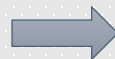
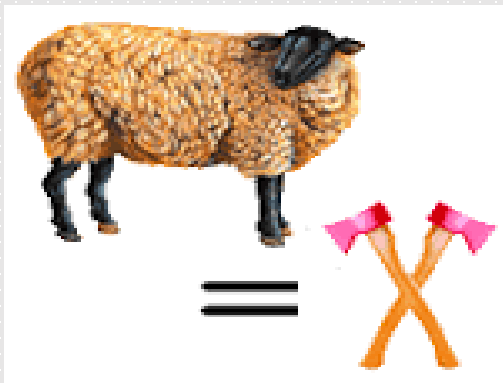


1.6 比特币：人类首次区块链 大规模社会实验

01

从物物交换到比特币



比特币，顾名思义，就是一种货币，跟人民币一样，是一种商品交换的媒介。

02

比特币

□ 2008年10月31日

Satoshi Nakamoto（中本聪）发表《Bitcoin: A Peer-to-Peer Electronic Cash System》

□ 2009年1月3日

比特币发行、交易和账户管理系统开始运行

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

Block #0

Summary		Hashes	
Number Of Transactions	1	Hash	00000000019d6689c085ae165831e9348763ae46a2a6c172b3f1b60a8ce26f
Output Total	50 BTC	Previous Block	00
Estimated Transaction Volume	0 BTC	Next Block(s)	00000000839ae6886ab5951d76f411475428afc90947ee320161bbf18eb0648
Transaction Fees	0 BTC	Merkle Root	4a5e1e4baab893a32518a88c31bc87f618776673e2cc77ab2127b7afdeda33b
Height	0 (Main Chain)		
Timestamp	2009-01-03 18:15:05		
Received Time	2009-01-03 18:15:05		
Relayed By	Unknown		
Difficulty	1		
Bits	486604799		
Size	0.285 KB		
Version	1		
Nonce	2083236893		
Block Reward	50 BTC		

Transactions

4a5e1e4baab89f3a32518a88c31bc87f618776673e2cc77ab2127b7afdeda33b		2009-01-03 18:15:05
No Inputs (Newly Generated Coins)		1A1zP1eP5QGefi... (Genesis of Bitcoin) 50 BTC

- ❑ 20世纪90年代初，互联网上悄然兴起了一个神秘的组织，叫做“密码朋克”。这个组织是一个由全球密码天才和黑客组成的松散联盟，维基解密的创始人阿桑奇就是密码朋克的核心成员之一。
- ❑ 他们不信任政府、公司或者其他组织在电子信息时代对于隐私的保护机制，希望通过密码学自行做出一个软件，来保护个人隐私。正是这个组织在十几年后，在全球掀起一场数字货币的大风暴。
- ❑ 2008年9月，金融危机席卷全球，世界各国为了应对危机，开始量化宽松政策，超发的货币开始大量稀释民众手中的财富，这使得美国引发了一系列抗议活动，比特币正是在这个时候登上历史舞台。

应用



比特币 Bitcoin

- 全球数字货币
- 比特币交易波动性大、流动性高，
受高频交易及对冲基金的喜爱

技术基础

去中心化

分布式
记录存储

区块链 Blockchain

- 经密码加密的完备分布式总账
- 在需要第三方监管的中介网络及清算系统
中发挥潜力
- 向其他需要较高信任机制的应用领域延伸

比特币不依靠指定的货币发行机构，而依据特定算法，通过大量的计算产生，也就是我们熟知的“挖矿”。在这个过程中，需要损耗大量的算力，付出大量电费、人工费、管理费用，这使得比特币在诞生的过程中附加了太多的价值。

基于密码学的设计，可以使比特币只能被真实的拥有者转移和支付，这同样确保了货币所有权与流通交易的匿名性。比特币与其他虚拟货币最大的不同，是它总数量有限，具有极强的稀缺性，比特币的总数量在最初设定时，就被系统永久限制在2100万个。

说说你与区块链的故事