www.qconferences.com
www.qconbeijing.com
www.qconshanghai.com

伦敦 | 北京 | 东京 | 纽约 | 圣保罗 | 上海 | 旧金山

London · Beijing · Tokyo · New York · Sao Paulo · Shanghai · San Francisco

QCon全球软件开发大会

International Software Development Conference

www.infoq.com/cn

InfoQueue

@InfoQ

infoqchina

软件
正在改变世界！

比特币带来了什么？

主讲人：张寿松 BtcTrade创始人

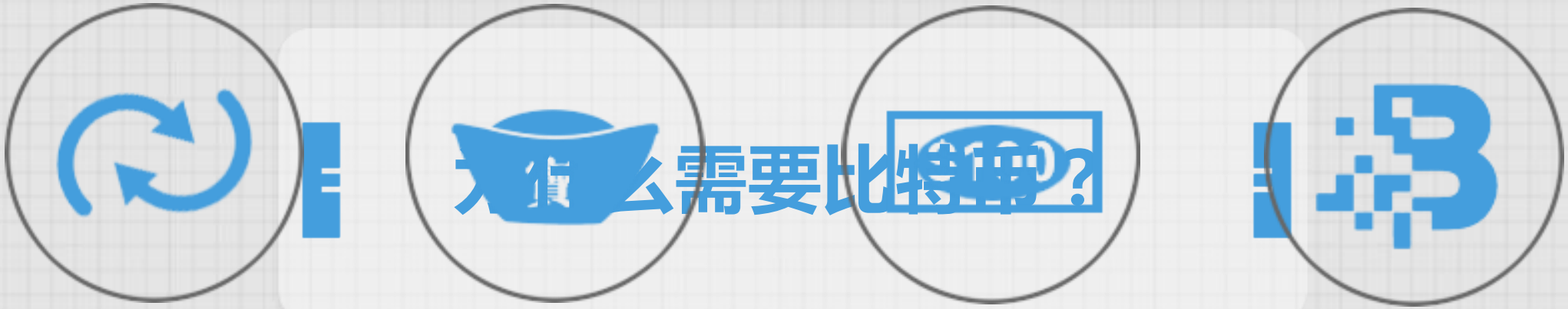
关于比特币的问题

比特币是不是货币？

比特币是不是传销？

比特币能不能赚钱？

【一】为什么需要比特币



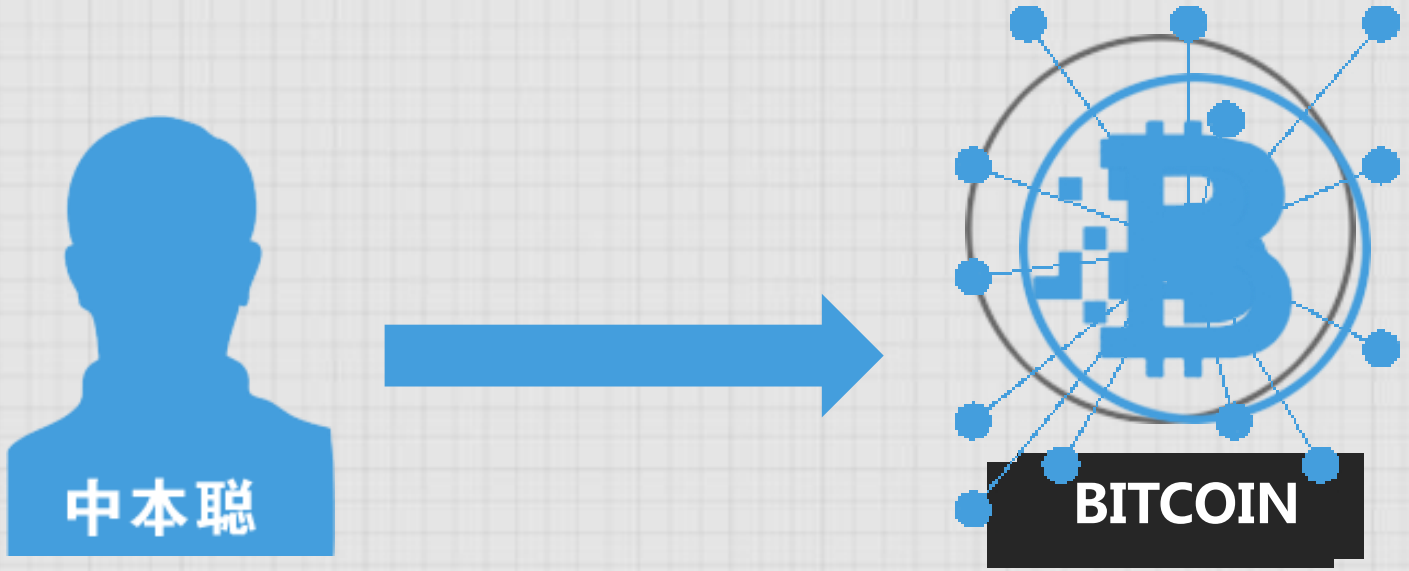
以物易物

实物货币

符号货币

虚拟货币

【一】为什么需要比特币



【二】比特币的工作原理

比特币的工作原理

【二】比特币的工作原理

钱 包

挖 矿

私 钥

公 钥

比特币地址

【二】比特币的工作原理

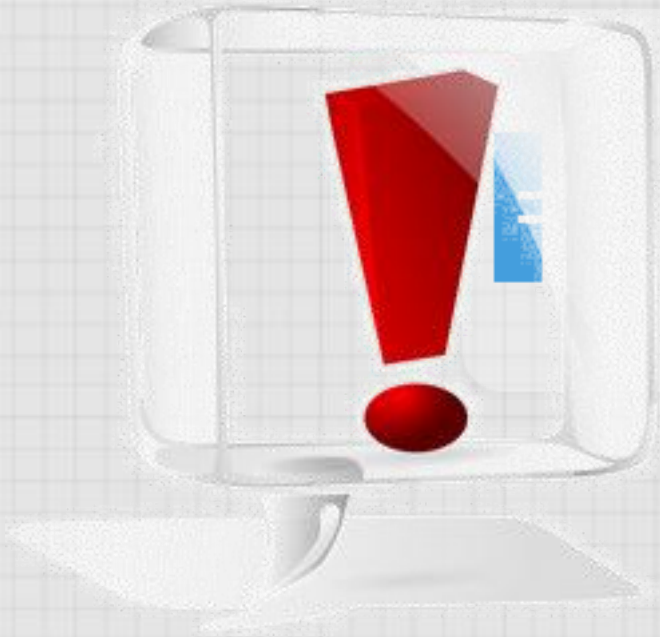
挖 矿

矿工的工作是整个系统的核心。

2009年1月9日中本聪获得最初50BTC

比特币总量：2100万个

【三】比特币的缺点



内在价值	51%攻击及其代价	总量控制和通缩
算法安全性	运算能力集中	衍生能力缺乏
升级隐患	交易速度	匿名、违法用途
系统缺陷	浪费	价格不稳……

【三】比特币的缺点

- 内在价值
- 算法安全性
- 升级隐患
- 系统缺陷
- 51%攻击及其代价
- 运算能力集中
- 交易速度
- 浪费
- 总量控制和通缩
- 匿名
- 衍生能力缺乏
- 违法用途
- 价格不稳

比特币不拥有“固有价值”，没有贵金属的锚定、没有同某种强势货币挂钩、没有国家信用的保证，完全是虚拟的而且，挖矿需要耗费大量的计算能力。

【三】比特币的缺点

- 内在价值
- 算法安全性
- 升级隐患
- 系统缺陷
- 51%攻击及其代价
- 运算能力集中
- 交易速度
- 浪费
- 总量控制和通缩
- 匿名
- 衍生能力缺乏
- 违法用途
- 价格不稳

比特币算法还没被发现有缺陷，安全问题只是风险。比特币的工作是加密、解密，用SHA256算法做计算，就像揉面团一样。目前来看，这还是很安全的，没有被破解的担忧，但在这种非中心化的金融系统中，一但被攻破，整个体系就要崩溃。之前，大家都认为MD5这种加密算法是安全有效的，但是山东大学的王晓云在碰撞攻破MD5但是攻破以后大家就不这么认为了。如果有人可以破解SHA256，那么他就可以偷偷地把比特币转移到自己钱包中。

【三】比特币的缺点

- 内在价值
- 算法安全性
- 升级隐患
- 系统缺陷
- 51%攻击及其代价
- 运算能力集中
- 交易速度
- 浪费
- 总量控制和通缩
- 匿名
- 衍生能力缺乏
- 违法用途
- 价格不稳

如果一个算法，可以通过升级来更新到下一个算法，那么对于比特币来说还是安全的。不断升级对于防范攻击、调整技术参数（货币总额、确认时间等）是十分必要的。但是这种分布式系统的升级，要同步执行起来非常困难。假设有一个老版本的比特币算法，还有一个新版本的算法，新版本的兼容老版本的，但是老版本的还不知道新的算法。某一时刻，全球的钱包有一部分升级了，有一部分还是老版本，这样全球来看比特币钱包的块链的最后形成超过6个块的分岔，叫硬分岔。

【三】比特币的缺点

- 内在价值
- 算法安全性
- 升级隐患
- 系统缺陷
- 51%攻击及其代价
- 运算能力集中
- 交易速度
- 浪费
- 总量控制和通缩
- 匿名
- 衍生能力缺乏
- 违法用途
- 价格不稳

大名鼎鼎的交易延展性问题，mtgox号称因为这个问题丢失了很多币

交易延展性问题

【三】比特币的缺点

- 内在价值
- 算法安全性
- 升级隐患
- 系统缺陷
- 51%攻击及其代价
- 运算能力集中
- 交易速度
- 浪费
- 总量控制和通缩
- 匿名
- 衍生能力缺乏
- 违法用途
- 价格不稳

由于交易确认取决于运算能力，所以如果有人拥有超过50%的比特币全网运算能力并怀有恶意，就可以让比特币系统承认任何交易，比如把别人的钱放到自己的钱包中，这称为51%攻击。

51%攻击

【三】比特币的缺点

- 内在价值
- 算法安全性
- 升级隐患
- 系统缺陷
- 51%攻击及其代价
- 运算能力集中
- 交易速度
- 浪费
- 总量控制和通缩
- 匿名
- 衍生能力缺乏
- 违法用途
- 价格不稳

中本聪原本希望挖矿分布在世界各地，这样系统会更安全。可是现在有钱有技术的人把自己装备成能力很强的矿工，计算量小的很多矿工联合起来组成矿池，对外是一个矿工，挖到了，大家分钱。于是现在的挖矿能力集中到少数矿池中，据说现在运算能力排名第一和第二的矿池，如果联合起来，就可以发动51%攻击

【三】比特币的缺点

- 内在价值
- 算法安全性
- 升级隐患
- 系统缺陷
- 51%攻击及其代价
- 运算能力集中
- 交易速度
- 浪费
- 总量控制和通缩
- 匿名
- 衍生能力缺乏
- 违法用途
- 价格不稳

比特币交易每十分钟做一次确认，获得6个确认后就被认为不可变更这笔交易了，即交易完全成功了。这样一笔交易需要一个小时才能完成。对于大额交易大家比较谨慎，1个小时到帐可以很满意了，但对于小额交易，实在是太慢了。去买一根冰激凌，要是等一个小时，不知道吃到的是什么了。

【三】比特币的缺点

- 内在价值
- 算法安全性
- 升级隐患
- 系统缺陷
- 51%攻击及其代价
- 运算能力集中
- 交易速度
- 浪费
- 总量控制和通缩
- 匿名
- 衍生能力缺乏
- 违法用途
- 价格不稳

矿工实际上所做的工作是算SHA256，也不做些有意义的事，就在揉面团！以前，寻找外星人、寻找梅森质数，大家就用到了分布在各地的计算机，需要大量计算的事还有很多，比如探矿地震波的计算、天气预报、大数据检索信息、新药的设计、电影的制作等等，在中国分布式计算总站上列出了很多有意义的工作。这些有用的事不做，为了得到比特币奖励，在玩揉面团的比赛。另外因为军备竞赛，大家所耗费的电能，最终将趋向于挖出的比特币的价值，看上去非常没有意义。

【三】比特币的缺点

- 内在价值
- 算法安全性
- 升级隐患
- 系统缺陷
- 51%攻击及其代价
- 运算能力集中
- 交易速度
- 浪费
- **总量控制和通缩**
- 匿名
- 衍生能力缺乏
- 违法用途
- 价格不稳

长期来看，比特币有一定数量极限，可以防止通货膨胀，只是比特币的主要买点之一。比特币不断的丢失和上限的预期形成了通缩。这也是比特币最遭经济学家诟病的地方：一个通缩的货币，对于一个经济体来说，不一定是好事，如果大家预期货币越来越值钱，就会把钱放在钱包里，而不是拿来流通。不断下降的消费支出让手里有钱消费者，觉得钱越来越值钱，具体表现在物价便宜了，而且有不断下调的趋势，所以不愿意现在就消费，而是持币观望，希望用更便宜的价格买到自己需要的东西，因而导致进一步消费支出不足和失业。失业的人就更没有消费能力了。

【三】比特币的缺点

- 内在价值
- 算法安全性
- 升级隐患
- 系统缺陷
- 51%攻击及其代价
- 运算能力集中
- 交易速度
- 浪费
- 总量控制和通缩
- 匿名
- 衍生能力缺乏
- 违法用途
- 价格不稳

比特币并不是真正的匿名，每一个交易都写在任何一个钱包中了，只是不容易把钱包中的地址与现实世界中的人对应而已。匿名货币丢了之后找不回来，这个大家都可以理解，因为哪一种货币丢了都找不回来的。

匿名

【三】比特币的缺点

- 内在价值
- 算法安全性
- 升级隐患
- 系统缺陷
- 51%攻击及其代价
- 运算能力集中
- 交易速度
- 浪费
- 总量控制和通缩
- 匿名
- 衍生能力缺乏
- 违法用途
- 价格不稳

比特币并不是真正的匿名，每一个交易都写在任何一个钱包中了，只是不容易把钱包中的地址与现实世界中的人对应而已。匿名货币丢了之后找不回来，这个大家都可以理解，因为哪一种货币丢了都找不回来的。

但是，各国政府对这种匿名还是非常反感的。匿名交易收不到税。原来小额的现金交易，国家收税可能有些困难，但是政府可以监管银行，拎着一大堆现金做交易不像是现代社会的行为，所以大额的交易没办法逃过政府监管。由于比特币的匿名特性，税务局可能收不到大额交易的税了。

【三】比特币的缺点

- 内在价值
- 算法安全性
- 升级隐患
- 系统缺陷
- 51%攻击及其代价
- 运算能力集中
- 交易速度
- 浪费
- 总量控制和通缩
- 匿名
- 衍生能力缺乏
- 违法用途
- 价格不稳

总量的控制对与比特币来说就没有了信贷扩张。银行吸收存款，然后再贷款出去。贷款的人拿着钱，毫无疑问是有钱的；存钱的人拿着存折，大家也认为他是有钱的，早期的人银子存到钱庄后拿着钱庄的票据就可以去买东西。这样名义上存钱的和借钱都是有钱的，世界上总的钱的数量就好像增加了。

银行的行为就是利用闲散资金，让资金流动起来，货币总量的增加可以加速经济的运转。比特币总量是固定的，不可能有这种行为。比特币的性质非常像黄金，有限，可分割，作为交易的中介。因为其有限性，在经济景气周期，会供不应求。由于比特币的交易手段只能是不能撤消的转让，交易手段就非常局限，很难进行金融创新。

【三】比特币的缺点

- 内在价值
- 算法安全性
- 升级隐患
- 系统缺陷
- 51%攻击及其代价
- 运算能力集中
- 交易速度
- 浪费
- 总量控制和通缩
- 匿名
- 衍生能力缺乏
- 违法用途
- 价格不稳

洗钱、资本逃逸、毒品贩卖、色情交易、军火交易、销赃等经常寻求各种匿名的支付方法。比特币的匿名属性正好满足了这些交易的需求。2014年2月俄罗斯政府对比特币使用者发出警告，称虚拟货币可能被用于洗钱或资助恐怖主义，并宣布将比特币视为与卢布并行的货币加以使用是违法行为。

此前2013年7月泰国外汇管理和政策部的高官也曾经表示，买卖比特币、用比特币买卖任何商品或服务、与泰国境外的任何人存在比特币的往来在泰国都被视为非法行为。不过2014年2月泰国央行允许比特币流通和交易，但是要求交易仅限于在泰国国内并以泰铢结算，而不得涉及其他海外货币。违法用途也是各国政府最头痛的一件事。

【三】比特币的缺点

- 内在价值
- 算法安全性
- 升级隐患
- 系统缺陷
- 51%攻击及其代价
- 运算能力集中
- 交易速度
- 浪费
- 总量控制和通缩
- 匿名
- 衍生能力缺乏
- 违法用途
- 价格不稳

比特币的价格波动大，不论是上涨还是下跌，对于延迟付款的买卖双方，总有一方利益受损，就会让人不愿使用比特币。如果签合同说过几天用比特币买一台手机，几天后比特币涨了买方就不愿意付钱，跌了，卖方不愿意给货。

作为世界货币，币值稳定是必须的。有人争辩说，目前比特币价格不稳定可能是交易量小，比特币市值不大，但是想想，以后如果比特币市值大了，市值同黄金或美元一样，比特币还要涨多少啊，这个过程中大家不用比特币了吗？

持续的价格过快上升也带来了后期的比特币投资者带来不公平的心理，妨碍了更多的人参与。

【四】其他虚拟币（山寨币）

【四】其他虚拟币（山寨币）

【四】其他虚拟币（山寨币）

莱特币

LiteCoin

莱特币于2011年11月9日上线，可以说是目前最成功的山寨币。莱特币的确认时间减少到2.5分钟，货币总量增加到8400万个，主要的是莱特币采用了不同于SHA256的加密算法——Scrypt算法，这个算法要求计算机更高级，运算能力目前不太可能集中到一起，与比特币相比有更分散的矿工。自从专门用来挖矿的比特币芯片开发出来后，做成芯片矿机，硬件替代了软件，运算能力更强，挖矿效率更高。

与比特币算法相同的山寨币如果没有其他保护，就有人拿比特币芯片矿机来挖这些山寨币，或进行51%攻击，使得这些山寨币价值一落千丈。由于莱特币算法不同，还保持金身不坏。目前Scrypt算法的山寨币要远多于SHA256算法的山寨币。

【四】其他虚拟币（山寨币）

质数币

PrimeCoin

寻找质数

质数币于2013年7月12日上线，它还是用工作量证明来挖矿，但是在挖矿的时候并不是单纯的计算加密算法，而是在寻找一种的质数，而质数是有用的，可以在通信加密中用到。

【四】其他虚拟币（山寨币）

格雷德币

GridCoin

分布式科学计算

格雷德币创立于2014年10月16日上线。是基于伯克利开放网络计算平台（BONIC）的数字货币。

【四】其他虚拟币（山寨币）

域名币

NameCoin

提供.bit域名

用分布式的方法解决域名被根节点域名服务区控制的问题

【四】其他虚拟币（山寨币）

万事达币

MasterCoin

分布式资产平台

万事达币为今后的分布式资产如股票、证券的发行提供了技术手段。其支持的交易包括比如发送交易、支付交易、要约交易、取消交易等，即将开发对赌、分红等功能。这些交易将会用于创建分布式资产，允许个人和企业创造分红产品和分配资产，避免依赖于中间商

【五】比特币思想

【五】比特币思想

100%透明慈善捐款

基于DAC模式的微博系统

DAC思想

100%透明投票

比特币不只是货币

谢谢大家

InfoQueue
Enterprise Software Development Community

特别感谢合作伙伴

InfoQueue
Enterprise Software Development Community

特别感谢媒体伙伴（部分）