区块链

占文(Zion) 2025.11.10

一页历史

- 公元前3000年，美索不达米亚的借贷
- 公元前600年，吕底亚王国金属货币
- 中世纪，美第奇家族商业银行
- 1602年，荷兰东印度公司发行股票
- 1694年，英国央行成立，（贵金属）信用纸币
- 19世纪，工业革命与现代保险、投资银行
- 1944年，布雷顿森林体系建立，**美元黄金**
- 1971年，美元脱钩黄金，（债务）信用纸币
- 2008年，比特币横空出世、**无中生有**
- ……

一种观点

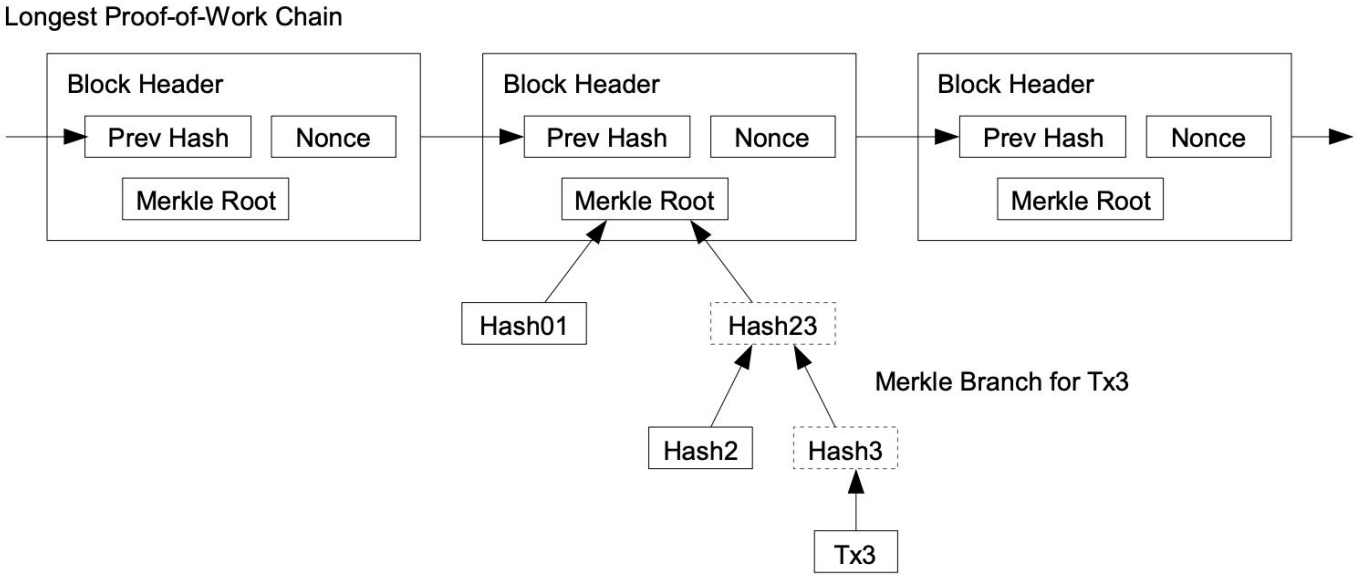
- 金融的本质是记账
  - 在公元前3000年的泥板上，记录谁欠谁多少谷物或银子
  - 一切金融都是“账本的延伸”
    - 货币是实物账本
    - 银行是中央账本
    - 区块链是分布式账本
- 记账是一种权力
  - 谁有资格定义、记录并被承认“谁欠谁、值多少”
  - 当央行修改利率时，实际上是在改写整个经济体的账本结构
- **货币是记账单位**
  - 谁定义记账单位，谁就拥有货币主权
    - 欧元、支付宝/微信，数字人民币、比特币
    - 货币的本质是“共同认可的记账单位”
      - 兼顾交换媒介、价值存储

一个名字

- 中本聪(Satoshi Nakamoto)
  - 中本聪的帖子
- 比特币:一个点对点**电子现金**系统
  - Proof-of-Work:无许可、去中心化的共识系统
    - 算力投票、概率共识
  - 每隔四年，产量减半
    - `50 -> 25 -> 12.5 -> 6.25 -> 3.125 -> … -> 0`
- 中本聪说
  - 2010-02-14 `I'm sure that in 20 years there will either be very large transaction volume or no volume.`
  - 2010-07-29 `If you don't believe me or don't get it, I don't have time to try to convince you, sorry.`
  - 2014-03-07 `I am not Dorian Nakamoto.`

一个区块

- 创世区块的内容
  - 时间印戳:1231006505 -> Sun Jan 04 2009 02:15:05 UTC+8
  - 事件证明：The Times 03/Jan/2009 Chancellor on brink of second bailout for banks



一把钥匙

- 非对称密码学
  - 如何安全地在不安全信道上 传递信息？
    - 无法窥探
    - 不可篡改
- 数学难题
  - 非对称原理：“易守难攻”
    - 质因数分解，离散对数、多项式
      - 关键是足够高的随机墒（反例：诈骗集团陈志被偷家）
    - 无公式解，只能暴力求解 (Brute-force)
      - 国家级算力也无可奈何
- 未来风险
  - 量子计算机
  - 新的数学工具

如何才能理解比特币？

- 密码学
- 概率论
- 分布式系统
- P2P网络
- 货币理论
- 经济学原理
- 博弈论
- ……

那么，你认为中本聪是个人还是团队？

一些书籍

《货币未来》

《精通比特币》

《精通以太坊》

《应用密码学》