

比特币工作原理浅析

-- 张娟摘录于网上



比特币受到各方的关注

监管派

中国：不是货币不能线下流通

法国：有金融风险非可信任投资

赞成派

美国：承认比特币合法暂不监管

德国：作为记账单位可用于缴税

沉默派

爱尔兰：推出比特币价差期权

印度：继续持袖手旁观的态度

内容概要

1

比特币概念

2

交易方式

3

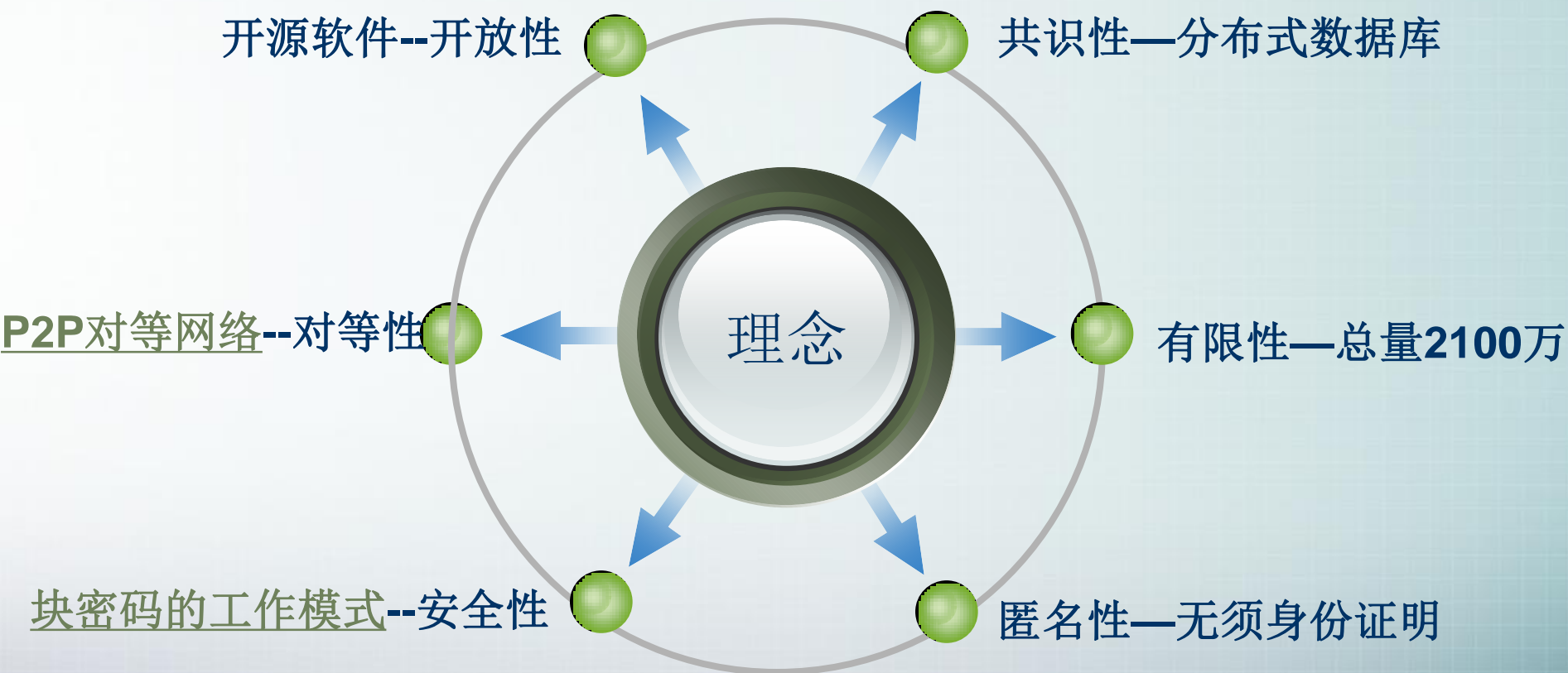
工作原理

4

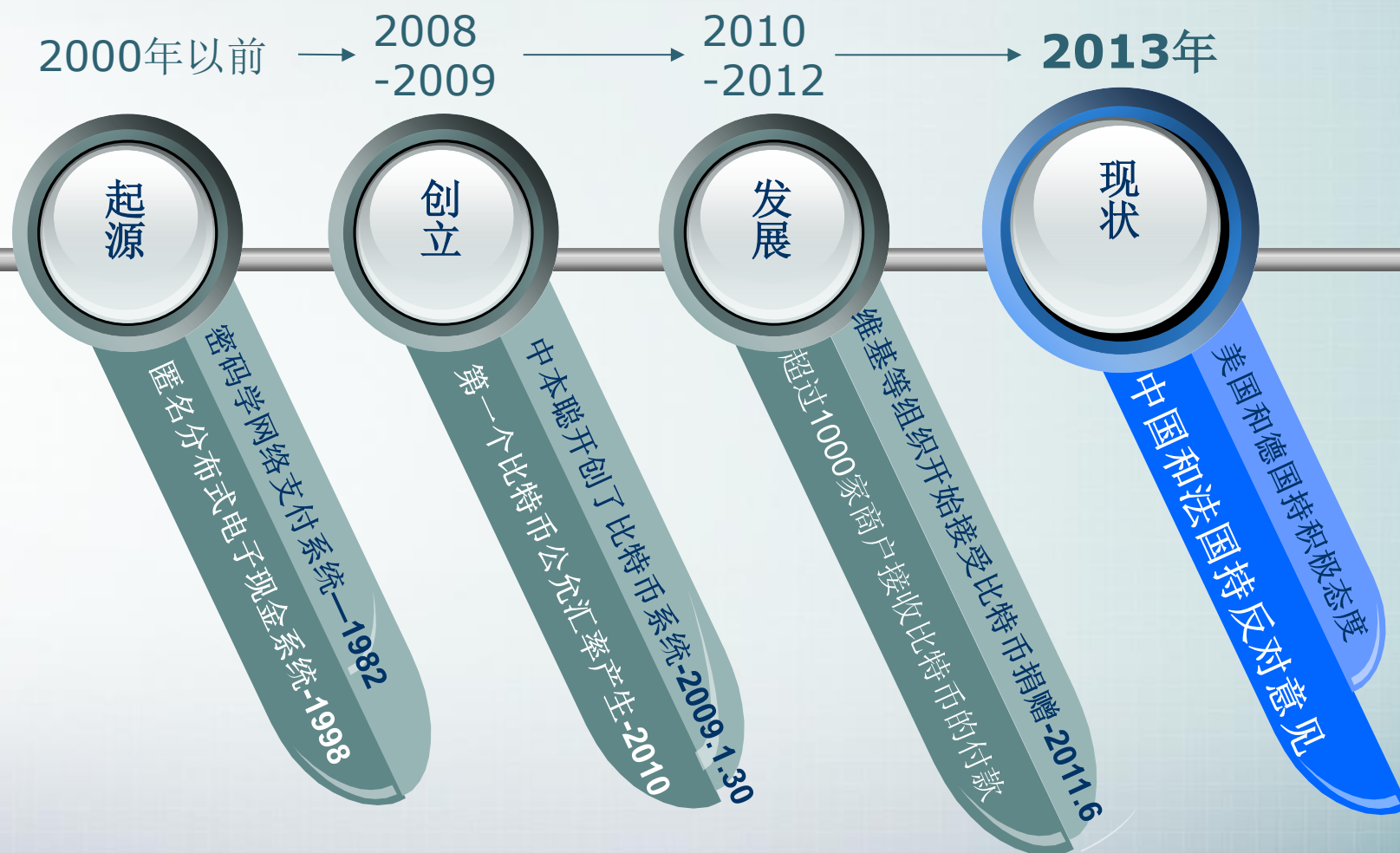
争议焦点

比特币概念

比特币是用户自治的、全球通用的加密电子货币，2008年由中本聪提出



比特币的发展历史及现状



与传统电子货币的差异

比特币	传统电子货币
去中心化	需要中心服务商
匿名的	实名的
存量有限、不能随意增发	可以无限增发
代码开放	封闭的
价值来源于用户逐步增多	法币背书

内容概要

1

比特币概念

2

交易方式

3

工作原理

4

争议焦点

交易方式

比特币的交易方式与传统电子货币十分类似。首先都需去相关网站下载客户端：

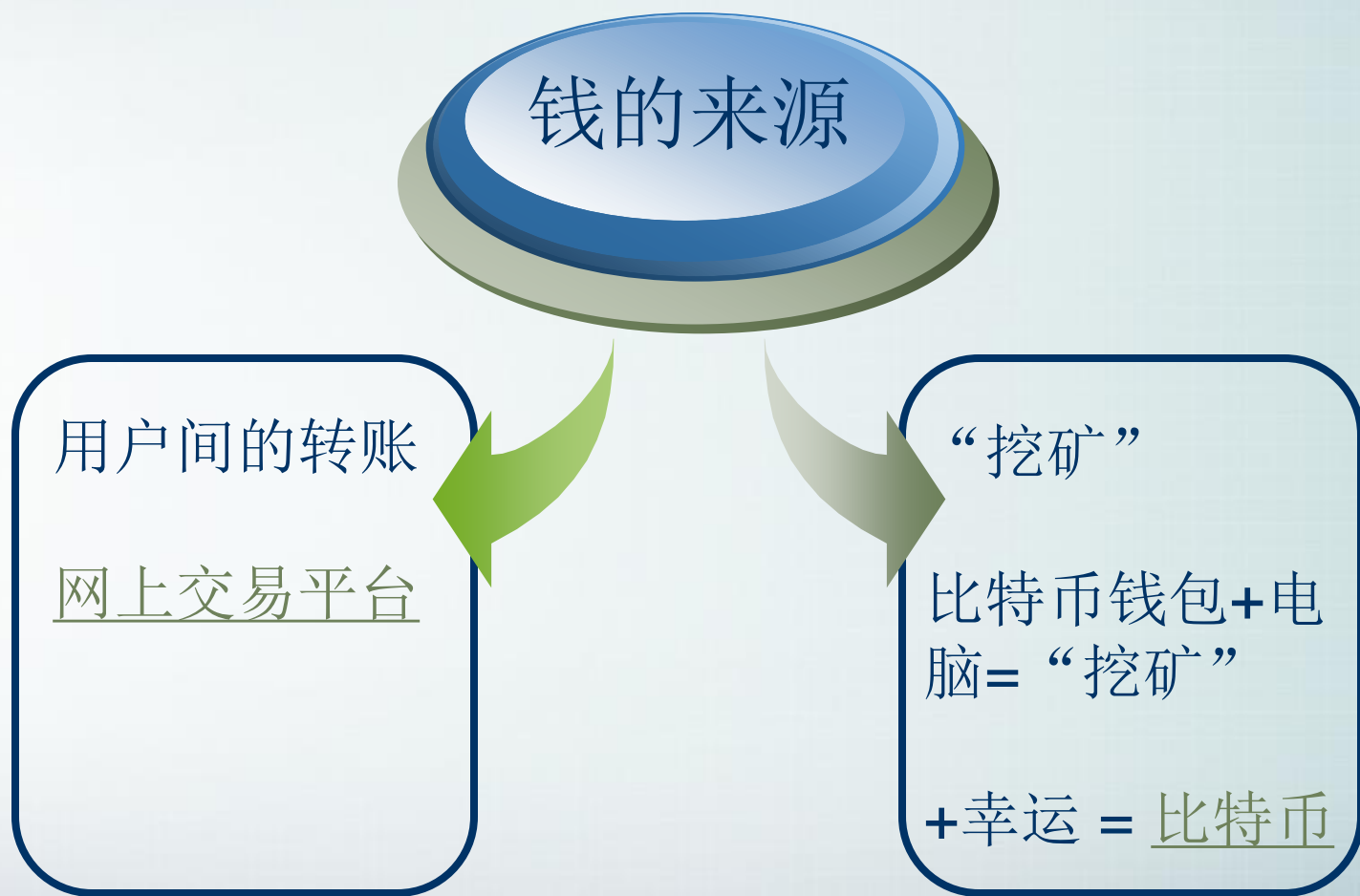
用户端名称	网址	许可协议
Multibit (云数据区块功能)	http://multibit.org/	MIT
Bitcoin-Qt (中本聪用户端)	http://sourceforge.net/projects/bitcoin/	MIT
My Wallet (在线钱包, 独立式)	https://blockchain.info/wallet	专有软件
Coinbase (在线钱包, 混合式)	http://coinbase.com	专有软件
Electrum	http://electrum.ecdsa.org/	GPL
Armory (具有离线储存功能)	http://bitcoinarmory.com	AGPL

比特币钱包 → 电子银行的客户端

比特币地址 → 银行卡号

比特币密钥 → 银行卡密码

交易方式



交易方式

交易确认—交易记录的保存

对于传统的电子货币，交易记录保存在银行中，但是由于比特币是去中心化的，所以需要所有用户共同维护一个全球统一的交易记录，并将数据储存在每个客户端中。

如何维护一个全球统一的交易记录呢？

1

将每笔未保存的交易记录串联起来，并用块密码工作模式加密

2

将交易记录打包加密，“挖矿”，系统每十分钟会选出一个幸运的“矿工”

3

将此幸运矿工打包加密的数据放入全球统一的数据链中，所有客户端实时更新数据，返回1

内容概要

1

比特币概念

2

交易方式

3

工作原理

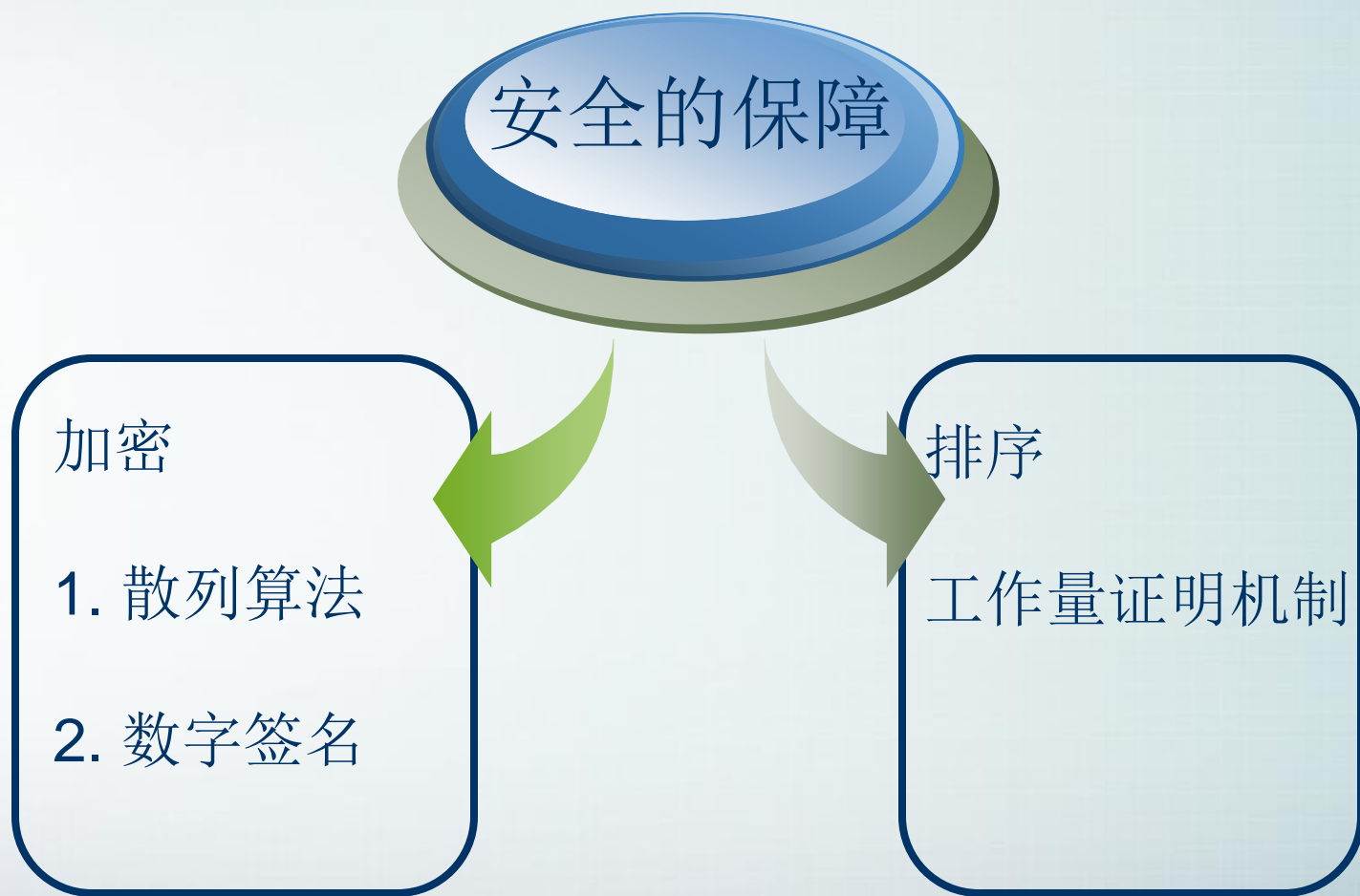
4

争议焦点

工作原理

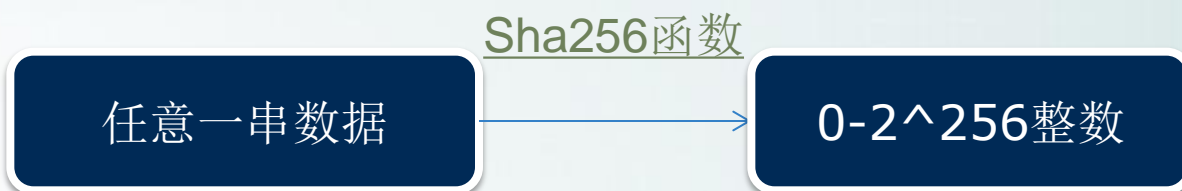


工作原理



工作原理

Sha256散列算法



- ◆ 不可逆性
- ◆ 相同数据结果相同，不同数据结果不同

工作原理

数字签名—非对称加密算法

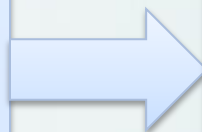
假设有三个交易单，代表用户1给用户2支付钱款“交易单1”，用户2给用户3支付钱款“交易单2”，用户3给用户4支付钱款“交易单3”。



工作原理

交易单签名过程

- 1.收款人的公钥
- 2.上一交易单数据
- 3.利用1和2的数据得出散列值 x
- 4.付款人私钥对 x 加密，得到付款人签名
- 5.将付款人签名附加在交易单中，发给收款人



交易单验证过程

- 1.付款人A的公钥，用于解密A的私钥
- 2.解密付款人的签名，获得散列值 x
- 3.收款人利用自己的公钥和上一交易单的数据，得到另一个散列值 y
- 4.如果 $x=y$ ，交易单有效

工作原理

- ◆ 全世界所有用户可以简单的对任何交易单进行验证
- ◆ 签字不仅与一张交易单相关，还跟和这笔钱相关的所有交易内容相关
- ◆ 一个用户，用同样的私钥签署不同的内容的交易单，签名也会不同



工作原理—建立全世界统一的交易记录

诚实节点

由于交易单是全网络广播。每个用户都可以得到所有交易单。其实，只要一个诚实的用户，根据接收到交易单的次序，创建的交易单记录，就可以给大家作为全局统一的账簿。

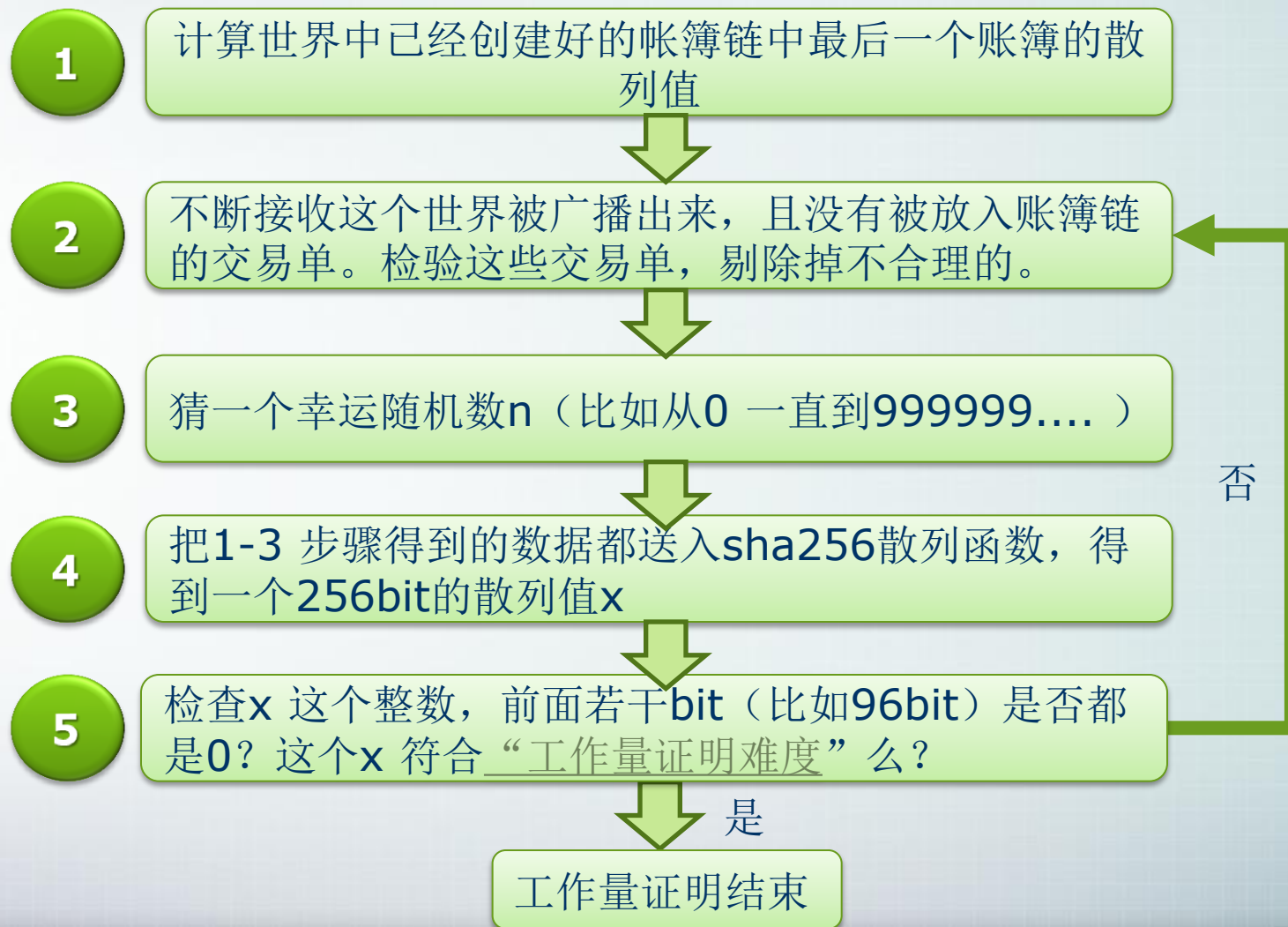
工作量证明

一个用户节点如果要试图创建一个被全网认可的新账簿（挖矿节点），要花很大力气做一些毫无意义的运算（挖矿）。运算结果可以被所有人容易的证明他确实做了这些工作。

运算

这里运算是散列值计算过程，并且计算结果要满足一些苛刻的条件。因此计算通常要重复上亿次，这种运算也称为“挖矿”

工作原理—建立全世界统一的交易记录



工作原理—建立全世界统一的交易记录

6

工作量证明结束，创建临时账簿，打包广播



7

世界中所有节点检测重复支付



8

帐簿链分支判断，最终创建账簿

全网账簿创建速度控制，平均每十分钟一个

工作原理一总结

- 非对称加密保证无法伪造别人支付给作弊者的交易单
- 工作量证明机制，保证数量占优的诚实节点产生的统一交易记录内容与次序真实
- 散列函数保证创建合法账簿极难，检验账簿合法性极其容易
- 时间戳保证交易顺序，无法修改账簿链
- 所有网络用户监督交易，保存全局统一交易记录备份

内容概要

1

比特币概念

2

交易方式

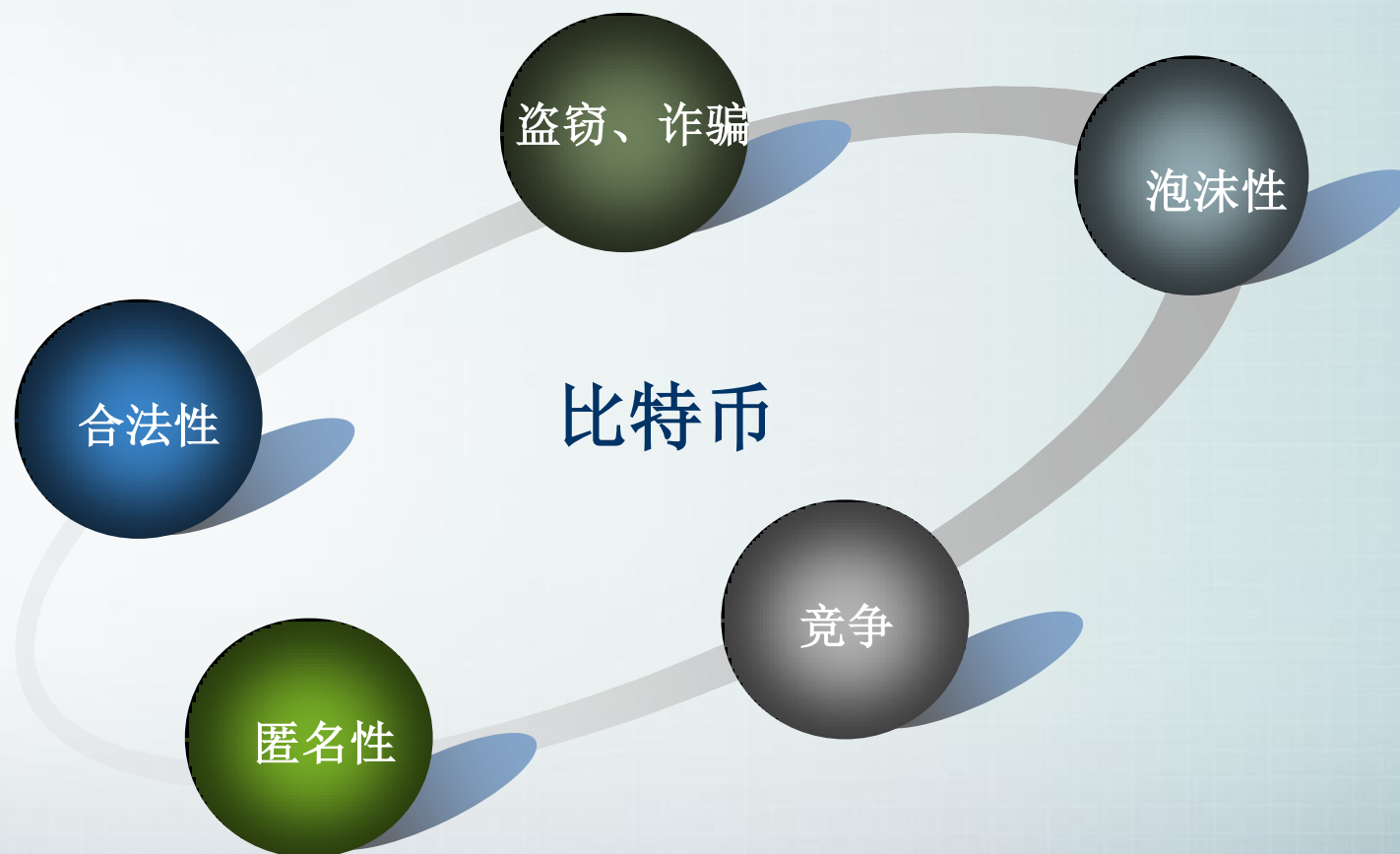
3

工作原理

4

争议焦点

争议



争议—盗窃和诈骗

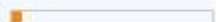
时间	事件
2011.6.19	Mt.Gox比特币交易中心的安全漏洞导致1比特币价格一度跌至1美分，原因是一个黑客从感染木马的电脑上盗用了该用户MtGox的证书。
2011.7	世界第三大比特币交易中心Bitomat的运营商宣布：记录着17,000比特币（约合22万美元）的wallet.dat文件的访问权限丢失。
2011.8	作为常用比特币交易的处理中心之一的MyBitcoin宣布遭到黑客攻击，并导致关机。涉及客户存款的49%，超过78000比特币（当时约相当于80万美元）下落不明。
2012.8	Bitcoinica在旧金山法院被起诉要求赔偿约46万美元。2012年，Bitcoinica两度遭到黑客攻击，被指控忽略客户资金的安全性以及伪造提款申请。
2012.9	Bitfloor交易中心也被黑客入侵，24,000比特币（约相当于25万美元）被盗。Bitfloor因此暂停运营。
2013.11	网络钱包服务商inputs.io被两个黑客入侵，盗走4100比特币，目前仅1比特币以上的账户可获得赔偿。

争议—盗窃和诈骗

最近在一个欧洲交易的银行因特网网上付款系统中就有100万比特币被盗；中国一家比特币交易公司GBL在10月份突然消失，410万的存款也不翼而飞。

比特币交易平台GBL诈骗案告破 负责人落网

作者：朱丽珍 发布：周勇 2013年12月3日14:01 来源：钱江晚报 我要评论 (1) 访问次数 2313

本文分数  1 | [+分](#) [-分](#)

在开始介绍这个案子之前，先给大家普及一下：什么是比特币？

简单地说，比特币与Q币、游戏币一样，诞生于互联网虚拟世界，比特币没有发行机构，而且它的总量是固定的，总共只有2100万个。

从今年上半年开始，炒比特币的风头相当猛烈，一个比特币，已经涨到5000多元人民币，而且还在持续疯涨中。为什么要炒比特币？因为按照比特币的价值理论，它的总量固定，用的人多了，单个的比特币的价值自然就上去了。

先别忙着眼热，得到比特币，也不是一件容易的事。

目前，人们可以通过两种方式得到比特币：一是自己生产，二是通过交易平台买卖。前者越来越难，后者是市场行为，存在很大风险。

前段时间，东阳人老乔在国内一知名比特币交易平台炒比特币，4天时间9万元被骗个精光。根据老乔这条线索，东阳警方介入侦查，发现这家交易网站其实是个骗子网站。

由此，国内首起比特币交易平台诈骗案告破，网站几名主要负责人也先后落网。

争议一匿名性

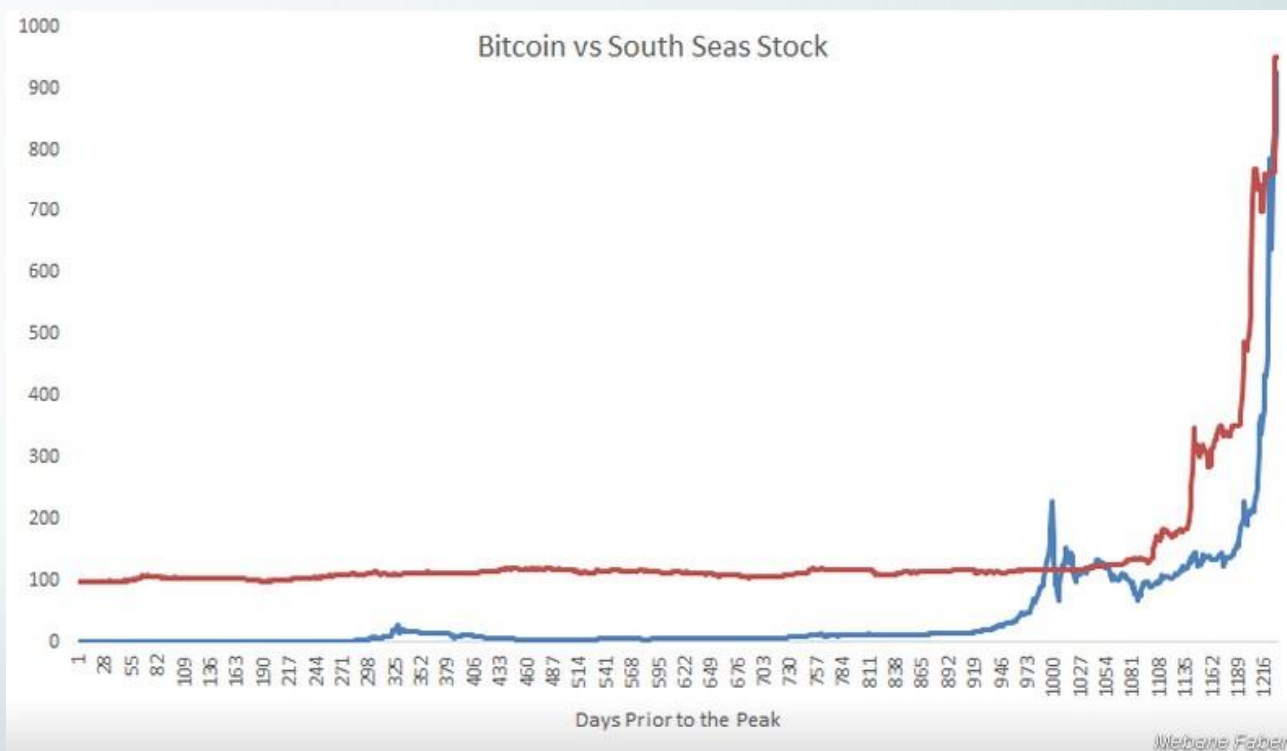
丝绸之路是一个匿名化的交易网站，自称为黑市亚马逊Amazon.com，比特币是它的唯一交易货币。2011年，纽约州参议员Charles Schumer和其他人致信给美国药品管理局，指责丝绸之路运用比特币洗钱，要求对丝绸之路和比特币展开调查。比特币虽是合法技术，被用在丝绸之路的网站中，为执法部门带来了很多难题。不过，开发比特币的核心成员Jeff Garzik表示，虽然各方的身份是匿名的，执法部门仍可以利用先进的网络分析技术，通过区块链中公开的交易记录流程来跟踪单个比特币用户。

此外，由于比特币的匿名性和无国度性，受到了自由主义者、黄金投资商、中国富豪甚至毒梟们的青睐。因此比特币作为一种和货币高度类似的商品，在反洗钱和纳税方面仍需各国政府的监管

争议一泡沫性

由于中国投资商大量在海外囤钱，比特币价格陡升，看起来很像经典的货币泡沫。

比特币与南海泡沫的比较



谢谢大家!

后面是附录，主要是对前面一些概念，例如交易单、散列函数、快密码工作模式等的解释

比特币总量



- ◆ 平均每十分钟，系统为“挖矿”的幸运儿发放一定数量的比特币
- ◆ 开始，平均每十分钟发放**50**个比特币，每四年减少一半，即**25**个比特币，以此类推，最终比特币的总发行量为**2100**万个。

算法如下：

开始四年发放的比特币数量为 $50 \times 6 \times 24 \times 365 \times 4 = 2628000$ 个

接下来四年发放的比特币数量为 2628000×0.5 个

再接下来四年发放的比特币数量为 2628000×0.5^2 个

.....

运用等比数列，算出比特币发行总量约为**2100**万个

网上有很多的“挖矿教程”，

<http://ishare.iask.sina.com.cn/f/37259630.html>

网上交易平台



火币网—中国最专业的比特币交易平台—现货交易



2011年6月，比特币的汇率约15美元，即100人民币

比特币发展历史及现状

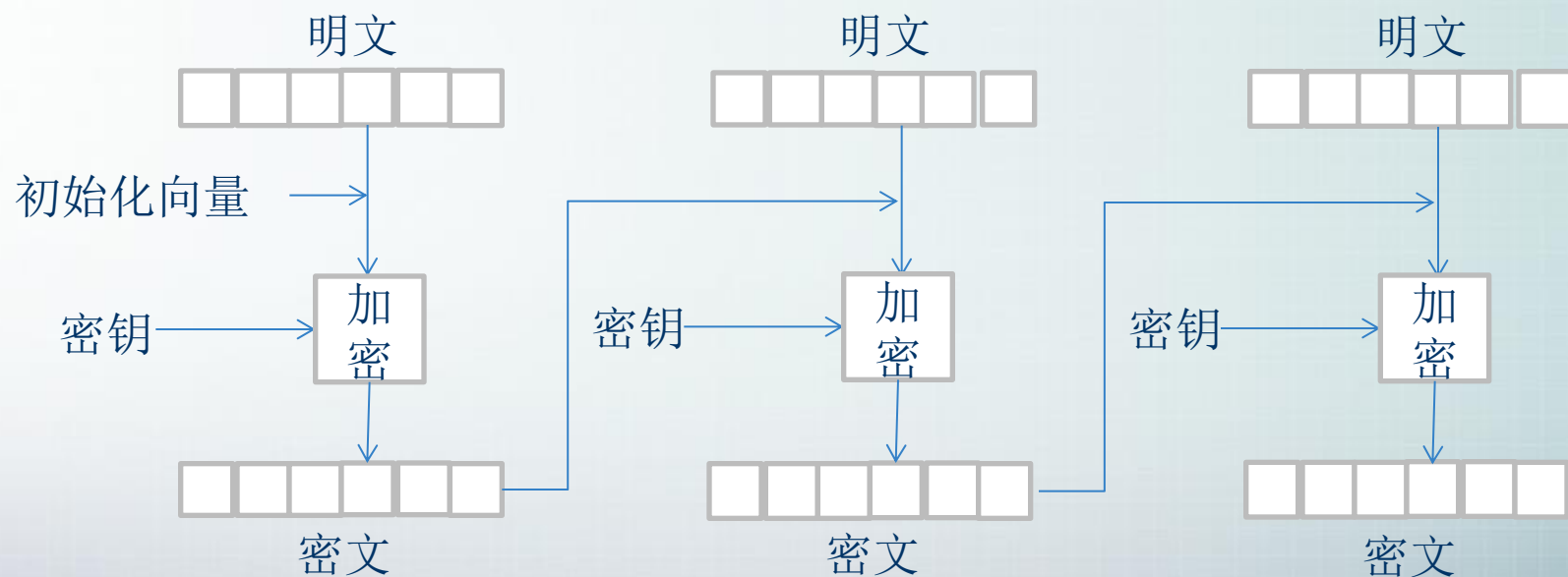


时间	事件
1982	David Chaum最早提出了不可追踪的密码学网络支付系统。
1990	Chaum将他的想法扩展为最初的密码学匿名现金系统
1998	Wei Dai发表文章阐述了一种匿名的、分布式的电子现金系统，他将其命名为“b-money”
2009.1.3	中本聪开创了比特币P2P开源用户群节点和散列函数系统，从此，其对等网络和它的第一个区块链开始运行，他发行了有史以来的50个比特币。
2010	在比特币论坛上，用户群自发交易中，产生了第一个比特币公允汇率。
2011.6	维基解密、自由网、Singularity Institute、互联网档案馆、自由软件基金会以及其他的一些组织，开始接受比特币的捐赠。
2012.10	BitPay发布报告说，超过1000家商户通过他们的支付系统来接收比特币的付款。

块密码的工作模式



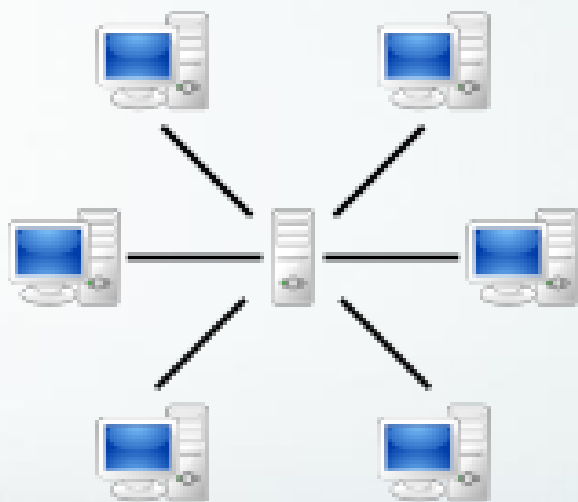
- ◆ 密码学中，块密码的工作模式允许使用同一个块密码密钥对多于一块的数据进行加密，并通过初始化向量的方法保证其安全性。
- ◆ 初始化向量，用于随机化加密一块数据，因此相同的明文，相同的密钥可以产生不同的密文。对应于比特币电子系统，同一用户使用同样的密码和交易也可以产生不同的加密的交易记录。



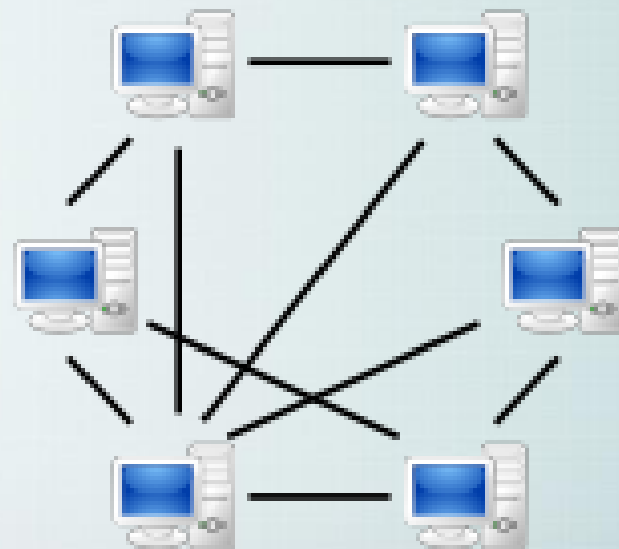
P2P对等网络



对等网络（peer-to-peer，简称P2P），又称点对点技术，是无中心服务器、依靠用户群（peers）交换信息的互联网体系。与有中心服务器的中央网络系统不同，对等网络的每个用户端既是一个节点，也有服务器的功能，任何一个节点无法直接找到其他节点，必须依靠其户群进行信息交流。



有中心服务器的中央网络系统



无中心服务器的对等网络系统

交易单示例



1. 交易单ID
2. 资金来源—上一交易单ID
3. 上一交易单付款人签字
4. 资金去向—收款人地址
5. 付款金额
6. 付款人签字—用于全世界鉴别，不能伪造（签字由付款人密钥、收款人公钥和上一交易单签字加密得来）

账簿示例



账簿ID

交易单 1

交易单 2

交易单 3

.....

交易单 n

上一账簿ID

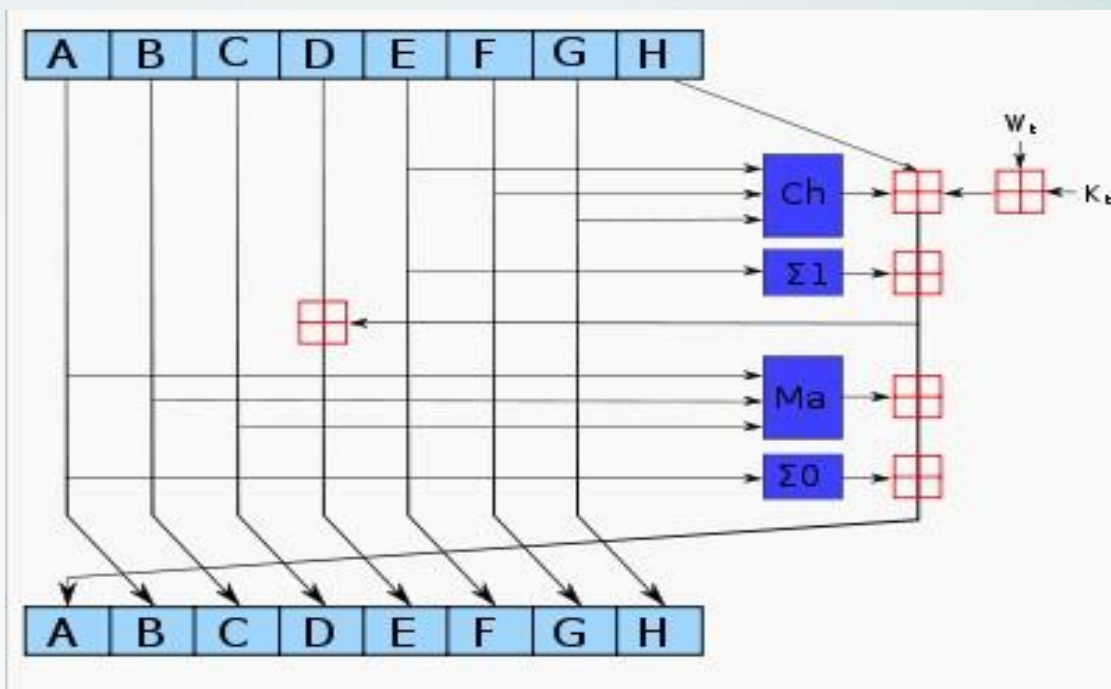
下一账簿ID

其他信息

账簿链示例



散列函数示例



SHA-2的第 t 个加密循环。图中的深蓝色方块是事先定义好的非线性函数。ABCDEFGH一开始分别是八个初始值， K_t 是第 t 个密钥， W_t 是本区块产生第 t 个word。原信息被切成固定长度的区块，对每一个区块，产生 n 个word（ n 视算法而定），通过重复运作循环 n 次对ABCDEFGH这八个工作区段循环加密。最后一次循环所产生的八段字符串合起来即是此区块对应到的散列字符串。若原信息包含数个区块，则最后还要将这些区块产生的散列字符串加以混合才能产生最后的散列字符串。

工作量证明难度



“工作量证明难度”：有一个本地难度标准。这个标准是一个浮点数，可以换算为一个256bit的整数。算出的sha256散列值x必须小于这个难度数字。

“工作量证明难度”随着电脑速度而变化，电脑速度越快，工作量证明难度越大，电脑计算出幸运随机数的速度变慢。因此通过调整“工作量证明难度”，可以控制账簿创建的速度。

临时账簿



账簿ID

初始比特币奖励交易单

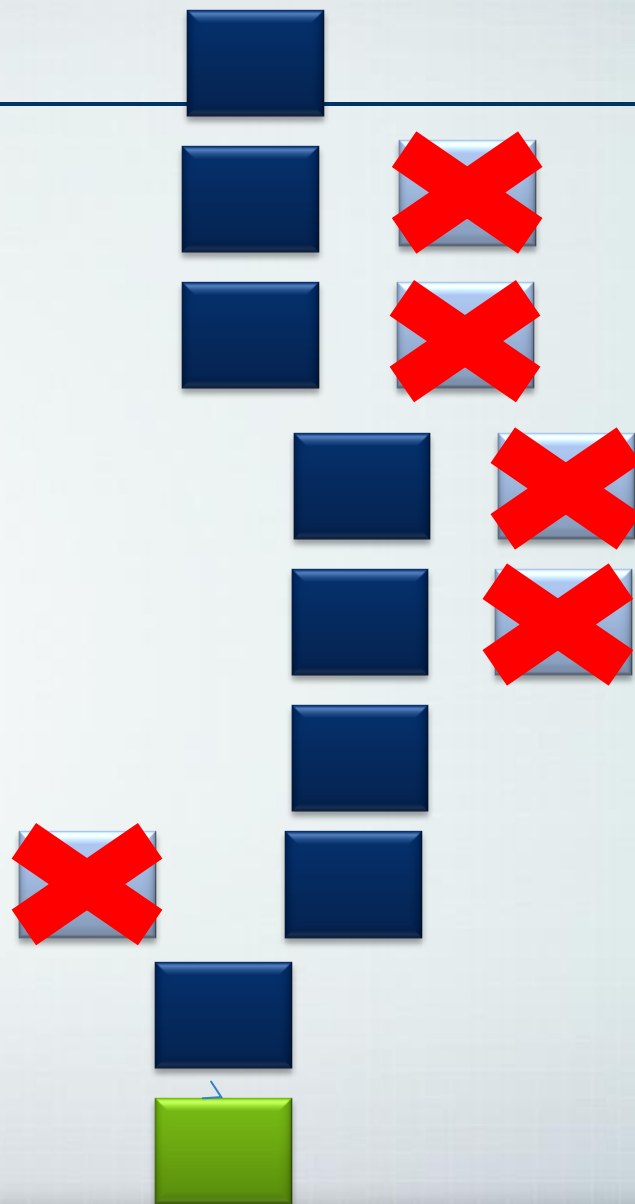
创建这个账簿过程中收到的交易单数据

上一个账簿的散列数据

幸运随机数

上一账簿ID

帐簿链分支判断



南海泡沫事件



南海泡沫事件（**South Sea Bubble**）是英国在**1720**年春天到秋天之间发生的一次经济泡沫，它与密西西比泡沫事件及郁金香狂热并称欧洲早期的三大经济泡沫，经济泡沫一语即源于南海泡沫事件。

事件起因源于南海公司（**South Sea Company**），南海公司在**1711**年西班牙王位继承战争仍然进行时创立，它表面上是一间专营英国与南美洲等地贸易的特许公司，但实际上是一所协助政府融资的私人机构，分担政府因战争而欠下的债务。南海公司在夸大业务前景及进行舞弊的情况下被外界看好，到**1720**年，南海公司更透过贿赂政府，向国会推出以南海股票换取国债的计划，促使南海公司股票大受追捧，股价由原本**1720**年年初约**120**英镑急升至同年**7**月的**1,000**英镑以上，全民疯狂炒股。

比特币价差期权



- ◆ 爱尔兰一家预测市场 **Predictious** 在今年12月份宣布推出新类型的衍生品合约——比特币价差期权。

- ◆ 看涨的投资者可以通过垂直价差获利，同时限制价格暴跌的风险；看跌的投资者可以通过用这种衍生品做空比特币。

- ◆ 除了比特币交易者，开采比特币的矿工也可以利用比特币的价差期权套期保值，降低投资开采硬件的相关风险

Bitcoin price to reach \$1400 before end of December 2013



Information

Trade

Market Depth

Sell at

0.55

Buy at

3.49

23 days left for trading this contract.

Trading start	Tuesday, November 19, 2013 10:00:00 PM GMT
Trading end	Tuesday, December 31, 2013 11:55:00 PM GMT
Event date	Wednesday, January 1, 2014 12:00:00 AM GMT
Event	Bitcoin all time high 2013
Long shares	Long shares will be resolved at m\$ 10.00 if this statement occurs, m\$ 0.00 if it doesn't.
Short shares	Short shares will be resolved at m\$ 0.00 if this statement occurs, m\$ 10.00 if it doesn't.

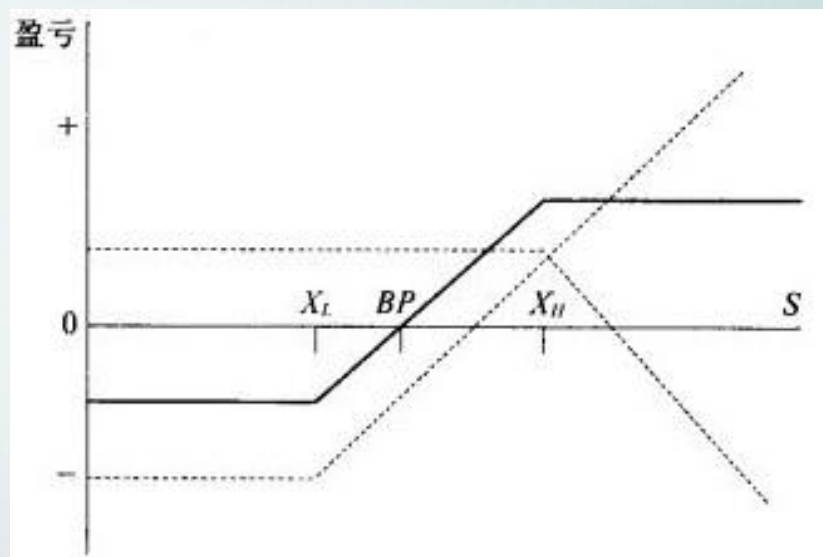
Price History



垂直价差



- ◆ 垂直价差是指投资者买入一个期权，而同时卖出另一个期权，这两个期权有着相同的标的物、相同的到期日，不同的执行价格
- ◆ 基本的垂直价差可分为四种具体的策略，即“牛市看涨期权价差”、“牛市看跌期权价差”、“熊市看涨期权价差”、“熊市看跌期权价差”。
- ◆ 牛市看涨期权价差是指投资者在买进一个执行价格较低的看涨期权的同时，卖出一个标的物、到期日相同，但执行价格较高的看涨期权





谢谢大家！

■ 大连商品交易所—张娟摘录于网上