去中心化数字货币应用挑战

徐刚

上海策赢网络科技有限公司

新星——去中心化数字货币

- 比特币市值1400亿人民币
- 以太坊市值300亿人民币
- 达世币
- 零币
- 央行数字货币

- 全球自由流通
- 不可随意增发
- 不可篡改
- 账本公开
- 匿名性
- 智能合约

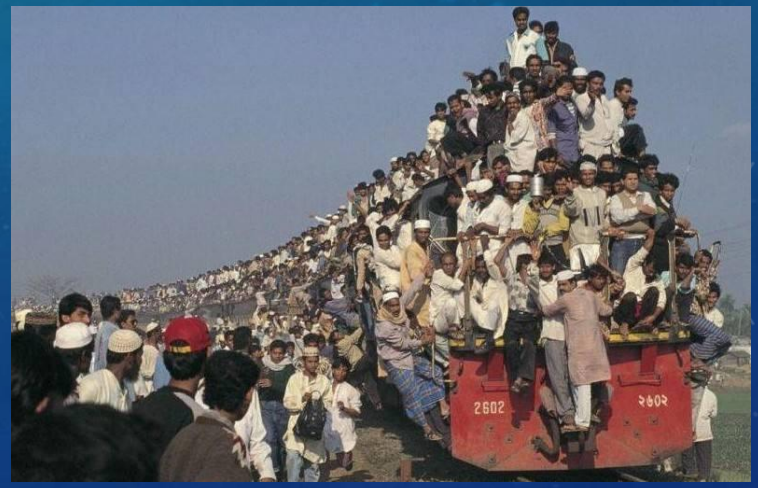
泼冷水

去中心化数字货币的应用挑战

- 容量限制
- 到账速度
- 手续费
- 分叉风险
- 监管障碍
- 私钥门槛
- 币值不稳
- 发行速度僵化
- 技术升级难题
- 能耗
- 被攻击风险
- ……

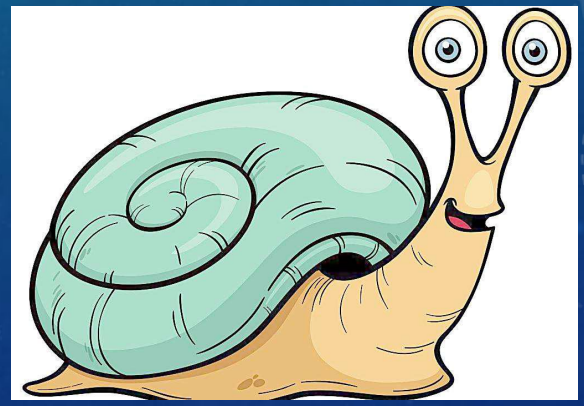
容量限制

- 比特币的区块链容量，每天只能承载70万笔转账
  - 只有主流平台的1%
- 比特币区块链已经满了很久了
  - 手续费飙升。单笔转账要5元人民币
  - 手续费低的转账长时间无法确认
    - 可以追加手续费
- 以太坊的区块链容量与比特币大致相当
- 解决方案：
  - 扩容
    - 会带来分叉风险，后述
  - 链外
  - 侧链



到账速度

- 比特币的平均确认时间10分钟
- 以太坊的平均确认时间14秒
- 但是，1次确认并不代表到账
  - 安全到账的标准：确认后发生的新矿市值大于转账金额
  - 以太坊每个区块5个币，折合约1500人民币
  - 如果转账100万，需要等待600个区块，折合2个半小时
- 确认时间是平均值，实际时间是随机正态分布
  - 比特币经常遇到1个小时的确认时间
- 解决方案：
  - 链外

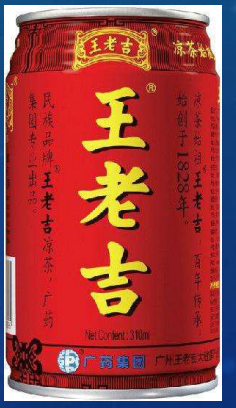


手续费

- 比特币的最低手续费是万分之一比特币，目前折合约1元人民币
- 去中心化系统，每笔交易需要被网络广播几十万次，被CPU验证几十万次，被硬盘存储几十万次
- 所以手续费不可能很低，否则就无法被收录
- 解决方案：
  - 链外

分叉风险

- 对于数字货币，大众最担心的是其不可复制性。
- 以太坊开了一个非常不好的先河，分叉成为了两个币
- 比特币的扩容，有很大的风险会分叉成两个币
- 分叉争夺的核心是冠名权。
- 解决方案：无



监管障碍

- 不能监管，就无法得到广泛认同
  - 反洗钱
  - 反恐
- 监管障碍：
  - 匿名性
  - 不可冻结
  - 自由跨境转账
- 现状：
  - 国内的交易中心无法提币
  - OTC交易平台暂停运行
- 解决方案：
  - 全球监管联盟
  - 侧链
  - 全新的支持监管的数字货币

私钥门槛

- 私钥是数字货币全部控制权
- 私钥泄露，则账户内所有的币都会被盗
- 私钥丢失，则账户内所有的币都成为死币
- 没有任何挽救措施
- 大众没有保管私钥的习惯，也不适应直接面对巨大的风险
- 解决方案：
  - 保险？有监守自盗风险
  - 链外

发行速度僵化

- 比特币发行速度4年减半
- 增速过快，则通胀
- 增速过慢，则：
  - 币价持续上升，不利于流通
  - 算力不足，币不够安全
- 无法应对特殊紧急需求
  - 例如次贷危机

技术升级难题

- 数字货币作为IT系统，有持续升级的需要
- 但是每次升级就必须发生一次硬分叉，风险非常大

能耗

- 比特币1年新矿市值约60亿人民币，大致可以折算为消耗60亿人民币的电力
- 按照0.3元/度计算，年消耗200亿度电
- 全球年发电量约25万亿度，比特币消耗约0.1%
- 如果比特币上涨10倍，则消耗1%电力
- 如果比特币上涨100倍，则消耗10%电力
- 解决方案：
  - 抑制涨幅

被攻击风险

- 51%攻击
- 垃圾信息攻击
- 节点DDOS攻击
- 解决方案：
  - 立法严惩。很难啊

总结

- 每一项技术都有其局限性，有些挑战是难于突破的
- 数字货币更像是鲶鱼，能够督促法币自律
- 去中心化发行、中心化运行可能是最有效的实现方式