



比特币历史

我们从哪里来？

-从 cypherp1 运动到摩根大通



历史回顾

你必须知道你从哪里来, 才能知道去哪里

基本比特币概念

比特币是什么？基本概念

➤ 加密货币：

- "一种数字货币, 使用加密技术来调节货币单位的生成并验证资金的转移, 独立于中央银行运作。
 - 建立在计算机科学、密码学和经济学相结合的基础上

➤ 比特币是一种加密货币

➤ "比特币" 可以指：

- 比特币 (大写)-协议、软件和社区
- 比特币 (通常小写)-单位

➤ 比特币纯粹作为软件存在



比特币特性

分散

无信

共识

- 比特币是一种没有中心控制点的数字货币。
 - 它通过达成 "分散共识" 来实现这一目标
 - # 这意味着没有故障或控制的中心点
- 比特币是 "不可信赖的"
 - # 意味着你需要信任 * 没有人, 以使您的交易。
- 适用于比特币的 "共识" 是节点网络在交易历史上的一致。

比特币的创新特性

- 开放式金融网络 + 假名
- 无边界
 - 汇款
- 抗审查性和 * 不可变
 - * 大部分
 - 不可逆付款
- 可编程货币
 - 更轻松集成, 因为网络的开放性

Send money to Brazil with westernunion.com

Family and friends are especially important during this time of year. Wherever you need to send money in Brazil, from Rio to São Paulo, you can count on Western Union. [Price your transaction here.](#)* Fees start at \$4.99 to send up to \$20 online. Mobile send fees start at \$1 to send up to \$10 for pickup in minutes.**

上午/<https://www.westernunion.com/us/en/send-money-to-brazil.html>

Traits of Money	Gold	Fiat (US Dollar)	Crypto (Bitcoin)
Fungible (<i>Interchangeable</i>)	High	High	High
Non-Consumable	High	High	High
Portability	Moderate	High	High
Durable	High	Moderate	High
Highly Divisible	Moderate	Moderate	High
Secure (<i>Cannot be counterfeited</i>)	Moderate	Moderate	High
Easily Transactable	Low	High	High
Scarce (<i>Predictable Supply</i>)	Moderate	Low	High
Sovereign (<i>Government Issued</i>)	Low	High	Low
Decentralized	Low	Low	High
Smart (<i>Programmable</i>)	Low	Low	High

https://www.reddit.com/r/Bitcoin/comments/4b8ne0/rbitcoin_faq_newcomers_please_read/

比特币的使用案例

- 汇款 *: 廉价、高效地跨境汇款
 - * 有争议
- 数字商品: 不可逆转的行业
- 机器到机器支付, 物联网
- 自治网络的货币
- 小额支付: 每篇文章的付款
- 数字黄金: 价值的替代储存



<https://cointelegraph.com/news/300-increase-in-bitcoin-buys-across-eu-as-greece-falls-into-arrears>

比特币是什么？基本概念

➤ 基本数据结构 (绝对知道这些)

- 交易: 比特币从输入地址转移到输出地址
- 块: 已时间限制的事务集合。
- 矿工: 验证交易记录并将其放入块中
- 区块链: 整个系列的块 "链" 在一起

➤ 正确的链条是最长的链条

- 矿工们竞相增加方块

➤ 比特币的价值从何而来？

- 比特币之所以有价值, 是因为人们相信它有价值。

早期时间线

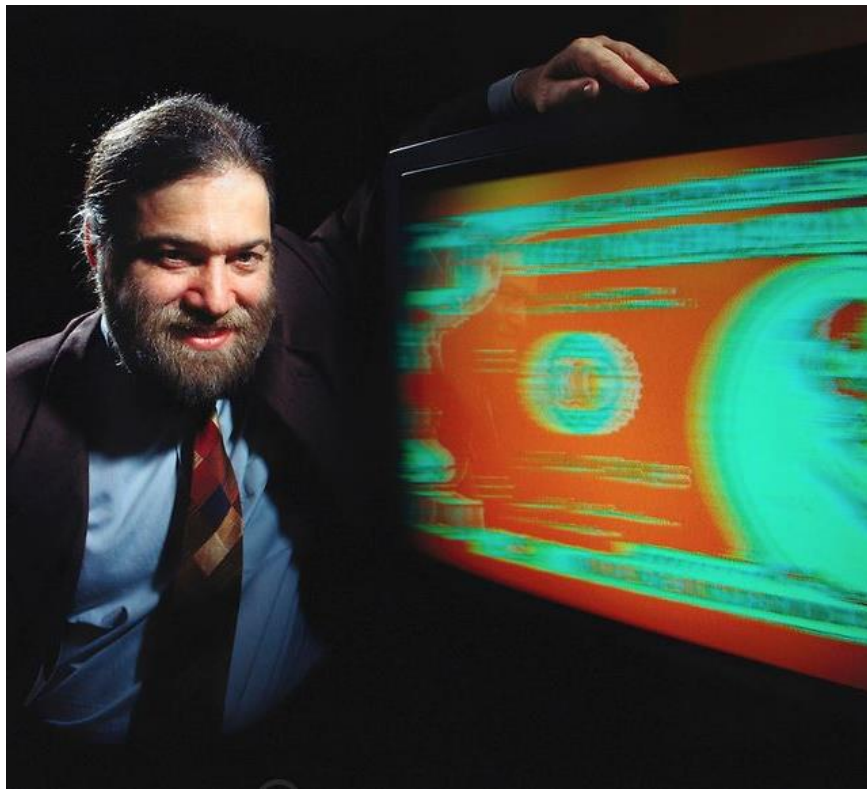
- ~ 1990年—开始从现金到数字的移动
- 1991年-digicash-david chaum
- 1992: cypherpunks 的起点。出版《赛弗朋克宣言》。
- 1997: hashrc—亚当后面
- 1998: b-钱-戴伟
- 2005: bitlin—尼克·萨博
- 2008: 比特币-中本佐藤

数字现金的问题

- 身份变成了新的钱
- 所有个人交易的完全可追溯性
- 对货币主权的全面账户控制单位
- 付款封锁和没收变得更加容易
- 完全消除非正规影子经济
- 接近绝对税收效率

david chaum-digicash

- 创作者: **david chaum**
- **1982年:** 论文 "无法追踪的付款的盲目签名" 已匿名或假名
- **1990年**的数字
- **digicash** 于**1998年**破产, **2002年**被收购
- **digicash** 专注于使事务匿名。
- 考虑到的是, 拥有数字支付将导致对人们的消费从而对私人生活有洞察的不可取的能力。



赛弗朋克宣言

- 鼻祖: eric hughes, 1993年
- "隐私不是秘密。"
- ". 在一个开放的社会中, 隐私需要匿名交易系统。"
- "开放社会中的隐私也需要密码学"
- "要想让隐私普及, 就必须是社会契约的一部分"

资料来源: <https://www.activism.net/cypherpunk/manifesto.html>

ink's Manifesto

in an open society in the electronic age. Privacy is not secrecy. A private matter is so in a sort of dealings, then each has a memory of their interaction. Each party can speak to all at all. If many parties speak together in the same forum, each can speak to all at all.

we must ensure that each party to a transaction have knowledge only of that which is necessary to the transaction. When I ask for a loan, I want to know who I am. When I ask for a loan, I want to know who I am. When I ask for a loan, I want to know who I am.

an open society requires anonymous transaction systems. Until now, cash has been the essence of privacy.

privacy also requires cryptography. If I say something, I want it heard only by those for whom it is intended. Furthermore, to reveal one's identity with assurance when the default is privacy.

governments, corporations, or other large, faceless organizations to grant us privacy out of the goodness of their hearts. We want to be free, it longs to be free. Information expands to fill the available storage space.

privacy if we expect to have any. We must come together and create systems which

adam back-hashcash

- 创作者: 亚当背
- 1997年: 创建 hashcash, "部分哈希碰撞为基础的邮费计划"
- 通过使发送者可以轻松地进行可验证的计算 (哈希), 从而防止垃圾邮件的保护系统
- 论文明确提到了可能的取缔数字
- 哈什金成为挖掘算法的基础。



魏代-b-钱

- 创办人: 戴伟
- **1998: b 货币的创作**
- **b-货币介绍**
 - 公钥假名
 - 使用现金创造货币
 - 保留分类帐的两种可能方法
 - 所有参与者检查 (pow)
 - 服务器提供抵押品 ((d) 指针)
- **缺失: 控制货币创造的一种方式**
 - 提出一些仍然集中的方法



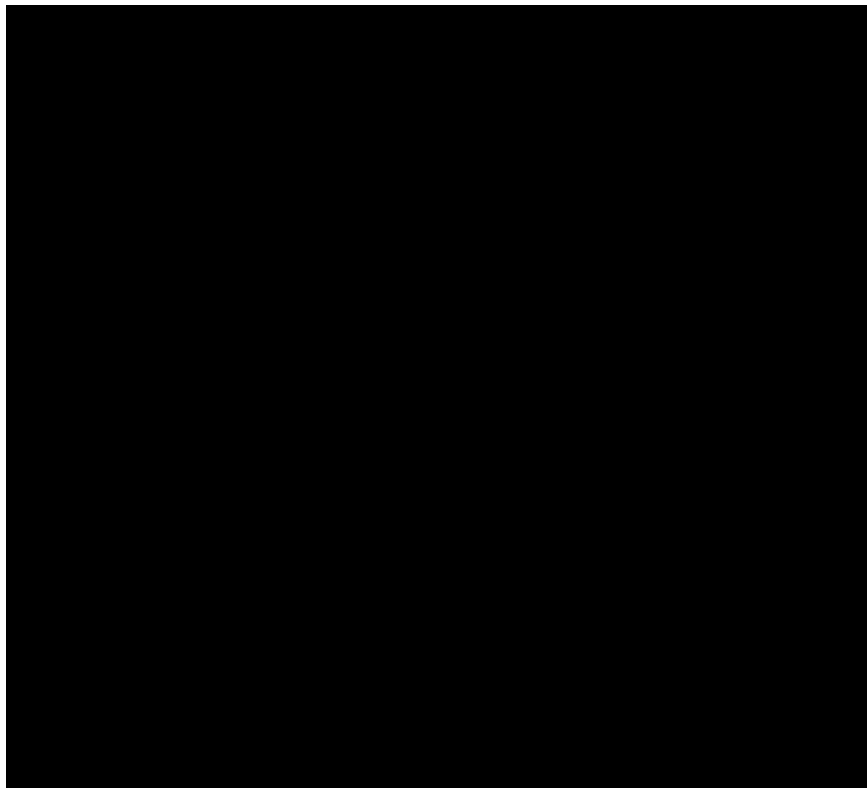
nick szabo-bitgold

- 创作者: 尼克·萨博
- **1998:** 位金子的创立
- 位黄金介绍
 - 时间戳
 - 使用现金创造货币
- 缺失: 保持节点诚实的激励措施
- 缺失: 一种保持令牌可替换的方法 (没有约定的设置难度的方法。一个令牌可能比另一个更困难)



中本佐藤-比特币

- 创办人: 中本佐藤
- **2008年:** 比特币的成立
- **2009年:** 比特币的实施
- 比特币用途
 - 公钥假名
 - 时间戳
 - 使用现金创造货币
 - 节点的角色: 矿工保持诚实 (难度调整)。哈希是度量
 - 用于交易 "批处理" 的默克树



总结

- 谁派的？ - 大卫·查姆, 最终 **digicash**, 从**1981**年开始
- 我应该送什么？ 郭伟代, **b-钱**, 但也哈勒芬尼·**rpow** 和尼克·萨博位黄金。**1997**年期间拟议 (**大麻现金**)-**2005**年。
- 我什么时候发送？ 中本佐藤, 比特币。解决硬币供应不能膨胀的方式, 以及通过在网络中添加块和角色来重用 **pow**。

白皮书

源:

<https://bitcoin.org/bitcoin.pdf>

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any

承认历史和背景



- 比特币在**2008年**或**2009年**没有 "启动"
- 比特币 (进而是所有的区块链) 是更大运动的一部分
- 它们是解决社会和政治问题的技术方式
- 它们会进化, 但这不应该意味着否认它们的起源。

比特币历史

比特币历史分解成几个有代表性的故事

- bitcore 前-2009年: 自由主义的梦想和理想
- 2009-2010年: 比特币的早期发展
- 2010-2012年: 丑闻、黑客攻击和非法活动
- 2013-2014年: 比特币吸引眼球
- 2014年: 商户验收
- 2013-2014年: 风险投资比特币创业公司
- 2014年至今: 以太爆炸 (以多种方式)
- 2015年至今: 比特币难以扩展
- 2015年至今: 银行对 "封锁链" 的兴趣上升

2009年前的 bitcince-2009: 自由主义的梦想与理想

自由主义的梦想

- 随着上世纪 80 年代和 90 年代技术的进步, 赛弗朋克运动应运而生
- cypher—n1 宣言: "隐私对于电子时代的开放社会是必要的"。
- 自由主义和密码学的根源
 - 自由主义是一个主张不侵略原则和自由放任政府的政治意识形态
 - 密码学是一门科学在第三方在场的情况下确保通信



cypherpunks 和加密无政府主义者

- 赛弗朋克们痴迷于技术将如何改变个人与国家之间的关系
- 希望人们拥有的新工具, 但关心的是人们如何保护自己的个人信息, 维护自己的隐私不受政府的影响



Untraceable Electronic Cash †
(Extended Abstract)

*David Chaum*¹ *Amos Fiat*² *Moni Naor*³

¹ Center for Mathematics and Computer Science
Kruislaan 413, 1098 SJ Amsterdam, The Netherlands

² Tel-Aviv University
Tel-Aviv, Israel

³ IBM Almaden Research Center
650 Harry Road, San Jose, CA 95120

CRYPTO 1988

DigiCash[™]



David Chaum

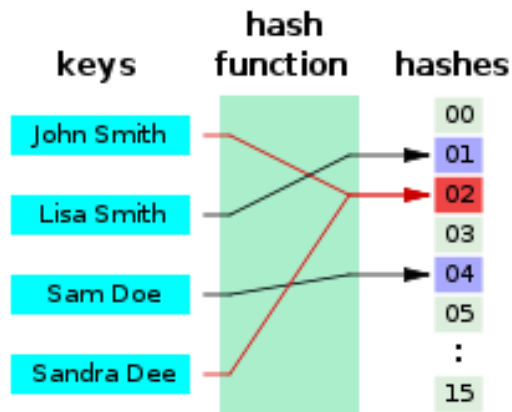
Photo: Declan McGullagh (2012)

兑换资金

- 现有的金融体系被视为对个人隐私的最大威胁之一
- **迪吉卡什**是早期加密货币最著名的例子
- digicash 的发明者 david chaum 使用了公钥密码学
- 不过, digiash 是一个中央组织, 这意味着 chaum 的公司需要确认每一个数字签名。
- 最终, chaum 的公司破产了, digicash 也随之破产了

加密创新

- cypherpunks 还致力于技术创新, 包括加密哈希功能。
- **哈希函数是一个数学公式, 很容易解决, 但很难反向工程。**
- cypherpunks 的早期实验继续遇到障碍, 导致失败



2009-2010年： 比特币的早期发展





dorian satoshi nakamoto

中本佐藤和比特币

- 中本佐藤是比特币的匿名创作者, 他写了一份9页的白皮书, 出色地结合了以往所有的努力, 创造了一个自我维持的数字货币。
- 尽管一些对历史感到沮丧的人对货币持悲观态度, 但一些早期的先驱者支持将这一项目作为解决过去问题的办法



创世纪块

- 创世纪区块开采2009年1月3日
- 起源块的造币基础参考了《伦敦时报》上一篇涉及财政大臣救助银行的报道
- 2009年1月12日与哈尔·芬尼的第一次比特币交易

Block 0²				
Short link: http://blockexplorer.com/b/0				
Hash ² : 00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f				
Next block ² : 00000000839a8c6886ab5951d76f411475428afc90947ee320161bbf18eb6048				
Time ² : 2009-01-03 18:15:05				
Difficulty ² : 1 ("Bits" ² : 1d00fff)				
Transactions ² : 1				
Total BTC ² : 50				
Size ² : 285 bytes				
Merkle root ² : 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b				
Nonce ² : 2083236893				
Raw block²				
Transactions				
Transaction ²	Fee ²	Size (kB) ²	From (amount) ²	To (amount) ²
4a5e1e4baa...	0	0.204	Generation: 50 + 0 total fees	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa : 50

六百万美元的披萨

- 2010年5月21日, 拉兹洛·汉尼茨为 10, 000 btc 购买了价值 25美元的比萨饼
- 这是世界上首次为有形资产进行比特币交易
- 10, 000 btc 现在相当于 5 79万美元



2010-2012年: 丑闻, 黑客, 非法活动

戈克斯山



- 2010年, gox 山成立, 并将自己合并为比特币开始阶段最大的比特币交易所。
- 在 6号/星期一, gox 山严重违反了安全规定, 导致欺诈交易, 并要求关闭该网站7天。
- 2014年, 哥克斯山在一起多年来一直没有被人注意的盗窃中丢失了 74 408个比特币
- 最终, 戈克斯山宣布破产

丝绸之路



- 2011年2月, 丝绸之路开业: 比特币市场丝绸之路启动了一个名为 "毒品易趣" 的毒品交易非法市场。
- 2013年10月, 美国联邦调查局关闭了丝绸之路, 缴获了价值360万美元的比特币
- 丝绸之路创始人罗斯·乌尔布里希特目前正在服无期徒刑, 不得假释



Shop by Category

Drugs 4,086

Cannabis 983

Dissociatives 77

Ecstasy 318

Opioids 350

Other 157

Precursors 18

Prescription 901

Psychedelics 587

Stimulants 405

Apparel 82

Art 5

Books 778

Collectibles 15

Computer equipment 42

Custom Orders 27

Digital goods 369

Drug paraphernalia 152

Electronics 36

Erotica 296

Fireworks 5

Food 4



100 x Anadrol 50MG
Oxymetholone (sealed)
\$12.41



1 gram MDMA
\$5.89



1/2g Cocaine
\$5.44



10 Pieces White Heart
130-150mg MDMA Content
\$4.49



Red and White Filter (10
packs x 20 cigarettes)
\$1.90



VEGA 100mg Sildenafil
citrate 4 tablets
\$1.50



10 gram Santa Maria
\$11.58

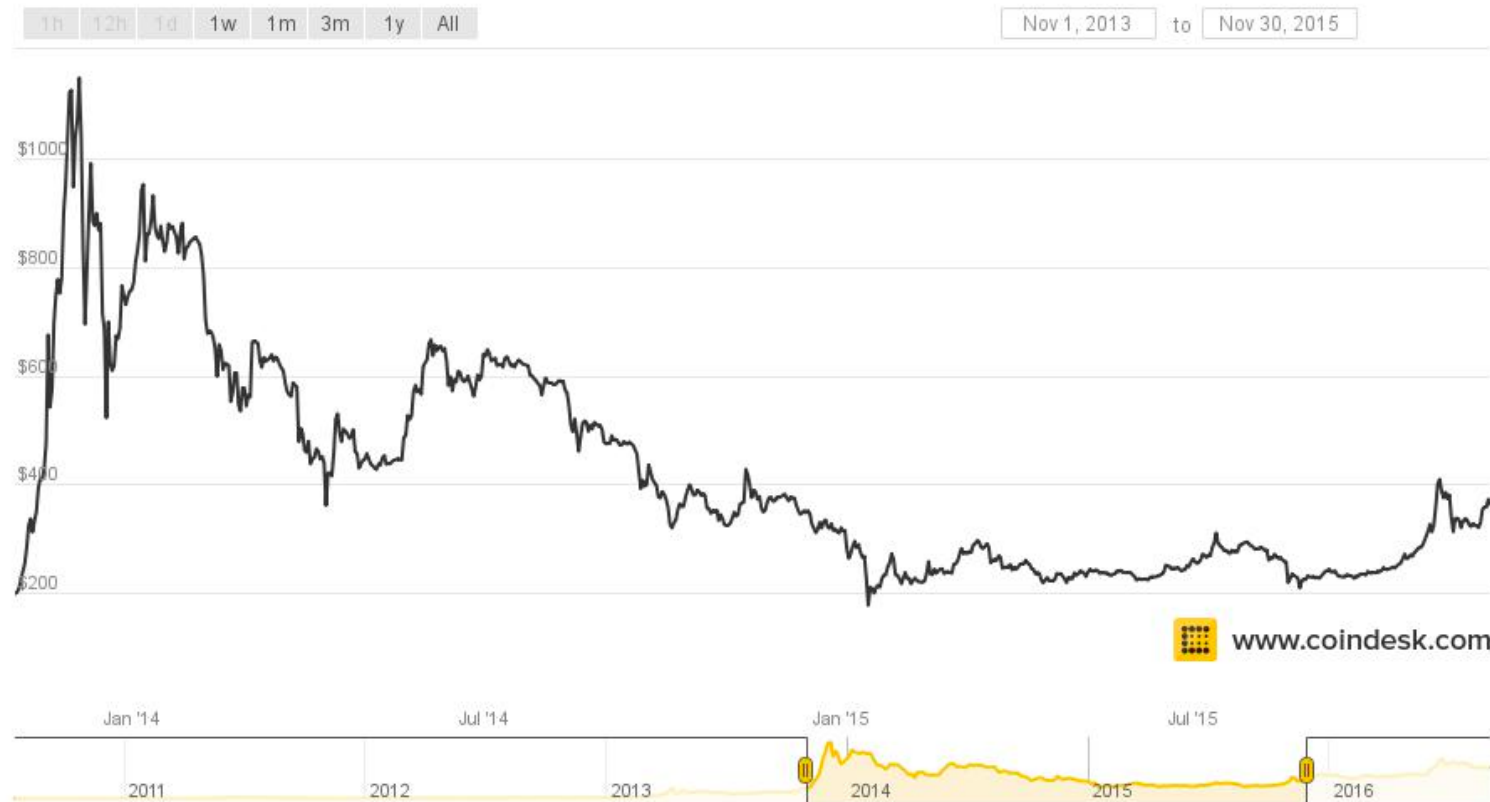


1/4 oz G13
\$8.13

比特币泡沫和爆裂



比特币价格泡沫和爆裂



2013-2014年： 比特币吸引眼球

炒作

(自科因台)

- 2014年2月山戈克斯据称损失了3.5亿美元的比特币 (74, 400 btc), 被指控破产
- 2014年3月比特币发明人 satoshi中本在加州发现的 '发现 '
- 2014年9月蒂姆·德雷珀: 比特币的价格仍然上涨到10美元

商户接受

(自科因台)

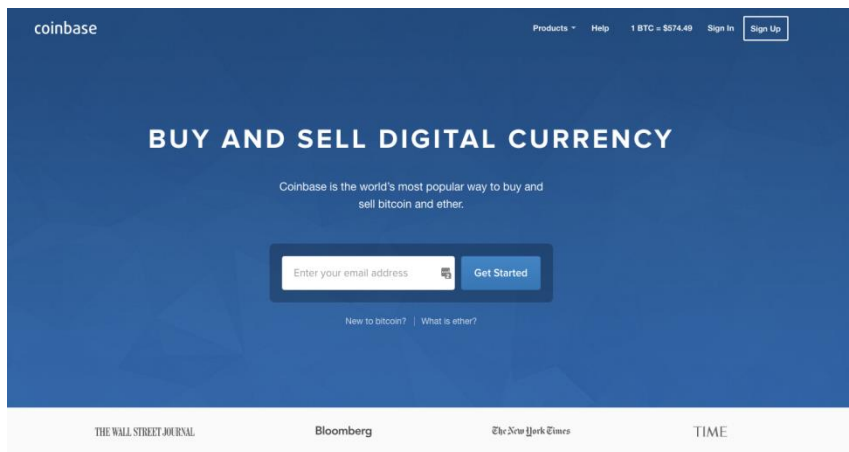
- 2014 年 1 月 . com 接受比特币
- 2014年1月, overstock. com 成为首家接受比特币的大型零售商
- 2014年4月新科罗拉多州大麻自动售货机将接受比特币
- 2014年9月 paypal 与科因基地, 比特支付
- 2014年12月微软接受比特币支付
- (2014年10月)"谁说那比特币不能给你买东西? ...

shitexpress是一种服务, 发送百 惠集装箱的马粪与个性化的消息为您。-科因台

2013-2014年： 风险投资的比特币初创企业

科因基地

- 硬币基地规模代表投资者的兴趣
- 在线钱包和交换
- 科因基地成立 2012年6月, 注册2012年夏季 y 组合
- 2013年5月: 500万美元 a 系列
- 2013年12月: 2 500万美元 b 系列
- 2015年7月: 7 500万美元 c 系列



coinbase

合资公司的崛起

- 硬币基地: 托管钱包
- bitfinex: 在线交易/交易平台
- 21 inc: 机器付款和嵌入式采矿
- 比特币: 允许商家接受比特币付款, 转换为美元
- 更改提示: 社交比特币小额支付
- 区块流: 比特币核心, 侧向, 研究



ANDREESSEN
HOROWITZ

种子轮

- 2013年4月26日
- 2014年33日
- 2014年3月26日圈子互联网金融
- 2014年4月21日
- 2014年6月16日
- 2014年8月20日链条
- 2014年10月7日区块链
- 2014年2010-2011年双贴士



BLOCKCHAIN



CIRCLE



**2014年至今：
以太吹起 (以多种方式)**

以太爆炸 (以多种方式)

比特币是基于简单的脚本语言。以太是一个土耳其完整版本的比特币。复杂分散应用的潜力

历史

- 2013年底: 在白皮书中描述的以太维塔利克 布特林
- 2014年7月和 8月: 以太众包
- 2015年7月30日: 以太区块链推出
- 2016年5月: 价值超过10亿美元的以太令牌价值

新治理模式的巨大潜力

- 2016年7月: dao 的崛起和黑客攻击

2015年至今: 比特币的扩展

方块辩论

- 比特币块每10分钟创建一次
- 2010年, 块大小限制减少到 1 mb
- 2015年, 比特币区块开始 "填满"
- 巨大的可扩展性问题
- 分裂的社区-封锁辩论
- 意义: 提出了关于分散治理、控制的问题
- 社区和法规

雷电网络

- 闪电网络是最流行的可扩展性解决方案
- 允许安全支付, 而不会冲击区块链
- 可伸缩性
 - 了解哈希计时器合同、状态通道、检查锁计时码验证

银行对 "封锁链" 的兴趣

银行对 "封锁链" 的兴趣

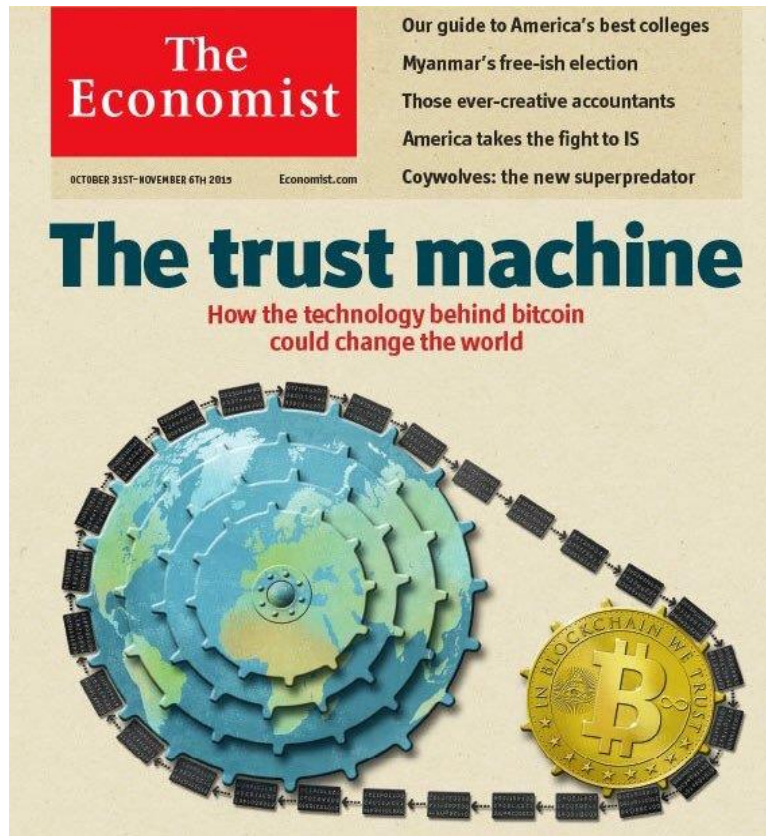
➤ 对 "私人区块链" 或 "允许的分类账" 的兴趣上升。

- 未打开
- 不可靠
- 没有像比特币那样的经济激励
- 将 "区块链" 与 "比特币" 分开

➤ con:

- 通常不使用共识
- 光荣的公钥加密

➤ 优点: 更合规性



"私人区块链" 倡议

➤ R3CEV

- 2015年9月开始

➤ 链

- 创业与金融公司合作建立开放标准

➤ 数字资产控股

- 由布莱斯大师创立

➤ 超帐项目: 开源区块链

- 由数字资产控股公司和 linux 基金会运营

➤ ibm 开放区块链

- 现在作为 "结构" 的超级分类帐项目的一部分

➤ 摩根大通朱诺项目



杰米·戴蒙在 bitcon 区块链上的报价

#衡量大型金融机构如何看待封锁链的一个方法是看看是什么摩根大通首席执行官杰米·戴蒙已经说, 随着时间的推移

2014年1月: "这是一个可怕的价值储备。它可以反复复制。

人们仍然不懂比特币



"It's a terrible store of value." CNBC

杰米·戴蒙在 bitcon 区块链上的报价

2014年10月: "[比特币开发商]
将尝试吃我们的午餐。这很好
。这就是所谓的竞争,我们将竞
争。

承认比特币的合法性



<http://static6.businessinsider.com/image/5527c91969beddfd15404336-480/jp-morgan-chase-and-company-ceo-jamie-dimon.jpg>

杰米·戴蒙在 bitcon 区块链上的报价

2015年11月: "虚拟货币, 在那里被称为比特币对美元, 这将被阻止。...任何政府都不会支持一个绕着边界走、没有同样控制的虚拟货币。这是不可能发生的。

银行家们讨厌缺乏控制。也许是威胁?



<http://fortune.com/2015/11/04/jamie-dimon-virtual-currency-bitcoin/>

杰米·戴蒙在 bitcon 区块链上的报价

2016年2月: "区块链是一项技术, 我们一直在研究..... 是的, 它是真实的。它可能会降低某些事情下实际应用的成本。...如果它被证明是便宜和安全的, 它将被采用的一大堆的东西。

将 "区块链" 与 "比特币" 分开



历史回顾

比特币是解决一个非常具体问题的办法。它可能会产生政治影响, 但却是一种工程解决方案

重构区块链

- 有一种倾向, 把自己的理想和意识形态投射到比特币和区块链上
- "快速" 事务 (在上下文中定义快速)
- 叉子的各种新定义
- 社会议程 (以) (即界定 "公平")
- 各种特征的可取性 (界定社会契约的选择)
- 治理 (定义什么是治理)
- 这些都不是比特币的目的



我们需要学会定义才能说话

1. 加密货币空间中充斥着模糊和混乱的定义：现金、货币、快速、安全等。
2. 为了谈论这些事情, 我们需要在每个辩论的基础上, 或者在上下文中笼统地明确界定这些术语
3. 如果我们不这样做, 我们将继续容易受到坏演员的社会攻击, 他们想把我们的言论与混乱的言论混为一谈, 煽动不和而不是诚实的分歧
4. 一旦我们有了明确的定义, 我们总是会意见不一。根本没有必要达成一致的目标。然而, 为了测试我们的系统, 我们需要完全开放和清楚测试参数是什么。
5. 如果没有这种明晰度, 我们必然会在没有任何建设性对话的情况下发生冲突。

来源

- 无法追踪的电子现金, **david chaum**:http://blog.koehtopp.de/uploads/chaum_fiat_naor_ecash.pdf
- 无法追踪的付款的盲签名, **david chaum**:<http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF>
- 《cypher克朋克宣言》, **eric hughes**:<https://www.activism.net/cypherpunk/manifesto.html>
- 哈希现金邮费的实施, 亚当回:<http://www.hashcash.org/papers/announce.txt>
- **b-钱**, 戴伟:<http://www.weidai.com/bmoney.txt>
- 可重复使用的工作证明, 哈尔·芬尼:<https://web.archive.org/web/20071222072154/http://rpow.net/>
- 安全财产所有权, 尼克·萨博:<http://nakamotoinstitute.org/secure-property-titles/-6.1-6。1>
- 位黄金, 尼克·萨博:<https://unenumerated.blogspot.nl/2005/12/bit-gold.html>
- 比特币白皮书, 中本佐藤:<https://bitcoin.org/bitcoin.pdf>
- 塞缪尔·法尔肯的各种职位:<https://www.linkedin.com/in/samuel-falkon-467a878b/detail/recent-activity/posts/>
- 比特币与赛弗朋克的崛起, 硬币台:<https://www.coindesk.com/the-rise-of-the-cypherpunks/>
- **bitcoin**: 政治攻击探测器和常见的任务, **giacomo zucco**:<https://youtu.be/jgwW7XZCKPU>

结束！

धन्यवाद

Hindi 印地
语

多謝

繁体中文

ขอบพระคุณ

泰语

Спасибо

俄语

谢谢

西班牙语

شكراً

阿拉伯语

谢谢

英语

奥布里加
多

巴西葡萄牙语

格拉齐

意大利
语

多谢

简体中文

丹克

德语

谢谢

法语

நன்றி

Tamil

泰米尔
语

ありがとうございました

日语

감사합니다

朝鲜语