

# 疯狂者游戏——全网唯一 不可伪造数据比特币原理 (概述)



# “比特币”是什么？

比特币是一种**虚拟货币**（数字货币）。

比特币是一种由开源的P2P软件产生的电子币，数字货币，是一种网络虚拟资产。比特币也被意译为“比特金”。比特币基于一套密码编码、通过复杂算法产生，这一规则不受任何个人或组织干扰，去中心化；任何人都可以下载并运行比特币客户端而参与制造比特币；比特币利用电子签名的方式来实现流通，通过P2P分布式网络来核查重复消费。每一块比特币的产生、消费都会通过P2P分布式网络记录并告知全网，不存在伪造的可能。

比特币的特点：

- 1.数字货币。
- 2.不依托于任何国家或组织而利用计算机技术独立发行。
- 3.通过P2P分布式技术实现，无中心点。
- 4.所有人均可自由的参与。
- 5.总量有限，不可再生。
- 6.本身机制开源，可以被山寨。



# 比特币的特点延伸

1. 较大的政策风险，国家组织是否会承认？

目前德国是唯一承认比特币具有合法货币地位的国家。  
美国表达了支持的态度。

2. 安全性如何得到保证，被盗了谁来给你找回？

11年MyBitcoin遭遇黑客攻击，7.8W比特币至今下落不明。

3. 总量有限决定了比特币极具投机色彩，价格犹如失控的过山车。

10年比特币仅为数美分一个，13年3月突破45美元/个，  
13年11月突破800美元/个。

4. 山寨币是否对比特币的生态造成威胁？

山寨币层出不穷，目前发展的比较好的山寨币有LTC（莱特币）。

5. 比特币本身机制是否存在未发现的致命漏洞？

比特币机制从目前来看似乎是“精妙绝伦、无懈可击、堪称神作”，  
但它毕竟仅存在了不到5年（09-13）。



# 比特币的技术原理

08年，一个名为“**中本聪**”的人在网络上发表了一篇论文《**比特币：一种点对点的电子现金系统**》（Bitcoin:A Peer-to-Peer Electronic Cash System）

“中本聪”是谁？“中本聪”是个匿名，无人知道其背后的真人是谁。

“中本聪”本人在完成了比特币的基本构建后就从网络上销声匿迹了，在偶尔的时候会出来冒个泡（比如有人呼吁维基解密应当接受比特币捐款时，“中本聪”说“不，不要这样。”

利用比特币进行的第一笔交易是在10年，一名用户通过发送10000枚比特币购买了一个披萨。



# 比特币的技术原理（交易）

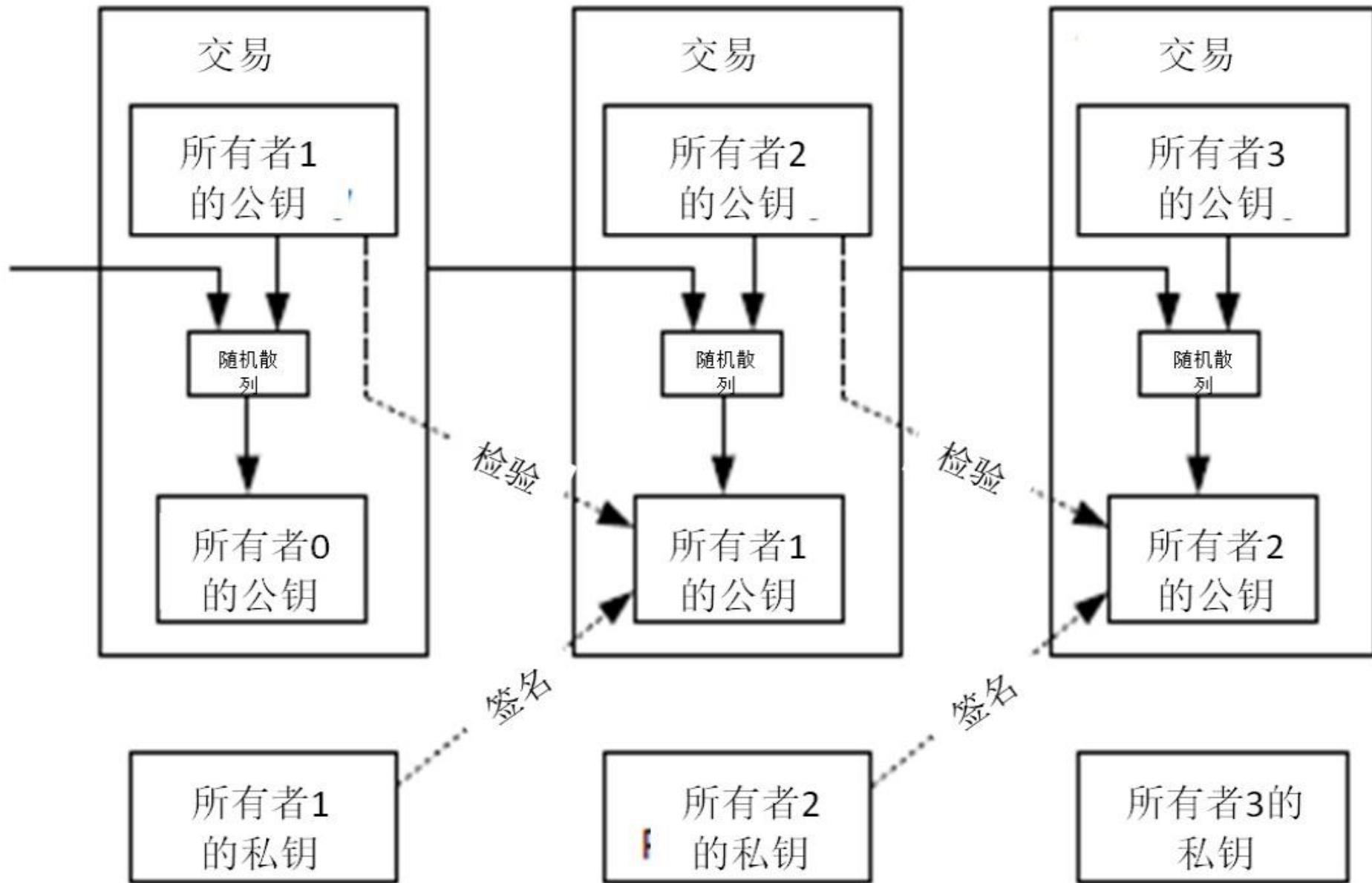
如何交易：每一位所有者（A）利用他的**私钥**对前一次交易T1和下一位所有者（B）的**公钥**（俗称：地址）签署一个随机散列的**数字签名**，A将此数据签名制作作为交易单T2并将其（交易单T2）**广播全网**，电子货币就发送给了下一位所有者。

要点：

1. 交易发起者的私钥：私钥为个人所知，他人无从知晓。
2. 前一次交易：前一次交易数据说明了该次交易的货币的来源（这部分货币是怎么到当前发起人这里来的）。
3. 下一位所有者的公钥：即交易接收方的地址，此数据说明了当前交易的目标是谁。
4. 数字签名：发起方将前一次交易数据和接收方公钥连接起来并对其求Hash值x，再利用自己的私钥对x加密，便得到了这份数字签名。



# 比特币的技术原理（交易）



# 比特币的技术原理（交易）

验证交易：

1. 利用交易T2中交易的发起方A的公钥对签名进行解密，得到整数x。
2. 将T1交易数据和B的公钥连接起来，用同样的Hash算法计算Hash值y。
3. 若 $x==y$ ，说明：
  - a. 这笔交易确实是A本人发起的，因为只有A本人的私钥才可以生成此签名（A同时也无法否认自己曾签署了此份交易）。
  - b. 交易的目的方确实是B。
  - c. 发起方确实是打算把交易T1中A获得的货币发送给B。

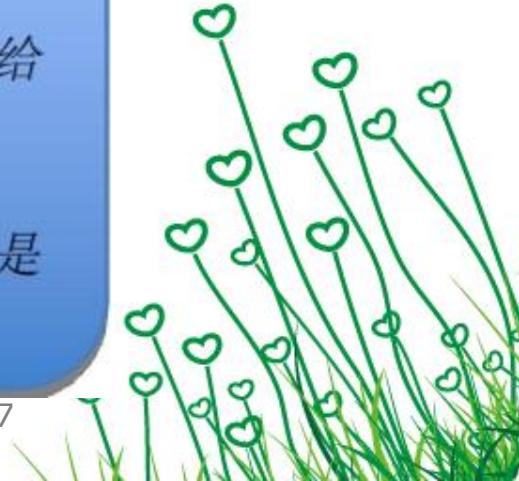


# 比特币的技术原理（交易单与Block）

交易单记录一笔交易的具体信息，比如付款人（交易发起方的公钥）、收款人（交易接收方的公钥）、付款金额（上一笔交易信息）、付款人签名（加密后的Hash值）等。

比特币虽然是电子货币，但比特币系统中并没有特定的数据结构用来单纯代表货币。本质上，比特币的存在是通过交易单来提现。通俗的来讲，现实生活中我们有实在的纸张来代表我们的货币（比如面值10块的RMB纸张代表着10块钱RMB），当我们去银行核对财务时银行也提供对账单来表示我们的货币去留。比特币的提现依托于交易单，**交易单类似于银行的对账单，其通过记录货币的去留来证明你有多少货币，而不是提供给你具体的货币单元。**

- 1 交易单 ID
- 2 资金来源——上个交易单 ID（张三的钱从哪里来的，比如王二），
- 3 王二对上一笔资金的签字（证明是王二给张三的）
- 4 资金去向——李四收款帐号，
- 5 数额——10 元，  
附加张三的签字（每个用户都能够鉴别这是张三签的 10 元交易单，不能伪造）



# 比特币的技术原理（交易单与Block）

Block(块、账簿)：记录交易单的数据单元叫做Block，一个Block上会记录很多交易单。

Block有很多份，**每个Block只记录比特币全网10分钟内的交易信息，每约10分钟产生一个新的Block。**

截止2013年11月24号10:24,全网已有27192个Block被生产出来。

当前Block数 271,192 当前难度 609,482,680

估下次难度(过 968 区块后) 685,630,899 ↑ 12.5%

全网算力(估) 5012.5TH/s

全网BTC总数 12029850 BTC



生产Block的过程，被形象的称为“挖矿”，生产工也被称为“矿工”。



# 比特币的技术原理 (Block的产生——挖矿)

Block怎么

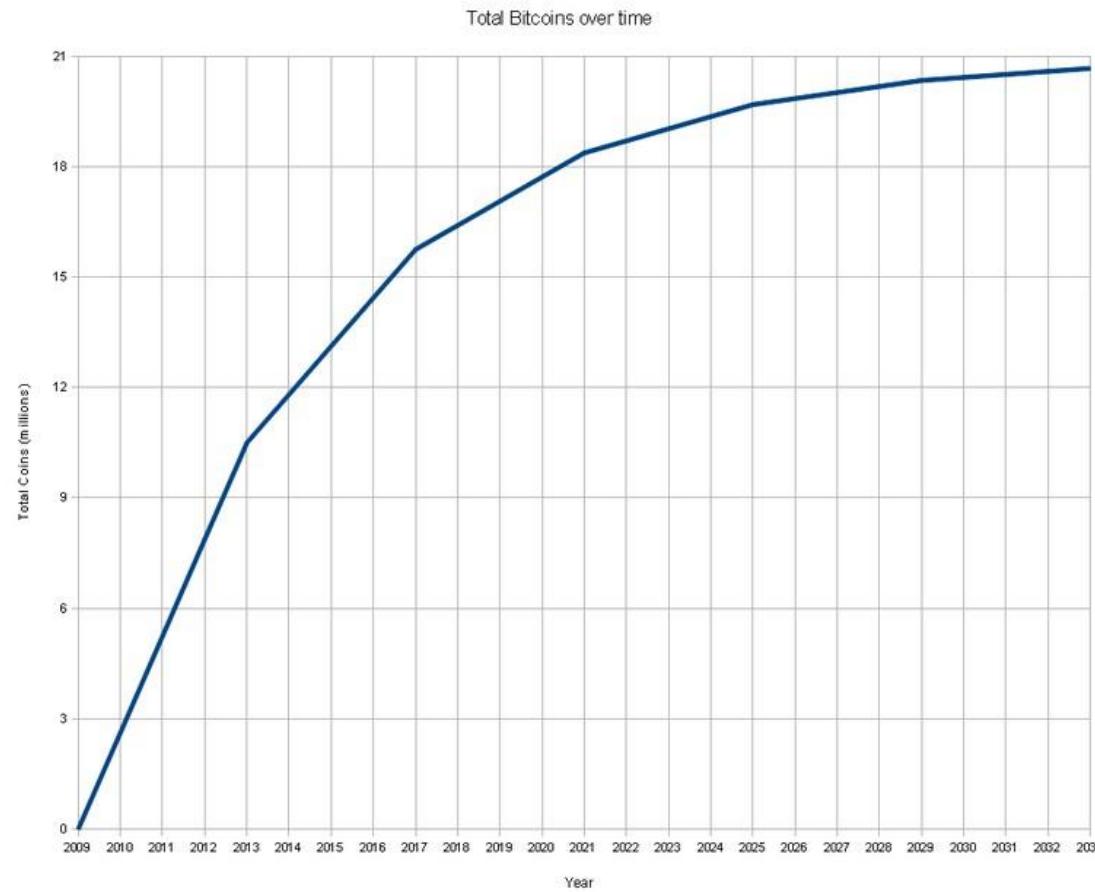
钱 (比特币)

一个

块里有

等比

比特币



最后比特币的实际可用个数应少于2100W，因为会有部分币随着拥有者的密钥丢失而永远的无法流通 (尽管记录这些币的交易单还在，但谁也无法使用它)

“  
ock者所有)

$$(1 - q^n)=0$$



# 比特币的技术原理（Block的产生——挖矿）

Block的产生细则：

全网每十分钟（算法动态调节至约十分钟产生一个）产生一个新的Block，每个新的Block含有的一一定数额的比特币归创建者所有，此规则称为“激励”。

比特币体系的设计要求：

Block应由那些最诚实最勤劳的节点产生，因而引入**工作量证明**机制。比特币体系倾向于认为：一个节点在提供信息之前付出了巨大的工作量，那么他可能是诚实的概率比较高（**他提供的Block中数据最有可能没有问题，当然无论如何其他节点也是会对其进行检查的**）。

具体产生原理：

节点尝试寻找一个随机数（又称“幸运数”），使得将最后一个Block的hash值、当前世界中尚未被加入到任何Block的交易单、随机数三部分组织起来送入SHA256算法计算出散列值X（256位），如果X满足一定条件（比如前20位均为0），那么该节点初步获得创建Block的权利。



# 比特币的技术原理（Block的产生——挖矿）

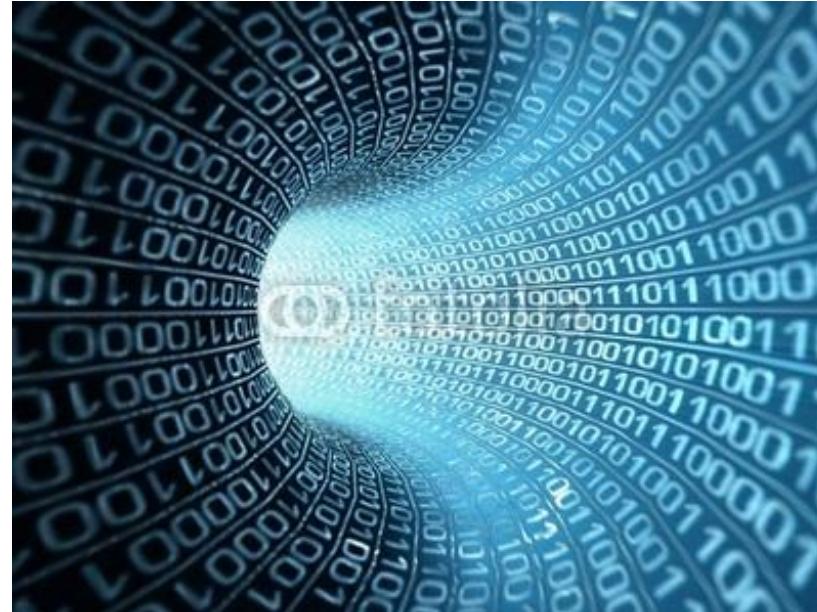
SHA256简介（密码学范畴）：

SHA256是一种求Hash值的算法，将任何一串数据输入到SHA256将得到一个256位的Hash值（散列值），相同的数据输入将得到相同的结果。

输入数据只要稍有变化（比如一个1变成了0）则将得到一个千差万别的结果，且结果无法事先预知（**雪崩效应**）。

**正向计算**（由数据计算其对应的Hash值）十分容易。

**逆向计算**（俗称“破解”，即由Hash值计算出其对应的数据）极其困难，以至于在当前科技条件下被视作不可能。



# 比特币的技术原理（Block的产生——挖矿）

**挖矿过程实际上就是反复去尝试寻找一个随机数**，该随机数加上其他数据后，SHA256算法计算它们的Hash值X，该X必须满足特定条件。

矿工为寻找该随机数而付出的劳动被看成是为生产新的Block而付出的工作量，通常需要反复尝试上亿次才能成功找到一个满足条件的随机数（小道消息：据说全世界至少有500台超级计算机被低调的拿来干这事）。



# 比特币的技术原理（Block的产生——挖矿）

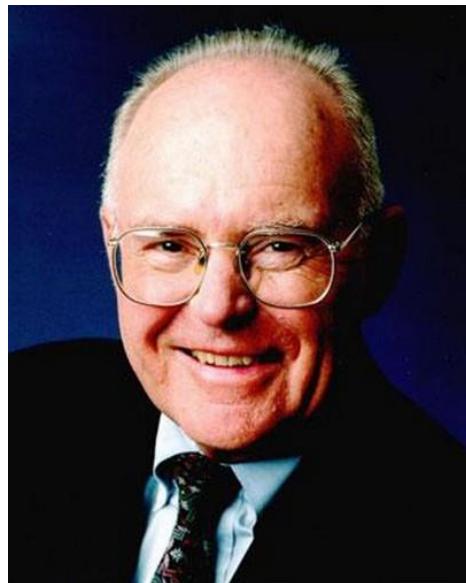
如何破解**摩尔定律**？

比特币体系要求平均10分钟才可产生新的Block，但是在计算机硬件日新月异的今天，如何做到这点？

戈登·摩尔（Intel创始人之一）指出（**摩尔定律**）：

集成电路上可容纳的电晶体数目，约每隔24个月便会增加一倍。

通俗的理解是：计算机的性能，每隔18个月会提高一倍。



摩尔



中本聪

# 比特币的技术原理（Block的产生——挖矿）

工作量证明**难度系数**:

对于每个Block存在一个难度系数，此系数可以转换为一个256位的整数，挖矿计算出的Hash值X必须小于该整数，此条件作为寻找随机数的附加条件。

当某时刻网络检测到新Block的产生速度不符合约10分钟一个时，将调解该系数（加大或者缩小），从而使下一个Block的产生速度符合预期。

全网每2周检测一次Block产生速度并依此对难度系数进行调节  
使得Block产生速度符合预期。

每个Block会记录其本身产生时的难度系数数值，因此每个节点  
都可以根据历史Block计算出当前的难度系数。



# 比特币的技术原理 (Block的组织方式:Block链)

Block链:

所有的Block以双向链表的方式链接起来，且每个Block都会保存其上一个Block的Hash值（这样Block之间的顺序一旦确定就无法更改）。只有一个Block无上一节点，即：创世Block（第一个Block）。

Block链全网唯一，每个节点都有相同的备份。Block链一旦有更新则全网通知。



# 比特币的技术原理（Block链的那些事儿）

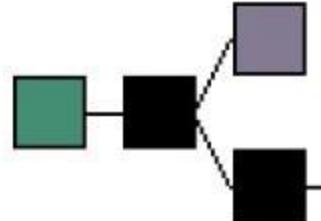
Block链的更新：

每当节点（矿工）计算出了一个符合条件的随机数时，**它仅仅获得了创建临时Block的权利**，它立即将相关数据打包好作为一个临时Block并广播全网。

每10分钟内全网不止一个节点能计算出幸运数字，即十分钟内会有多个节点在网络中广播它们各自打包好的临时Block（都是合法的）。通过谁先计算出谁后计算出来决定接受谁的临时Block转正显然很难做到，因为所有节点的时间不可能严格一致（而且可以任意被调节），而且网络传输有快有慢。

Block链分支：

某一节点若收到多个针对同一前续Block的后续临时Block，则该节点会在本地Block链上建立分支，多个临时Block对应多个分支。



# 比特币的技术原理（Block链的那些事儿）

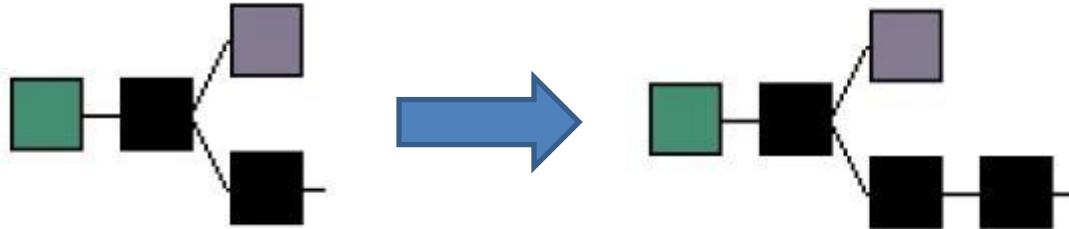
全网唯一的Block链是那支付出最大计算力的分支，也即**最长分支**。

节点总在它认为最有可能成为最长分支的分支上继续工作（否则一旦当前工作的分支被其他分支淘汰，那么当前做的计算工作会前功尽弃）。

节点按照以下原则决定在哪条分支（**最大期望分支**）上继续工作：

1. 不同高度的分支，总是接受最高的分支。
2. 相同高度，接受难度最大的。
3. 否则接受先收到的。

每当Block链高度增加，则重新选取最大期望分支（以分支的实际增长速度为准），当某分支的高度稳定的高于其他分支时，其他分支将会被网络彻底抛弃。



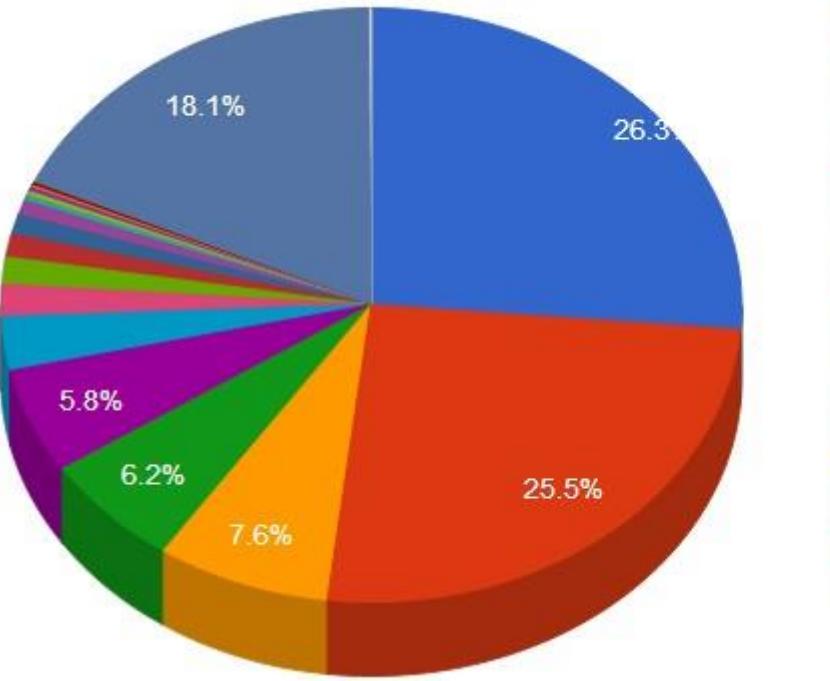
# 比特币的技术原理（Block链延伸）

按照上述  
则工作（

**分支博弈**

有利的分  
个节点而  
么必然导  
成为最长

的风险将  
该分支最



- BTC Guild
- GHash.IO
- Eligius
- slush - mining.bitcoin.cz
- Bitminter
- Eclipse Mining pool
- Discus Fish
- private pool
- p2pool
- ASICMiner
- Horrible Horrendous Terrible Tremendous Mining Pool
- Bitparking Merged Mining Pool
- Polmine
- ozcoin
- btcmp.com
- Give-Me-Coins
- Unknown
- Other

按照上述原

死守对自己的  
的。对于某  
抛弃），那  
使得该节点

们受益归零  
分支上工作，

## 实际算力分布



# 比特币的技术原理（安全体系）

## 二重支付（简单）：

二重支付即指攻击者几乎同时将同一笔钱用作不同交易。如A将50个币发送给B然后广播“A将50币发送给B”，几乎于此同时A又将这50个币发送给C然后广播“A将50币发送给C”。

比特币体系中由于各节点地位平等，不存在“中心节点”对交易单进行审核。因此无法通过审核先后顺序的方式来杜绝二重支付。

## 防御：

比特币世界从诞生到现在所有的交易记录都已交易单的形式存储在全网唯一的Block链中，每当节点在把新收到的交易单加入Block之前，会顺着交易的发起方其的公钥向前进遍历检查，检查当前交易所用的币是否确实属于当前交易发起方，此检查可遍历到该币的最初诞生点（即产生它的那块Block源）。虽然多份交易单可以任意序的广播，但是它们最终被加入Block时必定呈现一定的顺序。Block之间以Hash值作为时间戳则Block，这决定了任意一笔交易资金来源都可以被确定的回溯。



# 比特币的技术原理（安全体系）

## 二重支付（复杂）：

考虑如下一种情况，假设现在block高度为100，攻击者给商户发了一个交易10BTC，记作交易A，通常这笔交易会被收录进高度101的block中，当商户在101块中看到这笔交易后，就把货物给了攻击者。此时，攻击者便开始构造另一个高度为101的block，但用交易B替换了交易A，交易B中的输入是同一笔，使得发给商户的那笔钱发给他自己。同时，攻击者努力计算block，使得他的分支能够赶上并超过主分支，如果最终大家接受其分支为主干分支，这笔钱就成功的完成双重支付。

## 防御：

一个交易单要想被最终确认，首先需要被放入一个新成功创建的Block。再等待该Block的后续数个（一般是5个）Block被成功创建后，该交易才会被最终确定安全通过，即交易成功。

比特币世界Block链被增加6个后，Block链被修改的可能性机会降为0.

攻击者必须在10分钟内连续创建出6个合法Block才有可能将原链替换，这意味着攻击者在10分钟内产生的算力需超过比特币世界其他所有节点在60分钟内算力的总和。



# 比特币的技术原理（安全体系）

## 交易不可逆性：

比特币的交易体系决定了比特币世界里，任何一笔交易都不可逆，数据不可回滚。

## 交易双方匿名性：

交易所需提供的仅仅是交易双方的公钥（一个256位的整数），交易双方互相不知道对方是谁（当然，现实生活中商量好的除外）。

## 公钥与私钥资源的广阔性：

任意一个比特币世界用户可以在每次交易都生成一个新地址使得通过地址追踪拥有者更加困难，比特币钱包会自动代你管理好这些地址以确保所有地址中的财产都属于你。

### 交易（最新的最前）

0bab54090e0510e34543e78f5bd18cb82c12d17ba051f2ccb9aa97c3025170e9

1PbZLg75tWfG36R7t9UhH9vSnKzcCj1JLy



1NHpLeG6WRs5Zt4aho7EGYPN2GjCNbpA3V

# 比特币的技术原理（行情）



MT.GOX (外盘、日本) 的价格走势



# 比特币的技术原理（数据分析）



## 土豪持币走势

随着价格走高，比特币资源越呈聚集于少数人态势

# 比特币的技术原理（危机）

## 比特币悖论：

比特币的根本价值在于其货币属性（有成为世界货币的可能），因为比特币引发了投机者的狂热购买。

比特币价格的剧烈动荡及部分人对比特币的囤积（投机与投资），导致比特币逐渐失去交易支付功能，从而丧失货币属性。

一旦比特币丧失其货币属性，比特币将一文不值。



# 比特币的技术原理（商机）

1. 可对接各大交易平台的本地交易助手，具备特定条件触发委托、自动搬砖、行情预警、数据分析等功能。
2. 正规高效的交易平台。
3. 挖矿机的生产及代理。

