Bitcoin History

-From the Cypherpunk Movement to JPMorgan Chase

LING Zong, Ph. D.
Senior Software Engineer / Scientist
IBM Almaden Research Center
San Jose, California, U.S.A.

Historical Perspective

你必须知道你从哪里来，才能知道去哪里

You have to know where you come from in order to know where to go

Basic Bitcoin Concepts

What is Bitcoin? Basic Concepts

➢Cryptocurrency:
➢一种数字货币，使用加密技术来规范货币单位的产生和验证资金的转移，独立于中央银行运行
○计算机科学、密码学和经济学的结合
➢比特币是加密货币
➢“比特币”可以指:
○比特币(大写)-协议，软件和社区
○比特币(常规小写)—单位
➢比特币作为纯粹的软件而存在

- **Cryptocurrency:**
  - "A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank."
  - Built upon a combination of computer science, cryptography, and economics
- **Bitcoin is a cryptocurrency**
- **“Bitcoin” can refer to:**
  - Bitcoin (uppercase) - the protocol, software, and community
  - bitcoins (conventionally lowercase) - the unit
- **Bitcoin exists purely as software**

Bitcoin Characteristics

●比特币是一种没有中心点控制的数字货币。
○它通过达成“分散共识”来实现这一点
■#意味着不存在故障或控制的中心点
●比特币“不可信”
意思是你不需要信任*任何人来完成你的交易。
●适用于比特币的“共识”是指网络节点对交易历史达成一致。

Decentralized Trustless Consensus

- Bitcoin is a digital currency that has no central point of control.
  - It accomplishes this by reaching "decentralized consensus"
    - # which means that there is no central point of failure or control
- Bitcoin is "trustless"
  - # meaning that you need to trust* no one in order to make your transactions.
- "Consensus" as applied to Bitcoin is that the network of nodes agrees on the transaction history.

比特币的创新特性

Innovative Properties of Bitcoin

- **Open financial network + pseudonymous**
- **Borderless**
  - Remittances
- **Censorship-resistant and *immutable**
  - *Mostly
  - Irreversible payments
- **Programmable money**
  - Easier integration because openness of network

➢开放金融网络+伪典
➢无国界
➢汇款
➢抗审查的档案和
*不可变的
➢*主要是
➢不可逆转的支付
➢可编程的钱
➢容易集成,因为开放的网络

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.**

On 8/31/16 from https://www.westernunion.com/us/en/send-money-to-brazil.html

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

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

Use Cases of Bitcoin

汇款*:廉价而有效地跨境汇款
- *有争议
- 数字商品:不可逆的交易
- 机器机器支付,物联网
- 货币自治网络
- 小额支付:支付每条
- 数字黄金:替代价值储存手段

- **Remittances*: Sending money cheaply and efficiently across borders**
  - *Controversial

- **Digital goods: Irreversible trades**
- **Machine to machine payments, IoT**
- **Currency for autonomous networks**

- **Micropayments: Ex. Pay per article**
- **Digital gold: Alternative store of value**

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

What is Bitcoin? Basic concepts

➢基本数据结构(一定要了解这些)
○交易:传输的比特币输入地址输出地址
○区块:按时间戳收集交易。
○Miner:验证交易并将其放入块中
○区块链:整个系列的块被“锁”在一起
➢正确的链是最长的碳链
○矿工们竞相添加区块
➢比特币在哪里得到它的值?
○比特币有价值是因为人们相信它有价值

- **Basic data structures (definitely know these)**
  - Transactions: Transfers of bitcoin from input addresses to output addresses
  - Blocks: Timestamped collection of transactions.
  - Miner: Validates transactions and puts them into blocks
  - Blockchain: The entire series of blocks 'chained' together
- **The correct chain is the longest chain**
  - Miners compete to add blocks
- **Where does Bitcoin get its value?**
  - Bitcoin has value because people believe it has value.

~ 1990年开始运动从现金到数字
• 1991 - Digicash - David Chaum
1992:密码朋克的开始。出版《密码朋克宣言》。
Hashcash - Adam Back
• 1998:b -钱-戴伟
• 2005年:BitGold——尼克•萨博
• 2008:比特币——中本聪

Early Timeline

- ~ 1990 – Start of the movement from cash to digital
- 1991 - Digicash – David Chaum
- 1992: Start of the Cypherpunks. Publication of "A Cypherpunk's Manifesto".
- 1997: Hashcash – Adam Back
- 1998: B-Money – Wei Dai
- 2005: BitGold – Nick Szabo
- 2008: Bitcoin – Satoshi Nakamoto

数字现金的问题

Problems with Digital Cash

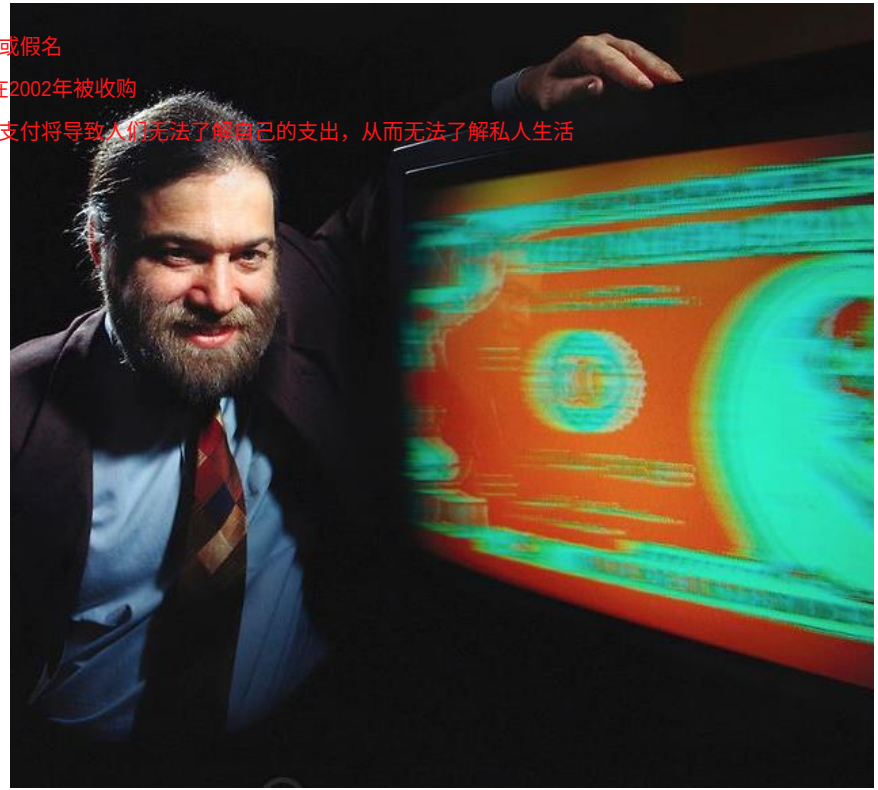
- Identity becomes the new money
  - 身份成为新的财富
  - 对所有个人交易进行全面跟踪
  - 对货币主权的完全账户控制单位
  - 支付封锁和没收变得更容易
  - 彻底消除非正式影子经济
  - 近乎绝对的税收效率
- Full traceability of all personal transactions
- Full unit of account control to the monetary sovereign
- Payment blockades and confiscation become easier
- Total elimination of the informal shadow economy
- Near absolute efficiency in tax collection

Source: https://www.slideshare.net/jonmatonis/bitcoin-cash-becoming-digital

David Chaum - Digicash

发起者:大卫Chaum
1982年:纸“盲签名”
无法追踪的付款”——匿名或假名
•1990年创立Digicash
•Digicash在1998年破产，在2002年被收购
•Digicash专注于匿名交易。
·当时的考虑是，拥有数字支付将导致人们无法了解自己的支出，从而无法了解私人生活

- Originator: David Chaum
- 1982: paper “Blind Signatures for Untraceable Payments” → anonymous or pseudonymous
- Founds Digicash in 1990
- Digicash goes bankrupt in 1998, bought out in 2002
- Digicash focuses on making transactions anonymous.
- The consideration was that having digital payments would lead to undesirable ability to have insight into people’s spendings and thus private life.



A Cypherpunks Manifesto

- Originator: Eric Hughes, 1993
- "Privacy is not secrecy."
- "...privacy in an open society requires anonymous transaction systems."
- "Privacy in an open society also requires cryptography"
- "For privacy to be widespread it must be part of a social contract."

发起者:埃里克•休斯1993年
- “隐私不是秘密。”
- “……开放社会中的隐私需要匿名交易系统。”
- “开放社会的隐私也需要密码学”
- “隐私要广泛传播，就必须成为社会契约的一部分。”

ınk's Manifesto

ın open society in the electronic age. Privacy is not secrecy. A private matter is sor

sort of dealings, then each has a memory of their interaction. Each party can speal
peech at all. If many parties speak together in the same forum, each can speak to al
: to.

we must ensure that each party to a transaction have knowledge only of that whicl
store and hand cash to the clerk, there is no need to know who I am. When I ask r
sage there and how much I owe them in fees. When my identity is revealed by the

pen society requires anonymous transaction systems. Until now, cash has been th
essence of privacy.

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

ments, corporations, or other large, faceless organizations to grant us privacy out
want to be free, it longs to be free. Information expands to fill the available storag

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

Source: https://www.activism.net/cypherpunk/manifesto.html

Adam Back - Hashcash

- Originator: Adam Back

发起者:亚当
•1997:Hashcash的创建，“基于部分哈希冲突的邮费方案”
•垃圾邮件预防系统，让发送者做容易验证的计算(哈希)
•文件明确提到可能违法的
Digicash
•Hashcash成为挖掘算法的基础

- 1997: creation of Hashcash, “A partial hash collision based postage scheme”
- Spam prevention system by making a sender do easily verifiable computations (hashing)
- Paper explicitly referenced possible outlawing of Digicash
- Hashcash becomes the basis of Mining algorithm.

Wei Dai – B-Money

发起者:魏戴
•1998:b货币的创造
•B-Money介绍
-公钥假名
-使用hashcash创造货币
-两种可能的记账方式
•所有参与者检查(PoW)
•服务器提供抵押品((D)PoS)
•缺失:控制货币创造的一种方式
-提出了一些仍然集中的方法

- **Originator: Wei Dai**
- **1998: creation of B-Money**
- **B-Money introduces**
  - Public Key pseudonyms
  - Creation of Money using hashcash
  - Two possible ways of keeping Ledger
    - All participants check (PoW)
    - Servers put up collateral ((D)PoS)
- **Missing: A way to control Money Creation**
  - Proposes a few ways that are still centralized

Nick Szabo - BitGold

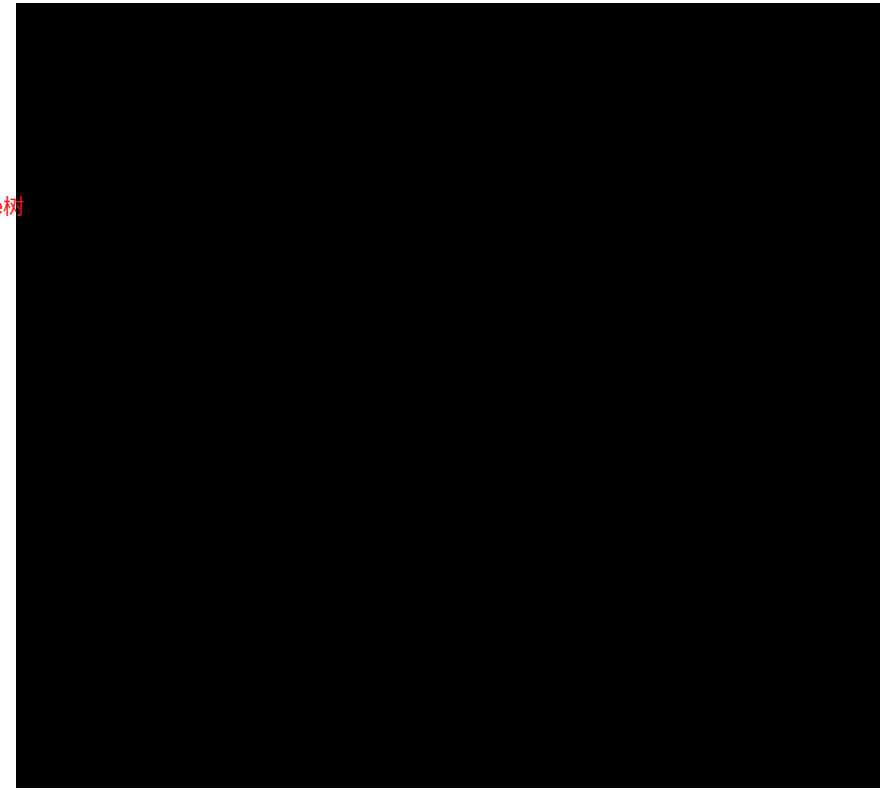
- **Originator: Nick Szabo**
- **1998: inception of Bit Gold**
- **Bit Gold introduces**
  - Timestamping
  - Creation of Money using hashcash
- **Missing: incentives to keep nodes honest**
- **Missing: A way to keep tokens fungible (no agreed way to set difficulty. One token might be made with significantly more difficulty than the other)**

发起者:尼克。萨博
•1998:比特金的开端
•一些黄金介绍
－时间戳
-使用hashcash创造货币
•缺失:保持节点诚实的激励机制
•丢失:一种让代币可替换的方法
(没有商定的方法设置困难。一个代币可能比另一个代币困难得多)

Satoshi Nakamoto - Bitcoin

- **Originator: Satoshi Nakamoto**
- **2008: inception of Bitcoin**
- **2009: Implementation of Bitcoin**
- **Bitcoin uses**
  - Public Key pseudonyms
  - Timestamping
  - Creation of Money using hashcash
  - Roles for nodes: miners are kept honest (difficulty adjustment). Hashing is metric
  - Merkle trees for transaction "batching"

发起者:Satoshi Nakamoto
•2008:比特币的诞生
•2009:比特币的实现
•比特币使用
-公钥假名
－时间戳
-使用hashcash创造货币
节点的作用:矿工是诚实的
(困难的调整)。哈希是规
-用于交易“批量”的Merkle树



Summary

谁发送?从1981年开始，大卫·肖姆(David Chaum)最终成为迪吉卡什(Digicash)
我该寄什么?→Wei Dai, b-money，还有Hal Finney RPOW和Nick
萨博一些黄金。在1997年(hashcash) - 2005年期间提出。
我什么时候发送?中本聪，比特币。通过在网络中添加块和角色，解决了硬币供应不能膨胀以及战俘被重用的问题。

- **Who sends**? → David Chaum, eventually Digicash, starting 1981
- **What do I send**? → Wei Dai, b-money, but also Hal Finney RPOW and Nick Szabo Bit Gold. Proposed in the period 1997 (hashcash) – 2005.
- **When do I send**? → Satoshi Nakamoto, Bitcoin. Solves the way coin supply cannot be inflated as well as PoW being reused by adding blocks and roles in the network.

Whitepaper

Source:
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

Acknowledge History and Background

比特币并不是在2008年或2009年“开始”的
•比特币(以及所有区块链)是一场更大运动的一部分
•它们是解决社会和政治问题的一种技术方式
•它们会进化，但这不意味着要否认它们的起源。

- Bitcoin did not “start” in 2008 or 2009
- Bitcoin (and by extension all blockchains) are part of a much larger movement
- They are a technological manner to solve a social and political problem
- They will evolve, but this should not mean deny their origins.

Bitcoin History

比特币的历史可以分为几个具有代表性的故事
- Pre比特币- 2009:自由主义的梦想和理想
- 2009 - 2010:比特币的早期发展
- 2010 - 2012:丑闻,黑客和非法活动
- 2013 - 2014:比特币吸引注意力
- 2014:商业承兑汇票
- 2013 - 2014:风险创业资助比特币
- 2014 -现在:Ethereum炸毁(以多种方式)
- 2015 -现在:比特币努力扩大规模
- 2015 -现在:从银行“ 区块链 ”上升的兴趣

Bitcoin history broken down into a few representative stories

Pre Bitcoin-2009:	**Libertarian dreams and ideals**
2009-2010:	**The early development of Bitcoin**
2010-2012:	**Scandals, hacks, and illegal activity**
2013-2014:	**Bitcoin attracts attention**
2014:	**Merchant acceptance**
2013-2014:	**Venture funded Bitcoin startups**
2014-Present:	**Ethereum blows up (in multiple ways)**
2015-Present:	**Bitcoin struggles to scale**
2015-Present:	**Rise of interest in “blockchain” from banks**

Pre Bitcoin-2009:
Libertarian Dreams and Ideals

Libertarian Dreams

与技术的进步在90年代和1980年代,Cypherpunk运动形成
•Cypherpunk宣言:“在电子时代的一个开放的社会，隐私是必要的。”
•植根于自由意志主义和密码学
〇自由主义是主张不侵略原则和自由放任政府的政治意识形态
〇密码学是在第三方存在的情况下确保通信安全的科学

- With the advance of technology in the 1980s and 90s, the Cypherpunk movement came into being
- Cypherpunk Manifesto: “Privacy is necessary for an open society in the electronic age.”
- Roots in libertarianism and cryptography
  - Libertarianism is a political ideology advocating the non-aggression principle and laissez faire government
  - Cryptography is the science of securing communication in the presence of third parties

Cypherpunks and Crypto-Anarchists

密码朋克痴迷于科技将如何改变个人和国家之间的关系
对人们拥有的新工具充满希望，但关心的是人们如何保护自己的个人信息并保护自己的隐私不受政府的侵犯

- Cypherpunks were obsessed over how technology would change the relationship between the individual and the state
- Hopeful about the new tools people had but concerned about how people could protect their personal information and maintain their privacy from government

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 McCullagh (2002)

Changing Money

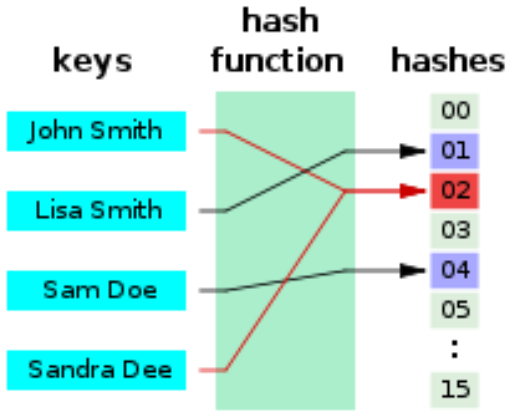
现有的金融体系被视为对个人隐私的最大威胁之一
➢DigiCash是cryptocurrencies早期最著名的例子
➢DigiCash的发明者,大卫•Chaum使用公开密匙加密
然而,DigiCash是中央组织,这意味着Chaum的公司需要确认每一个数字签名。
➢最终，乔姆的公司破产了，DigiCash也跟着破产了

- The existing financial system was viewed as one of the greatest threats to individual privacy
- **DigiCash** is the most famous example of the early cryptocurrencies
- The inventor of DigiCash, David Chaum, used public-key cryptography
- However, DigiCash was a central organization, meaning that Chaum's company needed to confirm every digital signature.
- Eventually, Chaum's company went bankrupt and DigiCash went down with it

Crypto-Innovation

- Cypherpunks also worked on technological innovations, including the cryptographic hash function.
- **A hash function is a math equation that is easy to solve but hard to reverse-engineer.**
- The early experiments of the Cypherpunks continued to hit hurdles that resulted in failure

· cypherpunk还致力于技术创新，包括加密哈希函数。
· 一个哈希函数是一个数学方程,很容易解决,逆向工程难。
· 密码朋克的早期实验不断遇到障碍，最终以失败告终



2009-2010:
The early development of Bitcoin

WHO IS?

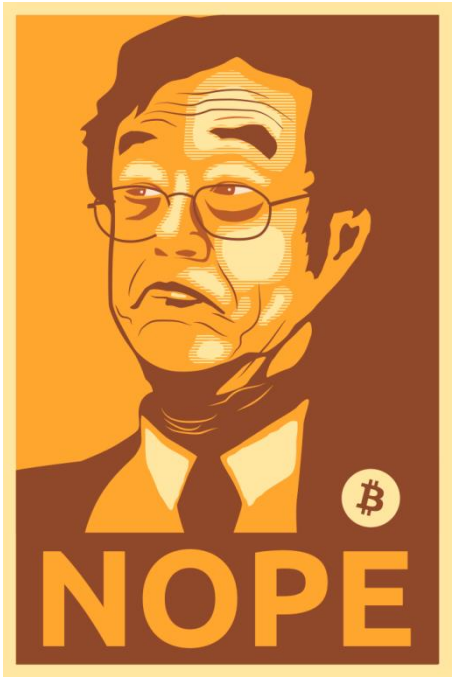
SATOSHI NAKAMOTO

Dorian Satoshi Nakamoto

Satoshi Nakamoto and Bitcoin

中本聪(Satoshi Nakamoto)是比特币的匿名创造者，他撰写了一份长达9页的白皮书，出色地结合了之前的所有努力，创造了一种自我维持的数字货币。
尽管一些人对历史感到失望，对货币持悲观态度，但一些早期的先驱支持该项目，认为它可以解决他们过去的问题

- Satoshi Nakamoto is the anonymous creator of Bitcoin who wrote a nine-page white paper that brilliantly combined all previous efforts to create a self-sustaining digital money.
- Although some, disheartened by history, were bearish on the currency, a few of the early pioneers supported the project as the solution to their past problems



Genesis Block

成因区块开采于2009年1月3日
创世纪积木的硬币底座参考了伦敦《泰晤士报》上一篇有关财政大臣救助银行的报道
2009年1月12日第一次比特币交易与哈尔芬尼

- Genesis block mined Jan 3, 2009
- The coinbase of the genesis block references a story in the Times of London newspaper involving the Chancellor bailing out banks
- First bitcoin transaction on Jan 12, 2009 with Hal Finney

Block 0

Short link: http://blockexplorer.com/b/0

Hash: 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Next block: 00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048

Time: 2009-01-03 18:15:05

Difficulty: 1 ("Bits": 1d00ffff)

Transactions: 1

Total BTC: 50

Size: 285 bytes

Merkle root: 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

Nonce: 2083236893

Raw block

Transactions

Transaction	Fee	Size (kB)	From (amount)	To (amount)
4a5e1e4baa...	0	0.204	Generation: 50 + 0 total fees	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa: 50

The Six Million Dollar Pizza

- On May 21, 2010, Laszlo Hanyecz purchased $25 worth of pizza for 10,000 BTC
- This was the world's first ever Bitcoin transaction for a tangible asset
- 10,000 BTC is now equivalent to $5,790,000

2010年5月21日，Laszlo Hanyecz用1万个比特币买了价值25美元的披萨
➢这是世界上第一个比特币交易的有形资产
➢10000 BTC现在相当于5790000美元

2010-2012:
Scandals, Hacks, Illegal activity

Mt. Gox

2010年Mt. Gox成立并巩固了自己作为比特币初期最大的比特币交易所的地位。
在6/19/11,Mt. Gox遭受了严重的安全漏洞，导致了欺诈交易，网站被关闭了7天。
2014年，Mt. Gox在一场盗窃中丢失了744,408枚比特币，多年来一直未被发现
最终，Mt. Gox宣布破产

- In 2010 Mt. Gox was established and consolidated itself as the biggest bitcoin exchange during the beginning stages of bitcoin.
- On 6/19/11, Mt. Gox suffered a significant breach of security that resulted in fraudulent trading and required the site to be shut down for seven days.
- In 2014, Mt. Gox lost 744,408 bitcoins in a theft that went unnoticed for years
- Eventually, Mt. Gox declared bankruptcy

Silk Road

2011年2月，“丝绸之路”开始营业:比特币市场“丝绸之路”推出了一个非法毒品交易市场，名为“毒品eBay”。
2013年10月,美国联邦调查局(FBI)关闭了丝绸之路,抓住3.6M美元的比特币
“丝绸之路”的创始人罗斯·乌布里希(Ross Ulbricht)目前被判终身监禁，不得假释

- On February 2011, Silk Road opened for business: Silk Road, a Bitcoin marketplace, launched an illicit marketplace for drug deals, called the eBay for drugs.
- On October 2013, the FBI shut down Silk Road, seizing 3.6M dollars worth of bitcoin
- Ross Ulbricht, the founder of Silk Road, is currently serving a life sentence without possibility of parole

Silk Road

anonymous market

messages 0 | orders 0 | account B0

Search Go

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

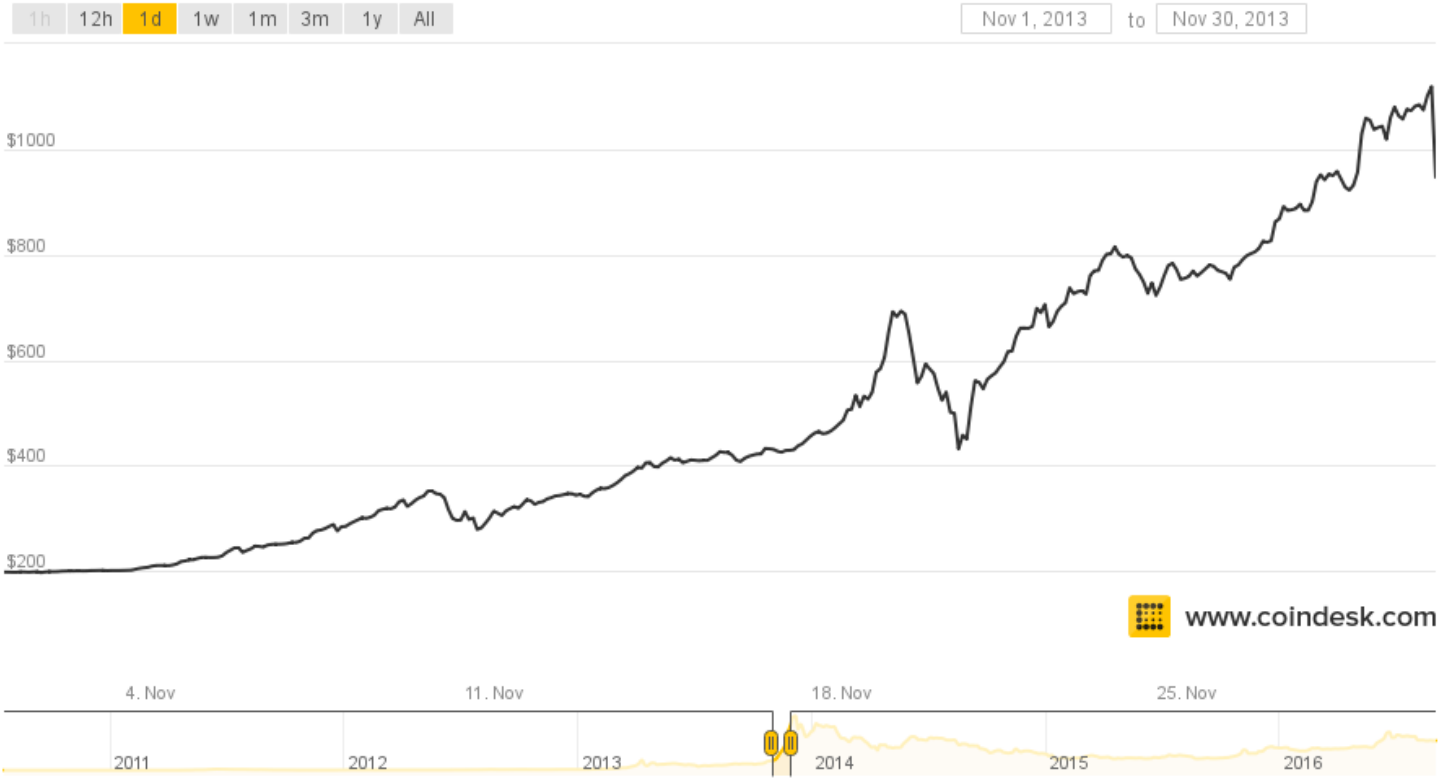
฿11.58

1/4 oz G13

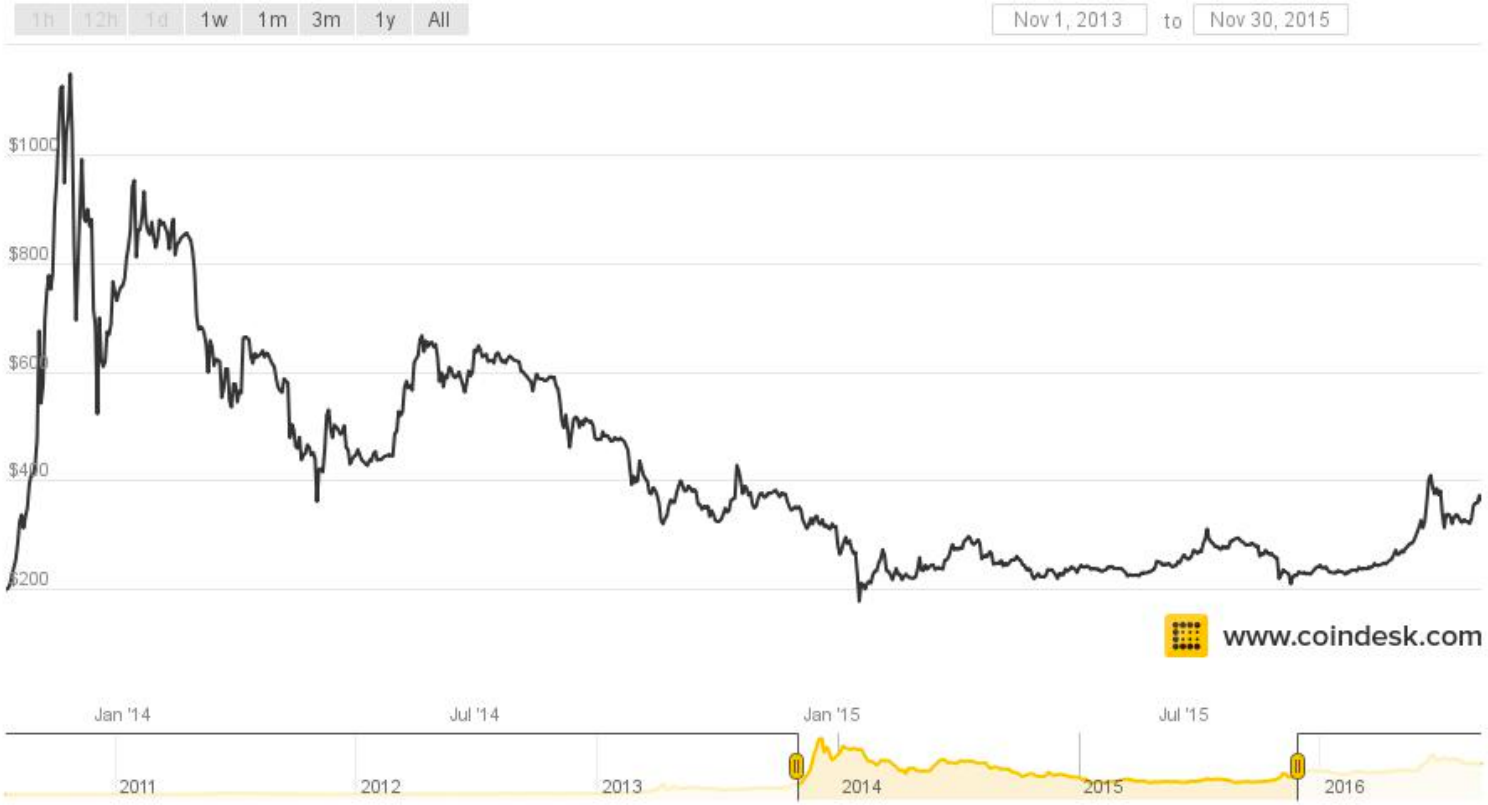
฿8.13

Bitcoin Bubble and Burst

比特币泡沫与破灭



Bitcoin Price Bubble and Burst



2013-2014:
Bitcoin attracts attention

Hype

(From CoinDesk)

(从CoinDesk)
2014年2月，Mt. Gox据称损失了3.5亿美元比特币(744,400比特币)，据传已经资不抵债
2014年3月，比特币发明者中本聪在加州“被发现”
2014年9月，蒂姆·德雷珀:比特币的价格仍朝着1万美元的方向前进

- 2014 Feb. Mt. Gox Allegedly Loses $350 Million in Bitcoin (744,400 BTC), Rumored to be Insolvent
- 2014 Mar. Bitcoin Inventor Satoshi Nakamoto 'Found' in California
- 2014 Sep. Tim Draper: Bitcoin's Price Still Headed to $10k

Merchant Acceptance 商业承兑汇票

色情网站接受比特币
2014年1月，Overstock.com成为第一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贩卖机将接受比特币
2014年9月，PayPal与比特支付、Coinbase合作
微软接受比特币支付
(2014年10月)“谁说比特币买不到东西？”...
Shitexpress是一项服务，它会将装有马粪的特百惠塑料容器寄给你，并为你附上个性化的信息。——CoinDesk

(From CoinDesk)

- 2014 Jan. Porn.com accepts Bitcoin
- 2014 Jan. Overstock.com Becomes First Major Retailer to Accept Bitcoins
- 2014 Apr. New Colorado Marijuana Vending Machines Will Accept Bitcoin
- 2014 Sep. PayPal partners with and Coinbase, BitPay
- 2014 Dec. Microsoft accepts Bitcoin payments
- (2014 Oct.) "Whoever said that bitcoin couldn't buy you things? ...

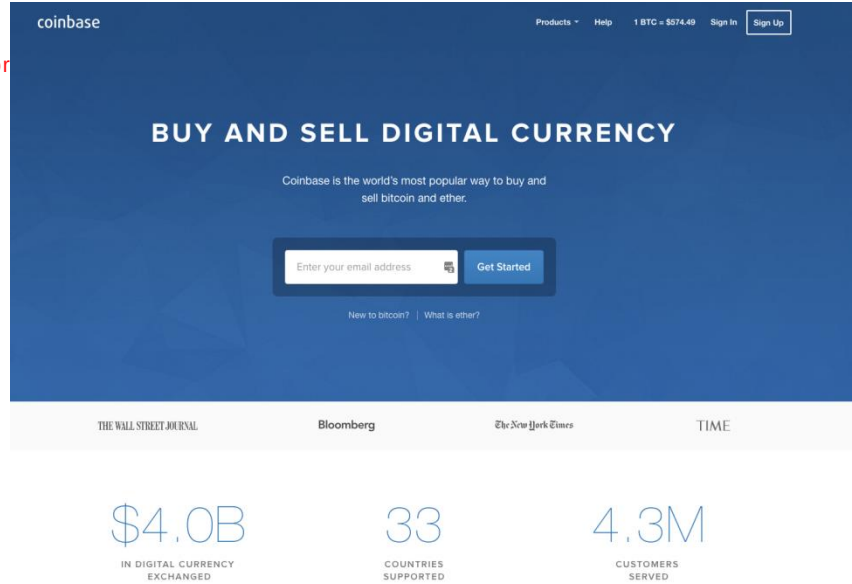
Shitexpress is a service that mails a tupperware container of horse manure with a personalized message on your behalf. - CoinDesk

2013-2014:
Venture funded Bitcoin Startups

Coinbase

Coinbase的大小代表投资者的利益
在线钱包和交换
Coinbase成立于2012年6月，注册于2012年夏季Y Combinator
2013年5月:500万美元A系列
2013年12月:2500万美元
2015年7月:7500万美元

- Coinbase size representative of investor interest
- Online wallet and exchange
- Coinbase founded June 2012, enrolled summer 2012 Y Combinator
- May 2013: $5 mil Series A
- December 2013: $25 million Series B
- July 2015: $75 million Series C



coinbase

风险投资创业公司的崛起

Rise of venture funded startups

Coinbase:主持的钱包
➢BitFinex:在线交换/交易平台
➢21公司:与嵌入式采矿机付款
➢BitPay:允许商家接受比特币支付,转换为美元
➢ChangeTip:社会比特币小额支付
➢Blockstream:比特币核心、Sidechains研究

- Coinbase: Hosted wallet
- BitFinex: Online exchange / trading platform
- 21 Inc: machine payments & embedded mining
- BitPay: allows merchants to accept Bitcoin for payment, convert to USD
- ChangeTip: social bitcoin micropayments
- Blockstream: Bitcoin Core, Sidechains, Research

PANTERA

BLOCKCHAIN CAPITAL

ANDREESSEN HOROWITZ

Seed Rounds

- 26-Apr-2013 Coinbase
- 13-Mar-2014 Xapo
- 26-Mar-2014 Circle Internet Financial
- 21-Apr-2014 Coinalytics
- 16-Jun-2014 Bitgo
- 20-Aug-2014 Chain
- 7-Oct-2014 Blockchain
- 2-Dec-2014 ChangeTip

2014-Present:
Ethereum Blows Up (in multiple ways)

Ethereum blows up (in multiple ways)

Bitcoin is based off simple scripting language. Ethereum is a Turing-complete version of Bitcoin. Potential for complex decentralized apps

History

- Late 2013: Ethereum described in whitepaper by Vitalik Buterin
- July and August 2014: Ethereum crowdsale
- July 30th 2015: Ethereum blockchain launched
- May 2016: Value of Ethereum tokens worth more than $1 billion

Huge potential for new governance models

- July 2016: The DAO rise and hack

比特币基于简单的脚本语言。Ethereum是图灵完整版的比特币。复杂的去中心化应用的潜力
历史
➢2013年底:白皮书中描述Ethereum Vitalik Buterin
➢2014年7月和8月:Ethereum crowdsale
➢2015年7月30日:Ethereum区块链
➢2016年5月:Ethereum标记价值超过10亿美元的价值
新的治理模式潜力巨大
➢2016年7月:DAO上升和黑客

2015-Present: Bitcoin Struggles to Scale

Blocksize Debate

每10分钟创建一个比特币块
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
划分社区-块大小辩论
意义:提出分散治理、控制的问题
社区和监管

- Bitcoin blocks created every 10 minutes
- In 2010, blocksize limit reduced to 1 MB
- In 2015, Bitcoin blocks started to "fill up"
- Huge scalability problem
- Divided the community - Blocksize Debate
- Significance: Raised questions on decentralized governance, control
- Community and regulation

Lightning Network

Lightning网络是最流行的可伸缩性解决方案
允许安全支付，而不触及区块链
可伸缩性
了解哈希时间锁合同，状态通道，检查锁定时间验证

- The Lightning Network is the most popular proposed solution to scalability
- Allows secure payments without hitting the blockchain
- Scalability
  - Learn about Hashed timelock contracts, state channels, CheckLockTimeVerify

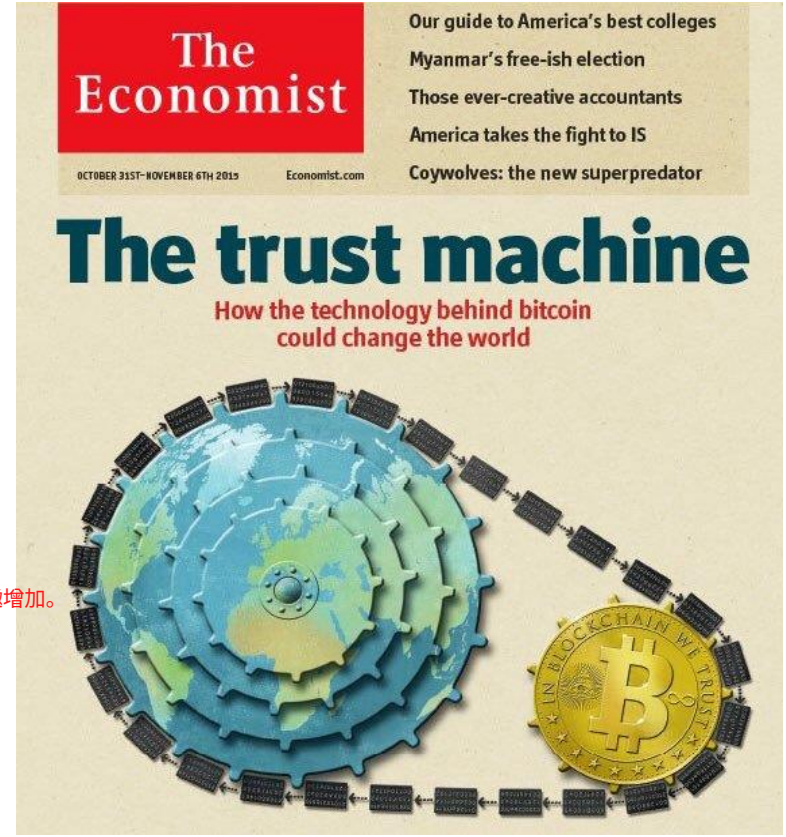
Interest in "blockchain" from banks

银行对区块链的兴趣

Interest in "blockchain" from banks

- **Rise of interest in "private blockchains" or "permissioned ledgers."**
  - Not open
  - Not trustless
  - No economic incentives like in Bitcoin
  - Separate "blockchain" from "Bitcoin"
- **Con:**
  - Often doesn't use consensus
  - Glorified public key cryptography
- **Benefit: More compliant**

对“私有区块链”或“授权账簿”的兴趣增加。
〇不开放
〇不是不可靠的
〇没有像比特币那样的经济激励
〇把“区块链”和“Bitcoin”分开
➢反对:
〇通常不使用共识
〇荣耀公钥密码术
好处:更多的兼容



"Private Blockchain" Initiatives

- **R3CEV**
  - Start Sept 2015
- **Chain**
  - Startup collaborating with financial firms on building an open standard
- **Digital Asset Holdings**
  - Founded by Blythe Masters
- **Hyperledger Project: Open source blockchain**
  - Run by Digital Asset Holdings and the Linux Foundation
- **IBM Open Blockchain**
  - Now part of Hyperledger project as "Fabric"
- **JP Morgan Juno project**

R3CEV
- 2015年9月开始
- 链
- 创业公司与金融机构合作建立一个开放的标准
- 数字资产控股有限公司
- 由布莱斯创办
- Hyperledger项目：开源区块链
- 由数字资产控股和Linux基金会
- IBM开放区块链
- 现在Hyperledger项目的一部分“织物”
- 摩根大通朱诺项目

Jamie Dimon Quotes on Bitcoin/blockchain

#衡量大型金融机构是如何看待区块链的一个方法是看看摩根大通首席执行官杰米·戴蒙在过去的一段时间里说了些什么
2014年1月：“ 这是一种糟糕的价值储存方式。它可以被一遍又一遍地复制。”
人们仍然不理解比特币

One way to gauge how large financial institutions came to view blockchain is to look at what Jamie Dimon, the CEO of JP Morgan Chase, has said over time

Jan 2014: "It's a terrible store of value. It could be replicated over and over."

People still don't understand Bitcoin

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

http://www.businessinsider.com/jp-morgans-jamie-dimon-on-bitcoin-2014-1

Jamie Dimon Quotes on Bitcoin/blockchain

2014年10月：“（比特币开发商）将试图吃掉我们的午餐。这很好。这就是竞争，我们将会竞争。承认比特币的合法性

Oct 2014: "[Bitcoin developers] are going to try and eat our lunch. And that’s fine. That’s called competition, and we’ll be competing.”

Conceding legitimacy to Bitcoin

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

Jamie Dimon Quotes on Bitcoin/blockchain

2015年11月:虚拟货币比特币对美元，这将被停止……没有哪个政府会支持一种没有同样控制的跨境虚拟货币。这是不会发生的。
银行家们痛恨缺乏控制。也许威胁

Nov 2015: “Virtual currency, where it’s called a bitcoin vs. a U.S. dollar, that’s going to be stopped. ... No government will ever support a virtual currency that goes around borders and doesn’t have the same controls. It’s not going to happen.”

Bankers hate the lack of control. Perhaps threatened?

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

Jamie Dimon Quotes on Bitcoin/blockchain

2016年2月:区块链是一项我们一直在研究的技术……是的，这是真的。在某些方面，它可能会降低实际应用的成本……如果它被证明既便宜又安全，它将被广泛采用。”
将“区块链”从“比特币”分离

February 2016: “The Blockchain is a technology, which we’ve been studying ... and yes it’s real. It could probably reduce the cost of real application in certain things. ... If it proves to be cheap and secure it will be adopted for a whole bunch of stuff."

Separate "blockchain" from "Bitcoin"

Historical Perspective

比特币是一个非常具体的问题的解决方案。它可能有政治上的影响，但它是一个工程上的解决方案

Bitcoin is a solution to a very specific problem. It may have political ramifications, but it is an engineering solution

人们倾向于将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(上下文定义为“快速”)
•分叉的各种新定义
•社会议程(无论哪个)(即:定义“公平”)
•各种特征的可取性(定义社会选择契约)
•治理(定义什么是治理)
•这些都不是比特币的目标

Retconning blockchain

- There is a tendency to project one’s ideals and ideology onto Bitcoin and blockchain

- “Fast” Transactions (define fast in context)
- Various new definitions of forks
- Social agenda (whichever) (ie. define “fair”)
- Desirability of various features (define social contract of choice)
- Governance (define what is governance)

- None of these are aims of Bitcoin

为了交谈，我们需要学会定义

We need to learn to define in order to talk

1. The cryptocurrency space is rife with vague and confusing definitions: cash, currency, fast, secure etc.
2. In order to talk about these things, we need to define these terms clearly, either on a per debate basis, or in general terms in context
3. If we do not, we will continue to be vulnerable to social attacks by bad actors who want to confuse our discourse with confusing statements, inciting discord instead of honest disagreements
4. We can always disagree once we have clear definitions. There is no need at all to be in agreement of aims. However, in order to test our systems, we need to be completely open and clear about what the testing parameters are.
5. Without that clarity, we are bound to clash without any constructive dialogue.

1.加密货币领域充斥着模糊和令人困惑的定义:现金、货币、快速、安全等。
2。为了讨论这些事情，我们需要在每次辩论的基础上或在上下文中对这些术语作出明确的定义
3.如果我们不这样做，我们将继续受到不良行为者的社会攻击，他们想用混乱的言论混淆我们的言论，煽动不和，而不是真诚的分歧
4. 一旦我们有了明确的定义，我们总是会产生分歧。根本没有必要就目标达成一致。然而，为了测试我们的系统，我们需要对测试参数是什么完全开放和清楚。
5. 如果没有这种明确，我们肯定会在没有任何建设性对话的情况下发生冲突

Sources

- Untraceable Electronic Cash, David Chaum: http://blog.koehntopp.de/uploads/chaum_fiat_naor_ecash.pdf
- Blind Signatures for Untraceable Payments, David Chaum: http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF
- A Cypherpunk's Manifesto, Eric Hughes: https://www.activism.net/cypherpunk/manifesto.html
- hash cash postage implementation, Adam Back: http://www.hashcash.org/papers/announce.txt
- B-Money, Wei Dai: http://www.weidai.com/bmoney.txt
- Reusable Proofs of Work, Hal Finney: https://web.archive.org/web/20071222072154/http://rpow.net/
- Secure Property Titles with Owner Authority, Nick Szabo: http://nakamotoinstitute.org/secure-property-titles/#selection-6.0-6.1
- Bit Gold, Nick Szabo: https://unenumerated.blogspot.nl/2005/12/bit-gold.html
- Bitcoin Whitepaper, Satoshi Nakamoto: https://bitcoin.org/bitcoin.pdf
- Various posts by Samuel Falkon: https://www.linkedin.com/in/samuel-falkon-467a878b/detail/recent-activity/posts/
- Bitcoin and the Rise of the Cypherpunks, Coindesk: https://www.coindesk.com/the-rise-of-the-cypherpunks/
- BITCOIN: POLITICAL ATTACK VECTORS AND COMMON MISCONCEPTIONS, Giacomo Zucco: https://youtu.be/jgwW7XZCKPU

END !


धन्यवाद
Hindi
多謝
Traditional Chinese
ขอบคุณ
Thai
Спасибо
Russian
Gracias
Spanish
Thank You
English
شكراً
Arabic
Obrigado
Brazilian Portuguese
多谢
Simplified Chinese
Danke
German
Grazie
Merci
French
நன்றி
Tamil
ありがとうございました
Japanese
감사합니다
Korean