



计算即权力：比原链设计哲学

长铁



*Product philosophy*  
产品的哲学

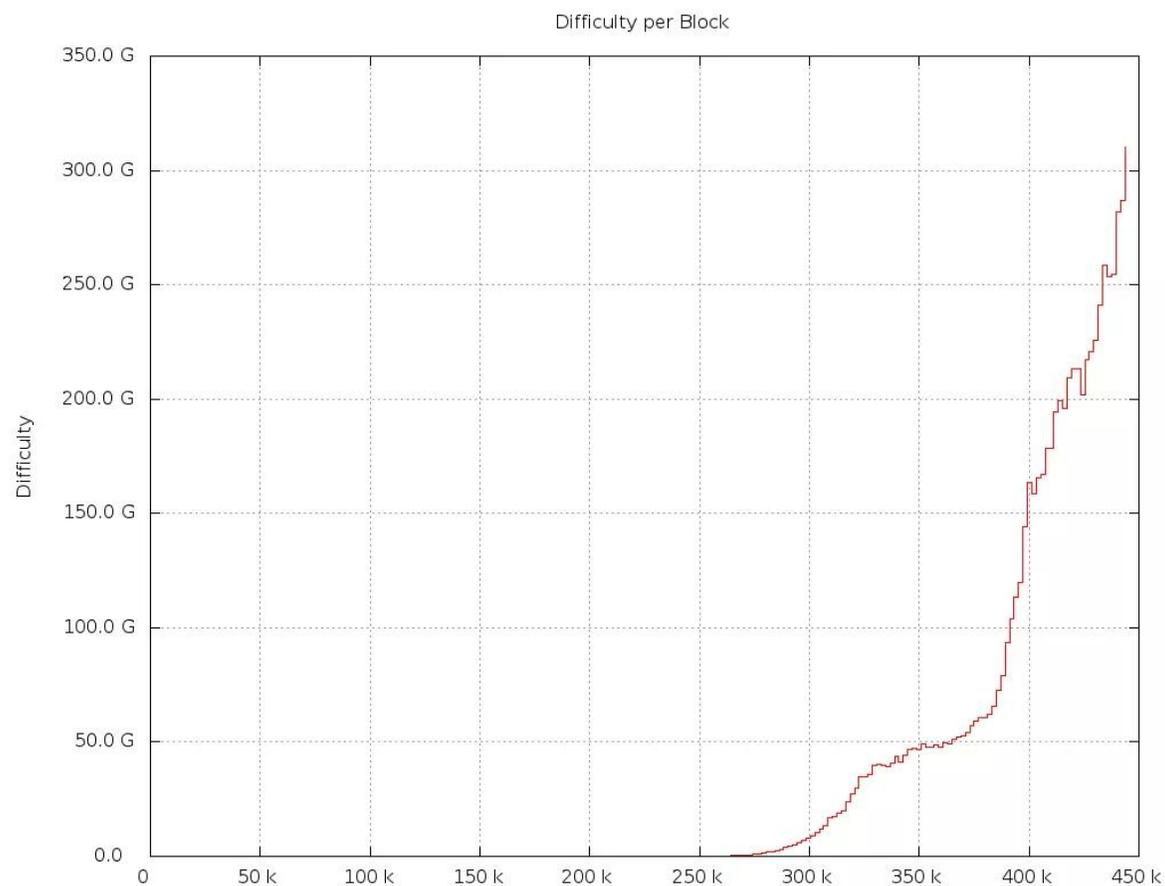
# 不重复发明车轮

- 比特币
- ① 非对称加密
  - ② 点对点技术
  - ③ 哈希现金 (*Hashcash*)
- 比原链
- ① 工作量证明 → AI ASIC友好型
  - ② *UTXO* → 扩展型 *BUTXO*
  - ③ *BIP44* → 通用地址格式, 支持多资产、多帐户
  - ④ *Odin* → 将开放数据索引用于资产登记
  - ⑤ 侧链 → 将侧链技术应用于资产的分红

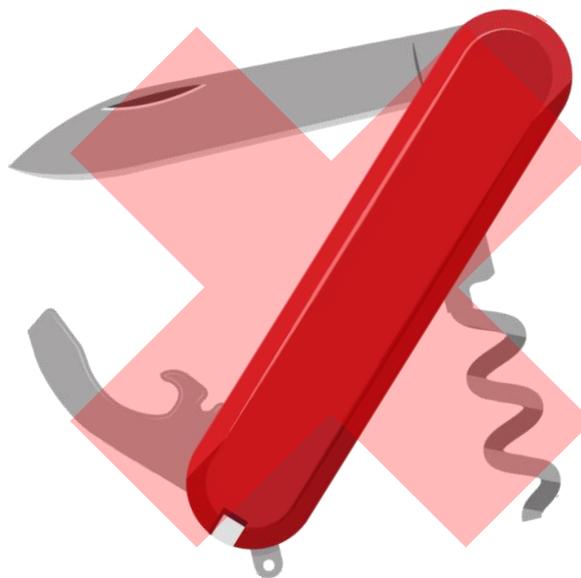
# 挖矿造成能源与硬件浪费



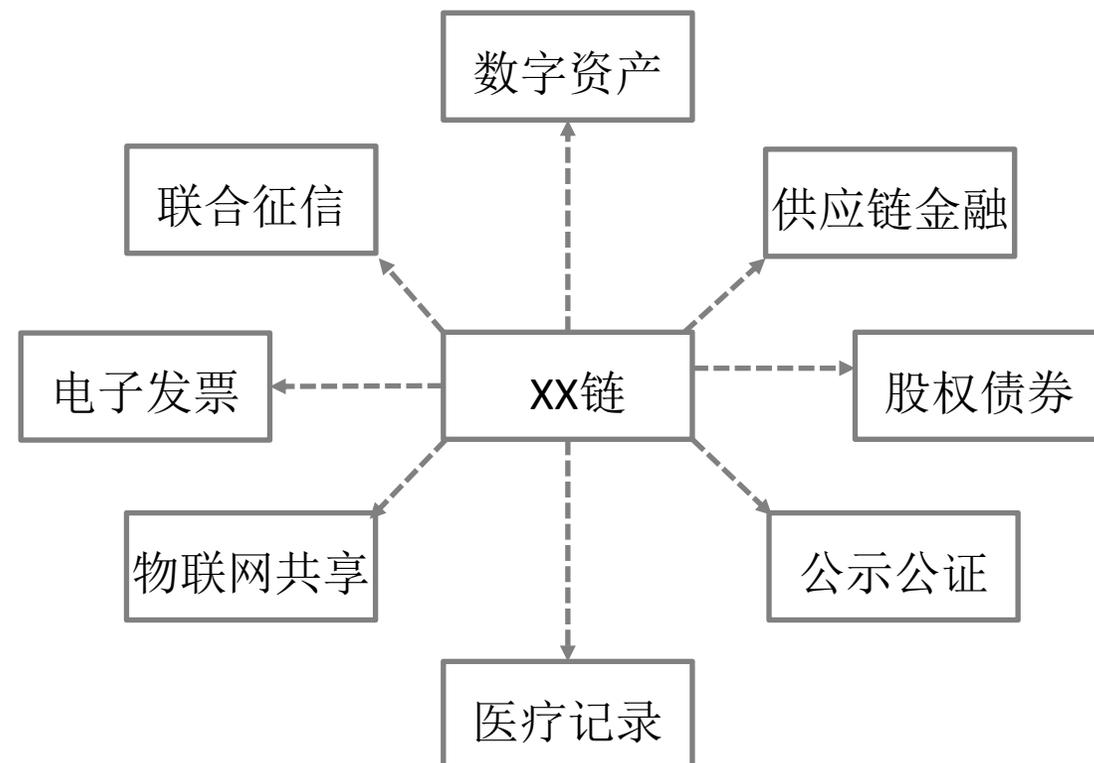
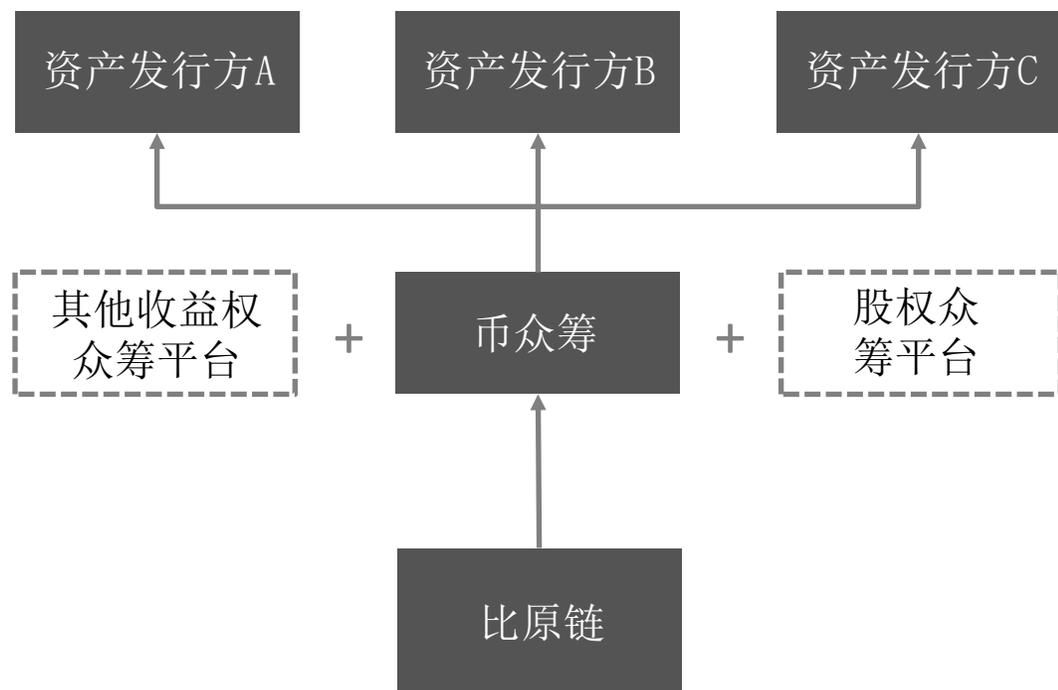
# 对人工智能ASIC友好的PoW算法



做一个钉锤，而不是瑞士军刀



# Financing plan 商业模式



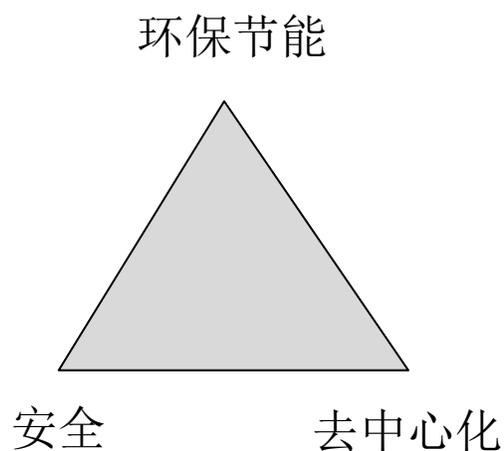
# 商业应用场景

- 场景一 收益权资产管理
- 场景二 非上市公司股权管理
- 场景三 证券化资产管理



*The philosophy of  
consensus*  
共识的哲学

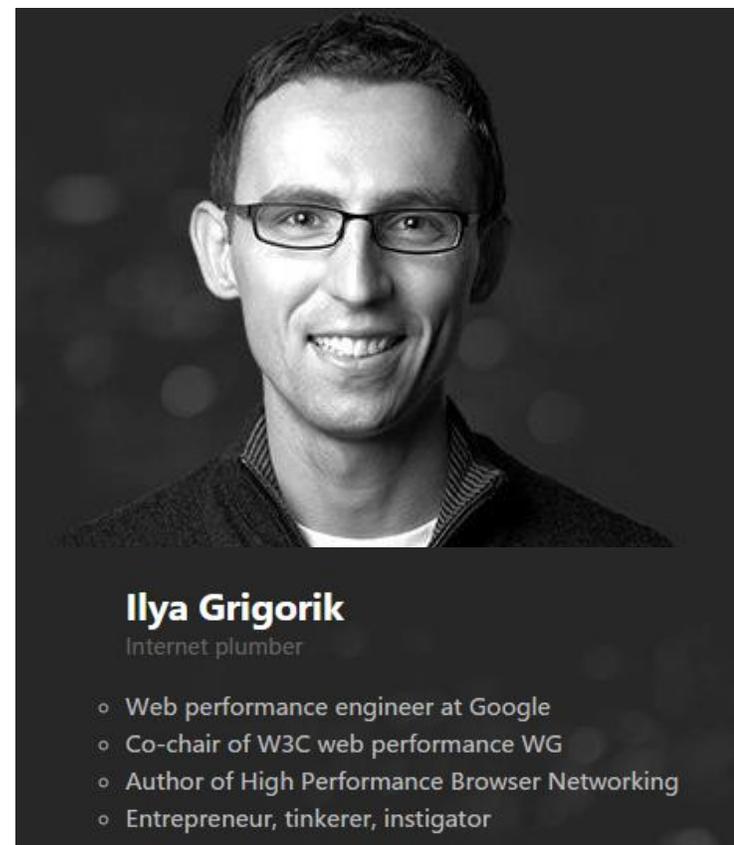
# 不可能三角



- 分布式计算领域：“*CAP*不可能三角”是指可用性(*A*)、一致性(*C*)、分区容错性(*P*)；
- 分布式域名领域：“*Zooko*不可能三角”是指如何能够给一个网址或某个用户一个身份识别符的同时，确保其安全性、去中心化和易用性；
- 区块链领域：“不可能三角”是指安全，环保（非计算性），去中心化；

# 最小可行区块链原理

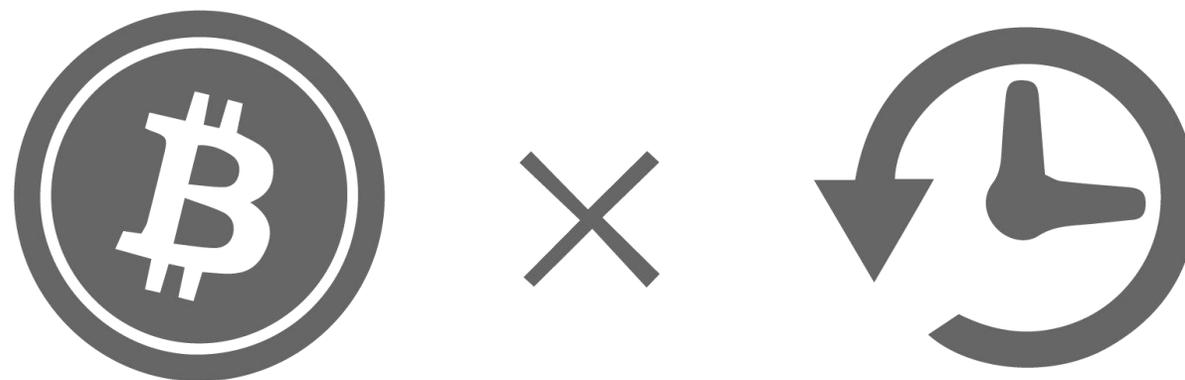
- ① 用三方记账法保障交易安全
- ② 用公钥基础设施（PKI）保障交易安全
- ③ 多方转移和验证
- ④ 重复消费和分布式一致性
- ⑤ 保护网络免受Sybil攻击
- ⑥ 建立最小可行区块链



# 比特世界与原子世界

原子世界	比特世界
随机性	伪随机 
天底下没有两片相同的树叶	一切东西皆可复制
熵增	熵减（负熵）
正态分布	幂律分布
竞争性资源	非竞争性资源
比特币	印刷机

# 什么是币天



币天 (Coin Day) = 币 x 天

# 一次典型的链上交易

## > 交易

交易ID	658d3990d547cacfdddb0caea0d7e83f0dc8a462f3323b1ba9e211e1d1bd36b8
时间	2015-06-04 07:45:56
交易大小	335 Bytes
交易费	0.00001 BTC
所属区块	359302
确认数	24527
总输出	120 BTC
总输入	119.99999 BTC
币天销毁	8.89
公共消息	

## > 交易列表

[显示脚本](#)

658d3990d547cacfdddb0caea0d7e83f0dc8a462f3323b1ba9e211e1d1bd36b8		(交易费: 0.00001 BTC) 119.99999 BTC	
3AgxodEvv9FZtm6LMgPxCSmBwhNSBdFsSk (转入)	120 BTC	12zY7Br2piQWfMWPd9rhbeNgoVP3Z5dnX9 (转出)	12.961 BTC
		3AgxodEvv9FZtm6LMgPxCSmBwhNSBdFsSk (转出)	107.03899 BTC

# 传统信用评价模型

$$R_n = R_{n-1} + r_n ,$$

$$r_n \in \{-1,0,1\} .$$

其中： $R_n$ 、 $R_{n-1}$  分别表示淘宝用户截止到第  $n$ 、 $n-1$  次交易之后所获得的信用得分，

$r_n \in \{-1,0,1\}$  表示 {差评，中评，好评}

# 基于币天销毁的信用评价模型

$$R_n = \sum_{i=1}^{i=n} R_i * W_i ,$$

$$W_i = C_i * D_i$$

$$R_i \in \{-1,0,1\}, \quad i, W_i, C_i, D_i \in (0, +\infty) .$$

$R_n$ 代表用户的信用值得分， $R_i$ 为第*i*次交易时用户所得的信用值， $W_i$ 为第*i*次交易时的币天销毁， $C_i$ 为第*i*次交易时的金额， $D_i$ 为第*i*次交易距离上一次交易所积累的时间。

Contact us  
结束页



比原链官方网站  
<http://bytom.io>



长铗  
Wechat ID:blockchain