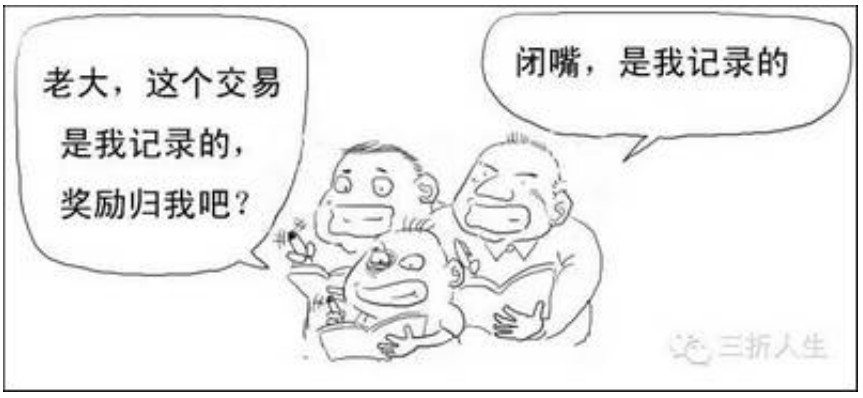
比特币交易

> 所谓比特币交易就是从一个比特币钱包向另一个中转.每笔交易都有数字签名来保证安全.交易生效那么就对多有人都公开.

钱包下载与使用：https://bitcoin.org/zh_CN/download

比特币如何生成

矿工的任务就是参与争夺记账权.24小时进行不停的哈希碰撞.这个过程简称挖矿.之所以有这个动力,是因为谁取得记账权.最新生成的比特币奖励就给谁



比特币产量减半问题

本质上是在模拟黄金,由于黄金储量有限,挖掘速率会越来越慢,因此比特币也被成为数字黄金,比特币生产也俗称挖矿),规定了在每产生**210000个区块**后,比特币产量减半,一开始每个区块产生50个比特币,后来逐步减半,直到逼近为零 (**逼近为零时,每笔交易手续费就成为矿工的收入来源**)

1. 6 * 24 = 144 (平均一天生产144个区块)
2. 210000 / 144 = 1458 (天) / 365 = 4年 (因此平均每4年产量减半)

计算每个阶段产生的比特币

起始区块	阶段	比特币/区块	年	阶段产量	阶段结束总量	已产占比
0	1	50.00000000	2009.007	10500000.00000000	10500000.00000000	50.00000006%
210000	2	25.00000000	2013.000	5250000.00000000	15750000.00000000	75.00000008%

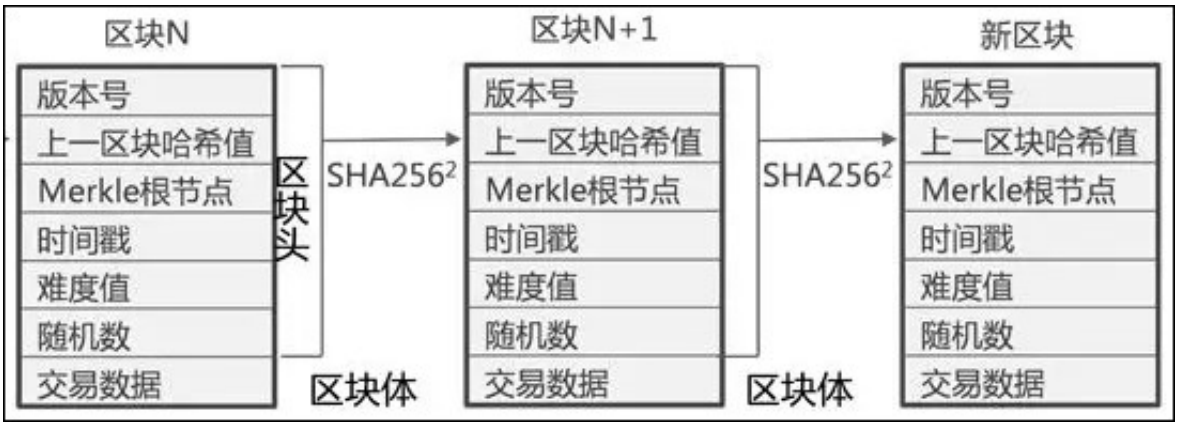
第一阶段：2009~2013年： 144(一天区块数) * 365 * 4(年) * 50(单区块奖励) = 10512000

比特币每年总量参考：http://www.8btc.com/21million00

如何看懂比特币区块

> 每个区块大小被限定在1M，每个交易大约250字节，所以每个区块最多容纳4000个交易。由于每个被认可的区块平均产生时间为10分钟，意味着每秒钟只能处理7个交易

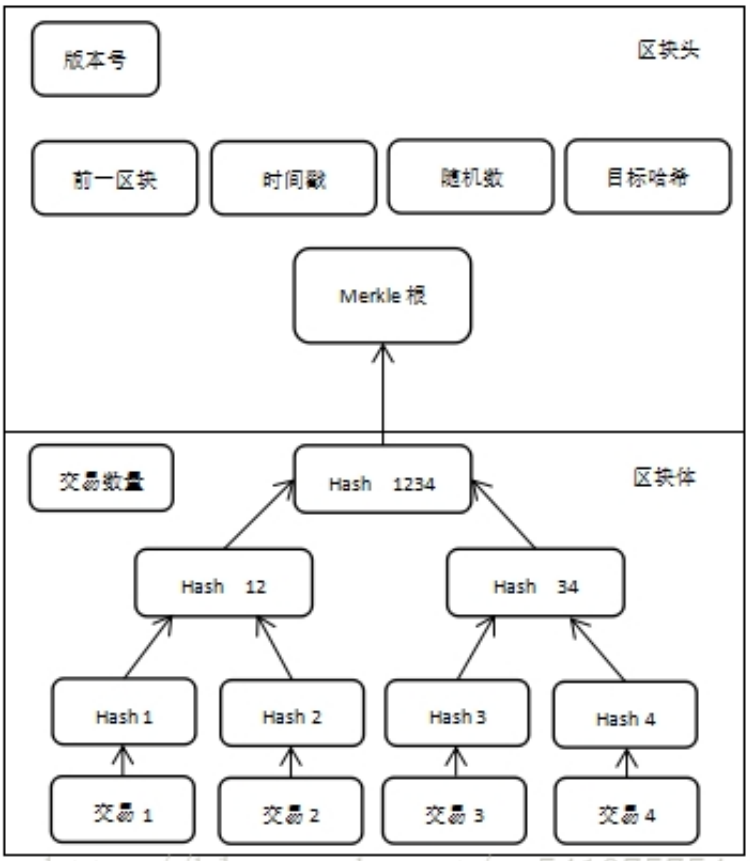
比特币区块：https://btc.com/



Merkle tree (默克尔树)

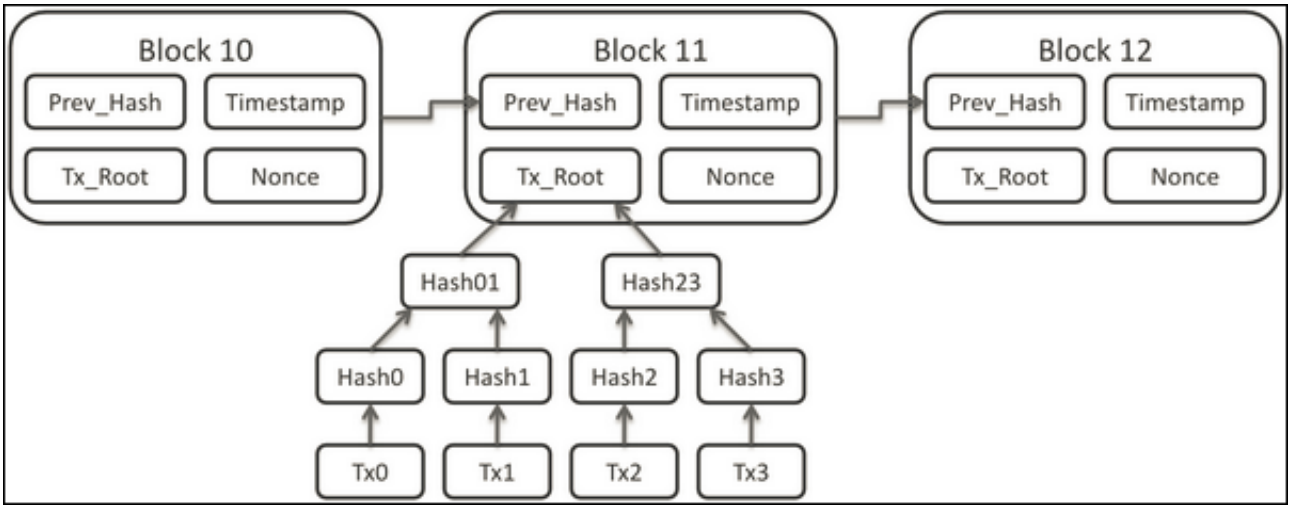
> Merkle树被应用在了交易的存储上。每笔交易都会生成一个hash值，然后不同的hash值向上继续做hash运算，最终生成唯一的Merkle根。并把这个Merkle根放入数据区块的区块头

默克树的内部结构

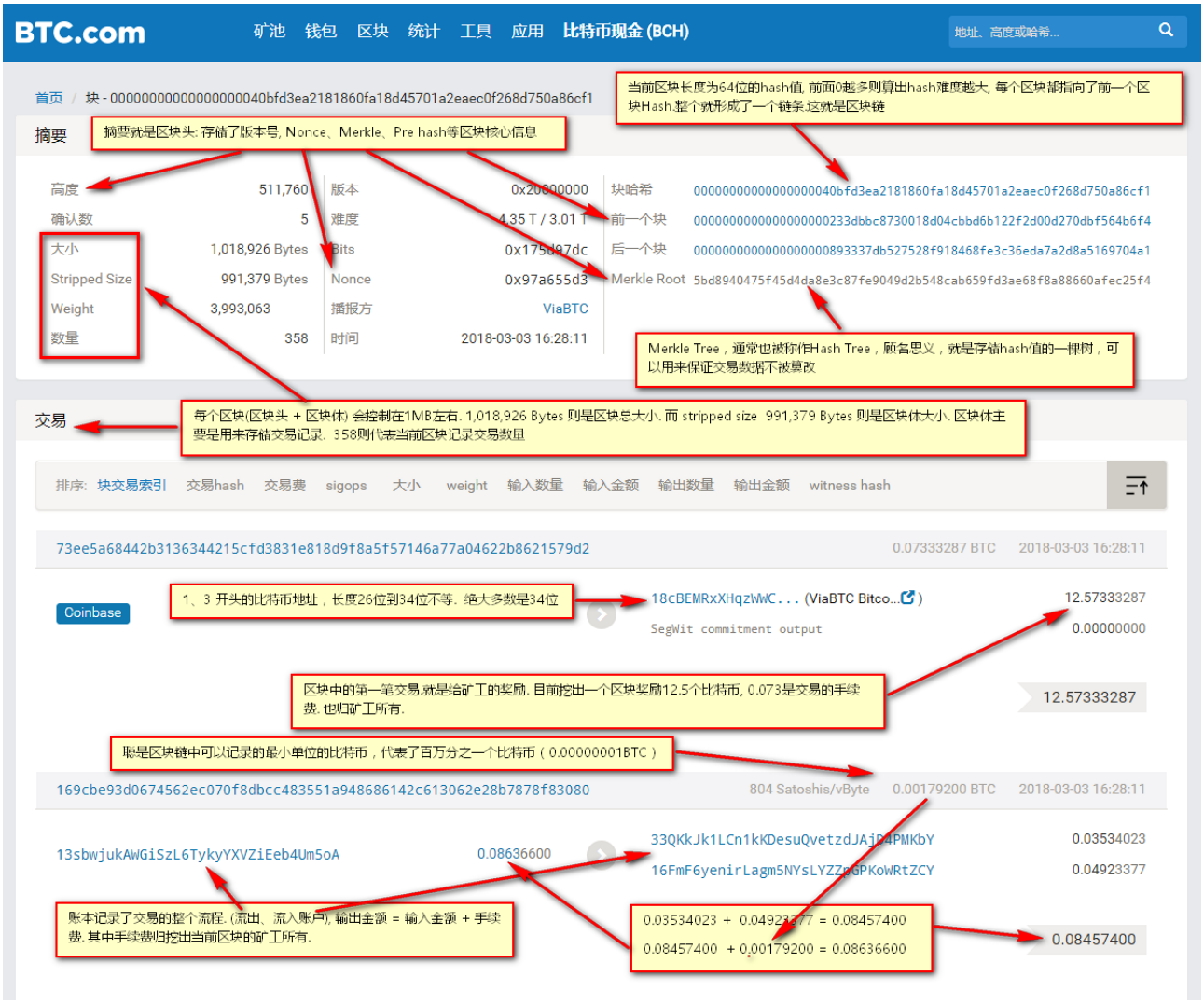


区块结构

默克尔树与区块的关系

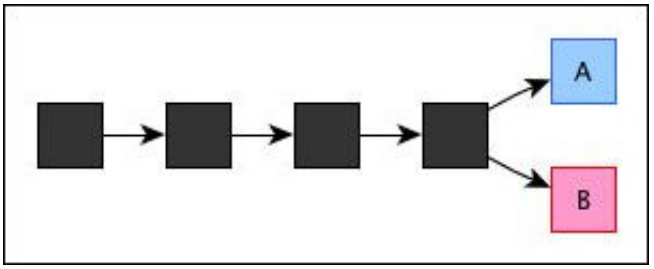


比特币区块解读

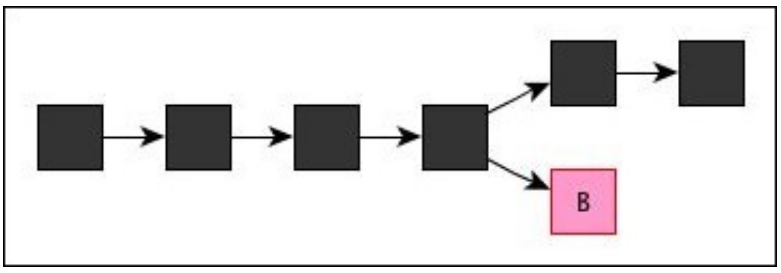


比特币解决双花问题

1. 每笔交易都需要先确认对应比特币之前的状态，如果它之前已经被标记为花掉，那么新的交易会被拒绝
2. 如果诈骗者利用网络延迟同一笔金额在不同电脑花两次.



下一个矿工选择在A基础上继续记账的话，A分支就会比B分支更长，根据区块链的规则，最长的分支会被认可



比特币分叉

> BTC,区块大小仅为1M(每笔交易250字节,因此一个区块只能容纳4000笔交易)，而且会出现交易延迟，交易费也越来越高.由于没有中央节点,社区意见很难统一,这就是数字货币常说的一言不合玩分叉!

软分叉与硬分叉

> 如果你遇到一个硬分叉,它意味着某种数字货币——比如比特币——的新版本软件和旧版本无法兼容,彼此看不顺眼,必须各走各路.而软分叉则不同,新版本要求更为严苛，不同意旧版本的一些规则；但旧版本比较憨厚，还能接受新版本软件.

硬分叉：BCH(比特现金)于2017年8月1日，比特币高度478558时分叉,开创了比特币分叉的先河,BCH的挖抗算法、矿机与BTC相同，一些矿池还加入BTC/BCH自动切换功能，可为矿工自动切换至收益高的币种

BCH官网：https://www.bitcoincash.org
数字货币价格查询：https://www.feixiaohao.com
BTC历史分叉查询：http://www.btc798.com/articles/14863.html

总结：虽然每次修改代码都会带来一些不确定性，对于用户来说有一定的风险，但是比特币现金通过这种方式将不断的创新，完善技术并提高用户体验，从而实现其“世界

最好的货币”的目标

比特币缺陷与解决方案

交易效率低和交易确认时间长的问题

1. 每秒处理笔数的峰值一般小于7笔. (每个区块大小被限定在1M，每个交易大约250字节，所以每个区块最多容纳4000个交易。由于每个被认可的区块平均产生时间为10分钟，意味着每秒钟只能处理7个交易)
2. 而2014年双11期间.支付宝实现了每秒处理47500笔交易的速度

解决方案：

1. BCH比特币进行扩容
2. ETH每挖一个区块奖励5个以太坊币,平均每10S左右出一个区块
3. EOS每秒 (10,000/s-100,000/s) EOS将使用并发机制来扩展网络，可能高达每秒数百万次的交易

EOS与ETH比较：http://www.sohu.com/a/216330641_481485

POW共识机制引发高耗能问题

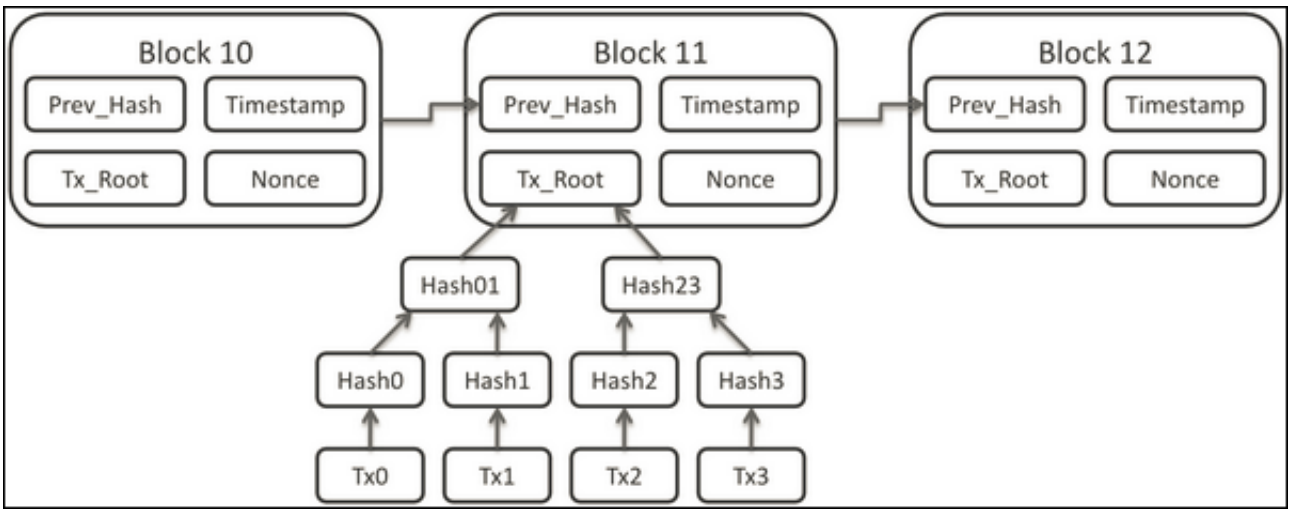
区块时一个高耗能的系统，每次参与竞争的有成千上万个矿工,但是只有1个矿工能获取记账权.其它参与竞争的99.999%以上的矿工算力都是浪费

解决方案：

1. 股权证明 (POS Proof of stake)，POS模式下拥有币龄的矿工更有可能挖到区块
2. 股权委托证明（DPOS）可以由相对较少数量的处理器来操作. 又避免的作弊问题

区块、区块链账本的容量问题

截止到2016年4月.比特币区块总数据容量已经达到了67GB.而且区块链还在不断增加.这给普通客户和移动端客户带来了很高的门槛.这也是造成了比特币全节点(Full Nodes)的数量.不增反减.



解决方案：

1. SPV轻钱包：
2. 网页版钱包: https://blockchain.info/zh-cn/wallet/#/
3. 阻止灰尘交易

比特币不是图灵完备的

比特币系统底层是简单非图灵完备的脚本.因此在比特币系统中只能完成账户的交易功能,缺乏其它应用场景想象空间

区块链的发展阶段：

1. V1.0：比特币,点对点金融支付
2. V2.0：引入智能合约,ETH为代码,主要与"金融"领域结合
3. V3.0：区块链与商业应用的结合,EOS代表

安全性问题

目前看,采用了非对称密码学原理是安全的.但是随着数据研究和量子计算机技术进一步发展.这些非对称加密算法是否能被破解呢. 也许在未来基于数据原理基础上的算法安全会变得越来越脆弱.那时区块链将会失去信任这最后一个根本的基石

去中心化责任问题

区块链去中性化意味着它没有一个正式组织或官方机构来操作.这样一出问题将没有机构或者组织对此负责.

区块链技术主要应用方向

> 以前的科技变革是是生产力提升,而区块链是生产关系的改善,共识机制为去中心化的数据提供了可信度,这将大大节省人与人之间合作的成本

区块链专利排名：https://www.cybtc.com/article-2997-1.html

思考：2017年5月的勒索病毒制造者什么选择比特币支付

1. 比特币地址匿名性
2. 完全去中心化导致无法监管也无法冻结
3. 比特币全球通用,流通非常方便,方便全球收款

支付宝爱心捐赠平台

https://bitrating.com/blockchain/85408.html

CryptoKitties迷恋猫

https://www.cryptokitties.co/

区块链的游戏特点：

1. 传统游戏,可能玩家花几百个小时玩一款游戏.随着游戏关服.玩家积累的荣耀、装备都可能随时打水漂,这个情况不是由玩家来控制的.完全由厂商决定
2. 代码、虚拟资产都会在区块链中永久的记录存储,不可能篡改、销毁
3. 打破发行渠道过于集中的现状.目前游戏发行厂商就几家.平台会抽取大量的费用.有些甚至到了8:2，这对游戏产业发展是很不利的

区块链与博彩业

1. 在日期和可审性方面，区块链创造的数据记录不可篡改，因而有助于追踪所有的交易，比如说一个客户和/或一场赌博。这也使得评估客户对业务的贡献，
2. 追踪任一网络博彩模式，避免诈骗和漏洞，奖励客户，提供审核报告更加容易。而在博彩的商业逻辑上
3. 区块链保证了高透明性，且可证实维护了博彩公平

区块链与版权保护

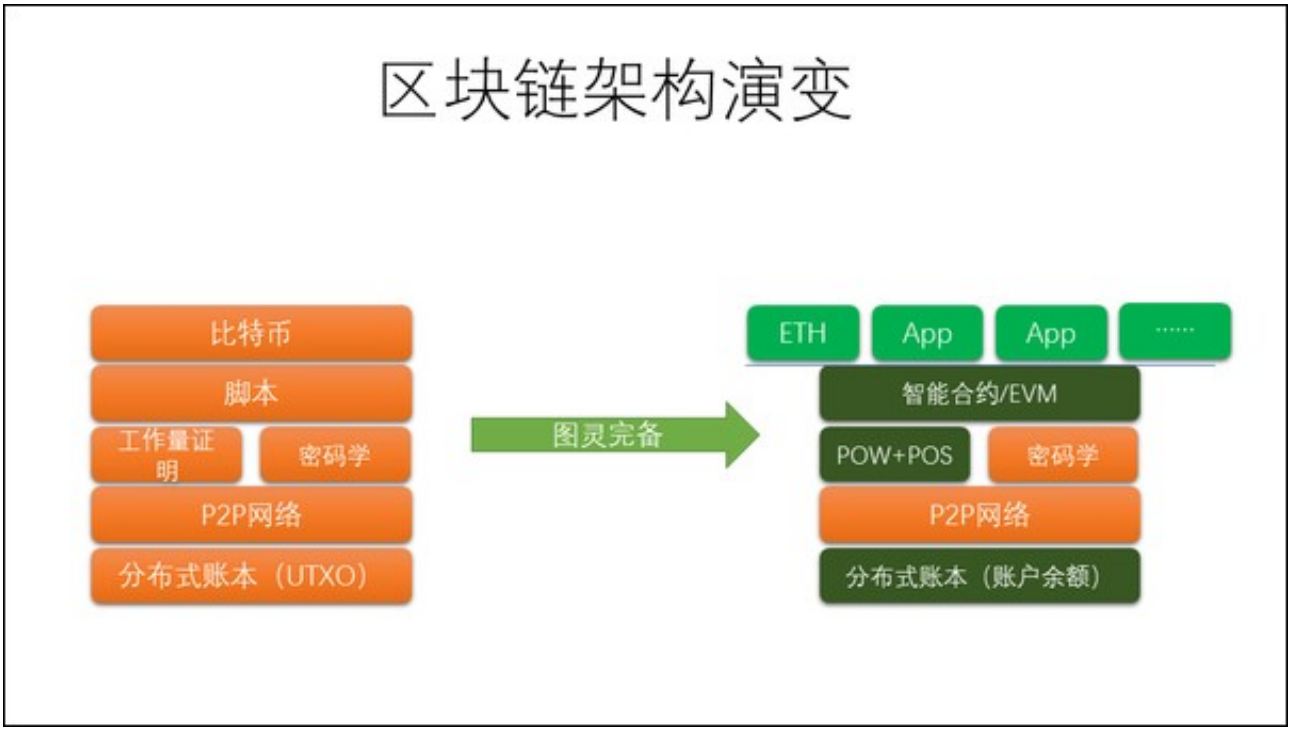
对于原创作品的登记，区块链技术可以非常方便地把时间戳与作者信息、原创内容等元数据一起打包存储到区块链上

落地应用：百度图腾
官网地址：https://image.baidu.com/eco/index#/
图腾介绍：http://www.chinaz.com/news/2018/0412/872765.shtml

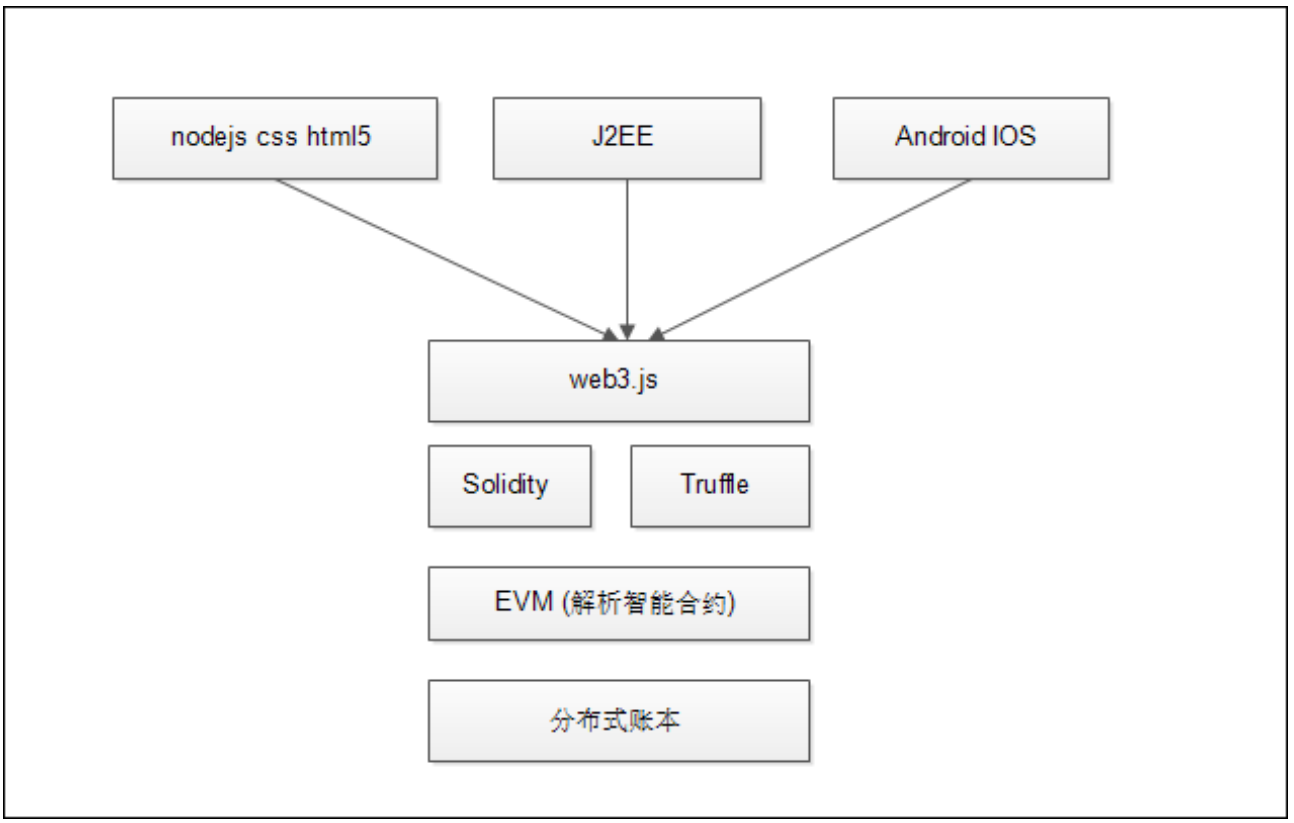
内训案例分享

1. 高校教师诚信问题
2. 不同医院如何共享病人信息

区块链架构演变



> 区块链架构与其它语言整合结构图


nodejs css html5
J2EE
Android IOS
web3.js
Solidity
Truffle
EVM (解析智能合约)
分布式账本