比特币、区块链和供应链金融

李波涛
libotao@yiguo.com
2018/3/6

分享交流主题

- 比特币（Bitcoin）
- 区块链（Blockchain）
- 以太坊（Ethereum）
- 超级账本（Hyperledger）
- 供应链金融（Supply Chain Finance）

比特币-Bitcoin

- 比特币&钱包
- 2009.1.3 比特币横空出世
- 发行了50 BTC

WannaCry袭击全球，索要BTC

https://blockchain.info/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

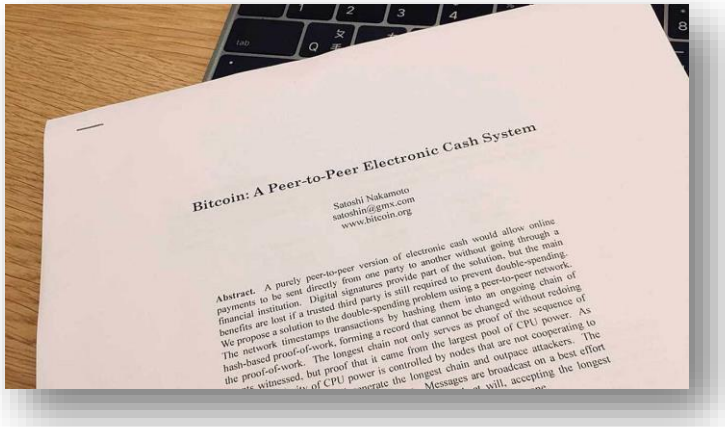
- 2017.5.12一种名为“WannaCry”的蠕虫勒索病毒成功偷袭了包括中国在内的全球百余国家，几乎以每秒感染1台电脑的速度快速攻陷医院、机场、ATM机、公司内网、学生电脑等等；
- 除了网络安全问题，“比特币”这个词也随着这次网络病毒肆虐火了起来。因为黑客在锁死电脑后，要求中毒者支付的“赎金”不是美元，不是人民币，不是欧元，而是“比特币”。
- 受害者电脑被黑客锁定后，病毒会提示支付价值相当于300美元的比特币才可解锁。

中本聪-BTC开发者兼创始者

神秘中本聪
YY-中国人本来聪明？

- 完全隐身，真实身份至今无人知晓；
- 明明可以靠才华吃饭，还要搞神秘；
- 既不动用手里十几亿美元的BTC，也不去申请专利，就连提名诺贝尔经济学奖候选人也不现身；

2008年发表论文：
Bitcoin: A Peer-to-Peer Electronic Cash System
比特币：一种点对点的电子现金系统



Bill Gates in 2014: Bitcoin is 'better than currency'

- "Bitcoin is better than currency in that you don't have to be physically in the same place and, of course, for large transactions, currency can get pretty inconvenient."

- Today, bitcoin is already running into some problems, including slow transaction times and the rising cost of transaction fees.
- Right now it takes an average time of 78 minutes to confirm a bitcoin transaction, according to Blockchain.com. But on Sunday the average time was as high as 1,188 minutes.

比特币是什么？

- 一种虚拟货币；没有实体，它只是计算机世界里的一串数字；
- 一种P2P形式的数字货币；
- 点对点传输，去中心化的支付系统；
- 不依靠特定货币机构发行；
- 稀缺性-总数限制在2100w个；

各方评价：

- 是一帮无政府主义者的乌托邦；
- 是人类经济史上的一次大革命；
- 是天才的技术创造（Bill Gates），也有人认为是有很多缺陷的一个开源软件；

Story：花10000个BTC购买2个披萨

Transaction View information about a bitcoin transaction

a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d

1XPTgDRhN8RFnzniWCddobD9iKZatrvH4 → 17SkEw2md5avVNyYgj6RiXuQKNwkXaxFyQ 10,000 BTC

10,000 BTC

Summary	
Size	23620 (bytes)
Weight	94480
Received Time	2010-05-22 18:16:31
Included In Blocks	57043 (2010-05-22 18:16:31 + 0 minutes)
Confirmations	454719 Confirmations
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	10,000.99 BTC
Total Output	10,000 BTC
Fees	0.99 BTC
Fee per byte	4,191.363 sat/B
Fee per weight unit	1,047.841 sat/WU
Estimated BTC Transacted	10,000 BTC
Scripts	Show scripts & coinbase

- 1 BTC=11,290.86 USD
- 10000 BTC=1+亿 USD

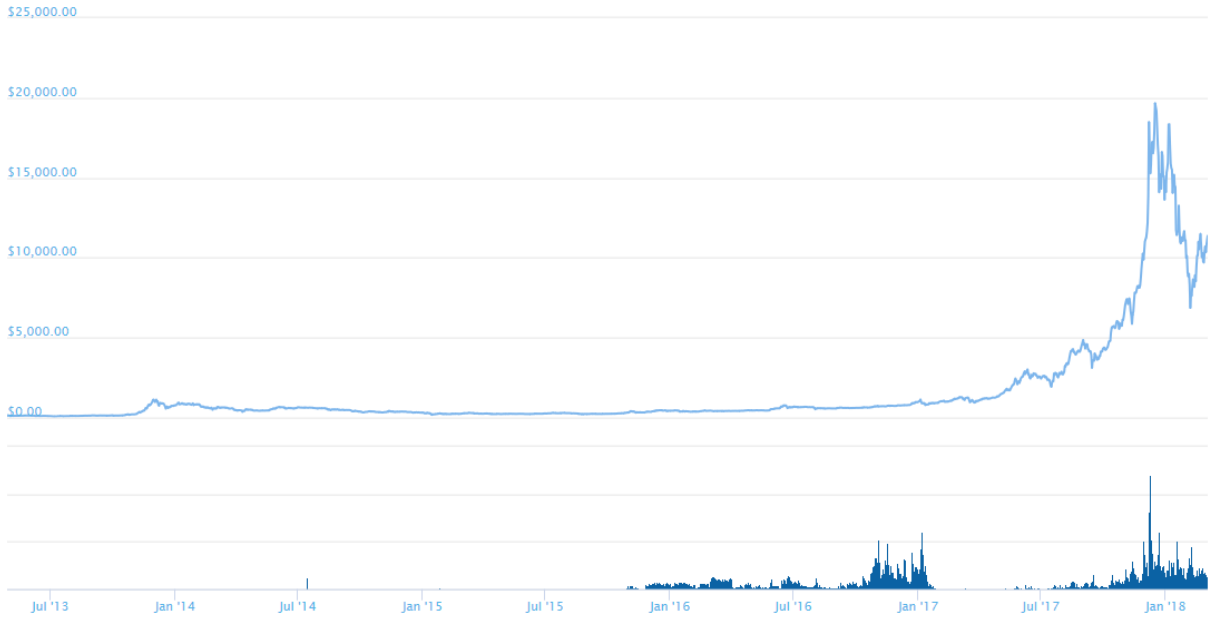
交易URL

Laszlo Hanyecz 41$-> Jercos 400$

2个人和超级富豪擦肩而过？

呵呵，和北上广深的房价一样

Bitcoin 价格及现状



- BTC钱包地址和余额、任何一笔交易记录，都是可以公开查询的。
- 最大的一个钱包地址是14万BTC，余额排名世界第一。
- 余额一万个BTC可以排到前100名，余额过千的人也不多。
- BTC的持有者仅占了世界人口的0.3%

币圈1天，人间1年。除了发展速度之快，还有就是获取财富的速度。

比特币价值

- 为什么一枚比特币值1.1万美元？为什么以太坊值1040美元？为什么Cryptokitty值10万美元？
- 所有加密货币都是稀有资产，数量有限。如果货币被人们接受并广泛使用，人们就要购买这些稀有资产，那么它的价值就会涨得比今天还要高。
- 当前的价格反应了某种加密货币的潜力，它未来可能会被人们广泛使用。

100万亿津巴布韦 < 1USD

Bitcoin’s first block

- 创世块-Genesis Block
- 2009-01-03
- https://blockchain.info/block-index/14849
- 当前：1700w BTC 总共：2100w BTC

Block #0

Summary	
Number Of Transactions	1
Output Total	50 BTC
Estimated Transaction Volume	0 BTC
Transaction Fees	0 BTC
Height	0 (Main Chain)
Timestamp	2009-01-03 18:15:05
Received Time	2009-01-03 18:15:05
Relayed By	Unknown
Difficulty	1
Bits	486604799
Size	0.285 kB
Weight	0.896 kWU
Version	1
Nonce	2083236893
Block Reward	50 BTC

Hashes	
Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Previous Block	0000000000000000000000000000000000000000000000000000000000000000
Next Block(s)	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Merkle Root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

Transactions

4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b			2009-01-03 18:15:05
No Inputs (Newly Generated Coins)	→	1A1zP1eP5QGefi... (Genesis of Bitcoin)	50 BTC
			50 BTC

比特币的钱包

- 比特币地址 – 类似于银行账号；
- 私钥- 类似于银行账号密码；
- 钱包- 用来生产、管理私钥和地址、接收和发送比特币的工具；
- 钱包的精髓就是用来保存私钥的。

下载地址：

- https://wallet.bitcoin.com/

比特币交易记录

- 每个交易都是一段数据，你私钥签完了以后会发送到全网；

基本信息如下：

- FROM（谁发送的，包括两部分）
  Previous tx: 你要花的这笔钱的那个账单的id， 也就是说，你花的任何一笔钱都应该有人转给你过，需要出示那个账单的id；
  scriptSig: 你对这笔交易的签名，就是把单子用你的私钥做hash，只有你能做这个hash；

  TO（谁接受，包括两部分）
  Value: 要发多少；
  scriptPubKey: 对方的公钥，比特币账户就是一段公钥；

实际的比特币交易记录

交易 关于比特币交易的信息

2a93e411d7cc829675d93fe2cd18fe32c89d8833757cede9d27d8fb2485ef968

1FdxRQ98hdB7LkLGCR9nNg47H9dxKqfGZq	FROM第一个账号	1Bet32kBtZzXViM… (BetCoin Dice 48 Percent)	TO第一个账号 0.08 BTC
1HDZFKdiSScJebn6e1dDDe2EREsGCfSPeS	FROM第二个账号	19sUtEnbHq2oV3wUHW72XrYEhuf5MTNe8z	TO第二个账号 0.09293282 BTC
17zeXYYuZ6LftCJ8cPBTYA52onHobzdaKV	FROM第三个账号		
FROM		TO	未确认的交易！ 0.17293282 BTC
			转账金额

总结	
大小	523 (字节)
收到所用的时间	2013-11-28 13:29:45
估计确认时间	2 小时 (队列位置870)
通过IP的传递	129.132.230.69 (whois)
想象	树图

输入和输出		
总输入	0.17303942 BTC	
总输出	0.17293282 BTC	总输入+费用=输出
费用	0.0001066 BTC	
估计成交的比特币	0.09293282 BTC	
scripts	显示script和coinbase	

网络传播（点击查看）

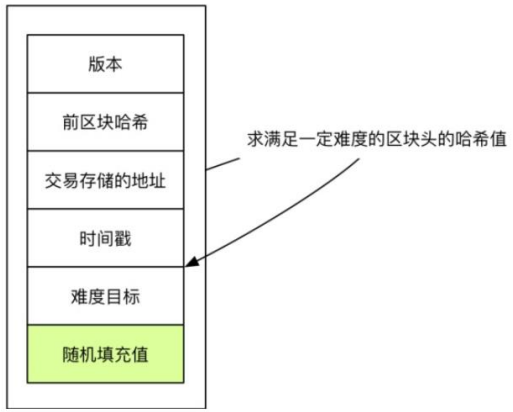
比特币的生态圈

- 币圈时代，第一波红利收获者？

挖矿-矿工和矿机

- 挖矿就是穷举随机数的算法，将上一个区块的hash值加上10分钟内的全部交易单打包，在加上一个随机数，算出一个256位的hash字符串，只要输入的随机数满足hash字符串的前面有XX个0就可以获得这个区块的记账权。
- 新产生的区块需要快速的广播出去，以便于其他节点进行验证，防止造假，每个区块上存着上一个区块的哈希值，可以追溯到源头。

抢夺区块的打包权



何年何月挖完？

BTC挖矿现状

比特币挖矿总共经历了以下五个时代：

- CPU挖矿→GPU挖矿→FPGA挖矿→ASIC挖矿→大规模集群挖矿

全球比特币挖掘所使用的电量之和，超过了全世界159个国家各自的用电量

使用189个ASIC芯片

F2Pool - 比特币矿池 ，中国最大的BTC和LTC矿池，BTC算力全球第4，LTC算力全球第2。

每10分钟只能处理1mb交易数据

我对BTC的看法

- 会挑战现有的国家货币吗？
- 存在严重泡沫吗？
- BTC和Blockchain是一回事吗？
- BTC和ICO（Initial Coin Offering）
- ICO和IPO

区块链-Blockchain

- 徐小平：all in 区块链；
- 蔡文胜：不参与才是最大的风险；

马云：很多人一生输就输在对新生事物第一看不见，第二看不起，第三看不懂，第四来不及。

国内区块链专利申请

国内区块链企业专利申请排行榜（2017年2月）

序号	单位名称	专利数量
1	布比（北京）网络技术有限公司	28
2	北京太一云科技有限公司（邓迪）	19
3	杭州复杂美科技有限公司	11
4	深圳市樊溪电子有限公司	11
5	杭州云象网络技术有限公司	10
6	江苏通付盾科技有限公司	9
7	深圳市淘淘谷信息技术有限公司	8
8	宁圣金融信息服务(上海)有限公司	6
9	惠众商务顾问(北京)有限公司	4
10	中国银联股份有限公司	4
11	瑞卓喜投（鑫苑）	30+

注：数据整理自中国专利局网站（截止2017年2月16日）

来呀 … 颠覆我吧

- 马老师还是马老师
- 你大爷还是你大爷

检索结果统计

申请人统计

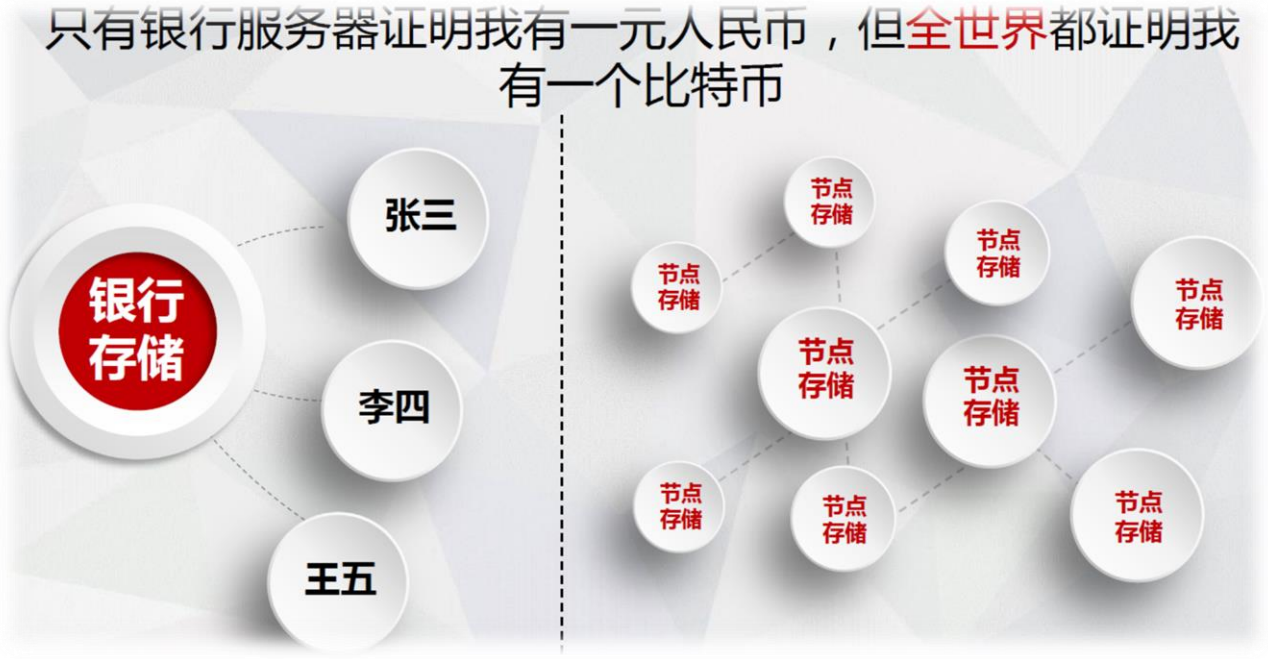
- 阿里巴巴集团控股… (54)
- 北京瑞卓喜投科技… (29)
- 布比（北京）网络… (27)
- 江苏通付盾科技有… (25)
- 杭州复杂美科技有… (21)
- 杭州云象网络技术… (21)
- 中国联合网络通信… (20)
- 电子科技大学 (18)
- 深圳前海达闼云端… (17)
- 杭州趣链科技有限… (17)
- 其他 (938)

国内区块链企业专利申请排行榜（2018年2月）

区块链技术-BTC核心

- 它是很多区块链接在一起，就组成了区块链
- 它是一种分布式账簿
- 它是一种去中心化的数据库
- 它是高度自治的交易体系
- 它是所有历史交易可追溯的
- 它是安全的，所有数据不可篡改

去中心化的数据库



传统中心化的存储体系与去中心化的存储体系的区别

- 分布式记账本，记录了所有的交易信息。
- 每一笔交易都永久的保存在区块数据中可供别人查询。这些数据区块存放在每一个节点中。
- 这些节点构成了BTC的分布式数据库系统。
- 任何一个节点挂了都不会影响整个系统。

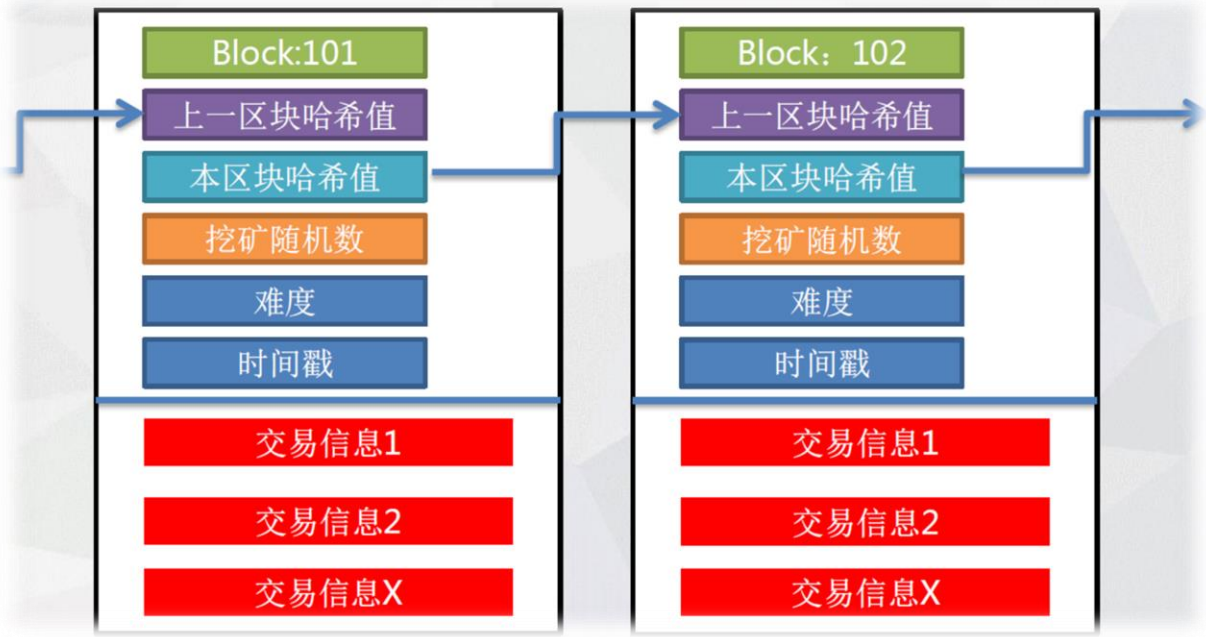
拜占庭将军问题：区块链的共识机制

- 中心化系统，听BOSS的指挥；去中心化系统，怎么办？
- 投票解决可以吗？少数服从多数。
- 但是如果有叛徒，9人投票，4人投进攻，4人投撤退，剩下1个叛徒，就惨了；

中本聪的思路：

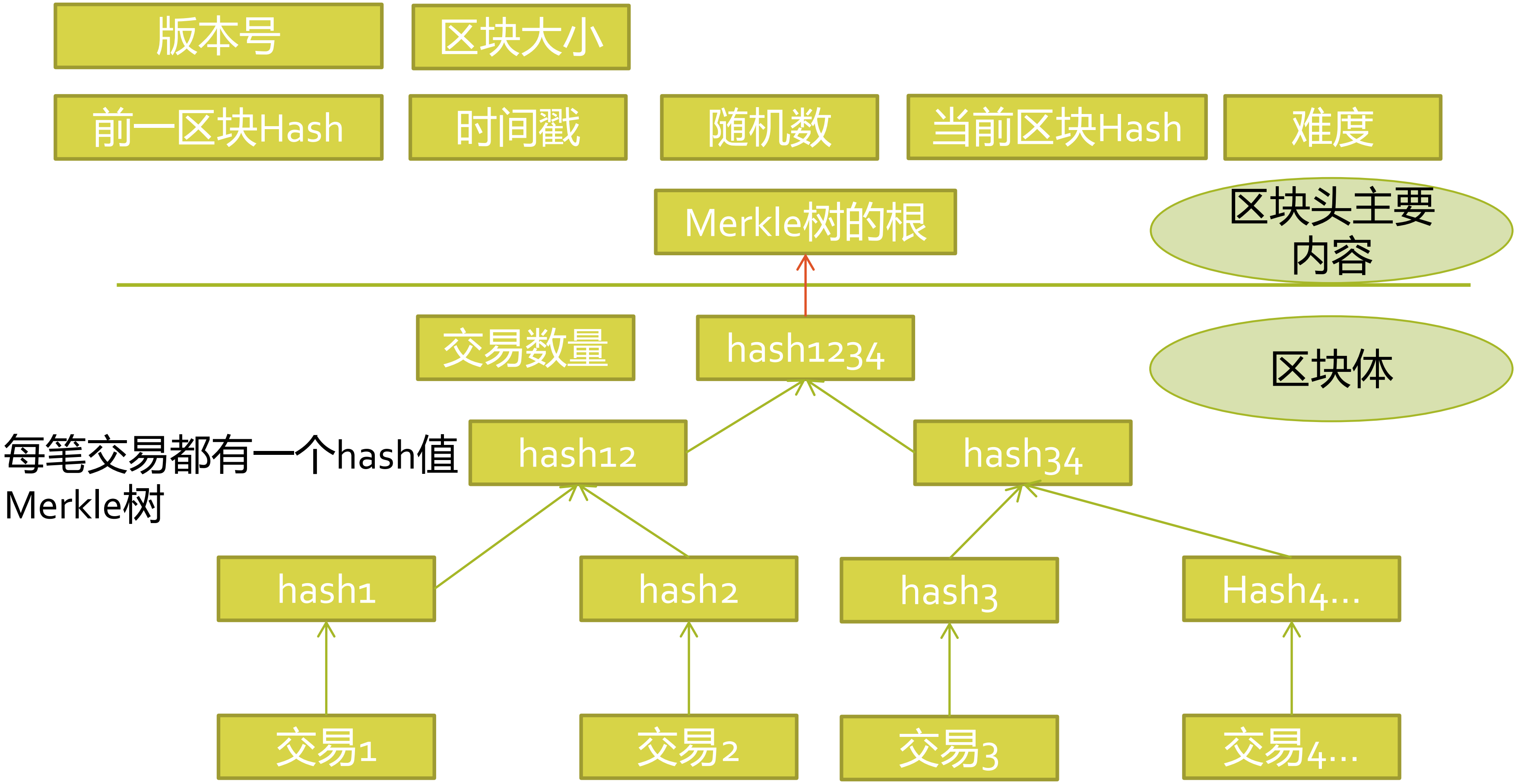
- 如果要做叛徒，攻击整个网络，需要付出相应的成本，而这个成本在比特币的PoW（Proof of Work 工作量证明）工作量共识机制下，就是要掌握整个网络50%以上的算力——换句话说，有50%以上的叛徒才行，而且大家可以想象一下这是多高的成本。
- 绝妙的是，如果真的掌握那么大的算力的话，用这些算力维护网络（诚实地挖矿）获得的收益其实会高于破坏网络。
- 聪明人们研究出了不少替代PoW的共识机制，如PoS权益证明，DPoS，PBFT算法。

很多区块链接在一起



- 将交易分组打包存储（目前一个block的大小为1M，一笔交易数据至少250字节，基本上每个block可以容纳近千条交易）；
- 区块和区块之间，通过前一个block的hash参数链接，形成链式的存储结构；

数据区块图-Block

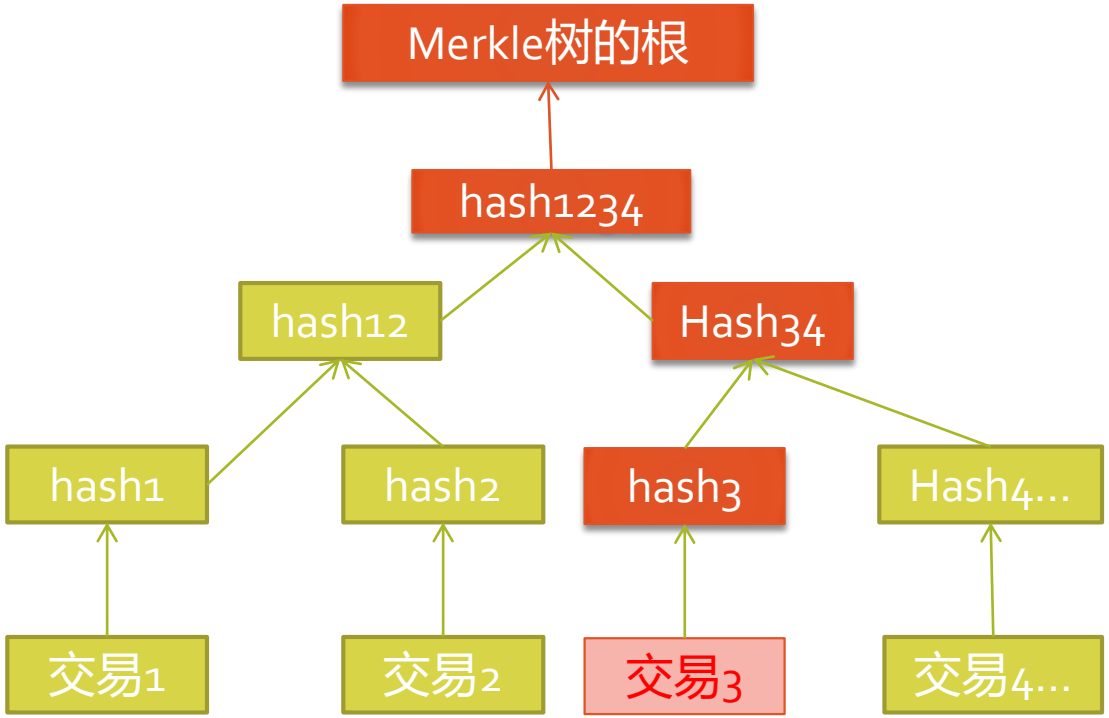


- Block由区块头和区块体构成；
- 区块头中含有一个Merkle根节点的字段，通过对区块体中所有交易记录，以二叉树的形式迭代地两两拼接，进行哈希操作，可以得到一个最终的哈希值，我们称之为Merkle根哈希；
- Merkle根哈希相当于是对区块中所有交易记录进行了一个快照，区块中交易记录的任意改动都可以通过比较Merkle根哈希而很容易地察觉。

Merkle树

- 每笔交易有一个hash值；
- 比如一个账单，把账单内容改了，hash值也改了，没人知道是否正确。
- 如果把多个交易的hash值关联到一起生成新的hash值就知道交易是否合法。
- 交易数据替换了之后，系统就会校验这个交易不合法。

这样，可以确保block数据的完整性。

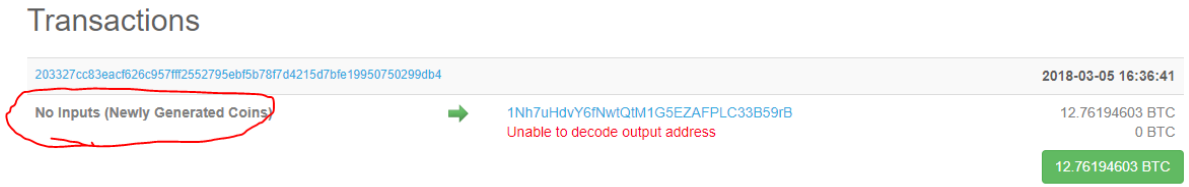


比特币账号模型UTXO

- UTXO（unspent transaction outputs）未花费的事务（交易）输出；
- 在比特币系统中，某笔资金的输入必须是另一笔未被使用的资金的输出；
- 比特币资产只有流水账，要获得当前余额，只能通过计算获得；

特殊情况：

- 创世块没有输入来源
- 挖矿的奖励没有输入来源



交易验证

- 验证来源是否合法（UTXO未花费的）；
- 数字签名是否合法；
- 网络节点只转发或者接受最先被监听的交易；

这些数据都会放在一个内存池中，也就是一个缓冲区；挖矿程序–从内存池中获取用来打包的交易数据，进行打包 SHA256(....)<TARGET

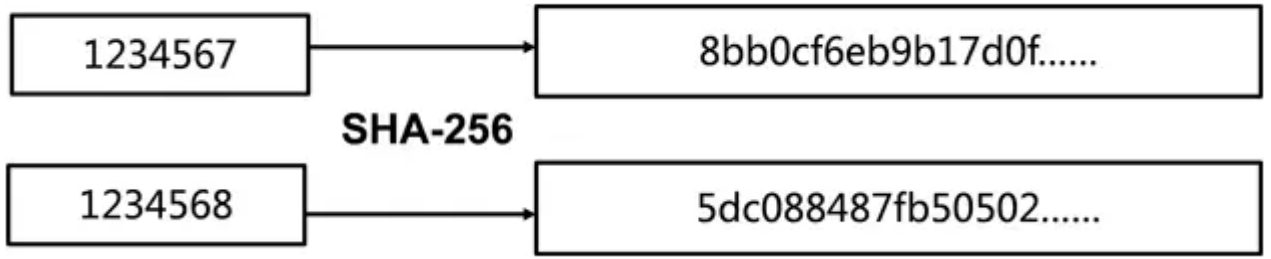
- 矿工挖出区块后，进行网络广播，传递给相连的节点；
- 节点收到后，还需要进行一系列的验证，比如block数据格式，时间戳等等；
- 交易发生的一刻起，比特币的交易数据就被盖上了时间戳；而当这笔交易数据被打包到一个区块中后，就算完成了一次确认；在连续进行6次确认之后，这笔交易就不可逆转了；

P2P网络

- Peer to peer network对等网络，也可以理解为点对点。
- 比特币的网络节点分为全节点和轻量级节点，全节点存储了所有的区块数据。
- 轻量级节点则只需要存储体积相对很小的区块头，实现简易支付验证（SPV-Simplified Payment Verification）。
- 一个区块头大概80字节大小，假设每10分钟生成一个新的区块，那么每年只会产生4.2MB的头信息数据。

哈希（Hash）加密

- 只要是相同的数据输入，一定会得到相同的结果，如果输入数据稍有变化，将得到一个千差万别的结果；
- SHA256还是一个单向不可逆的算法，即根据一个输入数算SHA256的结果很容易，但根据SHA256的结果反算输入数几乎是不可能。



非对称加密算法

- 比特币主要用了ECDSA（Elliptic Carve Digital Signature Algorithm），也就是椭圆曲线签名算法

这个算法有两个特性，注意这两点至关重要：

- a.只要知道私钥，可以算出相应的公钥；
- b.你用私钥签名过的东西，可以用公钥算一下是不是你签的；

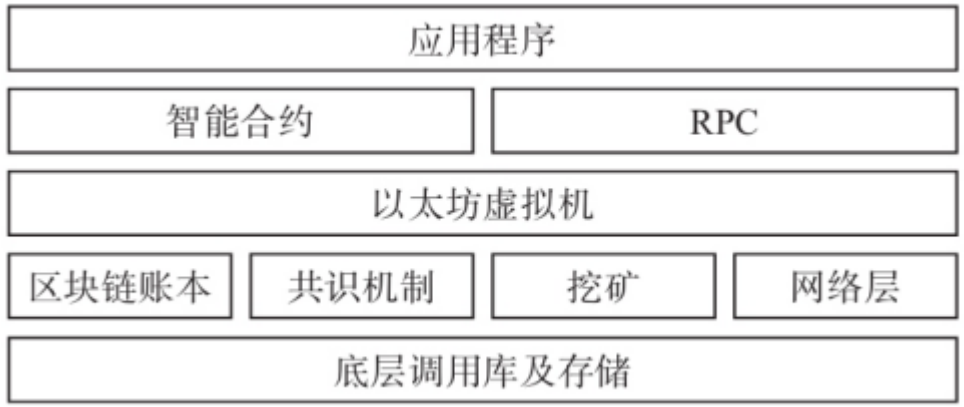
以太坊=区块链+智能合约

- 比特币仅仅设计为一个加密数字货币系统，是区块链技术的一个具体应用；
- 区块链2.0，可以在以太坊上编写智能合约应用程序，将区块链技术应用于数字货币以外的领域之中；
- 高效的共识机制；
- 具有图灵完备性；
- 支持智能合约，可以实现各种复杂商业逻辑；

长得像马云的90后☺

- 创始人：Vitalik Buterin（V神）
- 以太坊中文社区：http://ethfans.org/ ETHFANS
- 以太坊从诞生到2014年5月，全球已有200多个以太坊应用诞生，如TRIPIO项目白皮书。

以太坊的组成结构



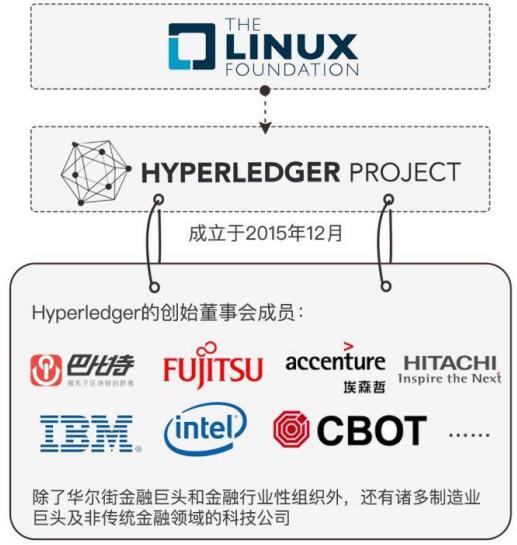
- 以太坊中的智能合约是运行在EVM(Ethereum Virtual Machine)虚拟机上的；
- 合约存储在以太坊的区块链上，编译为EVMC字节码；
- 以太坊具有账号的概念，可以直接获得当前的余额，比特币只有流水账；
- 以太坊的源码是维护在GitHub上的：https://github.com/ethereum；

Tripio 去中心化旅行服务方案

产品方案：

- Tripio 项目基于以太坊的智能合约开发。
- 以太坊是一个基于共识的、可扩展的、标准化的、特性完备的、易于开发的和协同的基础区块链。
- 通过以太坊内置的图灵完备的虚拟机技术，Tripio 重新定义交易方式和状态转换函数规则，构建旅行服务中的各种智能合约。
- 白皮书：http://trip.io/

超级账本Hyperledger



- 成立时间：2015年12月
- 是一个由Linux基金会管理的开源区块链项目, 由IBM、Intel、[illegible]等公司领衔参与；
- 是Linux基金会有史以来发展最快的开源项目；
- 百度金融加入Hyperledger超级账本 成为核心董事会成员，还有万达、腾讯等等；
- 目的是建立一个跨产业的、开放的、分布式账本技术平台，面向企业级开发；
- 开发源码：https://github.com/hyperledger

Hyperledger Project

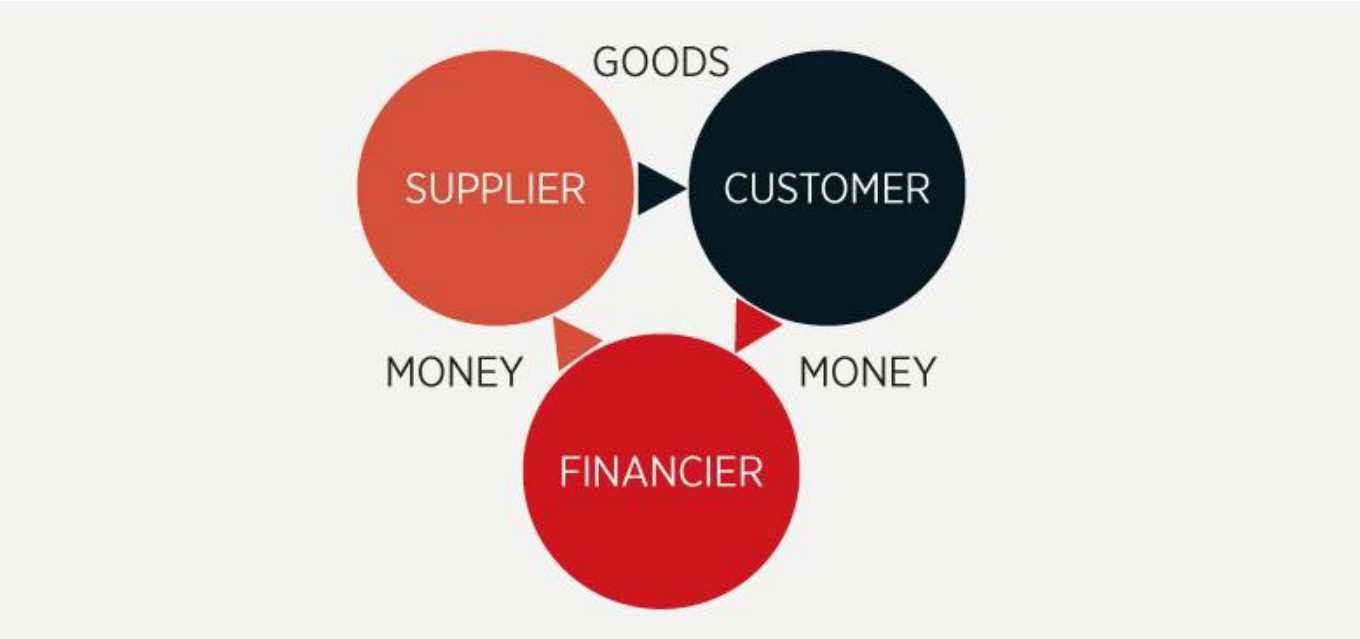
https://www.hyperledger.org

Fabric分布式账本解决方案

- Fabric是HyperLedger上的区块链项目之一，分布式账本，使用智能合约；
- 适用于构建企业间的联盟链；
- 需要许可授权，身份鉴定；
- Fabric组织的成员可以通过一个Membership Service Provider（成员服务提供者即MSP）来注册；
- Fabric和比特币、以太坊系统的区别

	比特币	以太坊	Fabric
加密数字货币	比特币	以太坊 / 合约代币	不支持
网络权限	完全公开	完全公开 / 许可	许可
交易事务	匿名	匿名 / 私有	公开 / 机密
共识机制	PoW（工作量证明）	PoW（工作量证明）	PBFT（实用拜占庭容错）
智能合约	不支持	支持	支持

供应链金融



- 业务痛点是什么？
- 商家资金周转率？
- 银行担心有风险？
- 如何多赢？

供应链金融模式

- 应收账款融资模式
  卖方将AR作为抵押，在线申请银行的信贷支持，解决资金难题；
- 电子订单融资模式
  核心企业向供应商发出采购信息，供应商确认；银行依据电子订单为供应商授信，解决资金难题；
- 存货融资模式
  仓储方存货监管，企业出具电子仓单向银行申请信贷支持；

供应链金融场景分析

- 参与方：银行金融机构、核心企业、供应商、经销商；
- 使用区块链技术的分布式共享账本，实现跨企业之间的信息流、物流和交易信息共享；
- 通过信用令牌（Credit Token）流转，而非现金流转，降低资金成本，减少对现金的依赖；
- 增加资金的流动性，提升资金的利用率；

Credit Token流转过程

- 供应商根据AR凭证提出AR上链；
- 核心企业确认AR真实性，将供应商的AR打包上链，同时上支付Credit Token（数字资产）；
- 供应商获得核心企业背书的Credit Token；
- 供应商根据Credit Token 到金融机构获取一定的提现率；


Thanks!