PoX的战争

区块链技术在金融工具中的应用

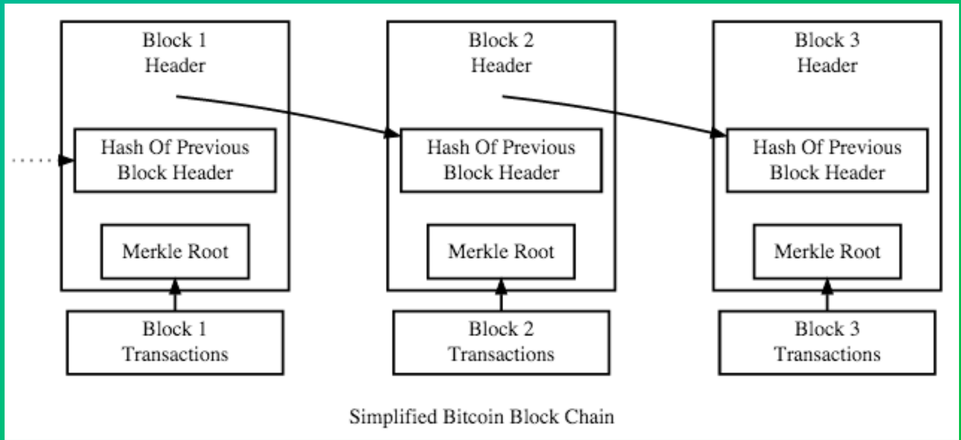
梧桐树

北京云图科瑞科技有限公司

BlockChain & PoX 简介

密码学货币的两大基石

BlockChain：一个公开的账本

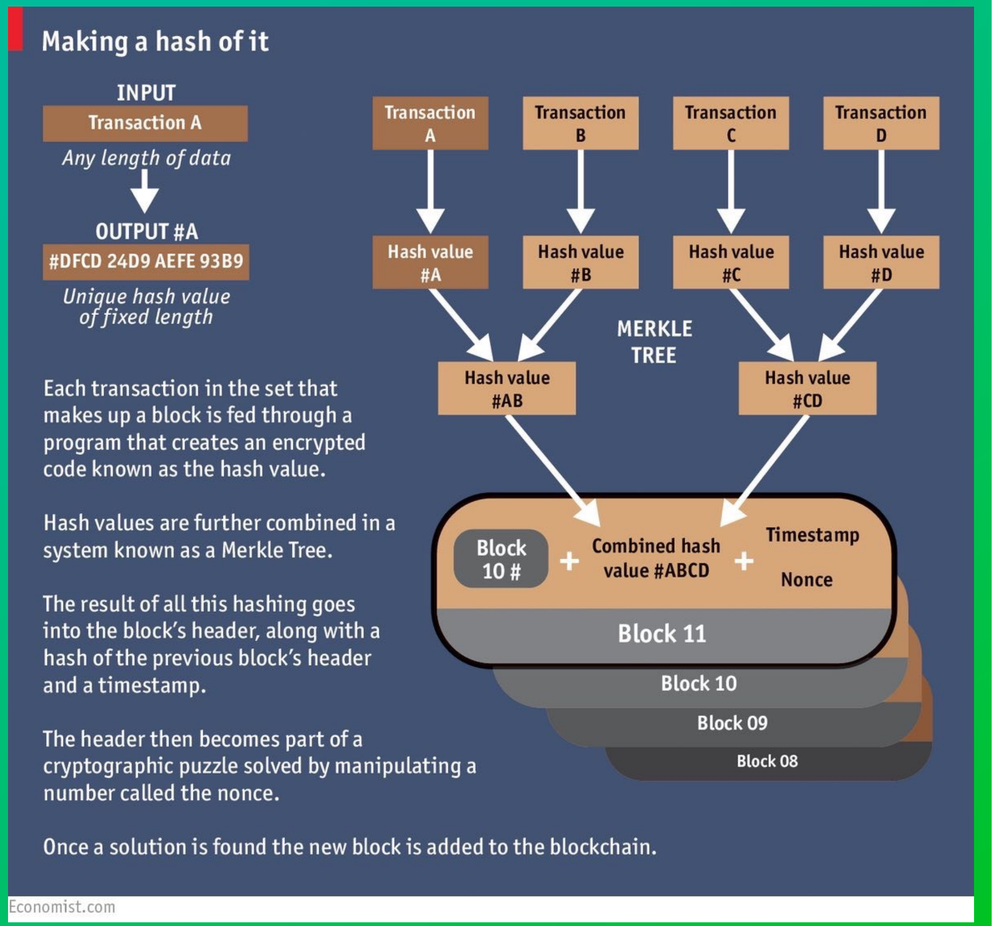


Simplified Bitcoin Block Chain

https://bitcoin.org/en/developer-guide

- BlockChain如其名，是Block的链表
- Block中有什么
  - 数据（比特币：交易、时间、随机数……）
  - 前一个Block的hash

BlockChain：一个公开的账本



- BlockChain的重要特性
  - 任何改动都会改变所属block的hash
  - 一个block改变之后的所有block hash都会发生改变

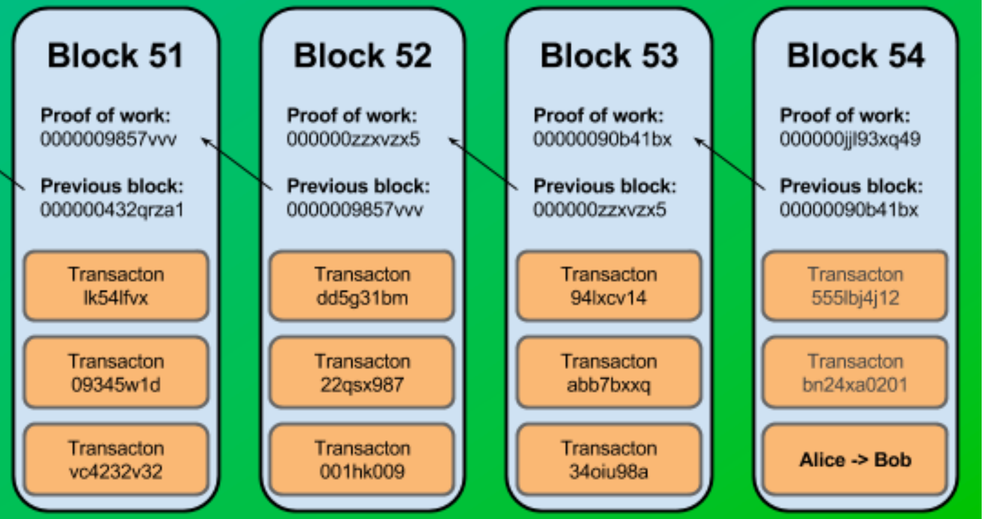
PoX：Proof of something

version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c81701000000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
...	

Block hash

0000000000000000 e067a478024addfe cdc93628978aa52d 91fabd4292982a50

http://www.righto.com/2014/02/bitcoin-mining-hard-way-algorithms.html



http://forexecho.info/bitcoin-mining-finding-blocks/

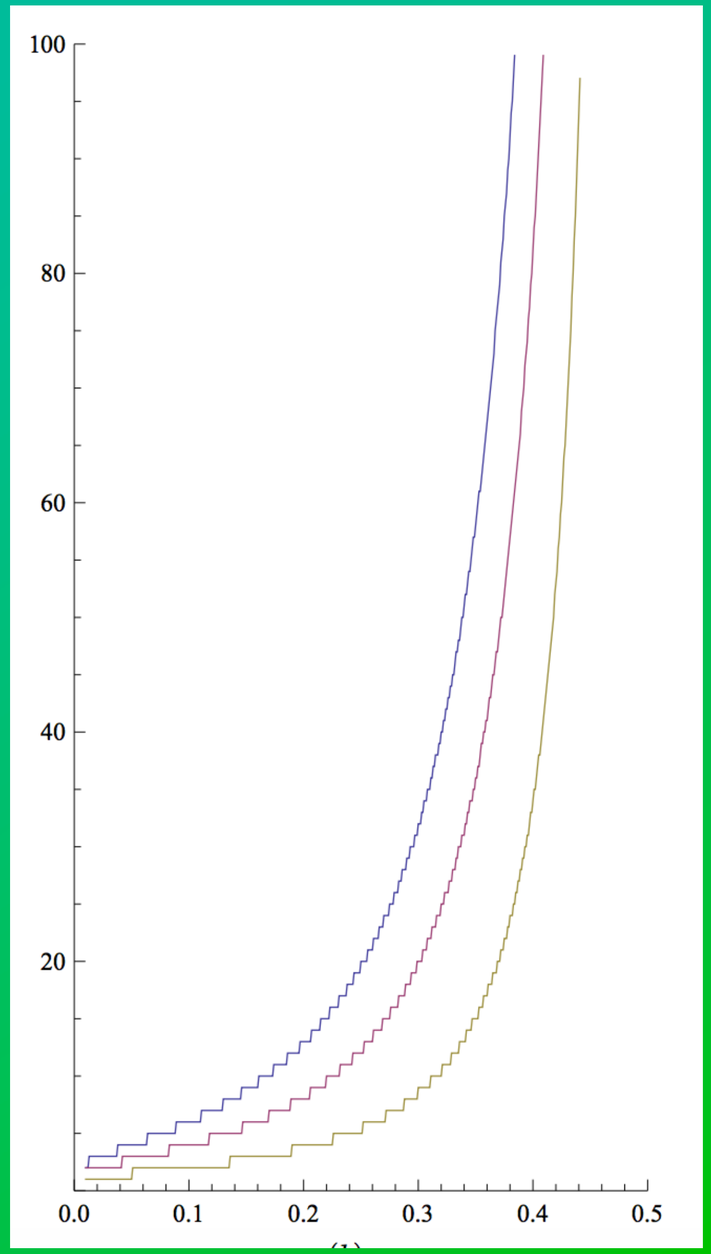
- 每个block的产生背后都有成本支撑
- 目前比特币全网算力约 450,000T Hashes/s，相当于5亿张顶级显卡
- 巨大的成本支撑起BlockChain的去中心化，使之成为一个自治的网络

PoX的演进之路

- Bitcoin: SHA256
- Litecoin: scrypt
- NXT: Stake
- Ripple: Validation
- ……

PoX：把不作恶变成无法作恶

- 利用BlockChain背后指数增长的成本来确保Block信用指数上升

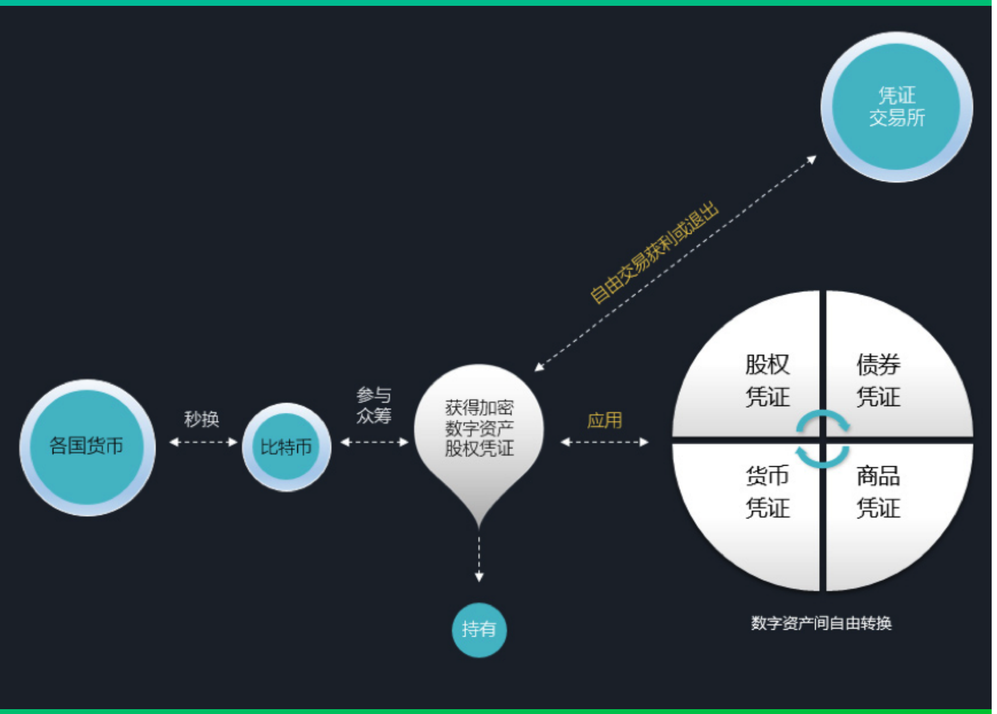


https://bitcoil.co.il/Doublespend.pdf

去中心化的信用共识

BlockChain的几种应用

去中心化的权属证明



- 去中心化保存凭证，由密码学货币保证，无需中间人
- 可用于股权证明、电子签名、公证等领域

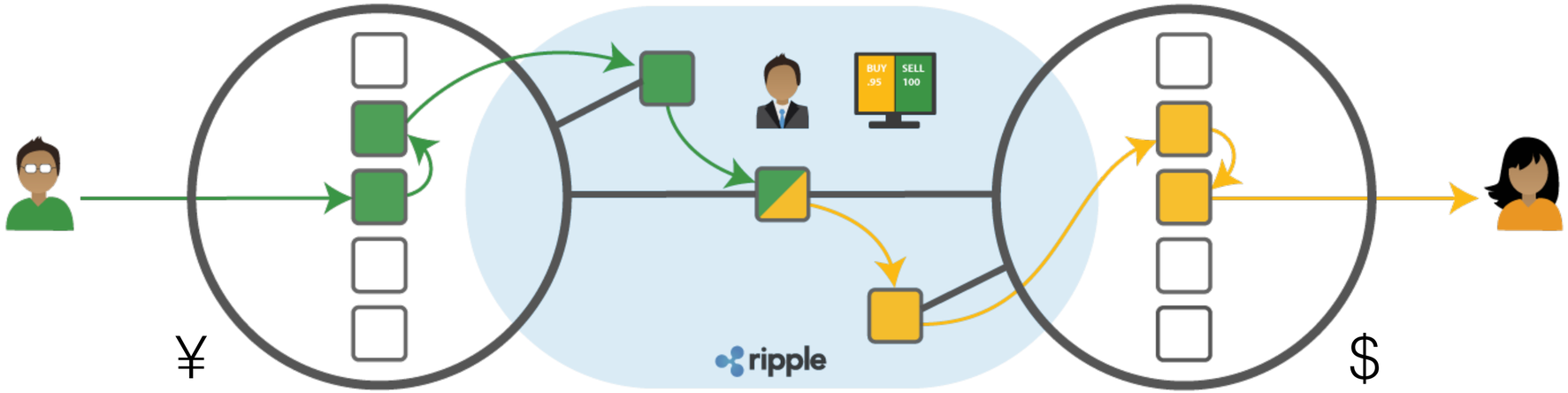
去中心化的权属证明

- bitshares：
  - 用户直接在去中心化的网络中发行数字资产，无需中间人
  - 数字资产交易亦不需要中间人

P2P借贷

- 借贷双方之间的事务就不不要任何中介机构或中间商的介入
- 所有的交易和协议透明公开，不需要第三方来监督合约的执行

去中心化的跨境支付

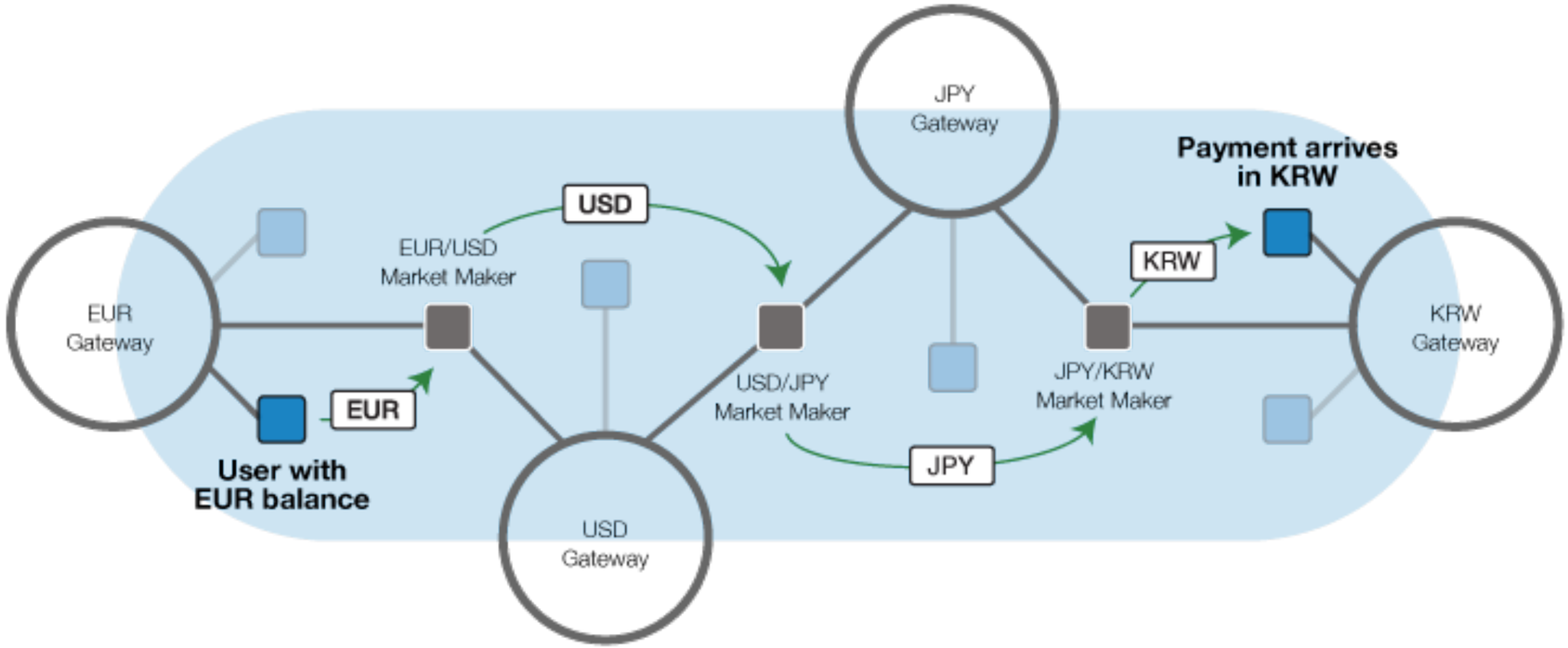


User A
Send CNY

Market Maker
Buy CNY for USD

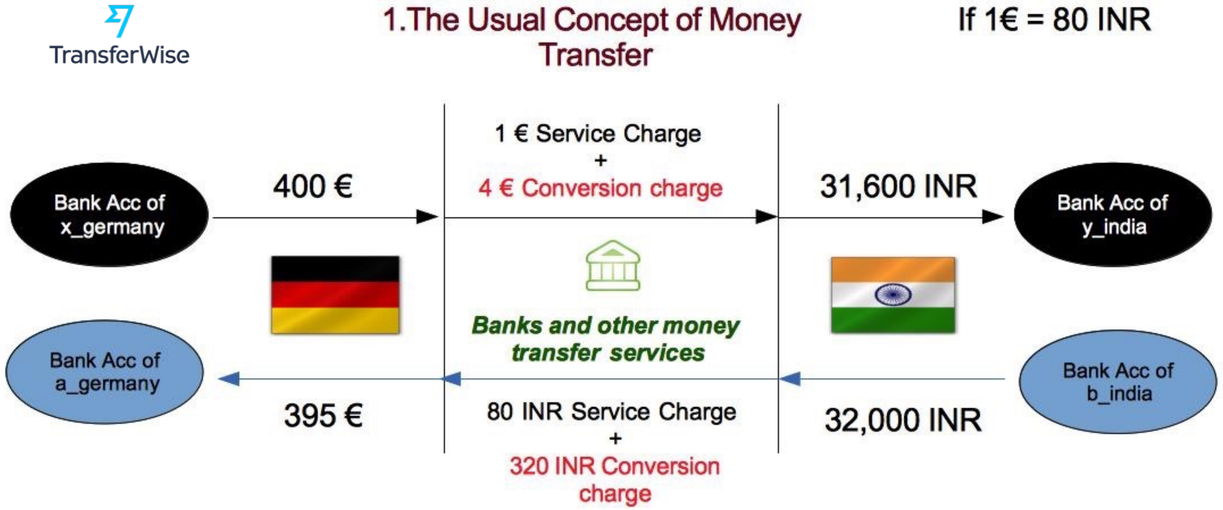
User B
Receive USD

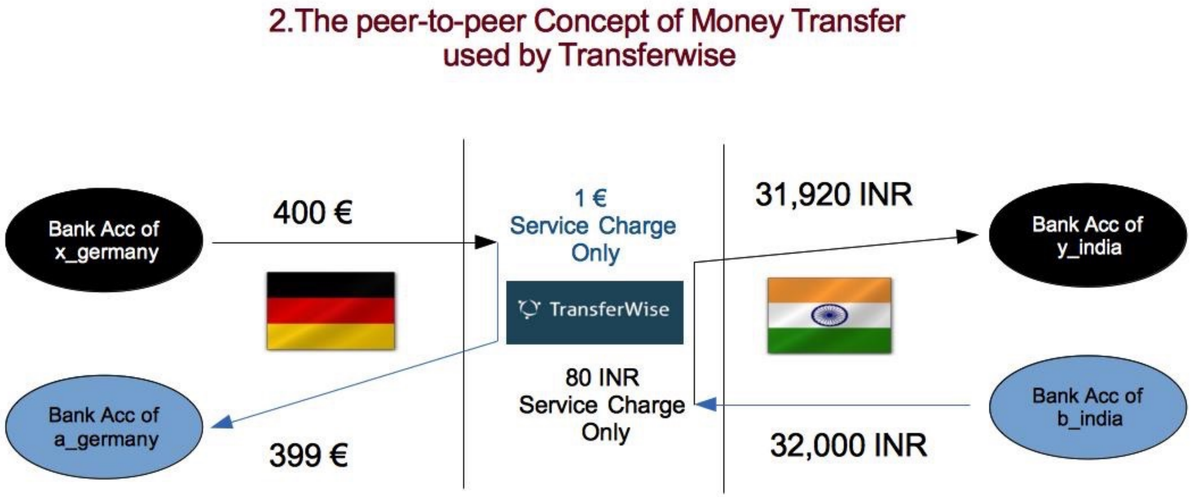
去中心化的跨境支付


JPY
Gateway
Payment arrives
in KRW
USD
EUR/USD
Market Maker
KRW
EUR
Gateway
KRW
Gateway
EUR
USD/JPY
Market Maker
JPY/KRW
Market Maker
JPY
User with
EUR balance
USD
Gateway

去中心化的跨境支付

TransferWise



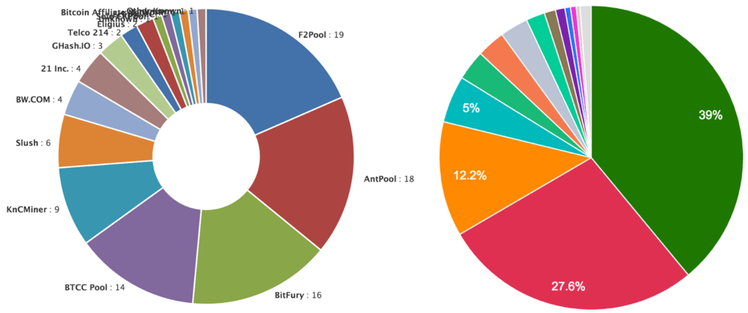


BlockChain不是万能的

去中心化的弊端

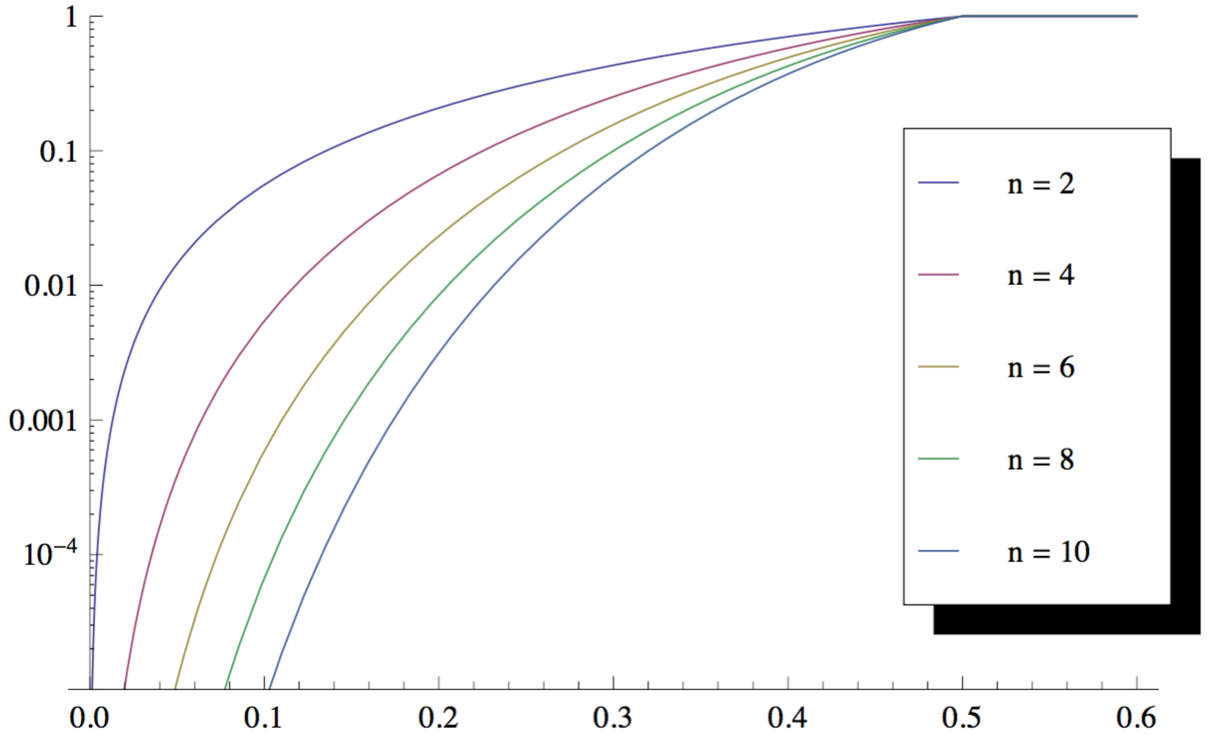
51%攻击

- 平衡算力分布



BTC

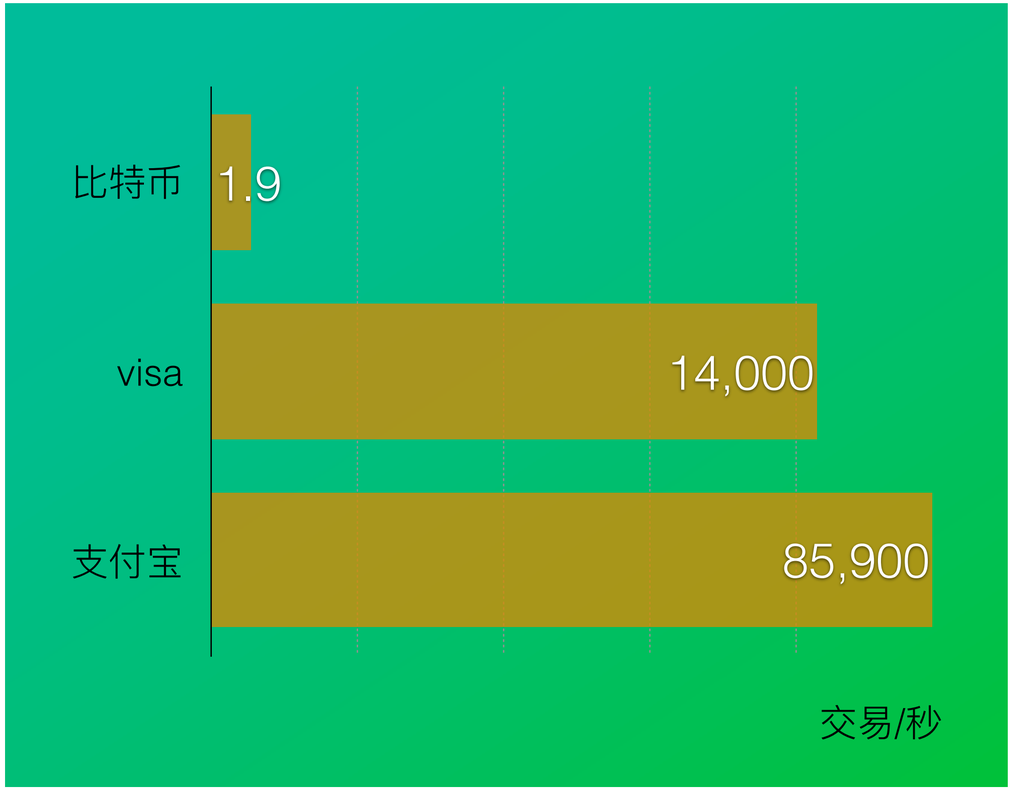
LTC



篡改不同确认次数的block对应成功概率所需的算力比例

处理能力

- 单机处理速度
- 数据传输速度
- 广播风暴



Thanks

- “梧桐树” 网站是 “北京云图科瑞科技有限公司” 拥有的专业技术支持网站。
- 致力于为机构客户提供专业的互联网金融、创新金融工具、云计算管理系统 等领域的核心技术服务。
- 专注于创新性金融工具设计，数字化资产交易平台建设，云计算实施与管理，以及后台的业务流程体系建设的咨询。