北京大学
PEKING UNIVERSITY

区块链技术与高校应用场景浅析

王博 北京大学计算中心

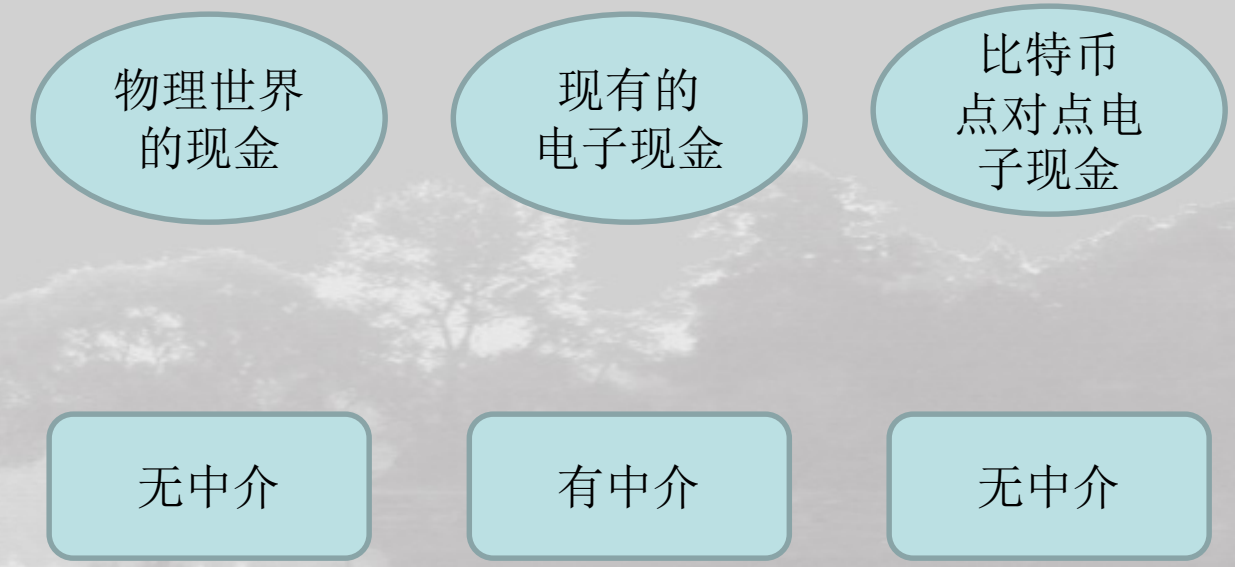
2019年11月13日

目录

- 区块链1.0 – 比特币
- 区块链2.0 – 以太坊对比特币的改进
- 区块链3.0
- 应用场景

比特币企图解决的问题

- 创造在数字世界中可用的电子现金，它可以点对点（个人对个人）交易，不需要任何中介参与



比特币原理：基础元素

- 分布式账本、去中心网络
  - 账本中央私有 =》公开分布在所有参与者手中（分布式网络）
  - 记录余额 =》记录交易（流水），根据初始状态推算余额

- 加密数字货币
  - 非对称加密：私钥签名（本人持有）、公钥验证（全体参与者持有）

$$Sign(\text{信息}, \text{私钥}) = \text{电子签名}$$

$$Verify(\text{信息}, \text{电子签名}, \text{公钥}) = \text{真/假}$$

  - Sign（“老张转账给老李10个比特币”，张三的私钥）= 电子签名，把签名放在这条转账信息的后面，这个签名就能保证此消息是老张发送的
  - 具体算法就是两次SHA256，特点是信息改动一点，签名改动巨大

比特币原理：挖矿（发起转账）

- 1、创世块规则：奖励老张50个币
- 2、老张给老李转10个币（标识代号、Sign签章、记录来源）
- 3、老李或网络上的任何人，都可以使用Verify方法验证该笔转账是否由老张本人发起（基于老张的私钥）
- 4、谁来验证老张有余额支付这一笔转账呢 —— 挖矿的工作

本页及后面几页挖矿原理说明图片及描述参考自：https://www.zhihu.com/question/20792042

$$Sign(\text{信息}, \text{私钥}) = \text{电子签名}$$

$$Verify(\text{信息}, \text{电子签名}, \text{公钥}) = \text{真}/\text{假}$$

比特币原理：挖矿（工作量证明）

- 5、每笔交易的发起人将交易单广播给全网络（所有矿工）

- 6、矿工定期将收集到的交易单填写到一张新的账簿页（Block）的“交易清单”一栏，将当前账簿最后一页的编号抄写到“上一页签章”一栏。随机生成一个“幸运数字”，最后将这页盖签名章（Sign），这页新的账簿纸就算完成了。
  - 矿工的工作量：规定前10位数均为0才有效。因此须不停修改唯一可变字段“幸运数字”，应用签章算法，直到满足条件。
  - 旷工的动力：每一页账簿的交易清单第一条交易为“系统给这个矿工奖励（新生成）50个比特币”。


```
20  class CBlockHeader
21  {
22  public:
23      // header
24      int32_t nVersion;
25      uint256 hashPrevBlock;
26      uint256 hashMerkleRoot;
27      uint32_t nTime;
28      uint32_t nBits;
29      uint32_t nNonce;
```

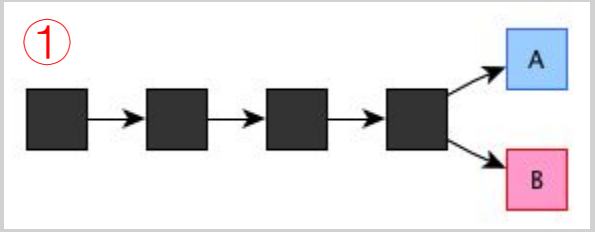
比特币的github地址：https://github.com/bitcoin/bitcoin

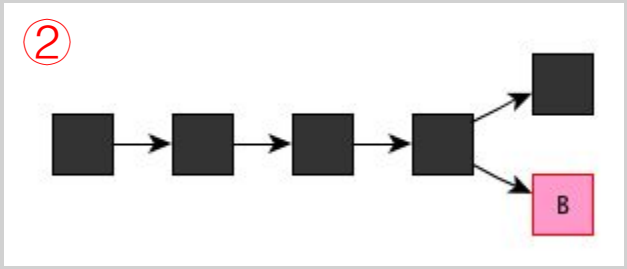
比特币原理：挖矿（Block确认）

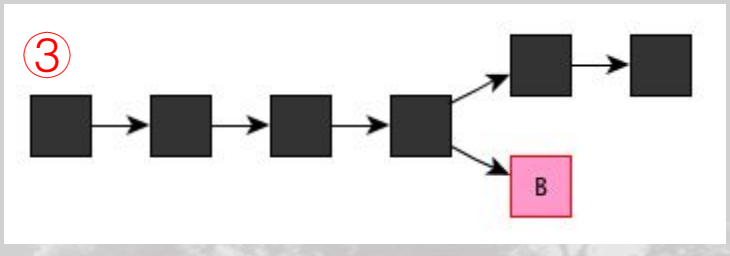
- 7、 任何矿工收到其他矿工送来的新账簿页时，立即停下手里的挖矿工作（即使进行了99.9%），进行账簿页确认：
  - 账簿页的签章有效：公钥Verify函数
  - 账簿页的前一页有效： “上一页签章”= 本地保存的最后一页签章
  - 交易清单有效（转账发起人有足够的余额）：交易信息里包含这笔钱是如何来的，还包含了记录来源交易的账单页编号（签章）。须向前回溯确认来源（转账或挖矿奖励）。交易列表中第一笔是系统奖励给生成这页账簿的矿工的50个，这笔交易大家都默认承认。
- 8、完成上述所有验证，将这张账簿纸并入该矿工的主账簿，继续下一页的计算。
- 9、对于挖到当前新页的矿工来说，如果后面收到其他矿工送来的新账簿页，其“上一页签章”为自己之前送出去的账簿页，则基本表示其工作成功被认可并得到了50个比特币奖励。
- 10、新账簿页被确认时，其中的交易也同时被确认，收款人可关注涉及自身的交易。

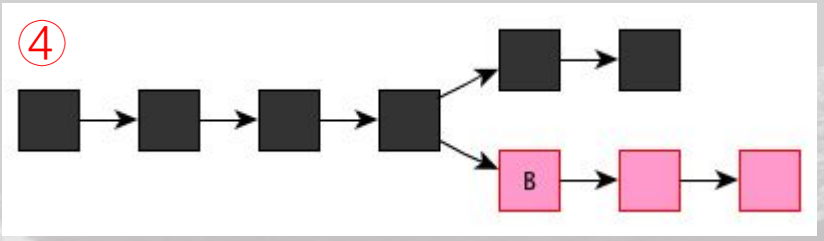
问题1：同时收到两份合法的账簿页

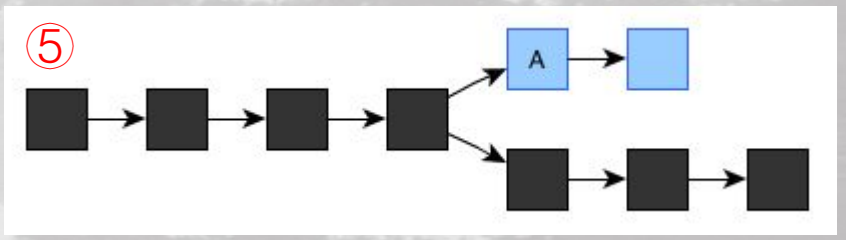
- 树形链









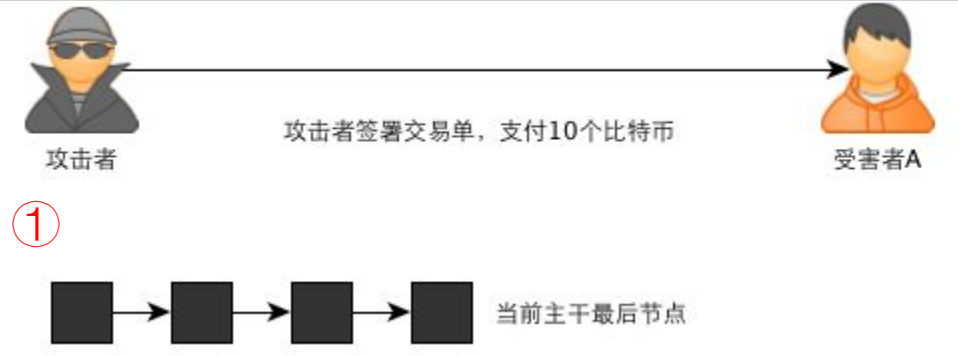


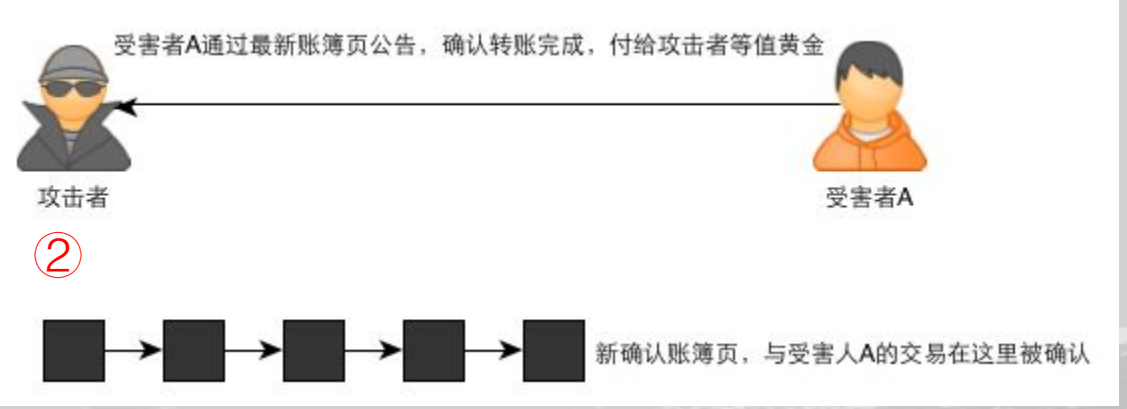
- 局部某一时刻可能存在不一致，但大方向是一致的，小分支会很快被淹没在历史中。

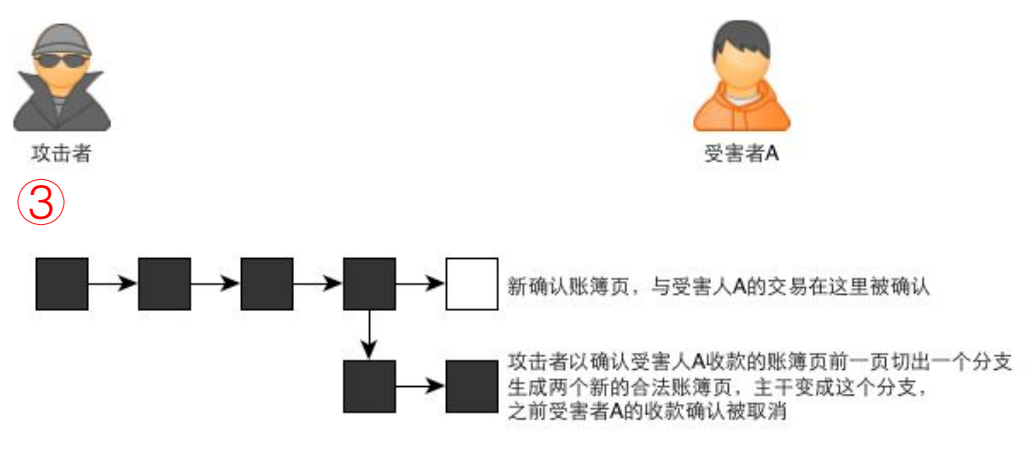
问题2：如果矿工伪造账簿怎么办

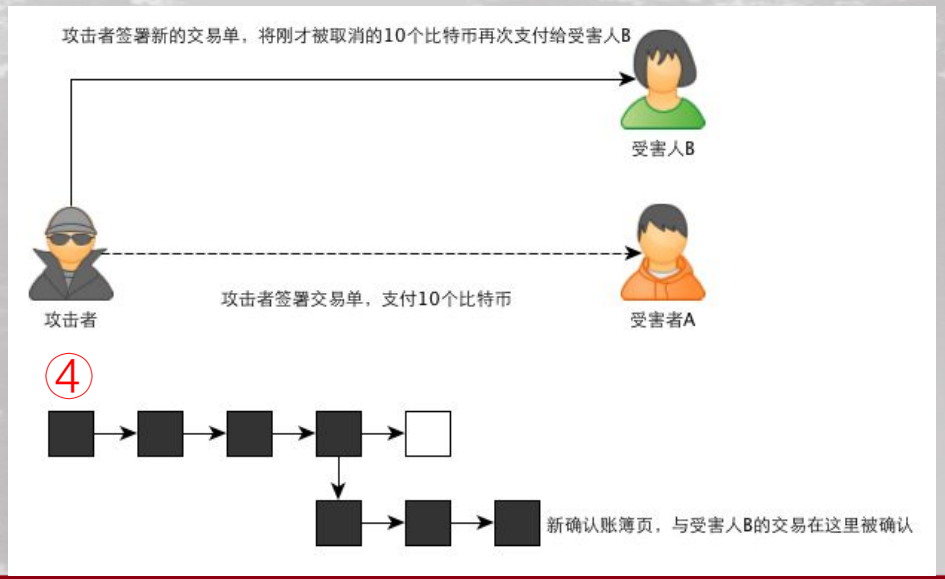
- 1、基于Sign机制，没有人能伪造他人身份进行付款
- 2、诚实的矿工不会承认不合法的交易（如某笔交易付款方余额不够）
- 3、只有一种可能的攻击行为：收款人确认收款后，付款人从另一条分支上建立另外的交易单，取消之前的付款，将同一笔钱再次付款给另一个人（即所谓的double-spending问题）

问题2：如果矿工伪造账簿怎么办









问题2：如果矿工伪造账簿怎么办

- 收款人不要在公告挂出时立即确认交易完成，而是等待各个矿工再挂出6张确认账簿
- 之前设定复杂的Sign签章规则，正是为了防御这一点。新账单页的生成须话费大量的工作量计算不同的幸运数字，那么攻击者在落后6页的情况下从另一个分支赶超当前主分支是非常困难的
- 只有掌握全网51%计算能力的黑矿工理论上才能完成伪造，收益远不如做良民挖矿。

问题3：比特币会不会严重通货膨胀

- 比特币规定每生成一页账簿，奖励50个比特币，后面每当账簿增加21,000页，奖励就减半
- 等账簿达到6,930,000页后，新生成账簿页就没有奖励了。此时比特币全量约为21,000,000个，这就是比特币的总量，所以不会无限增加下去。
- 当前奖励是12.5个比特币。

问题4：没有奖励后没人做矿工了？

- 没有奖励后，就没人做矿工了，岂不是没人帮忙确认交易了？

- 到时，矿工的收益会由挖矿所得变为收取手续费。例如，你在转账时可以指定其中1%作为手续费支付给生成账簿页的矿工，各个矿工会挑选手续费高的交易单优先确认。

问题5：矿工越多比特币生成越快？

- 不会。有难度系数！控制在10分钟左右生成一个新页，2周左右调整一次难度系数。

- 每创建2016个块后将计算新的难度，此后的2016个块使用新的难度。计算步骤如下：
  - 1、找到前2016个块的第一个块，计算生成这2016个块花费的时间。
    即最后一个块的时间与第一个块的时间差。时间差不小于3.5天，不大于56天。
  - 2、计算前2016个块的难度总和，即单个块的难度x总时间。
  - 3、计算新的难度，即2016个块的难度总和/14天的秒数，得到每秒的难度值。
  - 4、要求新的难度，难度不低于参数定义的最小难度。

问题6：公开的账簿，如何保护隐私

- 虽然每个人的代号是匿名的，但如果泄露了某个人的代号，账簿又是公开的，岂不是他的所有账目都查出来了？
- 确实是这样的。例如你要和某人交易，必然要要到他的代号才能填写交易单。因为收款人一栏要填入那人的代号。不过中本聪说可以提供无限制的保密印章，建议每一次交易用不同的保密印章，这样查账簿就追查不到同一个人的所有账目了。

真实的比特币信息

Latest blocks

View more

Height	Hash	Mined	Miner	Size
602686	0..a269d84013a8004f16401479bf6aced54fe098b...	15 seconds	F2Pool	1,240,022 bytes
602685	0..1146a49a420448c585f1c7b08bd1563b57a704...	19 minutes	BTC.com	1,252,738 bytes
602684	0..146fad7a81de7446989c414e9fd0a21f4285256...	37 minutes	Unknown	880,710 bytes
602683	0..67d8f244ca214d0498ba6da07b6fdcd36f0968...	48 minutes	Unknown	668,846 bytes
602682	0..59f1264f197ab974b4341dadbe6b39e88caba3c...	55 minutes	Unknown	1,006,258 bytes
602681	0..c9802908bbbfbc745e43b0649a9dafca408fe8...	1 hour	AntPool	1,264,616 bytes
602680	0..a54f9eda42711faca96f143747448e71c5d386af...	1 hour	F2Pool	548,758 bytes
602679	0..f1d5541a797ac7332a3c5c44b33ba5ed515833...	1 hour	ViaBTC	45,940 bytes
602678	0..3e05c5292de451679fbc0dc667011ff309af36c...	1 hour	ViaBTC	777,098 bytes
602677	0..7eb04119b7ebd25a4c92e3ecd03f4f72b6b6f52...	2 hours	Poolin	1,161,206 bytes
602676	0..12d1c2654803b705a28f25ac2f6721c74f0ec0b...	2 hours	Unknown	1,271,238 bytes
602675	0..bf8e93d2f9825d0af023ec428e2d1078af2e653...	2 hours	Poolin	1,516,833 bytes
602674	0..46a6f3e5d5c636309951d66c52a97035a80dfe...	2 hours	Unknown	1,397,330 bytes
602673	0..c7c497bb48e265bbc6a3502ef8466d2d14e000...	2 hours	Poolin	1,264,992 bytes
602672	0..9c2038627af636fe05b4a516cafd25a3bfc0dbd...	2 hours	F2Pool	1,251,990 bytes

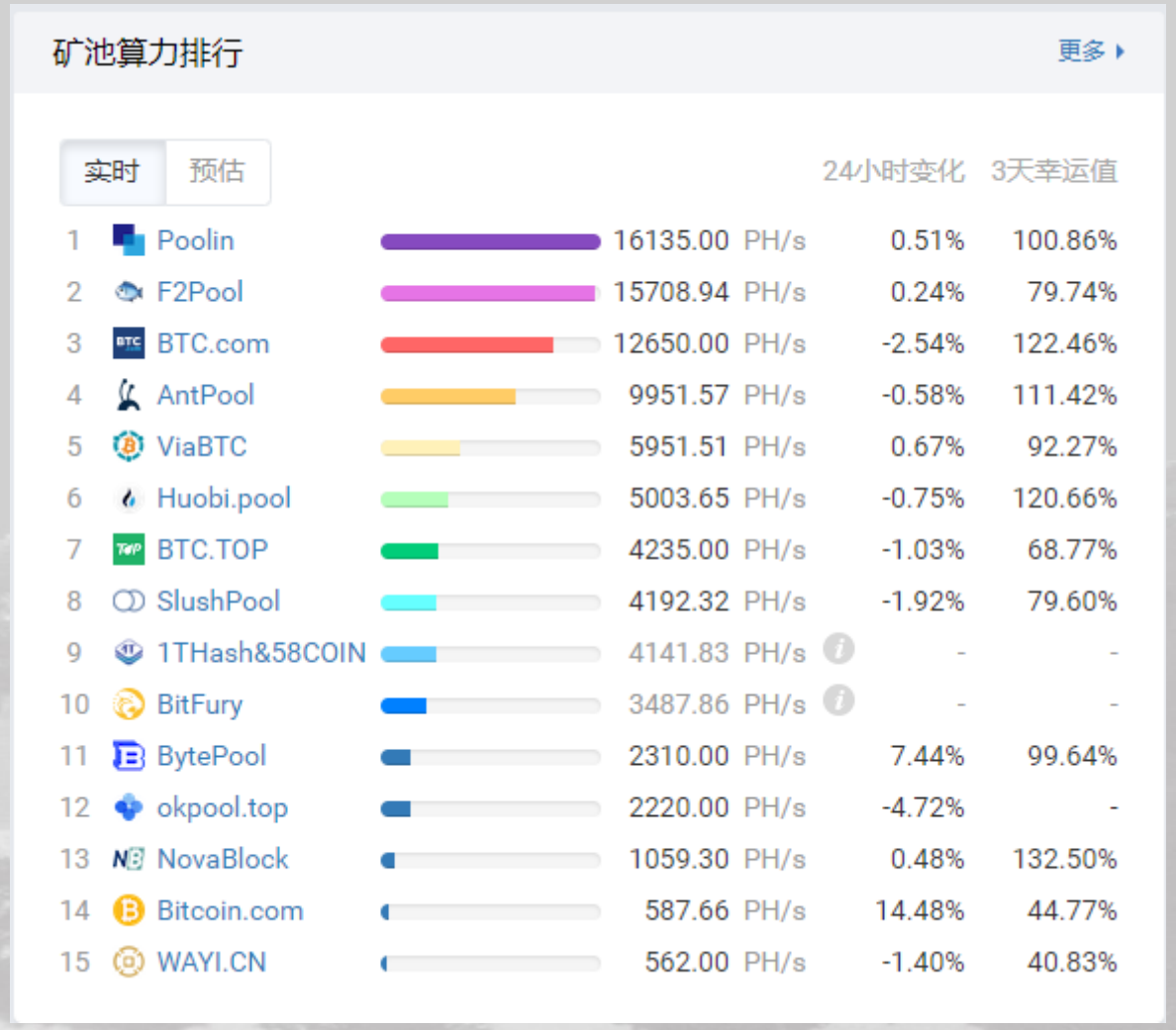
Block #600987

Summary	
Number Of Transactions	2937
Output Total	7,638.10527717 BTC
Estimated Transaction Volume	598.5583069 BTC
Transaction Fees	0.21472424 BTC
Height	600987 (Main Chain)
Timestamp	2019-10-25 12:31:50
Received Time	2019-10-25 12:31:50
Relayed By	F2Pool
Difficulty	13,691,480,038,694.45
Bits	387223263
Size	1283.718 kB
Weight	3998.394 kWU
Version	0x20C00000
Nonce	1493741200
Block Reward	12.5 BTC

Hashes	
Hash	00000000000000000011dfb6f12c0bac39cb919769fdfc3387f1920d5f8df10c
Previous Block	00000000000000000058bfc896b97558a425e7bcb35c8a0205c573249e0148
Next Block(s)	00000000000000000003786c953233a55e6e8ba97c47ec4df7959d79d4f67671
Merkle Root	25ea6853035235a8167aea06c99564212934342e2e4be930e304f12b716b0699

https://www.blockchain.com/explorer

矿池



矿池算力排行 更多

	实时 / 预估			24小时变化	3天幸运值
1	Poolin	16135.00	PH/s	0.51%	100.86%
2	F2Pool	15708.94	PH/s	0.24%	79.74%
3	BTC.com	12650.00	PH/s	-2.54%	122.46%
4	AntPool	9951.57	PH/s	-0.58%	111.42%
5	ViaBTC	5951.51	PH/s	0.67%	92.27%
6	Huobi.pool	5003.65	PH/s	-0.75%	120.66%
7	BTC.TOP	4235.00	PH/s	-1.03%	68.77%
8	SlushPool	4192.32	PH/s	-1.92%	79.60%
9	1THash&58COIN	4141.83	PH/s	-	-
10	BitFury	3487.86	PH/s	-	-
11	BytePool	2310.00	PH/s	7.44%	99.64%
12	okpool.top	2220.00	PH/s	-4.72%	-
13	NovaBlock	1059.30	PH/s	0.48%	132.50%
14	Bitcoin.com	587.66	PH/s	14.48%	44.77%
15	WAYI.CN	562.00	PH/s	-1.40%	40.83%

https://btc.com/

区块链1.0

应用层	实现转账与记账功能	
激励层	发行机制	分配机制
共识层	POW工作量证明	
网络层	P2P网络	广播机制 验证机制
数据层	Block Hash	Chain 梅克尔树 数字签名 非对称加密

应用层	比特币	加密数字货币
应用协议层	比特币协议	发行与转移
通用协议层	区块链	分布式账本、去中心网络

中本聪的论文： Bitcoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf

目录

- 区块链1.0 – 比特币
- 区块链2.0 – 以太坊对比特币的改进
- 区块链3.0
- 应用场景

以太坊

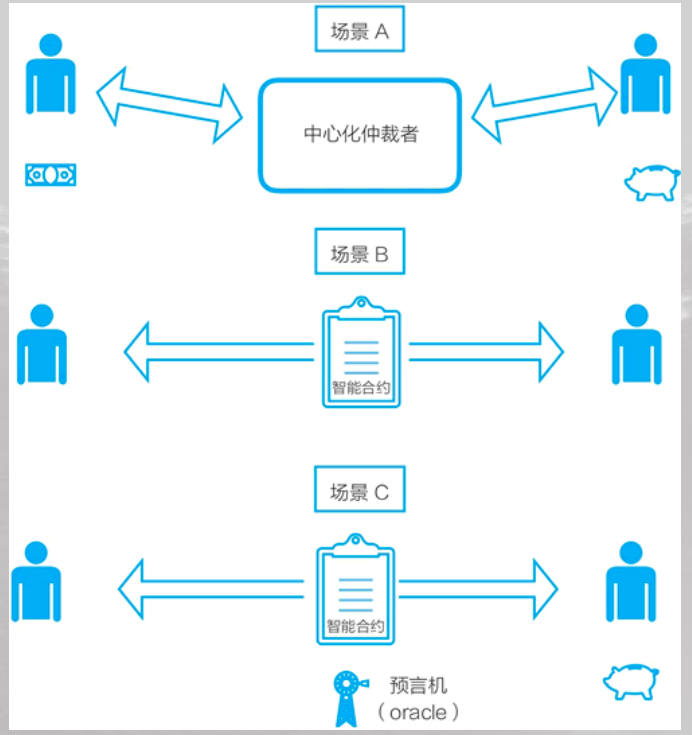
- 比特币的缺点
  - 缺少图灵完备性（lack of turing-completeness）
  - 价值盲（value-blindness）
  - 缺少状态（lack of state）
  - 区块链盲（blockchain-blindness）
- 以太坊
  - 一个图灵完备的脚本语言（Solidity）
  - 一个运行智能合约的虚拟机（EVM）
  - 一系列标准化的用于不同类型通证的智能合约

智能合约及通证

- 通证: 可流通的加密数字权益凭证
  - 数字形式凭证
  - 基于加密证据
  - 可流通
  - 可编程

- 资产类型
  - 链上资产、线上资产、线下资产

- 通证经济体
  - 链，区块链技术的落实。
  - 通证，通证的建立、分配与管理。
  - 社群，用户社区与投资社区等以价值共识形成的社群



淘宝购物

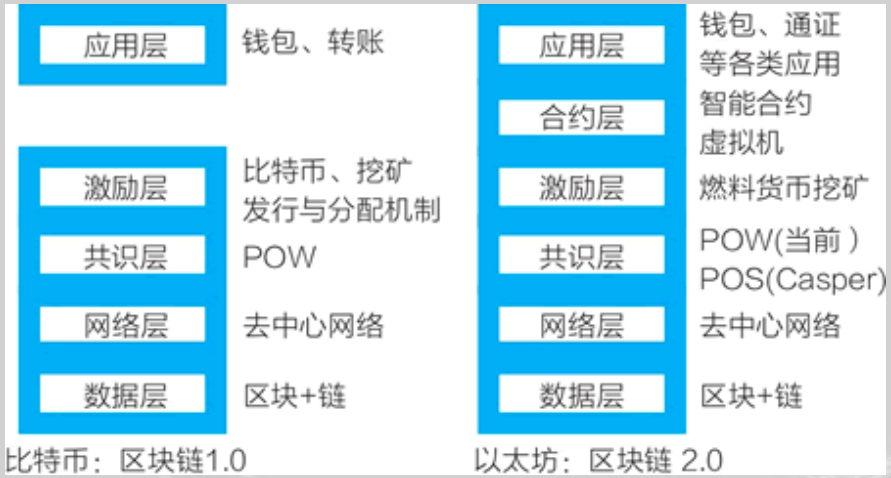
ERC20（可互换）
ERC721（不可互换）

买房

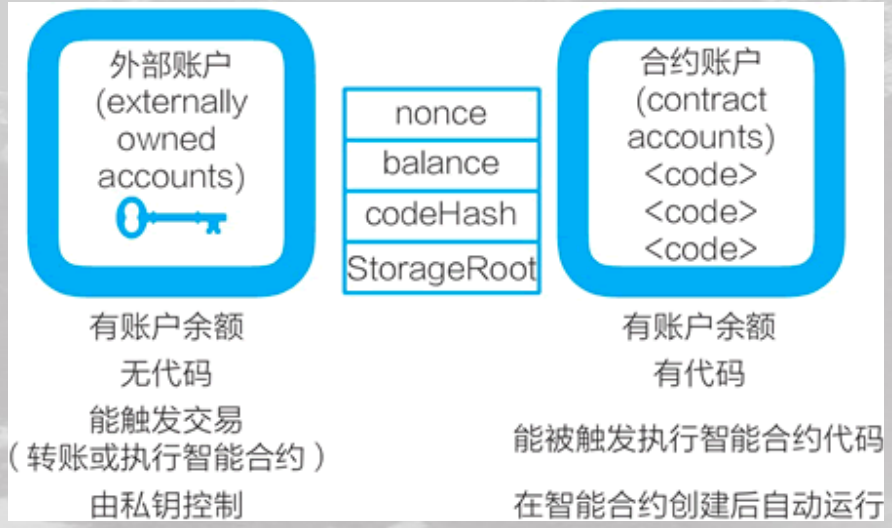
来源：C语言中文网的系列教程《区块链技术快速入门教程》

比特币 vs 以太坊

- 比特币与以太坊分层对比



- 以太坊加入了账户的概念



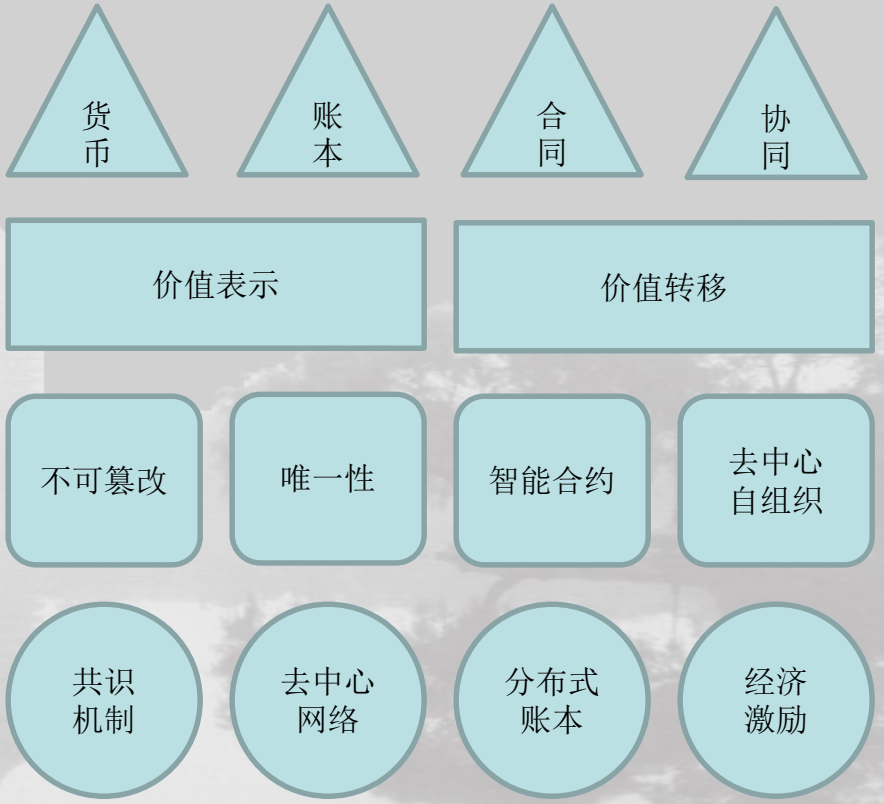
图片来源：C语言中文网的系列教程《区块链技术快速入门教程》

以太坊 —— The DAO众筹事件与以太坊分叉

- 事件
  - 2016 年 4 月 30 日，The DAO 项目在以太坊中进行代币众筹，到 5 月 28 日，这个项目筹集了 1150 万个以太币，以当时以太币的价格计算价值超过 1.5 亿美元，是当时最大金额的众筹。
  - 但是，在 2016 年 6 月 9 日，有开发者发现 The DAO 的智能合约存在漏洞，他还在开源平台上提交了修复代码。
  - 6 月 17 日，黑客利用漏洞向一个匿名的地址转移走了项目众筹来的 360 万枚以太币，占到总数的 1/3。
- 解决
  - 维塔利克（人称“V神”）提出了硬分叉方案（即从某个区块开始以太坊区块链不向前兼容），从而把 The DAO 众筹来的以太币夺回来，转移到一个恢复地址上，再还给参与众筹的人。在社区中获得了 85% 的投票支持，在 2016 年 7 月 21 日分叉成功
  - 一支是新的，叫以太坊（其代币叫 ETH）
  - 一支叫以太坊经典（Ethereum Classic，其代币叫 ETC）

区块链总结

- 不可篡改，不可复制的唯一性，智能合约，去中心自组织或社区化



信息传递 => 价值传递

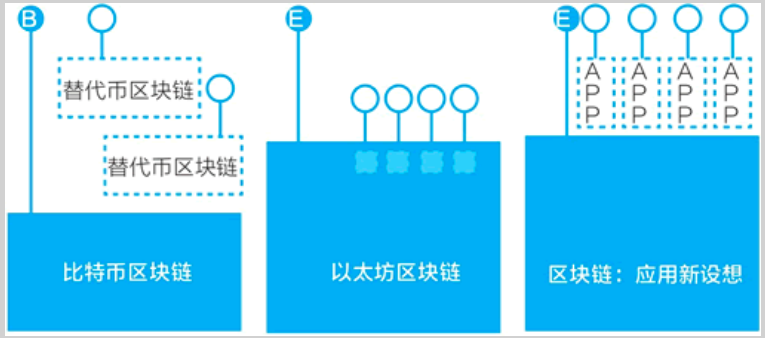
信任的机器

目录

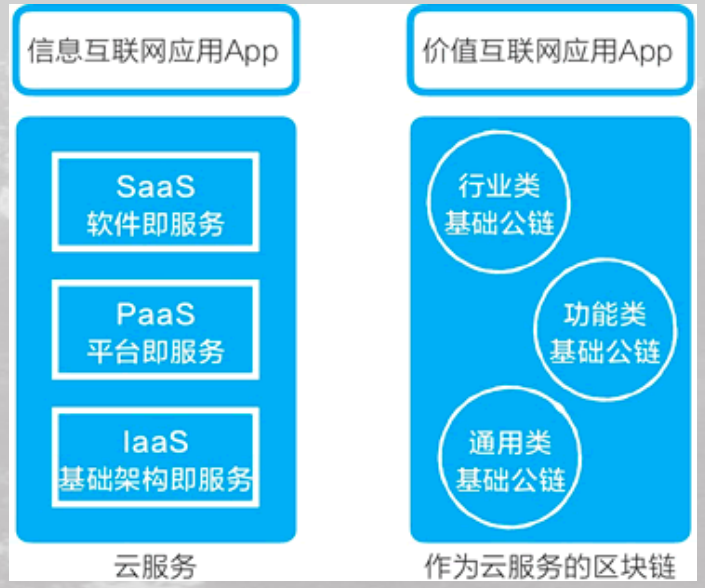
- 区块链1.0 – 比特币
- 区块链2.0 – 以太坊对比特币的改进
- 区块链3.0
- 应用场景

区块链未来的发展方向

- 走向应用



- 与云服务的类比



图片来源：C语言中文网的系列教程《区块链技术快速入门教程》

蚂蚁区块链产品大图

蚂蚁金服 ANT FINANCIAL

BaaS Marketplace & Solution

链上金融：跨境汇款 | 供应链金融 | 交易所 | 票据 | 保险

链上零售：跨境物流 | 商品溯源 | 药品溯源 | 广告营销

链上生活：医疗健康 | 租房租赁 | 版权 | 票据 | 公益 | 合同

安全管理

- 实名认证
- 抗DDoS攻击
- 密钥管理服务
- 访问控制
- IoT安全
- 操作审计

BaaS Plus

可信存证	通用溯源	实人认证
企业认证	跨链服务	智能合约安全检查

区块链服务 BaaS Core

联盟管理	智能合约管理	SGX/TEE	安全隐私	浏览器与监控	业务视图
节点管理	用户管理	证书密钥管理	日志与审计	链下数据同步	大文件处理

Hyperledger Fabric

AntChain
蚂蚁自研金融级区块链平台

合约工具	Cloud IDE	隐私保护
密码学安全	可信执行环境	FDMT存储
异步共识	合约与虚拟机	跨链技术

企业以太坊 Quorum

容器集群 Kubernetes

云资源层

弹性公网IP	负载均衡SLB	云数据库	容器镜像服务	云解析DNS	云企业网CEN
云服务器ECS	裸金属服务器	弹性块存储	文件存储NAS	虚拟专有网络VPC	高速通道

云资源管理平台（阿里云飞天平台）

计算资源	存储资源	网络资源

基础设施层

公共云　专有云

运维管理

- 云监控
- 资源编排
- OpenAPI Explorer
- 日志服务
- 数据库管理
- 计费管理

区块链的发展道路

- 区块链2.0之上的改进方向
  - 性能：POW（工作量证明法）、POS（权益证明法）、DPOS （股权代理人共识）、 RPCA（基于PAXOS的瑞波共识算法 ）等
  - 架构：云服务生态

- 五条路径
  - 通用类基础公链：以太坊、EOS、小蚁（NEO）、新经币（XEM）等
  - 功能类基础公链：专用于物联网的 IOTA、投票类的Follow My Vote、数字内的容Steem和币乎、专用于数字资产交换的比原链（Bytom）
  - 行业类基础公链：保险、供应链金融、游戏、政务等
  - 联盟链开源软件：超级账本HyperLedger （IBM 最初提出与研发，现在由开源软件组织 Linux 基金会管理）
  - 基础服务：跨链协议的云服务区块基石（ArcBlock）、定在做“区块链世界的连接器”的梵塔网络（Penta）、星际文件系统（InterPlanetary File System，IPFS）

目录

- 区块链1.0 – 比特币
- 区块链2.0 – 以太坊对比特币的改进
- 区块链3.0
- 应用场景

高校应用

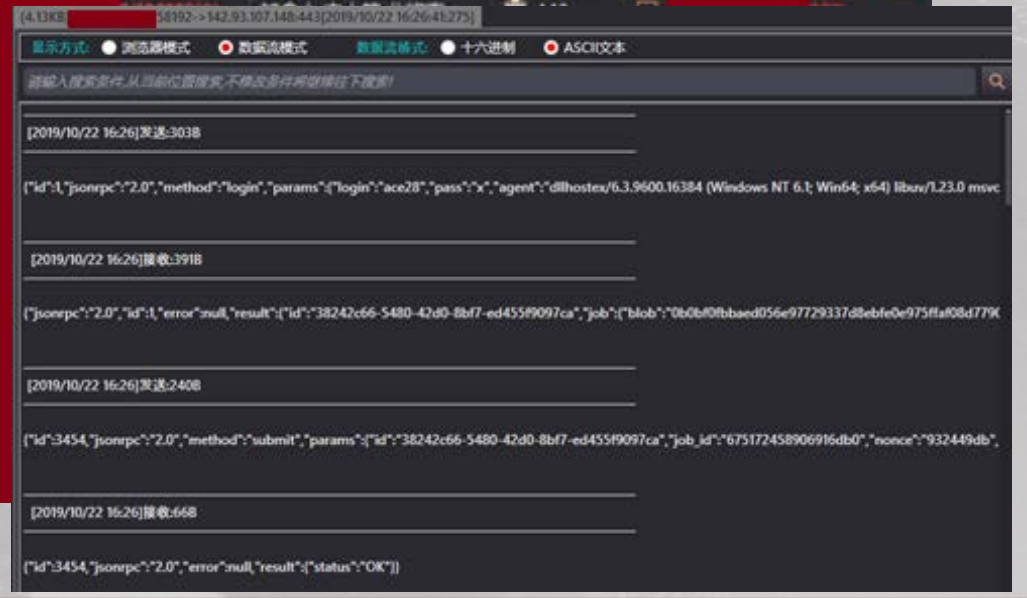
- 防
- 用

防：各种挖矿木马、病毒

触发条件	IP地址	应用	网段	IP属...	源IP地址	源端口	源IP地址地理位置	目标IP地址	目标端口	目标IP地址地理位置
请求域名：mine.moneropool.com,mine.moneropool.com	N/A	N/A	N/A	N/A	[redacted]122	53	中国,北京,北京,海淀,教...	[redacted].217	42338	中国,北京,北京,海淀,教...
请求域名：mine.moneropool.com,mine.moneropool.com	N/A	N/A	N/A	N/A	[redacted]122	53	中国,北京,北京,海淀,教...	[redacted].217	42980	中国,北京,北京,海淀,教...
请求域名：mine.moneropool.com,mine.moneropool.com	N/A	N/A	N/A	N/A	[redacted]122	53	中国,北京,北京,海淀,教...	[redacted].217	51316	中国,北京,北京,海淀,教...
请求域名：mine.moneropool.com,mine.moneropool.com	N/A	N/A	N/A	N/A	[redacted]122	53	中国,北京,北京,海淀,教...	[redacted].217	51316	中国,北京,北京,海淀,教...
请求域名：mine.moneropool.com,mine.moneropool.com	N/A	N/A	N/A	N/A	[redacted]122	53	中国,北京,北京,海淀,教...	[redacted].217	58624	中国,北京,北京,海淀,教...
请求域名：mine.moneropool.com,mine.moneropool.com	N/A	N/A	N/A	N/A	[redacted]122	53	中国,北京,北京,海淀,教...	[redacted].217	54676	中国,北京,北京,海淀,教...
请求域名：mine.moneropool.com,mine.moneropool.com	N/A	N/A	N/A	N/A	[redacted]122	53	中国,北京,北京,海淀,教...	[redacted].217	58691	中国,北京,北京,海淀,教...
请求域名：mine.moneropool.com,mine.moneropool.com	N/A	N/A	N/A	N/A	[redacted]122	53	中国,北京,北京,海淀,教...	[redacted].217	58691	中国,北京,北京,海淀,教...
请求域名：mine.moneropool.com,mine.moneropool.com	N/A	N/A	N/A	N/A	[redacted]122	53	中国,北京,北京,海淀,教...	[redacted].217	52650	中国,北京,北京,海淀,教...
请求域名：mine.moneropool.com,mine.moneropool.com	N/A	N/A	N/A	N/A	[redacted]122	53	中国,北京,北京,海淀,教...	[redacted].217	52650	中国,北京,北京,海淀,教...
请求域名：mine.moneropool.com,mine.moneropool.com	N/A	N/A	N/A	N/A	[redacted]122	53	中国,北京,北京,海淀,教...	[redacted].217	45688	中国,北京,北京,海淀,教...
请求域名：mine.moneropool.com,mine.moneropool.com	N/A	N/A	N/A	N/A	[redacted]122	53	中国,北京,北京,海淀,教...	[redacted].217	45688	中国,北京,北京,海淀,教...
请求域名：mine.moneropool.com,mine.moneropool.com	N/A	N/A	N/A	N/A	[redacted]122	53	中国,北京,北京,海淀,教...	[redacted].217	41537	中国,北京,北京,海淀,教...
请求域名：mine.moneropool.com,mine.moneropool.com	N/A	N/A	N/A	N/A	[redacted]122	53	中国,北京,北京,海淀,教...	[redacted].217	44735	中国,北京,北京,海淀,教...
请求域名：mine.moneropool.com,mine.moneropool.com	N/A	N/A	N/A	N/A	[redacted]122	53	中国,北京,北京,海淀,教...	[redacted].217	58624	中国,北京,北京,海淀,教...
请求域名：mine.moneropool.com,mine.moneropool.com	N/A	N/A	N/A	N/A	[redacted]122	53	中国,北京,北京,海淀,教...	[redacted].217	42146	中国,北京,北京,海淀,教...
请求域名：mine.moneropool.com,mine.moneropool.com	N/A	N/A	N/A	N/A	[redacted]122	53	中国,北京,北京,海淀,教...	[redacted].217	44735	中国,北京,北京,海淀,教...
请求域名：mine.moneropool.com,mine.moneropool.com	N/A	N/A	N/A	N/A	[redacted]122	53	中国,北京,北京,海淀,教...	[redacted].217	57229	中国,北京,北京,海淀,教...
请求域名：mine.moneropool.com,mine.moneropool.com	N/A	N/A	N/A	N/A	[redacted]122	53	中国,北京,北京,海淀,教...	[redacted].217	45949	中国,北京,北京,海淀,教...
请求域名：mine.moneropool.com,mine.moneropool.com	N/A	N/A	N/A	N/A	[redacted]122	53	中国,北京,北京,海淀,教...	[redacted].217	45949	中国,北京,北京,海淀,教...
请求域名：mine.moneropool.com,mine.moneropool.com	N/A	N/A	N/A	N/A	[redacted]122	53	中国,北京,北京,海淀,教...	[redacted].217	42146	中国,北京,北京,海淀,教...
请求域名：mine.moneropool.com,mine.moneropool.com	N/A	N/A	N/A	N/A	[redacted]122	53	中国,北京,北京,海淀,教...	[redacted].217	48650	中国,北京,北京,海淀,教...

防：各种挖矿木马、病毒

描述	触发时间	警报级别	类型	分类	触发条件	源IP地址	源IP地址地理位置	源端口	目标IP地址
疑似在进行挖矿行为	2019/10/22 16:26:53	高	数据流特征值警报	漏洞利...	内容:[A]"method": 内容:[A]"submit" 内容:[A]...	[redacted](挖矿)	中国,北京,北京_教育网	58192	[redacted](挖矿矿池)
疑似在进行挖矿行为	2019/10/22 16:26:54	高	数据流特征值警报	漏洞利...	内容:[A]"id": 内容:[A]"jsonrpc": 内容:[A]"erro...	[redacted](挖矿矿池)	加拿大,安大略,北约克	443	[redacted](挖矿)
疑似在进行挖矿行为	2019/10/22 16:26:55	高	数据流特征值警报	漏洞利...	内容:[A]"method": 内容:[A]"submit" 内容:[A]...	[redacted](挖矿)	中国,北京,北京_教育网	58192	[redacted](挖矿矿池)
疑似在进行挖矿行为	2019/10/22 16:27:03	高	数据流特征值警报	漏洞利...	内容:[A]"method": 内容:[A]"login" 内容:[A]"p...	[redacted](挖矿)	中国,北京,北京_教育网	58217	[redacted](挖矿矿池)
疑似在进行挖矿行为	2019/10/22 16:26:48	高	数据流特征值警报	漏洞利...	内容:[A]"method": 内容:[A]"submit" 内容:[A]...	[redacted](挖矿)	中国,北京,北京_教育网	58192	[redacted](挖矿矿池)
疑似在进行挖矿行为	2019/10/22 16:27:05	高	数据流特征值警报	漏洞利...	内容:[A]"id": 内容:[A]"jsonrpc": 内容:[A]"erro...	[redacted](挖矿矿池)	加拿大,安大略,北约克	443	[redacted](挖矿)
疑似在进行挖矿行为	2019/10/22 16:27:07	高	数据流特征值警报	漏洞利...	内容:[A]"method": 内容:[A]"submit" 内容:[A]...	[redacted](挖矿)	中国,北京,北京_教育网	58217	[redacted](挖矿矿池)
疑似在进行挖矿行为	2019/10/22 16:27:08	高	数据流特征值警报	漏洞利...	内容:[A]"method": 内容:[A]"submit" 内容:[A]...	[redacted](挖矿)	中国,北京,北京_教育网	58217	[redacted](挖矿矿池)
疑似在进行挖矿行为	2019/10/22 16:27:02	高	数据流特征值警报	漏洞利...	内容:[A]"method": 内容:[A]"login" 内容:[A]"p...	[redacted](挖矿)	中国,北京,北京_教育网	58217	[redacted](挖矿矿池)
疑似在进行挖矿行为	2019/10/22 16:26:46	高	数据流特征值警报	漏洞利...	内容:[A]"method": 内容:[A]"submit" 内容:[A]...	[redacted](挖矿)	中国,北京,北京_教育网	58192	[redacted](挖矿矿池)
疑似在进行挖矿行为	2019/10/22 16:26:45	高	数据流特征值警报	漏洞利...	内容:[A]"id": 内容:[A]"jsonrpc": 内容:[A]"erro...				
疑似在进行挖矿行为	2019/10/22 16:26:44	高	数据流特征值警报	漏洞利...	内容:[A]"method": 内容:[A]"submit" 内容:[A]...				
疑似在进行挖矿行为	2019/10/22 16:26:32	高	数据流特征值警报	漏洞利...	内容:[A]"method": 内容:[A]"submit" 内容:[A]...				
疑似在进行挖矿行为	2019/10/22 16:26:43	高	数据流特征值警报	漏洞利...	内容:[A]"method": 内容:[A]"submit" 内容:[A]...				
疑似在进行挖矿行为	2019/10/22 16:26:42	高	数据流特征值警报	漏洞利...	内容:[A]"method": 内容:[A]"submit" 内容:[A]...				
疑似在进行挖矿行为	2019/10/22 16:26:41	高	数据流特征值警报	漏洞利...	内容:[A]"method": 内容:[A]"login" 内容:[A]"p...				
疑似在进行挖矿行为	2019/10/22 16:27:12	高	数据流特征值警报	漏洞利...	内容:[A]"method": 内容:[A]"submit" 内容:[A]...				
疑似在进行挖矿行为	2019/10/22 16:26:33	高	数据流特征值警报	漏洞利...	内容:[A]"method": 内容:[A]"submit" 内容:[A]...				
疑似在进行挖矿行为	2019/10/22 16:26:47	高	数据流特征值警报	漏洞利...	内容:[A]"id": 内容:[A]"jsonrpc": 内容:[A]"erro...				
疑似在进行挖矿行为	2019/10/22 16:27:50	高	数据流特征值警报	漏洞利...	内容:[A]"method": 内容:[A]"submit" 内容:[A]...				
疑似在进行挖矿行为	2019/10/22 16:26:30	高	数据流特征值警报	漏洞利...	内容:[A]"id": 内容:[A]"jsonrpc": 内容:[A]"erro...				
疑似在进行挖矿行为	2019/10/22 16:27:58	高	数据流特征值警报	漏洞利...	内容:[A]"method": 内容:[A]"login" 内容:[A]"p...				
疑似在进行挖矿行为	2019/10/22 16:27:49	高	数据流特征值警报	漏洞利...	内容:[A]"id": 内容:[A]"jsonrpc": 内容:[A]"erro...				
疑似在进行挖矿行为	2019/10/22 16:27:48	高	数据流特征值警报	漏洞利...	内容:[A]"method": 内容:[A]"submit" 内容:[A]...				
疑似在进行挖矿行为	2019/10/22 16:27:41	高	数据流特征值警报	漏洞利...	内容:[A]"id": 内容:[A]"jsonrpc": 内容:[A]"erro...				



防：各种挖矿木马、病毒 —— 附带攻击行为

我们组的一台机器好像被入侵了，/usr/bin/Xorg被替换了，运行它会自动连接 s1000.us:3333

下面是网络连接状态：

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1375/sshd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      1181/cupsd
tcp        0      0 127.0.0.1:5939          0.0.0.0:*               LISTEN      1482/teamviewerd
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN      1659/dnsmasq
tcp        0      0 [redacted]115:22        [redacted]:43768        ESTABLISHED 5429/sshd: wly [pri
tcp        0      0 [redacted]115:41772     [redacted]9832          ESTABLISHED 1309/[netdns]
tcp        0      0 [redacted]115:35016     [redacted]3333          ESTABLISHED 5931/Xorg
tcp        0      0 [redacted]115:22        [redacted]:48298        ESTABLISHED 5974/sshd: wly [pri
tcp6       0      0 :::22                   :::*                    LISTEN      1375/sshd
tcp6       0      0 ::1:631                 :::*                    LISTEN      1181/cupsd
```

下面是/usr/bin/Xorg的输出：

```
 * ABOUT        XMRig/2.14.1 gcc/5.4.0
 * LIBS         libuv/1.8.0
 * CPU          Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz (1) x64 AES AVX2
 * THREADS      20, cryptonight, donate=0%
 * ASSEMBLY     auto:intel
 * POOL #1      s1000.us:3333 variant auto
 * POOL #2      [redacted]:3333 variant auto
 * COMMANDS     hashrate, pause, resume
[2019-07-22 12:47:06] use pool s1000.us:3333  [redacted]242
[2019-07-22 12:47:06] new job from s1000.us:3333 diff 120001 algo cn/r height 1883842
[2019-07-22 12:47:07] READY (CPU) threads 20(20) huge pages 0/20 0% memory 40960 KB
[2019-07-22 12:48:02] new job from s1000.us:3333 diff 120001 algo cn/r height 1883842
[2019-07-22 12:48:10] speed 10s/60s/15m 764.0 764.4 n/a H/s max 764.6 H/s
[2019-07-22 12:48:26] new job from s1000.us:3333 diff 120001 algo cn/r height 1883843
[2019-07-22 12:49:10] speed 10s/60s/15m 764.9 764.4 n/a H/s max 765.0 H/s
[2019-07-22 12:49:16] new job from s1000.us:3333 diff 120001 algo cn/r height 1883844
[2019-07-22 12:50:10] speed 10s/60s/15m 763.9 764.2 n/a H/s max 765.1 H/s
[2019-07-22 12:50:17] new job from s1000.us:3333 diff 120001 algo cn/r height 1883844
[2019-07-22 12:51:03] accepted (1/0) diff 120001 (401 ms)
[2019-07-22 12:51:10] speed 10s/60s/15m 763.9 764.0 n/a H/s max 765.1 H/s
[2019-07-22 12:51:17] new job from s1000.us:3333 diff 120001 algo cn/r height 1883844
[2019-07-22 12:52:10] speed 10s/60s/15m 763.8 763.8 n/a H/s max 765.1 H/s
[2019-07-22 12:52:12] new job from s1000.us:3333 diff 120001 algo cn/r height 1883845
```

```
root ssh:notty [redacted].105 Thu May 3 05:10 - 05:10 (00:00)
root ssh:notty [redacted].105 Thu May 3 05:10 - 05:10 (00:00)
root ssh:notty [redacted].105 Thu May 3 05:10 - 05:10 (00:00)
root ssh:notty [redacted].105 Thu May 3 05:10 - 05:10 (00:00)
root ssh:notty [redacted].105 Thu May 3 05:10 - 05:10 (00:00)
root ssh:notty [redacted].105 Thu May 3 05:10 - 05:10 (00:00)
root ssh:notty [redacted].105 Thu May 3 05:10 - 05:10 (00:00)
root ssh:notty [redacted].105 Thu May 3 05:10 - 05:10 (00:00)
root ssh:notty [redacted].105 Thu May 3 05:09 - 05:09 (00:00)
root ssh:notty [redacted].105 Thu May 3 05:09 - 05:09 (00:00)
root ssh:notty [redacted].105 Thu May 3 05:09 - 05:09 (00:00)
root ssh:notty [redacted].105 Thu May 3 05:09 - 05:09 (00:00)
root ssh:notty [redacted].105 Thu May 3 05:09 - 05:09 (00:00)
root ssh:notty [redacted].105 Thu May 3 05:09 - 05:09 (00:00)
root ssh:notty [redacted].105 Thu May 3 05:09 - 05:09 (00:00)
root ssh:notty [redacted].105 Thu May 3 05:09 - 05:09 (00:00)
root ssh:notty [redacted].105 Thu May 3 05:09 - 05:09 (00:00)
root ssh:notty [redacted].105 Thu May 3 05:09 - 05:09 (00:00)
root ssh:notty [redacted].105 Thu May 3 05:08 - 05:08 (00:00)
```

防：各种挖矿木马、病毒

关于近期服务器感染挖矿病毒实施网络攻击的紧急通知

发布时间：2019-08-30　发布单位：计算中心　阅读次数：1043

尊敬的校园网用户：

近日计算中心通过监测和校园网用户报告，并由计算中心现场勘察并提取日志和恶意样本进行分析后，确认部分校园网Linux服务器感染挖矿病毒，进行挖矿与DDoS攻击。目前发现的感染原因全部是通过操作系统的ssh、ftp、telnet等服务的弱口令进入操作系统，再植入挖矿病毒。

针对发现已感染的服务器，计算中心将一对一通知相应管理员，请收到通知后立即整改。也请全校使用Linux服务器的管理员务必按照下列方式排查是否感染挖矿病毒。

判断服务器是否感染挖矿病毒：

1、查看/usr/bin/或/etc/systcl/目录下存在config.json文件，该文件中包含如下类似内容：

```
"pools": [
                {
                        "url": "s1000.us:3333",
                        "user": "r",
                        "pass": "x",
                        "keepalive": true,
                        "nicehash": false,
                        "variant": -1,
                        "tls": false,
                        "tls-fingerprint": null
                },
        ],
```

其他病毒文件包括：

/usr/bin/org
/lib/scr.so
/lib/libdev.so.1
/etc/update
/etc/upgrade
/etc/systcl
/etc/systcl/systcl.conf
/usr/bin/config.json
/etc/ld.so.preload

2、查看是否连接异常端口（3333或9832端口）。

3、查看服务器是否有异常计划任务。

感染挖矿病毒的服务器的处理：

1. 断开网络连接。
2. 用移动硬盘拷贝出有用的数据。
3. 低格硬盘。
4. 重装操作系统。
5. 清除不必要的系统和用户账号，关闭不必要的进程。
6. Root用户口令设置为强口令，其他用户的口令也必须设置为强口令。
7. Redis服务限源访问或设置访问认证。
8. 启用系统防火墙，仅允许系统业务端口开放。
9. 及时给系统和应用软件打补丁，修复漏洞。
10. 导入备份数据，恢复应用系统。

密码设置方法：

不用弱密码，弱密码指仅包含简单数字或字母的组合，如：123、12345678、abc、root、admin等；

避免“大众”密码，如：用户名、生日、abc123等；

设一个自己能记住的密码，如：古诗词、一句话缩写+数字/字符等，bq11yhy_201809（八千里路云和月）。

防：信息安全

- 可能被针对的攻击：密码算法安全、协议安全、使用安全（丢失私钥）、系统安全

来源：《2018年区块链行业应用研究报告》，亿欧智库

高校应用

- 防
- 用

北京大学
PEKING UNIVERSITY

习近平：把区块链作为核心技术自主创新重要突破口

2019年10月26日

人民日报
RENMIN RIBAO
人民网网址：http://www.people.com.cn

2019年10月
26
星期六
己亥年九月廿八
人民日报社出版
国内统一连续出版物号
CN 11-0065
代号1-1
第26040期
今日8版

习近平在中央政治局第十八次集体学习时强调

加快推动区块链技术和产业创新发展
把区块链作为核心技术自主创新重要突破口

- 要强化基础研究，提升原始创新能力，努力让我国在区块链这个新兴领域走在理论最前沿、占据创新制高点、取得产业新优势
- 要抓住区块链技术融合、功能拓展、产业细分的契机，发挥区块链在促进数据共享、优化业务流程、降低运营成本、提升协同效率、建设可信体系等方面的作用

新华社北京10月25日电　中共中央政治局10月24日下午就区块链技术发展现状和趋势进行第十八次集体学习。中共中央总书记习近平在主持学习时强调，区块链技术的集成应用在新的技术革新和产业变革中起着重要作用。我们要把区块链作为核心技术自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动区块链技术和产业创新发展。

浙江大学教授、中国工程院院士陈纯就这个问题作了讲解，并谈了意见和建议。

中共中央政治局各位同志认真听取了讲解，并进行了讨论。

习近平在主持学习时发表了讲话。他指出，区块链技术应用已延伸到数字金融、物联网、智能制造、供应链管理、数字资产交易等多个领域。目前，全球主要国家都在加快布局区块链技术发展。我国在区块链领域拥有良好基础，要加快推动区块链技术和产业创新发展，积极推进区块链和经济社会融合发展。

习近平强调，要强化基础研究，提升原始创新能力，努力让我国在区块链这个新兴领域走在理论最前沿、占据创新制高点、取得产业新优势。要推动协同攻关，加快推进核心技术突破，为区块链应用发展提供安全可控的技术支撑。要加强区块链标准化研究，提升国际话语权和规则制定权。要加快产业发展，发挥好市场优势，进一步打通创新链、应用链、价值链。要构建区块链产业生态，加快区块链和人工智能、大数据、物联网等前沿信息技术的深度融合，推动集成创新和融合应用。要加强人才队伍建设，建立完善人才培养体系，打造多种形式的高层次人才培养平台，培育一批领军人物和高水平创新团队。

习近平指出，要抓住区块链技术融合、功能拓展、产业细分的契机，发挥区块链在促进数据共享、优化业务流程、降低运营成本、提升协同效率、建设可信体系等方面的作用。要推动区块链和实体经济深度融合，解决中小企业贷款融资难、银行风控难、部门监管难等问题。要利用区块链技术探索数字经济模式创新，为打造便捷高效、公平竞争、稳定透明的营商环境提供动力，为推进供给侧结构性改革、实现各行业供需有效对接提供服务，为加快新旧动能接续转换、推动经济高质量发展提供支撑。要探索“区块链+”在民生领域的运用，积极推动区块链技术在教育、就业、养老、精准脱贫、医疗健康、商品防伪、食品安全、公益、社会救助等领域的应用，为人民群众提供更加智能、更加便捷、更加优质的公共服务。要推动区块链底层技术服务和新型智慧城市建设相结合，探索在信息基础设施、智慧交通、能源电力等领域的推广应用，提升城市管理的智能化、精准化水平。要利用区块链技术促进城市间在信息、资金、人才、征信等方面更大规模的互联互通，保障生产要素在区域内有序高效流动。要探索利用区块链数据共享模式，实现政务数据跨部门、跨区域共同维护和利用，促进业务协同办理，深化“最多跑一次”改革，为人民群众带来更好的政务服务体验。

习近平强调，要加强对区块链技术的引导和规范，加强对区块链安全风险的研究和分析，密切跟踪发展动态，积极探索发展规律。要探索建立适应区块链技术机制的安全保障体系，引导和推动区块链开发者、平台运营者加强行业自律，落实安全责任。要把依法治网落实到区块链管理中，推动区块链安全有序发展。

习近平指出，相关部门及其负责领导同志要注意区块链技术发展现状和趋势，提高运用和管理区块链技术能力，使区块链技术在建设网络强国、发展数字经济、助力经济社会发展等方面发挥更大作用。

区块链 + 跨境金融：SWIFT的问题

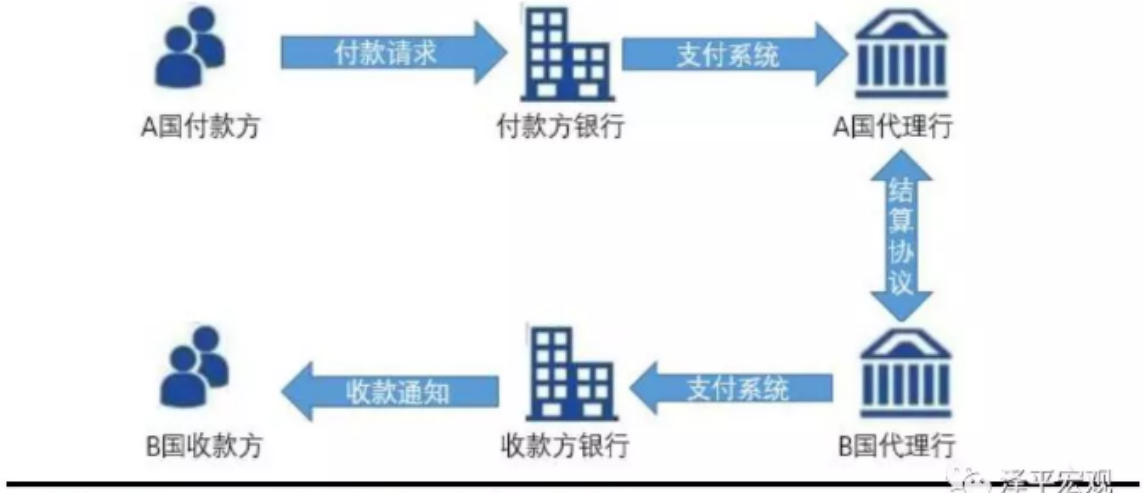
- 从收款方到付款方的单次交易需要25-35美金的交易费用，其中因交易时间过长造成的流动性损失占比达34%，资金运作成本占比达24%。

- 总部设在比利时，由美国主导！

SWIFT形式耗时长，手续费高

SWIFT主要为金融机构的结算提供金融交易的电文交换业务，提供规则统一的金融行业安全报文服务和接口服务。由于跨境金融机构间系统不相通，直接结算成本高昂，同时业务占比低以及对手方存在不确定性，很难构建直接合作关系。代理行的存在、协议的沟通以及交易信息的反复确认**使得结算周期平均需要3-5天，其中通过SWIFT进行交易确认往往需要1-2天。**

图表13：SWIFT 电汇结算体系往往需要通过多个中间代理行



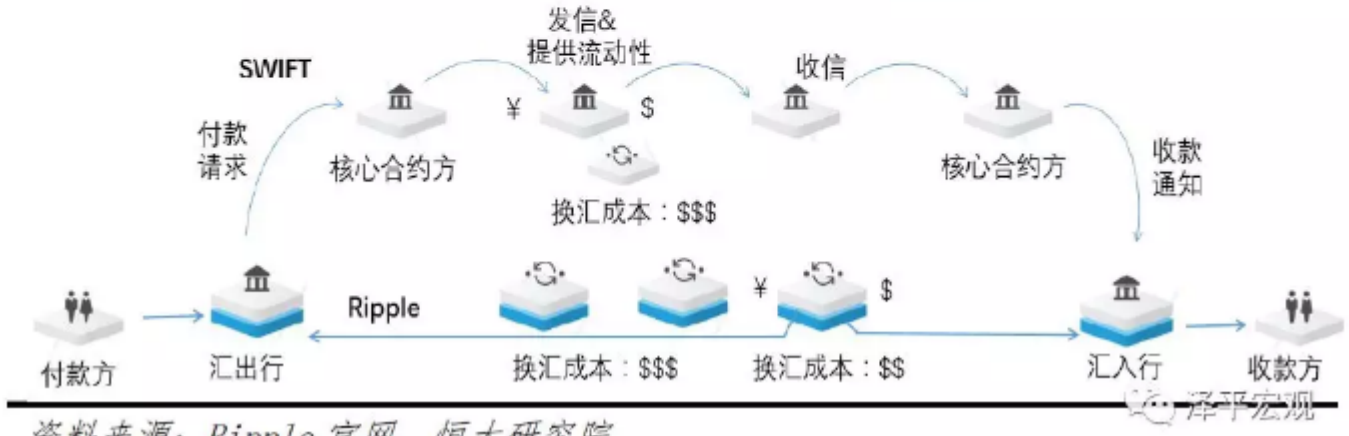
资料来源：SWIFT 年度报告，恒大研究院 来源：恒大研究院《区块链研究报告》， 任泽平

区块链 + 跨境金融：Ripple

- 根据Ripple（美国区块链公司）估算，银行间每笔交易的成本将从5.56美元下降到2.21美元，降低60%，以2016年通过SWIFT完成的30多亿次支付类报文数量计算，2016年可以节约大约100亿美元的费用。

Ripple成立于2012年，采用联合共识机制并由金融机构扮演做市商，从而提供去中心化的跨境外汇转账。银行间的交易支付信息上传到节点服务器后经过投票确认即可完成交易，从而节约了银行通过SWIFT进行的对账和交易信息确认时间，**将原本1-3天左右的交易确认时间缩短到几秒钟，整体的跨境电汇时间缩短到1-2天。**Ripple目前已经有90家金融机构成员，包括加拿大皇家银行、渣打银行、西太平洋银行等，还有75家在协商中。

图表15：Ripple 降低了收款行和付款行之间的成本



资料来源：Ripple 官网，恒大研究院

来源：恒大研究院《区块链研究报告》， 任泽平

区块链 + 金融: DCEP

- 2019年9月4日，《中国日报》报道称，央行数字货币已开始进行“闭环测试”
- DCEP vs LIBRA

（1）DCEP与人民币可以1:1自由兑换，支持连接中央银行；
（2）DCEP采用商业银行和中央银行的双层制度，适应国际上各主权国家现有的货币体系；
（3）DCEP是主权货币，是纸质人民货币的替代，可以确保现有货币理论体系依然发挥作用；
（4）DCEP可以基于特殊设计，可以不依赖于网络进行点对点的交易。

来源：《2018年区块链行业应用研究报告》，亿欧智库

区块链 + 金融: 中国的新航道

- 500年的西方金融体系、100年的美元国际结算、人民币国际化
- wintel => 高通+Android

- 对DCEP的猜测
  - 双层运营体系：上面一层是人民银行对商业银行，下面一层是商业银行或商业机构对老百姓。
  - 支付宝和微信可以成为全球自由流动的最佳途径
    - （1）截止2018年，支付宝已经可以在200个国家和地区使用；
    - （2）支持美元、英镑等20余种货币的直接交易；
    - （3）可以在全球主要38个国家和地区跨境支付；
    - （4）支付宝在中国将现金交易降低到不足交易总量的2%、并正在世界范围内逐步取代现金交易。

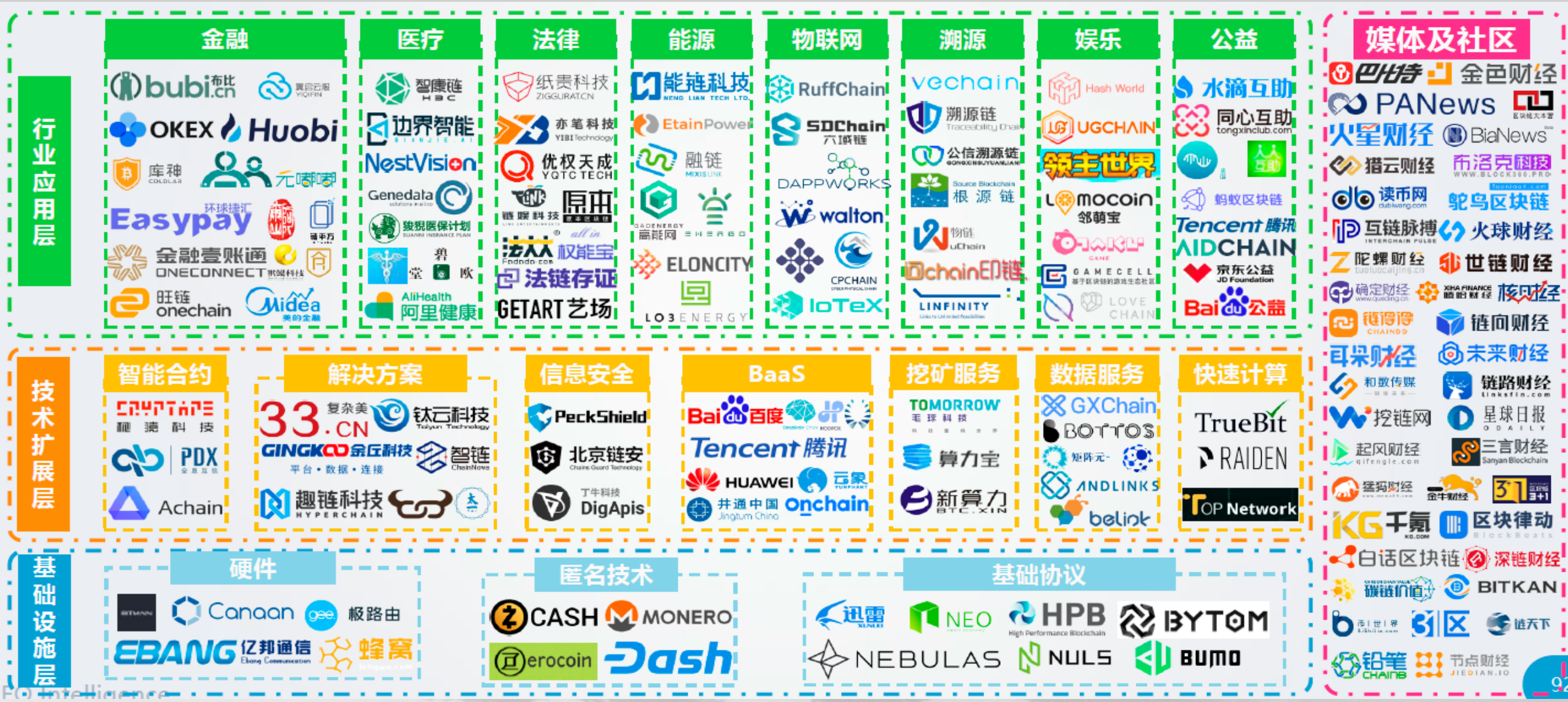
区块链的其它应用场景

- 赋能：范围广、跨主体、提效率、降成本
- 区块链+全球贸易物流
  - 对进口商、出口商、制造商：端到端的信息透明可以实时监管物流全流程，增加各个环节沟通效率
  - 对港口和集装箱集中地管理：提高空箱利用率和资源错配率
  - 对海关等检查机关：信息正确提高批审效率
  - 对运输管理商：优化货物运输路线和日程安排
  - IBM与马士基合作从鹿特丹港到新泽西纽瓦克港的运输。马士基时间上节省超40%，成本降低超20%。
- 区块链+供应链金融
  - 互联网金融平台点融网和富士康集团旗下金融平台富金通合作推出区块链金融平台“Chained Finance”，首先将核心企业的应付账款转化为区块链上的线上资产eAP，eAP可以在各级供应商之间流通（用于支付或用于融资取现）
  - 对于供应链上的中小企业，传统模式下融资成本高达25%以上，在Chained Finance平台可降低至10%以下
- 区块链+征信
  - LinkEye是一套基于区块链技术的征信共享联盟链解决方案，构建联盟成员（金融公司）之间的征信数据共享和服务平台。区块链的签名机制保证了数据的不可篡改，从而完成失信人名单共享，同时开放对外查询接口，向社会共享数据。
  - 解决了“信息孤岛”问题、征信数据归属问题

应用条件

- 高并发：至少支持百万级别的用户
- 免费：对终端用户免费，对应用开发者提供各种选择
- 维护：轻松升级和故障修复
- 性能：
  - 延迟低（尤其是交易的确认）
  - 串行性能，有些应用程序由于必须顺序执行命令，无法用并行算法进行实现
  - 并行性能，大型应用程序需要在多个CPU和计算机之间分配工作负载

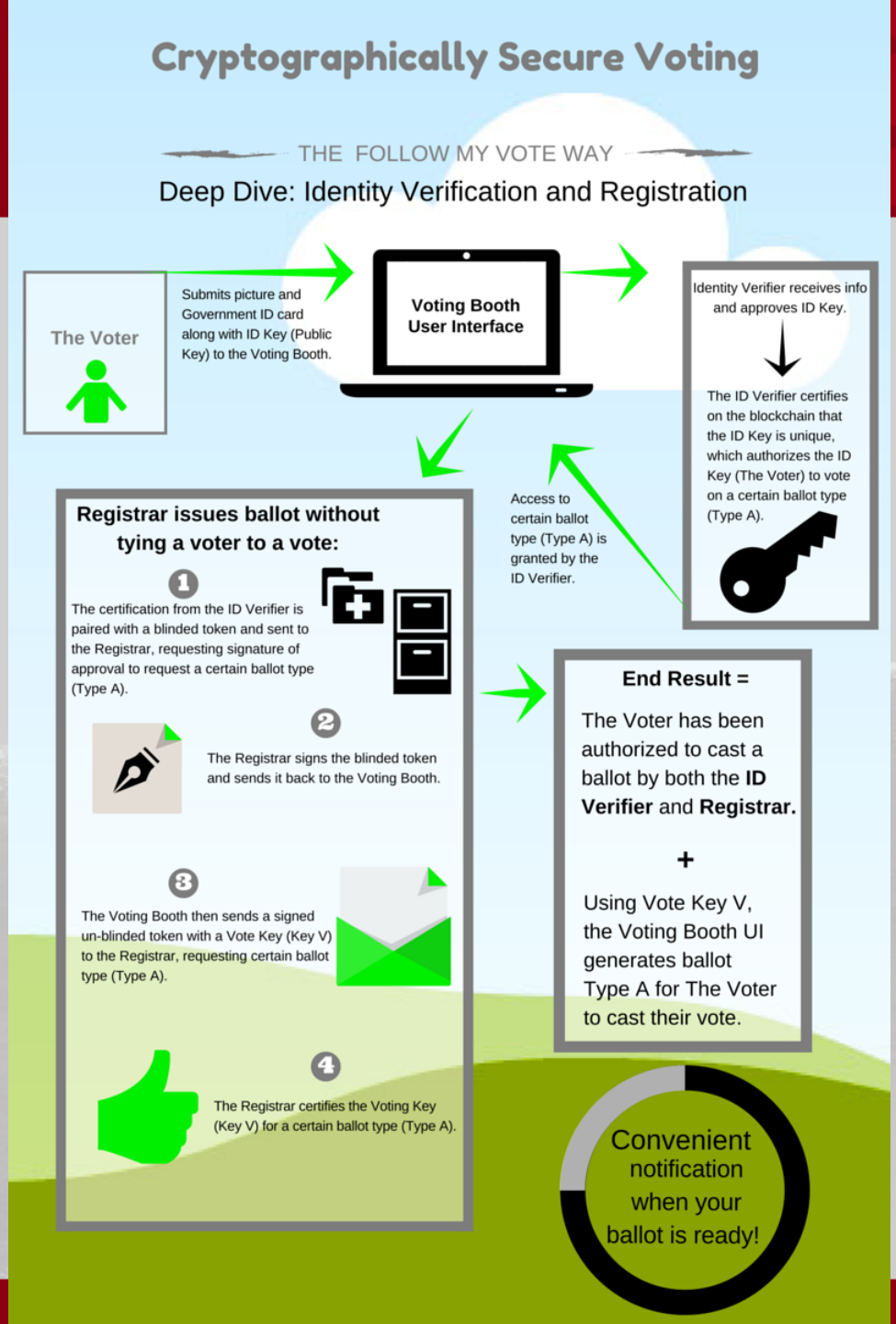
- 赋能：范围广、跨主体、提效率、降成本



来源： 《2018年区块链行业应用研究报告》，亿欧智库。区块链产业部分企业图谱

高校应用：可信的投票

- 双key机制
  - Verifier不知道用户的投票结果
  - Registrar不知道投票人的身份



https://followmyvote.com/

高校应用：区块链协同产品（OA）

- 共享身份认证体系：安全、可靠、具备公信力的身份认证体系
- 分布式存储：用户身份认证信息、合约文书的完整信息、用户的关键行为信息的链上多点存储、不可撰改
- 数据控制权、共享权：基于许可链或者联盟链，设立拥有这些数据的控制权，控制不同的机构对这些数据访问
- 智能合约：合约脚本化、智能化，减少人为操作，优化商业信用环境。

北京大学
PEKING UNIVERSITY

谢谢