

---

# 区块链技术简介

---

卢洋

- 
- 1. 个人简介
  - 2. 区块链技术
  - 3. 比特币
  - 4. 加密货币本质

---

# I. 个人情况简介

- 姓名：卢洋
- 学历：工学博士
- 学习经历：哈尔滨工业大学，本硕博
- 博士毕业后工作经历：曾就职于上海华为技术有限公司，现就职于许继集体哈尔滨电工仪表研究所

# 研究方向及技能

---

## I. 研究方向：

- 大数据、云计算、机器学习；

## 2. 技能：

- Linux、Docker、Hadoop、Spark、Akka、Kafka、Cassandra、Mesos、Kubernetes；

## 3. 编程语言：

- Python、Go、Scala、Java、C++。

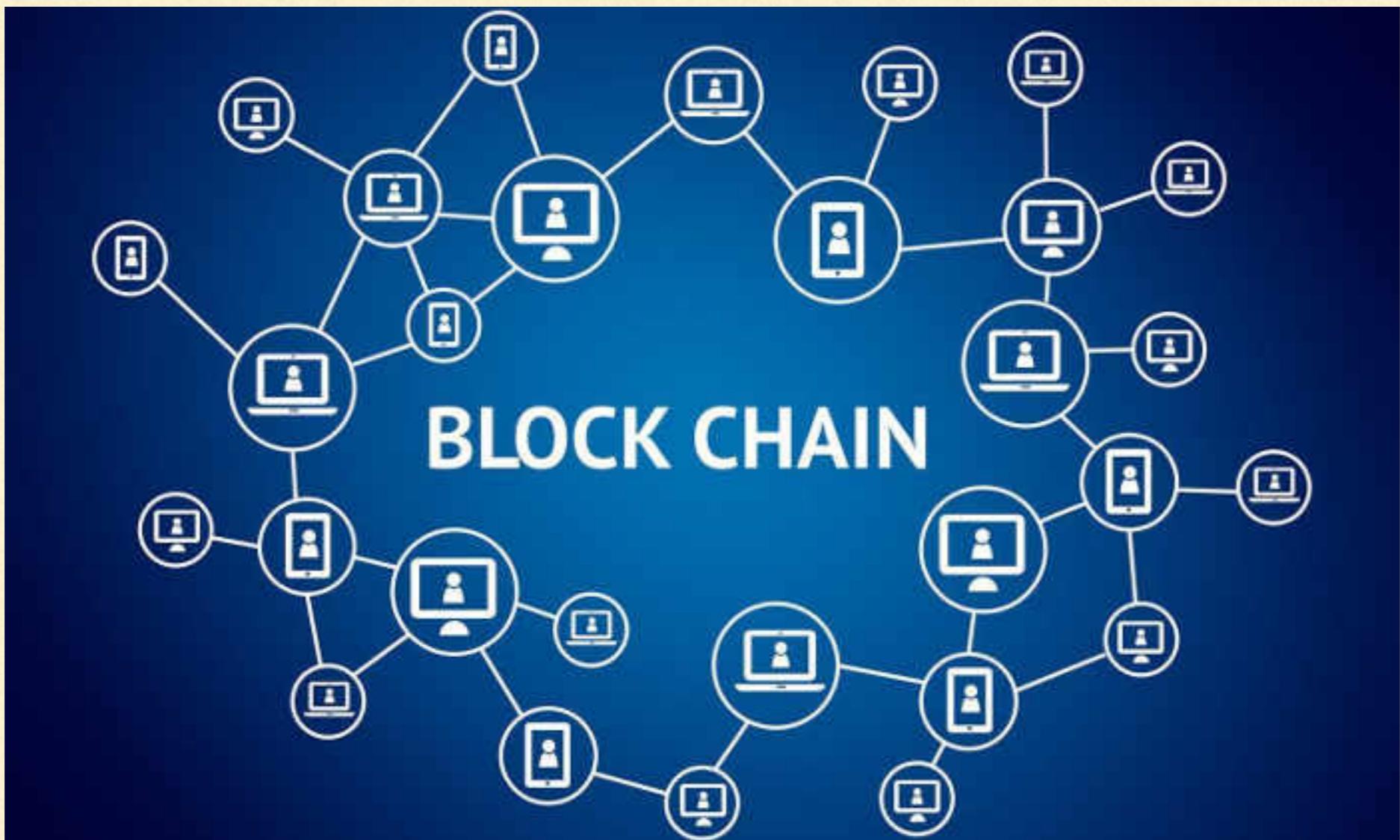
---

## 2. 区块链技术及加密货币介绍

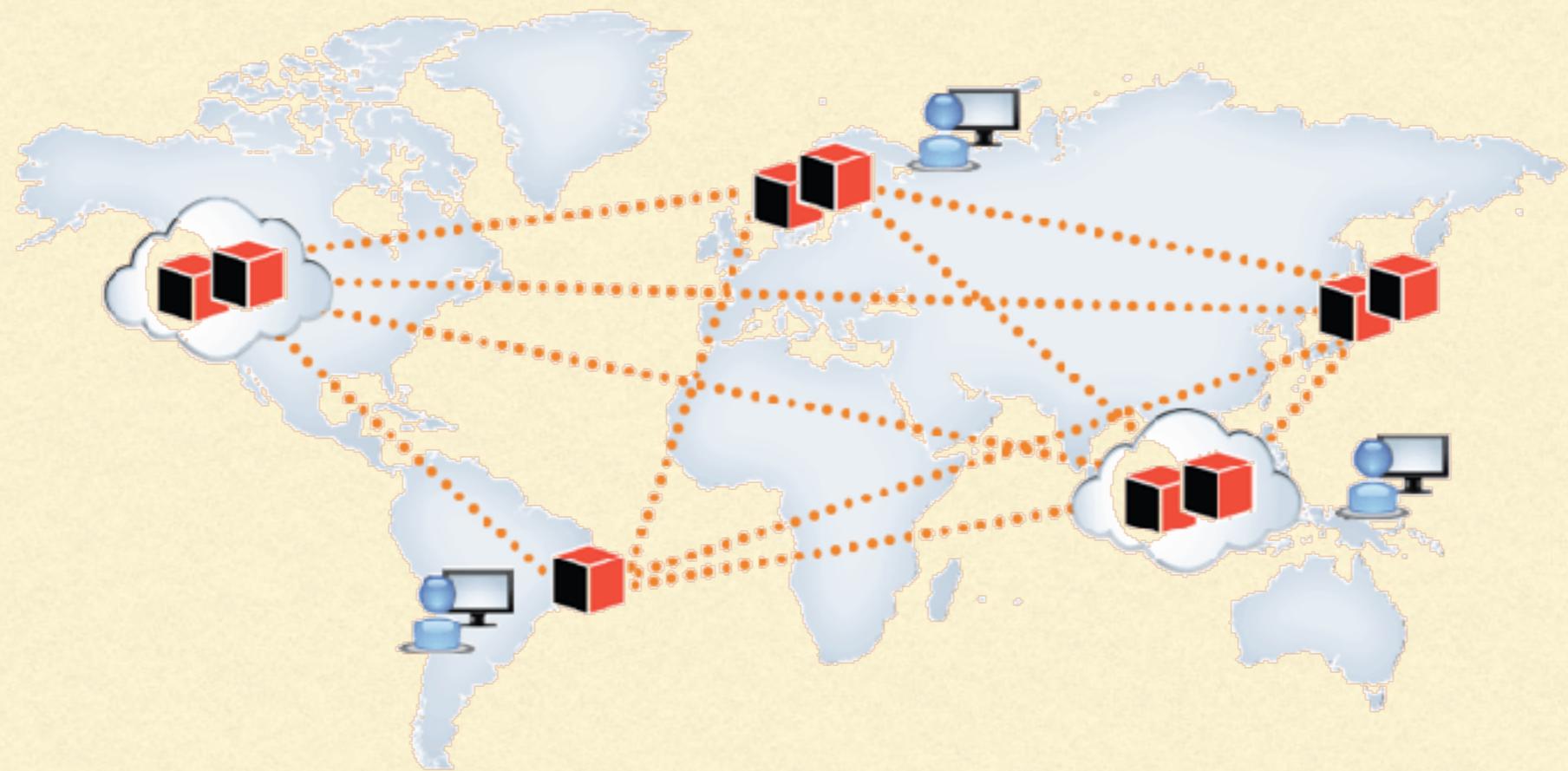
---

“理论是灰色的，而生命之树常青。”

-哥德



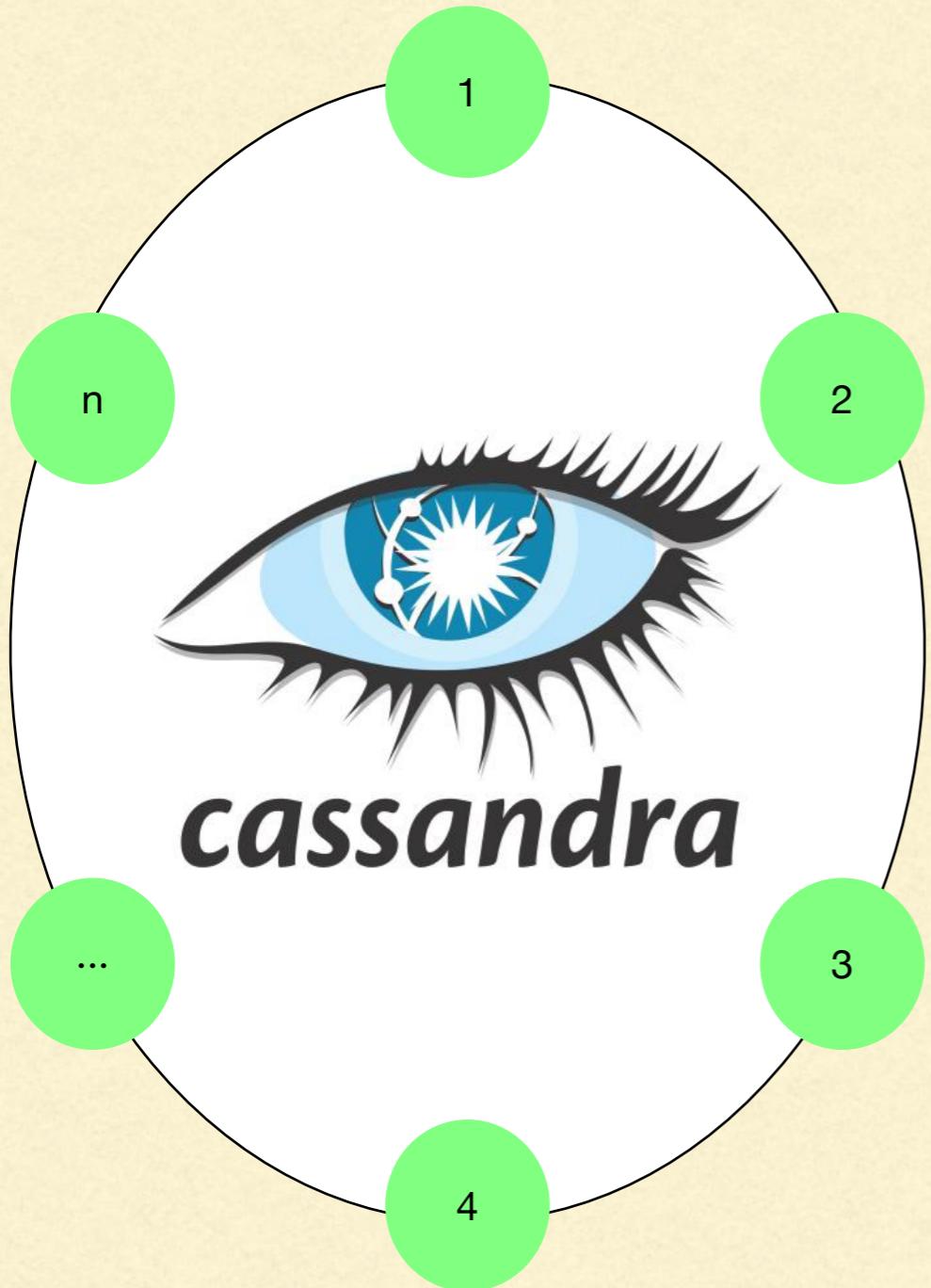
区块链是数字加密货币背后的技术。



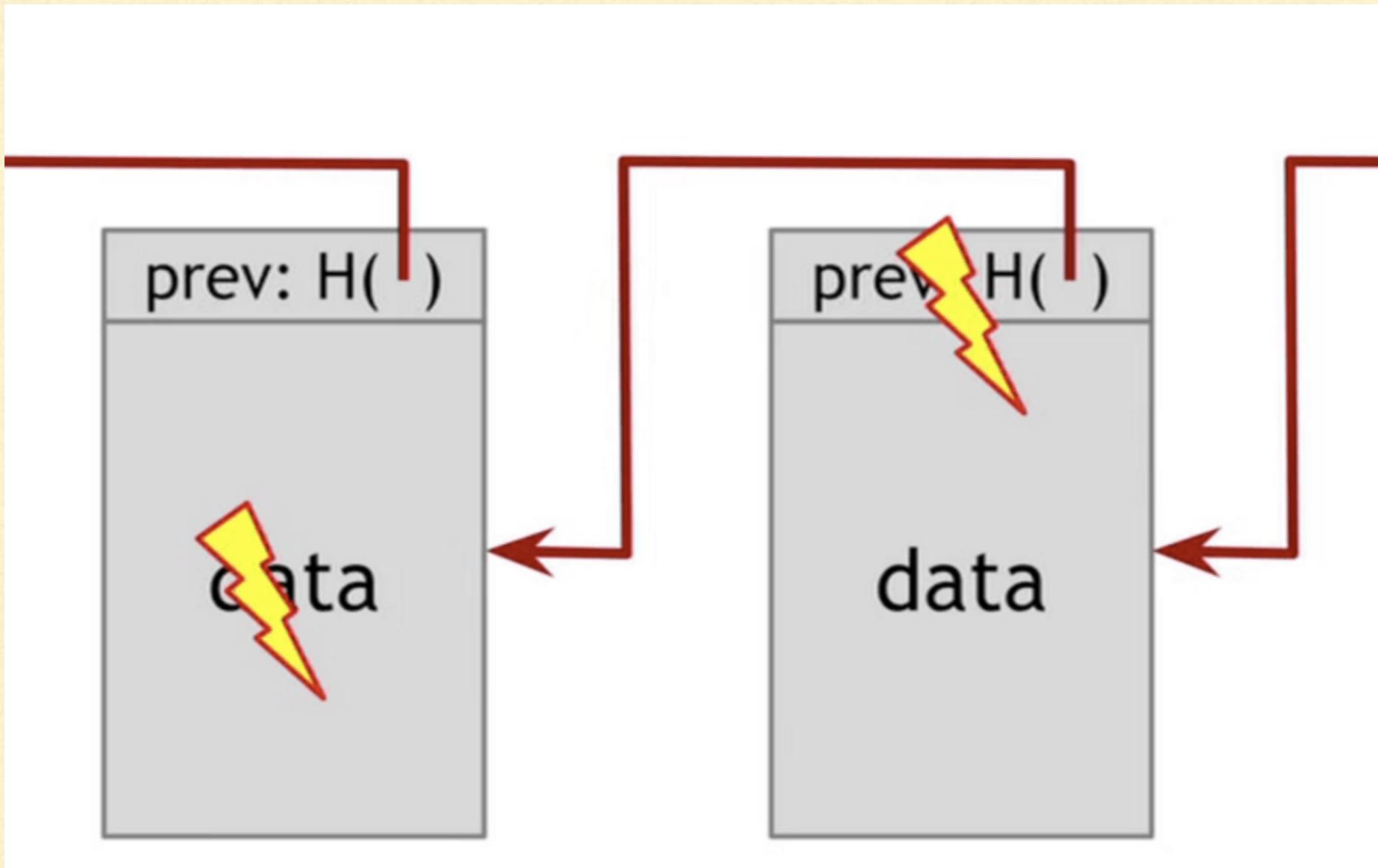
区块链：一种特殊的分布式数据库。

特点：

- 作用：存储信息，需要保存的信息可以进行写入，并能够读取；
- 去中心化：没有中心节点，节点平等。

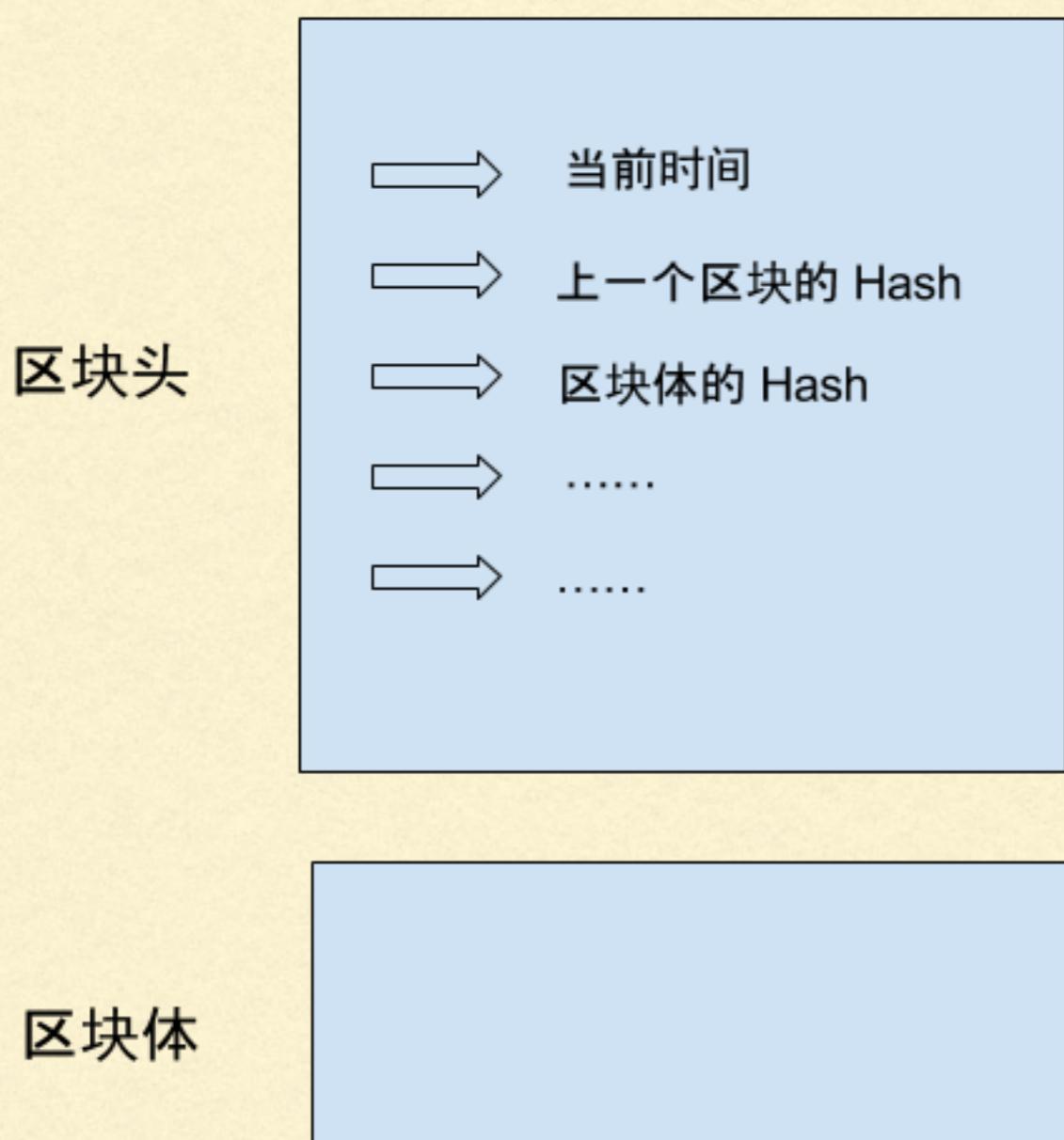


- 分布式数据库非新发明，已存在，如Cassandra。
- 相比之下，区块链没有中心管理员、彻底地去中心化。
- 因为无人管理，所以无人可以控制。



- 区块链由一个个区块（block）组成。
- 区块很像数据库记录，每次写入数据，就是创建一个区块。

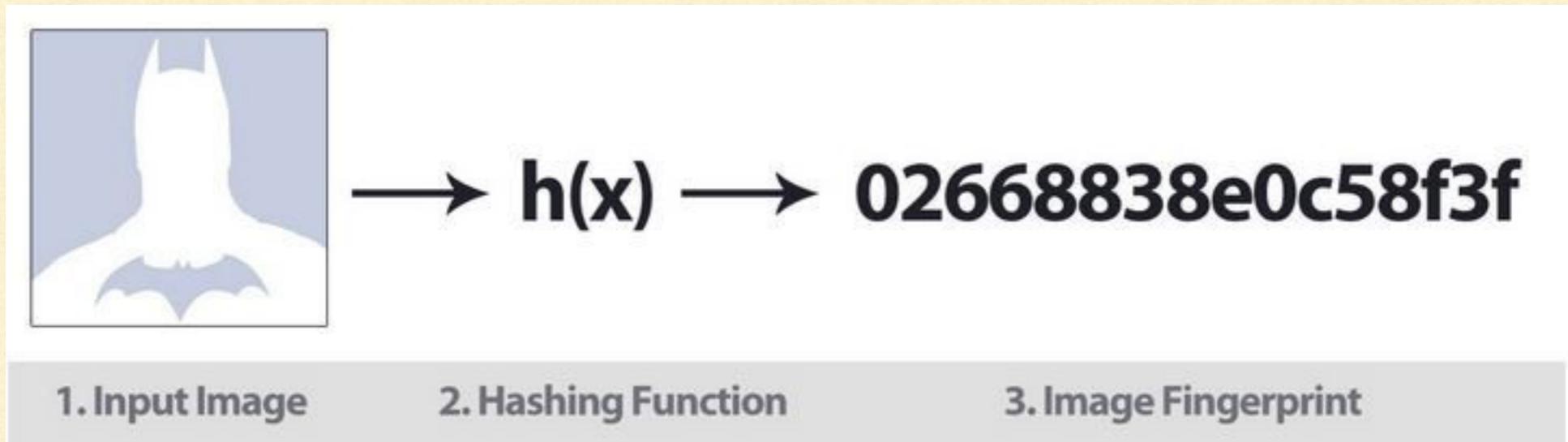
## 每个区块包括两部分：



- 区块头 (head) : 记录当前区块的特征值；
- 区块体 (body) : 实际数据。

区块头包含了当前区块的多像特征值：

- 生成时间；
- 实际数据（即区块体）的哈希；
- 上一个区块的哈希；
- .....



- 哈希：计算机对任何内容，计算出的相同长度的特征值。
- 区块链的哈希长度是256位，即不论原始内容是什么，最后都会计算出一个256位的二进制数。
- 理论上，一个字符串经过计算得到的哈希，其它字符串也有可能得到相同的哈希，但概率极低，可以近似认为不可能发生。

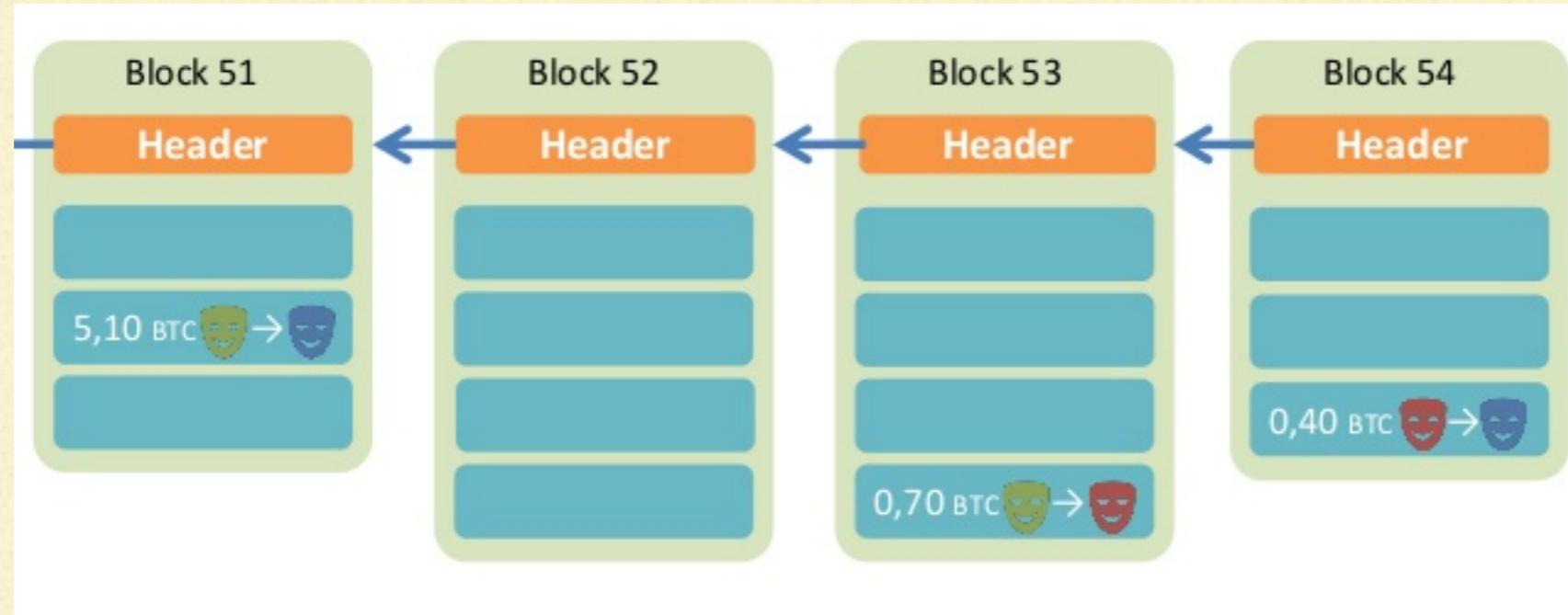
因此，就有两个非常重要的推论：

- 
- 推论1：每一个区块的哈希都是不一样的，可以通过哈希表示区块；
  - 推论2：如果区块的内容改变了，其哈希一定会变化。

---

$$\text{Hash} = \text{SHA256}(\text{Head})$$

- 区块与哈希一一对应，每个区块的哈希针对“区块头”（head）进行计算，即：将区块头的各项特征值，按照顺序连接，组成一个很长的字符串，再对该字符串计算哈希。
- SHA256是区块链的哈希算法。



- 区块头包含：当前区块体的哈希、上一个区块的哈希。  
意味着：当前区块体内容改变，或上一个区块的哈希改变，必然会引起当前区块的哈希变化。
- 因此，修改一个区块，导致该区块的哈希变化。为了让后面的区块还能与之相连，就必须依次修改后面所有的区块，否则被修改的区块就脱离了区块链。
- 计算非常耗时，短时间内修改多个区块，几乎不可能（除非掌握全网51%的算力）。
- 通过联动机制，区块链保证了自身的可靠性，数据一旦写入，就无法篡改。

- 保证节点同步，新区块产生速度不能过快。
- 区块链发明者中本聪故意让添加新区块变得困难，其设计为：每十分钟，全网才能产出一个区块，即一小时六个。
- 产出速度通过设置海量计算达成；也就是说，只有通过极其大量的计算，才能得到当前区块的有效哈希，从而将新区块添加到区块链。
- 这个过程即为“挖矿”（mining），计算哈希的机器叫“矿机”，操作矿机的人称为“矿工”。



## Block #100000

**BlockHash** 00000000003ba27aa200b1cecaad478d2b00432346c3f1f3986da1af33e5015

## Summary

Number Of Transactions	4	Difficulty	14484.16236122
Height	100000 (Mainchain)	Bits	1b04864c
Block Reward	50 BTC	Size (bytes)	957
Timestamp	Dec 29, 2010 7:57:43 PM	Version	1
Mined by		Nonce	274148111
Merkle Root	0f3e94742aca4b5ef85488dc37c06c3...	Next Block	100001
Previous Block	99999		

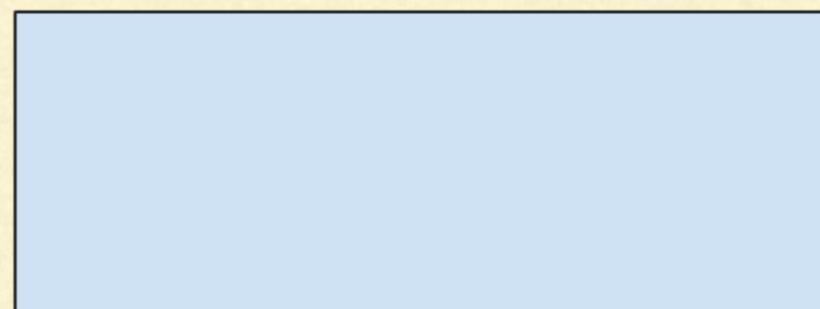
```
target = targetmax / difficulty
```

- 何为有效：  
只有小于目标值 (target) 的哈希才是有效的；否则，无效。

## 区块头



## 区块体

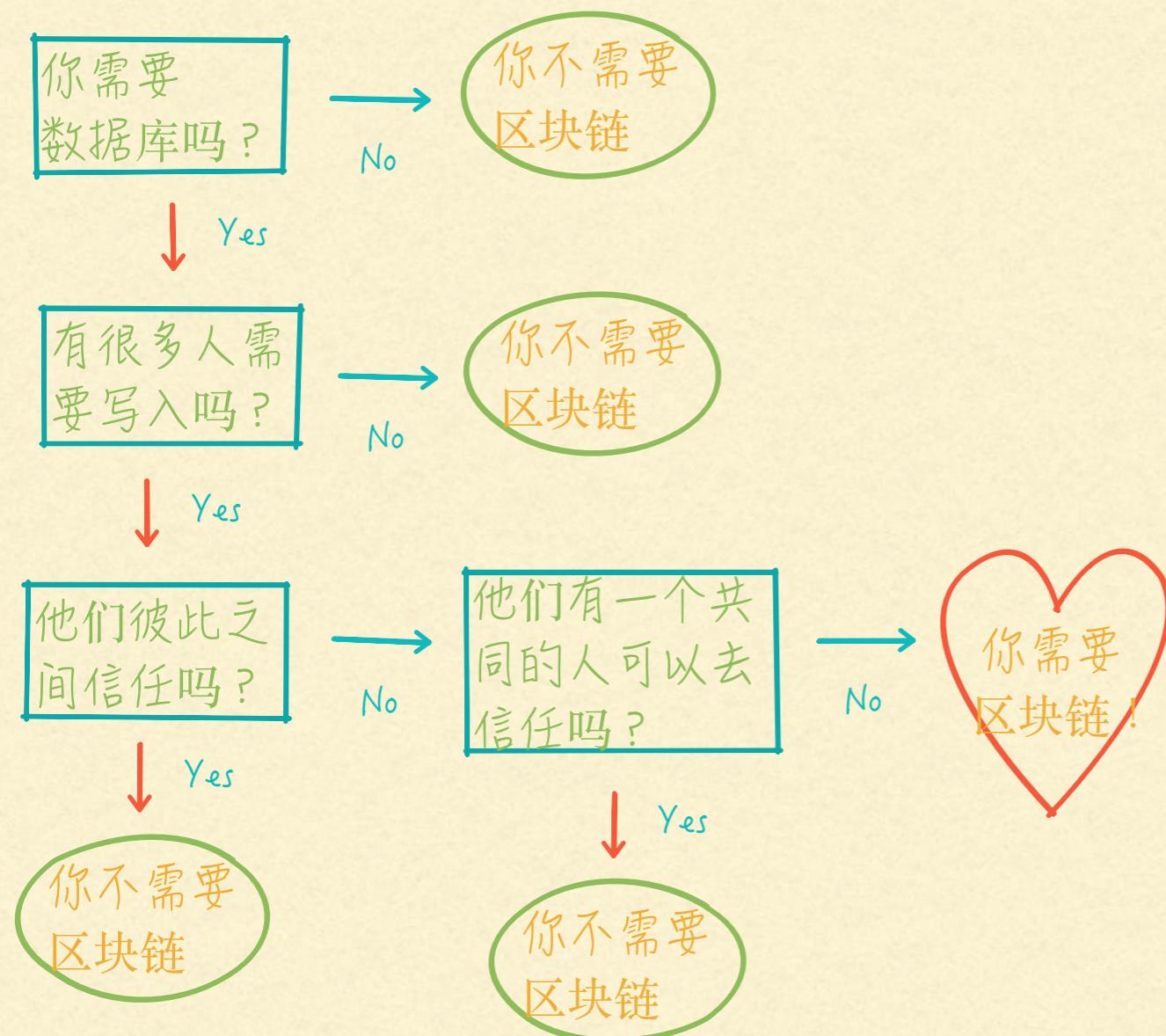


- 当前区块的哈希由区块头唯一确定。如果要对同一区块反复计算哈希，意味着区块头必须不停的变化，否则不可能计算出不一样的哈希。
- 区块头所有的特征值都是固定的，为了让区块头发生变化，中本聪添加了一个随机项，即Nonce（number once的缩写）。
- Nonce是一个随机数；根据协议，Nonce是个32位的二进制值，即最大可到21.47亿。
- 挖矿本质：矿工去猜出Nonce的值，使得区块头的哈希可以小于目标值，从而能够写入区块链。Nonce非常难猜，目前只能通过穷举法进行试错。

- 区块链作为无人管理的分布式数据库，从2009年开始已经运行了8年，没有出现大的问题，证明其可行性。
- 然而，为了保证数据的可靠性，区块链也有其自身的代价：
  - I. 效率：数据写入区块链，最少要等待十分钟，所有节点都在同步数据，则需要更长时间；
  2. 能耗：区块的生成需要矿工进行无数无意义的计算，非常消耗能源。

## ■ 区块链适用的场景非常有限：

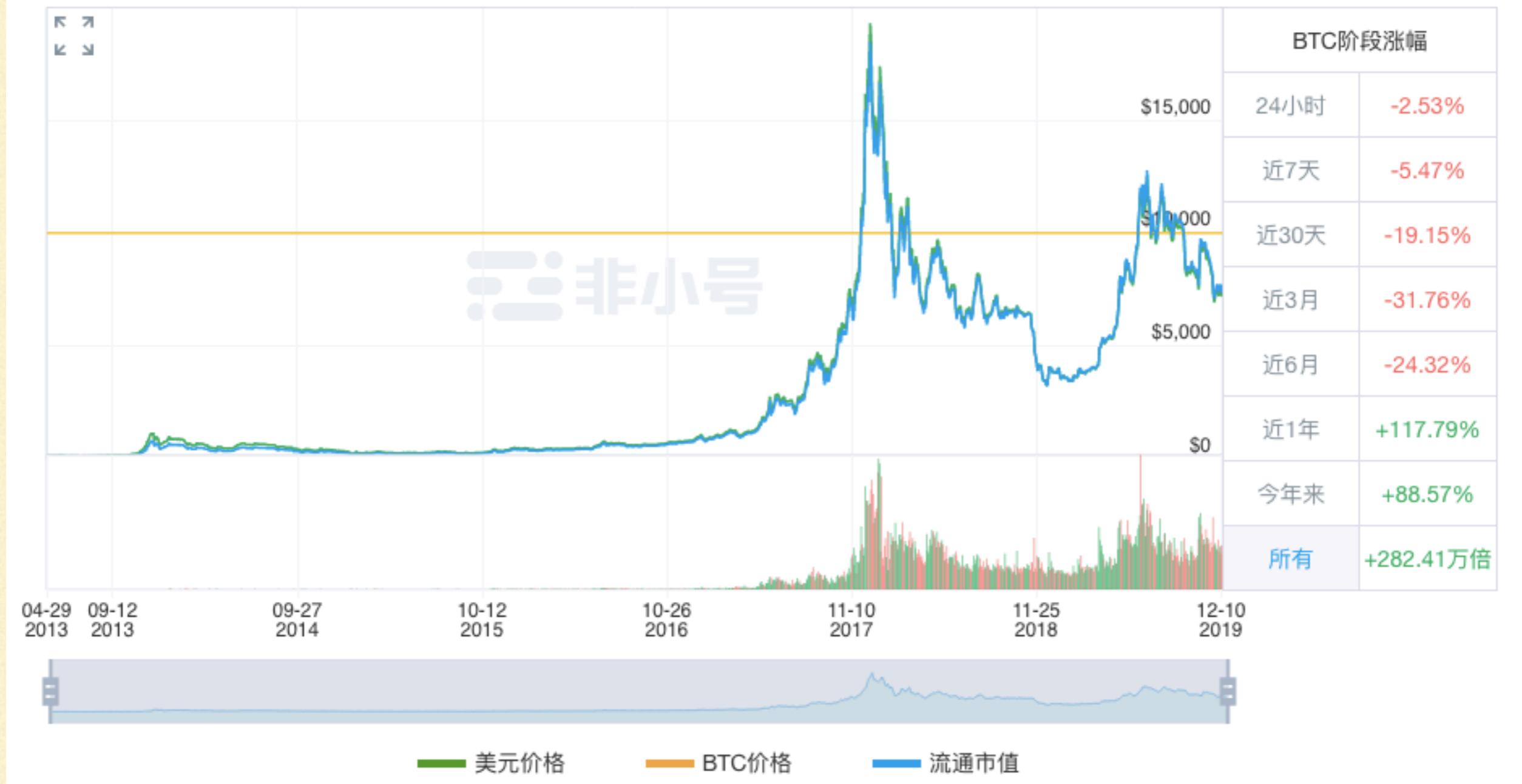
1. 不存在所有成员都信任的管理当局；
2. 写入的数据不要求实时性；
3. 挖矿的收益能够弥补本身的成本。



- 目前，区块链最大的应用场景（可能也是唯一的应用场景），就是以比特币为代表的加密货币。

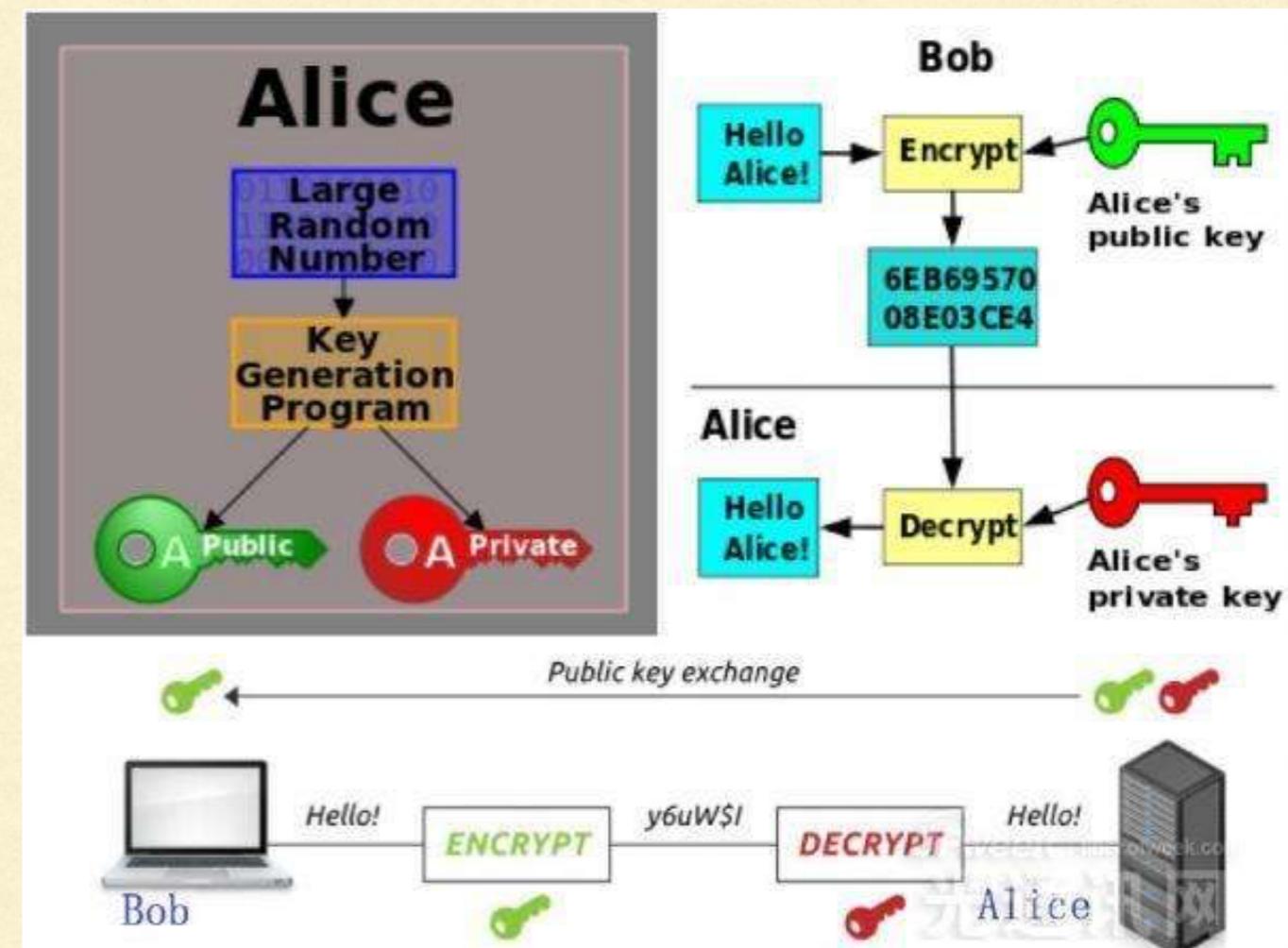
---

### 3. 比特币

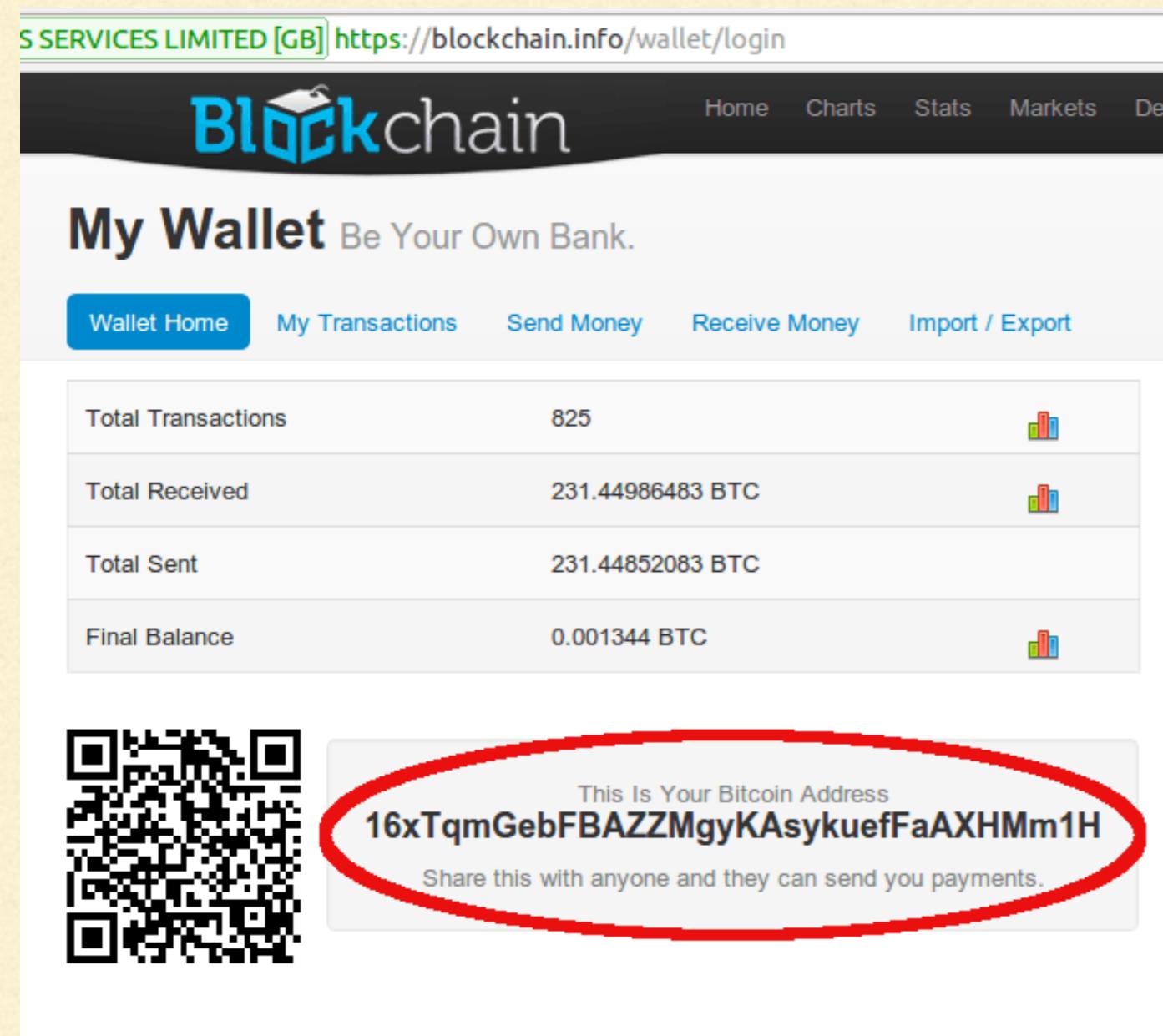


## 非对称加密

- 非对称加密：加密和解密需要两把钥匙，一把公钥和一把私钥。
- 公钥公开，任何人都可获取；私钥保密，只有拥有者才可使用。
- 公钥和私钥可以用于信息加密，在加密货币的应用场景下，秘钥可以加密钱。
- 比特币（及其它加密货币）的原理：简单概括为，非对称加密保证了支付的可靠性。



- 对于比特币来说，钱不是支付给个人，而是支付给一个私钥。
- 比特币交易需要拥有自己的私钥和公钥。
- 开户，获得钱包，钱包保存秘钥。
- 根据协议，公钥512位，不方便传播；协议为公钥生成160位指纹，写成十六进制，约为26到35个字符，指纹也称作钱包的地址。



# 交易流程

## 申报交易

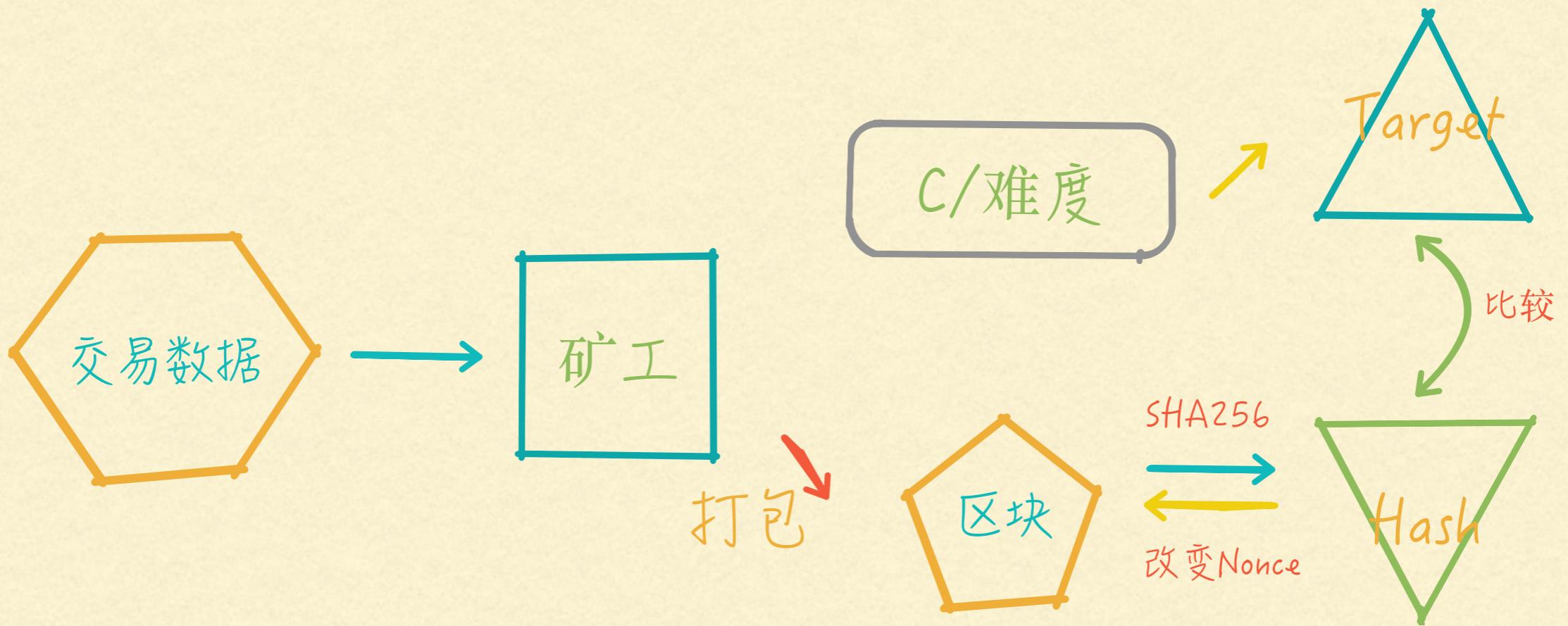
1. 上一笔交易的Hash（从哪里得到这些比特币）；
2. 本次交易双方的地址；
3. 支付方的公钥；
4. 支付方私钥生成的数字签名。

## 验证交易

1. 找到上一笔交易，确认支付方的比特币来源；
2. 算出支付方公钥的指纹，确认与支付方的地址一致，从而保证公钥属实；
3. 使用公钥去解开数字签名，保证私钥属实。

Number <sup>?</sup>	Hash <sup>?</sup>	Time <sup>?</sup>	Transactions <sup>?</sup>	Total BTC <sup>?</sup>	Size (kB) <sup>?</sup>
<a href="#">356987</a>	<a href="#">141a6f95b2...</a>	2015-05-18 13:28:14	1714	17353.00313324	749.227
<a href="#">356986</a>	<a href="#">13cff723ec...</a>	2015-05-18 13:11:53	2114	23805.24520712	749.204
<a href="#">356985</a>	<a href="#">1128aa2601...</a>	2015-05-18 12:27:49	594	6119.90095486	392.306
<a href="#">356984</a>	<a href="#">140b0f27b9...</a>	2015-05-18 12:20:14	1087	7849.33374079	544.102
<a href="#">356983</a>	<a href="#">d1ea5bc1c7...</a>	2015-05-18 12:08:01	830	7799.27270534	455.006
<a href="#">356982</a>	<a href="#">76634b52be...</a>	2015-05-18 11:58:42	221	1706.08443753	152.745
<a href="#">356981</a>	<a href="#">ab5a643167...</a>	2015-05-18 11:57:28	756	7245.57902445	372.38
<a href="#">356980</a>	<a href="#">b780d34ab0...</a>	2015-05-18 11:46:36	383	4623.1382688	430.319
<a href="#">356979</a>	<a href="#">110a166e82...</a>	2015-05-18 11:41:08	2276	19539.64880577	999.931
<a href="#">356978</a>	<a href="#">4501065561...</a>	2015-05-18 11:01:11	1250	17106.20270042	772.021

- 确认交易后，交易还不算完成。交易数据必须写入数据库，才算成立，对方才能真正收到钱
- 比特币使用特殊的数据库保存交易数据：区块链。



- 所有的交易数据会传送到矿工那里，矿工负责将交易数据写入区块链；
- 矿工负责把交易信息打包，组成区块，然后计算该区块的哈希；
- 矿工间竞争，谁先算出hash，谁就可以添加新的区块到区块链，交易信息也随之写入区块链。



- 比特币协议规定：挖到新区块的矿工得到奖励。
  - 最初（2008年）：50个比特币；
  - 每四年减半；
  - 目前（2018年）：12.5个比特币；
  - 2140年：0。
- 矿工收益：
  - 区块奖励金+交易手续费。

---

## 4. 加密货币的本质



目前，各种各样的加密货币。

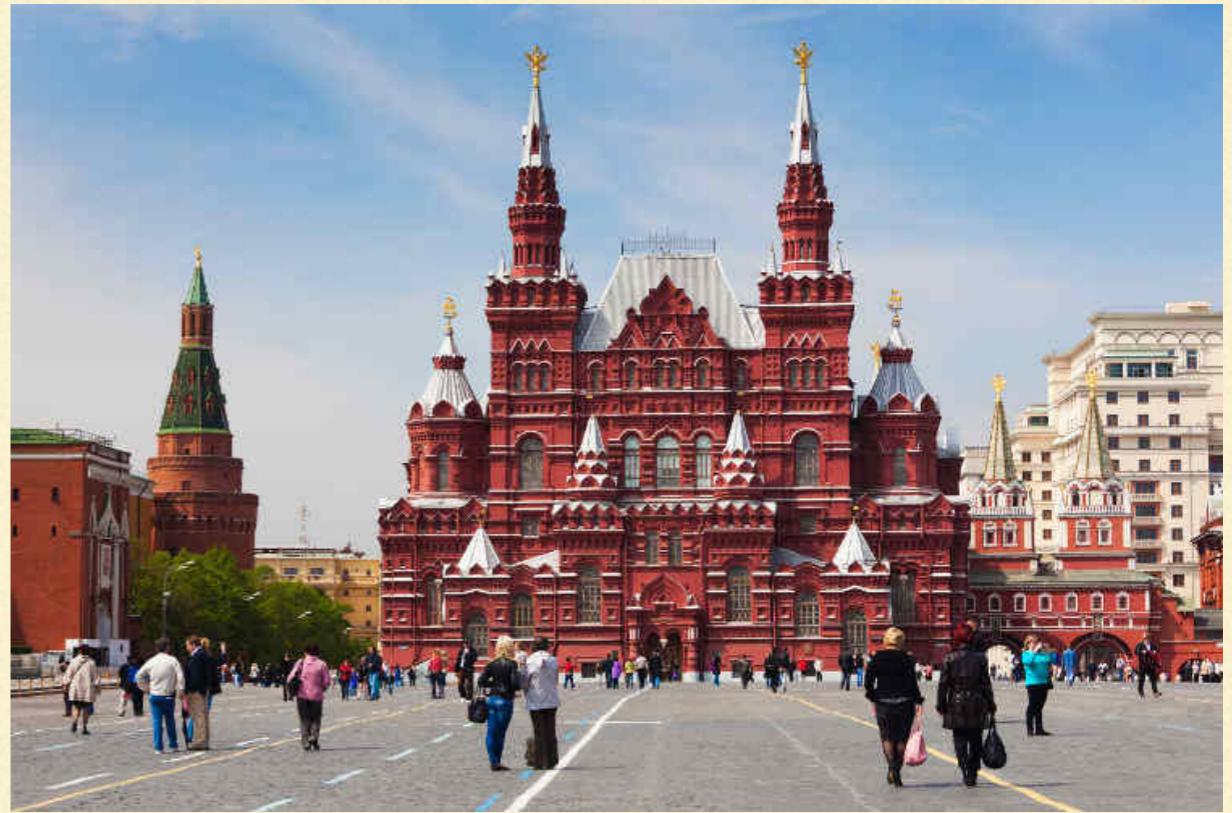
---



# **WHAT IS CRYPTOCURRENCY?**



- 钱是什么？
- 人民币、美元、金银财宝。
- 有价值就是钱？



- 价值普遍认同。
- 钱的本质，或者说货币的本质，就是其可信性。



- 可信 -> 钱，有没有价值？不重要。
- 比特币要解决的核心问题：创造一种可信的数字凭证。
- 比特币的基础：密码学。
- 因此称为加密货币。



By-lushulan No.20140912145749170672

昵图网 www.nipic.com

- 比特币的三个特点，保证其可信性：
  - 1. 不会被轻易偷走：有私钥才能拿到别人的钱，正常情况下，拿不到私钥；
  - 2. 无法伪造：每个比特币都能追溯其来源，而所有比特币都来自矿工奖励。新建区块 -> 获得奖励，很难，无法伪造；
  - 3. 无法大批生产：比特币发型速度稳定。现在每十分钟新增12.5个，每四年递减，最终停止增长。纸币：政府滥发 -> 通货膨胀。



Justin Sun ✅ @justinsuntron · 5分

I officially announce I've won the record-setting 20th-anniversary charity lunch hosted by @WarrenBuffett. I'll also invite #blockchain industry leaders to meet with a titan of investment. I hope this benefits everyone. #TRON #TRX #BTT #BitTorrent

● 翻译推文



128



87



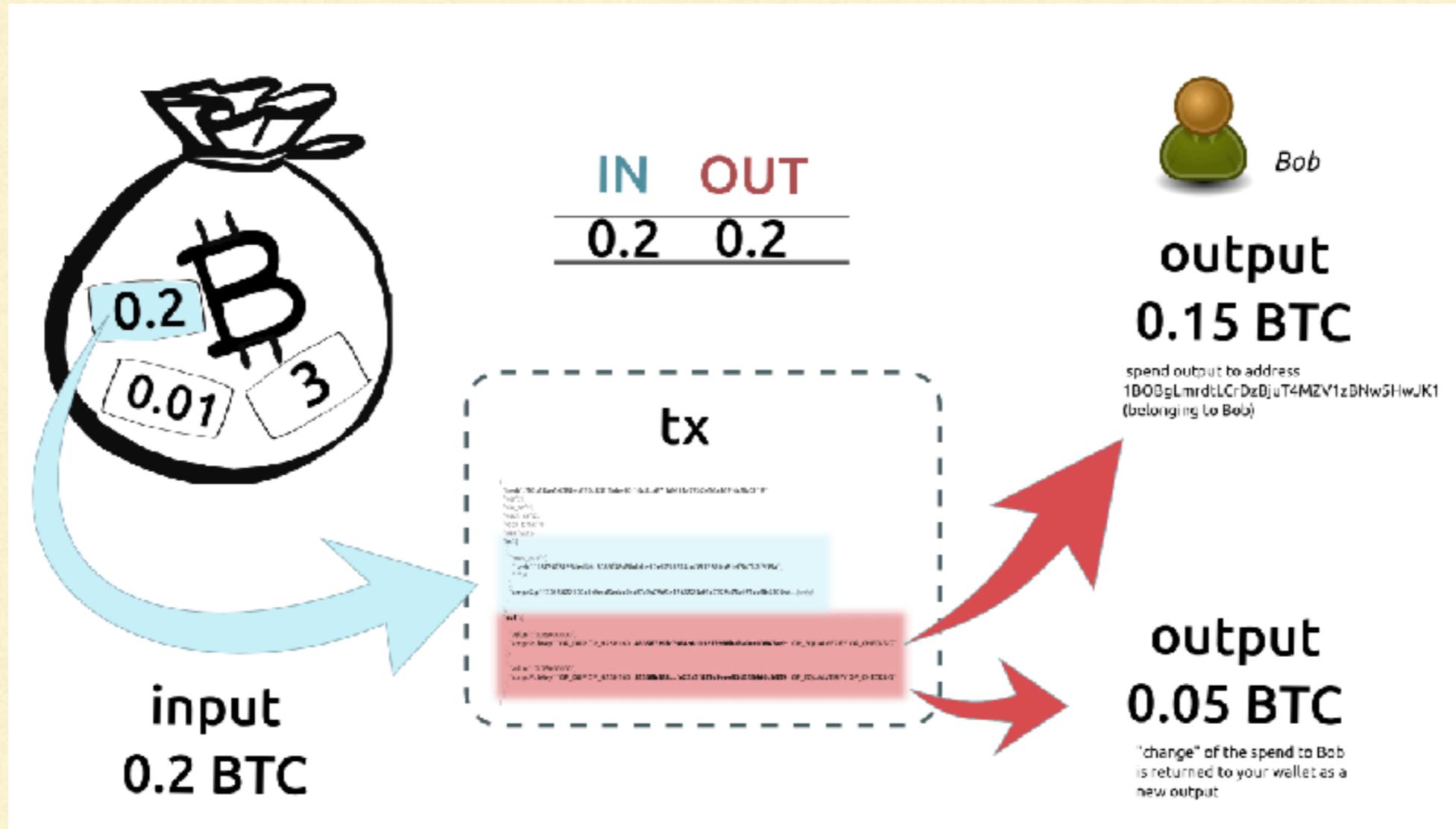
264



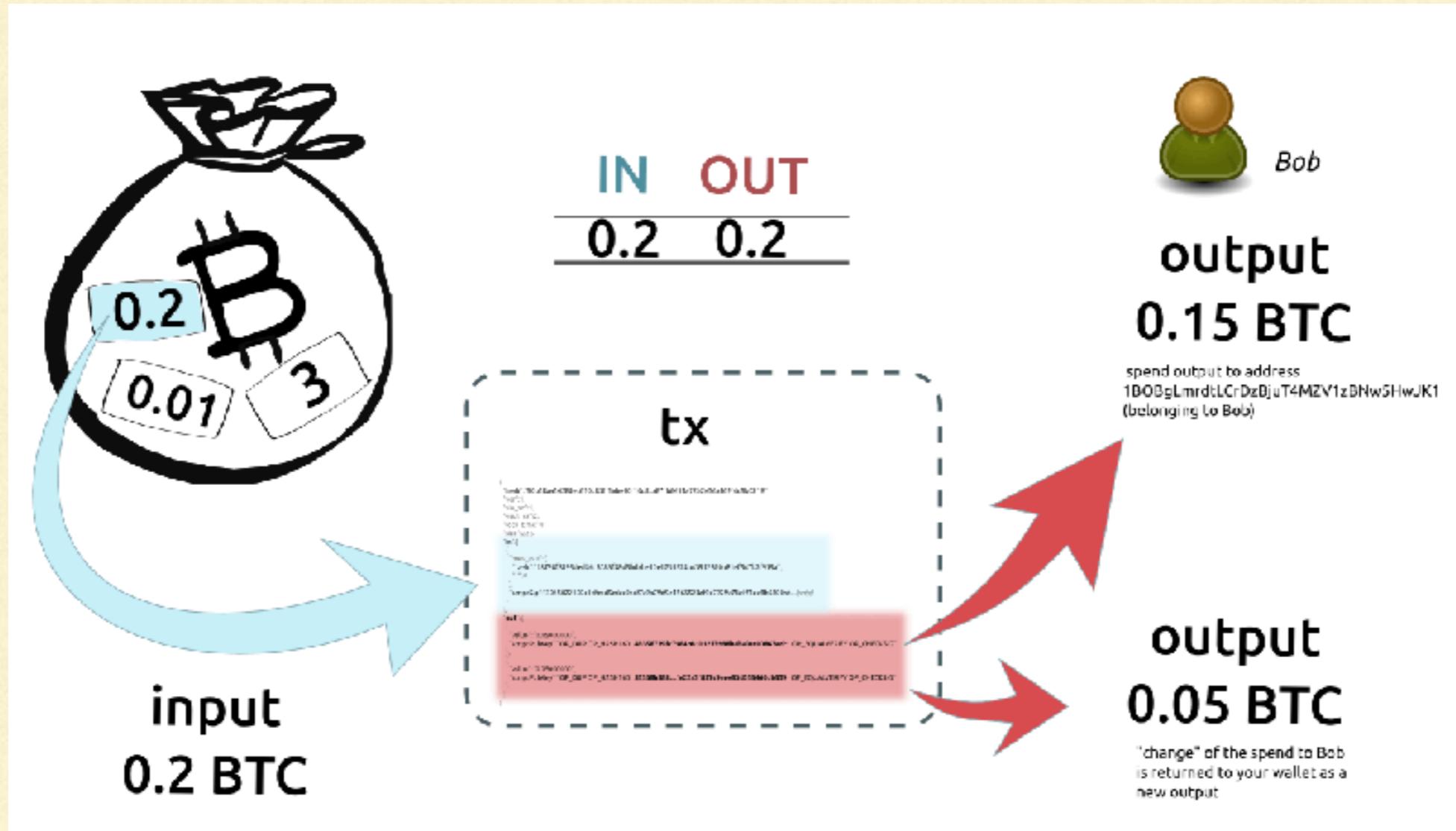




- 比特币需要实体嘛？
- 钱都有实体，怎么可能存在无形的钱？
- 钱就应该是无形的，那些实体的钱其实是对物质材料的浪费，由于技术不发达，不得不做成实体。
- 区块链 == 中央记账系统。



- 区块链就是一个数据库，记载了所有的交易，用作中央记账系统，分布在无数个节点之上。
- 每笔交易的核心，就是一句话，比如“张三向李四转移了1个比特币”。为了证明这句话可信，张三为它加上了数字签名。任何人都可以用张三的公钥，证明这确实是张三本人的行为。另一方面，其他人无法伪造张三的数字签名，所以不可能伪造这笔交易。
- 矿工们收到这句话，首先验证数字签名的可信性，然后验证张三确实拥有这些比特币（每一笔交易都有上一笔交易的编号，用来查询比特币的来源）。验证通过以后，就着手把这句话写入区块链了。一旦写入区块链，所有人就都可以查询到，因此这笔比特币就被认为，从张三转移到了李四。



- 区块链的作用就是把这句话永久保存下来了，让任何人都可以查看，并且任何人（包括张三本人在内）都无法再修改了。
- 货币是什么？其实就是这句话“张三向李四转移了1个比特币”。这一句话就完成了一次支付。我们平时用人民币支付，其实只是用纸币表达这条信息。如果每个人都可以实时写入/读取中央记账系统（区块链），那么完全可以不携带货币。
- 数字货币的本质，就是一条可信的数据库记录。数据库记录了你拥有了多少钱，由于这个记录可信，你就真的因此拥有了这笔购买力。