Hosted by Pawket

2023-3-18

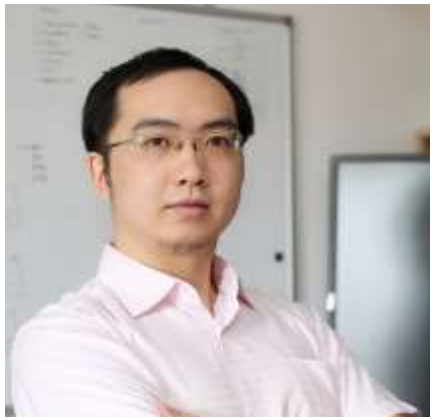
区块链发展史

区块链开发工作坊

时间：2023年3月18日 14:00-17:30

地点：国康路100号上海国际设计中心22楼多功能厅

个人介绍

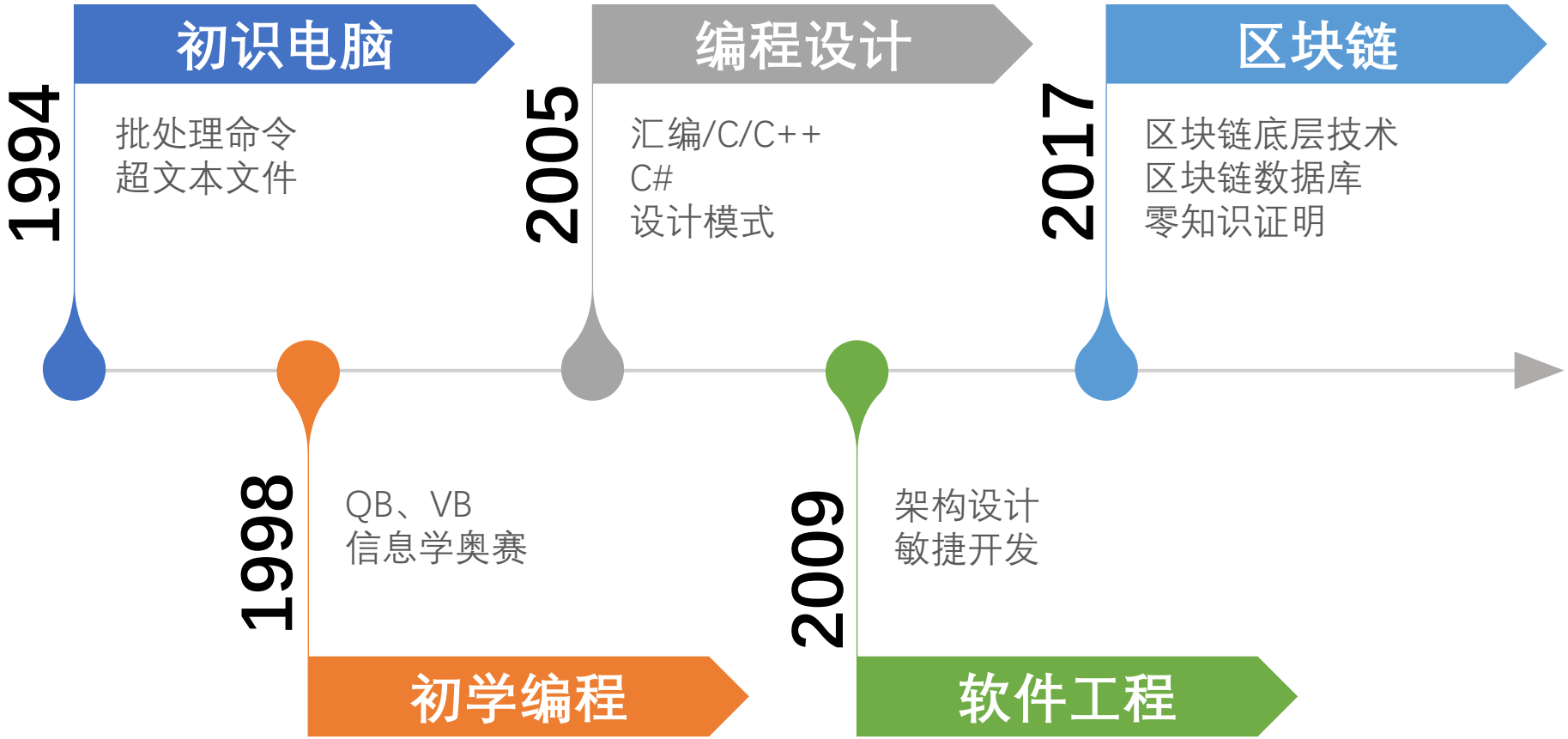


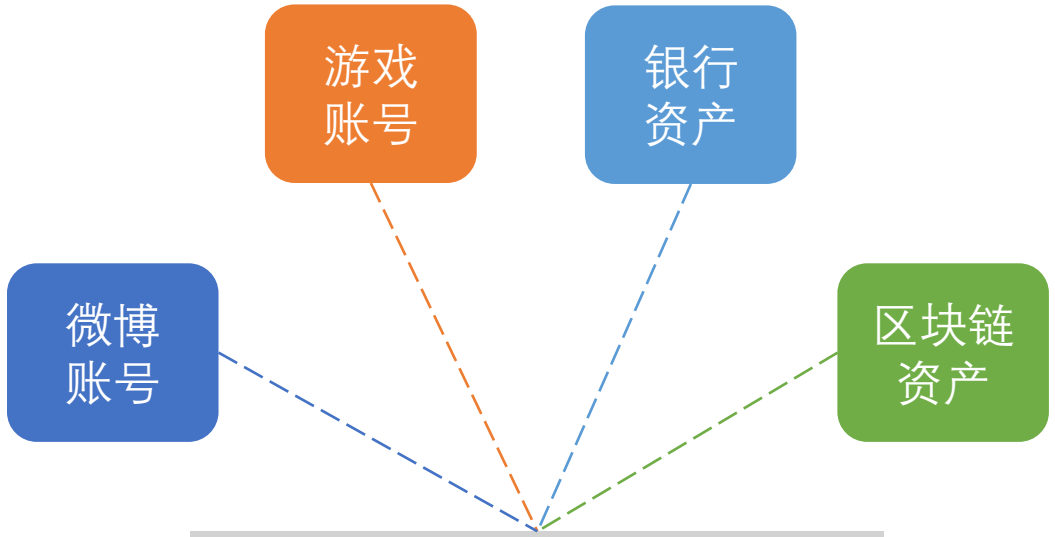
梁爽

区块链 架构师

上海交大 计算机博士生

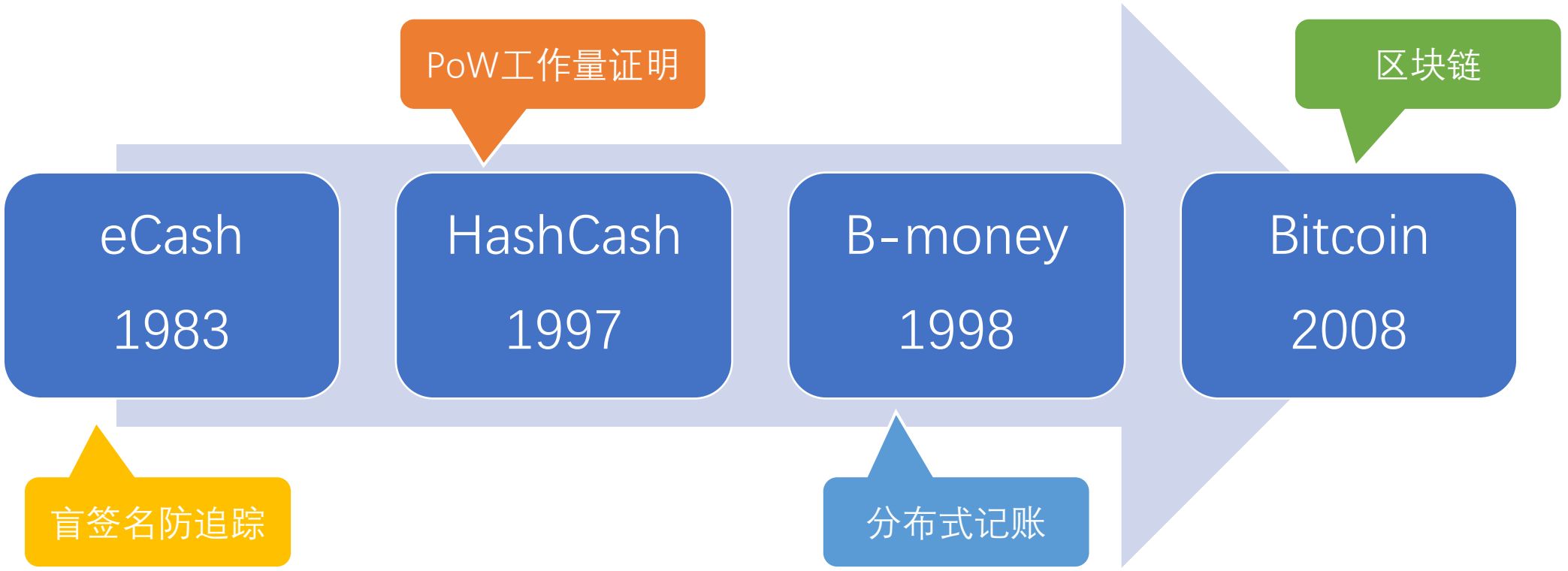
微信：icerdesign
微博：@wizicer
Github: @wizicer
Twitter: @icerdesign
LinkedIn: www.linkedin.com/in/icerdesign





你的数字资产真的是你的吗？

密码数字货币技术历史



如何防双花?

区块链是什么？

事务

事务指一次信息记录的行为，
如一项存证或一笔转账交易

区块链是什么？

区块

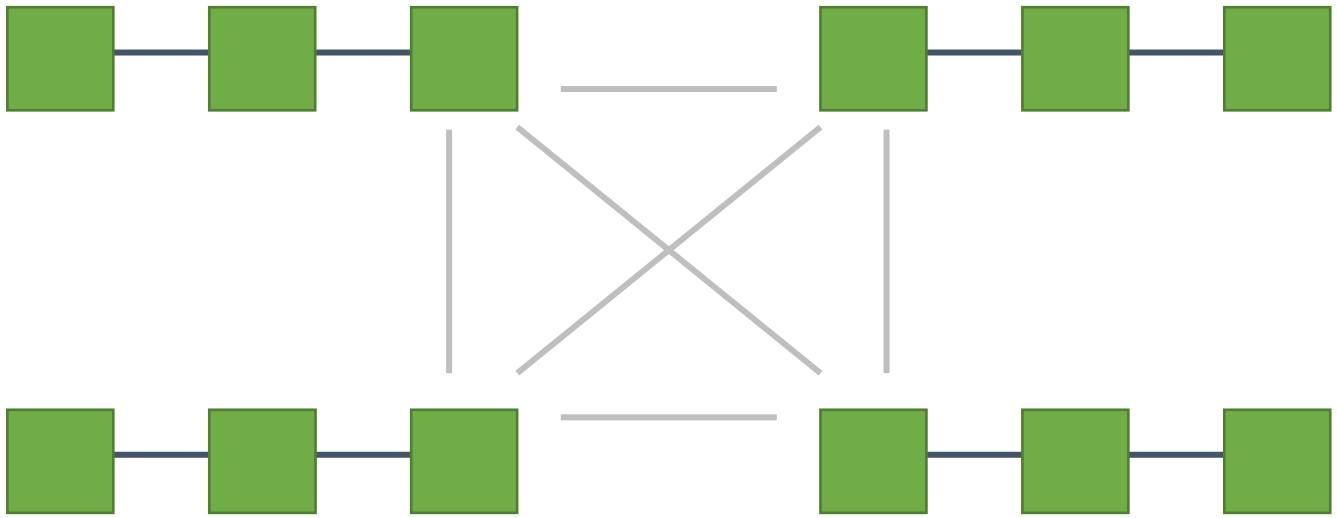
同一时间段的一系列事务信息，汇总为一个区块

区块链是什么？

块链式数据结构
（狭义区块链）

按时间顺序，区块顺序相连的一种链式数据结构

区块链是什么？



分布式账本
（广义区块链）

利用分布式节点共识，形成价值互联的分布式基础架构

比特币的设计目标

建立一个不会被人操控的去中心化银行

并且永远不会宕机的系统

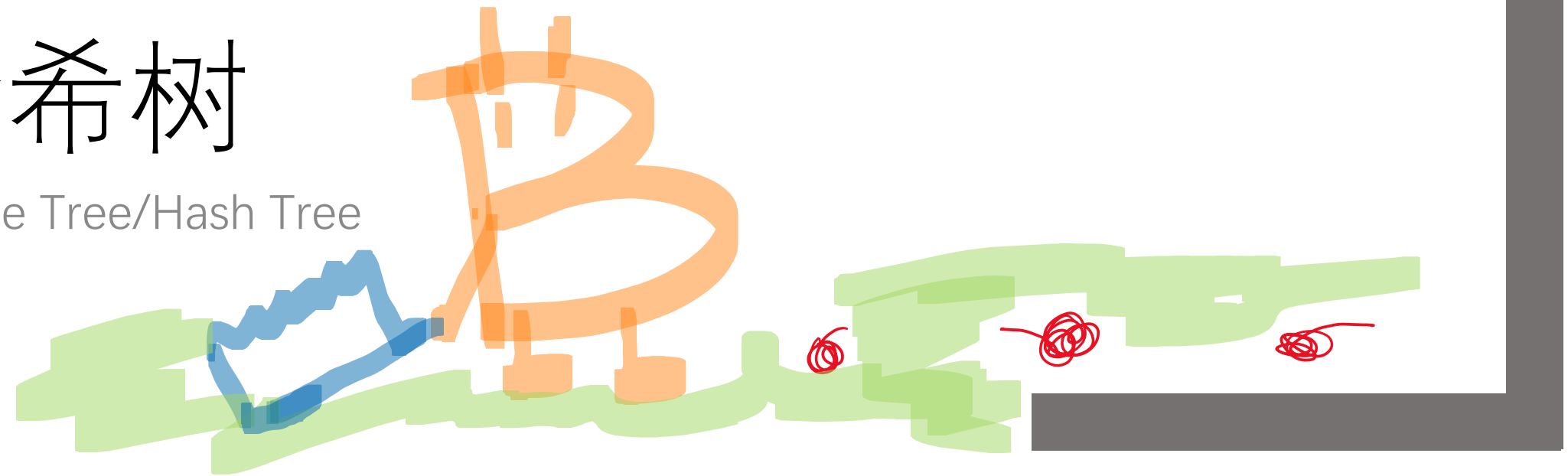
为此设计了分布式账本及编程能力有限的比特币

比特币的技术手段

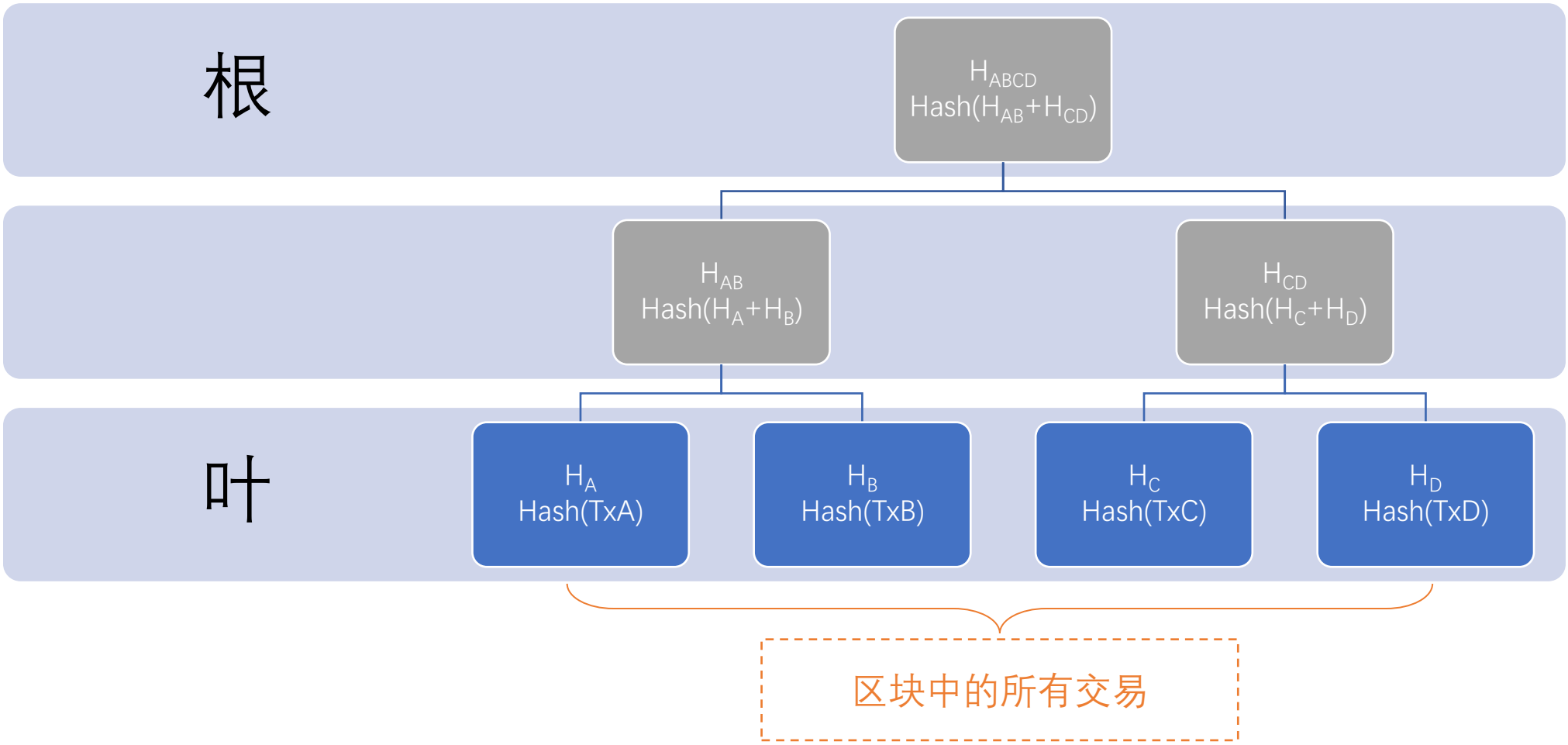
- 哈希树(Merkle Hash Tree)
- 未使用的交易输出(UTXO)
- 椭圆曲线算法
- 脚本锁定结构

哈希树

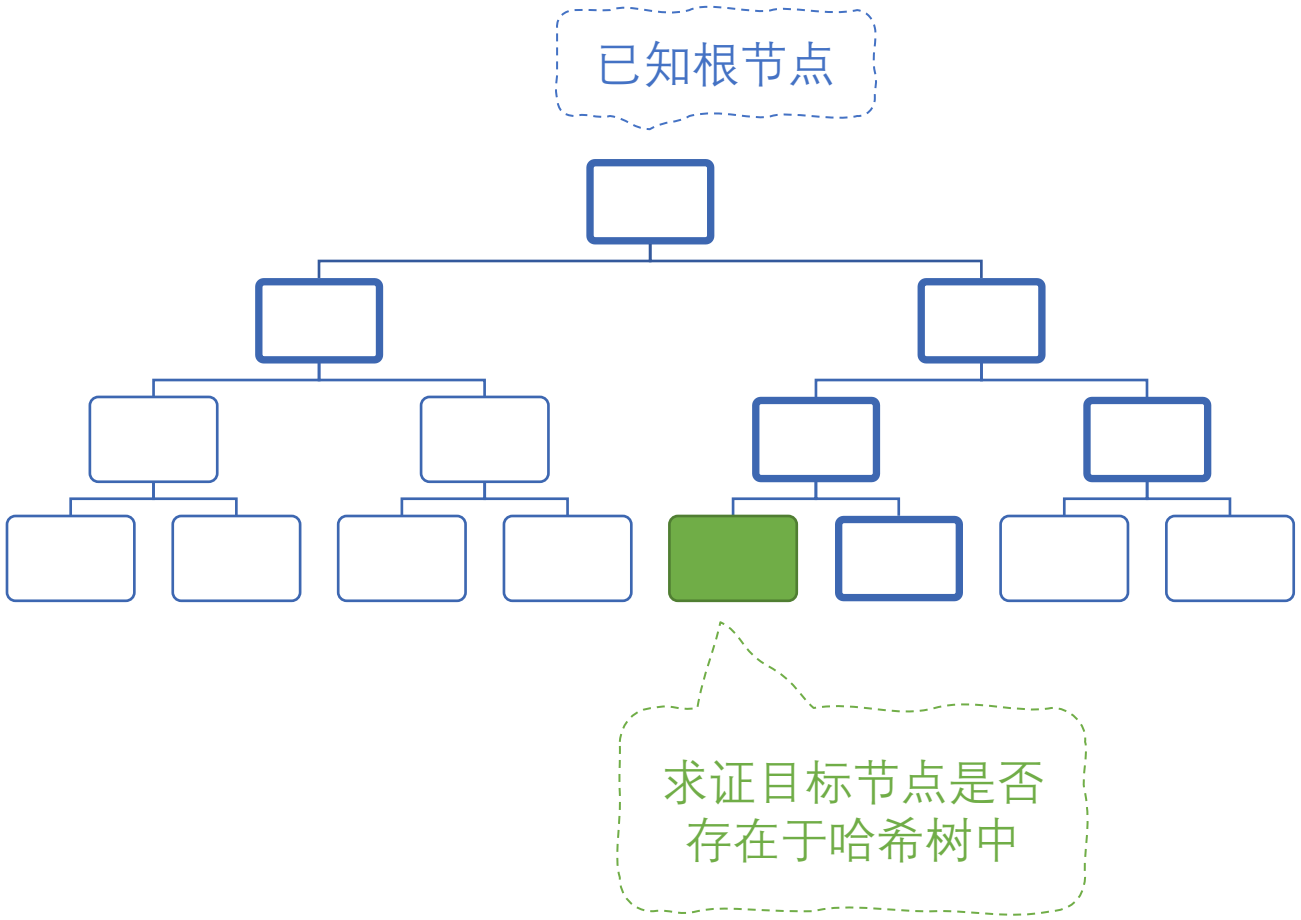
Merkle Tree/Hash Tree



建立哈希树


根
叶
H_{ABCD}
Hash(H_{AB}+H_{CD})
H_{AB}
Hash(H_A+H_B)
H_{CD}
Hash(H_C+H_D)
H_A
Hash(TxA)
H_B
Hash(TxB)
H_C
Hash(TxC)
H_D
Hash(TxD)
区块中的所有交易

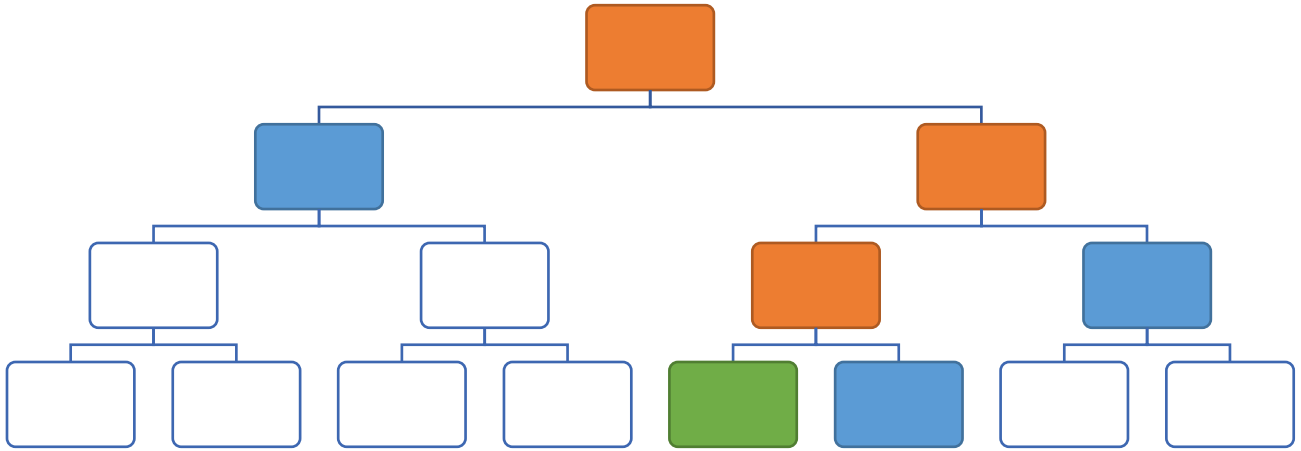
哈希树的轻量验证



图例

目标节点

哈希树
的轻量验证



复式记账交易结构

UTXO（Unspent Transaction Output）未使用的交易输出

30+20=50

20+30=50

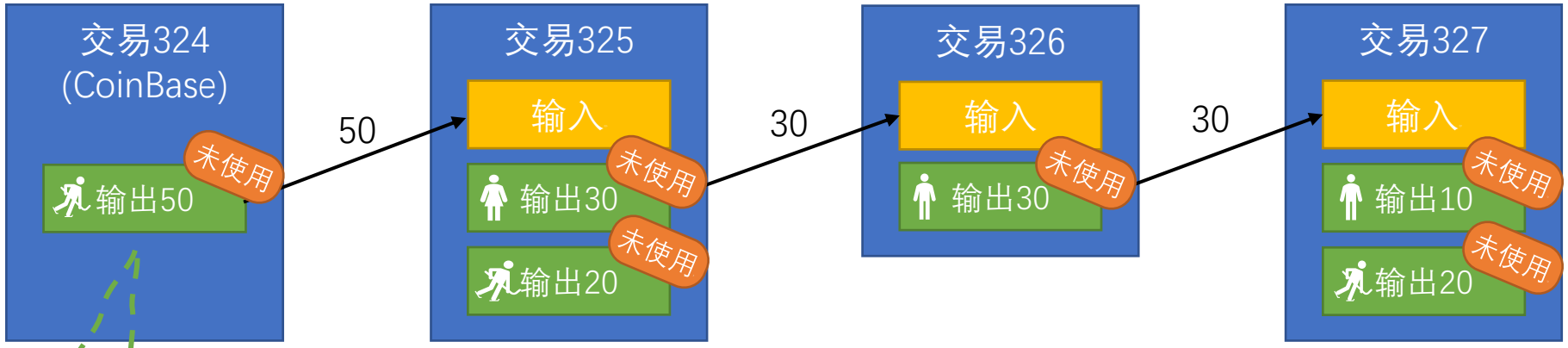
40+10=50

矿工挖矿获得50

矿工->Alice: 30

Alice->Bob: 30

Bob->矿工: 20



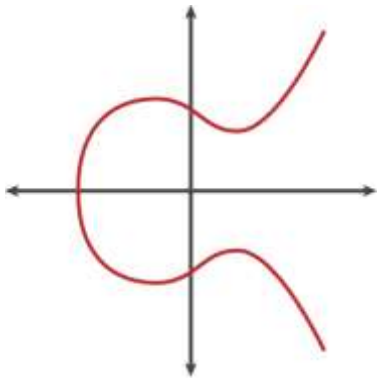
未使用的
交易输出

30+20=50

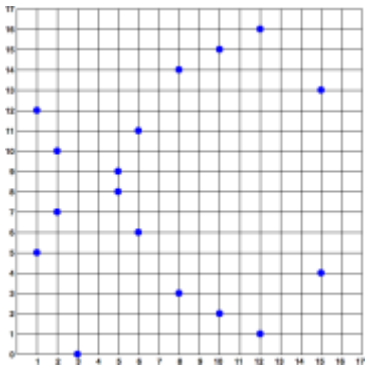
20+30=50

20+10+20=50

椭圆曲线算法（ECDSA）

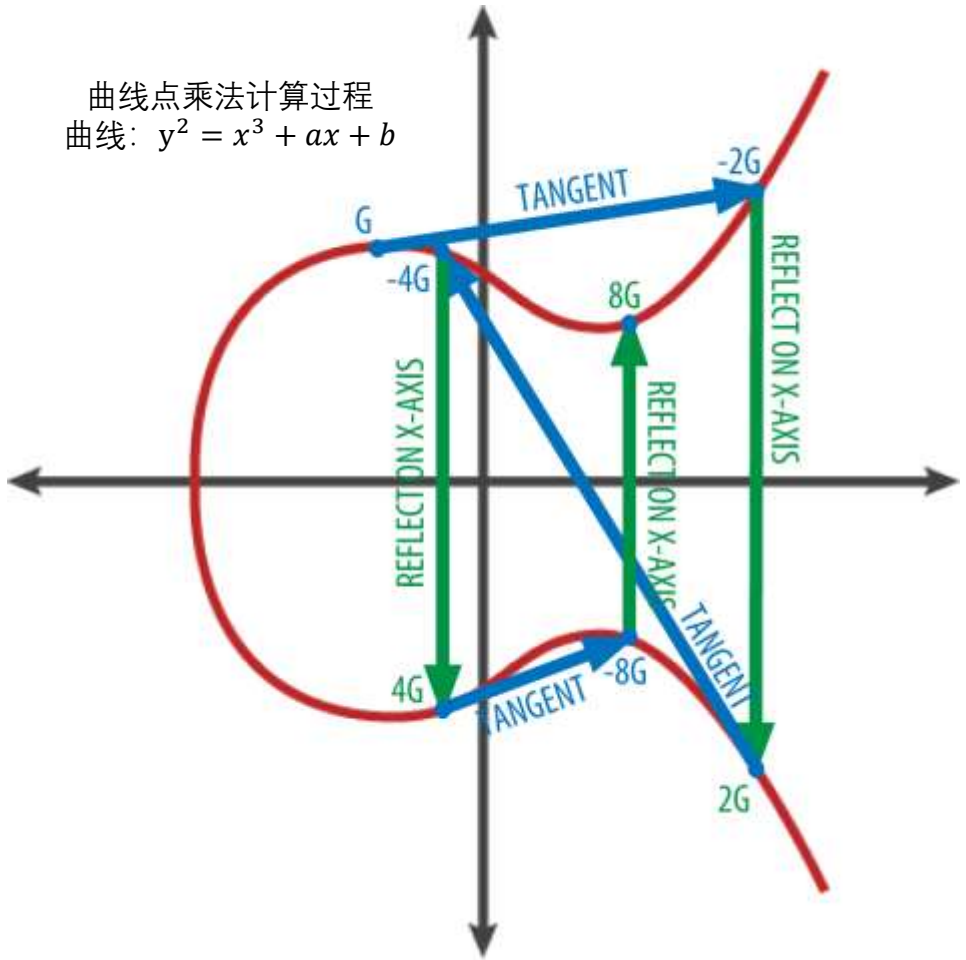


实域上的曲线



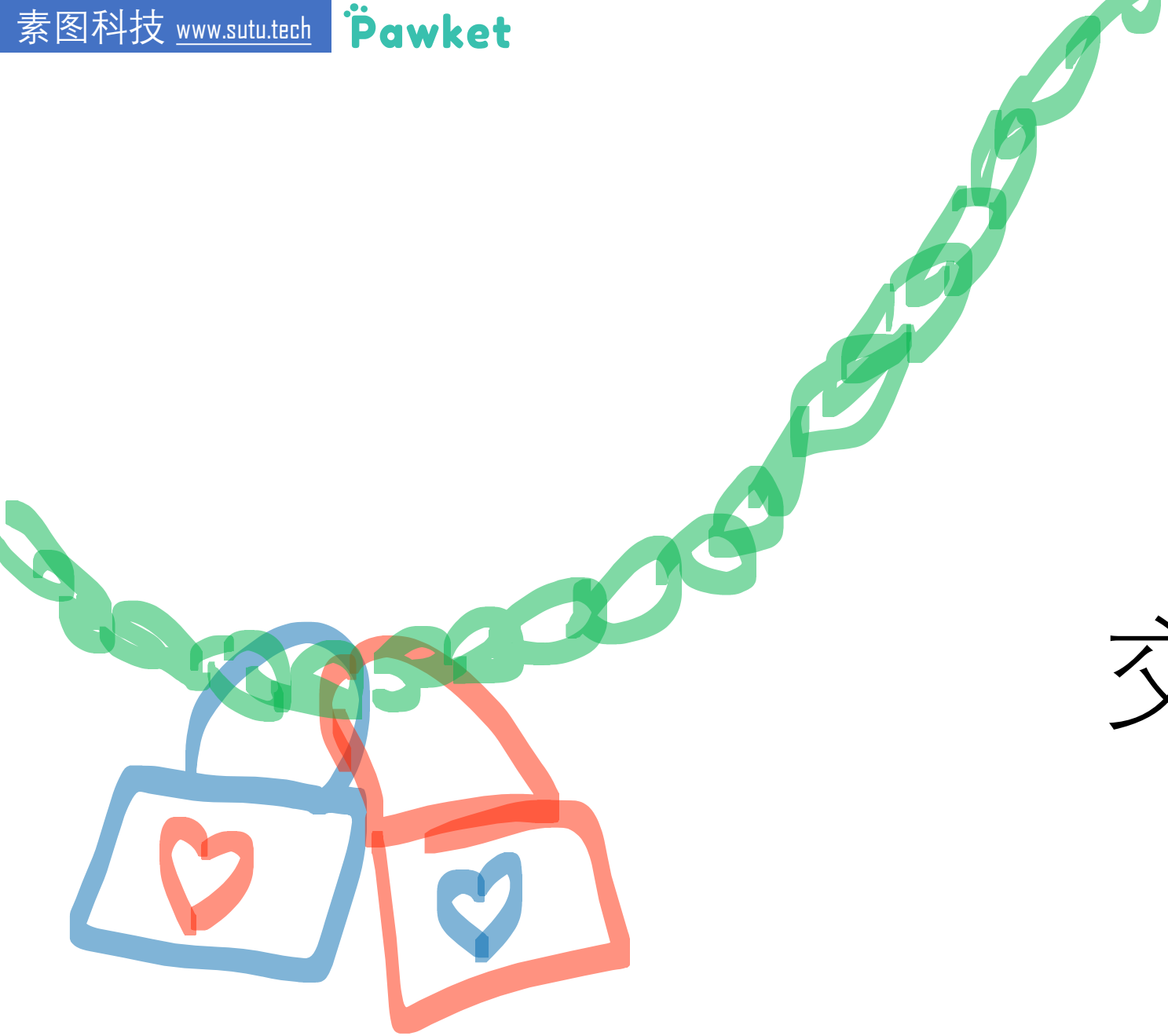
有限域上的曲线

曲线点乘法计算过程
曲线：$y^2 = x^3 + ax + b$



- 私钥=任意正实数
- 公共定义：
  - 曲线参数
  - 基础点
  - 阶次
- 公钥=私钥*基础点

https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch04.asciidoc



交易锁定结构

范例：P2PKH
Pay-to-PubkeyHash

锁定脚本(ScriptPubKey)

- *DUP HASH160 <公钥哈希> EQUALVERIFY CHECKSIG*

解锁脚本(ScriptSig)

- *<签名> <公钥>*

验证方式

- *【解锁脚本+锁定脚本】一起放入栈虚拟机运行*
- *期望结果为“成功”（true）*

被比特币禁用了的操作符

比特币栈虚拟机被故意设计成图灵不完全

故所有验证都可以在可预测的时间内完成

对验证区块有威胁的操作符也被禁止使用

OP_CAT
OP_SUBSTR
OP_LEFT
OP_RIGHT
OP_2MUL
OP_2DIV
OP_MUL
OP_DIV
OP_MOD
OP_LSHIFT
OP_RSHIFT

比特币的设计目标

建立一个不会被人操控的去中心化银行

并且永远不会宕机的系统

为此设计了分布式账本及编程能力有限的比特币

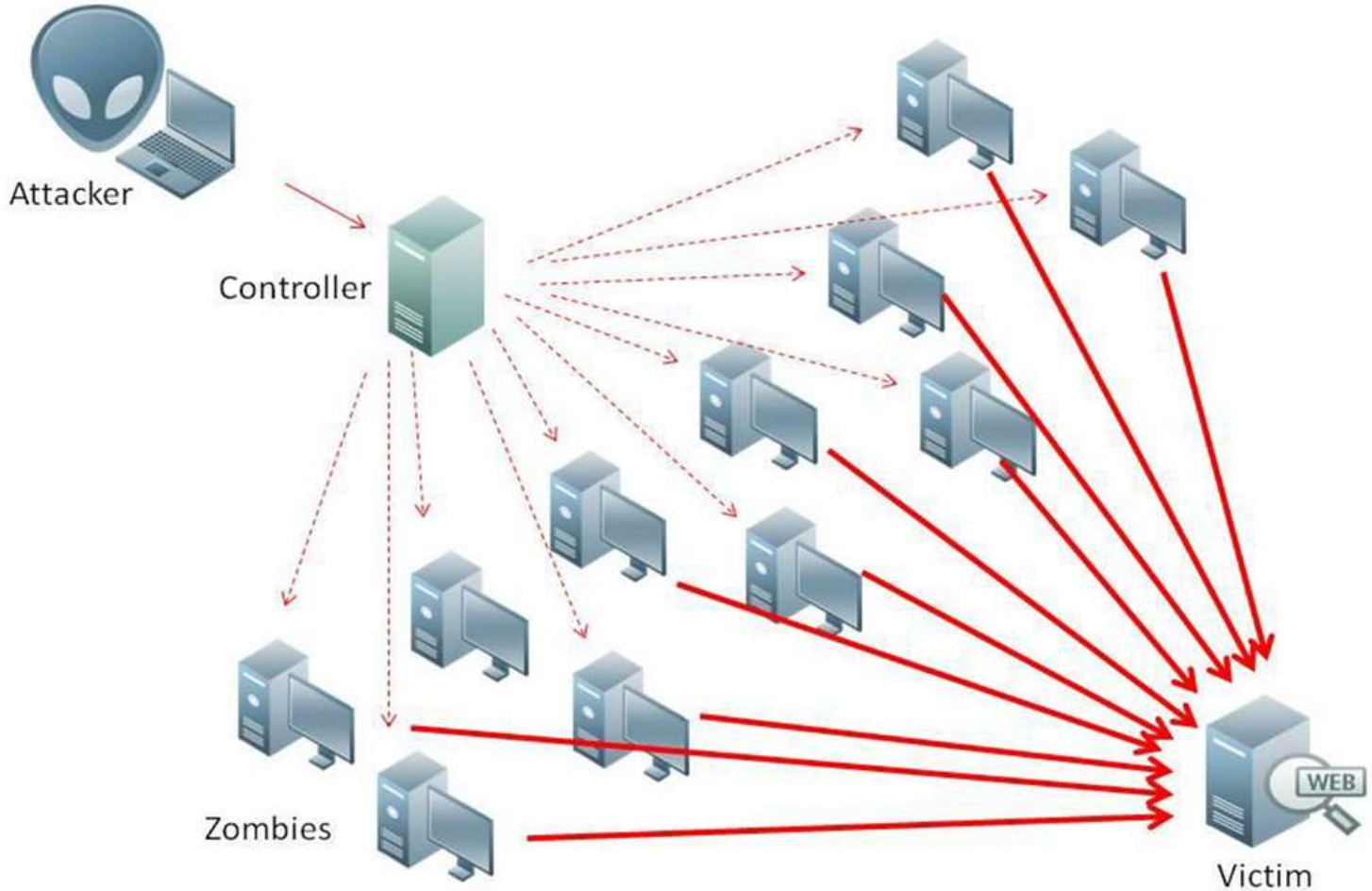
以太坊的设计目标

弥补比特币的智能合约功能有限的问题

并且应确保不能受到DoS攻击

为此设计了可燃烧的以太币

DoS拒绝服务攻击



https://www.realnets.com/our-blog/massive-ddos-attacks-lizardstresser/

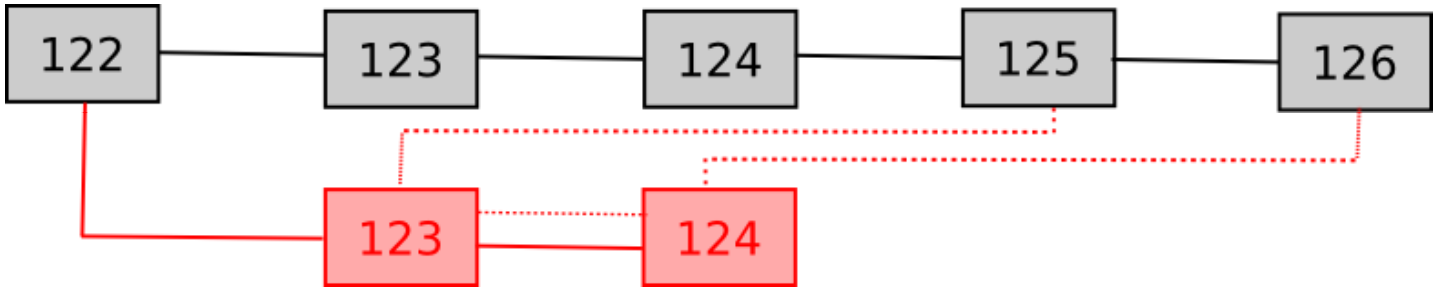
技术手段

- 共识协议（提高共识速度）
- 账户模型（通用服务）
- EVM虚拟机及Gas机制（全能且防DoS）

GHOST 共识协议

GHOST共识协议可以解决以下问题

- *在网络上的块生成速度*
- *矿工过于集中的问题*

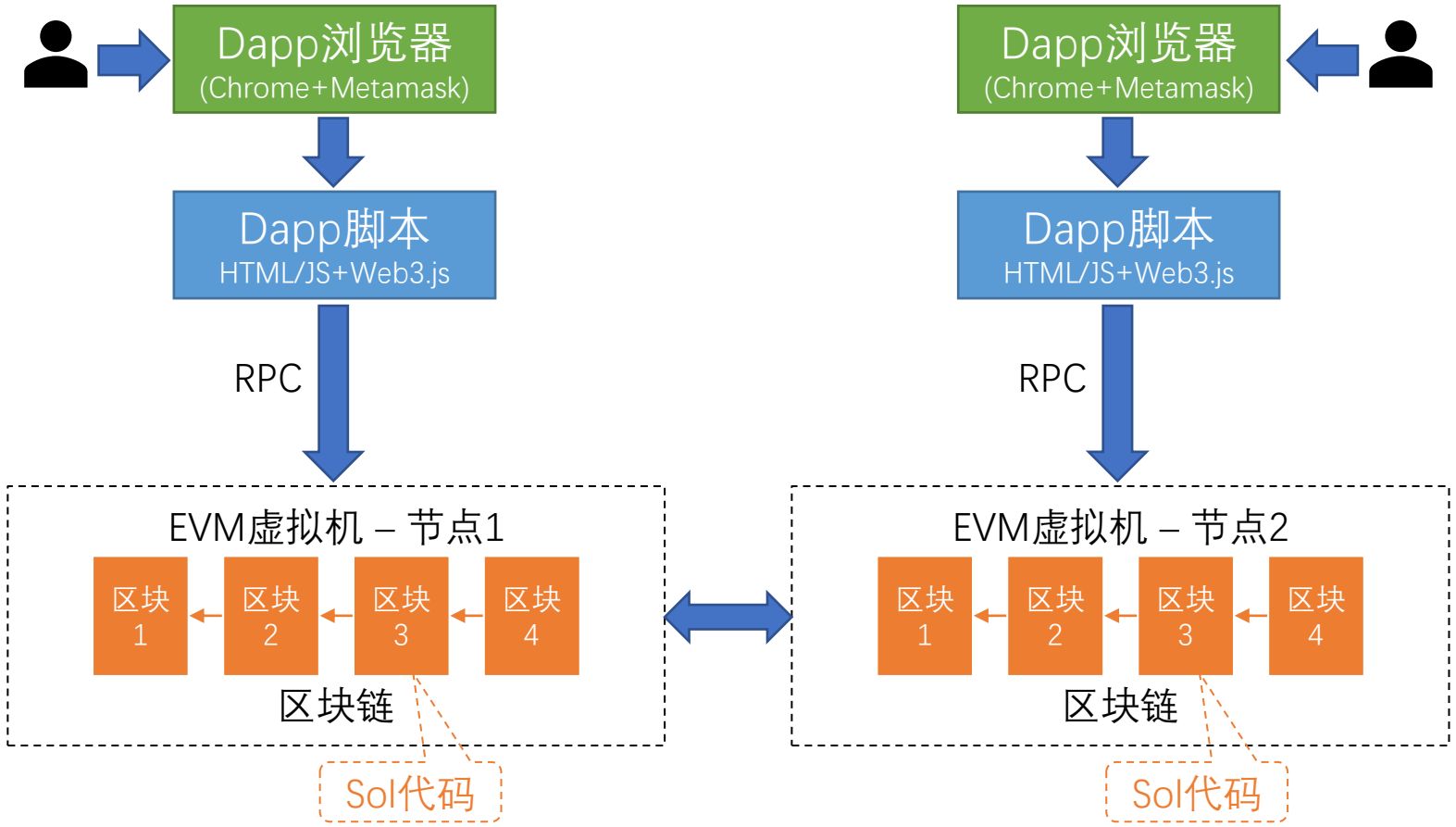


执行机制

EVM

执行过程

执行流程


Dapp浏览器
(Chrome+Metamask)
Dapp脚本
HTML/JS+Web3.js
RPC
EVM虚拟机 – 节点1
区块1
区块2
区块3
区块4
区块链
Sol代码
Dapp浏览器
(Chrome+Metamask)
Dapp脚本
HTML/JS+Web3.js
RPC
EVM虚拟机 – 节点2
区块1
区块2
区块3
区块4
区块链
Sol代码

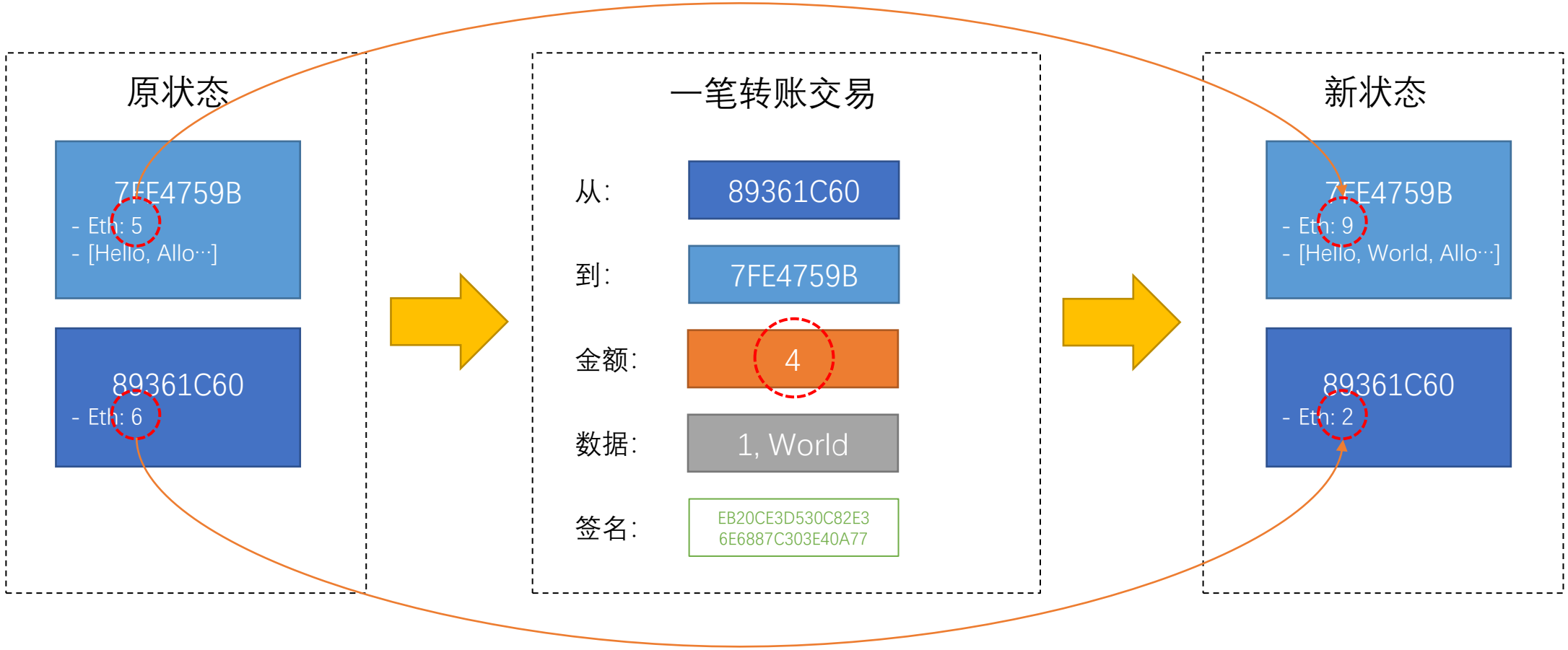
状态转换


原状态
7FE4759B:0
89361C60:1
C2900679:2
BA3130A7:3
18775100:4
一笔交易
使用:
签名:
89361C60:1
EB20CE3D530C82E3
6E6887C303E40A77
C2900679:2
60E4533E3D4820B6
57DF5D506C22023A
创建:
6F4B60C2:0
6F4B60C2:1
6F4B60C2:2
新状态
7FE4759B:0
BA3130A7:3
18775100:4
6F4B60C2:0
6F4B60C2:1
6F4B60C2:2

状态转换

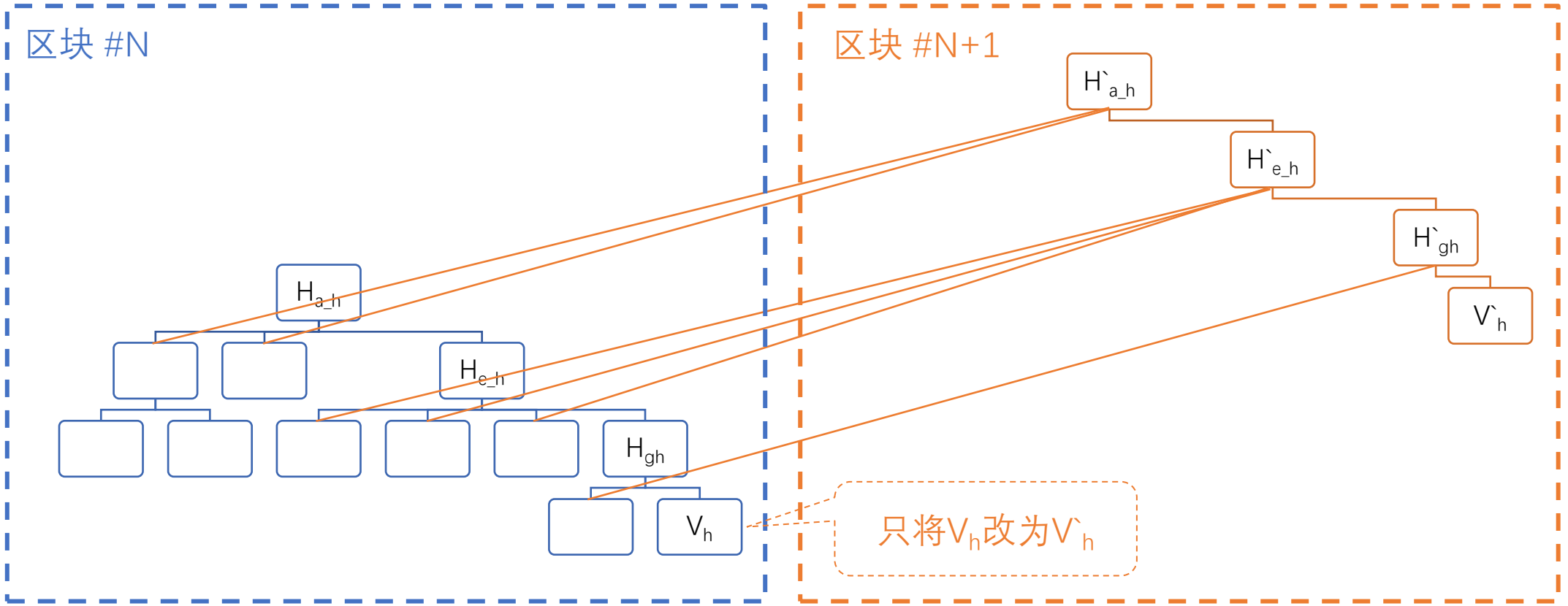

原状态
7FE4759B
- Eth: 5
- [Hello, Allo···]
89361C60
- Eth: 6
一笔转账交易
从:
89361C60
到:
7FE4759B
金额:
4
数据:
1, World
签名:
EB20CE3D530C82E3
6E6887C303E40A77
新状态
7FE4759B
- Eth: 9
- [Hello, World, Allo···]
89361C60
- Eth: 2

状态转换
(观察以太币的变化)



状态转换
（观察状态的变化）

状态转换的存储方法



以太坊的设计目标

弥补比特币的智能合约功能有限的问题

并且应确保不能受到DoS攻击

为此设计了可燃烧的以太币

EOS的设计目标

解决以太坊上每笔交易都要花费的问题

并且仍旧需要防止DoS的发生

设计以代币持有量代表计算资源的机制

技术手段

- 利用WASM执行（便于移植）
- 数据存储在IPFS（数据层）

Chia的设计目标

解决比特币的耗电和智能合约功能受限的问题

并且共识仍旧安全、合约更加智能

设计时空证明共识及Chialisp智能合约语言

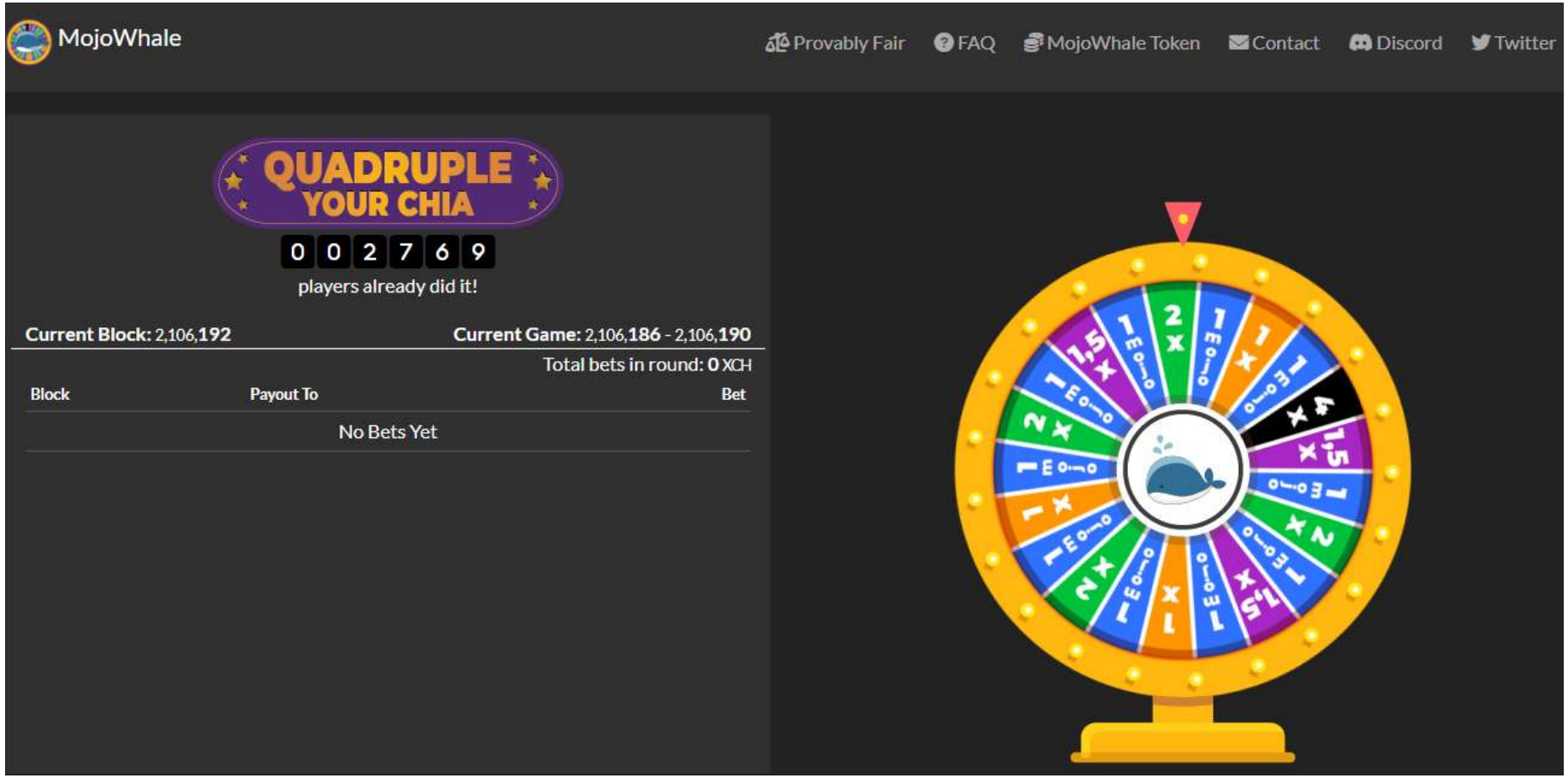
技术手段

- 可验证延迟函数（VDF）
- 时空证明（PoST）
- 智能合约Chialisp

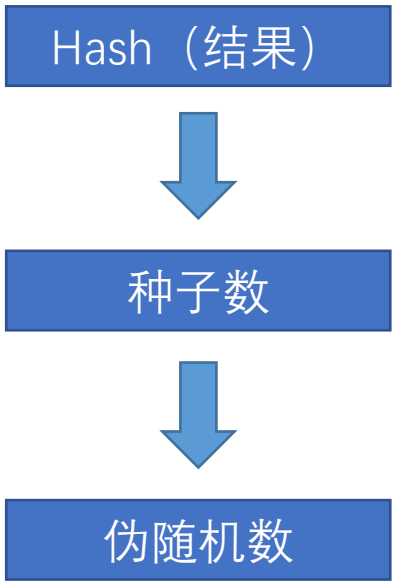
可验证延迟函数

VDF (Verifiable Delay Function)

VDF作为随机信标


MojoWhale
Provably Fair
FAQ
MojoWhale Token
Contact
Discord
Twitter
QUADRUPLE
YOUR CHIA
0 0 2 7 6 9
players already did it!
Current Block: 2,106,192
Current Game: 2,106,186 - 2,106,190
Total bets in round: 0 XCH
Block
Payout To
Bet
No Bets Yet

确保随机性



场景

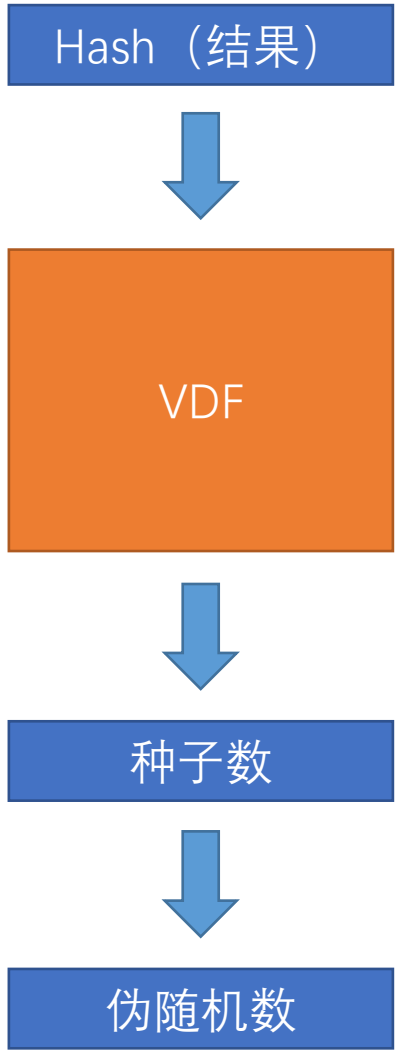
- 利用上次结果作为下次计算的随机数种子

问题

- 控制结果以控制种子数，使得随机数有利于自己

解决

- 增加VDF环节，使得验证随机数是否有利于自己的成本大幅提高



时空证明

PoST（Prove of Space-Time）

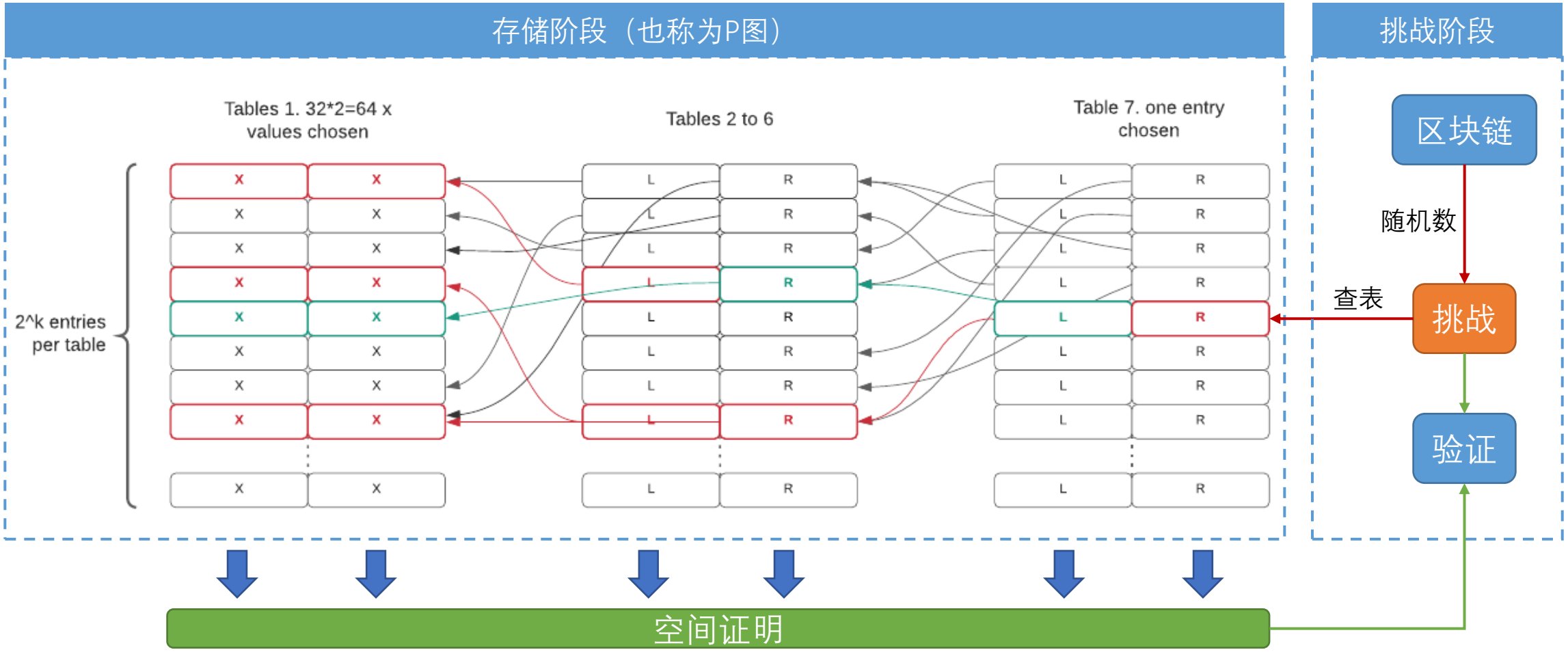
时空证明 Prove of Space-Time

在**一段时间内**证明**拥有一定量**的磁盘空间

时间证明 Prove of Time
方法：VDF

空间证明 Prove of Space
方法：查表

空间证明


存储阶段（也称为P图）
挑战阶段
Tables 1. 32*2=64 x values chosen
Tables 2 to 6
Table 7. one entry chosen
2^k entries per table
区块链
随机数
查表
挑战
验证
空间证明

Chia的设计目标

解决比特币的耗电和智能合约功能受限的问题

并且共识仍旧安全、合约更加智能

设计时空证明共识及Chialisp智能合约语言

未来区块链的设计目标

解决效率与安全的问题

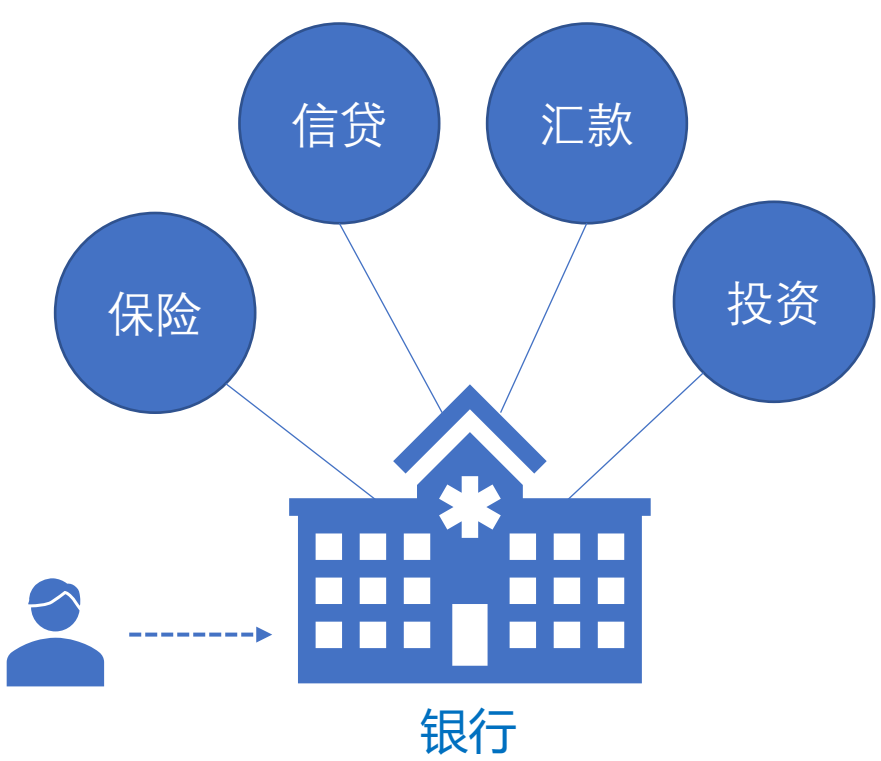
并且共识依旧足够去中心化

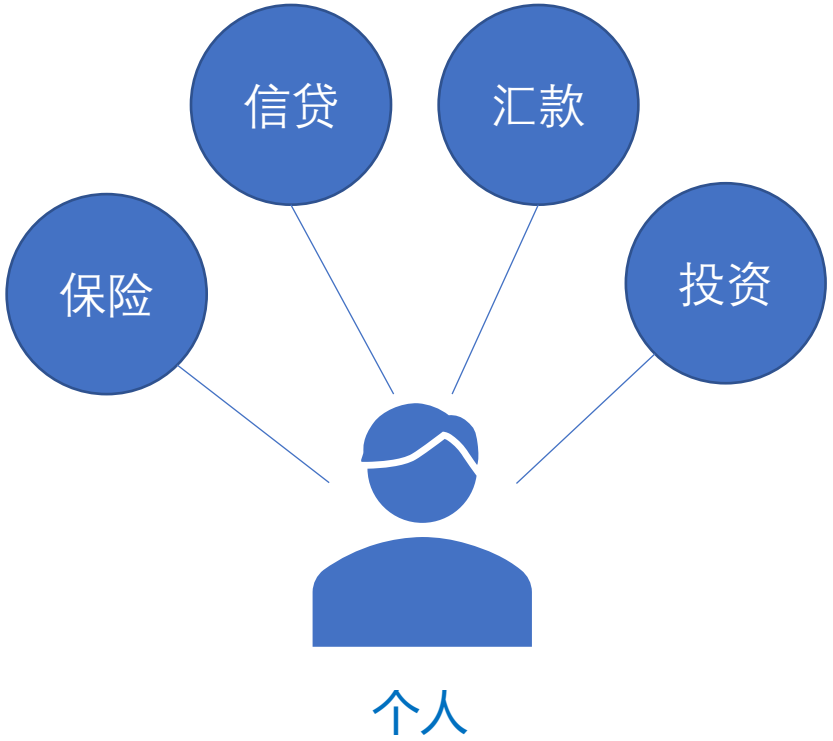
例如DAG、ZK等技术都被大范围实验中

区块链的华丽乐章才刚开始

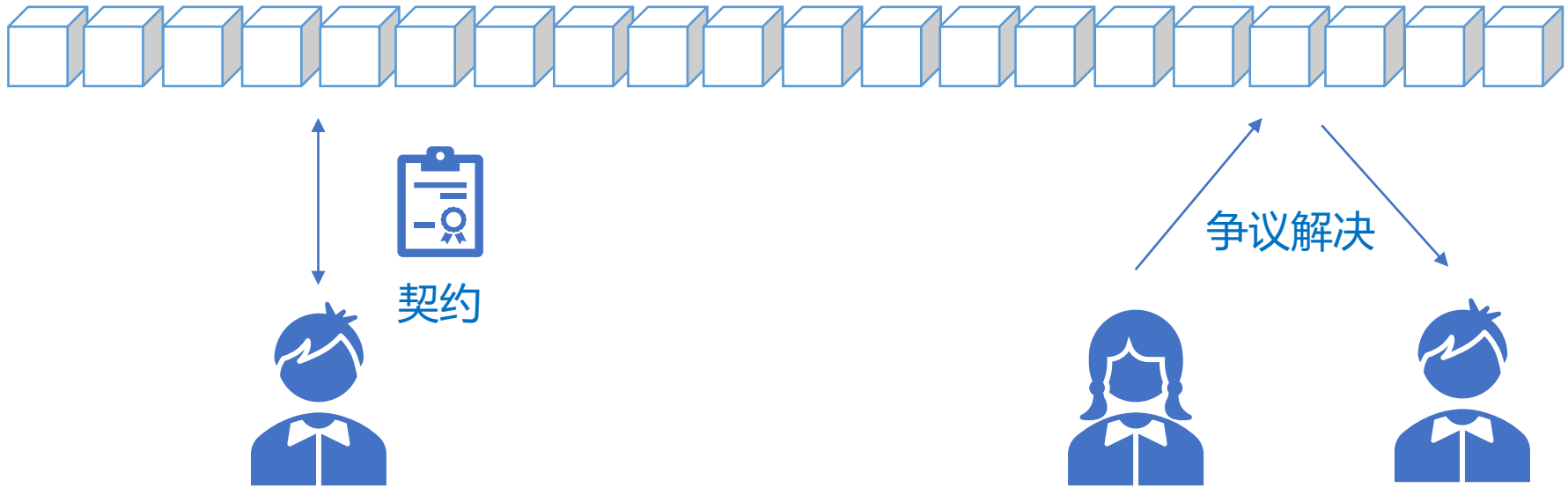
区块链带给我们的未来

金融自由化

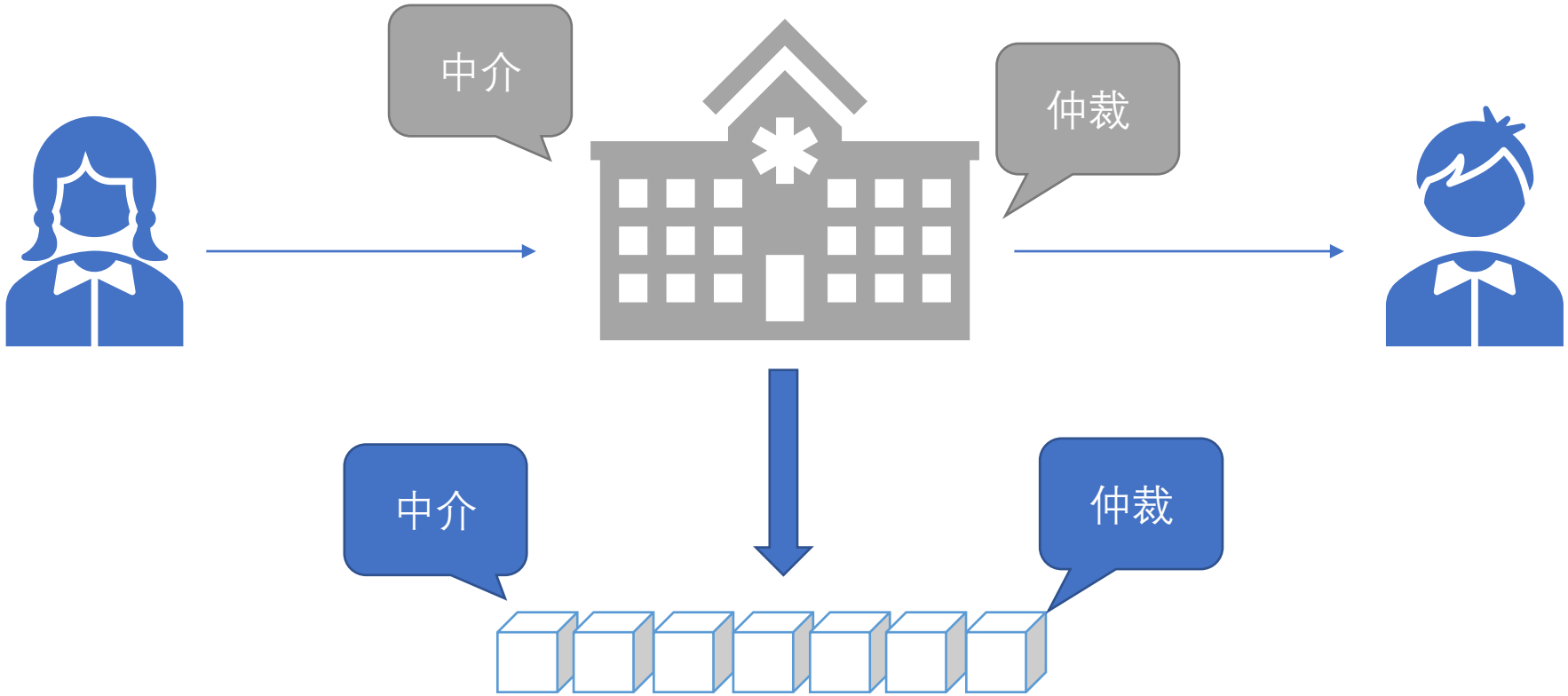




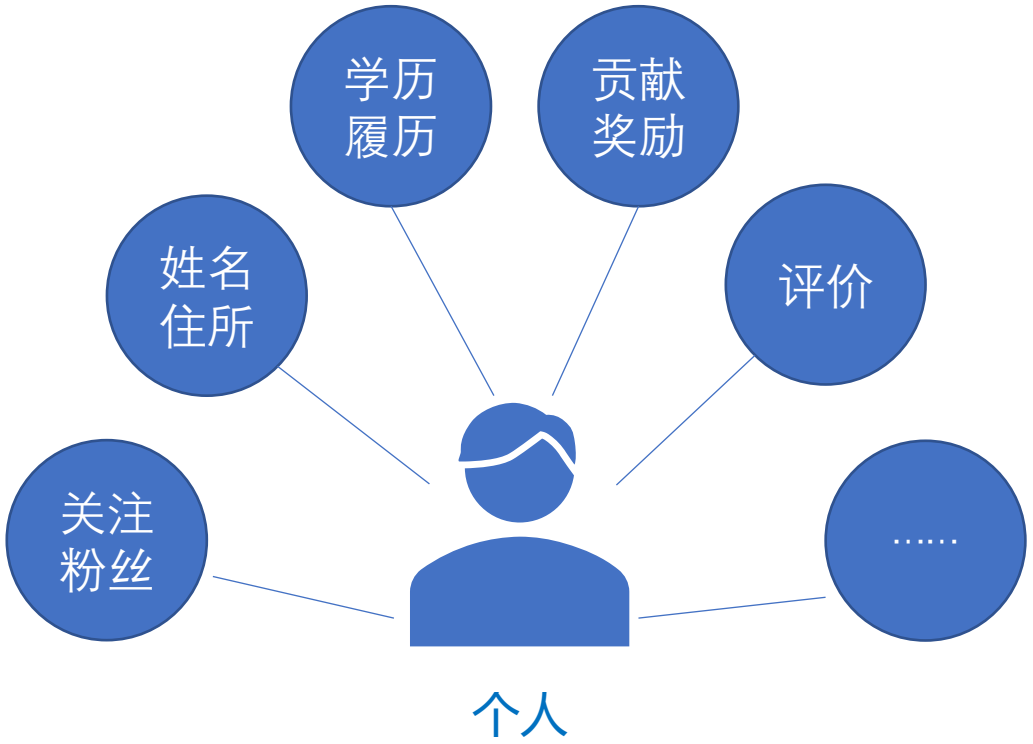
电子化适用范围更广



个人间的直接交易更活跃



自己的资产由自己管理



Chialisp SH Workshop

区块链开发工作坊

时间：3月18日 14:00-17:30

地点：国康路100号上海国际设计中心22楼多功能厅

2023 Mar 18th, 14:00-17:30

议程：

14:00-14:20 从B到C，区块链的发展史

14:20-15:00 Chia的技术路线图

15:00-15:40 丢币的N种方式（如何保障钱包安全？）

15:40-16:00 茶歇

16:00-16:40 Chialisp开发入门

16:40-17:00 Chia NFT介绍

17:00-17:30 现场提问时间