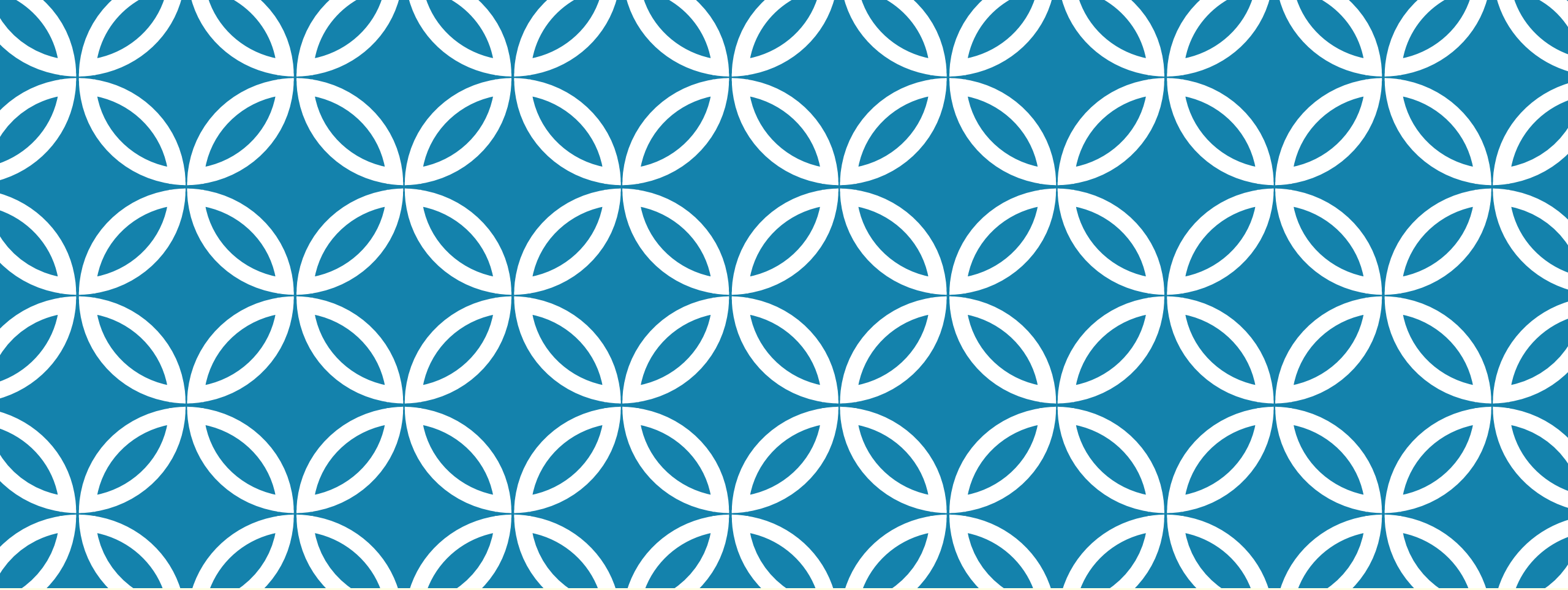
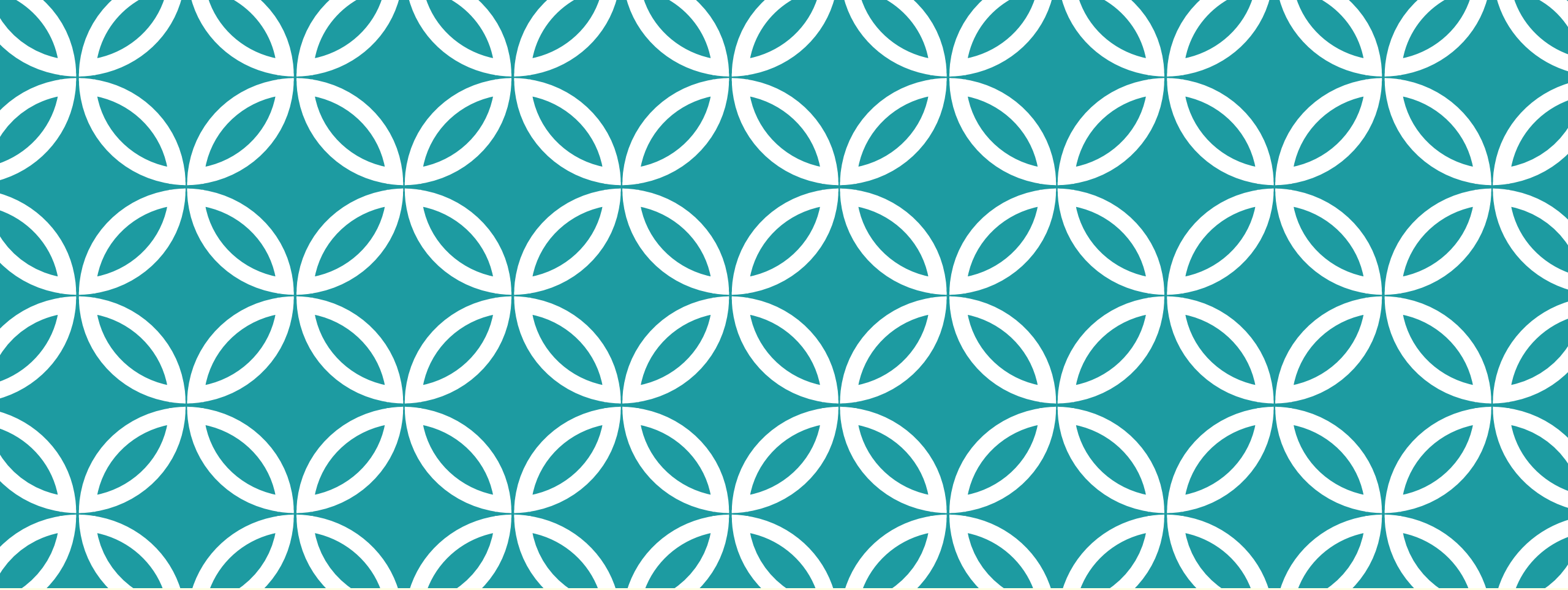


比特币的源起与现在

A brief introduction to Cypherpunks and Bitcoin Protocol



一。密码朋克运动

About Cypherpunks

一。互联网与信息安全

- 个人计算机的出现（1970 年代）

- 互联网的出现（1980 年代）

信息可以持久保存；个人信息面临更多的暴露

二。公钥密码学的发明

- 对称加密的困难
  - 密钥递送难题
- 非对称加密（公钥密码学）的概念
  - Diffie, Hellman, 1976
- 第一种公开的非对称加密算法
  - RSA，1977
- 公钥数字签名的安全性概念，1988

三。DAVID CHAUM，密码朋克的起点

- 赛博空间里的隐私权
  - 通信隐私权
    - 《不可追踪的电子邮件、回邮地址和数字假名》
  - 交易隐私权
    - 《用于不可追踪的支付系统的盲签名》

三。DAVID CHAUM，密码朋克的起点

- 盲签名
  - 支付方 A，银行 B，收款方 C
  - 数字签名、盲化函数、随机函数

1. A 生成随机数 x，生成盲化数 c(x)，把 c(x) 交给 B
2. B 签名 c(x)，即形成 s`(c(x))，交回给 A，同时在 A 账户上扣钱
3. A 检查签名，并使用解盲函数，计算 c`(s`(c(x)))，得出 s`(x)
4. B 将 s`(x) 交给 C
5. C 用 B 的公钥检查签名，即 s(s`(x)) = x；如无误，将 s`(x) 交给 B
6. B 检查签名，然后给 C 账户加钱

三*。盲签名的另一个版本

由 David Chaum 的学生 David Wagner 为绕过专利而创造

支付者 Alice，铸币厂 Bob，接收者 Carol

1. 铸币厂 Bob 公开公钥 B
2. Alice 取一个秘密消息 secret message，使用特殊的哈希成曲线点函数 hash_to_curve(sectet message)，再加上盲化公钥 R = r.G，得出 A_ = hash_to_curve(sectet message) + R
3. Alice 把 A_ 交给 B，B 返回 M = b.A_
4. Alice 解出 A = M – r.B = b.A – r.B
   = b.htc(secret message) + br.G – br.G
   = b.htc(sectet message)
5. Alice 以 (A, secret message) 给 Carol 支付
6. Carol 要立即跟 B 通信以防止重复花费

四。ADAM BACK，工作量证明

- 用单向随机函数找出具有特征的值
  - 找出一个 3 个 0 开头的哈希值
- 用于抵御垃圾邮件轰炸
- 具有稀缺性的数据
  - 何种意义上具有稀缺性?

五。NICK SZABO 与 WEI DAI，问题的推进

- Nick Szabo
  - 研究法学、经济学、计算机
    - “智能合约”概念的提出者
  - 《受信任第三方是安全漏洞》
  - 《货币的起源》
  - 《货币、区块链与社会可扩展性》
  - 《可信任计算的黎明》

五。NICK SZABO 与 WEI DAI，问题的推进

- Bit-Gold
  - 公钥密码学作为账户系统
  - PoW 作为货币
    - 通货膨胀问题
      - 时间戳问题
      - “打包成标准单位”
  - 重复花费问题
    - PBFT 的注册小组

五。NICK SZABO 与 WEI DAI，问题的推进

- Wei Dai（戴维）
  - 独立维护 Crypto++ 代码库，LessWrong 问答论坛活跃用户
  - Crypto-Anarchist
    - “在这里，暴力不是消失了，而是彻底失去意义了，因为参与者的真名和地理位置永远不会暴露”

五。NICK SZABO 与 WEI DAI，问题的推进

- b-money
  - 每个人都运行的复制型数据库，记录公钥与资金的关系
  - 工作量证明用于发行货币
    - 如果一个 PoW 耗时 100 小时，而在市场上，100 小时的运算价值 3 个标准篮子商品的价值，则所发行的货币面额为 3
  - 带仲裁的交易系统（智能合约）

五。NICK SZABO 与 WEI DAI，问题的推进

- b-money
  - 质押货币成为服务器（PoS 概念）
  - 以拍卖发行货币
    - 服务器给出增发数量
    - 人们承诺用一定的计算量竞拍一定的数额

戴维的元问题与启示

六。HAL FINNEY，勇敢大于一切

- PGP 软件的主要贡献者之一

- RPOW（可复用的工作量证明）
  - 用户 A 向服务器提交工作量证明，注册货币
  - 获得货币的用户 A 可向用户 B 支付（发送 PoW）
  - B 向服务器检查是否已被用过
  - 服务器检查完成，给 B 发送新的货币
  - 服务器运行在“CPU 安全模块”上

- 《比特币与我》

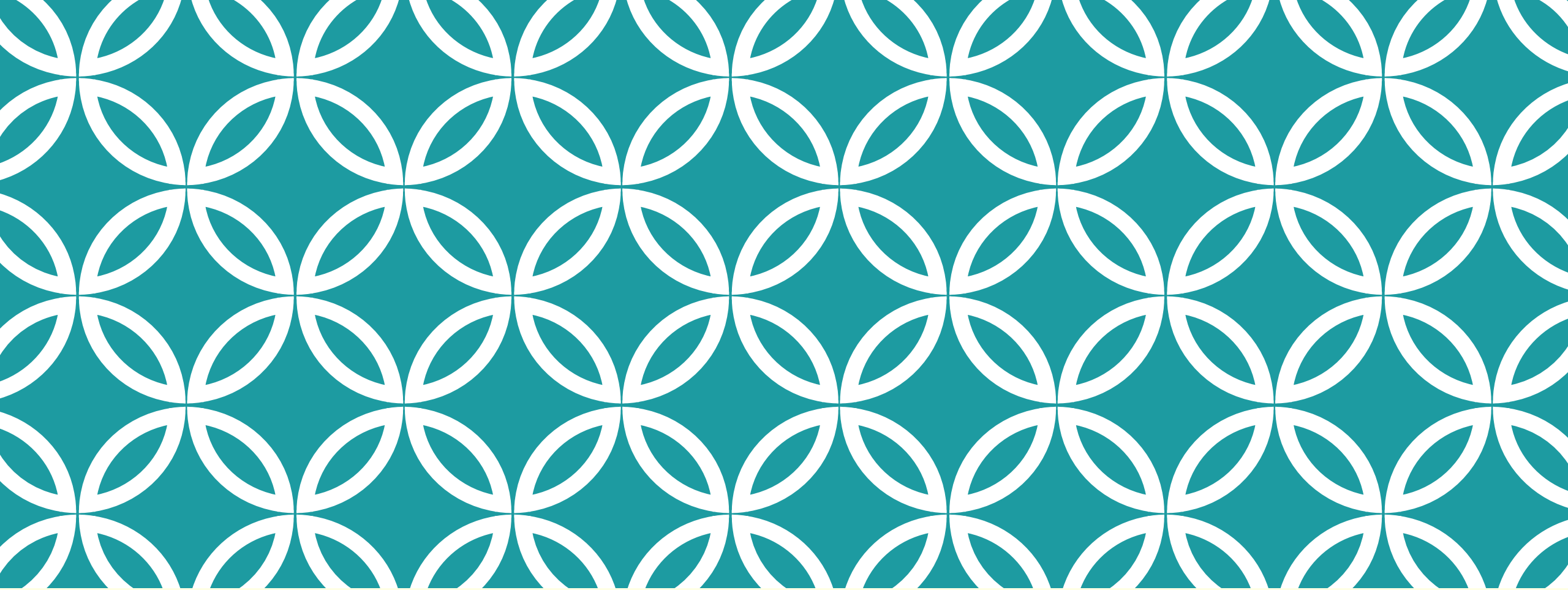
七。总结

1. 稀缺性
   - PoW

2. 抗重复花费
   - PBFT 注册表
   - HSM-based Authority

3. 抗通胀
   - None

4. 匿名性
   - 公钥密码学



二。白皮书与比特币

Nakamoto, the white paper and bitcoin

一。点对点网络

- “他们很擅长砍掉 Napster 这样的有中心的网络的头，但对 Gnutella 和 Tor 这样完全点对点的网络似乎束手无策。” —— 中本聪

- 在完全点对点的网络中，以前的密码朋克所提议的方法都不管用，因为节点是随时进入和退出的

二。工作量证明

- 交易以成批次（区块）的形式在整个网络中确认并得到处理

- 必须为每一个区块提供一个**有效的工作量证明**

- 每个区块都必须承诺自己的上一个区块（以前序区块的哈希值的形式），以及本区块内的交易

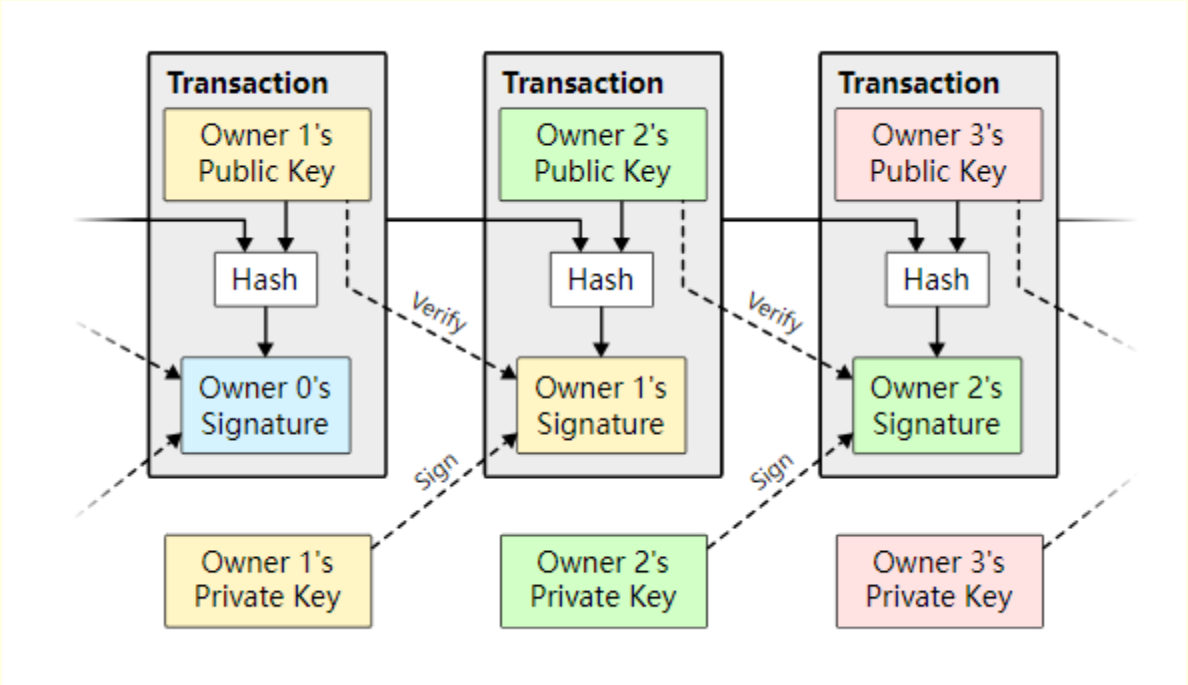
三。中本聪共识

- 节点以累积最多工作量证明的链条为正确的链

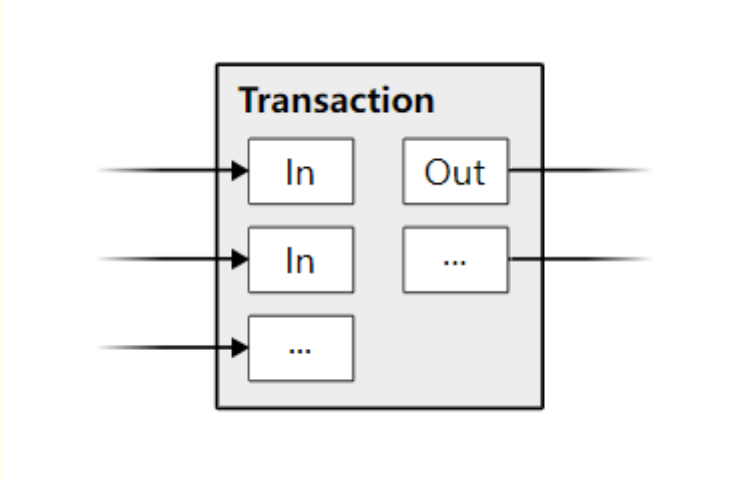
- 根据过往一段时间内的区块生成数量，全网所有节点重新调整所要求的工作量证明的难度

四。资金的形式与交易

- 交易的输出（TXO）
- 公钥为身份验证手段



四。资金的形式与交易

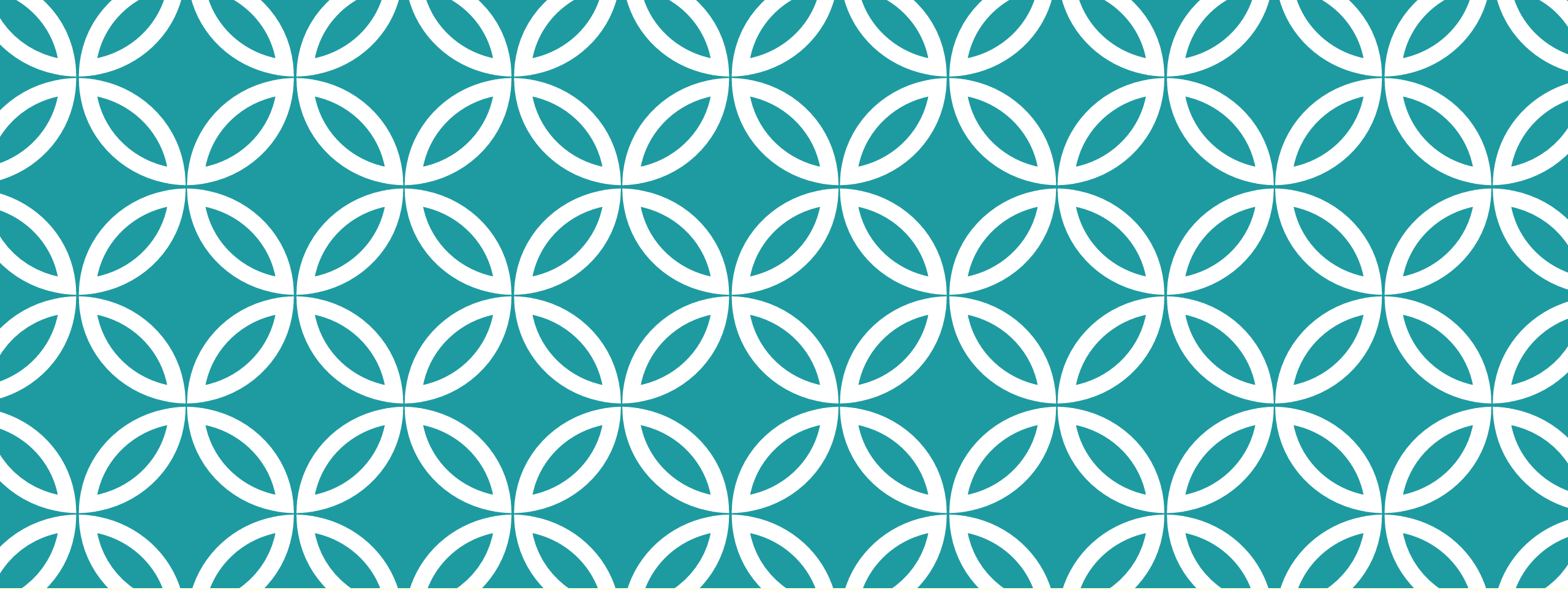


五。A MILE STONE, NOT A BIBLE

- “最长链” --» “最重链”
- “滚动平均值” --» “确定周期（2016个区块）”
- “公钥” --» “脚本公钥”
- “输入所有权同一” --» 可被 coinjoin 打破

五。A MILE STONE, NOT A BIBLE

- 比特币白皮书勘误
- 比特币的学术谱系
- 不完整比特币开发史
- 比特币软分叉激活史



三。比特币的价值

Value positions of Bitcoin

一。互联网货币

- 抗审查
- 信任最小化
  - 保证全节点的运行负担足够小，每个人都能运行自己的全节点
    - 小区块
- 闪电网络

二。货币

- 货币主义
  - 一种通胀可以预测的货币
- 新制度经济学
  - 一种验证成本极低的货币
- 尼克·萨博
  - 一种无法伪造其奢侈特性的货币
- 奥地利学派
  - 货币生产的伦理
  - 货币的绝对数量并非关键