2016

区块链架构与应用

李赫

目录

CATALOG

01

PART 01

第一部分
从比特币谈区块链原理

比特币来源

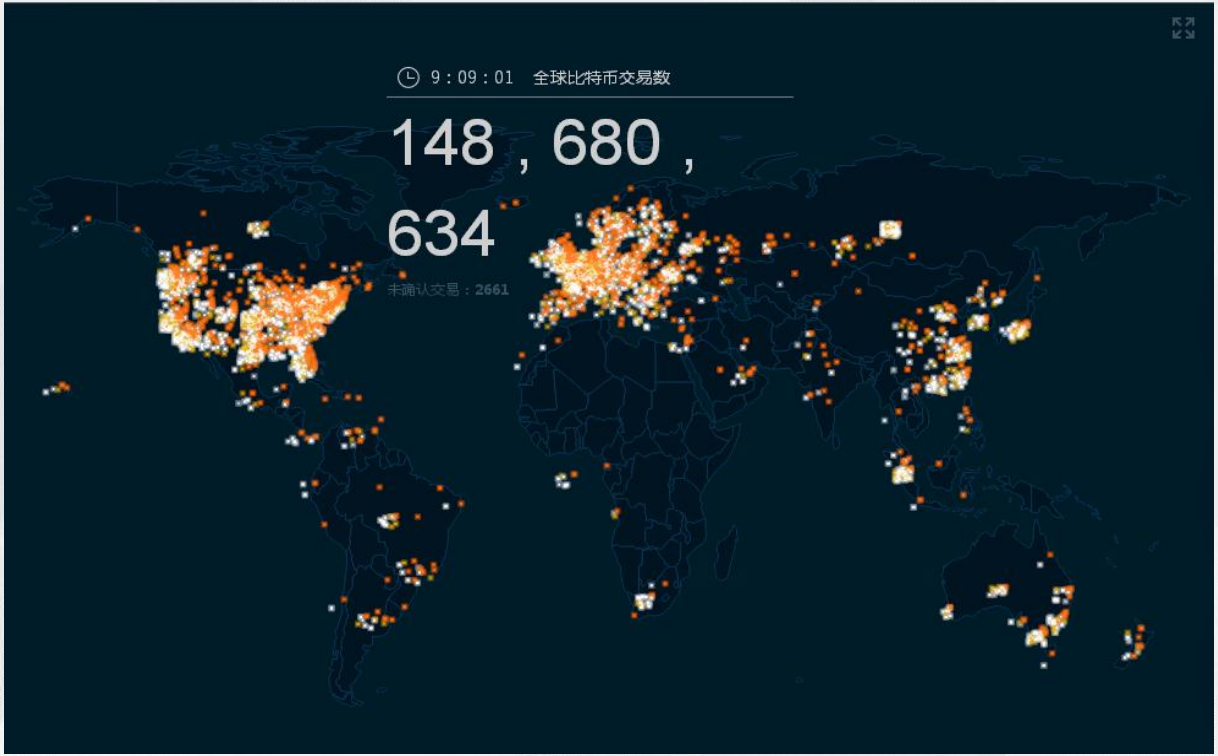
- 挖矿
- 购买

比特币存储

李赫的比特币钱包地址：
1FenAHzk5FD6zLhH8
8XxBb7C6VU163S8iN

只有银行服务器证明我有一元人民币，但全世界都证明我有一个比特币

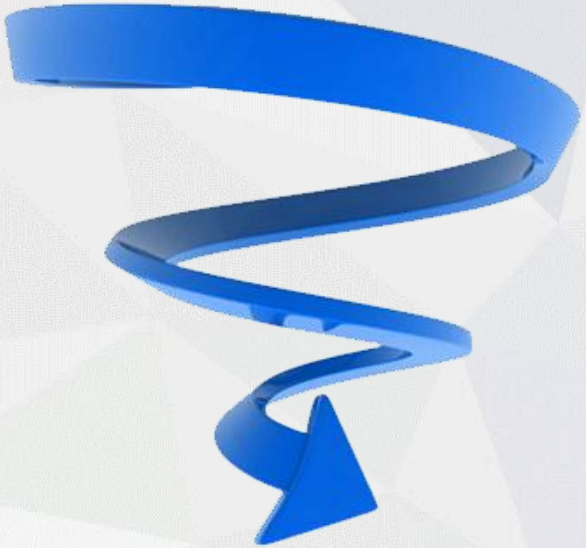
区块链想象成比特币网络的数据库



- 完整备份
- 历史记录
- 块状存储
- 交易广播

比特币能否作为货币应用于经济？

螺旋式通缩最后导致经济逐步停滞



银行业实现的电子现金的特性

- 独立性：密码学安全
- 不可重复花费
- 匿名性
- 不可伪造性
- 可传递性
- 可分性

那么比特币是什么？

Bitcoin：A Peer-to-Peer Electronic Cash System

基础货币 currency

1. 法定准备金
2. 超额准备金
3. 公众现金
4. 银行库存现金

现金流通方式

1. 纸钞
2. 银行IC卡
3. 比特币
4. Modex等电子现金系统

02

PART 01

第二部分
区块链基础架构

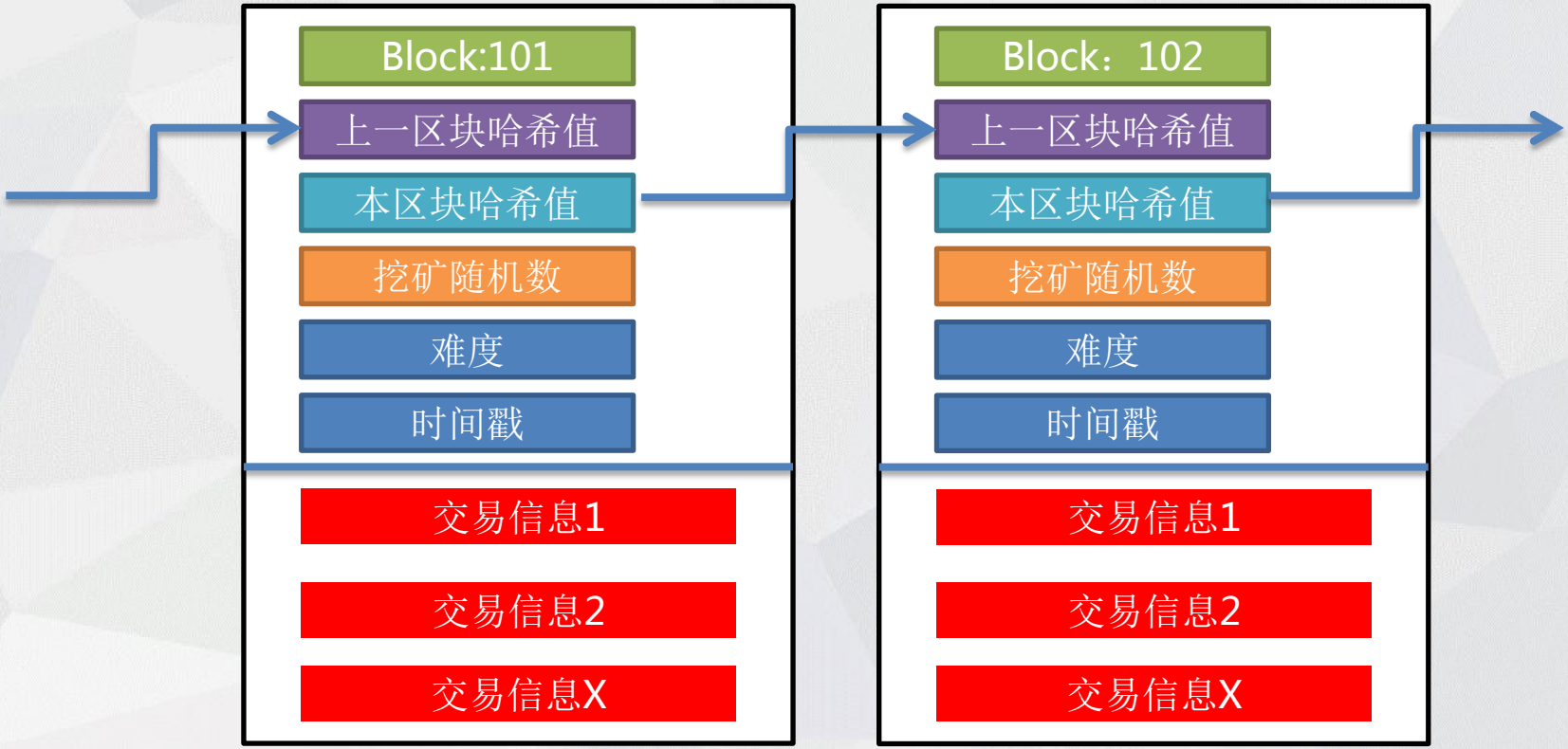
※ 区块与链　　※ 特征分类

※ 技术架构　　※ 演化史

2008年金融危机，顶级金融机构（雷曼兄弟和美林）一夜之间倒闭，甚至出现了冰岛国家主权债务违约，促使业界加速探索去中心化，但一直进展缓慢。

当比特币出现时，才真正看到了去中心化的希望，业界从比特币中提取了其中的技术体系架构，称之为区块链技术，并不断发展完善。

什么是区块和区块链

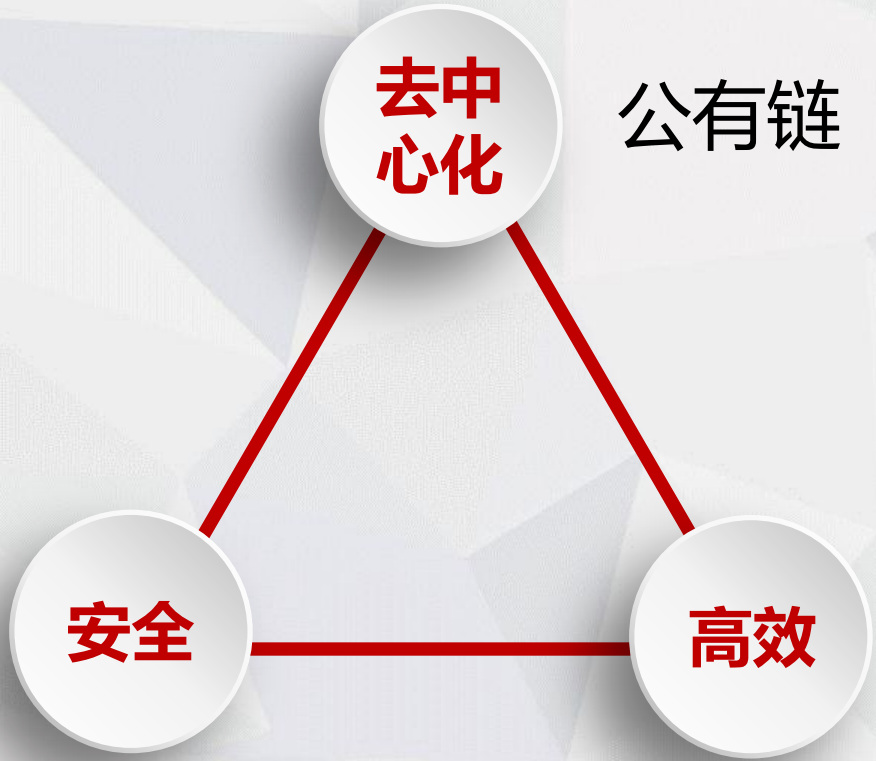

Block:101
上一区块哈希值
本区块哈希值
挖矿随机数
难度
时间戳
交易信息1
交易信息2
交易信息X
Block：102
上一区块哈希值
本区块哈希值
挖矿随机数
难度
时间戳
交易信息1
交易信息2
交易信息X

区块链基础架构

区块链有哪些分类

公有链	联盟链	私有链
• 任何人均可自由参加和退出	• 加入和退出需要经过联盟授权	• 权力完全控制在一个组织中

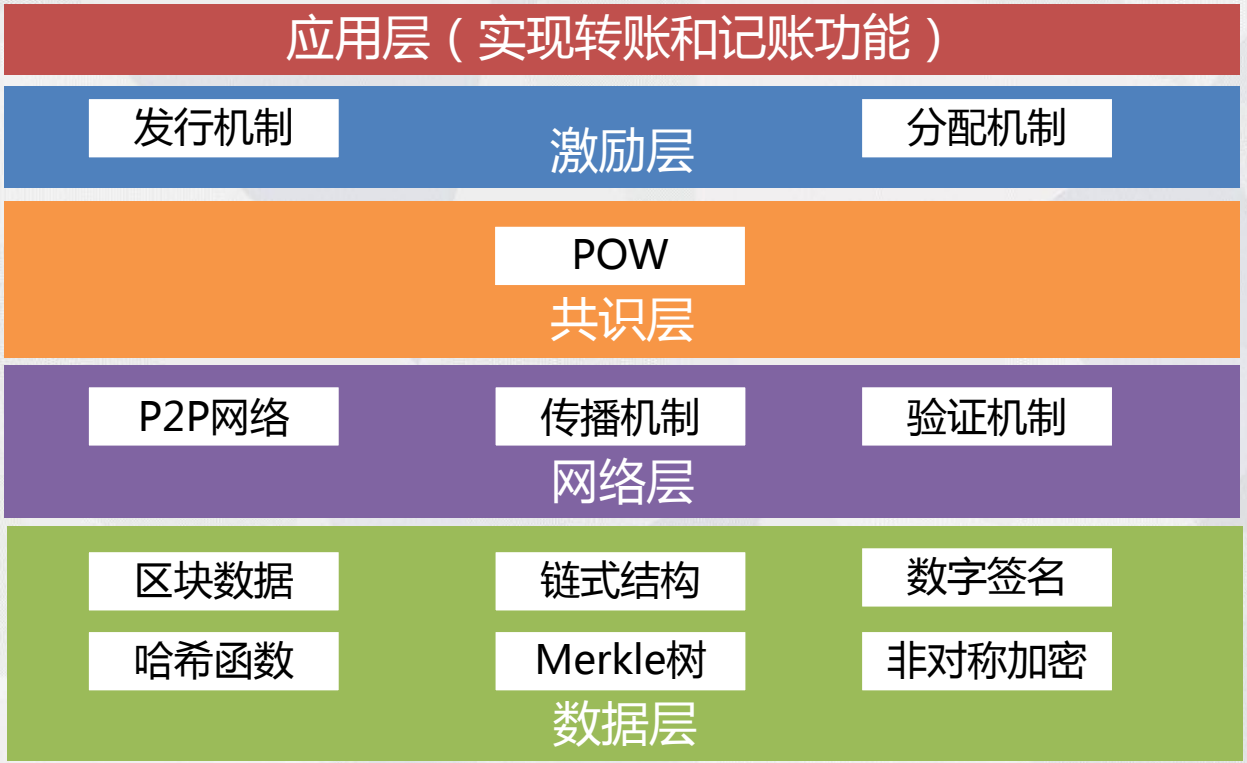
蒙代尔不可能三角



公有链

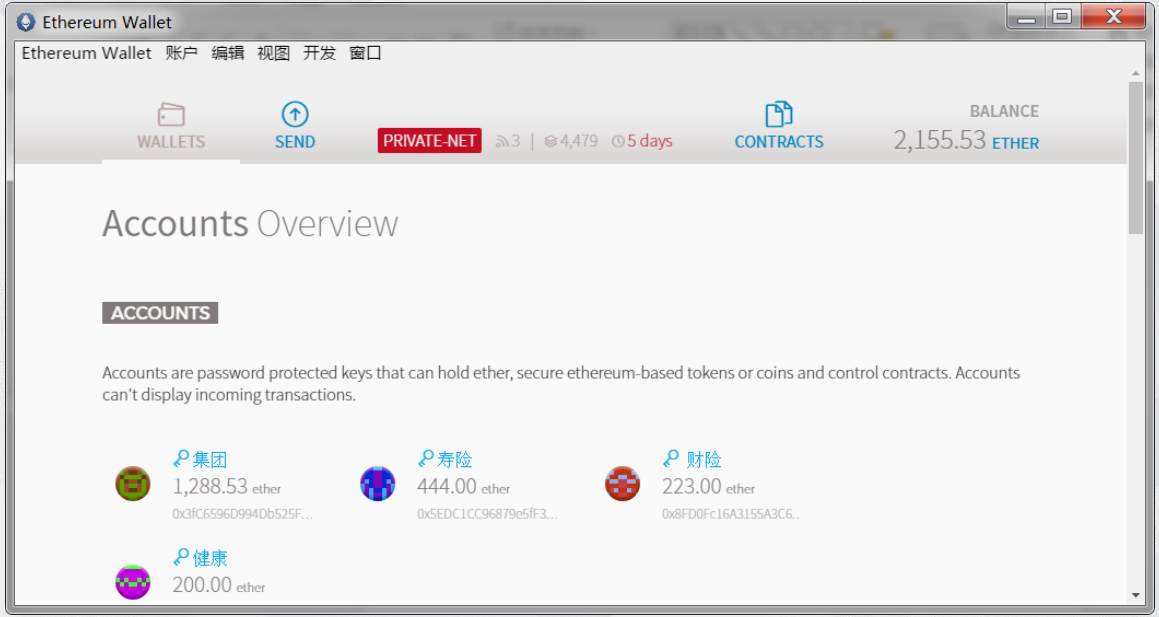
联盟链

区块链基础技术架构


应用层（实现转账和记账功能）
发行机制
激励层
分配机制
POW
共识层
P2P网络
传播机制
验证机制
网络层
区块数据
链式结构
数字签名
哈希函数
Merkle树
非对称加密
数据层

应用层主要由客户端完成记账转账功能

- 应用层
- 激励层
- 共识层
- 网络层
- 数据层



应用层

激励层

共识层

网络层

数据层

■ 发行机制，激励机制

以比特币为例，所有的比特币均通过奖励给那些创建新区块的矿工的方式产生，该奖励大约每四年减半。目前比特币系统每10分钟产生一个新区块，每个区块奖励12.5个比特币给矿工，这是货币发行的方式。

■ 另一个激励的来源则是交易费

所有交易都需要支付手续费给记录区块的矿工，如果某笔交易的交易费不足，那么矿工将拒绝执行

应用层

激励层

共识层

网络层

数据层

■ 拜占庭将军问题

刘备，关羽，张飞，赵云和魏延，任意两人都不是吕布的对手，所以必需三人联手才能打败吕布，所以进攻时必需三员将领同时上阵才能取胜，但是在将领中有叛徒，叛徒会假传命令，拜占庭问题实质就是在分布式的网络中如何在有不明数量的作恶节点的情况下仍然达成共识。

工作量证明机制 Proof of Work, POW

- 所有节点都平等的计算一个数学难题，最先获得答案的节点将获得这个区块的发布权。全网算力同时形成区块链的一道防火墙，降低黑客攻击风险。

挖矿---工作量证明

SHA256(SHA256(Version+HashPreBlock + Merkle_root + Timestamp + Bits + Nonce)) ≤ 难度数

- 难度数：目标哈希值，根据全网算力动态变化
- Nonce：矿工不断尝试的随机数，小于TargetHash的Nonce就是答案。
- Merkle Tree：一种哈希二叉树,使用它可以快速校验大规模数据的完整性。

区块链基础架构

应用层

激励层

共识层

网络层

数据层

CPU挖矿 → 显卡挖矿 → 专用芯片矿机 → 矿池

应用层

激励层

共识层

网络层

数据层

■ “双花”问题

简单的说就是如何保证每一笔数字现金都只会被花掉一次，避免重复支出。

区块链为每一笔交易加入了时间戳，使用了UTXO模型

■ 51%攻击

51%攻击并不能修改数据，但是可以产生“双花”攻击

应用层

激励层

共识层

网络层

数据层

■ 为什么区块10分钟发布一次

区块的间隔时间越短，包含的交易越少，浪费也越大，网络延迟对区块链的稳定影响也越大，容易形成分叉。

■ 如何保证区块发布时间保持在10分种

每完成2016个块，根据出块的平均时间调整一次难度。

应用层

激励层

共识层

网络层

数据层

■ P2P网络

又称点对点技术，是没有中心服务器、依靠用户群交换信息的互联网体系。P2P架构天生具有耐攻击、高容错的优点。由于服务是分散在各个结点之间进行的，部分结点或网络遭到破坏对其它部分的影响很小。实际就是我们经常下电影的BT技术

应用层

激励层

共识层

网络层

数据层

- P2P 网络每个节点以区块链的形式全量存储着所有的全部交易记录

- 硬分叉

应用层

激励层

共识层

网络层

数据层

非对称加密

- 公钥和私钥成对出现，公钥公开，私钥保密。
- 私钥加密的信息只有对应的公钥才能解密
- 公钥加密的信息只有对应的私钥才能解密

应用层

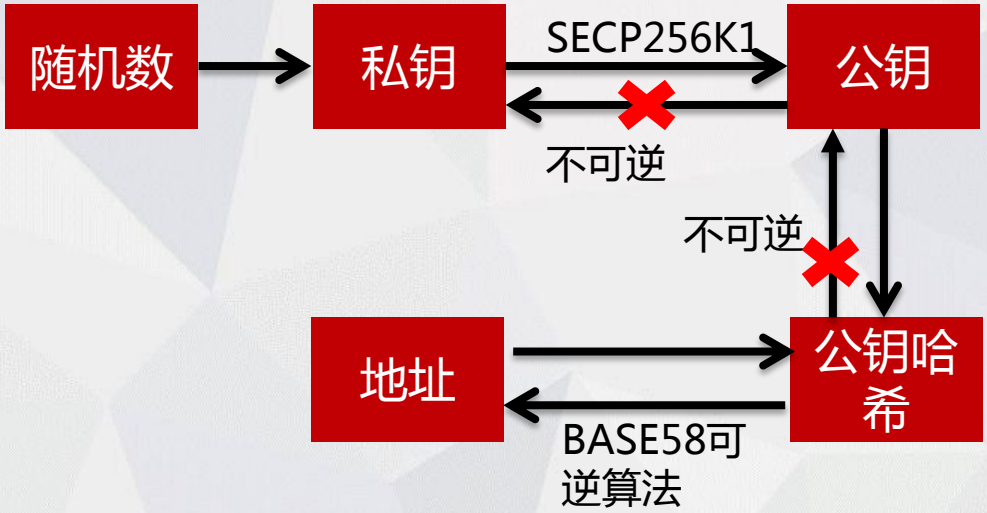
激励层

共识层

网络层

数据层

钱包地址生成



应用层

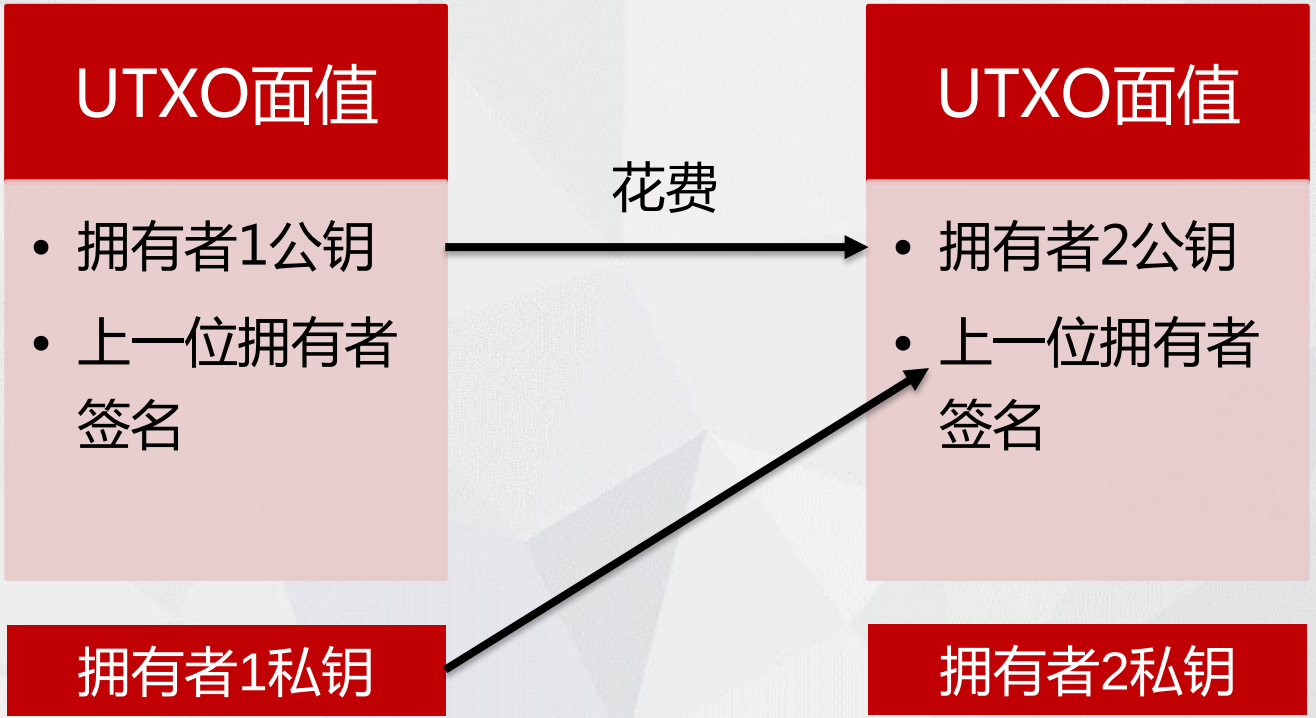
激励层

共识层

网络层

数据层

UTXO（未花费的交易输出）



应用层

激励层

共识层

网络层

数据层

交易数据包含哪些信息

TxHash:此交易的加密哈希值

From：钱包地址

To：对方钱包地址

Tx_in:UTXO,UTXO...

Tx_out:UTXO,UTXO...

交易主信息

应用层

激励层

共识层

网络层

数据层

矿工交易数据的验证

区块链演化史

1.0

电子现金
去中心化交易

2.0

智能合约、数字资产、各行业应用

3.0

去中心化互联网？
去中心化社会治理？

区块链1.0的局限性

以比特币为代表的区块链1.0产生了很多应用，主要以各种特色的电子货币为主，最多的行业应用是小额支付、外汇兑换、博彩和洗钱。

03

PART 01

第三部分

区块链2.0

※ 特点　※ 智能合约

※ 2.0技术架构

区块链1.0和区块链2.0对比

2.0	1.0
图灵完备	非图灵完备：只能执行有限类型指令
支持智能合约	不支持智能合约
定位于平台，可实现各种应用	定位于具体某一应用如支付网络

区块链2.0

从全球账本到全球计算机

更快交易速度,高达3000TPS **2.0**

1.0 交易速度5-20TPS

无资源消耗，支持POS,DPOS,PBFT等无消耗共识机制 **2.0**

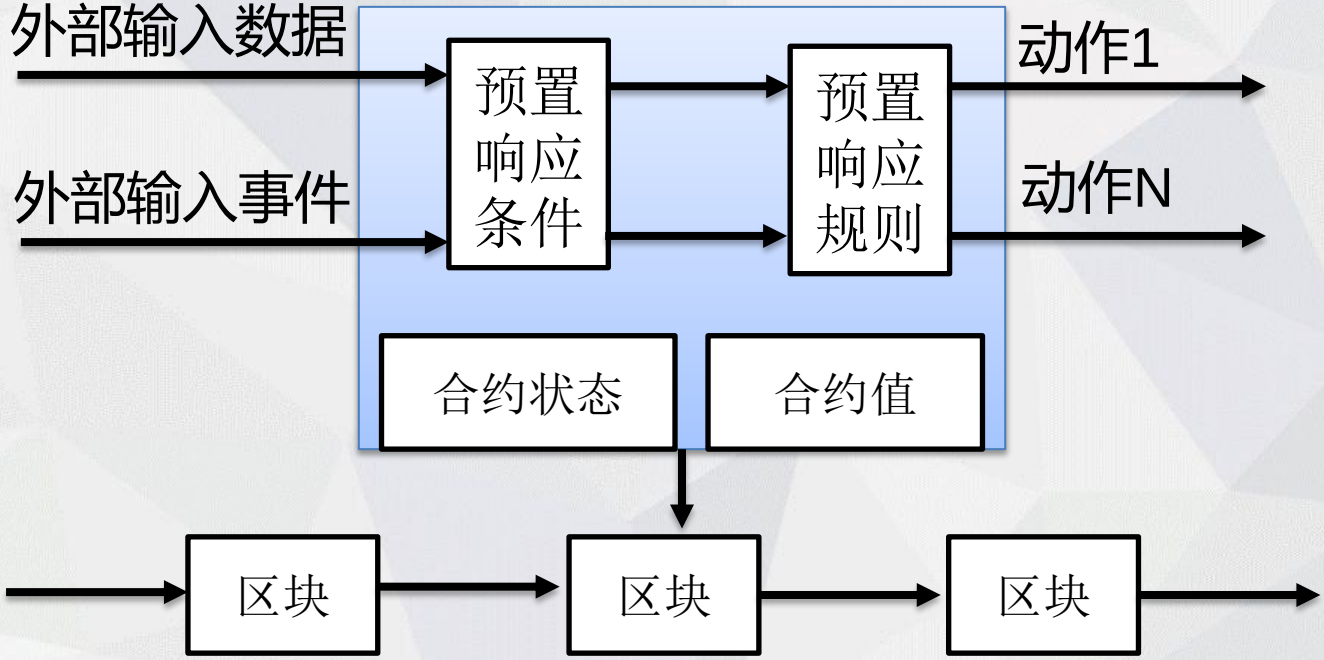
1.0 比特币使用的算力超122029 TH/s，相当于5000台天河2号A运算速度，每天耗电几十万人民币(估算)

什么是智能合约？
（目前尚没有明确定义）

智能合约是由事件驱动的、具有状态的、获得多方承认的、运行在一个可信、共享的区块链账本之上的、且能够根据预设条件自动处理账本上资产的程序。

智能合约的优势是利用程序算法替代人仲裁和执行合同。

智能合约模型



智能合约长什么样？

```
contract Sample
{       uint value; //定义变量
        function Sample(uint v) {  //初始化
        value = v;      }
        function set(uint v) { //定义存储函数
                value = v;      }
        //定义取值函数
        function get() constant returns (uint) {
                return value;
        }
}
```

Solidity

Go语言

JAVA

自定义语言

为什么传统IT系统无法实现智能合约？

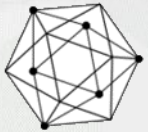
常见具备2.0特性的区块链

以太坊---本文以此为例

2015年正式版发布，用户和应用丰富

LISK

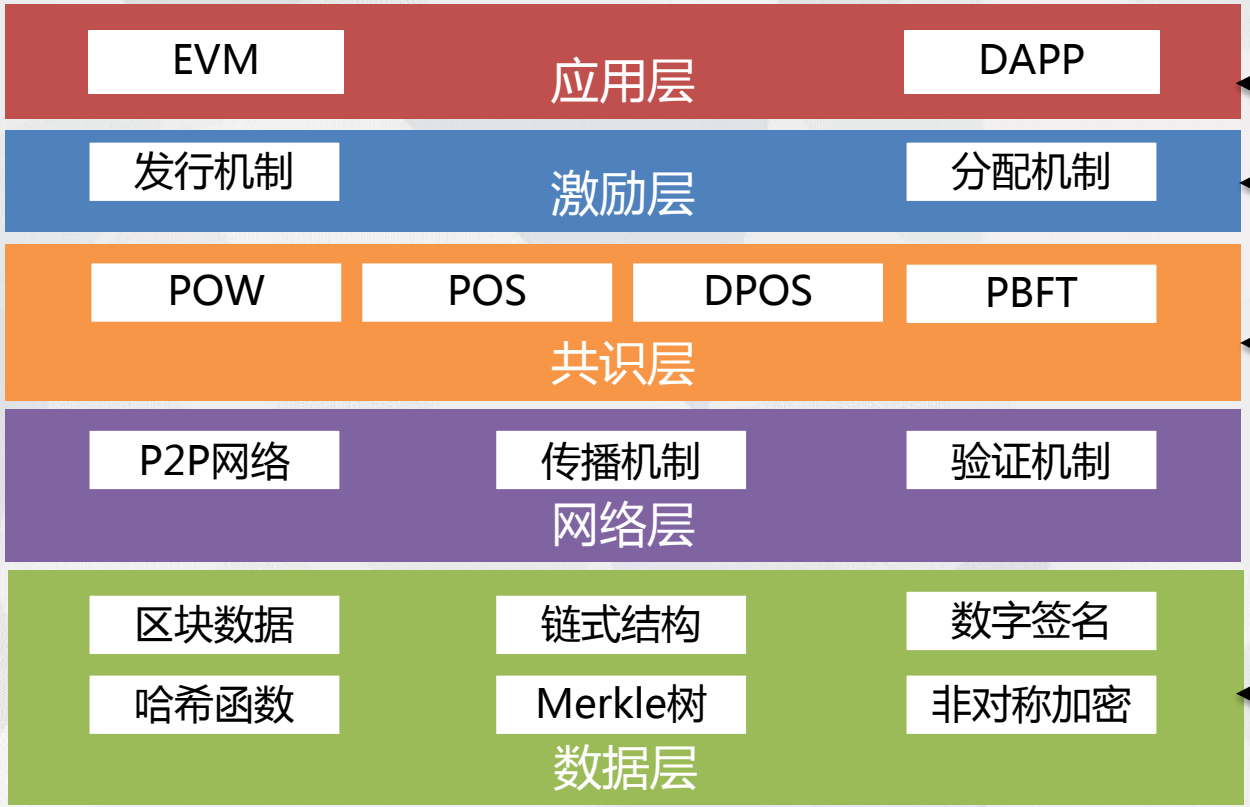
2016年6月正式版发布，用户和应用很少



Hyperledger

定义为企业级区块链，由linux基金会管理

架构升级



应用层增加了智能合约功能

缩短出块时间为16秒

加入DPOS、POS和PBFT

扩充了区块，支持发送数据和变量，采用优化的加密算法和Merkle树

交易数据中加入了Input data

TxHash:此交易的加密哈希值

From：钱包地址

To：对方钱包地址

Value:转账金额

Input data：输入的数据、变量

交易主信息

区块链2.0

合约层

激励层

共识层

网络层

数据层

PBFT	股权证明 POS	授权股权 DPOS
• 通过数学算法实现,不需代币，33%容	• 股份制，通过币天数决定记账权，适合公	• 民主议会制，通过选举决定记账权，适合

■ 优点

不需要大量算力进行挖矿，可以大量的节省资源消耗，同时提高交易的速度，以太坊未来采用POS共识机制后，可以实现秒级确认。

■ 缺点

PBFT不能防范女巫攻击，不适合公有链，但性能很好。POS和DPOS需要代币参与，不合适行业应用。

合约层

激励层

共识层

网络层

数据层

- 降低区块间隔到16秒，为防止分叉，加入叔伯块的奖励

由于区块生成间隔时间太短，延迟2秒都对整个网络的POW运算有很大影响，容易分叉，为鼓励维护主链，分叉的区块也有奖励

合约层

激励层

共识层

网络层

数据层

■ 以太坊虚拟机（EVM）

以太坊中智能合约的运行环境。如果做比喻的话智能合约运行更像是JAVA程序，JAVA程序通过JAVA虚拟机（JVM）将代码解释字节进行执行，以太坊的智能合约通过以太坊虚拟机（EVM）解释成字节码进行执行

智能合约部署原理

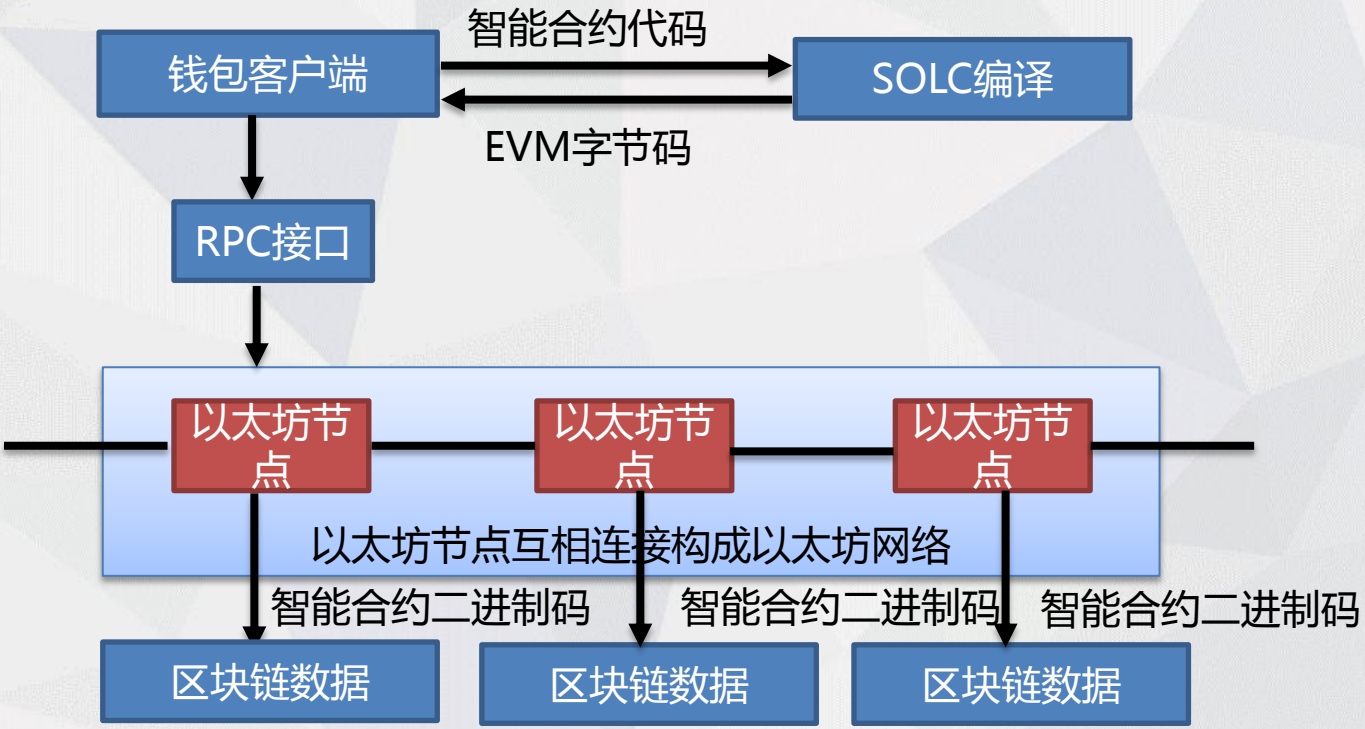
合约层

激励层

共识层

网络层

数据层



部署的数据流

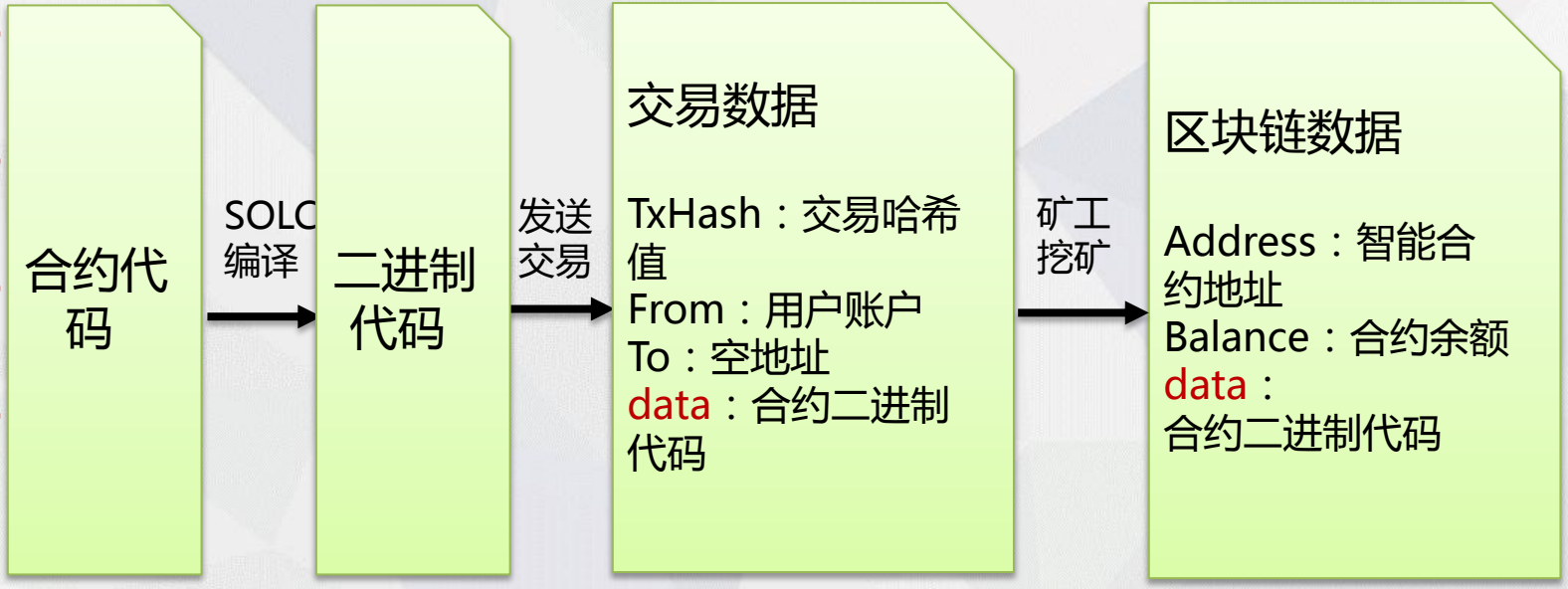
合约层

激励层

共识层

网络层

数据层



智能合约运行原理

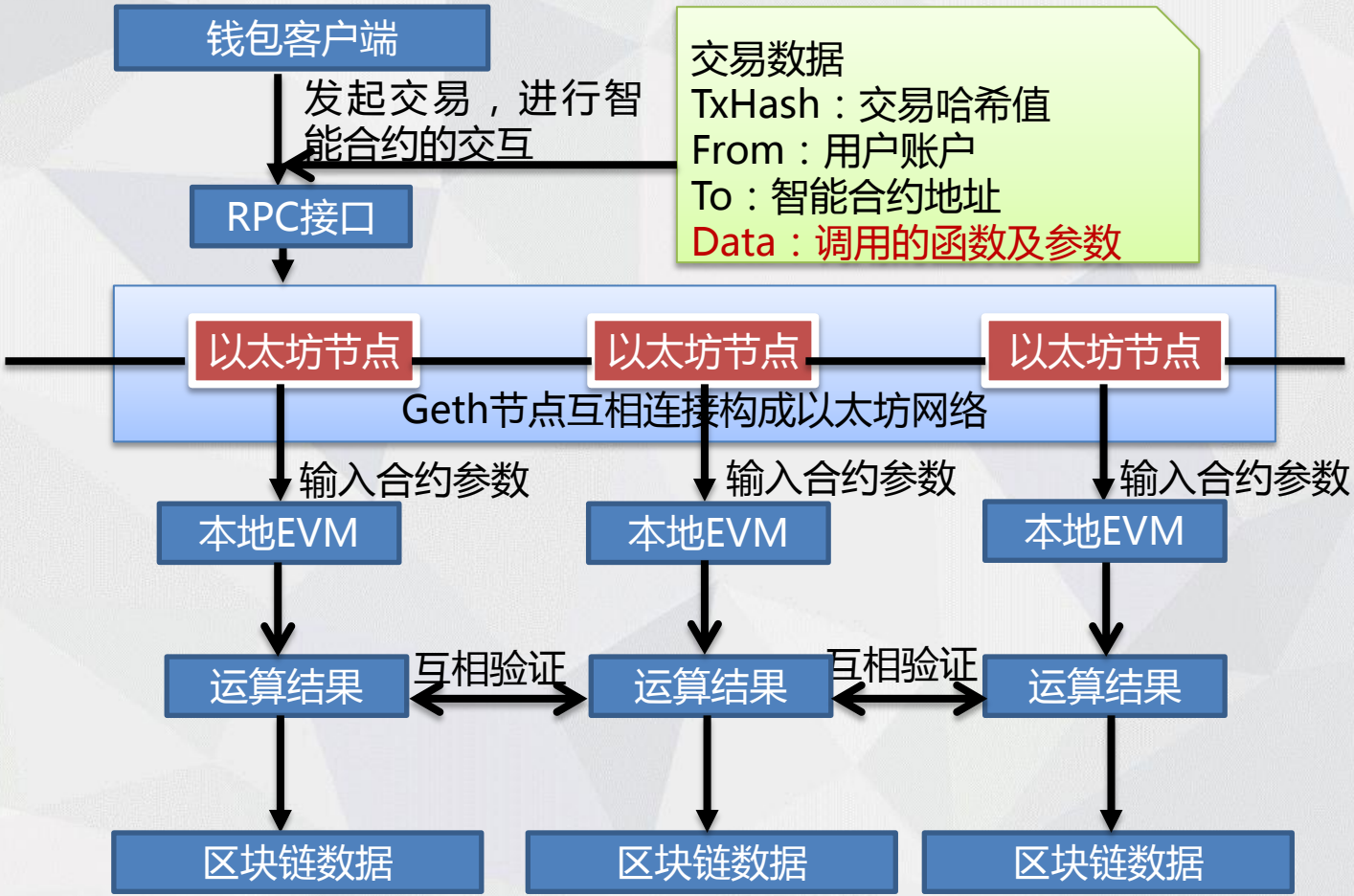
合约层

激励层

共识层

网络层

数据层



GAS

合约层

激励层

共识层

网络层

数据层

- 如果有人提交1T代码量的智能合约给区块链怎么办？
- 如果有人恶意写入无限循环代码放入区块链怎么办？
- GAS如何防范以上情况？
- 为什么不用以太币

智能合约示例及GAS消耗


```
1  //Sample contract
2  contract Sample
3  {
4      uint value;
5      function Sample(uint v) { max execution cost: 20147 gas
6          value = v;
7      }
8      function set(uint v) { max execution cost: 20138 gas
9          value = v;
10     }
11     function get() constant returns (uint) { max execution cost: 247 gas
12         return value;
13     }
14 }
15
```

以上代码部署运行一次大约使用0.0013以太币，约合人民币9分钱

智能合约与其他IT系统对接

- RPC接口

以太坊节点程序Geth在8545端口提供了JSON RPC API ，数据传输采用JSON格式，可以执行Web3库的各种命令，可以向前端，比如Mist等图形化客户端提供区块链的信息，默认访问地址为http://localhost:8545

智能合约与DAPP

合约层

激励层

共识层

网络层

数据层

智能合约相当于服务器后台，要实现与用户的友好体验，还需要一个前台页面，通过RPC接口与后台对接，实现网页访问，部署在服务器上，拥有完整的智能合约+前台交互界面的组合体，称为Dapp

04

PART 01

第四部分

区块链2.0应用

※ 目前状态

※ 新型信用体系

※ 互助保险

※ 应用误区

区块链2.0应用

摩根士丹利、富国银行、高盛、汇丰银行、法国外贸银行、加拿大丰业银行、中国平安集团、中国外汇交易中心等五十多家全球顶级金融机构组成R3区块链联盟

区块链2.0应用

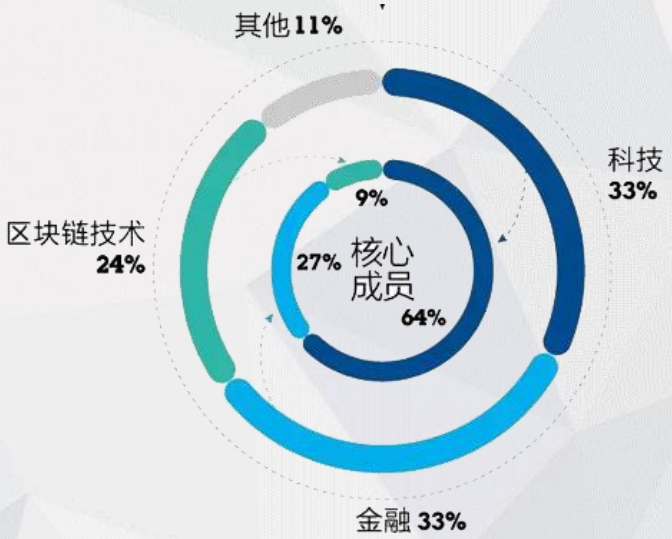
区块链联盟Hyperledger成员分布

THE LINUX FOUNDATION

Linux基金会成立于2000年

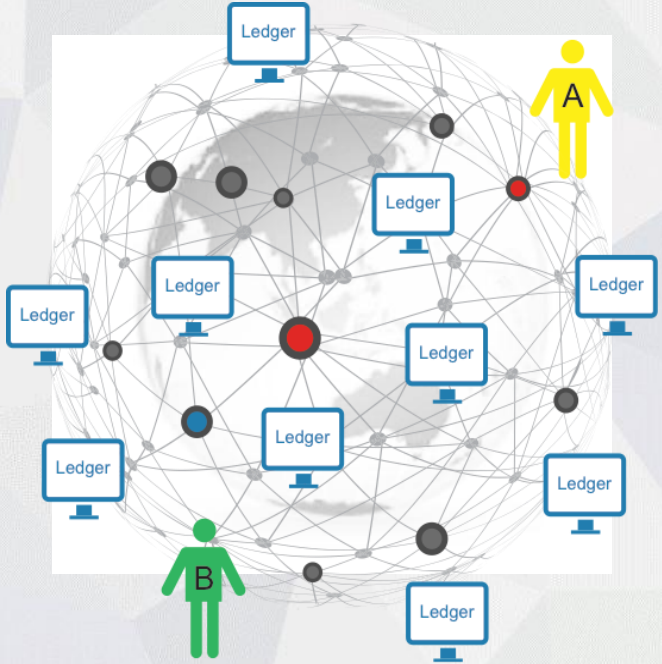
HYPERLEDGER PROJECT

成立于2015年12月



区块链2.0应用

传统金融模式



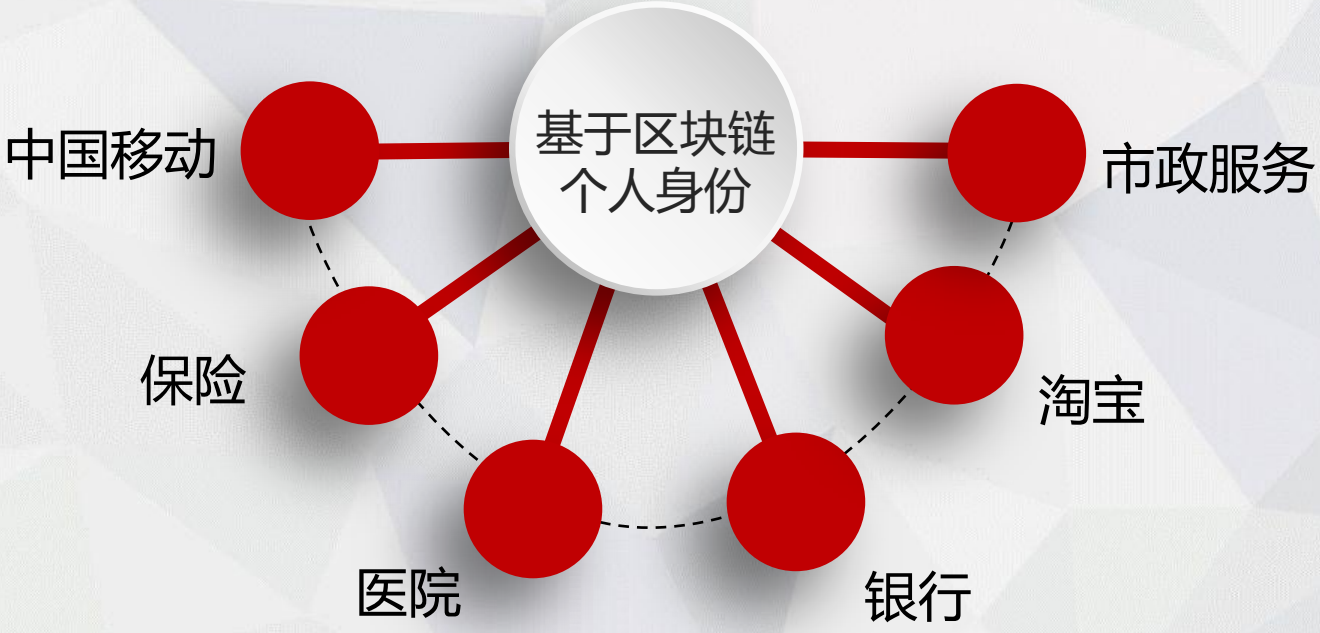
区块链模式

最重要的应用领域是金融。

金融业属于强监管，应用一定要注意合规！

常见的金融应用

真正属于用户自己的信用体系



互助保险

风险共担
经济互助

使用区块链的公开透明，不可篡改自证清白，建立个人到个人的信任

区块链应用注意事项

1. 区块链和智能合约能实现的，现在有IT系统都能实现
2. 区块链实现的不是性能的提升，而是业务模式的改变，相反性能大幅度下降，核心是去中介化
3. 只能实现对链内内生的信息信任，对外界引入的信息无法建立信任
4. 区块链应用不需要币

区块链2.0应用

区块链伪应用

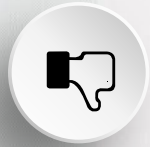
1、智能合约实现保险自动理赔

2、区块链实现海淘奶粉防伪

区块链不合规应用

1、保险业通过区块链共享客户信息，快速征信，不怕骗保

2、目前的基于区块链的网络互助



无人监管的资金池，严重违规

无偿付准备金刚性给付

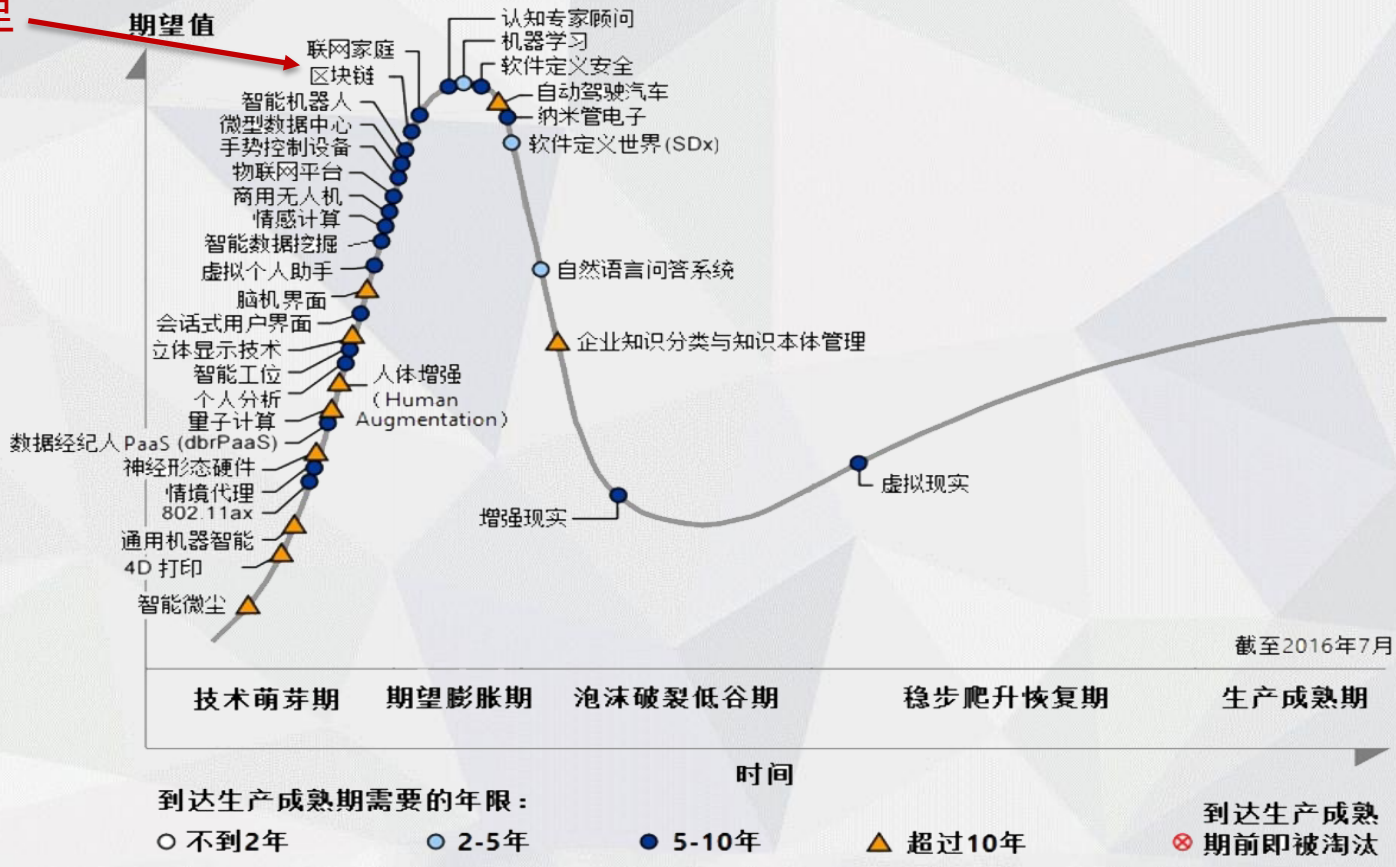
不满足偿付能力监管要求

无监管兜底，公司倒闭后保单失效

区块链2.0应用

我在这里

区块链的Gartner图



冷静　专业　坚持

2016

汇报完毕 感谢观看

李赫 18600686891