# 区块链技术与应用

## 第十八讲 比特币：开启区块链江湖

主讲人：赵其刚

# 比特币


比特币

# 比特币的发展历史

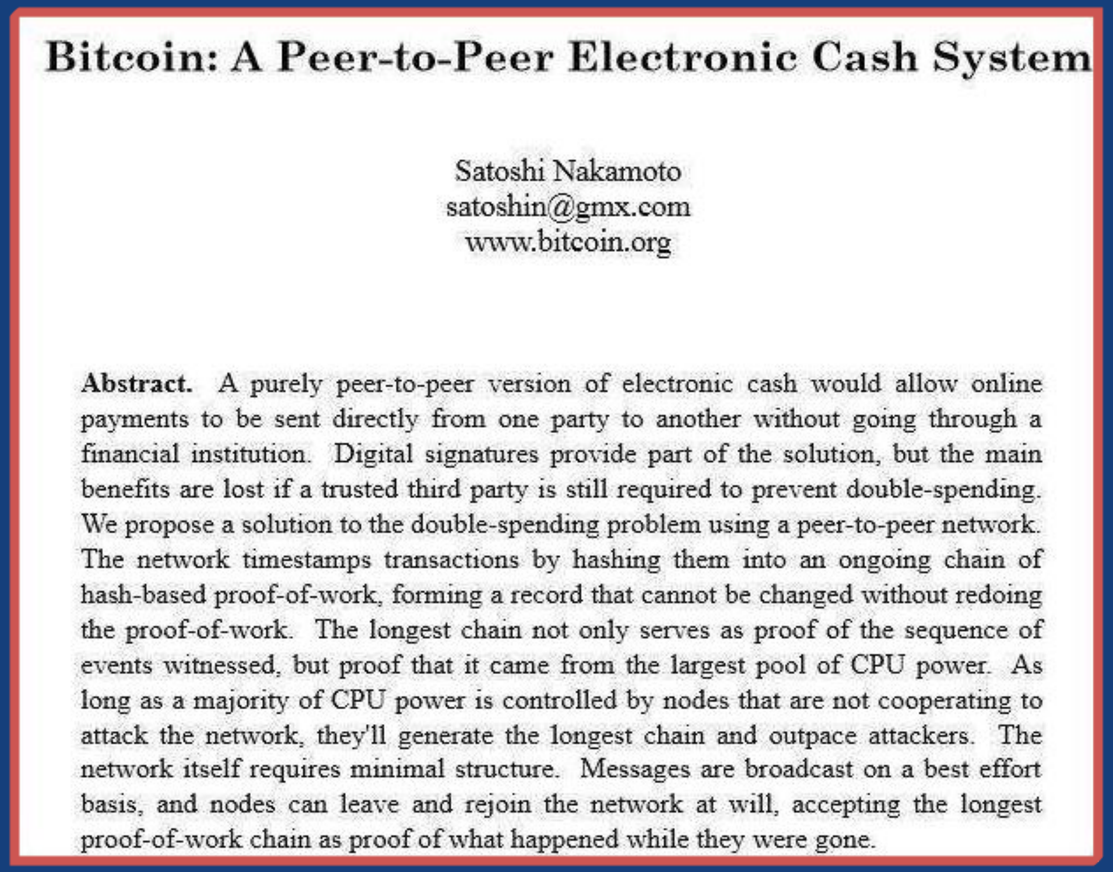
## Bitcoin: A Peer-to-Peer Electronic Cash System

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.

- 比特币的概念和解决方案

# 比特币的发展历史



**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.

结合多个数字货币发明，如**B-money**和**HashCash**，创建一个完全去中心化的电子现金系统。

- 比特币的概念和解决方案

# 比特币的发展历史

分布式计算系统（“工作量证明”算法）

- 每隔10分钟进行一次的全网“选拔”，能够使去中心化的网络同步交易记录。

# 比特币是一种区块链应用

- 比特币是一种协议、一种网络、一种分布式计算创新的代名词，是区块链技术的典型和开创性应用。

比特币系统依赖于完全透明的数学原理

分布式计算 | 经济学 | 计量经济学领域

# 比特币的生产过程

比特币是一个分布式的点对点网络系统

- 没有“中央”服务器，也没有中央发行机构

“挖矿”

- 验证比特币交易的同时参与竞赛来解决一个数学问题

# 比特币的生产过程

平均每10分钟就有人能验证
过去这10分钟发生的交易

新币

本质

- 挖矿把央行的货币发行和结算功能进行分布式，用全球化的算力竞争来取代对中央发行机构的需求。

# 比特币的生产过程

**比特币的本质** ▶ 一堆复杂算法所生成的特解

- 特解是指方程组所能得到有限个解中的一组。
- 每一个特解都能解开方程并且是唯一的。

# 比特币的生产过程


比特币=钞票的冠字号码

挖矿的过程：通过庞大的计算量不断的去寻求这个方程组的特解，被设计成了只有2100万个特解，比特币的上限就是2100万个。

# 比特币的生产过程

## 挖掘比特币

下载专用的比特币运算工具 → 注册各种合作网站 → 把注册来的用户名和密码填入计算程序中 → 点击运算就正式开始

# 比特币的生产过程

完成Bitcoin客户端安装 → 获得一个Bitcoin地址

安装好比特币客户端 → 分配一个私钥和一个公钥

- 需要备份包含私钥的钱包数据，保证财产不丢失。
- 若不幸格式化硬盘，个人比特币将会完全丢失。

# 比特币的关键技术

## 关键的创新点

1. 去中心化的点对点网络（比特币协议）
2. 公共的交易账簿（区块链）
3. 去中心化的数学的和确定性的货币发行（分布式挖矿）
4. 去中心化的交易验证系统（交易脚本）

# 比特币的软件构成

- 比特币的软件主要包括：

路由 | 区块链数据库 | 挖矿 | 钱包服务

# 比特币的软件构成

- 一个完整的比特币节点软件包括：

# 比特币的节点

- 比特币节点：都具有全网络的路由功能，参与验证并传播交易及区块信息，发现并维持与对等节点的连接。

“全节点” 保有一份完整的、最新的区块链数据备份的节点

全节点能够独立自主地校验所有交易，而不需借由任何外部参照

# 比特币的挖矿

**矿节点**（比特币区块封装节点）

- 运行工作量证明（**proof-of-work**）算法，以相互竞争的方式创建新的区块。

部分挖矿节点 = 全节点，保有区块链的完整拷贝

- 参与矿池挖矿的节点是轻量级节点，依赖矿池服务器维护的全节点进行工作。

# 比特币的实质

## 用户钱包

- 用户接入比特币网络的交互软件，用于桌面客户端进行比特币的转帐及比特币区块链的数据查询操作。

# 比特币的软件实现

开源的比特币软件主要采用C++语言编写

- 区块数据处理
- 哈希计算
- 块创建
- 块验证
- 挖矿
- 工作量证明
- 比特币奖励
- P2P网络

# 比特币

比特币：区块链的一种开创性应用，其发展与运行历程证明了区块链技术的安全性、可靠性与稳定性，以及构建“信任”网络的可行性。

# 比特币

- 计算机科学家TedNelson周日在网络上发布视频称：

比特币的创始人是京都大学数学教授
望月新一（Shinichi Mochizuki）

假名：中本聪（Satoshi Nakamoto）

# 比特币


望月新一

- 高中就读于菲利普埃克塞特学院
- 16岁进入美国普林斯顿大学
- 22岁时以博士身份离校
- 33岁就成为正教授

# 比特币


- 2014年3月7日，传闻比特币创始人是多利安·中本

# 比特币


## 猜测

- “中本聪”是个真实的名字
- 一名64岁的日裔美国人
- 喜欢收集火车模型
- 曾供职大企业和美国军方

# 比特币

猜测

多利安·普伦蒂斯·中本聪（Dorian Prentice Satoshi Nakamoto）

多利安·中本S（Dorian S. Nakamoto）

# 比特币

# 比特币

- **2014年9月9日， eBay宣布， 该公司子公司Braintree将开始接受比特币支付。**

该公司已与比特币交易平台**Coinbase**达成合作

# 比特币

eBay市场交易平台

PayPal业务

旅行房屋租赁社区Airbnb

租车服务Uber

- Braintree的主要业务：面向企业提供支付处理软件，该公司在2013年被eBay以大约8亿美元的价格收购。

# 比特币

- **2017年1月22日晚间**

火币网、比特币中国与OKCoin币行称

为抑制投机，防止价格剧烈波动，2017年1月24日中午12：00起收取交易服务费，服务费按成交金额的0.2%固定费率收取，且主动成交和被动成交费率一致。

- **2017年5月5日**

OKCoin币行网的2017年数据显示，比特币的价格刷新历史，最高触及9222元人民币高位。

# 比特币

- **2017年1月24日中午12：00起**

  中国三大比特币平台正式开始收取交易费。

- **2017年9月4日**

  央行等七部委发公告称中国禁止虚拟货币交易。

- **2017年12月17日**

  比特币达到历史最高价**19850**美元。

- **2018年11月25日**

  比特币跌破**4000**美元大关，现稳定在**3000**多美元。

# 比特币

- **2019年4月**

  比特币再次站上5000美元大关，创年内新高。

- **2019年5月12日**

  比特币近八个月来首次突破7000美元。

- **2019年5月14日**

  据coinmarketcap报价显示，比特币站上8000美元，24小时内上涨14.68%。