区块链的八大共识机制

共识机制是指以去中心化的方式就网络的状态达成统一协议的过程。 也被称为共识算法，有助于验证和验证信息被添加到分类账簿，确保只有真实的事务记录在区块链上。

1. **PoW 工作量证明**:

通过哈希计算找出合理数据的步骤来完成（多劳多得）。其验证过程需要大量的数据计算，而其他节点却很容易验证计算结果是否正确。缺点是消耗大量能源（电力与硬件损耗），以及 51%攻击。

2. PoS 权益证明：

同样需要通过计算找出合理的哈希值来完成。但不同的是权益证明机制通过节点持有加密货币的时间和数量来判断节点的权益大小。优点是无需每个节点的大量运算，节省能源，且能有效的防止 51%攻击。缺点是大数量节点权力过大，对区块链记账享有绝对支配权的情况，容易引发信任问题。

3. DPoS 委托权益证明：

DPoS 委托权益证明通过由持币人投票选举出一定数量的代表来达成共识。代表轮流获得记账权记账，且履行不好可被投票除名。任期结束，再次选举。

4. 容量证明/空间和时间证明：

是工作量证明的改进，关注的是内存而非处理能力。在挖掘开始之前，容量证明也要求节点将预先计算的哈希值存储在其硬盘驱动器和其他内存单元上，这个过程称为绘图，绘图使容量证明成为比工作证明更快的机制。节省能源且可能促进技术的发展。

5. 唯一节点列表(UNL)：

核心是允许某些节点签署交易，任何用户都可以简单地验证签署的区块是否是最新的。UNL 非常类似于向某些网站颁发数字证书的证书颁发机构，节点由不同的实体运营，降低了受到 Sybil 攻击的可能性。UNL 共识机制也是目前较快的机制之一。然而，最大的缺点是它是一个比其他共识机制更加集中的区块链系统。

6. 已用时间证明：

通过关注随机化来取代工作量证明系统的低效率和诱导浪费的竞争。经过时间证明会随机为其节点提供一个计时器对象。计时器首先到期的节点将负责发布下一个块。该系统为拜占庭将军问题的随机领导者选择方面提供了有效的解决方案。但缺点是已被证明存在一些严重漏洞，导致难以建立信任共识机制。且难以保证计时器对象节点的唯一性以及纯随机的分配会导致用户利用多节点来增加被选中的概率。

- 拜占庭将军问题:

简介：拜占庭将军问题是一个协议问题，拜占庭帝国军队的将军们必须全体一致的决定是否攻击某一支敌军。问题是这些将军在地理上是分隔开来的，并且将军中存在叛徒。叛徒可以任意行动以达到以下目标：欺骗某些将军采取进攻行动；促成一个不是所有将军都同意

的决定，如当将军们不希望进攻时促成进攻行动；或者迷惑某些将军，使他们无法做出决定。如果叛徒达到了这些目的之一，则任何攻击行动的结果都是注定要失败的，只有完全达成一致的努力才能获得胜利。拜占庭假设是对现实世界的模型化，由于硬件错误、网络拥塞或断开以及遭到恶意攻击，计算机和网络可能出现不可预料的行为。

内涵：在互联网大背景下，当需要与不熟悉的对方进行价值交换活动时，人们如何才能防止不会被其中的恶意破坏者欺骗、迷惑从而作出错误的决策。进一步将“拜占庭将军问题”延伸到技术领域中来，其内涵可概括为：在缺少可信任的中央节点和可信任的通道的情况下，分布在网络中的各个节点应如何达成共识。

与比特币的关系：中本聪发明的比特币很好的解决了拜占庭将军问题。其最终解决的是互联网交易与合作过程中的四个问题：1.信息发送的身份追溯；2.信息的私密性；3，不可伪造的签名；4.发送信息的规则。

7. 权威证明：

权益证明质押硬币，权威证明质押声誉。该机制快速且可扩展，同时不浪费能源。但不遵循去中心化原则，可以轻松实施审查及资金冻结等行为。

8. 有向无环图 DAG：

1OTA 使用的 Tangle 也是 DAG 共识机制的一种形式。在这种机制中，每个块必须有两个父块。所以，为了通过 DAG 共识机制完成一笔交易，用户需要验证自己之前的两笔交易。这种机制的最大优势是它可以减少延迟和交易费用。缺点是无法提高可扩展性，极易受到攻击（34%的哈希算力就可以破坏系统）。

区块链技术暂时没有完美的共识机制，仍需要新的共识机制来突破极限。

区块链技术（本科）——吴永东

引论

区块链的本质：不可篡改的数据库。

区块链密码技术

1. 哈希算法

可以将任意长度的消息或数据压缩成固定长度的摘要。是一种对任何数据创建其数字指纹的方法。

评价散列函数的标准包括：正向快速，输入敏感，不易碰撞，单向性。

- 比特币中的哈希函数

SHA-256：构造区块链的区块；RIPEMD160：生成比特币的地址。

SHA-2 是一个密码散列函数算法标准，可再细分为六个不同的算法标准，具有不同的哈希值长度、不同的循环次数以及相同的算法结构。

- SHA-256

预处理：附加填充比特使报文长度对 512 取模后的余数是 448，最少补 1 位，最多补 512 位。后加上 64bit 的原始数据长度 0x18，组成 512bit 的序列。因此消息块可以分成 512bit 的整数倍。

初始化：8 个哈希储值 h0----h7 和 64 个哈希常量 kt(t=0...63)是固定的取值。

2. 数字签名

一种公钥密码技术，达到类似普通签名的效果。包括签名 sign()和验证 verify()两部分。

区块链-北大肖臻

BTC-网络

flooding 传播，在区块链上传播的比特币区块最大限制为 1MB。

支付宝退款与区块链的回滚是两种不同的操作，退款是重新发起的一笔交易而回滚是取消已有的交易。

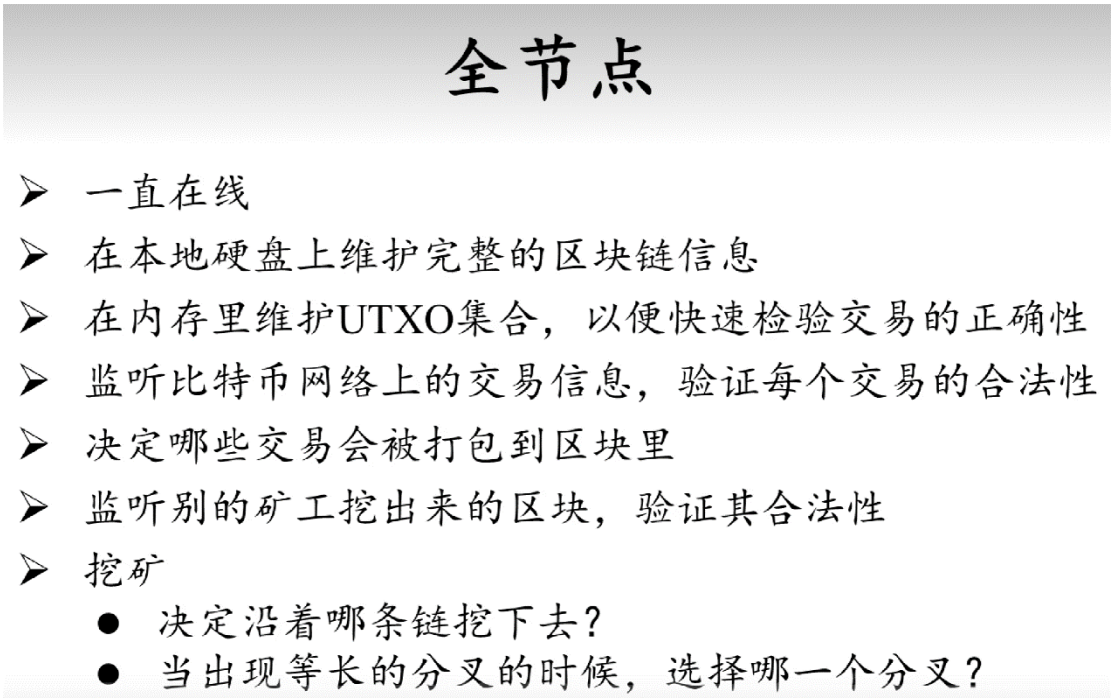
BTC-挖矿难度，挖矿难度同目标阈值成反比。若是难度过小，区块链极易发生大分叉，分散整体算力，恶意区块便可集中算力延长非法链，导致%51 攻击只需要十几的算力即可成功。

以太坊的难度较小，导致了分叉很容易出现，所以利用了一种新的共识机制：ghost，对分叉中的 orphan block 也给予奖励。

比特币每 2016 个区块调整挖矿难度，时间消耗维持在两周。每次调整最多正负四倍难度，防止意外情况导致难度波动。如何使得所有区块都调整难度？这个规则写在代码里并且开源，但对于恶意节点不更改难度时，诚实节点拒绝接受其区块。

BTC-挖矿：

全节点：



轻节点：

轻节点

- 不是一直在线
- 不用保存整个区块链，只要保存每个区块的块头
- 不用保存全部交易，只保存与自己相关的交易
- 无法检验大多数交易的合法性，只能检验与自己相关的那些交易的合法性。
- 无法检测网上发布的区块的正确性
- 可以验证挖矿的难度
- 只能检测哪个是最长链，不知道哪个是最长合法链

如果只交易，不挖矿，则只需维持一个轻节点。

挖矿过程中，若发布了新区块，则需重新设置开始挖新区块，因为挖矿的无记忆性不会因为之前挖的久而有更高的挖到比特币的可能。

挖矿设备：CPU->GPU（大规模并行运算、矩阵运算）->ASIC 芯片专用于挖矿（性价比最高）

矿池：包括多个矿工，并进行利益分配。矿工只负责提供算力即可。矿主统计每个矿工的工作量（近似 nonce），待出块时分配比特币。矿池的收款地址是矿主的，所以不可能存在偷发区块获得奖励的可能。但因为矿池的存在，使得比特币系统更容易受到 51%攻击，且矿池里的矿工也并非全是恶意的，因为他们只是在为矿池做哈希计算。且 51%算力并非绝对的阈值，因为发布区块的结果都是概率的。

攻击方式：1.分叉攻击；2.Boycott 联合抵制；

BTC-比特币脚本

脚本的运行基于栈结构，所有操作都压入栈然后出栈执行。

Proof of Burn：使得任何人都可以通过销毁很少的比特币而获得像比特币区块内写入内容的机会，从而达到某种声明。

交易结构

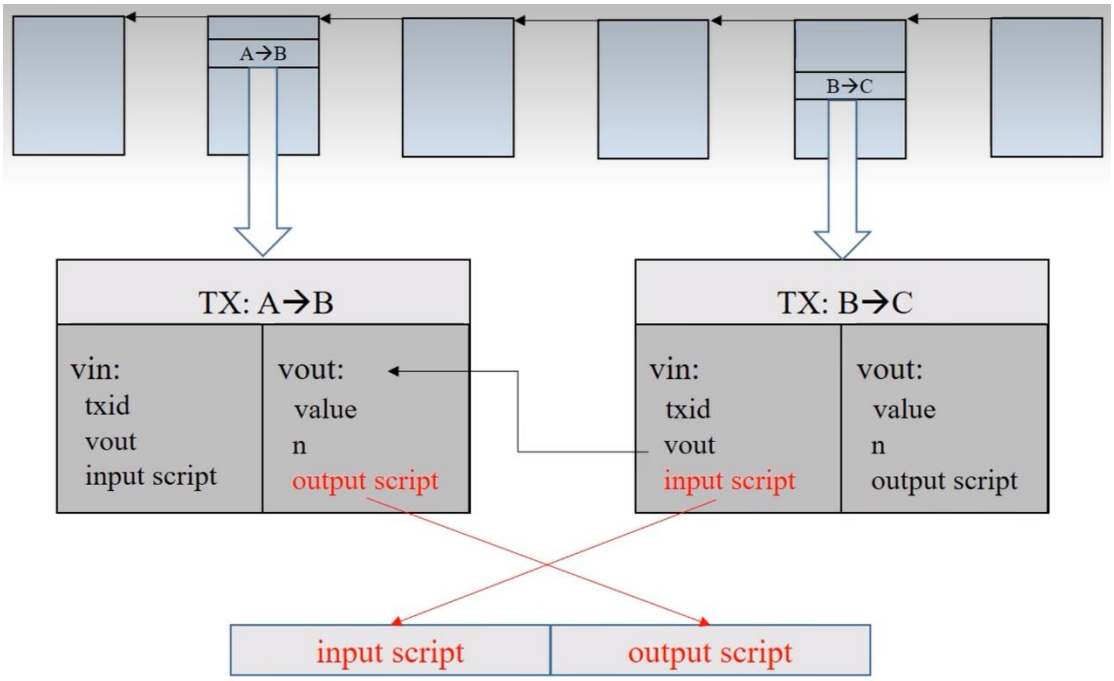
```
"result": {
    "txid": "921a…dd24",
    "hash": "921a…dd24",
    "version": 1,
    "size": 226,
    "locktime": 0,
    "vin": […],
    "vout": […],
    "blockhash": "00000000000000002c510d…5c0b",
    "confirmations": 23,
    "time": 1530846727,
    "blocktime": 1530846727
}
```

交易的输入

```
"vin": [{
    "txid": "c0cb…c57b",
    "vout": 0,
    "scriptSig": {
        "asm": "3045...0018",
        "hex": "4830...0018"
    },
}],
```

交易的输出

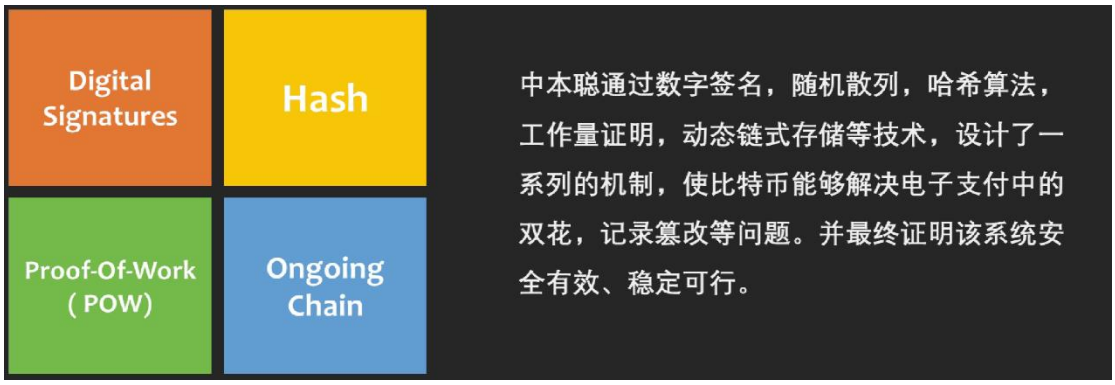

```
"vout": [{
    "value": 0.22684000,
    "n": 0,
    "scriptPubKey": {
        "asm": "DUP HASH160 628e…d743 EQUALVERIFY CHECKSIG",
        "hex": "76a9…88ac",
        "reqSigs": 1,
        "type": "pubkeyhash",
        "addresses": [ "19z8LJkNXLrTv2QK5jgTncJCGUEEfpQvSr"]
    }
 },{
    "value": 0.53756644,
    "n": 1,
    "scriptPubKey": {
        "asm": "DUP HASH160 da7d…2cd2 EQUALVERIFY CHECKSIG",
        "hex": "76a9…88ac",
        "reqSigs": 1,
        "type": "pubkeyhash",
        "addresses": ["1LvGTpdyeVLcLCDK2m9f7Pbh7zwhs7NYhX"]
    }
}],
```

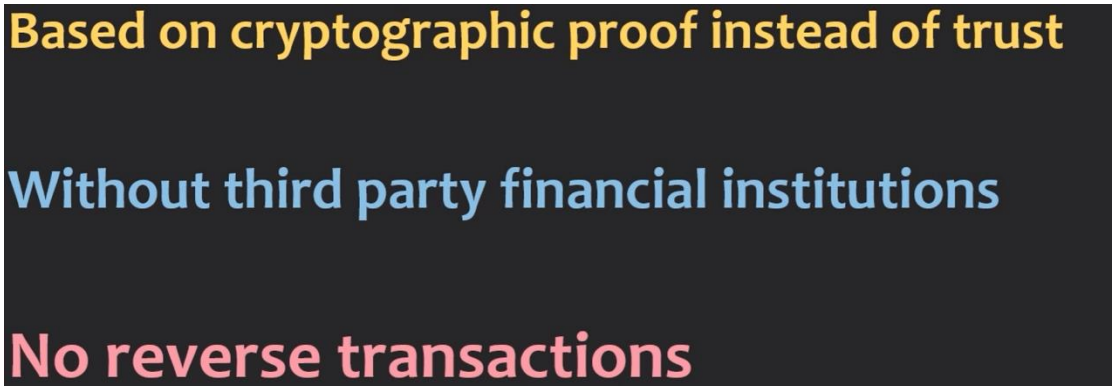



《精通比特币》

比特币白皮书 Bitcoin: A Peer-to-Peer Electronic Cash System

https://www.bilibili.com/video/BV1Hh411Z7id/?spm_id_from=333.1007.top_right_bar_window_custom_collection.content.click&vd_source=0959d2714128b6c18ac26903e455254b





背景

互联网的金融贸易，其电子支付信息几乎全部需要可信赖的第三方（金融机构等）才能实现。但存在着内生性的、基于信用的模式的弱点，只要存在第三方中介便无法避免：

1. 互联网贸易存在问题

- 交易可逆

  传统互联网贸易无法实现完全不可逆的交易，因为金融机构会不可避免地出面调节争端。

- 成本

  金融中介在交易过程中会收取手续费。

- 交易自由度

  中介限制了日常的小额支付，无法运用在日常支付中。

- 售后

  缺乏不可逆的支付手段，互联网贸易便会由于很多商品或服务本身是无法退货的而受限。

- 信息泄露

  由于有潜在的退款的可能，就需要交易双方拥有信任。而商家也必须提防自己的客户，因此会向客户索取完全不必要的个人信息。

2. 区块链的提出

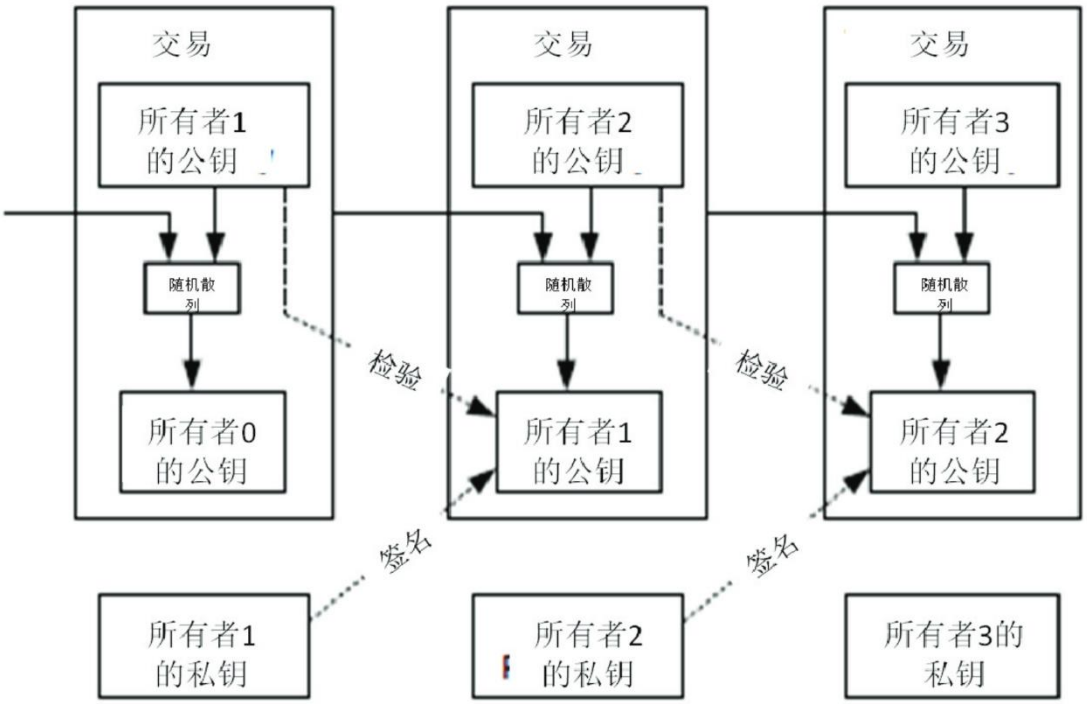
因此，需要一种电子支付系统：
为了取缔第三方中介→选择基于密码学原理而非基于信任。
为了避免卖家受欺诈→杜绝了回滚交易的可能。
为了保护买家→使第三方担保机制易于设立。
一种通过点对点分布式的时间戳服务器来生成依照时间前后排列并记录的电子交易证明。时间戳的添加解决了双重支付问题，安全性则是基于算力，只要恶意算力不大于一半，系统则安全。

交易过程

现阶段交易模型分为两种：基于账户的交易与基于 UTXO 的交易，比特币属于后者。

1. 如何定义电子货币

一枚电子货币（an electronic coin）是这样的一串数字签名：每一位所有者通过对前一次交易和下一位拥有者的公钥(Public key) 签署一个随机散列的数字签名，并将这个签名附加在这枚电子货币的末尾，电子货币就发送给了下一位所有者。而收款人通过对签名进行检验，就能够验证该链条的所有者。

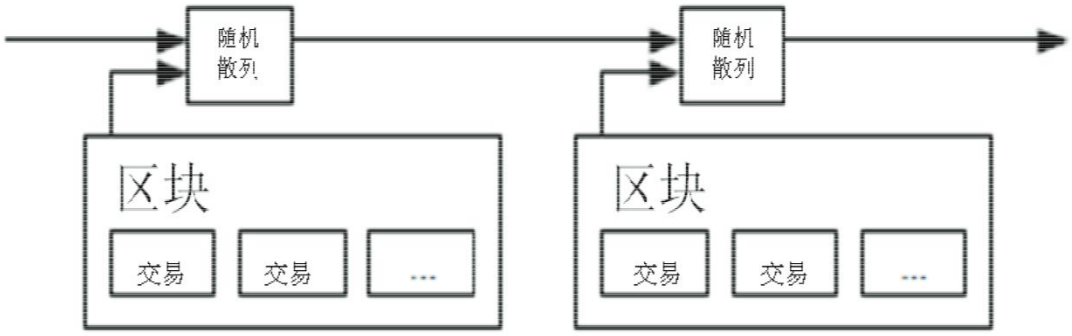


2. 双重支付的解决

由于无法通过数字签名确定该货币是否被双重支付，需要考虑额外的方法来完成该确定。在系统中，如果要取缔第三方中介机构完成去中心化，则需要将交易信息公开宣布。使整个系统的参与者共同见证交易，从而确保交易期间的该交易首次出现。

时间戳服务器

时间戳服务器通过对以区块(block)形式存在的一组数据实施随机散列而加上时间戳，并将该随机散列广播。每一个随后的时间戳都包含着前一个，从而形成了增强，以此来证明时间的顺序。



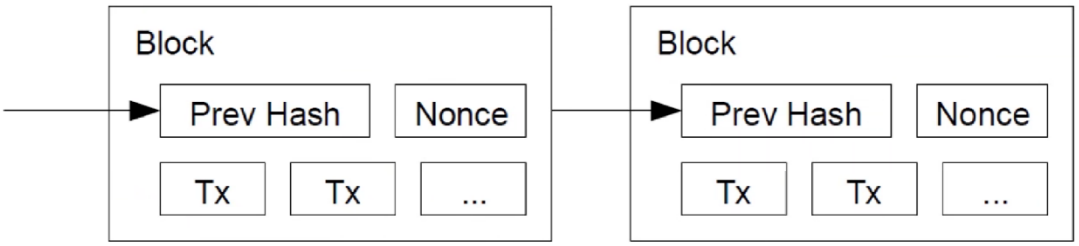
投票权-POW 工作量证明机制

在区块中补增一个随机数(Nonce)，这个随机数要使得该给定区块的随机散列值出现了所需的那么多个 0。我们通过反复尝试来找到这个随机数，直到找到为止，这样我们就构建

了一个工作量证明机制。若要更改该块的信息，则需要重新完成该块以及之后所有块的工作量，这几乎是不可能的。

工作量证明 Proof-of-Work

Hash (nonce || prev_hash || tx || ... || tx) < target



工作量证明机制也解决了投票权分配的问题，本质是按算力投票。投票的大多数即为最长链。攻击者若想修改链条是极其困难的。

由于硬件升级带来的算力提升，POW 的难度采用移动平均目标的方法确定。

网络

如何运行整个分布式系统呢？步骤如下：

1）新的交易向全网进行广播；

2）每一个节点都将收到的交易信息纳入一个区块中；

3）每个节点都尝试在自己的区块中找到一个具有足够难度的工作量证明；

4）当一个节点找到了一个工作量证明，它就向全网进行广播；

5）当且仅当包含在该区块中的所有交易都是有效的且之前未存在过的，其他节点才认同该区块的有效性；

6）其他节点表示他们接受该区块，而表示接受的方法，则是在跟随该区块的末尾，制造新的区块以延长该链条，而将被接受区块的随机散列值视为先前新区快的随机散列值

Tips：

若收到到多个区块广播，会在先收到的区块上工作，但也会保留另一个备份，直到哪一个先挖出新区块后转换阵营工作。

交易的广播也并非抵达全部节点，因为会被整合进区块中，区块的广播对交易信息具有很强的容错能力。且丢失区块时也允许节点下载区块的请求。

激励

节点得到的奖励=出块奖励+交易手续费用

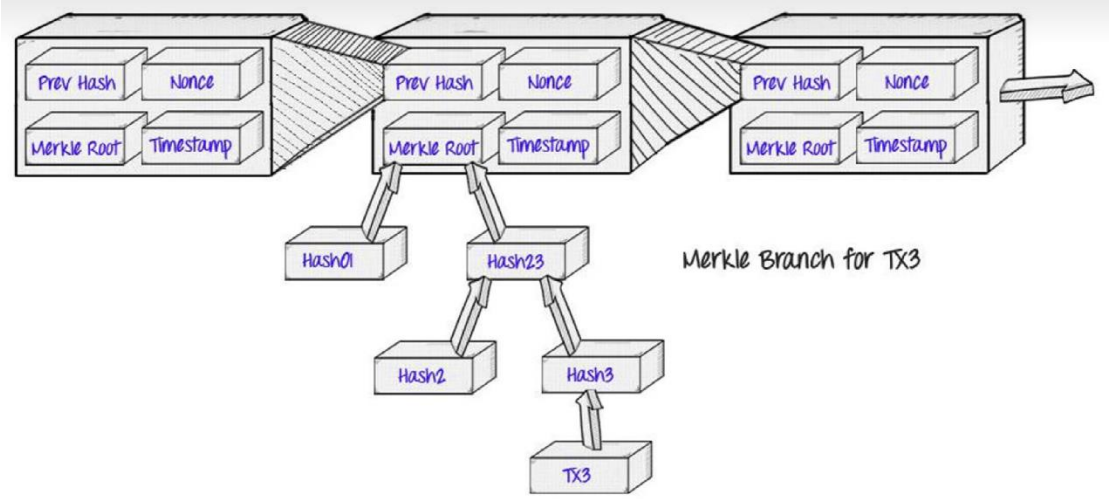
交易手续费用=交易的 input-交易的 output

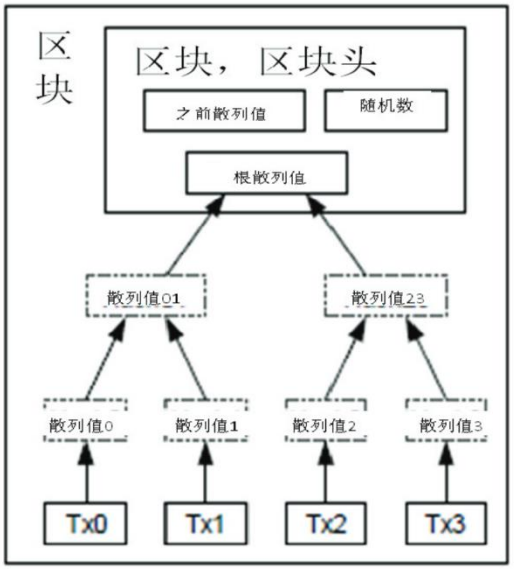
激励的存在使得具有一半以上算力的节点选择诚实挖矿获得的收益要比破坏系统，损失

财富有效性来的更大。

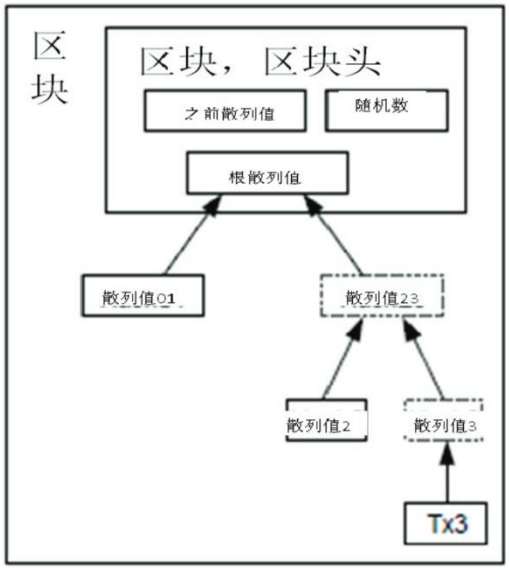
回收硬盘空间

如果最近的交易已经被纳入了足够多的区块之中，那么就可以丢弃该交易之前的数据，以回收硬盘空间。为了同时确保不损害区块的随机散列值，交易信息被随机散列时，被构建成一种 Merkle 树（Merkle tree）的形态，使得只有根(root)被纳入了区块的随机散列值。通过将该树（tree）的分支拔除（stubbing）的方法，老区块就能被压缩。而内部的随机散列值是不必保存的。





以Merkle树形式散列的交易

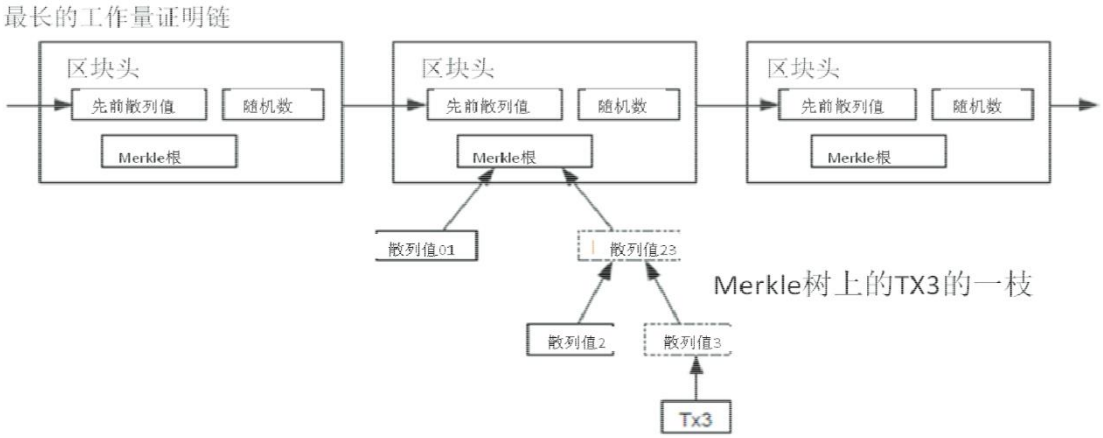


将Tx0-2从区块中剪除

简化交易证明

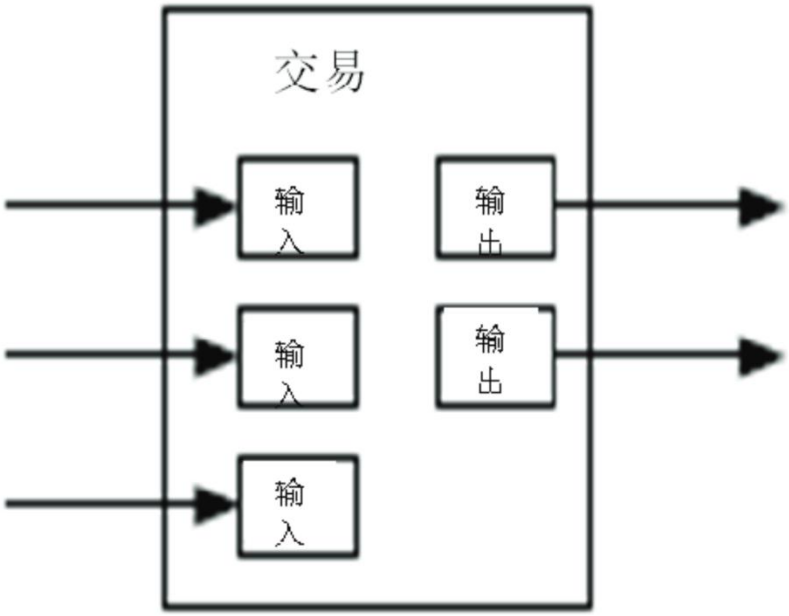
不用运行完整的节点也能进行支付验证的方式。全节点所需内存大约几百 G，而轻节点只需要保存最长共识区块链的区块头即可。

但这种方式遇到攻击也是不可靠的，需要同全网进行对照。

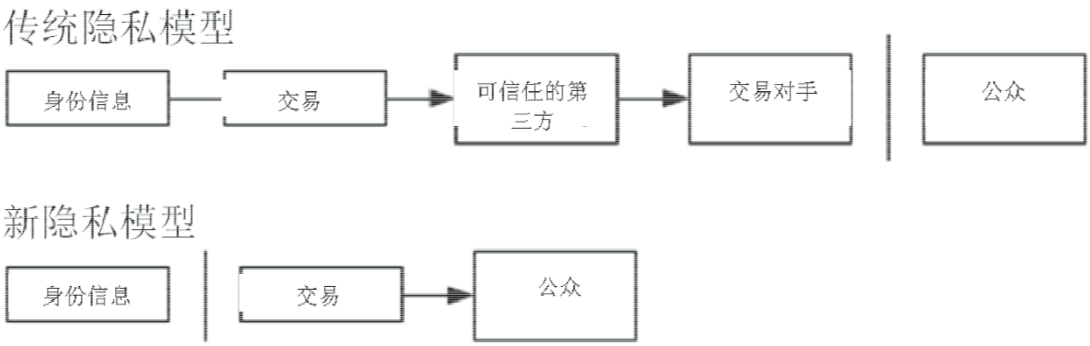


价值的组合与分割

交易可以有多个输入（并行输入），至多两个输出：支付与找零。



隐私



比特币模型中，交易记录完全公开记录在链上，但是由于公私钥对任何人都可以产生，交易双方的身份信息是匿名的。

额外的隐私操作，可以考虑每次交易均使用新地址，以避免追溯到同一拥有者。但缺点是一旦被确定一个公钥的所属，就可由追溯出此人其他所有交易。

面临攻击的计算

拿走其他账户的钱：这是不可能的，因为这个需要破解对方的私钥，这在现在的计算能力下是无法实现的。

双重支付：这是可能的，但成本极高。需要算力大于百分之五十且额外计算出双花时的区块以及之后的所有区块。且只能拿回自己花费的那一部分。

结论

归根到底为一种去中心化的经济学，包含了一个 P2P 电子货币系统所需要的全部规则和激励措施。

区块链技术解析

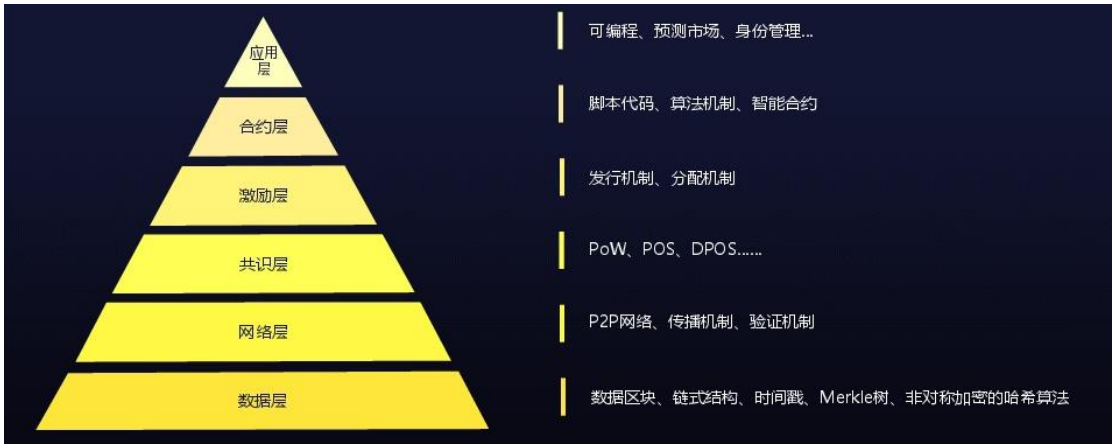
1. 什么是区块链？

一种促进人类大规模协作的技术手段，解决了多点之间相互信任以及利益分配的问题。

细节实现上：利用块链式数据结构来验证与存储数据、利用分布式节点共识算法，来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约，来编程和操作数据的一种全新的分布式基础架构与计算方式。

2. 区块链的运作原理

- 区块链系统的六层结构划分：



数据层：封装了底层数据区块，以及相关的数据加密和时间戳等基础数据和基本算法；
网络层：则包括分布式组网机制、数据传播机制和数据验证机制等；
共识层：封装网络节点的各类共识算法；
激励层：将经济因素集成到区块链技术体系中来，主要包括经济激励的发行机制和分配机制等；
合约层：主要封装各类脚本、算法和智能合约，是区块链可编程特性的基础；
应用层：封装了区块链的各种应用场景和案例。所有的二次开发应用都基于这一层面的，就类似于众多的 APP 基于 IOS 和安卓底层操作系统一样。

- 区块链在技术上的革新点在于：

分布式账本——不可篡改性与去中心化：每个节点记录完整的账目，都可以参与监督与作证交易合法性，避免了单一记账的弊端；同时多节点记账无惧单一节点账目受破坏或丢失，确保了安全性。
非对称加密和授权技术——匿名性、安全性：存储在区块链上的交易信息是公开的，但账户身份信息是高度加密的。
共识机制——开放性、自治性：达成怎样的共识来认定记录的有效性？不同的共识机制应用于不同场景，在效率和安全性之间取得平衡。
智能合约——不可逆性、强制性：基于可信且不可篡改的数据，自动化执行预先定义的规则与条款。

3. 区块链的出现与社会影响

由于 08 年金融危机而设计出的。
原始区块链是一去中心化的数据库，包含被称为区块的列表，有着可持续增长并排列整齐的记录。每个区块都包含时间戳和前一区块的 hash 值，使得区块链数据不可篡改，在数据记录下的那一刻数据将不可逆。这是一种保护措施，可以应用于高容错的分布式计算系统。区块链使得混合一致性成为可能，适用于记录事件、标题、医疗记录和其他需要收录数据的活动、身份识别管理，交易流程管理和出处证明管理。
为了解决金融危机的问题，建立一个不被任何组织和机构组织操控的，基于机器信任，代码信任的，去中心化的电子现金系统。区块链提供了无中介，无需信任单节点，全网共识的一种网络方法。可以防止我们在与陌生人进行价值交换活动时，被恶意欺诈的风险。
其颠覆性在于社会的“信任关系”，当社会关系的基础协议依赖于可信任的底层技术时，信息和交易都变得开放透明、不可篡改，社会规则和建立在此基础之上的组织形态也会发生重大的变化。

4. 现有问题——三元悖论

区块链系统事实上不可能同时在“去中心化”，“安全性”，“可扩展性”上达到最佳，只能做到降低某方面的能力换取另两领域的提升。

- 追求去中心化和安全性，则无法达到可扩展性：

比特币区块链技术便是一种极致追求“去中心化”和“安全”的技术组合。缺乏高效的可扩展性，对大型内容的处理上存在效率问题。

1）从数据结构上，它采用拥有时间戳的“区块+链”的结构，在可追溯、防篡改上具备安全优势，也易于分布式系统中的数据同步。但是若需要对信息进行查询、验证，则涉及到对链的遍历操作，而遍历是较为低效率的查询方式。

2）在数据存储上，它的每一个节点都下载和存储所有数据包，利用强冗余性获得强容错、强纠错能力，使得网络可以民主自治，但同时也带来了巨大的校验成本和存储空间损耗。它并不像分布式数据库那样随着节点的增加可以通过分布式存储提高整体存储能力，而只是简单地增加副本。未来随着区块链技术所承载的内容增多,单个节点的存储空间将是个问题。

3）在并发处理上，比特币区块链技术最终只允许一个 “矿工”获得记账权建立一个交易区块，这种机制可以有效保证一个民主网络运行的安全和稳健，但其实质上是拥有所有数据的整个“链条”在进行串行的“写”操作。相比关系数据库将数据分为若干表，仅仅根据操作涉及的数据锁定若干表或表中的记录、其他表仍能并发处理相比，比特币区块链技术的串行操作效率远低于普通数据库。

4）在对内容的验证上，比特币区块链让每个节点都拥有所有的内容，同时对区块内的所有内容进行哈希，这增强了：民主性、隐私性、安全性。但是这种整体哈希的设计思路则意味着，不能以地址引用的方式存储数据，否则由于所引用地址上所存储的信息由于并未进行哈希校验而可能存在篡改。

- 追求可扩展性与安全性，则无法完全实现去中心化

为了解决 PoW 的低效性，可能会采用权益证明（Proof of Stake）、股份授权证明（Dele - gate Proof of Stake）等机制，但无论哪种机制，实际上都是对“去中心化”的退让，形成了部分中心化。在比特币为代表的公有链基础上，又衍生出联盟链、私有链等。

联盟链技术只允许预设的节点进行记账，加入的节点都需要申请和身份验证，这种区块链技术实质上是——在确保安全和效率的基础上进行的“部分去中心化”或“多中心化”的妥协。

私有链技术的区块建立掌握在一个实体手中，且区块的读取权限可以选择性开放，它为了安全和效率已经完全演化成为一种“中心化”的技术。

- 追求可扩展性与去中心化，则必须牺牲安全性

基于 P2P（Peer-to-Peer）的视频播放软件，是一个极端的案例。一个节点在下载观看

视频文件的同时，也不断将数据传输给别人，每个节点不仅是下载者同时也是传输者，使资源的分享形成不再依赖于中央服务器的“去中心化”模式。由于视频一秒有 24 帧，少量图片的局部数据损坏并不影响太多的视觉感官，但是用于数据校验而出现的图像延迟则是不可接受的。于是 P2P 视频播放软件牺牲了“安全”性，允许传输的数据出现少量错误。在这种去中心化的网络中，参与的节点越多，数据的传播越快，传播的效率越高。这种方式对于某些行业或许适合，对于严谨的金融业来说，数据的错误是不可接受的，安全也是金融业所首要考虑的问题。

5. 区块链技术展望

当今社会的商业成本高昂，两个公司之间签订了一个合约，需要建立很多机制来保证合同能顺利执行。当出现一方违约的情况，就需要法院和律师、警察来协助我们判决和推动执行。在区块链的世界中，可以通过智能合约来自动执行类似合约，可以帮助我们节省大量的人工和时间成本，人们几乎不需要担心任何节点发生意外，也没有人能够恶意地去破坏或者篡改。

区块链通过升级现代商业社会的三个基石来改变世界：

复式记帐法——传统的复式记帐法变成了分布式账本；

有限制度公司——有限公司制度变成了 DAO 分布式自治组织；

分布式自治组织（decentralized autonomous organization，DAO ），有时也被称为分布式自治公司（DAC），是一种以公开透明的计算机代码来体现的组织，其受控于股东，并不受中央政府影响。一个分布式自治组织的金融交易记录和程序规则是保存在区块链中的。目前分布式自治组织确切的法律地位还不清楚。

分布式自治组织的特征之一是通过使用区块链技术提供一个安全的数字账本，以追踪在整个互联网的金融互动，通过信任的时间戳和传播一个分布式数据库来抗伪造。[3]:229[4][9] 这种方法使得金融事务中无需涉及一个互相可接受信任的第三方，从而简化交易。[4] 对双方信任的第三方的取代以及避免了不同版本合约交换的重复记录所带来的好处，基本可以抵消基于区块链的高昂交易成本和相应的数据汇报问题。例如，如果监管机构允许，区块链的数据在原则上可能取代公共文件，例如契据和称号。[3]:42[4] 在理论上，一块链的项目允许多个基于云计算的用户进入一种松散耦合的点对点的智能合约式的协作关系。[3]:42[10]

丹尼尔拉里默在2013年9月7日发表的一篇文章中第一次提出概念“分布式组织公司”[11] 并且在2014年在比特股，2018年在EOS.IO（页面存档备份，存于互联网档案馆）中实现。[12][13][14][15][16]

维塔利克·布特林声称，只要拥有了基于图灵完备的平台的智能合约，分布式自治组织一旦启动，能在没有人为管理行为条件下，一直有序运行。[17]基于区块链技术，于2015年启动的以太坊，一直被称为符合了图灵完备的要求，因此能支持这样的分布式自治组织。[3]:229[18][19] 分布式自治组织的目标是开放平台，使个人能控制自己的身份和他们的个人数据。[20]

保护私有财产的法律制度——保护私有财产的法律制度变成了智能合约。同时也拥有着极多的应用前景：

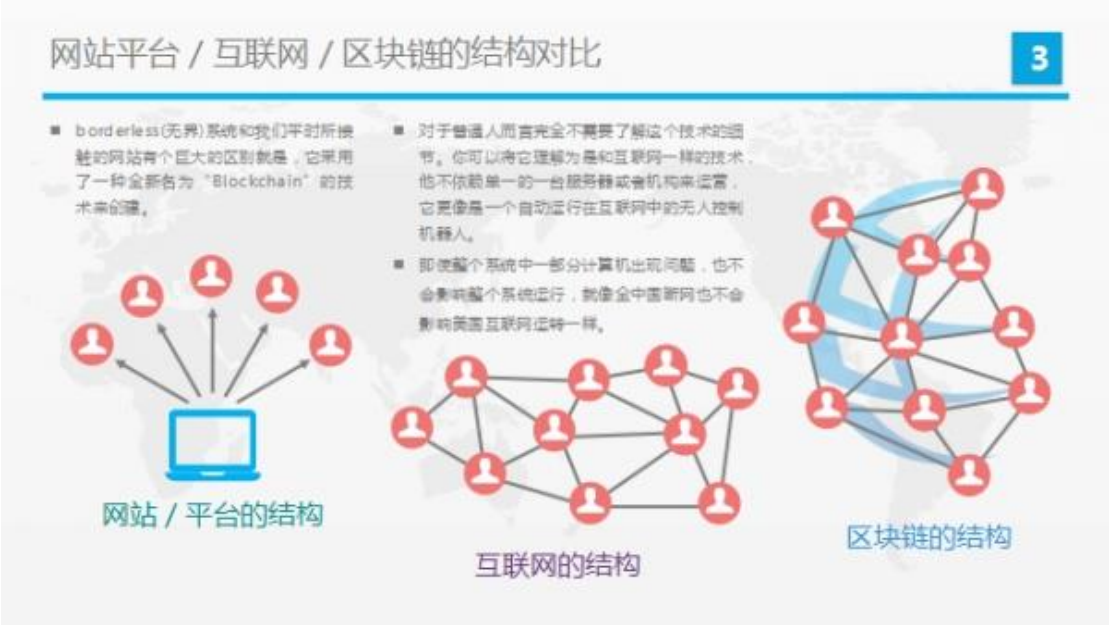
- 物联网

IBM 曾经提出一个叫做《设备民主》的白皮书，里面提出：到 2050 年，全世界至少有 1 千亿设备会被连入物联网。但是到现在为止，全球还没有合适的设备，能同时管理数亿个同时连入的终端。即使有这样一个中心化管理设备，本身的安全性也有极大的隐患。中心化的设备一旦瘫痪，整个物联网都会瞬间崩溃。因此 IBM 的结论是：区块链是目前我们想到的管理物联网的最好方案，依靠安全可靠的分布式系统来做底层的物联网管理。

- 去中心化的交易系统

由于区块链交易系统的透明性使得传统交易中可能存在的虚假交易是不可能的。

中心化的交易所已经一次又一次的让世界知道，它们是多么的不可靠和不值得信任。无论它们规模有多么庞大，有多少审计、监管机构或是保险公司，那些全球中心化的银行和交易所，还是每天都充斥着各种欺诈、滥用职权或者盗窃行为。而去中心化让 Borderless 面对失败时具有鲁棒性(Robustness)。当一个中心化的交易所被泄露数百万美元将会瞬间影响数千个用户，而一个去中心化的系统被攻击、或者出现故障只会影响单个用户和他的资金。用户能够控制他们自己的安全性，这其实可能远比任何中心化实体要好得多。

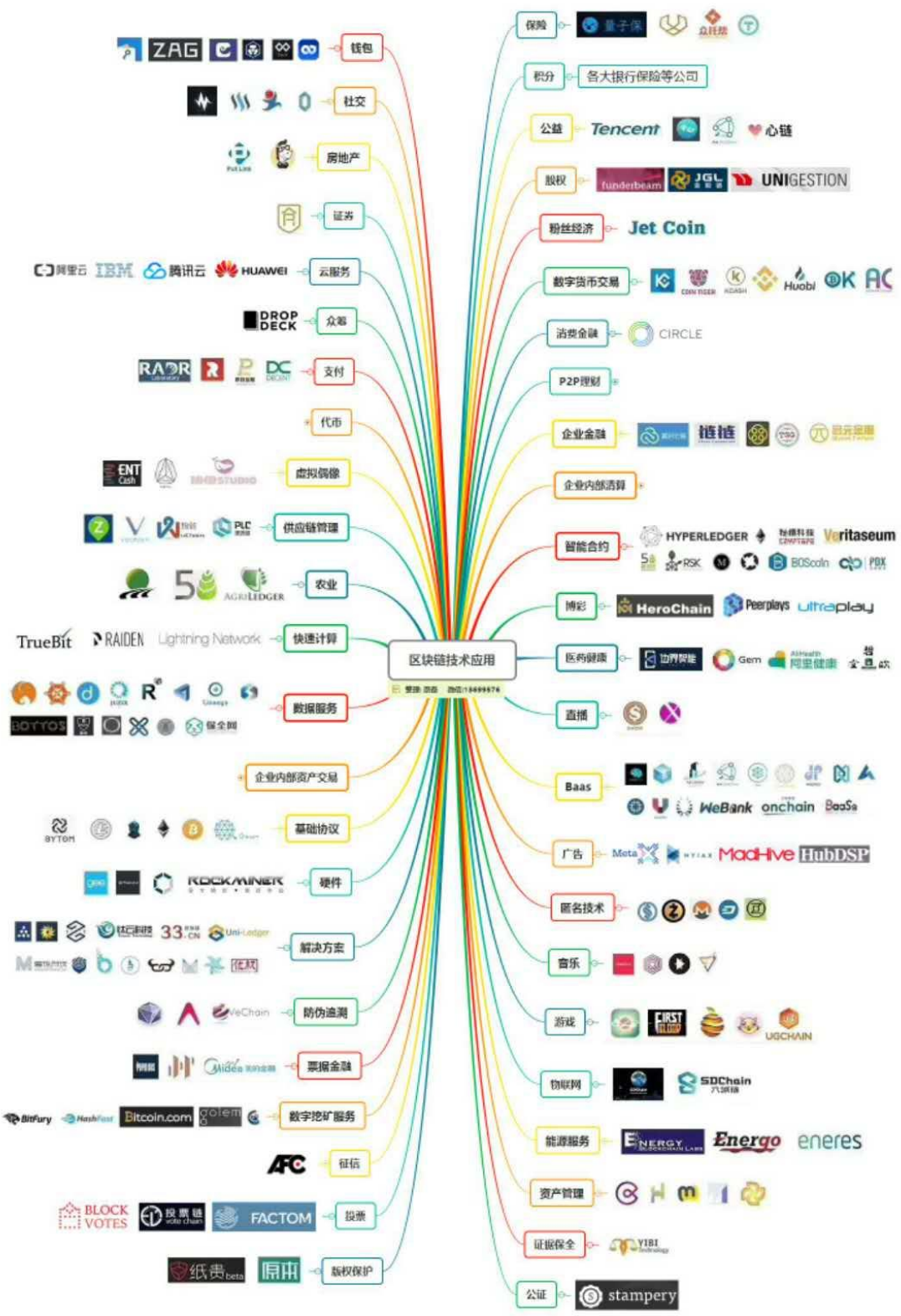


- 去中心化存储

传统的网络下，访问网络或服务器文件都离不开 HTTP 协议。当你输入网址，点击网页连接，就会向中心服务器地址寻找文件。如果有很多人同时访问，就容易造成网络堵塞，速度很慢。现在有一种基于区块链的分布式存储式技术叫做 ： IPFS (星际文件系统: Inter Planetary File System)，这个概念非常棒，未来有可能会取代传统的 HTTP 协议。IPFS 将文件碎片化存储在距离用户最近的计算机或服务器中，这样加载速度就会大幅提升。如果你所在的城市或者邻居有节点，那速度就更快了，甚至可以等同于访问本地文件。

- 医疗领域

生物资料如身高，血糖，血压等数据流失也许不会造成损失，但另一些生物资料的泄露在未来是绝对危险的，如虹膜和指纹。这带来的可能不是医疗上的灾难，而是整个金融系统的灾难。区块链很可能是目前唯一的解决方案。因为区块链不仅仅能够杜绝篡改，还能够提供多权限的复杂管理。



区块链的账户模型

https://zhuanlan.zhihu.com/p/438552382

账户模型

1. 基于账户的模型

如银行账户，在数据库中维护一条数据，余额的增加减少均基于该数据进行。

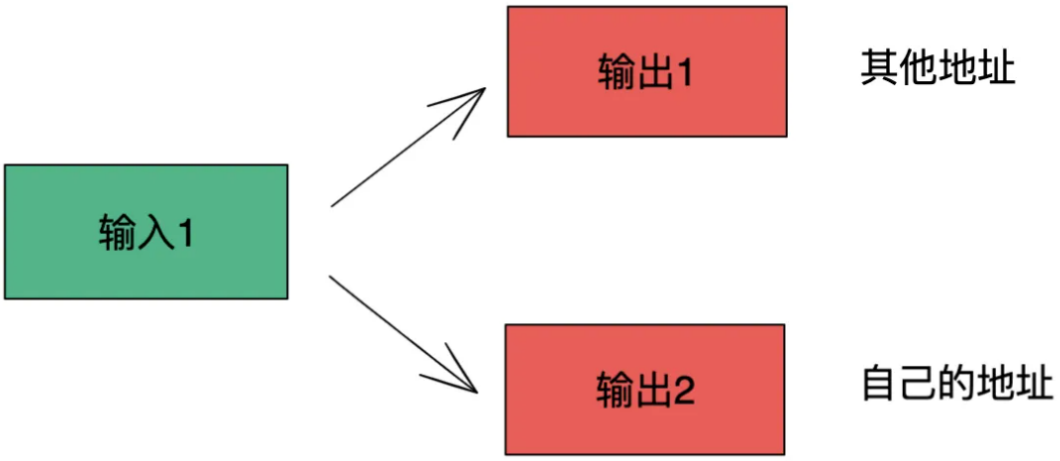
2. 基于交易的模型

比特币的 UTXO 模型是基于交易的，所有记录记录在交易中，获取账户余额需要通过所有交易推算。

比特币的交易类型

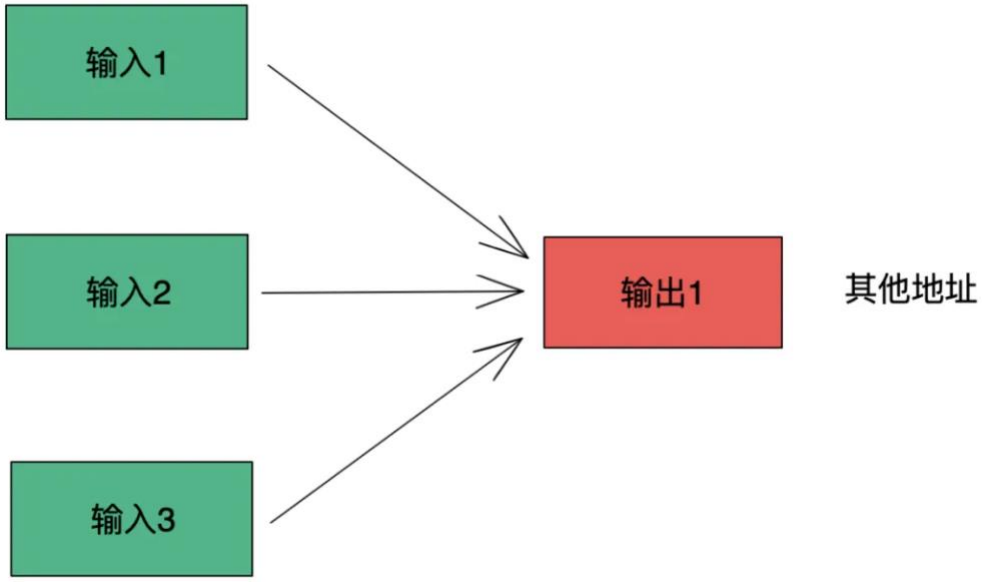
1. 一分二（支付）

由单个 UTXO 分为两部分，一部分负责支付，一部分负责找零。



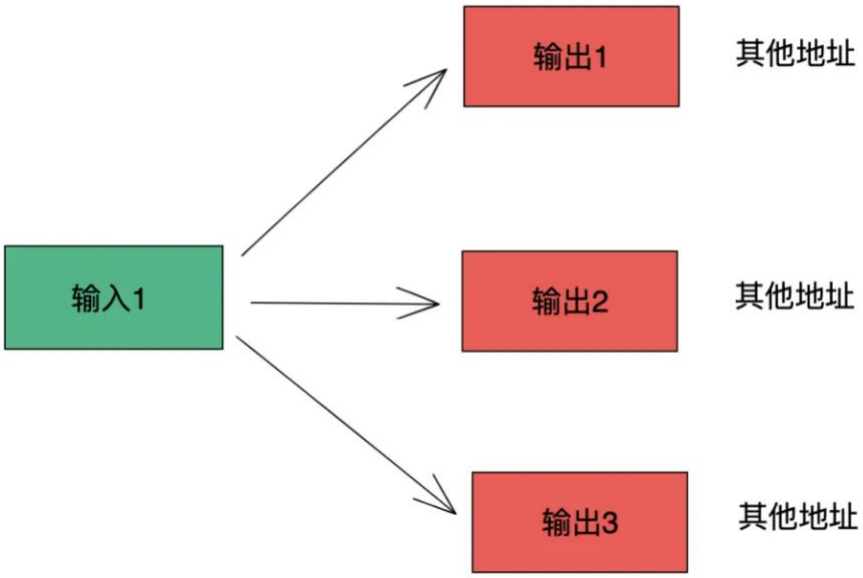
2. 多合一

支付一笔比特币时将多个 UTXO 凑在一起，形成新的 UTXO，相当于零钱换大额钞票。



3. 一换多

需要给多人发送比特币时，将一个大 UTXO 换成多个小 UTXO，相当于大额钞票换小额钞票。



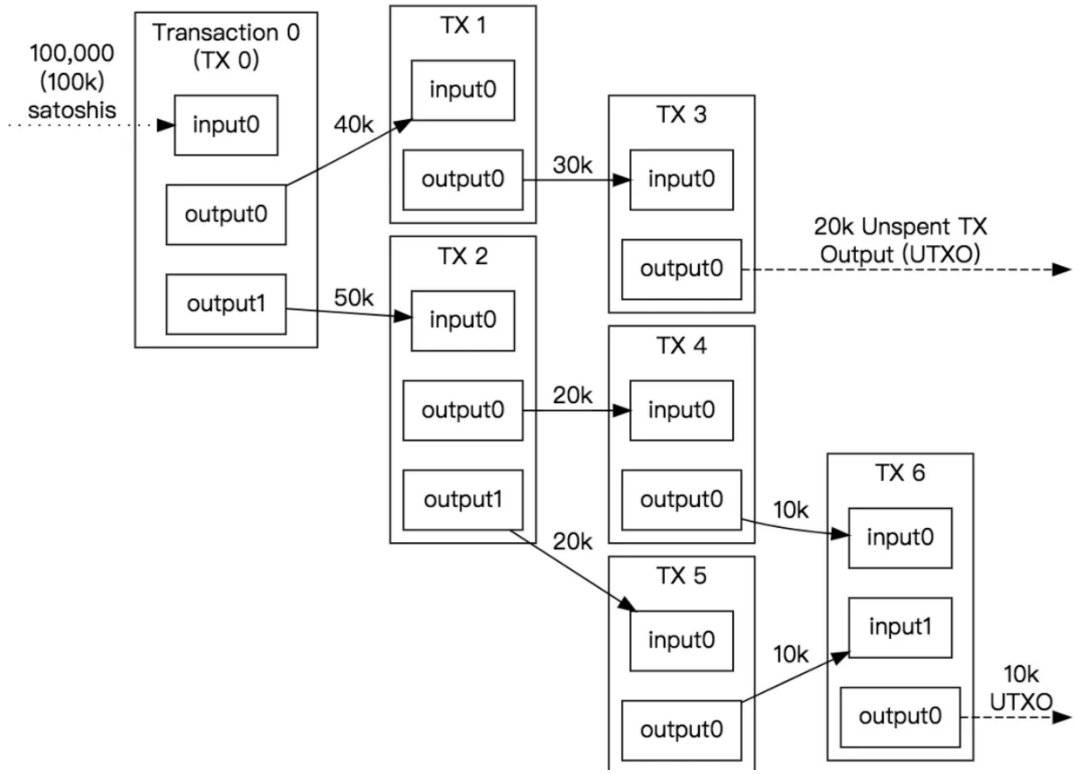
UTXO 模型

UTXO 由全节点遍历比特币账本后提取，之后在内存中维护。

链上查询 UTXO 耗时很长，全节点会扫描整链，生成地址和 UTXO 的映射关系以便交易时快速查询：

地址	UTXO
1JctmVUHHfchRQHR....	utxo1
1JctmVUHHfchRQHR....	utxo2
1JctmVUHHfchRQHR....	utxo3

在交易时，全节点会在集合中寻找符合条件的 UTXO，后用所有者的私钥签名来发起交易。每一笔交易都会花掉一些 UTXO，同时也会生成一些新的 UTXO。假如现在你有一笔 2 BTC 的 UTXO，但这时候需要支付给一个人 0.5 BTC，那么这个交易就会把这个 UTXO 拆成 0.5 和 1.5 BTC （由于有手续费，实际会略小于 1.5 ）的两个 UTXO，0.5 BTC 的 UTXO 会发送到别人的地址下，1.5 BTC 的 UTXO 会返回到你的地址下，这个方式也被称之为找零。被拆成两部分的 UTXO 也会被重新加入到 UTXO 的集合，供后面的交易使用，然后就会形成下面的交易链：



UTXO 中的每一个输出要给出产生该输出的交易 hash，以及在这个交易中是第几个输出。流通的比特币，都来源于最开始比特币区块的产出，即铸币交易。

交易所的比特币

还有一点需要注意，有很多中心化的交易所会提供比特币的交易，但交易所里面的比特币不是基于 UTXO。

当你在交易所充币的时候，交易所会为你设立一个账户，然后后续所有的交易都是基于这个账户进行的，并不会和链进行交互。

这样做有两个好处，第一个交易的速度更快，比特币网络上一笔交易的确认需要等不少时间，当交易很多时，速度会更慢。第二，省下了不少手续费。由于不与链交互，自然就不用交易的手续费。当然，交易所本身还是会从你的每一笔交易中收费。

也就是说，在交易所里的交易，并不是真正在链上进行交易。只有在把币从交易所提走的时候，才会把币打回到链上的地址。

区块链 layer1&layer2 解读

https://zhuanlan.zhihu.com/p/410557922

Layer1 和 Layer2 的概念并不单单指的是以太坊网络，而业内借鉴计算机网络通信体系架构的 OSI 模型（Open System Interconnection Reference Model，即开放式系统互联通信参考模型），将区块链逻辑架构划分为三层——Layer0、Layer1 和 Layer2。

第 0 层对应 OSI 模型的底层协议，大致包括物理层、数据链路层、网络层和传输层。第一层（Layer 1）大致包括数据层、共识层和激励层。而第 2 层（Layer 2）则主要包括合约层和应用层。

按照这个维度来划分，像我们所熟悉的比特币网络、以太坊主网等主流公链都属于 Layer 1 的范畴。只不过，由于在当前众多的公链项目中，以太坊是运行智能合约、DAPP 最多的公链，也是锁仓资产价值和日均交易量最大的公链，所以在有关以太坊网络 Layer1 和 Layer2 不同扩容方案的讨论也是最多的，所以在本文中，如没有特殊说明，所提到的 Layer1 和 Layer2 一般以以太坊为主。通俗来说，在以太坊网络中，Layer 1 的主要作用就是确保网络安全、去中心化及最终状态确认，做到状态共识，并作为一条公链网络中可信的“加密法院”，通过智能合约设计的规则进行仲裁，以经济激励的形式将信任传递到 Layer2 上；而 Layer2 则以追求更高效的性能为终极目标，从上面区块链技术逻辑架构示意图中，我们可以看到，作为第二层网络，可以替 Layer1 承担大部分计算工作，近年来，不少项目都是基于 Layer2 搭建的，从而将交易行为从主链上分离出来，降低一层网络的负担，提高业务处理效率，从而实现扩容。在这个过程中，Layer2 虽然只做到了局部共识，但是基本可以满足各类场景的需求。

目前行业内比较贴切的是将 Layer1 和 Layer2 的关系和中央银行与商业银行的关系来类比：把 Layer1 承担着中央银行的角色，而 layer2 则是各大商业银行。在现行主流的金融系统中，所有的资产都必须在中央银行结算，而具体的流通过程可以同时发生在中央银行和商业银行。因为如果所有人都去央行结算的话，势必会发生业务拥堵的情况，更好的解决办法当然是由商业银行来先处理大量交易业务，然后由各个商业银行和中央银行结算一次整体业务，这样才能使得整个金融系统更加高效有序的运转起来。所以从中我们能够得到的启示就是，对于在以太坊网络中存在的交易拥堵、手续费居高不下的问题，一个可行的解决方案就出炉了——将以太坊的资产存入 Layer2，之后的资产流动交易环节都在 Layer2 上进行，只把最终结算过程放到 Layer1 上就可以了。

闪电网络-LN

https://academy.binance.com/zh/articles/what-is-lightning-network

闪电网络简介

1. 闪电网络是什么?

闪电网络运行在区块链之上，旨在加速点对点交易。闪电网络即所谓的链下离线支付网络。闪电网络是在比特币网络上运行的第二层协议。闪电网络的主要目的是支持在较短的时间内确认更多交易，从而给用户带来更快的交易。交易在链下收集，以此形成有效地缓冲区，以供比特币网络进行最终处理。或 Layer 2 解决方案。

闪电网络独立于比特币网络，拥有自主节点和软件，但仍需与主链通信。如要进出闪电网络，需在区块链中创建特殊交易。

2. 闪电网络的细节?

个人的首笔交易实际上是在与其他用户建立一种智能合约。智能合约可以设想为与其他用户共持的私人账本。用户可在这本账本中写入多笔交易。这些记录仅对用户与交易对手可见，且基于设置的特性，双方无法作假。

这种迷你账本称之为“通道”。例如，Alice 和 Bob 分别向智能合约投入 5 BTC。他们的通道中此刻各自有 5 BTC 的余额。然后，Alice 写入账本“向 Bob 支付 1 BTC”。现在，Bob 有 6 BTC，Alice 余 4 BTC。Bob 日后又将 2 BTC 发还给 Alice。余额更新后，Alice 有 6 BTC，而 Bob 剩 4 BTC。他们可以这样持续操作一阵。

任意一方随时可将通道当前的状况发布到区块链中。届时，通道两端的余额分配到双方各自的链上地址。

顾名思义，闪电交易快如闪电。无需等待区块确认，即可在互联网连接允许时快速支付。

3. 闪电网络的必要性

比特币区块链需要一定的更新和优化，但在如此庞大的生态系统中协调变化十分棘手，因为要面临硬分叉和潜在灾难性漏洞等风险。保护巨额价值安全是当务之急，而在链上的实验极为危险。

若将试验区块移出区块链进行，便不会对比特币区块链造成实际影响。Layer2 提供了解决方案。这样，终端用户超常链上交易，同时增加了链下交易的选择。

闪电网络的优点

1. 可扩展性

闪电网络只需要开启和关闭闪电网络的费用，且开启后可免费进行数千场交易。从宏观角度来看，如果有更多人选择闪电网络等链下解决方案，区块空间的使用效率将得到提高。小额、高频次的转账通过支付通道进行，而区块空间则用于大额交易和通道开启/关闭。如此一来，访问系统的用户群体数量增加，可扩展性进而获得长久发展。

2. 小额支付

比特币设有最低交易金额，约为 0.00000546 BTC。但闪电网络将交易限额压得更低，按目前最小的单位来算，为 0.00000001 BTC，或一聪。

3. 隐私

闪电网络提供更高的保密程度。各方无需在网络上扩散自己的通道信息。区块链中可能会显示“该交易开启了通道”，但不会透露交易详情。如果参与者选择将通道设为私密状态，则交易进展仅本人可见。

且通道之间允许串联，假设 Alice 和 Bob 共享通道，Bob 又与 Carol 共享另一个通道，则 Alice 和 Carol 可通过 Bob 相互发送付款。如果 Dan 与 Carol 建立连接，Alice 同样可向他发送付款。试想将这种模式扩展到支付通道相互连接的庞大网络中。按照这样的设置，只要通道关闭，就无法确定 Alice 究竟向谁发送了资金。

闪电网络的底层原理

1. 多重签名地址

多重签名（或英文简称“multisig”）是可供多个私钥支付的地址。用户创建多重签名后，就能指定用于支付资金、签署交易所需的私钥数量。例如，5 取 1 方案指五个密钥生成一个有效签名，且签署交易仅需一个密钥。3 取 2 方案表示，如有三个密钥，需其中两个才能支付费用。

要预置闪电网络通道，参与者需在 2 取 2 方案中锁定资金，即仅需两个私钥用以签署交易，而转移代币同样需要两个私钥。这样，未经 Alice 同意，Bob 无法把资金转出地址，反之亦然。这样，彼此的合作更加高效，但存在结束时一方拒绝释放资金的可能，故尽可能在交易方互相信任的情况下开启。

2. 哈希时间锁合约（HTLC）

该机制可强制执行 Alice 与 Bob 之间的“合约”，如果其中一方不按规则行事，则另一方可采取补救措施，将资金撤出通道。HTLC 结合了哈希锁和时间锁两种技术，对支付通道中各种拒不配合的操作采取补救措施，也可用于创建条件支付。

- 哈希锁

哈希锁是加在交易中的条件，具体需证明自己知道某个秘密才能动用资金。发送方对一段数据进行哈希运算，并将带有哈希值的交易发送给接收方。接收方只有提供出与哈希值匹配的初始数据（即秘密），才能动用资金。唯一能获取该数据的途径是由发送方告知。

- 时间锁

时间锁是防止在特定时间前动用资金的限制条件，可指定具体时间，或特定区块高度。

交易细节

Alice 和 Bob 建立通道后，各自提供秘密 As 和 Bs,并分享秘密的哈希值 h(As)、h(Bs)。Alice 和 Bob 在向多重签名地址发布首笔交易之前，还需创建一系列承诺交易，即防止对方扣押资金的补救措施。

两者各设立承诺交易，一个支付自身拥有的地址，另一个锁进新的多重签名地址，签名后交给对方。

这些支出资金来自于尚未拨款的的 2 取 2 多重签名，故这些部分签名的交易只有在多重签名启动和运行后才能使用。

把交易发布到初始的 2 取 2 多重签名地址中去，就可以在交易对手放弃该通道时收回资金。交易确认后，通道将开启并运行。第一对交易显示的是迷你账本的当前状态。这时，账本向 Bob 支付 3 BTC，并同样向 Alice 支付 3 BTC。

Alice 要向 Bob 支付新款项时，两人会创建两笔新的交易来取代第一组交易。操作方式如出一辙，这笔交易会由各自签署一半。只是 Alice 和 Bob 要先放弃他们的旧秘密，并为下一轮交易交换新的哈希值。

双方均可随时签署和发布最近的一笔交易并在区块链完成“结算”。然而，签署发布方需等待时间锁到期，而另一方可马上花销费用。请记住，如果 Bob 签署和发布了 Alice 的交易，她就能拥有一次无条件输出。

双方可达成共识同时关闭通道，即合作关闭。这是资金返回链上最便捷的途径。但是，

如有一方没有回应或拒绝合作，另一方可在时间锁到期后收回资金。

安全

假设 Bob 现有余额为 1 BTC，要怎样才能阻止他发布余额更高的旧交易？毕竟他已经从 Alice 那里拿到了半签名的交易，他只需加上自己的签名就可以发布了，对吧？

没有任何措施能阻止他这样操作。但如果真要这么做，他可能会损失全部余额。假设他确实发布了旧交易，交易内容是向 Alice 支付 1 枚代币，并向我们此前提到的多重签名地址支付 5 枚代币。

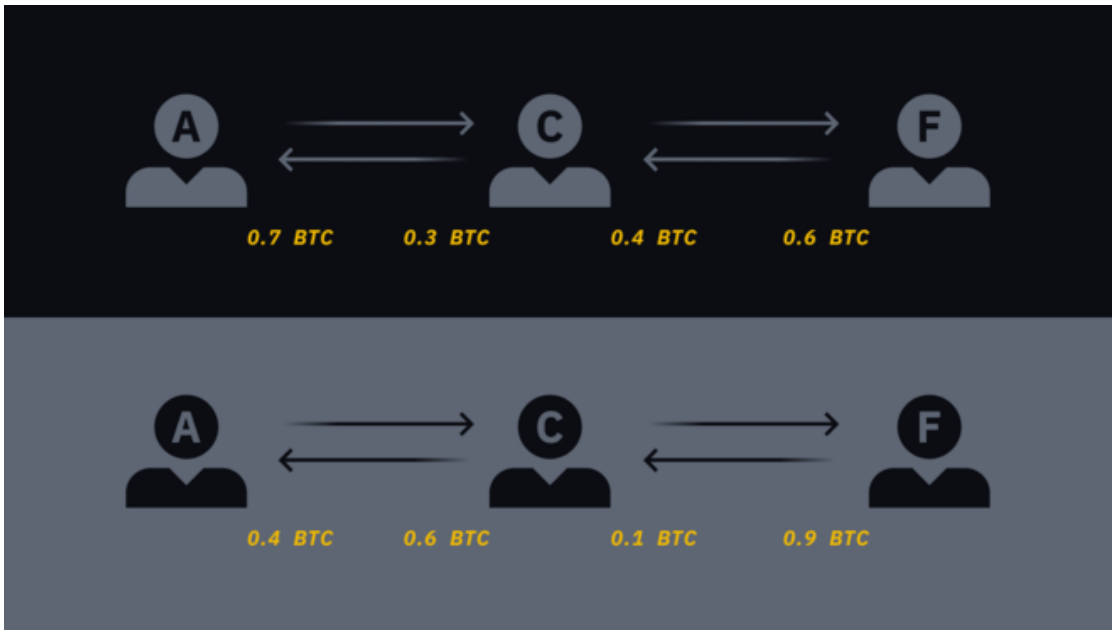
Alice 马上就会收到代币，但 Bob 必须等到时间锁到期才能从多重签名地址进行花销。是否记得我们上面提过，还要具备另一个条件，Alice 才能立即动用同一笔资金？她需要一个自己当时不掌握的秘密。但是现在她已经知道这个秘密了——第二轮交易刚刚创建，Bob 泄露了这个秘密。

在 Bob 只能静待时间锁到期时，Alice 就能挪走所有资金。这种带有惩罚性质的机制确保参与者不会打歪主意试图作假，否则交易对手将获得他们的代币。

通道支付

通道之间可以建立连接，否则闪电网络无法有效支持支付功能。同时闪电网络支持跨越多个“跳点”的支付方式，可能只需要少量费用。

每个节点包含本地余额和远程余额。本地余额是指一方可“推送”到通道另一端的金额，而远程余额则是指交易对手可推送回本地一方的金额。但由于跨点支付会导致中间结点的货币余额减少，可能不足以支付，进而影响闪电网络的流动性。如下图，当 A 对 F 支付 0.3BTC 时，导致的中间节点最大可支付数从 0.3BTC 减少到 0.1BTC，中间节点流动性变差。



结论

闪电网络限制了部分的交易能力，即支出不能超过锁定在通道中的金额，但提升了交易速度。进而存在一些“枢纽”节点，一种强流动性，关联密切的枢纽节点担起通道支付中间节点的责任，和去中心化思想相反。

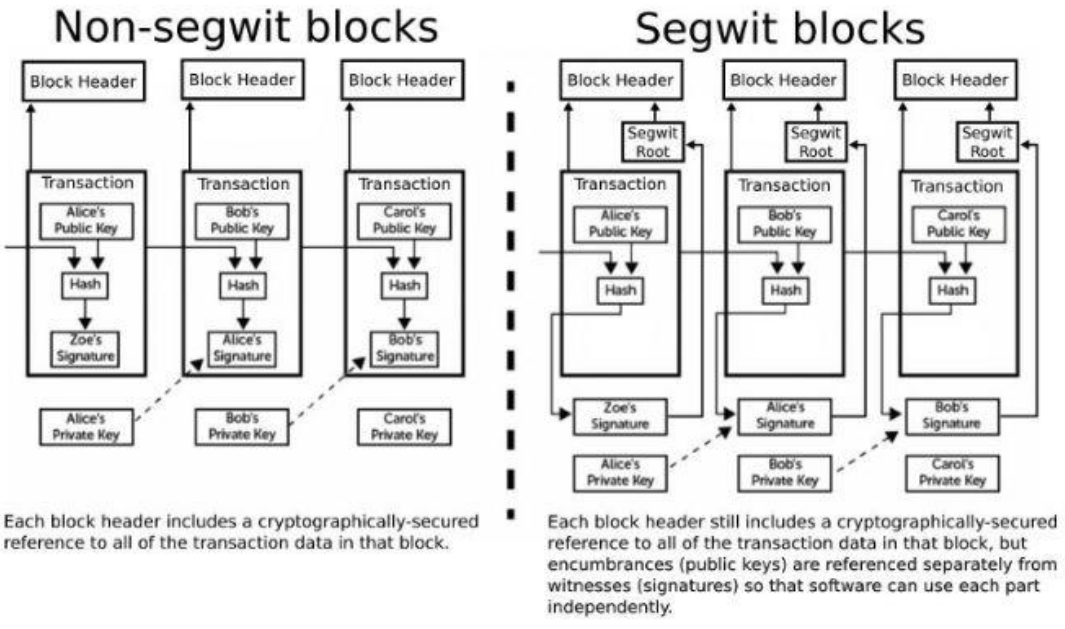
隔离见证（SegWit）

https://academy.binance.com/zh/articles/a-beginners-guide-to-segretated-witness-segwit
https://zhuanlan.zhihu.com/p/32613487

什么是隔离见证

比特币的扩容一直是个问题，闪电网络 Lightning Network 是一个方向。闪电网络的启动必须基于更多的用户使用隔离见证地址。隔离见证 (SegWit) 是 2015 年开发的升级协议。引入该概念是为了解决区块链网络当下面临的可扩展性问题。目前通过软分叉升级为 SegWit 协议的比特币地址约占 53%。

隔离见证的主要思想是重新组织区块数据，使签名不再与交易数据存储在一起。换句话说，SegWit 升级包括将验证人（签名）与交易数据隔离。这能够将更多交易存储在单个区块中，从而增加网络的交易吞吐量。



An illustration of the old and new transaction serialization posted by David A. Harding.

隔离见证的优势

比特币网络约十分钟生成一个块，区块大小直接影响可确认的交易数量。目前而言，处理速度约为 7 笔/秒。

隔离见证并不仅仅是区块大小的增加，它更是一种工程解决方案，可以在不增加区块大小限制的情况下增加有效区块的大小（这将需要硬分叉）。更具体地说，实际区块大小仍为 1 MB，但有效块大小的限制为 4 MB。

1. 容量增加

隔离见证的最大优势之一就是增加区块容量。通过从交易输入中删除签名数据，可以在一个区块中存储更多交易。

交易包括两个主要部分：输入和输出。本质上，输入包含发送者的公共地址，而输出包含接收者的公共地址。但是，发送人必须证明他们已经转移了资金，并且必须使用数字签名。

如果没有隔离见证，则签名数据最多可占用一个区块的 65%。使用隔离见证，会把签名数据从交易的输入中移除。这使有效区块大小从 1 MB 增加到大约 4 MB。

2. 速度提升

同样区块可容纳交易数量增多，则每秒处理的交易数（TPS）变大。

智能合约

https://zhuanlan.zhihu.com/p/413502024

智能合约是什么

智能合约是电子版合同、数字化合约、智能化合约，是将合同合约用代码写成一段程序，这段代码一旦写好就公之于众，且无法修改无法篡改，当外界条件发生变化如违约或合同到期，智能合约会自动触发，无需认为操作。

智能合约有效的解决了陌生人之间的信任问题，允许无第三方担保的情况下达成交易。

基于区块链的智能合约构建及执行分为如下几步：1、多方用户共同参与制定一份智能合约；2、合约通过 P2P 网络扩散并存入区块链；3、区块链构建的智能合约自动执行。

智能合约的优势

1. **无中介**

   完全依托技术让用户之间自主建立合约。

2. **透明公正**

   智能合约会用代码将条件写得清清楚楚并记录在区块链上，整个过程由程序执行，连包括编写这个代码的开发者都不能篡改。

3. **灵活**

   用户之间可以自由建立智能合约，没有对象的限制。

非同质化代币-NFT

非同质化代币（英语：Non-Fungible Token，简称：NFT），是一种众筹扶持项目方的方式，也是一种被称为区块链数位账本上的数据单位，每个代币可以代表一个独特的数码资料，作为虚拟商品所有权的电子认证或凭证。由于其不能互换的特性，非同质化代币可以代表数位资产，如画作、艺术品、声音、影片、游戏中的项目或其他形式的创意作品。虽然作品本身是可以无限复制的，但这些代表它们的代币在其底层区块链上能被完整追踪，故能为买家提供所有权证明。诸如以太币、比特币等加密货币都有自己的代币标准以定义对 NFT 的使用。

DApp：去中心化应用

https://zhuanlan.zhihu.com/p/36431908
https://www.weiyangx.com/295213.html

DApp 是什么

DAPP 就是基于 P2P 对等网络而运行在智能合约之上的分布式应用程序，区块链则为其提供可信的数据记录。

DApp 就是 D+App，D 是英文单词 decentralization 的首字母，单词翻译中文是去中心化，即 DApp 为去中心化应用。DAPP 就是在底层区块链平台衍生的各种分布式应用，是区块链世界中的服务提供形式。DAPP 之于区块链，有些类似 APP 之于 IOS 和 Android。不同的 DAPP 会采用不同的底层区块链开发平台和共识机制，或者自行发布代币（也可以使用基于相同区块链平台的通用代币）。

DApp 是对 App 的丰富完善。因为 DApp 直接和区块链技术挂钩，和交易数据、交易资

产有关联，和不可篡改去中心化存储有关联。对于 DApp，需要满足三个条件：1、运行在分布式网络上；2、参与者信息被安全存储，隐私得到很好的保护；3、通过网络节点去中心化操作。

DApp 的特点

1. **DApp 通过网络节点去中心化操作。**

   可以运行在用户的个人设备之上，比如：手机、个人电脑。永远属于用户，也可以自由转移给任何人。

2. **DApp 运行在对等网络。**

   不依赖中心服务器，不需要专门的通信服务器传递消息，也不需要中心数据库来记数据。数据保存在用户个人空间，可能是手机，也可能是个人云盘。

3. **DApp 数据加密后存储在区块链上。**

   可以依托于区块链进行产权交易、销售，承载没有中介的交易方式。

4. **DApp 参与者信息被安全储存。**

   可以保护数字资产，保证产权不会泄露、被破坏。

5. **DApp 必须开源、自治。**

   可以由用户自由打包生成，签名标记所属权。它的发布不受任何机构限制。 各种创意与创新可以自由表达和实现。

DApp 与 App

DApp 就是智能合约+App。站在开发角度来看，DApp 是前端界面+智能合约，前端就

是和用户交互的，可以选择各种命令，智能合约自然就是和区块链(分布式数据库)交互。

APP 相对于 DAPP 有四大问题，一是截留用户数据，二是垄断生态平台，三是保留用户权利，四是限制产品标准扼杀创新。

DAPP 与 APP 区别主要有两个方面，一是 APP 在安卓或苹果系统上安装并运行，DAPP 在区块链公链上开发并结合智能合约；二是 APP 信息存储在数据服务平台，可以运营方直接修改，DAPP 数据加密后存储在区块链，难以篡改。

对比 APP，两者最大不同就是中心化与去中心化。App 先要有钱，所以先融资;然后再有人，所以招齐人后再开发运营。而 DApp 则是继承传统 App 并结合区块链的特点所形成的产物，它更像是众筹模式、共享模式和去中心化模式，DApp 先有发起人或组织，写好白皮书明确了共识机制和 token 分配与激励，持有 token 的人即为股东，直接和 DApp 的盈利关联(也可以说用户即是股东)，持有的 token 像股票可以买卖，在支持的交易所交易，所以持有该 DApp 的 token 相当于拥有所有者权益。可以想象，未来各个领域都会有 DApp，每个人都将因 token 分类、以 token 群分。

DApp 的分类

1. 根据去中心化的对象

一般而言，去中心化包括以下几类，一是基于计算能力的去中心化（如 POW 机制），二是基于存储能力的去中心化（如 IPFS），三是基于数据的去中心化（如 STEEMIT）；四是基于关系的去中心化（如去中心化 ID）。

2. 根据去中心化的方法

大致可以分为两类 DAPP，分别是中介自动化 DAPP 与中介竞争化 DAPP。其中中介自动化 DAPP 是通过中介自动化而去中心化，如通过区块链转移产权，把从国家掌控的集中程序转变成为需要任何中介，原先的中介成为自动化程序；而中介竞争化 DAPP 则是通过竞争去中心化，没有完全摆脱中介，而是让参与者选择他们信任的人，也就是说通过竞争去中心化。

3. 根据网络服务形式的不同

DAPP 可以分为四类，包括(1)媒体播放器，需要 CPU 原生代码虚拟机来去掉播放器中介；(2)Web 服务(网站)中介利用用户数据作恶，需要类似最新的 Lambda 服务器(无数据 Web 服务)来解决；(3)运营商中介作恶，需要去中心化 P2P 网络，的确这也不一定需要区块链；(4)基于共识的用户态智能合约，只有这个需要区块链。

DApp 前景

应用的方向在于和物联网、共享经济的结合，比如无人驾驶汽车应用。使用区块链技术的非中心化管理明显好于中心化管理。车辆将路况信息时刻写入区块链，避免了服务器故障或传输网络延迟导致的驾驶安全问题。

除了上面利用区块链技术做到汽车与汽车之间的信息通信，进一步，人工智能也可以充分利用区块链技术加智能合约，做到机器与机器之间的通信交流，需要基于区块链技术的成熟来实现。

1. **DApp 通俗定义定义**

   前端+智能合约+token（通证经济）

2. **开发流程**

   写白皮书->明确共识机制->token 激励机制->智能合约开发->去中心化社区自治。

去中心化身份 DID

https://zhuanlan.zhihu.com/p/77290826

DID 即去中心化身份 Decentralized ID

[具体写在 IoT 身份认证中]

物联网-IOT

https://www.zhihu.com/question/343675446/answer/2214617223

物联网是什么

物联网（Internet of Things，简称 IoT）是指通过各种信息传感器、射频识别技术、全球定位系统、红外感应器、激光扫描器等各种装置与技术，实时采集任何需要监控、 连接、互动的物体或过程，采集其声、光、热、电、力学、化学、生物、位置等各种需要的信息，通过各类可能的网络接入，实现物与物、物与人的泛在连接，实现对物品和过程的智能化感

知、识别和管理。物联网是一个基于互联网、传统电信网等的信息承载体，它让所有能够被独立寻址的普通物理对象形成互联互通的网络 。是互联网基础上的延伸与扩展。

物联网的特点

1. 全面感知

利用 RFID、传感器、维码等随时随地获取物体的信息，包括用户位置、周边环境、个体喜好、身体状况、情绪、环境温度、湿度，以及用户业务感受、网络状态等。

2. 可靠传递

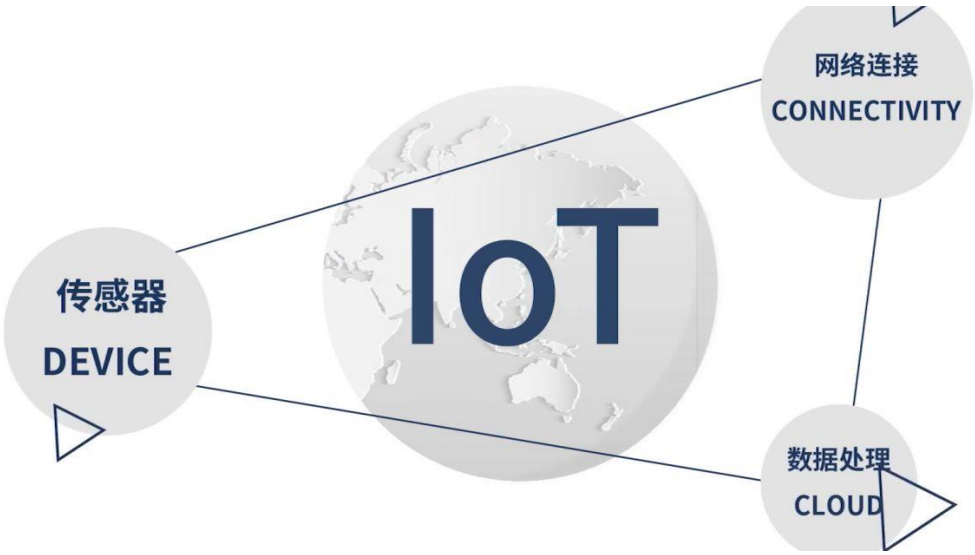
通过各种网络融合、业务融合、终端融合、运营管理融合，将物体的信息实时准确地传递出去。

3. 智能处理

利用云计算、模糊识别等各种智能计算技术，对海量数据和信息进行分析和处理，对物体进行实时智能化控制。

物联网的工作流程

物联网主要分为 3 个组成部分，传感器(device)使物能够接受信息，感知信息，网络连接(connectivity)低功率广域网络协议，数据处理(cloud)云计算。



1. 传感器

传感器被安装在各种产品中，它们就是万物互联的物，这些传感器或者是芯片，让产品拥有感知能力和数据处理能力，同样，传统的家电产品，也可以借助这些芯片智能化。

2. 网络连接

产品在收集完了数据之后，就要上传到云端进行云端进行集中处理，这个过程中就是通

过网络连接(connectivity)来完成，5G 虽强，但是并不适用所有情境下的传输要求，物联网还需要低功耗，长距离的传输协议。即低功率广域网络。

3. 数据处理

数据处理的目的在于，将原始的数据转换为有用的信息，数据处理一般都是在云服务器上完成，这些服务器就是智能音箱的大脑，数据在这里进行处理过后，再以直观易懂的形式返回给用户。

物联网的体系架构

1. 感知/延伸层

感知/延伸层是物联网的皮肤和五官一识别物体，采集信息。感知层包括二维码标签和识读器、RFID 标签和读写器、摄像头、 GPS、传感器等，主要作用是识别物体，采集信息。

2. 网络层

传输网络层是物联网的神经中枢和大脑一信息传递和处理。网络层包括通信与互联网的融合网络、网络管理中心和信息处理中心等。网络层将感知层获取的信息进行传递和处理。

3. 应用层

业务与应用层是物联网的“社会分工”一与行业需求结合，实现广泛智能化。应用层是物联网与行业专业技术的深度融合，与行业需求结合，实现行业智能化，这类似于人的社会分工，最终构成人类社会。

区块链预言机（BlockChain Oracle）

https://zhuanlan.zhihu.com/p/52369816

注：Chainlink 是一个在以太坊区块链上的去中心化数据预言机（英语：Blockchain oracle）网络，旨在将区块链智能合约与可信任、防篡改的现实世界数据来源实时连接起来。

预言机是什么

区块链外信息写入区块链内的机制，一般被称为预言机(oracle mechanism) 。预言机的功能就是将外界信息写入到区块链内，完成区块链与现实世界的数据互通。它允许确定的智能合约对不确定的外部世界作出反应，是智能合约与外部进行数据交互的唯一途径，也是区块链与现实世界进行数据交互的接口。

DAPP 类比的话就是 APP，那么预言机可以形象的比做 API 接口 （API 是一组定义、程序及协议的集合，通过 API 接口实现计算机软件之间的相互通信）。预言机是区块链和现实世界之间的纽带，可以实现数据互通的工具。

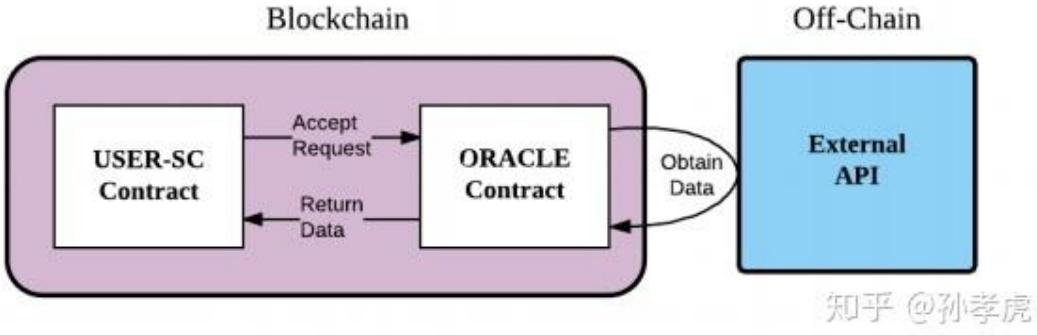
预言机的细节

由于智能合约无法主动去获取链外的数据，只能被动接受数据。而区块链是一个确定性的、封闭的系统环境，目前区块链只能获取到链内的数据，而不能获取到链外真实世界的数据，区块链与现实世界是割裂的。

一般智能合约的执行需要触发条件，当智能合约的触发条件是外部信息时（链外），就必须需要预言机来提供数据服务，通过预言机将现实世界的数据输入到区块链上，因为智能合约不支持对外请求。

区块链是确定性的环境，它不允许不确定的事情或因素，智能合约不管何时何地运行都必须是一致的结果，所以虚拟机（VM）不能让智能合约有 network call（网络调用），不然结果就是不确定的。

也就是说智能合约不能进行 I/O（Input/Output，即输入/输出），所以它是无法主动获取外部数据的，只能通过预言机将数据给到智能合约。



预言机的应用

一切需要与链下进行数据交互的 DApp 都需要预言机。金融衍生品交易平台、借贷平台、快递追踪/IoT、稳定币、博彩游戏、保险、预测市场等，目前最主要的场景就是 DeFi。

在 DeFi 中，需要获得 ETH 的实时价格，来判断所抵押的加密货币是否达到了平仓价格

进而触发平仓。但由于实际节点延迟，计算速度等，节点获得的价格不同，无法达成共识甚至导致系统崩溃。

目前有很多项目自己搭建的预言机在运行，但存在单点故障，易受攻击的缺点。

DeFi-去中心化金融

https://baike.baidu.com/item/DeFi/60830213?fr=aladdin
https://www.zhihu.com/question/324838085

DeFi 生态的开发者们常常把稳定币、借贷市场和去中心化交易所（DEX）看作 DeFi 的“三驾马车”。

DeFi 是什么

DeFi，即“去中心化金融（Decentralized Finance）”，也被称为“开放式金融”。是以比特币和以太币为代表的加密货币，区块链和智能合约结合的产物。有了去中心化金融，市场始终开放、自由。没有集中管理机构可以阻止付款或拒绝访问任何内容。 以前有可能出现人为错误的缓慢服务，替代为由任何人都可以检查和审查的代码来处理，变得自动和安全。这是一种加密经济模式，允许包括放贷、借款、做多/做空、赚取利息的金融行为。

DeFi 有两大支柱，一是以比特币和以太币为代表的稳定币，二是实现交易、借贷和投资的智能合约。

首先，DeFi 是加密金融体系的一种模式。按照是否涉及加密资产，可以将金融体系区分为传统金融体系（不涉及加密资产）和加密金融体系。其中，按照是否要依托中心化的金融机构或者交易场所，可以将加密金融体系划分为 DeFi（不依托）和 CeFi（中心化金融）。

其次，DeFi 的核心在于“去中心化”。DeFi 通过运用加密货币和智能合约在区块链上提供交易、借贷和投资等金融服务，但不依托于任何中心化的金融机构、中介或交易场所。换言之，DeFi 提供了与传统金融服务类似金融服务，同时实现了金融脱媒。

第三，DeFi 还具有相当高的匿名性。运用 DeFi 交易（借贷）的双方可以直接达成交易，所有合同和交易细节都记录在区块链上（on-chain），并且这些信息很难被第三方察觉或发现。

功能	服务	加密金融体系		传统金融体系
		去中心化金融（DeFi）	中心化金融（CeFi）	
交易	资金转移	去中心化稳定币（如 DAI）	中心化稳定币（如 USDT 和 USDC）	传统支付平台
	资产交易	去中心化加密货币交易所（如 Uniswap）	中心化加密货币交易所（如币安和 Coinbase）	交易所和场外经纪商
	衍生品交易	去中心化加密衍生品交易所（如 Synthetix 及 dYdX）		
借贷	担保贷款	去中心化加密借贷平台（如 Aave 和 Compound）	中心化加密借贷平台（如 BlockFi 和 Celsius）	活跃于回购和证券借贷的做市商
	无担保贷款	加密信用协议（如 Aave）	加密银行（如 Silvergate）	商业银行和其他非银行贷款
投资	投资工具	去中心化加密投资组合（如 Yearn 和 Convex）	加密基金（如 Grayscale 和 Galaxy）	投资基金

DeFi 的起源

在创造了基本的「token」之后，加密数字货币界希望能够把金融交易的一部分，也给去中心化，这就是 DeFi 的由来。把金融去中心化最大的难点，不在于技术，而在于用什么来取代「信用衍生」。

区块链的设计赋予了加密货币「资产」的特性，具有很强的抗审查、抗监管的能力。将同样的玩法移植到金融交易上，如借贷，由于不受中心化机构的监管，很容易发生违约。DeFi 要解决的就是这个问题，要在区块链上模拟出我们平常见到的金融交易，像最基本的借贷和各种高级的金融衍生品。

DeFi 利用去中心化实现信用衍生，基本过程如借贷、抵押和所有权转移则均由智能合约解决。目前是通过跨链来解决抵押，通过保证金制度来解决杠杆，最终实现了类似于信用衍生一样的操作。

跨链保证金实现了等额抵押，DeFi 也允许超额抵押，但为了避免坏账，智能合约可能会强制平仓。任何导致坏账的行为都会触发智能合约的平仓操作。这其实是将所有节点当作了恶意节点来对待。

有了杠杆、有了抵押、有了资金池。金融最基本的东西都具备了，理论上什么复杂的衍生品都能设计出来的。但是，现实里还是会存在各种问题：黑客完全可以人为的制造区块链的阻塞，让智能合约的执行延迟，而在延迟的过程中，价格可能就发生了变化了，进而导致坏账和亏空。

一个抗监管、抗审查、还依赖于计算机技术具体实现的去中心化的金融衍生品平台，称之为金融的丛林社会都可以，别说对于普通人，就是对于庄家，风险都是巨大的。

DeFi 与传统金融

传统金融的问题与两者的对比如下：

了解去中心化金融潜力的最佳方法是了解目前存在的问题。

- 有些人无法设立银行帐户或使用金融服务。
- 无法获得金融服务会阻碍人们就业。
- 金融机构可能会阻止您获得报酬。
- 金融服务的一个隐性收费就是个人数据。
- 政府和中央机构可以随意关闭市场。
- 交易时间通常限于特定时区的营业时间。
- 由于内部的人工流程，资金转移可能需要几天时间。
- 金融服务存在溢价，因为中介机构需要分成。

去中心化金融	传统金融
您持有您的钱。	资金由机构持有。
您可以控制自己的资金流向和使用方式。	您必须相信机构不会错误地管理资金，比如借给风险借款人。
资金转移在几分钟内完成。	如果人工处理，支付可能需要几天时间。
匿名交易。	金融活动与您的身份紧密相连。
去中心化金融对任何人开放。	您必须申请使用金融服务。
交易时间 24 小时不间断。	根据人工作息时间制定交易时间。
建立在透明基础上 - 任何人都可以查看产品数据并检查系统运行状况。	金融机构是闭门造车：您不能要求查看他们的贷款历史，管理资产的记录，等等。

去中心化交易所-DEX

https://zhuanlan.zhihu.com/p/115975299

去中心化交易所是 DeFi 生态中非常重要的一环，它在 DeFi 生态中的角色相当于中心化交易所（CEX）在整个加密货币市场的角色。但由于效率较低以及用户规模小，故并没有很活跃。DEX 具有完全去中心化、透明、开放的特性

交易所的核心环节就是充提、下单、订单撮合、资金结算、提现，中心化的交易所（CEX）上述所有的环节均由交易平台本身撮合完成。而 DEX 则是把上述所有环节都置于链上，由智能合约执行全部操作，这样用户的交易过程就无需任何可信任的第三方。

由智能合约驱动的 DEX 可以为用户省去负责的 KYC 审核，也可以帮助用户消除中心化交易所“拔网线”、暗中操纵价格、交易量造假和跑路带来的风险，所有的交易记录都在链上可查。

事实上，DEX 的发展完全取决于底层公链性能的发展

自动做市商-AMM

https://zhuanlan.zhihu.com/p/398668686

DeFi 领域去中心化交易所 DEX 能够崛起的一个核心原因是引入了什么是自动做市商（AMM）模式。AMM 又称自动化做市商，它是去中心化交易所（DEX）最为关键的技术之一，已被证明是最具影响力的 DeFi 创新之一，它们能够为一系列不同代币创建和运行可公开获取的链上流动性。

做市商-MM

“做市商”的英文原文是 Market Maker，换句话理解：在没有市场的地方，做市商 Make（做，创造）了一个市场出来。这里所谓的“没有市场的地方”，并非指市场不存在，而是是指交易市场的活跃度不够。市场本身是为了解决供需双方进行买卖交换的需求的，不过要想达成交易，必须要买方和卖方在同一时刻、对同一价格都有交易意愿。这件事说起来简单，不过不活跃的市场想要在同一时刻汇集起合适的买家和卖家并非易事。

做市商通俗来讲就是“倒爷”，其存在的意义，就是为了解决市场流动性不足带来的交易时间难以匹配的问题。

自动做市商

任何市场都可能存在没有足够的有机流动性以支持活跃的交易的状况，做市商本质上就是通过促进这些市场中不会发生的交易来缓解这一问题的代理商。AMM(Automated Market Maker)的出现，相当于把他们这个角色给真正的去中心化了。

自动化做市商（AMM），使用算法“机器人”在 DeFi 等电子市场中模拟这些价格行为。自动化做市商（AMM）不需要用户去挂单，而是直接根据算法计算出两个或者多个资产之间相互交易的汇率，实现不用挂单等待的“即时交易”。但是这样的“交易池”，需要做市商预先存放一定数量的资产作为底仓，才能够有更好的流动性，以及更小的交易滑点。虽然存在不同的去中心化交易所设计，但基于 AMM 的 DEX 始终实现了最大的流动性以及最高的日均交易量。

每个用户都可以把自己的代币扔到流动池里，成为一个小的做市商，然后享受交易对手续费分红。且流动池资金是去中心化开源合约控制，AMM 交易数据全部上链，不像传统 CEX 的平台币销毁或是分红，毕竟没有人知道他们手续费真的挣了多少，平台币流通了多少等等。而在 AMM 这里，一切透明。更重要的是，你的资产依旧在你个人控制的钱包里，而不是进了交易平台，所以资产依旧 100%安全，这是传统 CEX 无论如何不可能实现的。

AMM 从根本上改变了用户交易加密货币的方式，与传统的订单簿交易模式不同，AMM 的交易双方都是和链上流动性资产池在进行交互。流动性池允许用户以完全去中心化和非托管的方式在链上的代币之间无缝切换。而流动性提供者，则通过交易费用赚取被动收入，而

交易费用基于其对资产池贡献的百分比。

AMM 有着基于不同函数的多种类型。

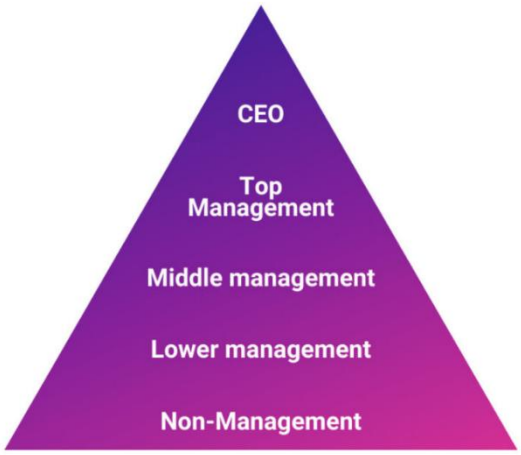
去中心化自治组织（DAO）

DAO 即“去中心化自治组织”，由智能合约中的计算机代码自动执行组织或企业的决策，或由代币持有者投票决定。它将以最为去中心化的方式实现目标，且没有任何集权或层次结构。

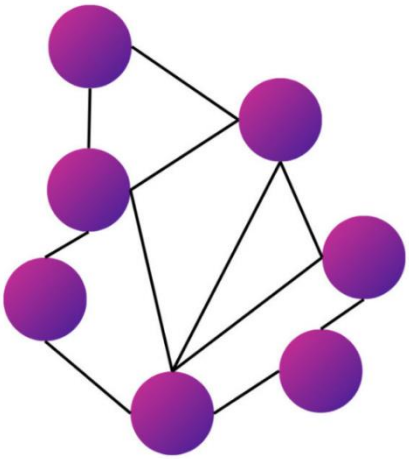
DAO 实通过区块链和智能合约来实现部分流程和决策自动化。它旨在减少人力投入，提高组织的自动化和协作能力。

DAO 相关的代币，可以代表对不同事项的投票权（类似于公司的股票），也可以用于不同的用例(组织花费、奖励用户等)。DAO 具备投票能力和与之相关的激励机制；它打破了传统组织的等级制度，确保在参与者之间能达成决策共识。部分 DAO 还针对某些事项向非代币持有者开放投票。当组织的规则被编码到智能合约中时，将带来无限的可能。

此外，一些 DAO 允许利益相关者就其未来发展提出建议。在这种情况下，提议者需要先抵押部分代币（也就是所谓的提议门槛），以防止无意义的建议泛滥。



A legal entity with employment contracts


No centralized entity;
No employment contracts

DAO 具备更高的自由性，因为参与者的国籍没有限制或者规则。这意味着世界各地的人可以决定投资哪些全球性组织，既公平也没有排他性。链上交易的强大功能还简化了在 DAO 中出售股票的过程，而无需像现在这样的技术和复杂的财务问题。

16 年，由于黑客发现 DAO 函数库的漏洞，盗走了 7000 万美元，因此以太坊分为了 ETH 和 ETC 两种。

DAO 最初的设想是实现比特币基于中央货币和中央机构。其目标在于成为无集权且不会失败的“不可阻挡的组织”。它们独立运行，不受权益持有者投票的影响。DAO 是一种开放的、无国界的、不受政府审查的组织，即一种更加“民主”的组织。但 DAO 仍需要被证明是一种可靠且有利可图的发展组织方式。

DAO 的成功与否与大众对区块链技术的理解以及在如何看待社会和经济方面的观念转变有关。金融革命始于比特币和加密货币，但是当 DAO 成熟到足以取代传统组织时，将是一场重大变革。传统经济将永远转变为更去中心化的经济，人人参与其中，对自己想要的产

品或服务拥有发言权。这将使我们自由地追求不同的目标，并有希望建立一个更好和更公正的社会。

区块链+物联网

https://www.zhihu.com/question/53414917/answer/807066906

融合背景

物联网面临着安全挑战。

随着物联网的发展，大量部署在传统数据中心、云内的基础设施（存储、计算、网络）将不可避免的被推出机房，重新部署在边缘和终端设备上。

这样发展的结果就是大量边缘设备缺少机房的物理屏障，并且部署在防火墙外，将面临严重的安全挑战：

1、单个边缘设备易于被黑客通过物理手段攻克；

2、边缘或终端设备可自组织地加入某一物联网系统；

3、系统缺乏对设备的控制权，进而缺乏对恶意设备的识别及防范能力。

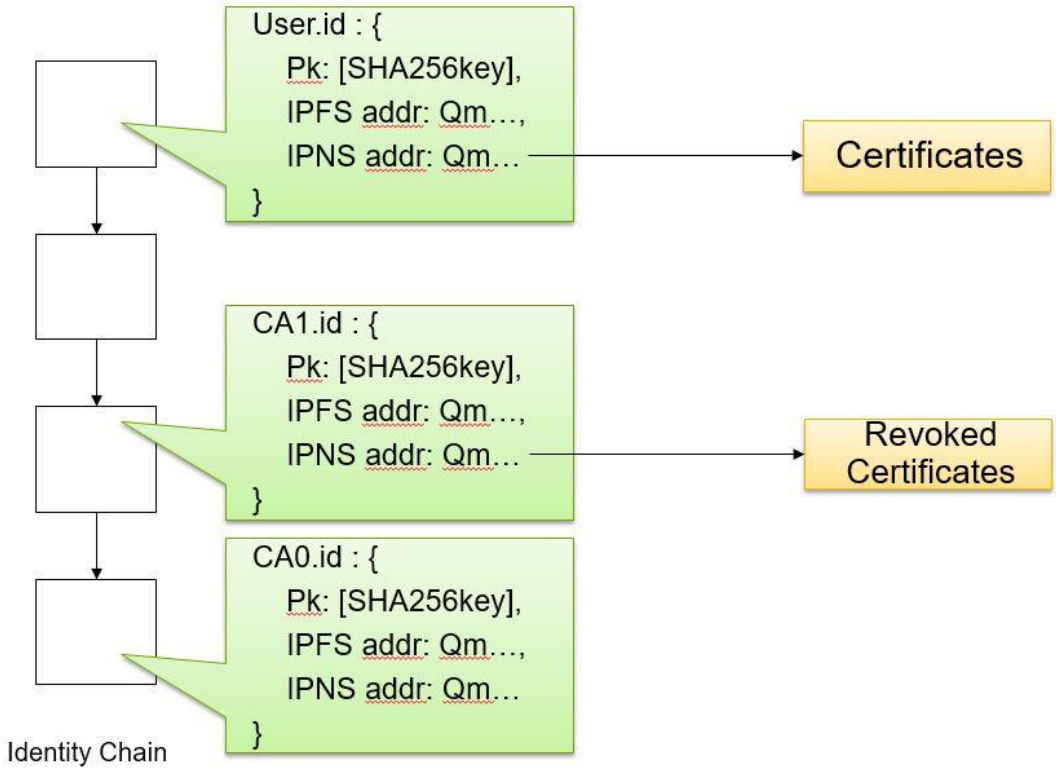
同时，传统的中心化管理方式难以在物联网时代有效工作：物联网时代的边缘与终端设备数量巨大，单一中心服务器或集群难以有效管理如此大规模设备，中心化系统面临严重性能瓶颈。所以这个时候，区块链最显著的数据永久保存和防篡改就排上了用场。幸运的是，做为大规模分布式去中心化系统，区块链通过哈希链及共识算法，提供了数据永久保存及防篡改特性，可以有效地辅助物联网解决各类安全问题。此外，通过有效利用区块链的去中心化特性，亦可以构建去中心化文件系统、去中心化计算系统等，为物联网的发展提供有效支撑。

相关技术

1. 去中心化身份

不同组织机构签发的身份需要在物联网中互联互通。身份信息不应该由单一的中心化机构控制。区块链可以很好的解决上述问题，实现去中心化的身份管理，把身份的所有权还给设备或用户本身。

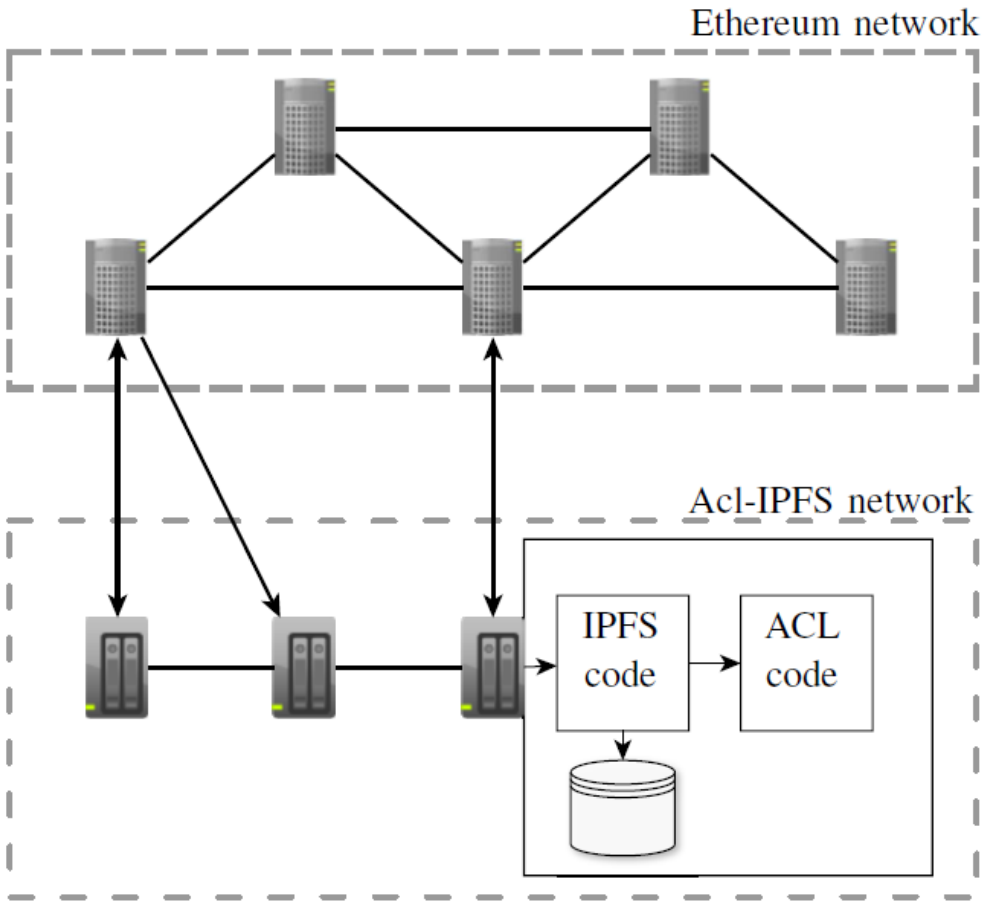
一种思路是将 IPFS 与区块链结合，达成一种去中心化的身份管理解决方案。



一种去中心化身份实现方案。使用区块链技术将人类可读的 ID 与公钥绑定，并去中心化地存储在区块链上，永久保存。每个 ID 对应的证书信息可以保存在 IPFS 上。

2. 去中心化访问控制

使用区块链代替传统中心服务器，物联网数据则保存在去中心化的文件系统，如 IPFS 上。IPFS 通过 ACL 代码链接区块链网络，由链上智能合约进一步实现去中心化访问控制。



3. 增加 IoT 的数据置信度

IoT 设备产生的原始数据可以记录在分布式防篡改文件系统（如 IPFS）之上，而对应的元数据则可以记录在区块链之上，实现数据可溯源、防篡改。

应用场景

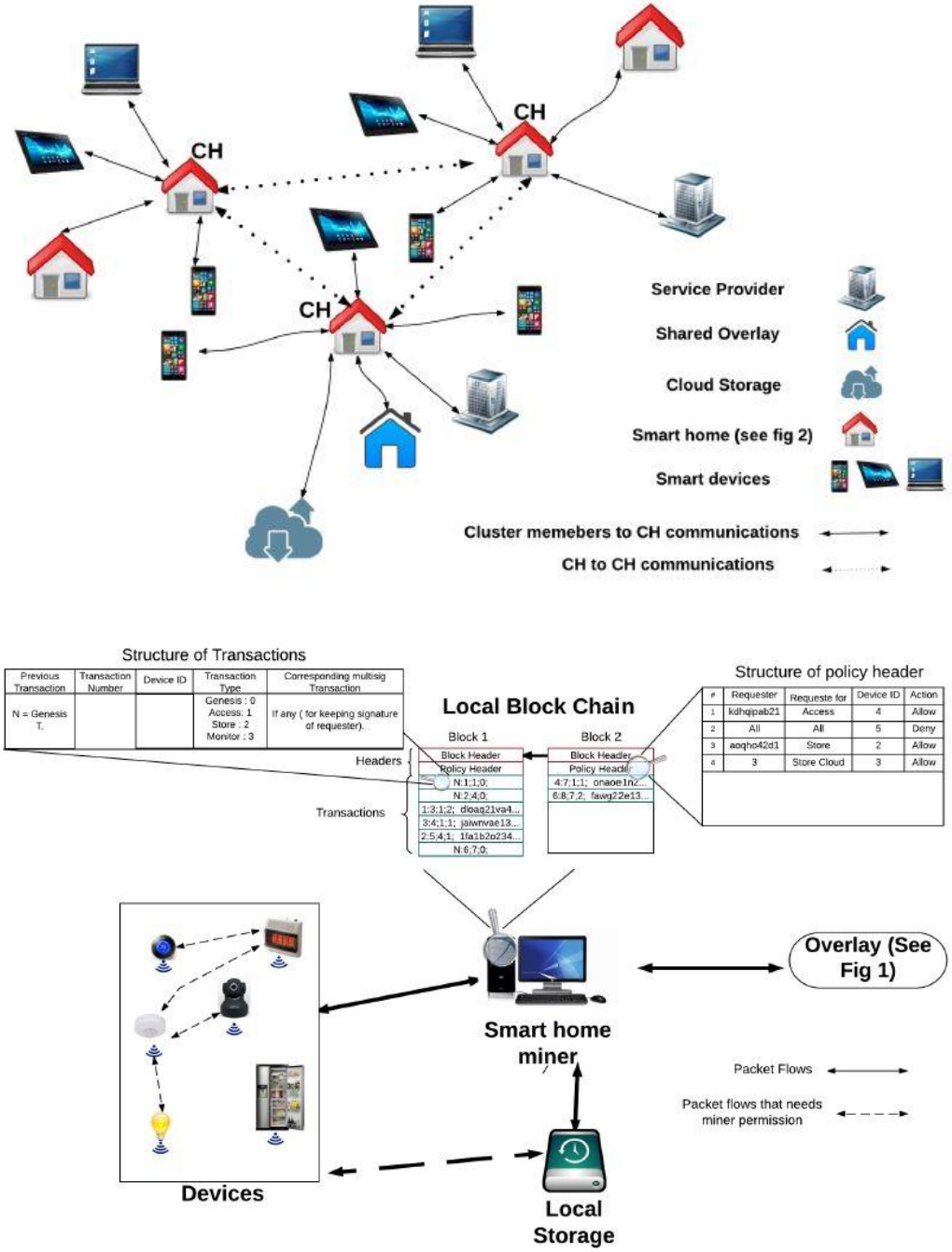
1. IoT 数据孤岛胶水

由于数据与计算可能由不同的组织和机构提供，区块链可以在节点互相缺乏信任的情况下起到“数据审计”的作用，从而成为黏合 IoT 数据孤岛的“胶水”！

2. 智能家居

智能家居由于包含家中数据，对安全性要求极高。通过区块链连接家中智能设备，并与服务提供商、云及其它智能家庭连接，可辅助实现智能家居中万物互联，并同时保护了用户隐私，提高系统整体安全性。

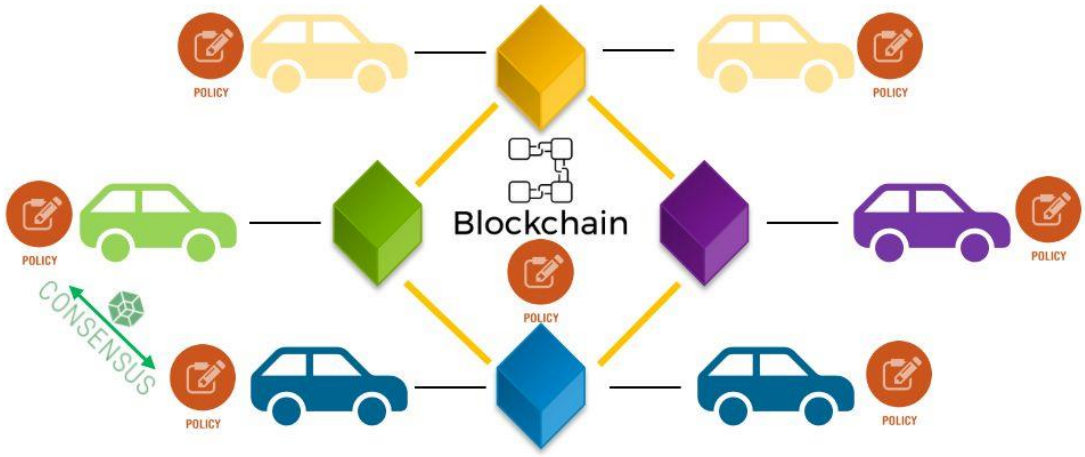
一种智能家居架构如下图：



3. 车联网

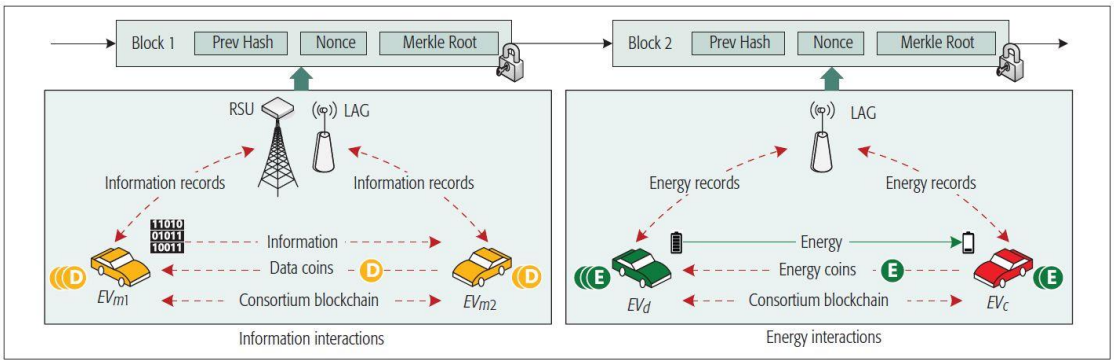
由于车辆来自不同制造商，车辆间通信依然面临缺乏信任的问题。区块链可以作为一个虚拟的中心服务（虽然它本质上是去中心化的）存在：所有的车辆从区块链获取核心车联网控制策略，无论这些车辆是否属于同一品牌；

车企可以在自身的区块链节点上配置不同的策略审批准则。任何车企均可以尝试发布新的车联网控制策略，这种策略会在全网生效，包括那些不同品牌的车辆。但新策略只有获得所有网内车企批准才会在区块链上生效，从而提供给所有联网的车辆使用；不同车辆通过从自己信任的区块链节点获取（事实上相同的）车联网控制策略，从而实现车辆间顺畅的点对点交互。



4. 智能电网与新能源汽车

新能源汽车云与边缘（Electric vehicles cloud and edge, EVCE）计算，做为物联网的一个典型应用场景，同时涉及到信息和能量的传输与交易。使用区块链同时打通强弱电的连接，可以为 EVCE 提供透明（Transparency）及可溯源（Traceability）的安全保障。



星际文件系统-IPFS

星际文件系统（InterPlanetary File System，缩写为 IPFS）是一个旨在实现文件的分布式存储、共享和持久化的网络传输协议。目标是取代传统互联网协议 HTTP。

1. IPFS 是一个协议，类似 http 协议

定义了基于内容的寻址文件系统
内容分发
使用的技术分布式哈希、p2p 传输、版本管理系统

2. IPFS 是一个文件系统

有文件夹和文件
可挂载文件系统

3. IPFS 是一个 web 协议

可以像 http 那样查看互联网页面
未来浏览器可以直接支持 ipfs:/ 或者 fs:/ 协议

4. IPFS 是模块化的协议

连接层：通过其他任何网络协议连接
路由层：寻找定位文件所在位置
数据块交换：采用 BitTorrent 技术

5. IPFS 是一个 p2p 系统

世界范围内的 p2p 文件传输网络
分布式网络结构
没有单点失效问题

6. IPFS 天生是一个 CDN

文件添加到 IPFS 网络，将会在全世界进行 CDN 加速
bittorrent 的带宽管理

7. IPFS 拥有命名服务

IPNS：基于 SFS（自认证系统）命名体系
可以和现有域名系统绑定

区块链技术指南

https://yeasy.gitbook.io/blockchain_guide/

跨链智能合约

https://blog.chain.link/cross-chain-smart-contracts-zh/

跨链智能合约是去中心化的应用，由多个部署在不同区块链网络的智能合约组成。这些智能合约之间可以实现互操作性，并共同构成一个完整的应用。这种创新的设计范式对多链生态的发展起到了关键的推动作用，并将有潜力利用不同区块链、侧链和 layer 2 网络的独特优势，打造出全新的智能合约用例。

多链生态的崛起

因为以太坊是第一个支持完全可编程智能合约的网络，大部分智能合约应用都部署在以太坊主网。它具有先发优势，还因为它创建了不断增长的网络效应、去中心化的基础架构、成熟的开发工具以及庞大的 Solidity 开发者社区。但同时使得算力供不应求，用户需寻找低成本的替代方案。越来越多的智能合约开始部署在其他 layer 1 区块链、侧链以及 layer 2 rollup 上，多链生态由概念变成了现实。

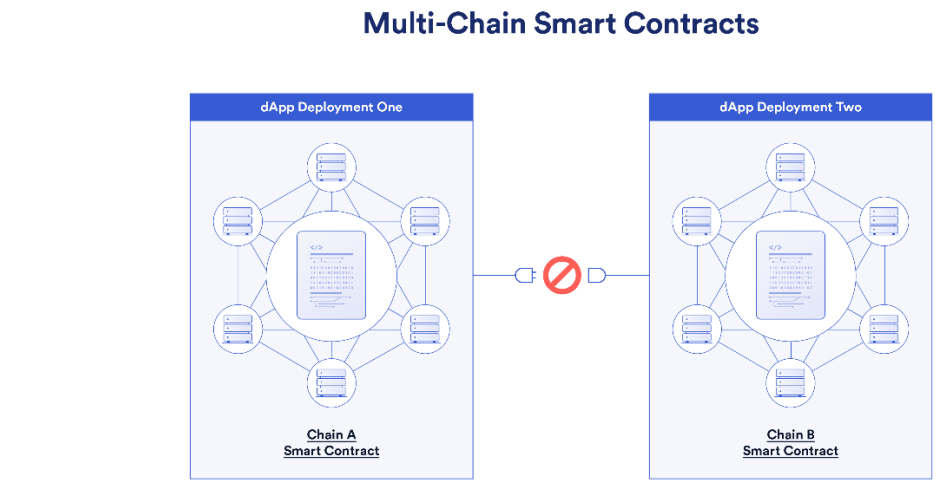
每个侧链和 layer 2 都有自己独特的扩容方案和去中心化方案，在机制设计、共识、交易执行、数据可用性以及隐私方面也各具特色。需要一种理想的多链生态来并行不同链。

以太坊社区使用的多链策略，采取了以 rollup 为中心的发展路线，通过部署多个 layer 2 扩容方案来提升以太坊生态的吞吐量。Layer 2 网络提高了以太坊智能合约的交易吞吐量，因此单笔交易费得以降低，并同时保持了以太坊主网的安全优势。具体方案是利用欺诈证明（fraud proof）或有效性证明（validity proof），在以太坊区块链上验证链下计算。之后还会利用数据分片技术来扩展 rollup calldata 的性能。

越来越多的开发者都在多个区块链上部署智能合约代码库，以充分利用多链生态的优势。项目开发多链智能合约，既可以扩大用户群，又可以在低成本的区块链上试验新功能，以此规避成本风险。这种多链策略在多个 DeFi 垂直领域逐渐形成了势头。比如，SushiSwap DEX 部署到了 15 条不同的区块链上；Beefy Finance 的收益聚合器部署到了 12 条链上；Aave 的货币市场则部署到了 3 条链上。

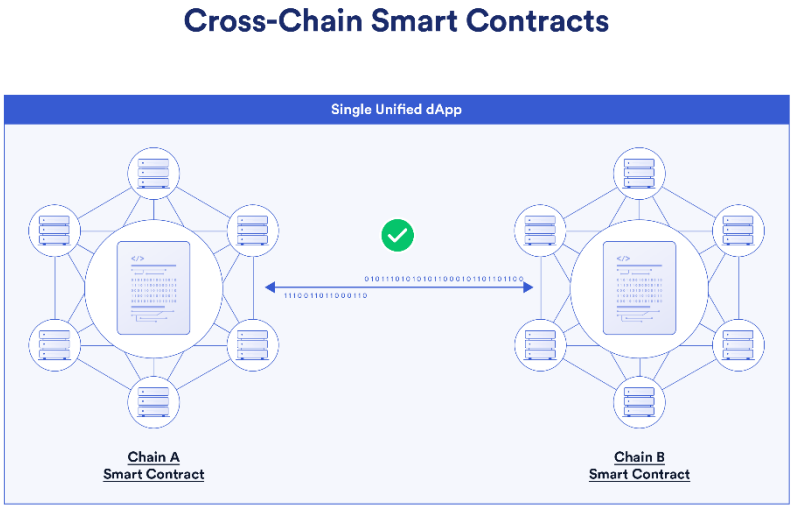
首先，多链智能合约的代码每部署到一个新的区块链上，都需要创建一份原应用的副本，这就意味着应用不再具有唯一性。相反，部署在每条链上的智能合约都管理着自己的内部状态（比如追踪账户余额），而不同区块链上的合约几乎或甚至完全不能直接交互（跨链交互极其困难）。虽然用户可以访问任何一条链上的应用副本，但不同链上的用户体验不能保证完全一样。多链智能合约本质上是不同链上互相孤立的 DApp 副本。安全、性能、成本问题都是需要考虑的。

多链智能合约最大的瓶颈是：在不同区块链、侧链和 layer 2 上部署的智能合约之间几乎或甚至完全无法实现互操作性。虽然现在可以使用通证桥来实现多链部署，但要安全地跨链传输数据则需要采用一种全新的思路来设计智能合约的基础架构。



跨链智能合约

跨链智能合约是去中心化的应用，由多个部署在不同区块链网络的智能合约组成。这些智能合约之间可以互相通信，并共同构成一个完整的应用。事实上，跨链智能合约其实是一个完整的 DApp 将逻辑分别部署在不同的区块链上。



最底层需要设计一种跨链智能合约，使得不同链上的智能合约可以分别执行不同的任务，而所有智能合约又都保持同步，并共同实现同一个应用场景。这样，开发者就可以利用不同区块链的优势，实现独特的价值。比如：去中心化的应用可以利用第一条区块链的抗操纵性来追踪资产所有权；利用第二条区块链的高吞吐量来实现低延时交易；利用第三条区块链的隐私性来识别用户身份；并利用第四条区块链的去中心化存储功能来储存元数据。

实际应用

1. 跨链交易平台

用户在跨链去中心化交易平台（DEX）上执行交易时可以跨越各个区块链的通证池获得流动性，以解决多链 DEX 流动性分化的问题。比如，用户在交易时，其存入的通证可以被分割并桥接至不同区块链，以获得最佳的交易执行价格；然后再将交易完成后的通证桥接回原来的区块链并存入用户钱包。这样一来，所有区块链上的流动性都会被盘活，用户可以享受到更低的交易滑点，并且每条链上的流动性提供方都可以获得更高的交易费收入。

另外，跨链 DEX 的用户还可以将一条链上的原生通证换成另一条链上的原生通证。比如，用户可以将以太坊上的以太币换成比特币区块链上的比特币。这样一来，用户无需通过包装通证或中心化的交易所，就可以灵活交易各个区块链上的原生通证。

2. 跨链收益聚合

跨链收益聚合可以将用户存入的资金放置在各条链上的 DeFi 协议中。这样一来，用户就无需手动将通证资产桥接到其他链上以最大化收益，并轻松获得更高的收益。因此，这将极大改善多链 yield farming 的体验，所有繁琐的流程都将得到简化。

除此之外，这个机制还能扩大 DeFi 应用在新兴区块链上的 TVL，并以此盘活多链生态的流动性。

3. 跨链借贷

跨链货币市场可以推动跨链借贷市场的发展，用户可以在一条链上存入抵押资产（如以太币），并在另一条链上贷入通证资产（如 USDC）。这样一来，用户既可以将抵押资产放在更加安全的区块链上，又可以在吞吐量更高的区块链上贷入通证资产，并将资产放到这条链上的应用中产生收益。

跨链货币市场的用户还可以在另一条利率较低的区块链上贷入通证资产，然后将资产桥接回第二条区块链上还贷款。这将有助于统一不同区块链上的收益率，为低流动性、高利率的货币市场降低贷款成本。

4. 跨链 DAO

去中心化的自治组织（DAO）可以利用跨链互操作性，在一个或多个高吞吐量的区块链网络中展开链上投票，并且将投票结果发送回核心治理合约所在的成本较高的区块链上。这样做不仅可以为 DAO 的参与者降低交易成本，还能实现链上透明且抗操纵，并激励更多人参与。

另外，跨链 DAO 还可以无缝治理并修改不同区块链上的智能合约参数，拓宽一个或多个链上环境中持币者的治理范围。

5. 跨链 NFT

跨链 NFT 市场的用户可以在任何区块链上发布或竞拍 NFT。这将提升 NFT 的流动性，并且 NFT 可以在竞拍结束后在不同区块链之间无缝传输。另外，某一区块链上的游戏也可以采用跨链互操作性来追踪另一条区块链上的 NFT 所有权。因此，用户能够将 NFT 安全地储存在任意区块链上，并同时在其他区块链的游戏中使用这些 NFT。

“门店式”智能合约

现有的单链或多链智能合约可以部署“门店式”智能合约（storefront smart contract），以充分利用多链生态的优势。门店式智能合约为用户提供了一个入口，用户可以通过其访问其他链上的智能合约应用。用户可以通过这类智能合约，在不离开原有区块链环境的前提下，将资产存放在另一条链上的去中心化应用中。

用户无需手动将资产桥接至其他区块链上的智能合约中，他们甚至都不用知道智能合约到底在哪条区块链、侧链或 layer 2 上运行。对用户来说，其他区块链上的应用使用起来跟原生应用没有任何区别。

所有已经运行的去中心化应用，比如衍生品交易平台或货币市场，都可以通过向后兼容的方式添加门店式智能合约。由于智能合约本身具有可组合性，现有协议可以通过无需许可的方式添加跨链互操作性。流畅的用户体验和更高的互操作性，将极大推动多链经济的发展。

跨链互操作性协议（CCIP）

如今大多数区块链网络在本质上仍然是相互孤立的。也就是说，这些区块链之间无法直接发送和接收数据。要实现跨链智能合约，就需要在链与链之间搭建跨链桥。

目前为止，跨链桥主要聚焦于在不同区块链之间传输通证，常见的方式是基于一条链上的原生资产在另一条链上铸造包装资产。然而，跨链智能合约需要通用化程度更高的桥来传输数据包、通证和指令。这类基础设施必须保证安全性和可靠性，并且代码库必须经过严格审计，以确保传输的消息不会被操纵，能够及时传到目标链上，并且可以经受住区块链重组等外部因素的考验。去中心化的预言机网络（DON）很好地解决了区块链预言机问题（即：区块链无法访问链下资源）；同样地，DON 也可以安全地实现区块链互操作性。

Chainlink 网络可以兼容任何区块链上的协议，目前已集成至了一系列区块链、侧链以及 layer 2。因此，Chainlink 有足够的能力推动多链生态向跨链智能合约转型。为了实现这一目标，Chainlink 目前正在开发跨链通信的全局开源标准，即跨链互操作性协议（CCIP）。

与普通的跨链桥不同的是，CCIP 可以让智能合约跨越所有区块链安全地传输数据和通证。智能合约可以用任何方式对数据消息进行加密或解密，因此具有极高的灵活性。值得一提的是，CCIP 将利用目前已在运行的 Chainlink 预言机节点。这些节点不仅具有极高的可靠性和防篡改性，而且还能兼容任何区块链，目前已经为多链 DeFi 经济保障了数百亿美元的价值。

----分界线----

比特币：

通过高昂的挖矿代价，解决分布式账本数据一致性的问题。但同时带来了巨大的资源浪费。利用强冗余性获得强容错、强纠错能力。

经济学知识

一级市场与二级市场

做市商

做市商是指在证券市场上，由具备一定实力和信誉的独立证券经营法人作为特许交易商，不断向公众投资者报出某些特定证券的买卖价格（即双向报价），并在该价位上接受公众投资者的买卖要求，以其自有资金和证券与投资者进行证券交易。买卖双方不需等待交易对手出现，只要有做市商出面承担交易对手方即可达成交易。

做市商通过做市制度来维持市场的流动性，满足公众投资者的投资需求。做市商通过买卖报价的适当差额来补偿所提供服务的成本费用，并实现一定的利润。

保证金制度

在期货交易中，任何交易者必须按照其所买卖期货合约价格的一定比例（通常为 5%～10%）缴纳资金，作为其履行期货合约的财力担保，然后才能参与期货合约的买卖，并视价格确定是否追加资金，这种制度就是保证金制度，所交的资金就是保证金。

超额抵押

超额抵押是指抵押人以同一抵押物为一个或几个债权设定抵押时，这些抵押所担保债权大于抵押物价值情形。

平仓

平仓是源于商品期货交易的一个术语，指的是期货买卖的一方为对销以前买进或卖出的

期货合约而进行的成交行为。平仓是在股票交易中，多头将所买进的股票卖出，或空头买回所卖出股票行为的统称。

期货交易的全过程可以概括为建仓、持仓、平仓或实物交割。建仓也叫开仓，是指交易者新买入或新卖出一定数量的期货合约。平仓是指交易者了结持仓的交易行为，了结的方式是针对持仓方向作相反的对冲买卖。

期货交易中的平仓相当于股票交易中的卖出。由于期货交易具有双向交易机制，与开仓相对应，平仓也有买入平仓(对应于卖出开仓)和卖出平仓(对应于买入开仓)两种类型。

交易滑点

滑点，是指在进行交易时，客户下达的指定交易价格与实际成交价格存在较大差别的一种现象。每个交易者都会碰到滑点，不管他们交易的是股票、外汇还是期货。其出现原因可能是：1.市场报价断层；2.网络延迟；3.LastLook；4.外汇经纪商操纵。