区块链技术

北京大学 软件与微电子学院
School of Software and Microelectronics, Peking University

Huiping Sun(孙惠平)
sunhp@ss.pku.edu.cn

Blockchain Technology

上次课程内容

技术驱动金融

1 新经济蓝图

- 区块链+
- 存证
- DAPP
- 数字化

2 应用逻辑

- 机动车挑战
- 机动车链
- 防欺诈
- 平台系统

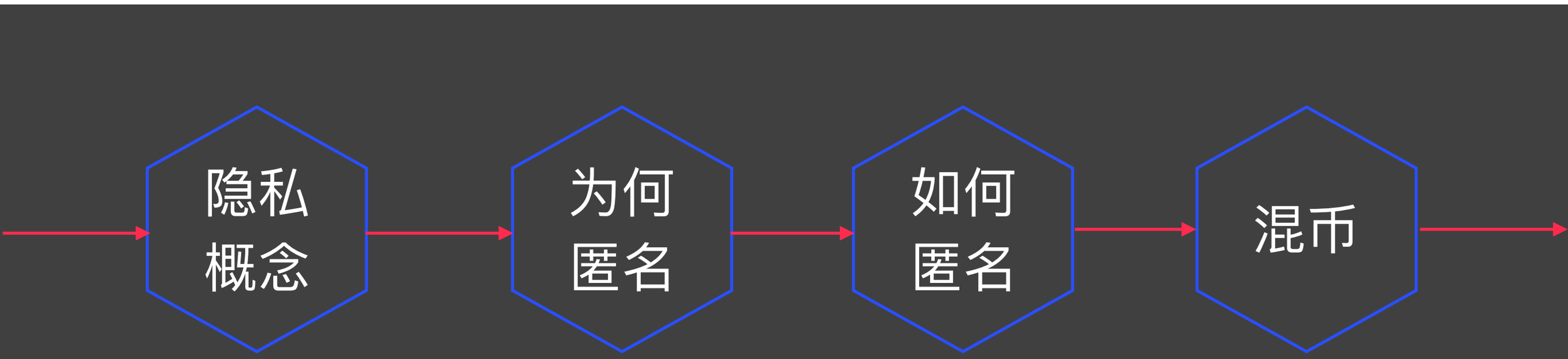
3 保险应用

- 保险背景
- 自动化
- 风险定价
- 里程表

4 其余应用

- 国际贸易
- 服务平台
- 供应链金融
- 政务应用

匿名



比特币是安全的匿名的加密货币

比特币不能帮你逃脱NSA的监控

隐私：定义

- 任何人的私生活、家庭、住宅和通信不得任意干涉，他的荣誉和名誉不得加以攻击，人人有权享受法律保护，以免受这种干涉和攻击。

The Right to be Let Alone

隐私：正面和方面

私人空间

家庭
城邦

公共空间

private：私
privare：剥夺

私人空间

社交空间

公共空间

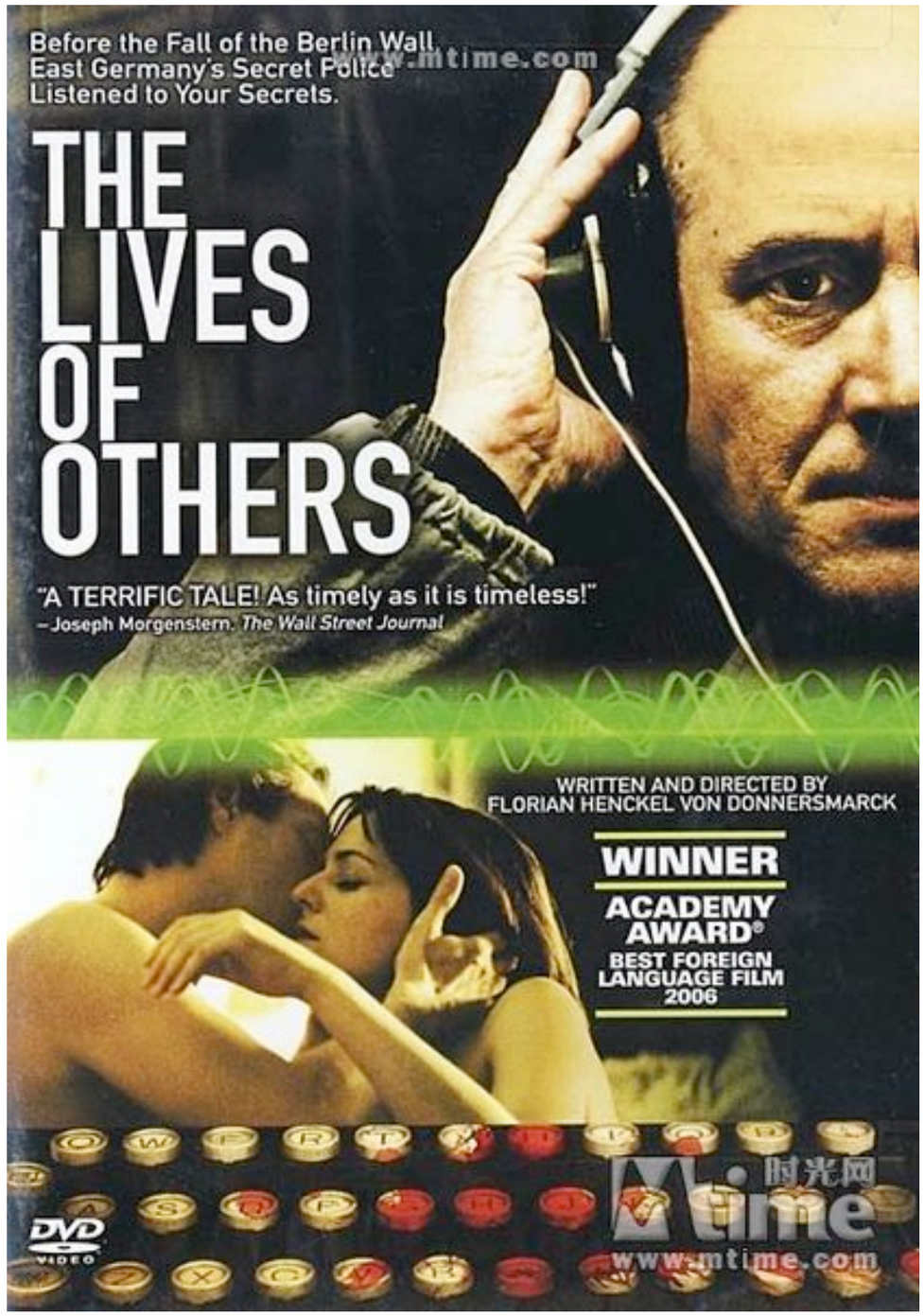
照相机　　摄像机　　网络

摄像头　　闭路监控　　大数据

GPS　　智能手机　　物联网

隐私: 两个电影


1984
The Film of the Year


Before the Fall of the Berlin Wall,
East Germany's Secret Police
Listened to Your Secrets.
THE LIVES OF OTHERS
"A TERRIFIC TALE! As timely as it is timeless!"
– Joseph Morgenstern, The Wall Street Journal
WRITTEN AND DIRECTED BY
FLORIAN HENCKEL VON DONNERSMARCK
WINNER
ACADEMY AWARD®
BEST FOREIGN LANGUAGE FILM
2006
DVD VIDEO
www.mtime.com

隐私：相关事件

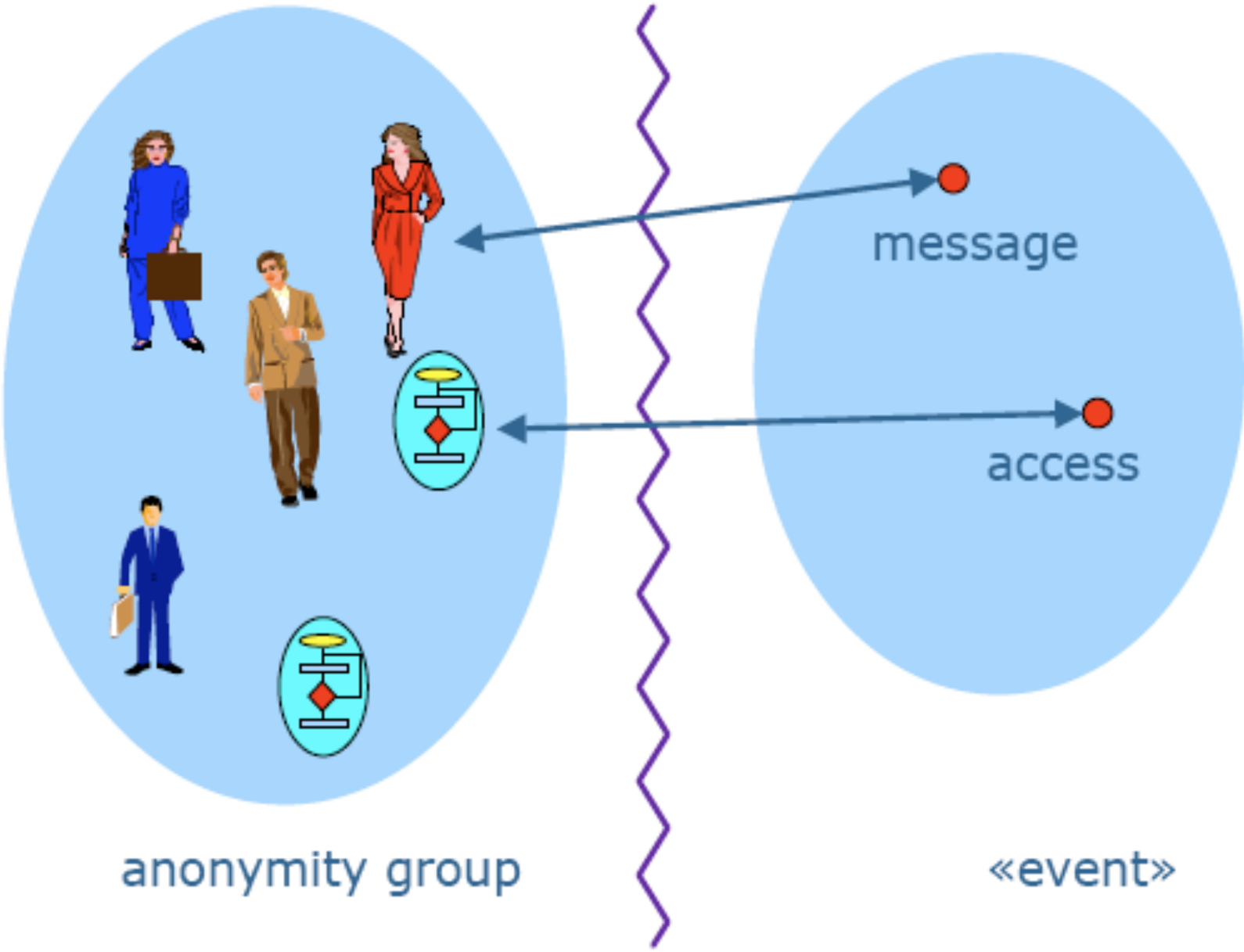
http://maherarar.net/

Cambridge Analytica

facebook

Google:
Don't be evil.

隐私保护



无关联性

比特币的匿名性

- 匿名：没有名字
  - ✶ 交易的时候不使用真实的姓名
  - ✶ 交易的时候完全不使用任何名字
- 比特币使用公钥Hash作为地址
- CS：匿名＝化名＋无关联性
- 比特币具有化名性
- 把比特币地址和真实身份关联起来并不困难

比特币为什么需要匿名

- 比特币的交易信息是公开的
- 旁路攻击、污点分析、匿名集合(定量)
- 匿名的好坏、匿名的道德评判(洗钱等)

- 同一个用户的不同地址应该不易关联
- 同一个用户的不同交易应该不易关联
- 同一个交易的交易双方应该不易关联

K匿名

Name	Age	Gender	State of domicile	Religion	Disease
Ramsha	29	Female	Tamil Nadu	Hindu	Cancer
Yadu	24	Female	Kerala	Hindu	Viral infection
Salima	28	Female	Tamil Nadu	Muslim	TB
sunny	27	Male	Karnataka	Parsi	No illness
Joan	24	Female	Kerala	Christian	Heart-related
Bahuksana	23	Male			
Rambha	19	Male			
Kishor	29	Male			
Johnson	17	Male			
John	19	Male			

数据脱敏

匿名集合

Name	Age	Gender	State of domicile	Religion	Disease
*	20 < Age ≤ 30	Female	Tamil Nadu	*	Cancer
*	20 < Age ≤ 30	Female	Kerala	*	Viral infection
*	20 < Age ≤ 30	Female	Tamil Nadu	*	TB
*	20 < Age ≤ 30	Male	Karnataka	*	No illness
*	20 < Age ≤ 30	Female	Kerala	*	Heart-related
*	20 < Age ≤ 30	Male	Karnataka	*	TB
*	Age ≤ 20	Male	Kerala	*	Cancer
*	20 < Age ≤ 30	Male	Karnataka	*	Heart-related
*	Age ≤ 20	Male	Kerala	*	Heart-related
*	Age ≤ 20	Male	Kerala	*	Viral infection

比特币去匿名

Bitcoin

Bitcoin is a secure and anonymous digital currency. Bitcoins cannot be easily tracked back to you, and are safer and faster alternative to other donation methods. You can send BTC to the following address:

36EEHh9ME3kU7AZ3rUxBCyKR5FhR3RbqVo

Various sites offer a service to exchange other

零钱地址的随机化

惯用法则

非零钱地址通常不是新地址

5

3

6

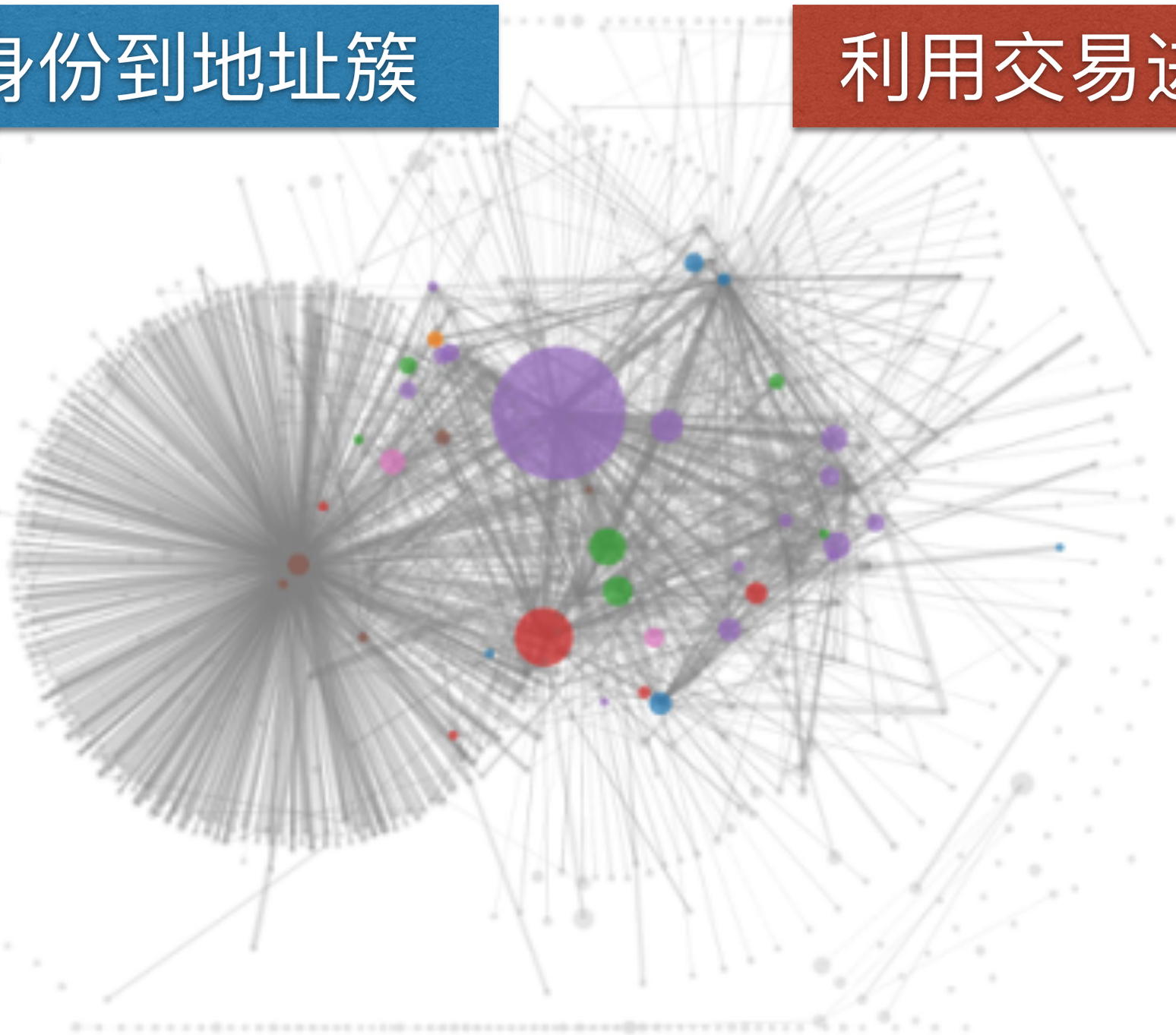
8

Single transaction

地址簇关联

关联真实身份到地址簇

利用交易进行标记



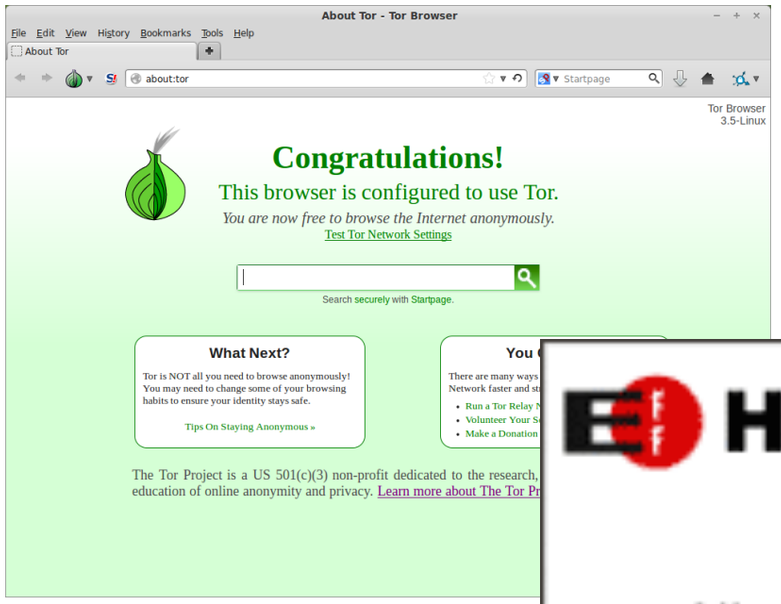
辨识个人：直接交易、通过服务提供商、疏忽

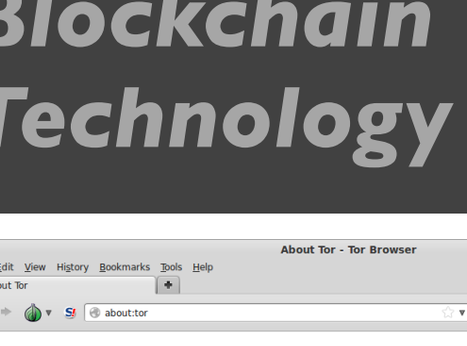
网络层去匿名

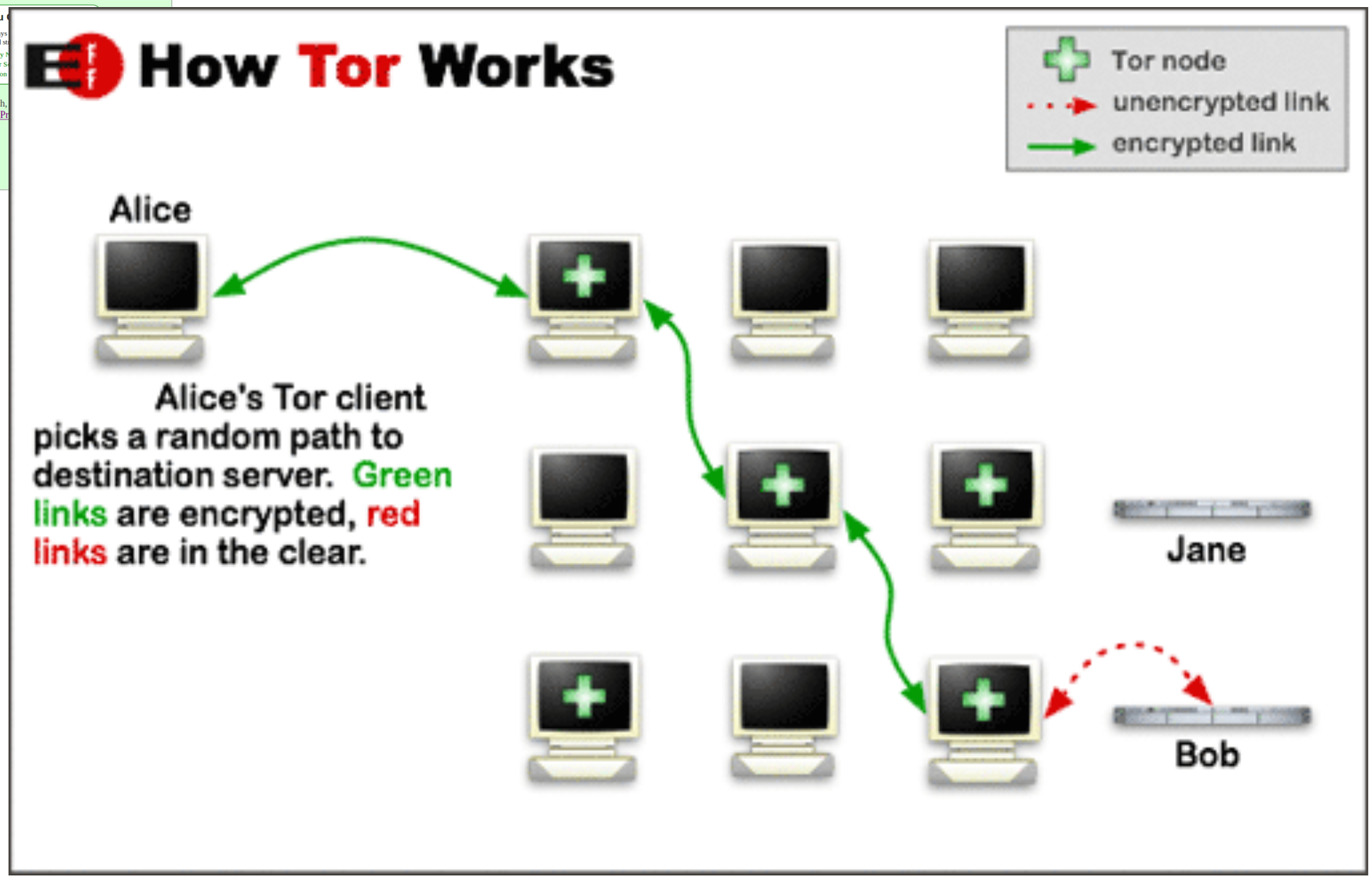
协议分析

第一个通知及交易的节点很可能就是交易源头

Tor

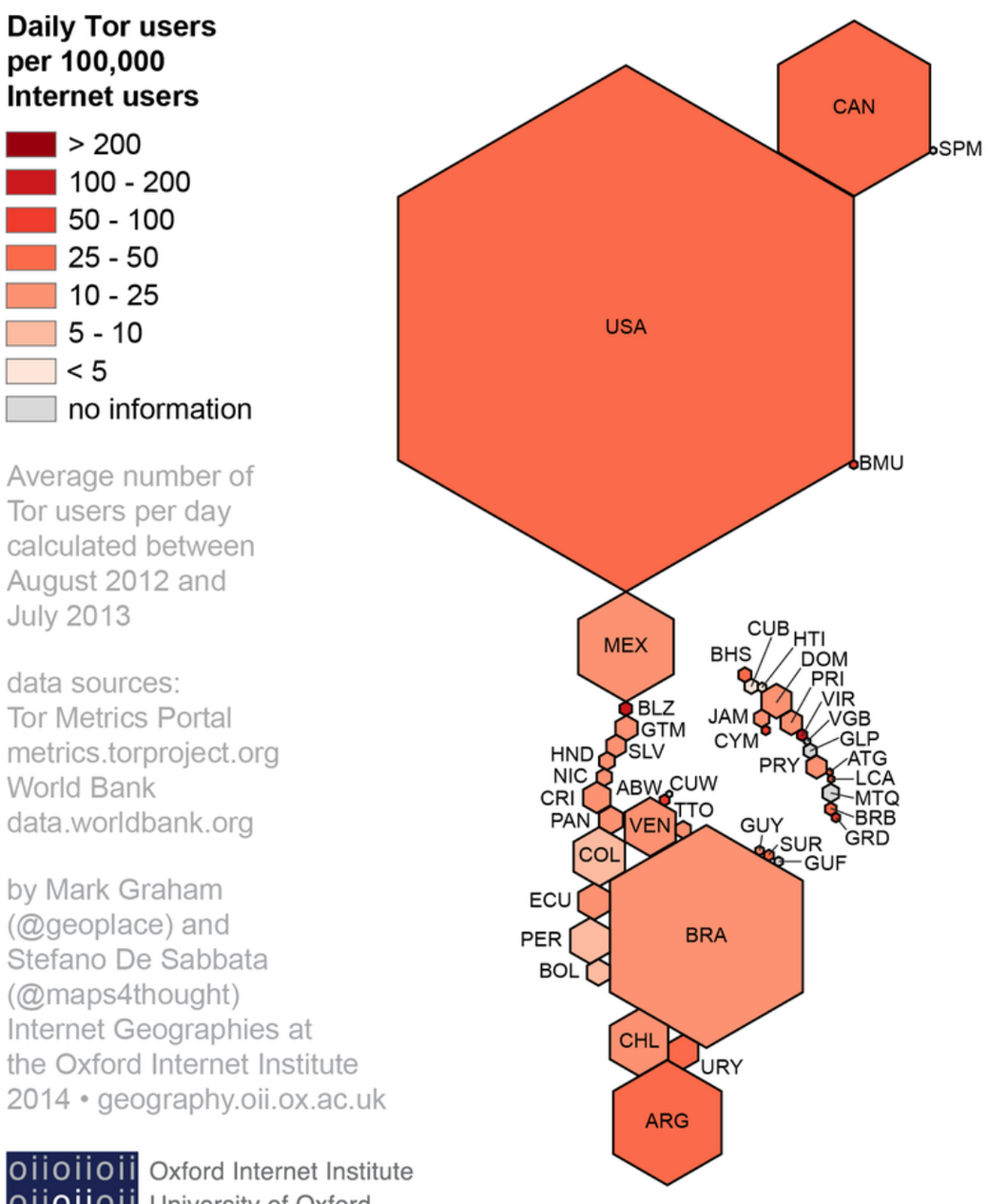

About Tor - Tor Browser
File Edit View History Bookmarks Tools Help
About Tor
about:tor
Startpage
Tor Browser 3.5-Linux
Congratulations!
This browser is configured to use Tor.
You are now free to browse the Internet anonymously.
Test Tor Network Settings
Search securely with Startpage.
What Next?
Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.
Tips On Staying Anonymous »
The Tor Project is a US 501(c)(3) non-profit dedicated to the research,
education of online anonymity and privacy. Learn more about The Tor Pr



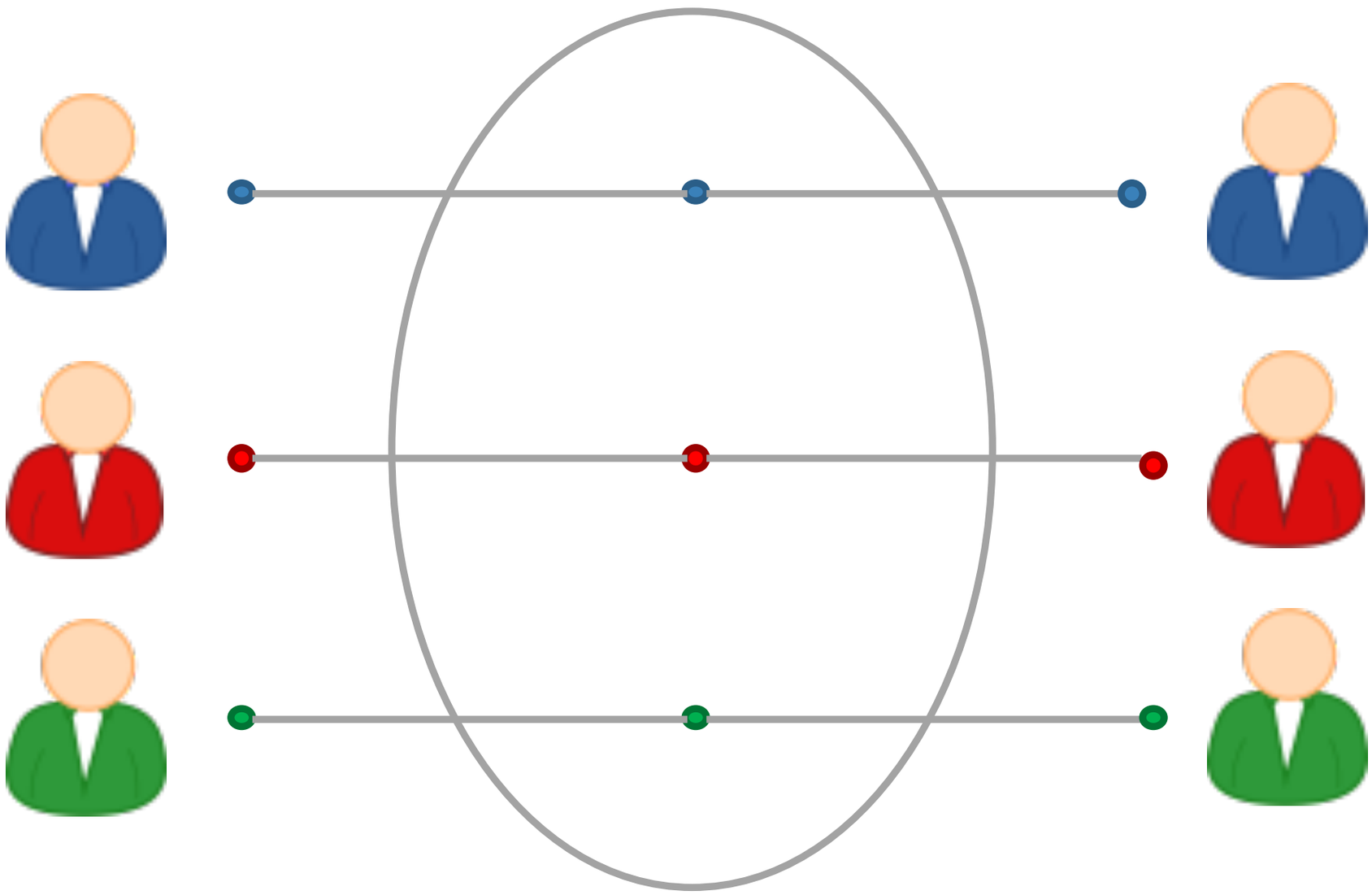

How Tor Works
Tor node
unencrypted link
encrypted link
Alice
Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Bob

Tor使用情况

The anonymous Internet



混币模式

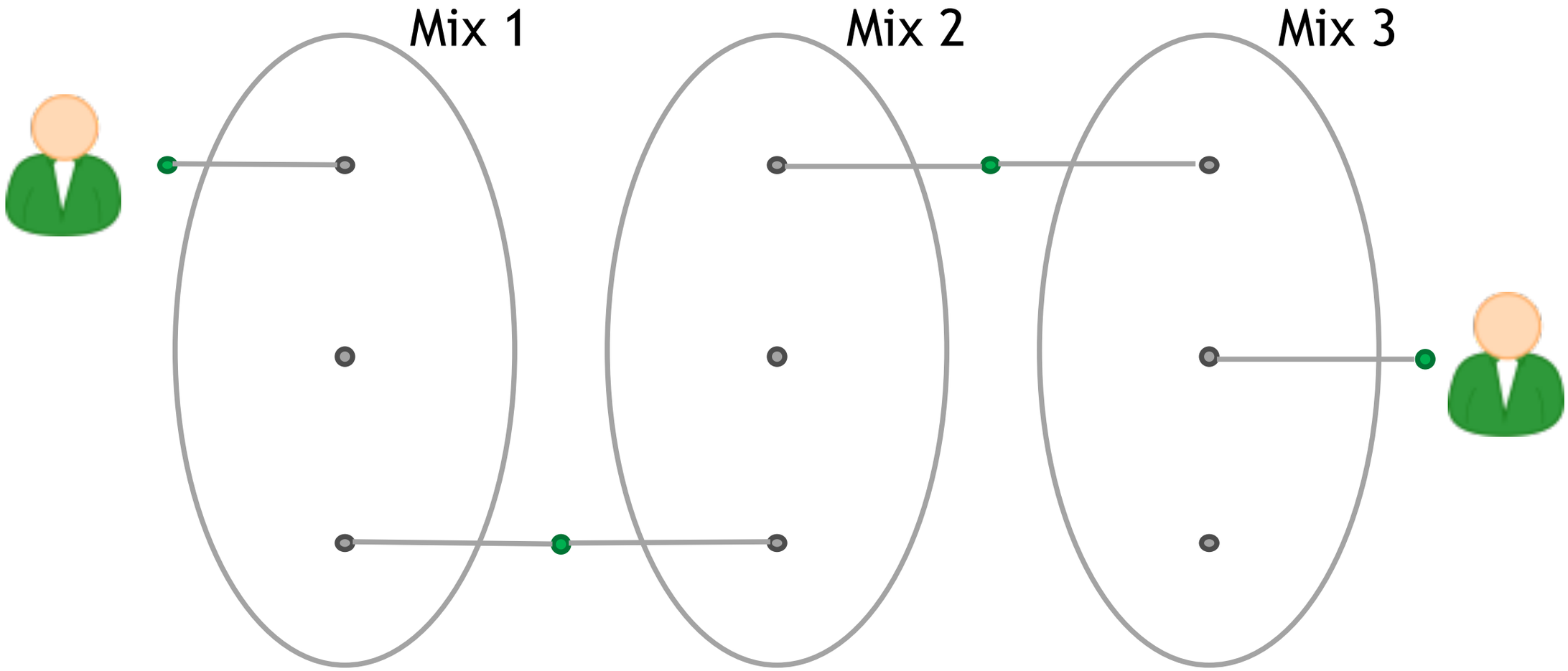


在线钱包

引入中介节点

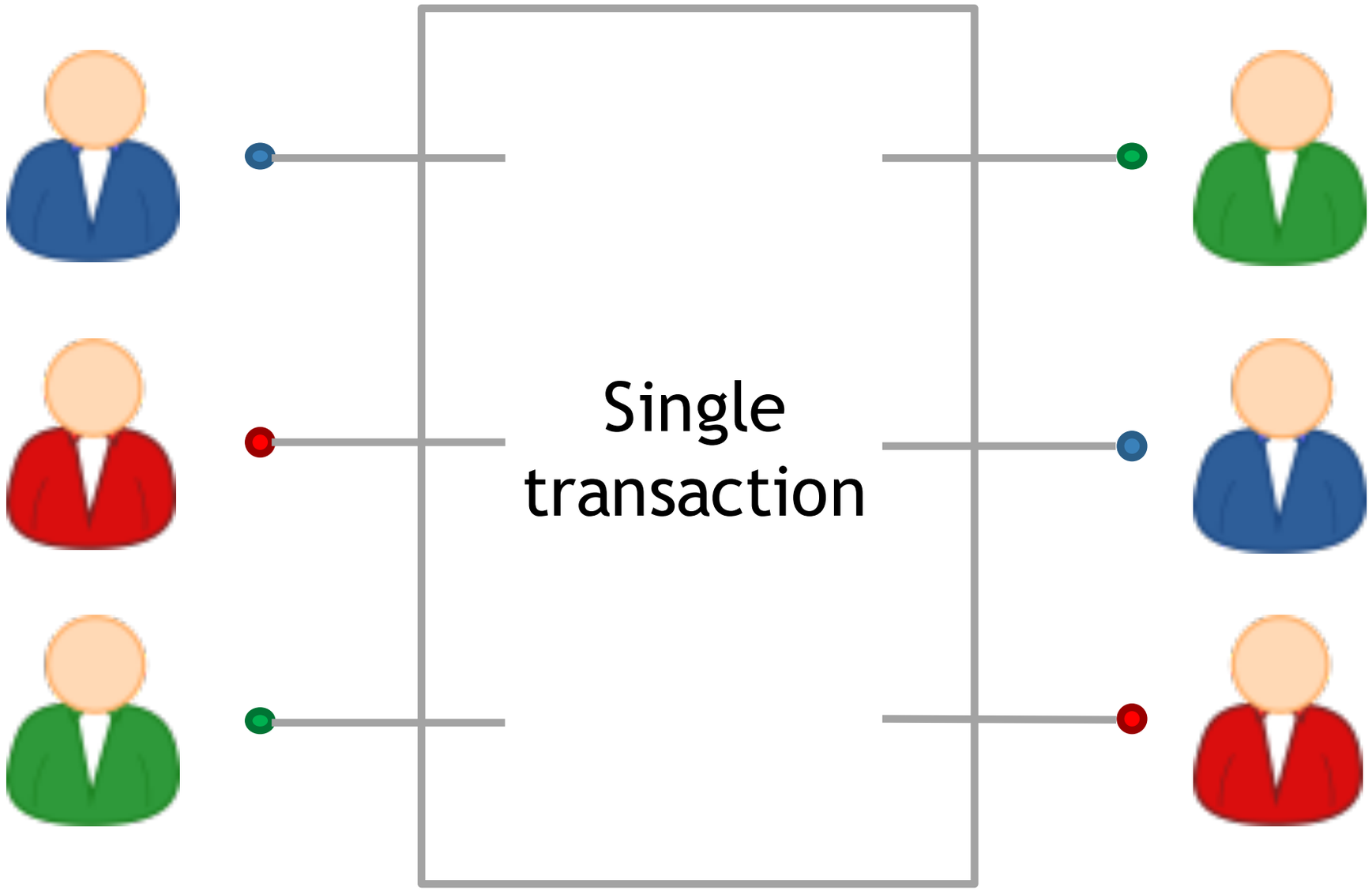
专项服务

多层混币



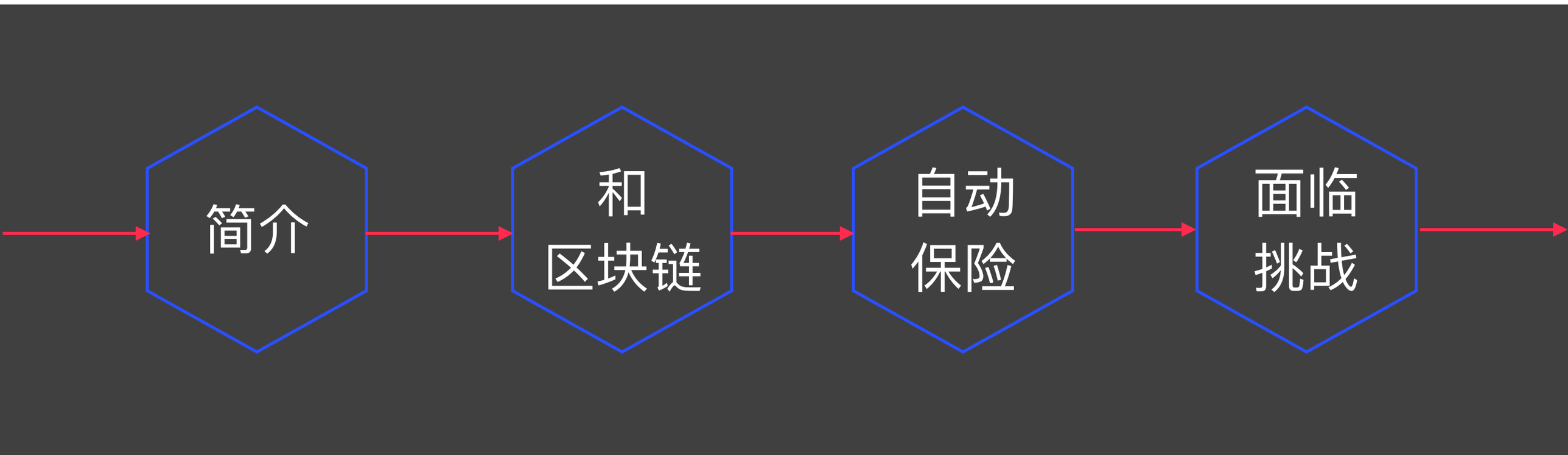
多重

分布式混币



分布式

智能合约



智能合约简介

一组数字形式描述的承诺

包括合约参与方可以执行这些承诺的协议

Nick Szabo 1990

ethereum

以太坊 2013

实际合约 | 部分合约 | 非合约

规则逻辑 | 软件代码 | 自动执行

身份标识 | 系统状态 | 发生事件

Blockchain Technology

智能合约和区块链

自动执行

非区块链智能合约

- 参与方认证
- 合约协商
- 编码合约
- 状态设定
- 合约发布
- 合约上链
- 合约更新
- 合约执行

智能合约在区块链上存储并执行

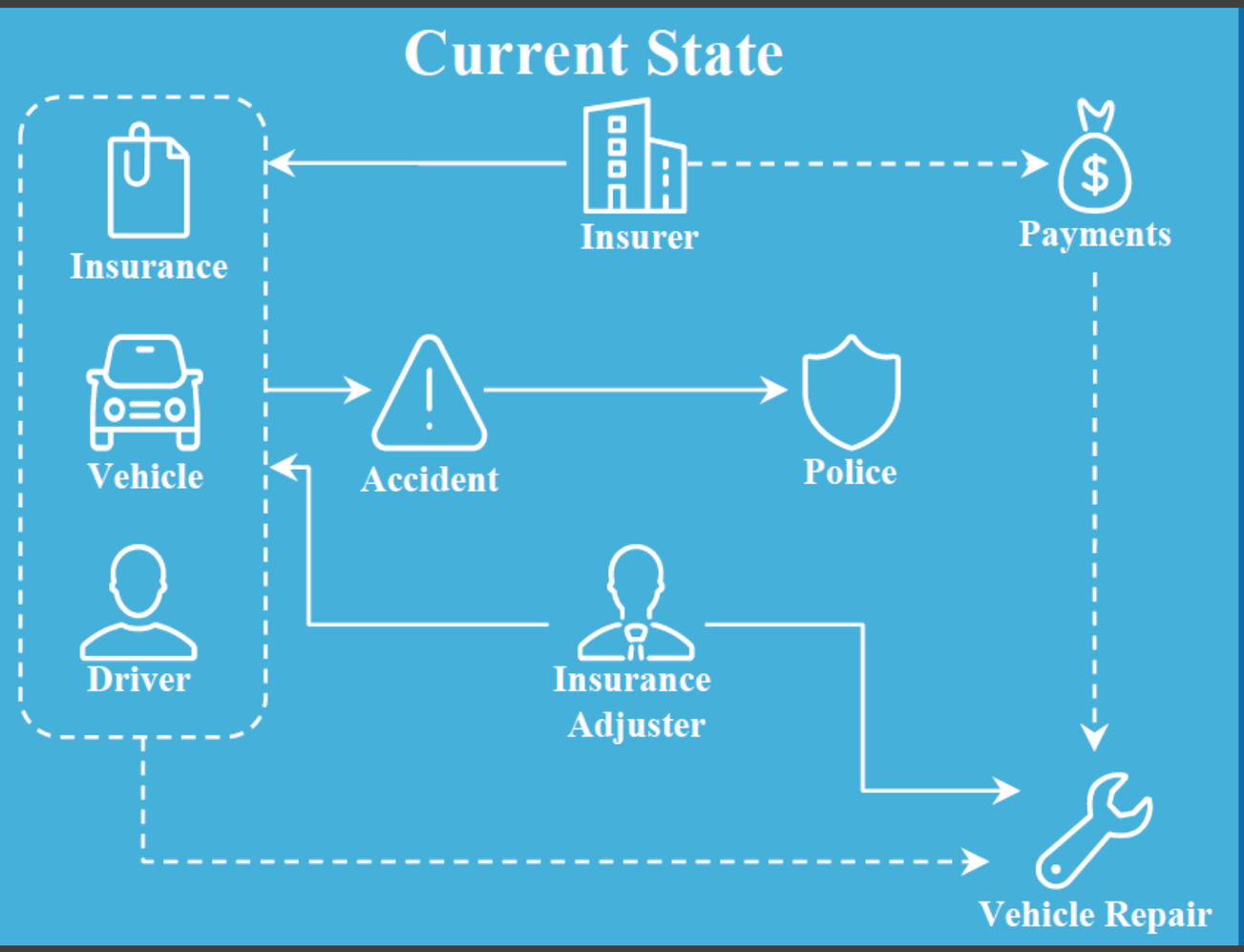
Block #FCAC
prev #618C
</> contract 2E12…
</> contract FECB…
</> contract 21E0…
…

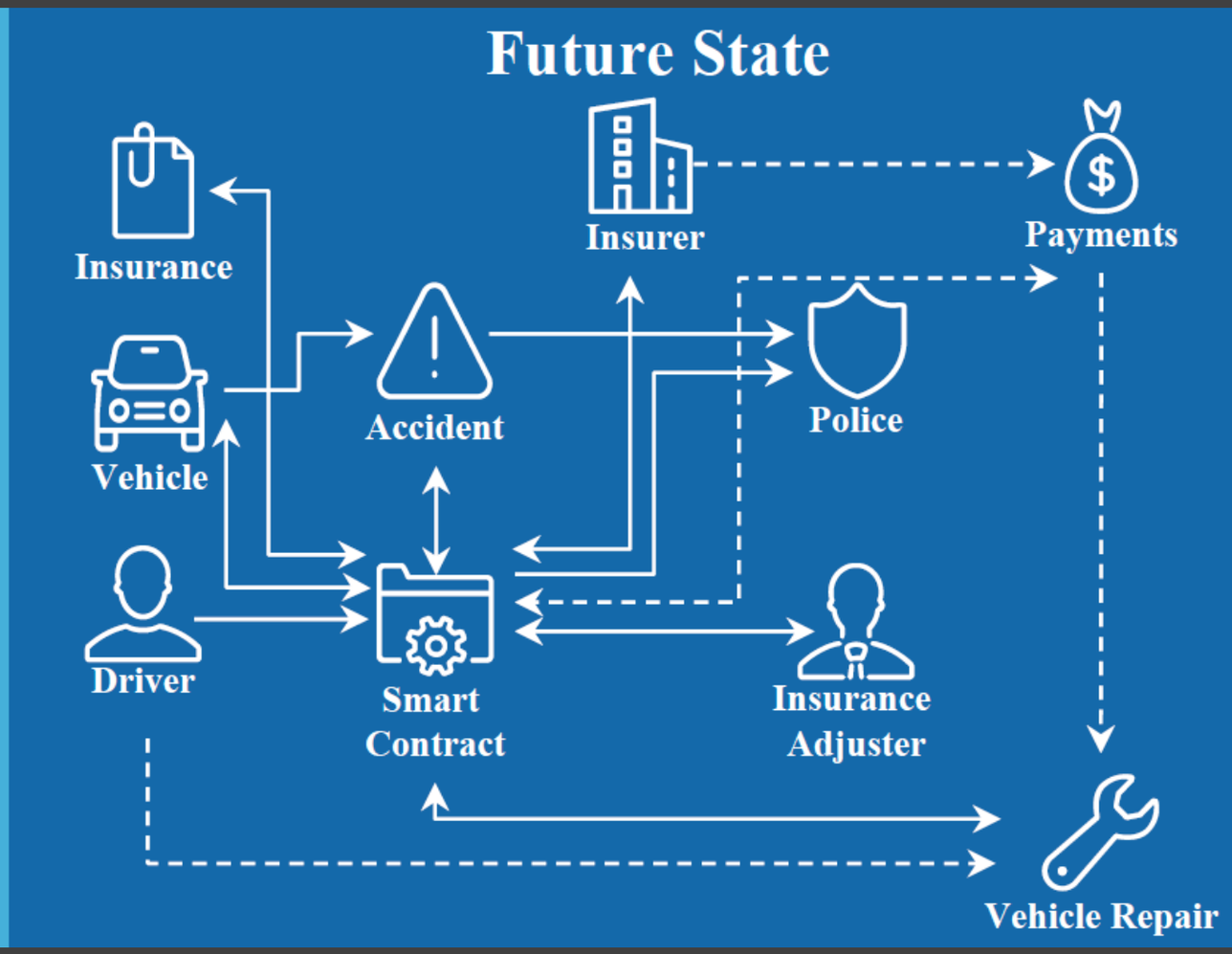
Block #51E5
prev #FCAC
</> contract 0EBF…
</> contract 7B4E…
</> contract 3390…
…

Block #
prev #
</> con
</> con
</> con
…

Blockchain Technology

智能合约应用案例 - 自动保险





P2P保险

指数保险

多方保险

资产管理

智能合约面临挑战

操作风险

- 缺乏有效的后备和故障切换机制
- 有时候依赖其余系统来履行合约
- 智能合约平台有可能存在问题
- 区块链存在硬分叉可能性

技术风险

- 任何软件都存在漏洞
- 人是会犯错误
- 网络、计算机、服务器风险
- 外部预言机失败、崩溃

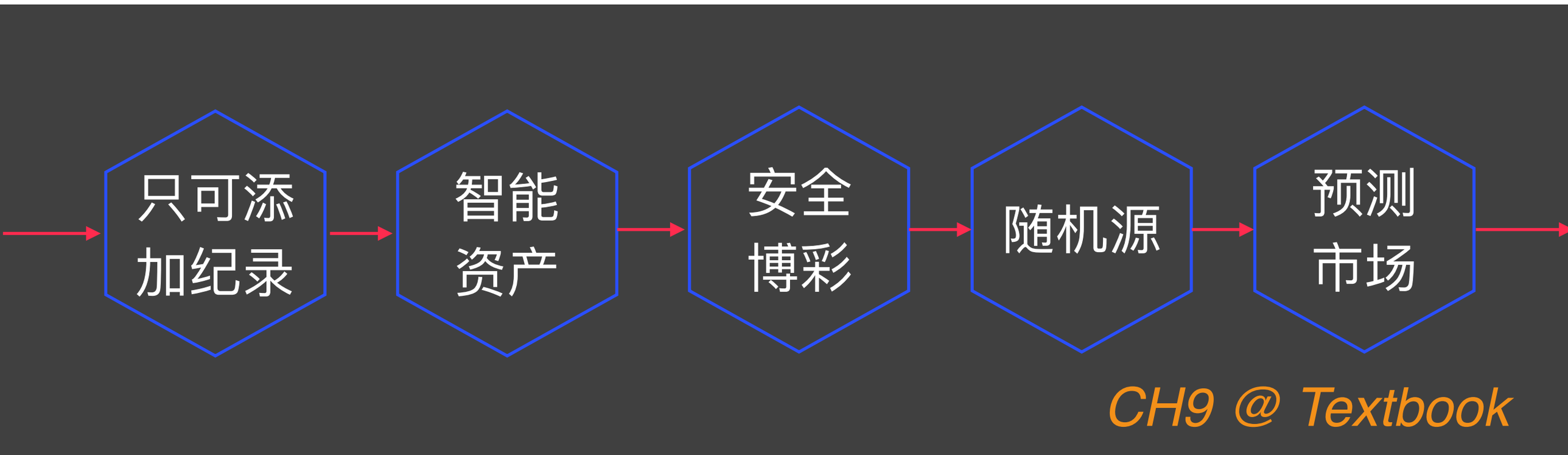
安全

- 智能合约执行的正确性判断
- 智能合约的安全性
- 相关系统的安全性
- 外部预言机的安全保证

监管

- 智能合约也可能包括不合法代码
- 内部人可以操控智能合约
- 智能合约实际执行和宣传不符
- 外部预言机被操纵

比特币作为平台



CH9 @ Textbook

比特币平台

- 比特币已经work，基于比特币能做什么？

- 作为一个只能增加的记录
- 作为一个智能资产
- 建立博彩系统
- 建立公共随机数源
- 建立预测市场

安全时间戳

- 时间TI公布H(r, x)，TI后可以公布r和x

时间戳　Hash指针　安全时间戳

- 证明创意的有限性
- 证明一些事件的先后顺序

版权登记的区块链应用　电子证据　面临挑战

预测未来

TWEETS 5 FOLLOWERS 3,925 More

Tweets Tweets and replies

FIFA Corruption @FifNdhs · 17h
There will be a goal in the second half of ET
17K 3.3K

FIFA Corruption @FifNdhs · 17h
Gotze will score
19K 3.8K

FIFA Corruption @FifNdhs · 17h
Germany will win at ET
17K 3.4K

FIFA Corruption @FifNdhs · 17h
Tomorrows scoreline will be Germany win 1-0
18K 3.6K

FIFA Corruption @FifNdhs · 17h
Prove FIFA is corrupt
15K 2.7K

FIFA2014

腐败指责

FIFA Corruption @fifndhs
Germany will win at ET
17 hours ago Reply Retweet Favorite 12K more

FIFA Corruption @fifndhs
Argentina will win in penalties
17 hours ago Reply Retweet Favorite

FIFA Corruption @fifndhs
Gotze will score
17 hours ago Reply Retweet Favorite 14K more

FIFA Corruption @fifndhs
There will be a goal in the second half of ET
17 hours ago Reply Retweet Favorite 12K more

FIFA Corruption @fifndhs
Kroos will score
17 hours ago Reply Retweet Favorite

FIFA Corruption @fifndhs
Lahm will score
17 hours ago Reply Retweet Favorite

FIFA Corruption @fifndhs
Palacio will score
17 hours ago Reply Retweet Favorite

离线时间戳


26
guardtime
guardtime.com
15 July 2009 00:00:00 UTC
AAAAAA-CKLUOA-AAI7FX-EKPAMP
VRUBSC-7DQE7O-TZBCP4-MS5S65
UEOSEC-UU2A3N-OCCCIR-PLM4PG
MARK
Friday July 17 2009
S&P 500 index
1000
950
Change on day -0.08%
Latest
US equities
Wall Street struggled for traction as concerns about the potential collapse of commercial lender CIT Group
FTSE 100 index
4600
4400
Change on day +0.35%
UK equities
Gains for banking stocks helped leave the FTSE 100 index on track for its best week since March after positive results from
FTSE Eur
950
900
850

刊登广告

比特币里的安全时间戳

- 直接把钱打到数据的Hash上，而不是一个公钥地址上
- 容易、兼容
- 消耗币、需要矿工一直追踪

- 使用OP_RETUTN,
- 返回错误代码、不能二次使用
- 便宜
- 非标准交易

OP_RETURN
<arbitrary data>

非法内容

没有办法防止

可以提高代价
P2SH

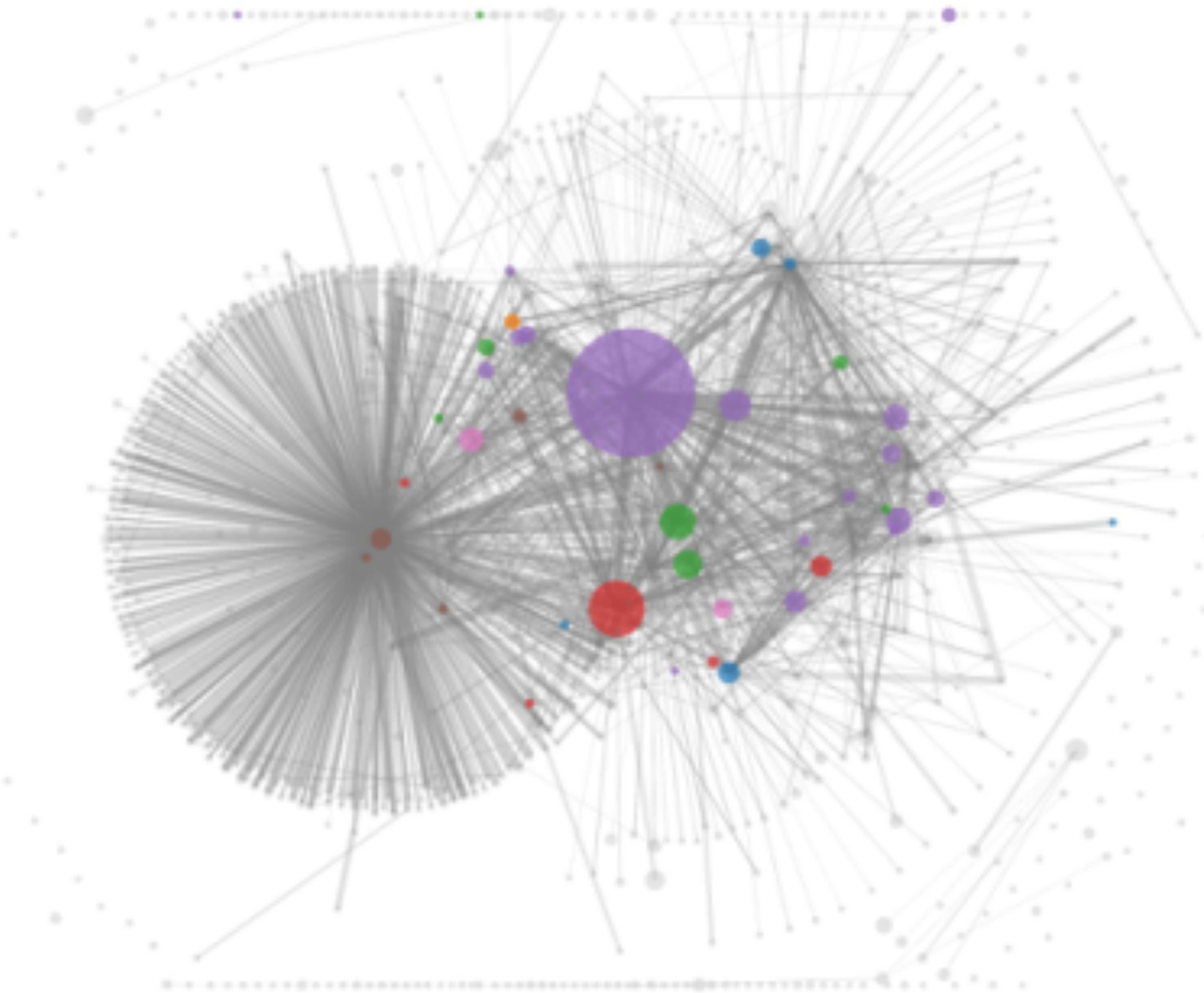
技术归技术

管理归管理

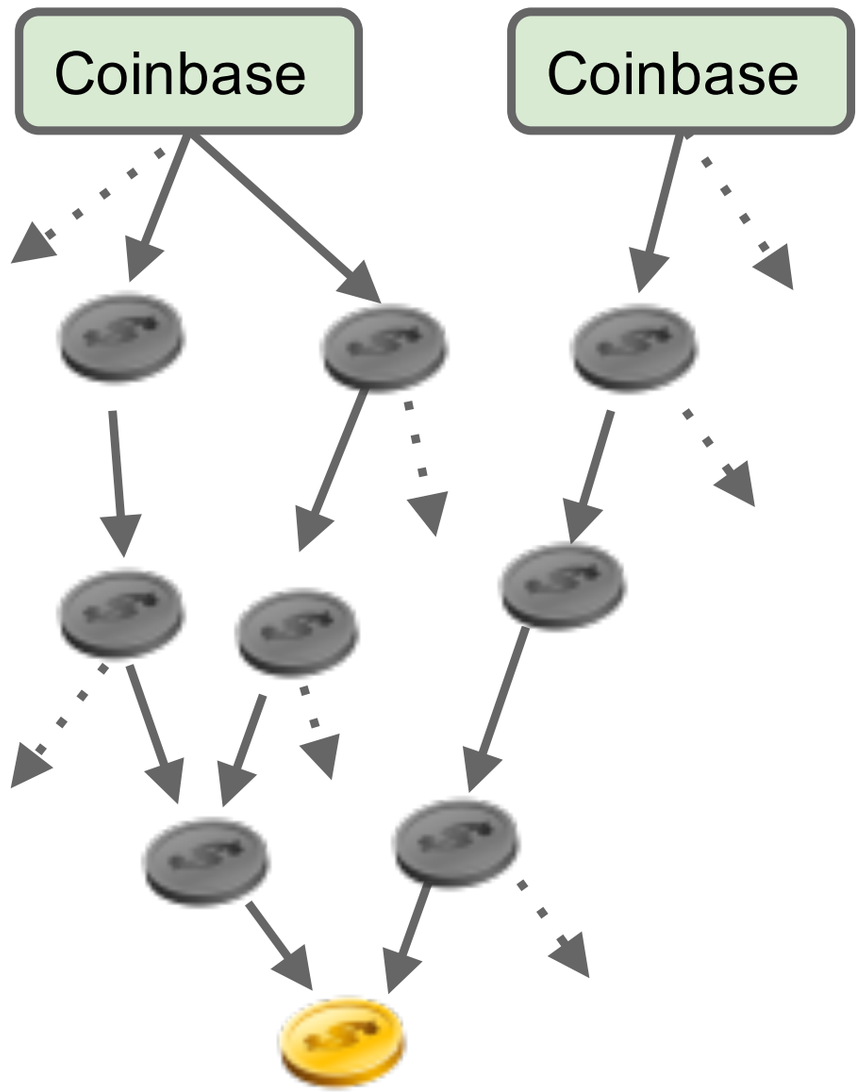
法律归法律

比特币交易历史

每一个比特币都是唯一的



每一个比特币都携带一些交易历史



可互换性

给货币增加元数据信息

成功平台的额外应用

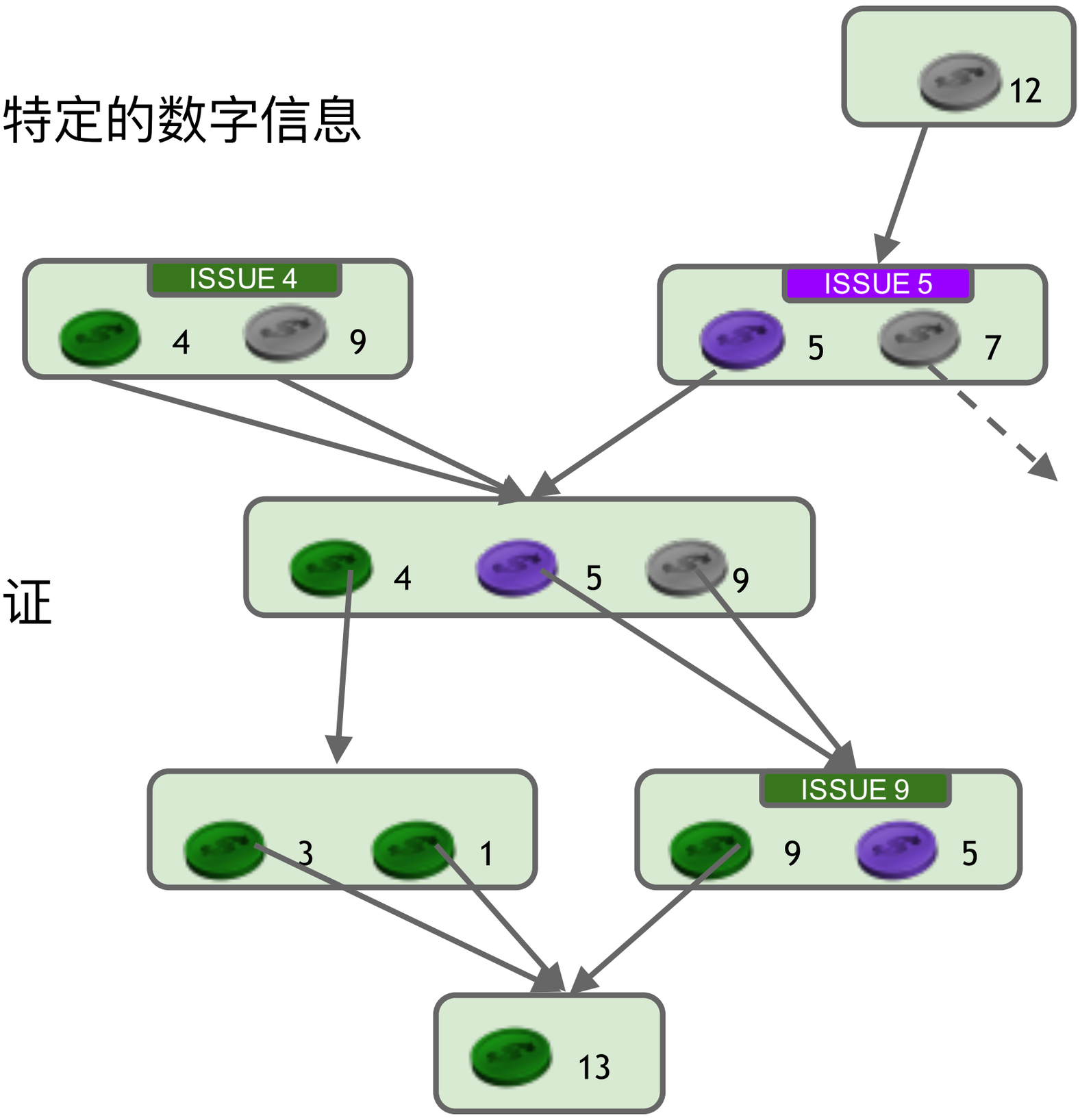
认证应用

"Bill #L11180916G hereby grants the holder admission to the Yankees game on Aug 18, 2014"

$SIGN_K(M, \#)$ →

染色币

染色：特定的数字信息



自己验证

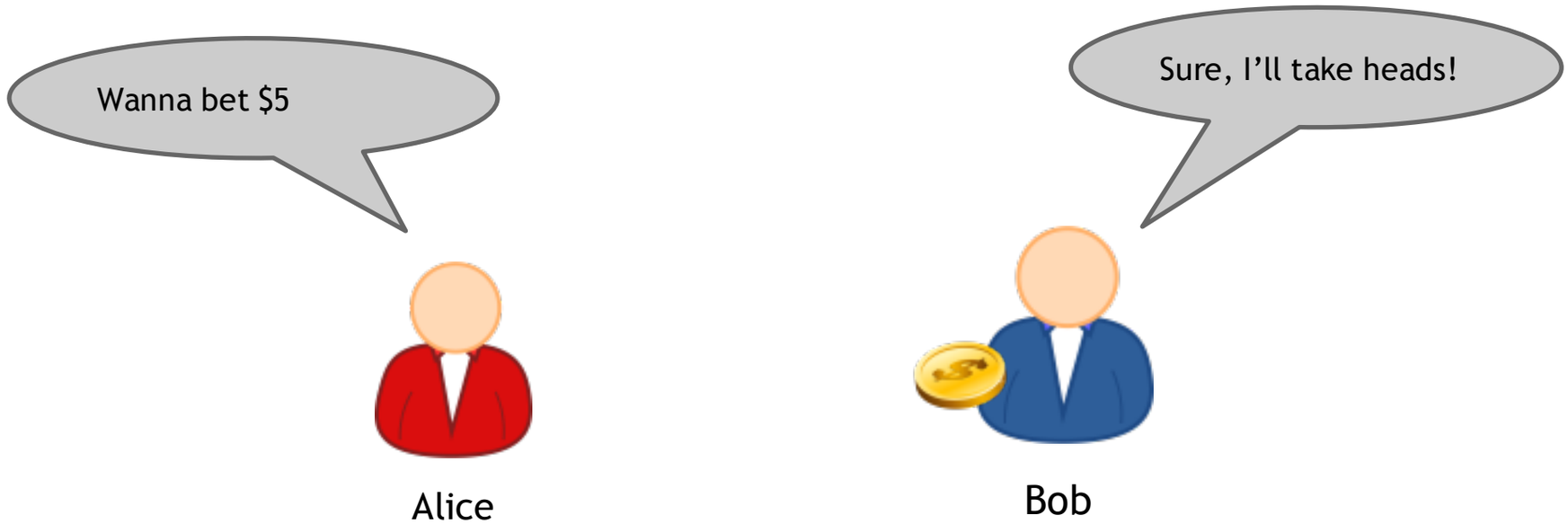
数字资产

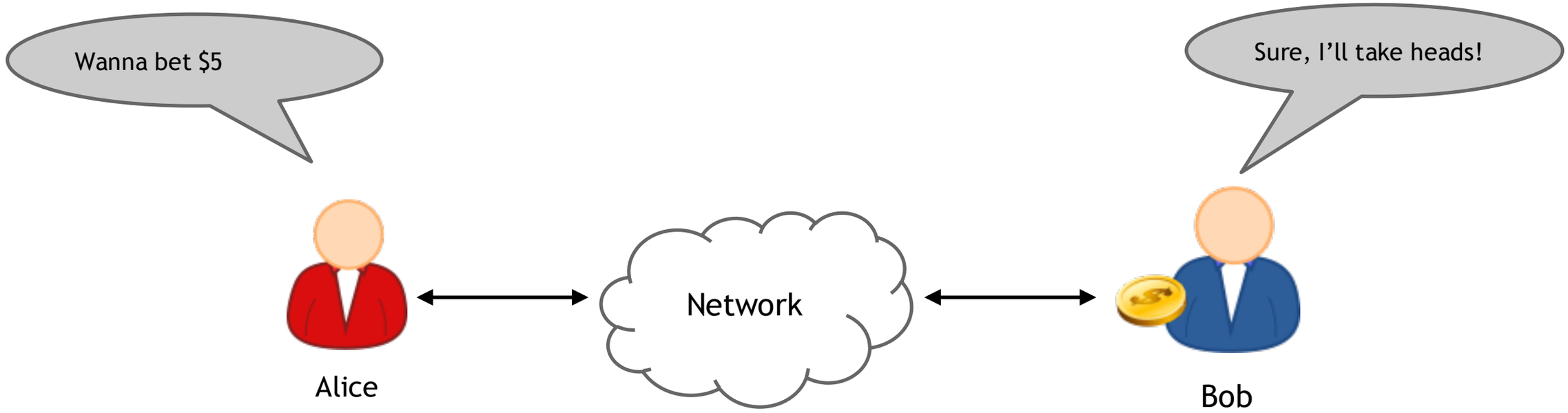
物理资产

股票

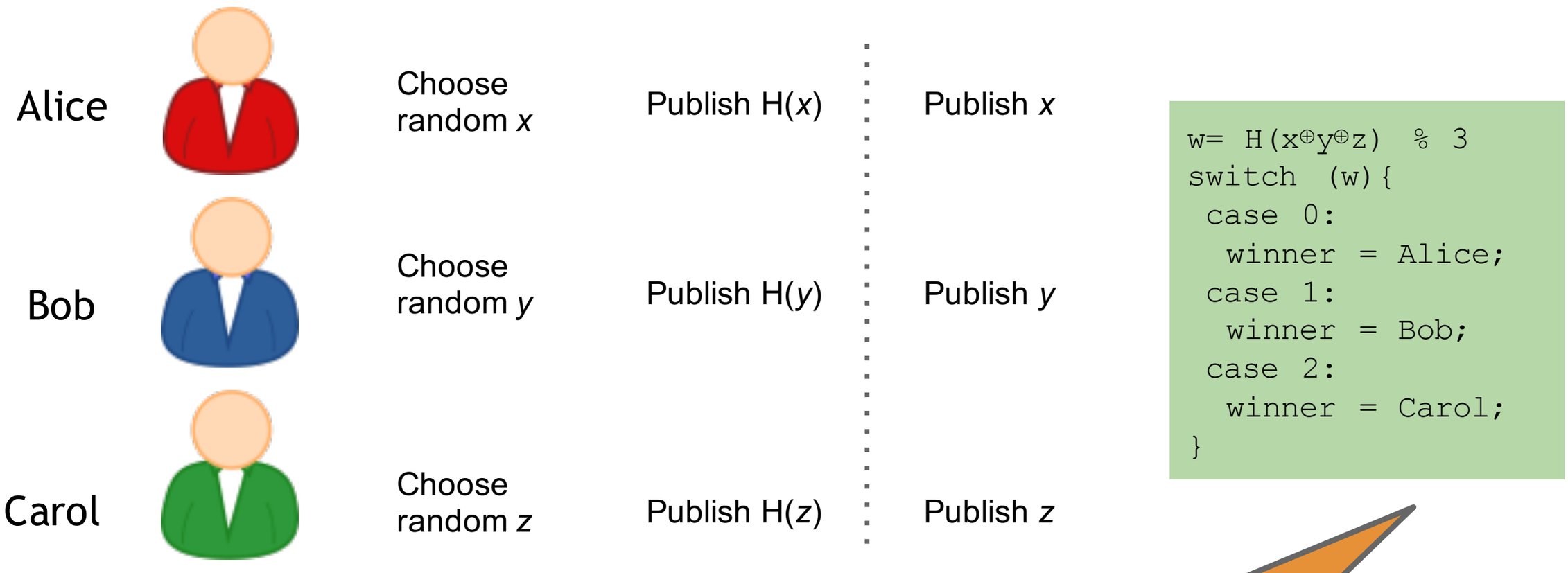
域名币

博彩

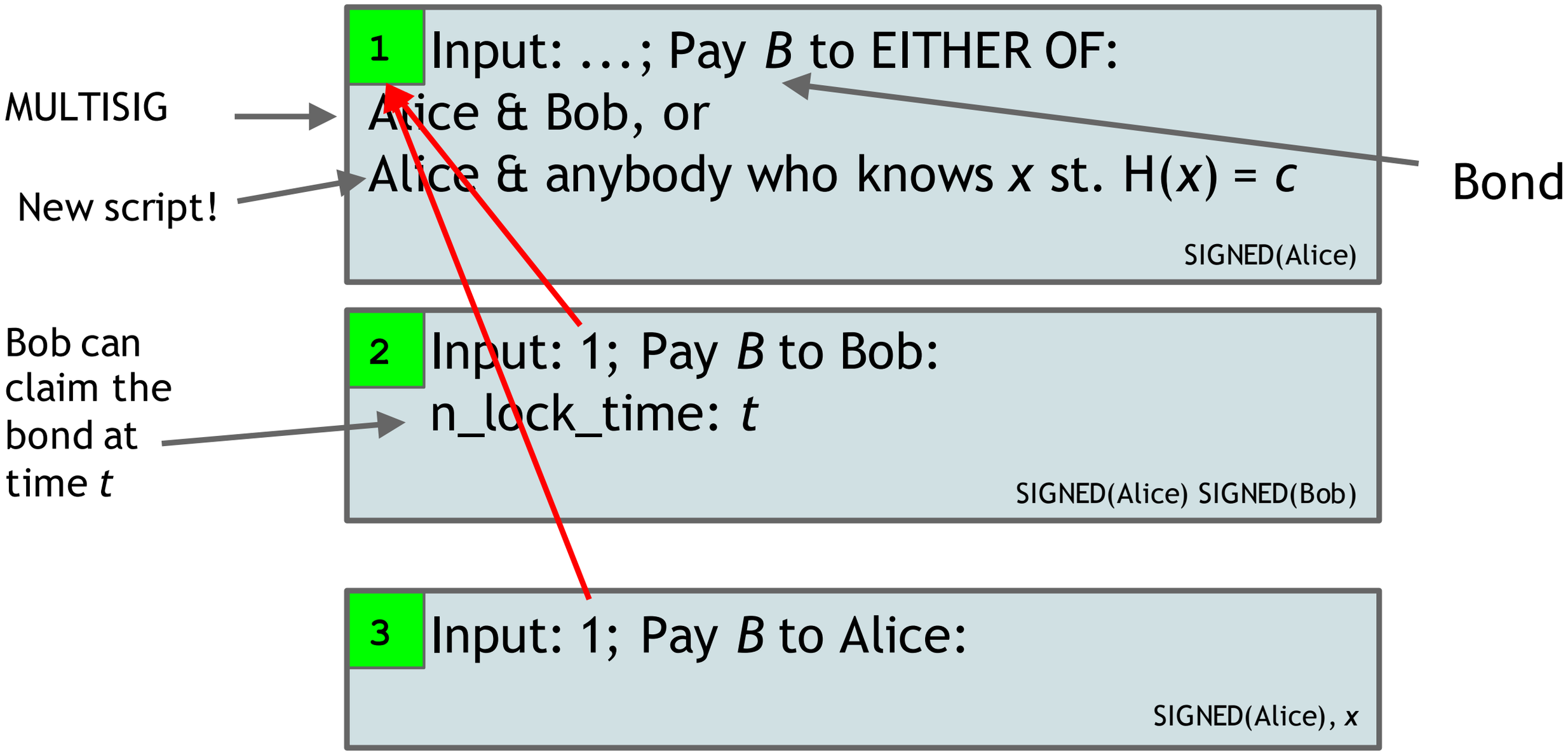

Wanna bet $5
Sure, I'll take heads!
Alice
Bob


Wanna bet $5
Sure, I'll take heads!
Network
Alice
Bob

在线博彩

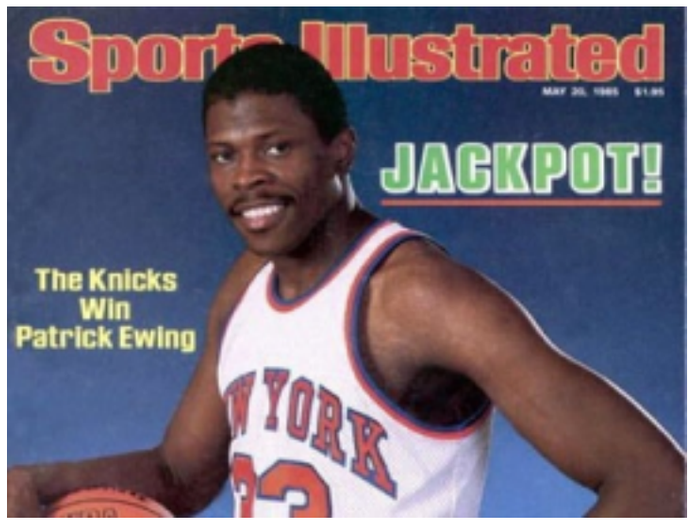

Round 1
Round 2
time
Alice
Choose random x
Publish H(x)
Publish x
Bob
Choose random y
Publish H(y)
Publish y
Carol
Choose random z
Publish H(z)
Publish z
w= H(x⊕y⊕z) % 3
switch (w){
case 0:
winner = Alice;
case 1:
winner = Bob;
case 2:
winner = Carol;
}
Hash function guarantees nobody can win with probability more than 1/3

时间约束的在线博彩

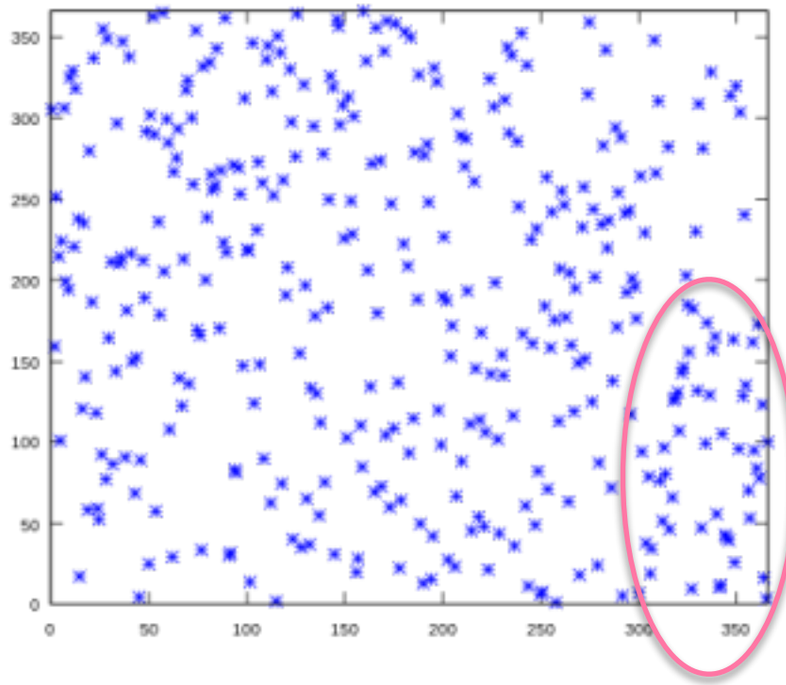

1
Input: ...; Pay B to EITHER OF:
Alice & Bob, or
Alice & anybody who knows x st. H(x) = c
SIGNED(Alice)
MULTISIG
New script!
Bond
2
Input: 1; Pay B to Bob:
n_lock_time: t
SIGNED(Alice) SIGNED(Bob)
Bob can claim the bond at time t
3
Input: 1; Pay B to Alice:
SIGNED(Alice), x
x revealed if Alice reclaims her bond

随机源

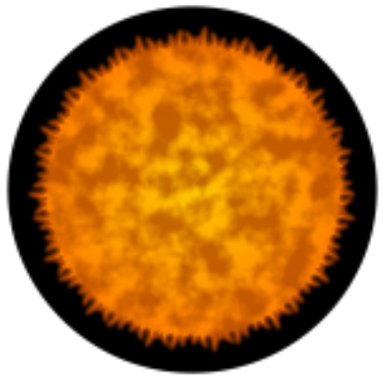

NBA
DRAFT
LOTTERY

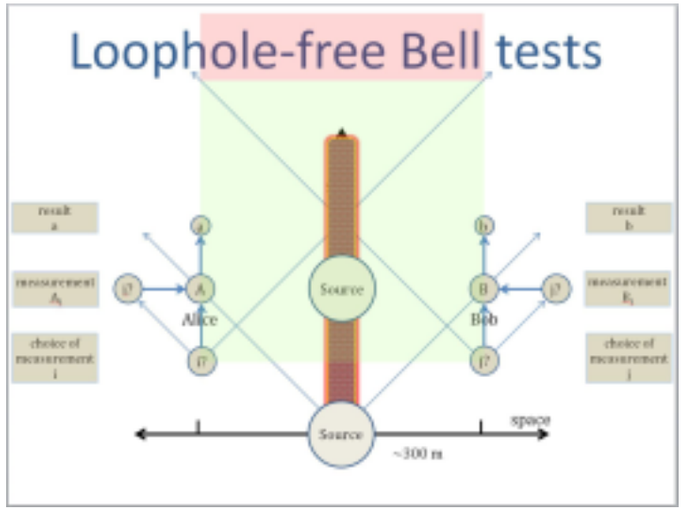

Sports Illustrated
JACKPOT!
The Knicks
Win
Patrick Ewing

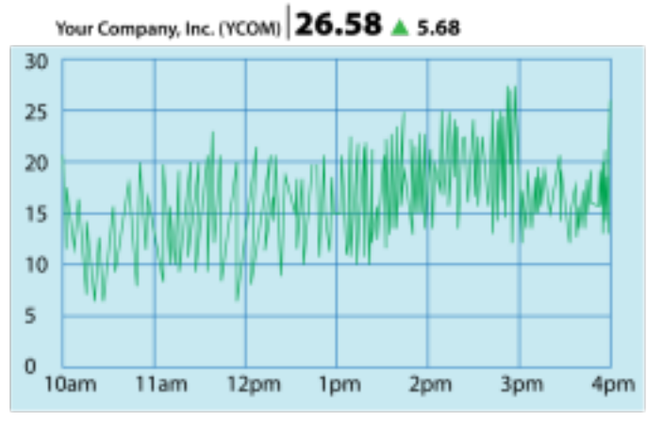

Bent Corner


350
300
250
200
150
100
50
0
0
50
100
150
200
250
300
350

随机源

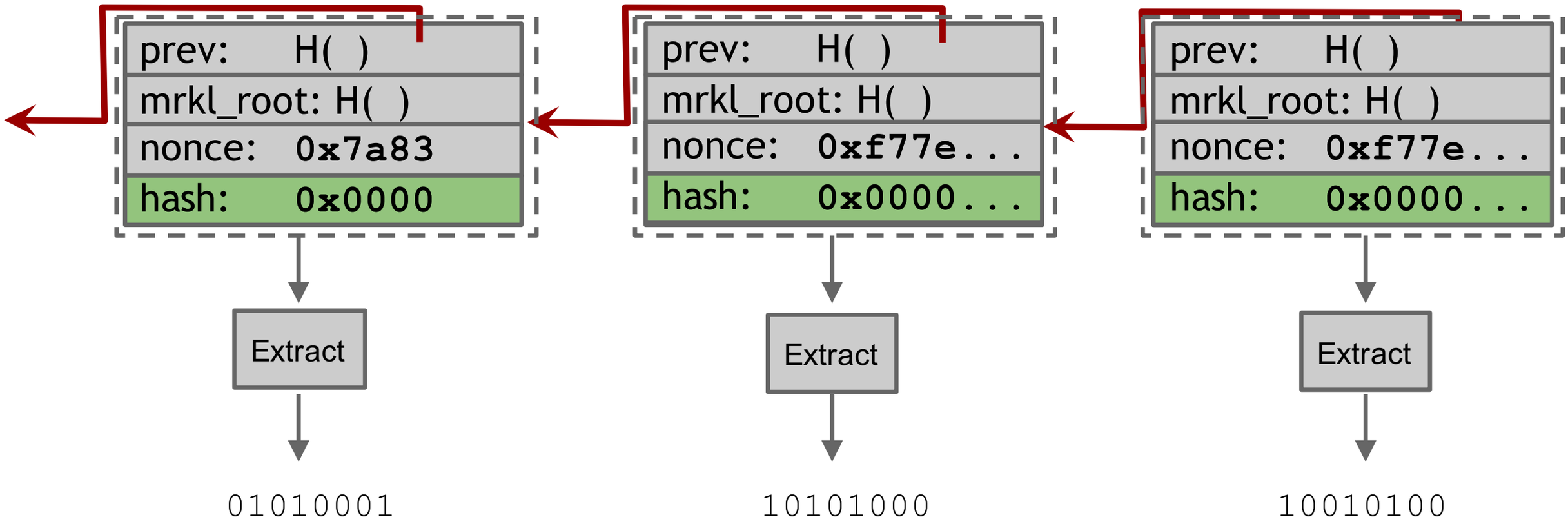



Loophole-free Bell tests
Source
Alice
Bob
Source
space
~300 m


Your Company, Inc. (YCOM) 26.58 ▲ 5.68
30
25
20
15
10
5
0
10am
11am
12pm
1pm
2pm
3pm
4pm


BINGO

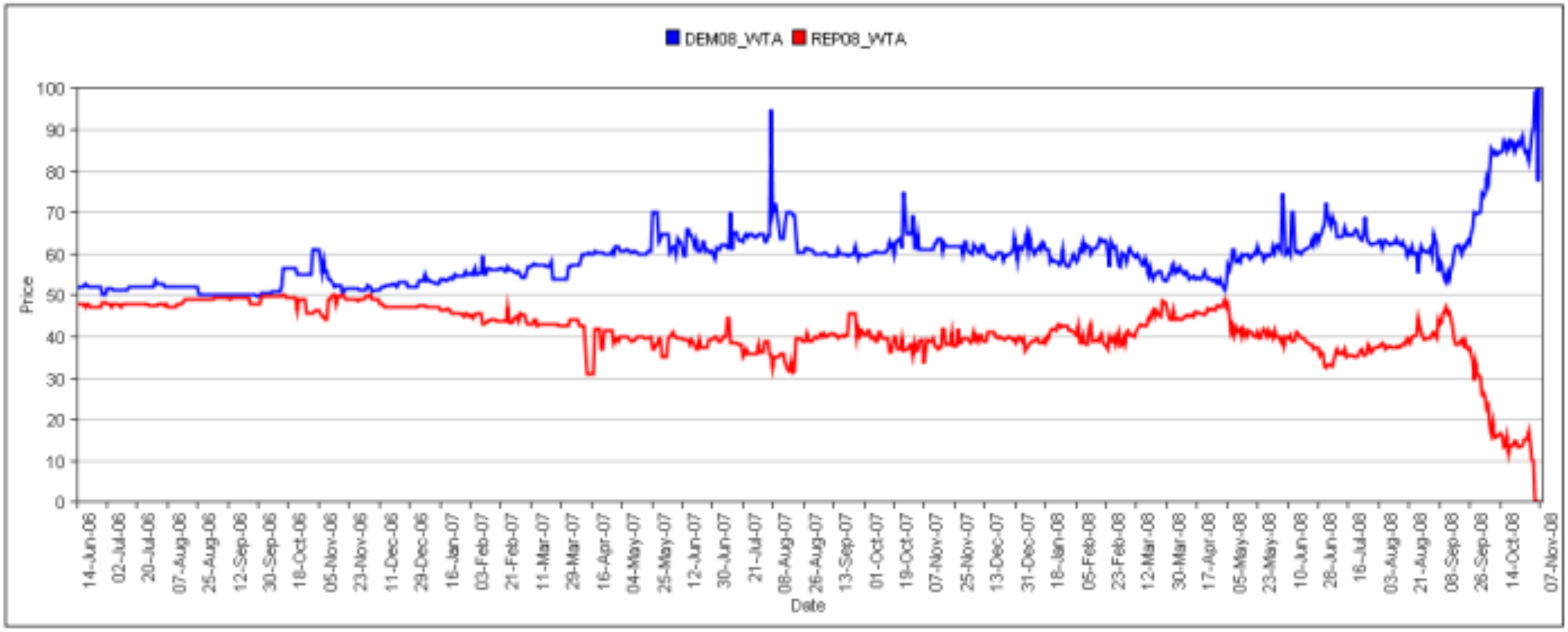
比特币作为随机源


prev: H( )
mrkl_root: H( )
nonce: 0x7a83
hash: 0x0000
Extract
01010001
prev: H( )
mrkl_root: H( )
nonce: 0xf77e...
hash: 0x0000...
Extract
10101000
prev: H( )
mrkl_root: H( )
nonce: 0xf77e...
hash: 0x0000...
Extract
10010100

预测市场

2014世界杯					
pre-tournament	0.12	0.09	0.22	0.01	0.05
after group stage	0.18	0.15	0.31	0.06	0.00
before semis	0.26	0.21	0.45	0.00	0.00
before finals	0.64	0.36	0.00	0.00	0.00
final	1	0	0	0	0

2008总统选举



Iowa Electronic Markets

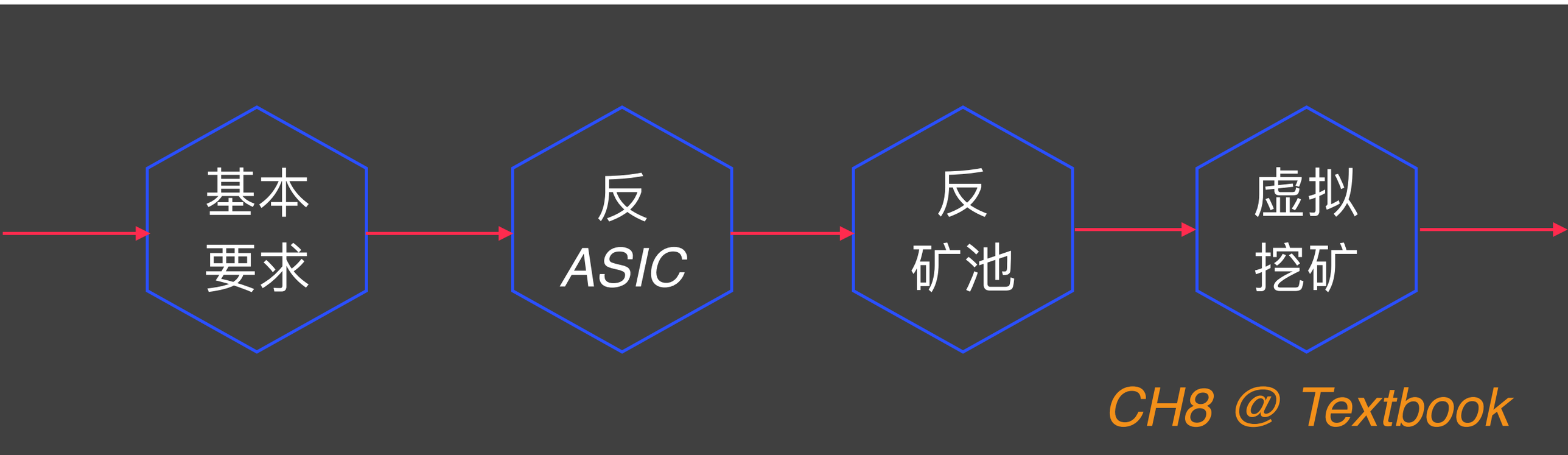
Reality Keys

优缺点

Orange?

Yellow?

其他挖矿

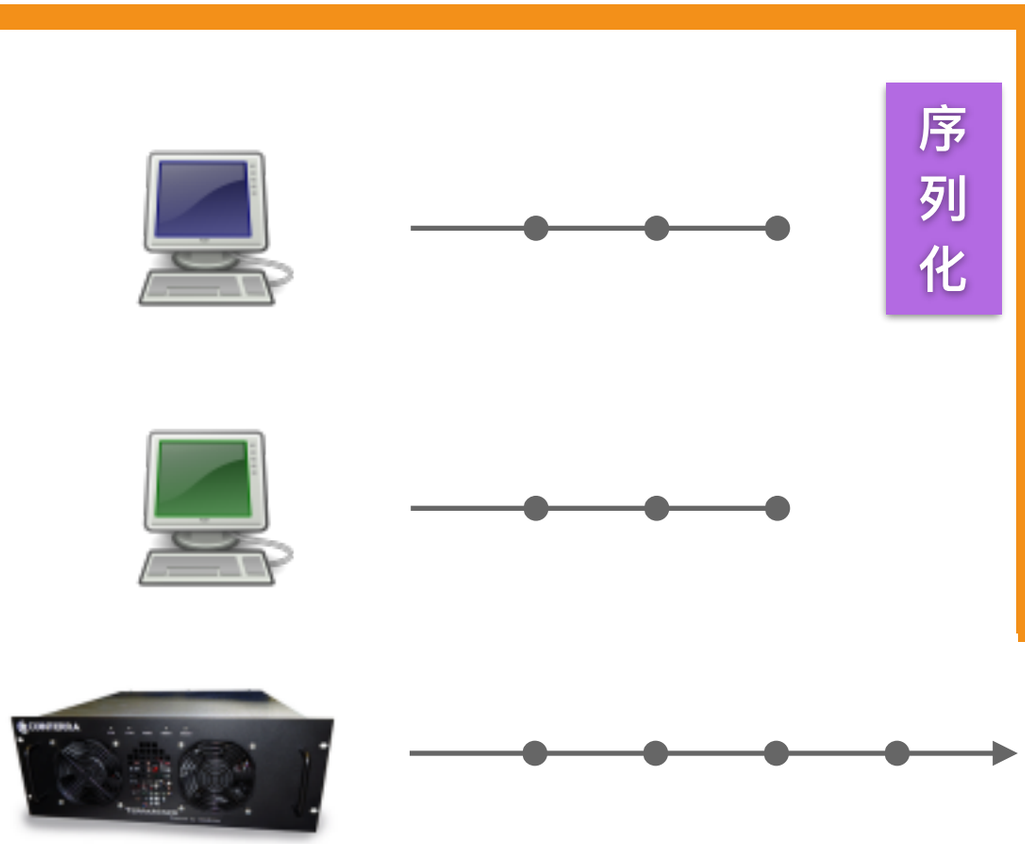


挖矿算法基本要求

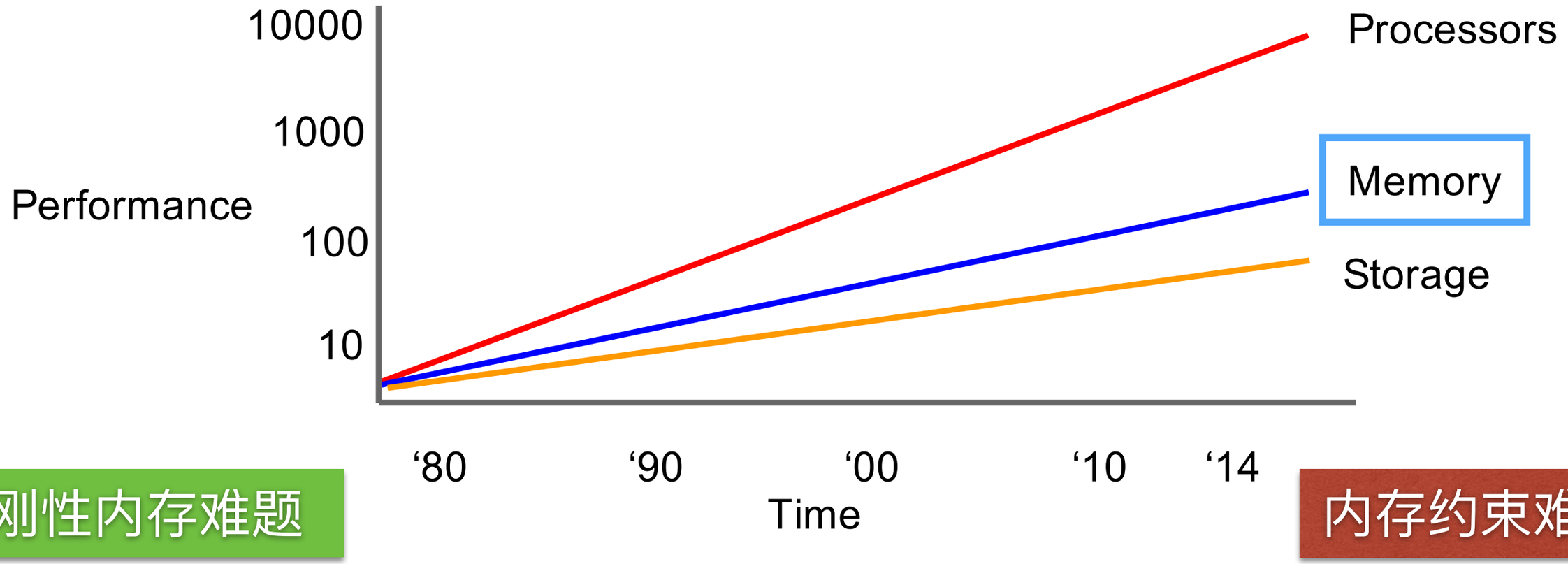
挖矿算法是比特币系统的核心

需要一个难题计算复杂

- 挖矿难题的结果要求验证简单
- 挖矿难题的难度可调节的特性
- 成功概率和所贡献的算力成比例



反ASIC



刚性内存难题

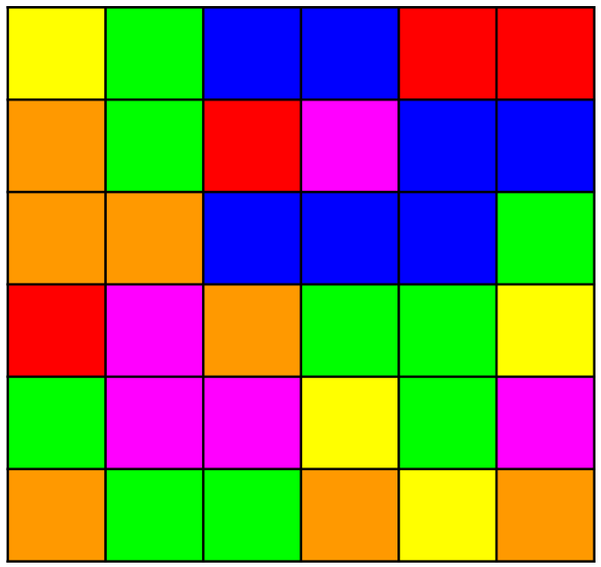
内存约束难题

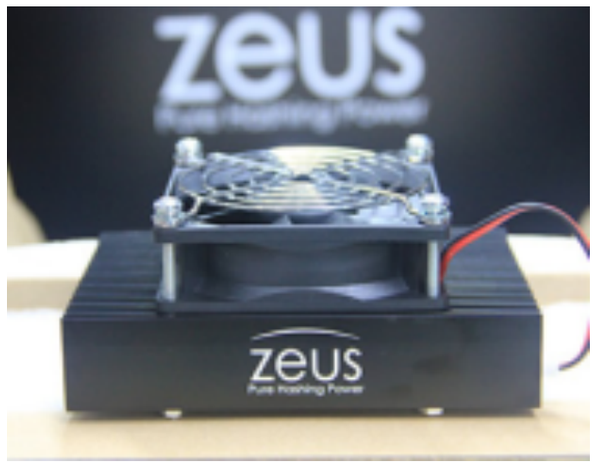
Scrypt

比特币前就存在加密个人口令

2009

反ASIC





检验成本过高

内存使用参数设置过低

DASH

组合多种Hash算法

XI I

参数

反ASIC是否可能

SHA256

反ASIC是否有问题

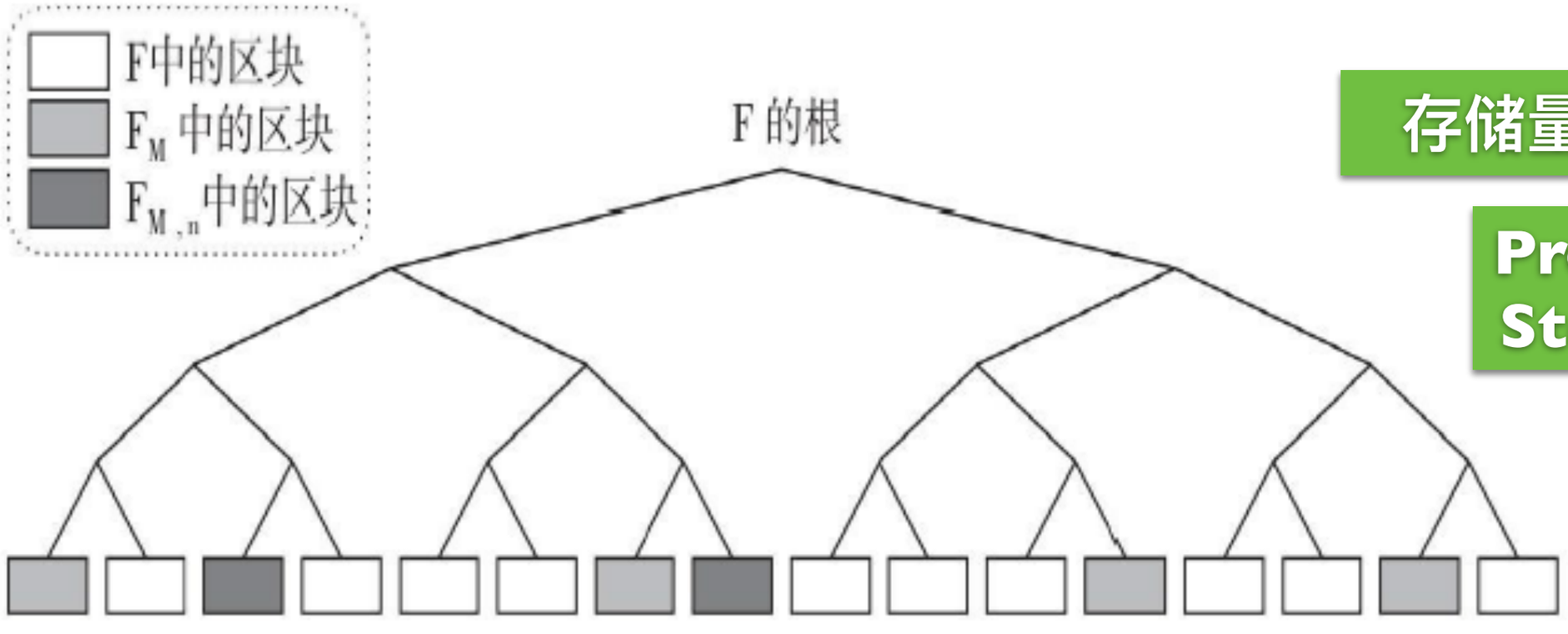
Blockchain Technology

有效工作量证明

挖矿能量消耗问题

志愿者计算项目

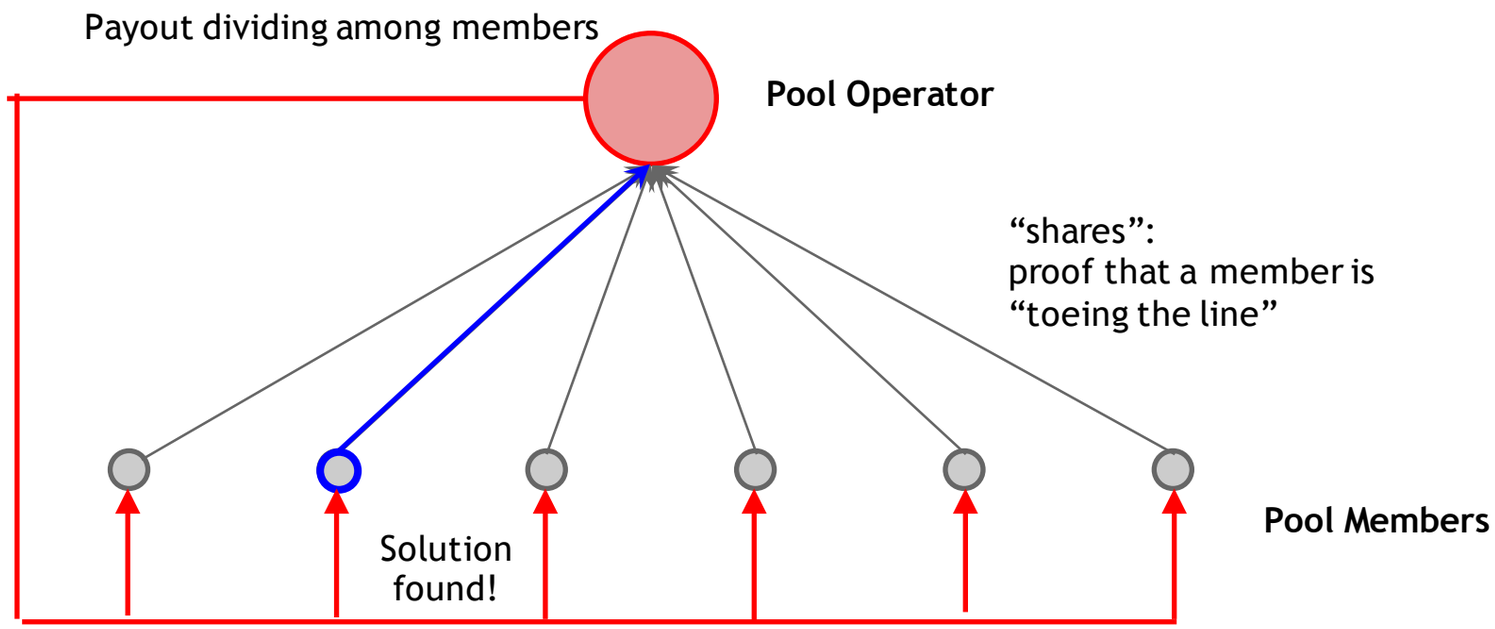
分布式存储



存储量证明

Proof of Storage

不可外包的难题



防止矿池的产生

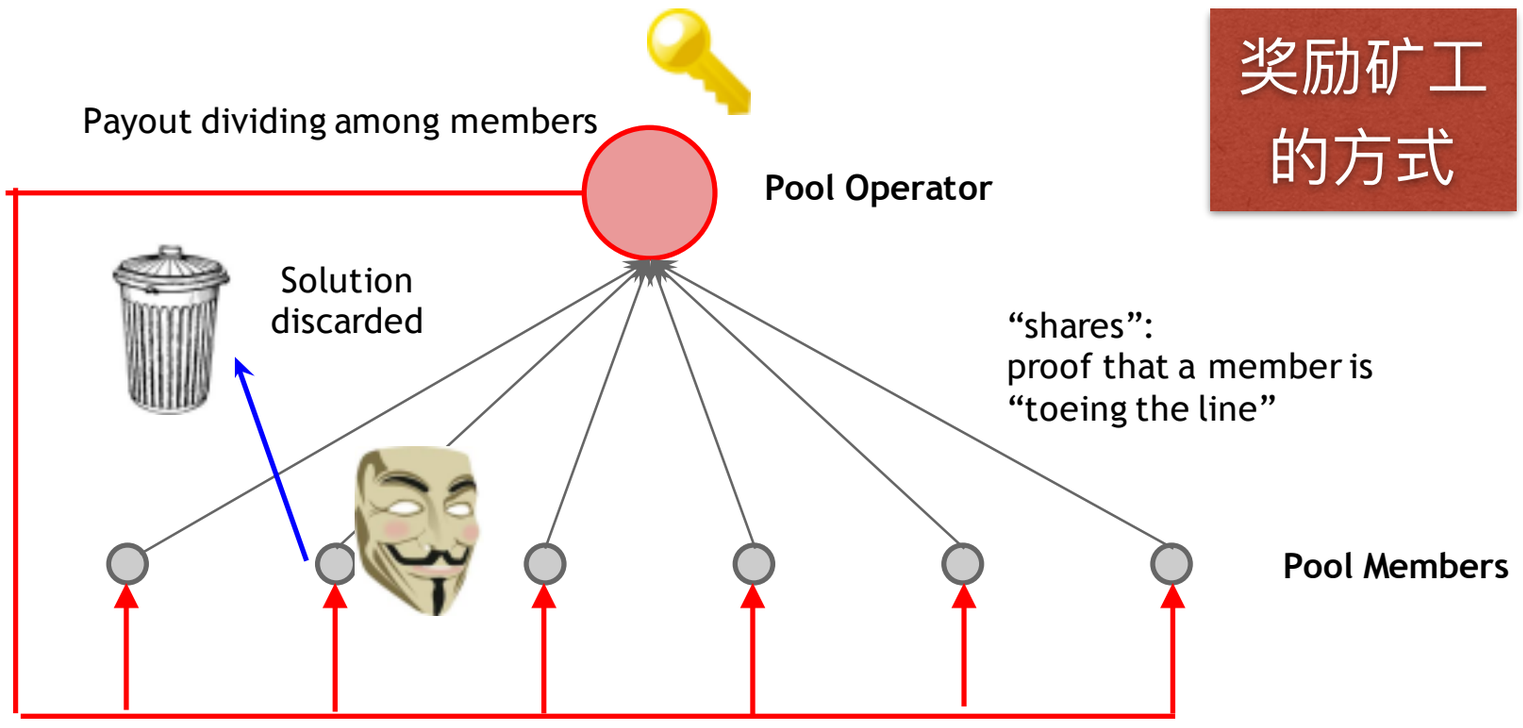
中心化、安全

区块丢弃攻击

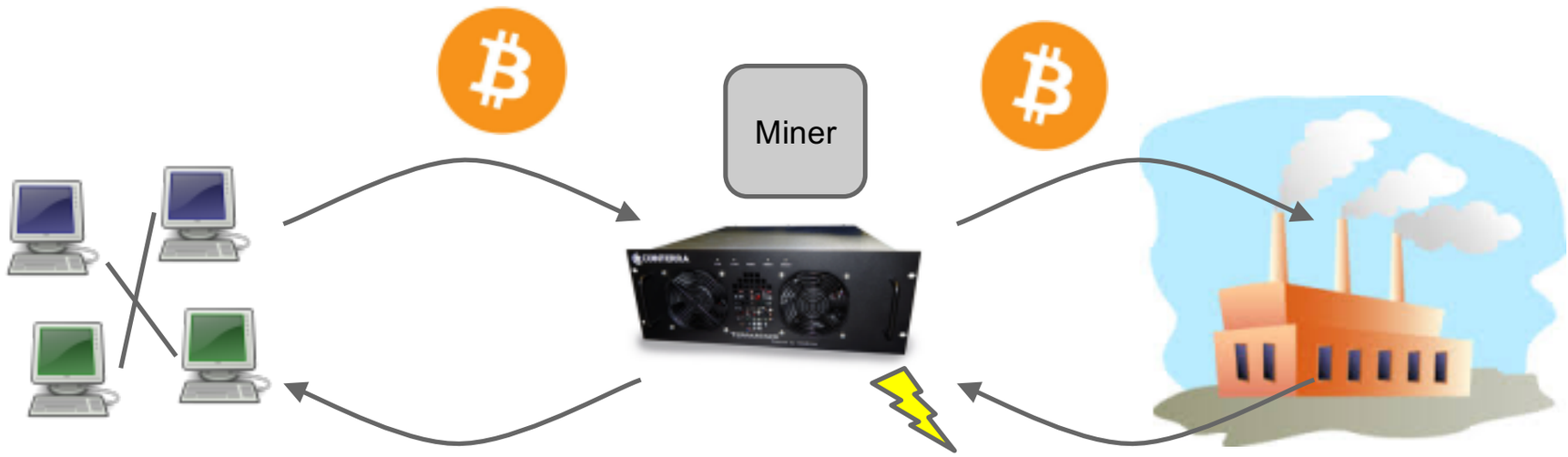
奖励破坏

区块数字签名的哈希值
低于一个特定的目标

奖励矿工
的方式



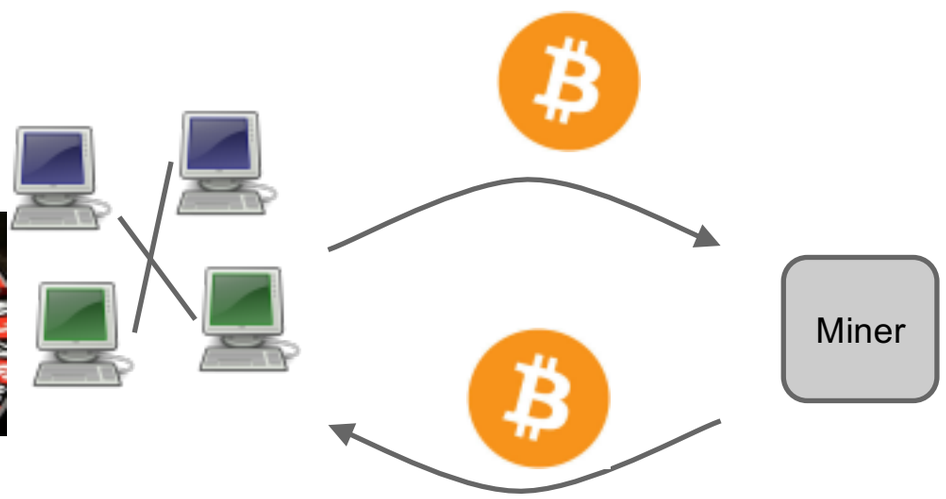
虚拟挖矿



权益证明

分叉攻击

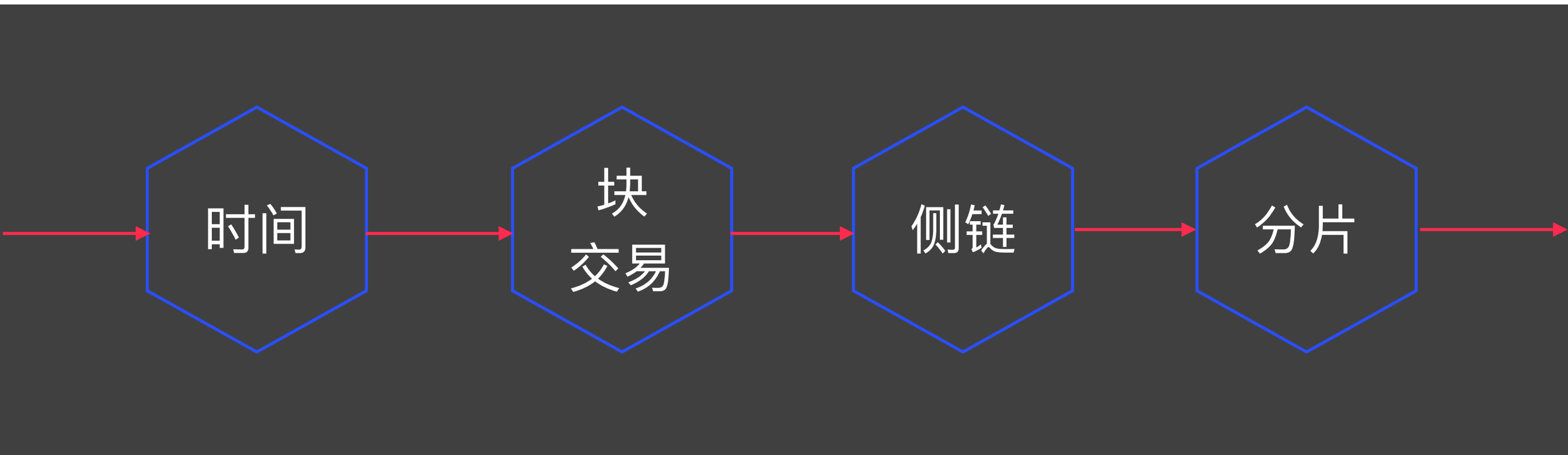
检查点



2012 点点币

币拥有量交易

可扩展性



性能扩展

分布式

共同维护

匿名化

开放参与

高币值

大规模

吞吐量

时延

可扩展性

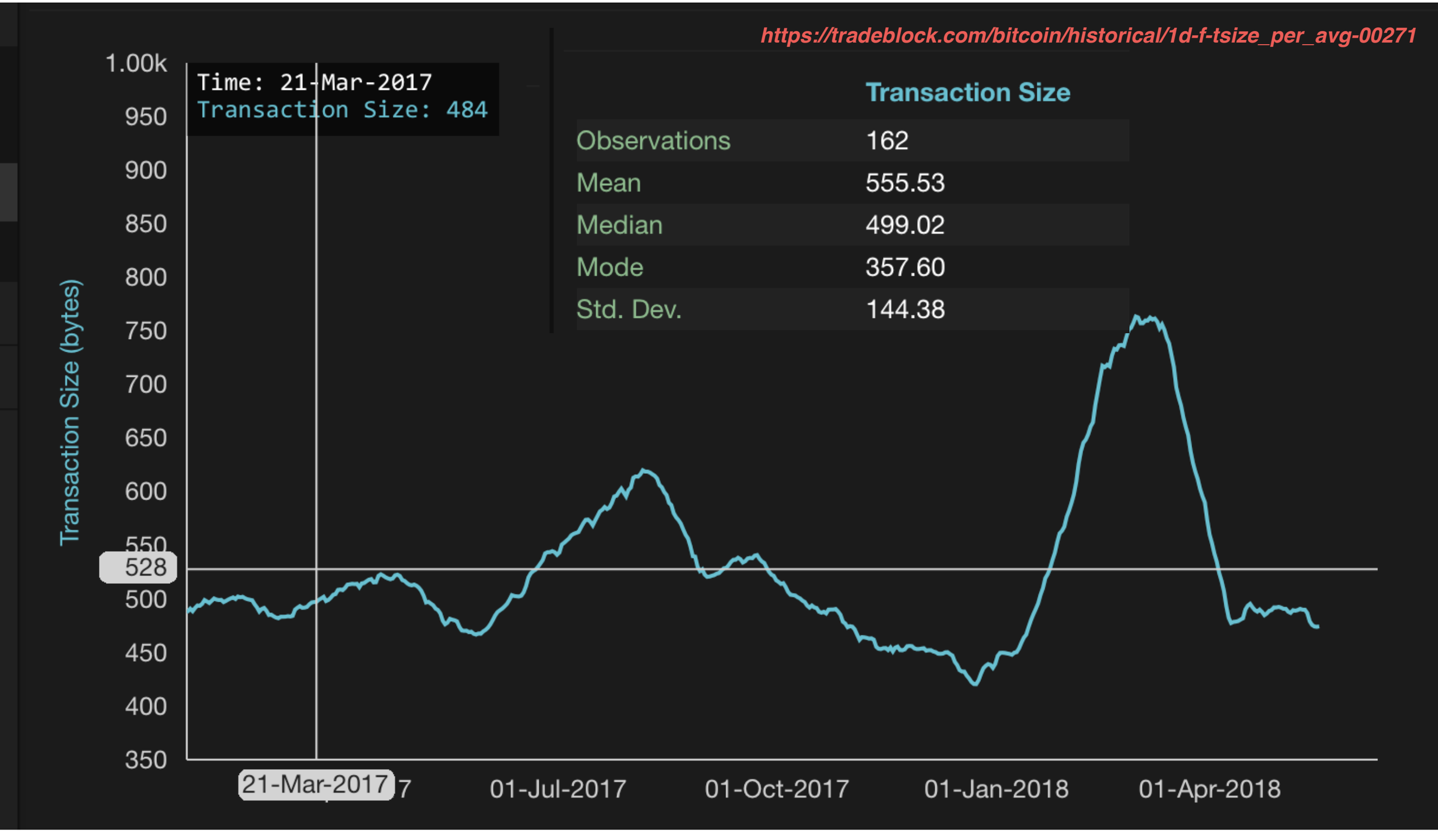
链下扩容

微块

分片

比特币的TPS

https://tradeblock.com/bitcoin/historical/1d-f-tsize_per_avg-00271

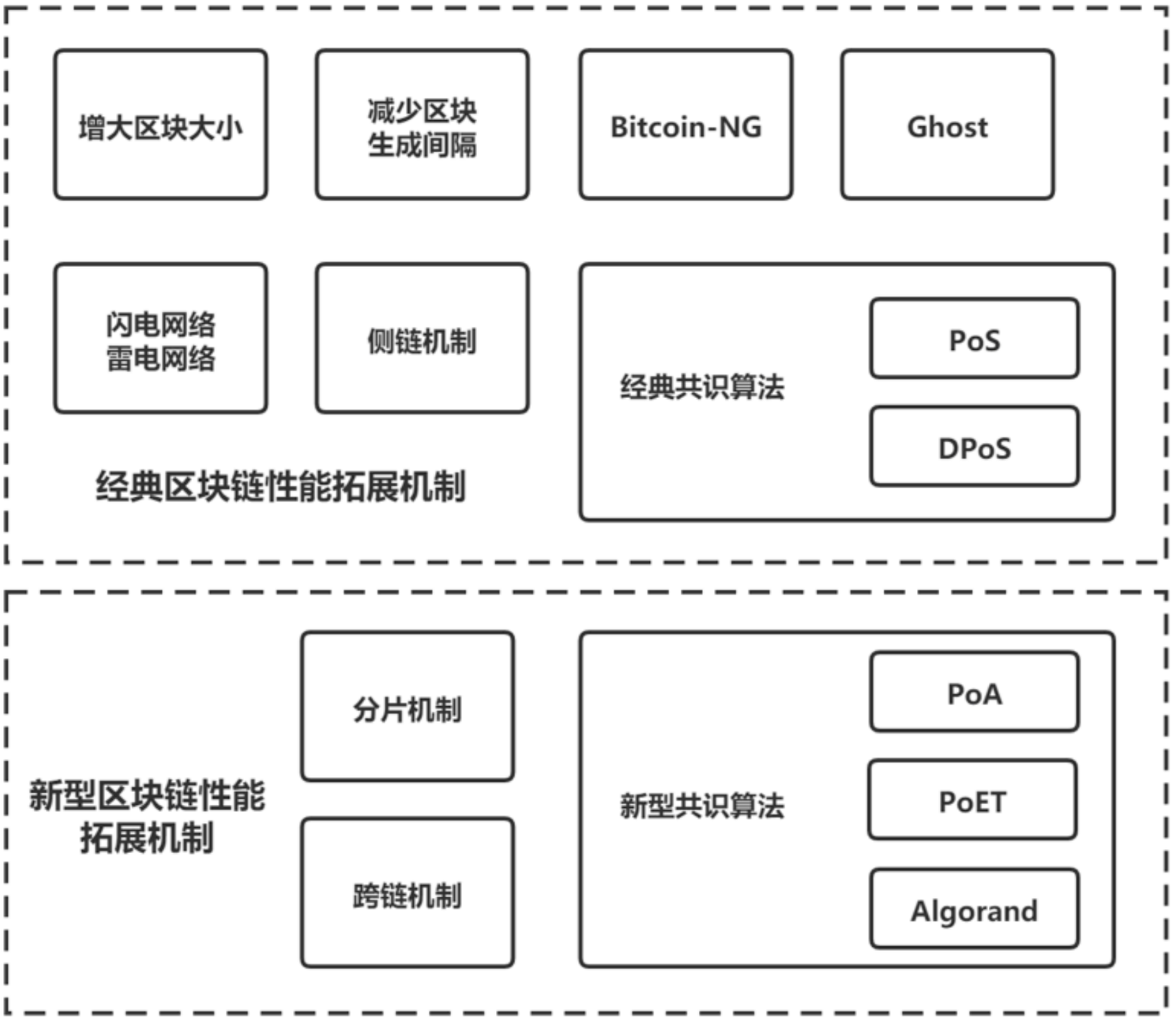


Blockchain Technology

没有比较没有伤害

	3	3.2
PayPal™	150	450
VISA	2000	56000

可扩展性分类


增大区块大小
减少区块生成间隔
Bitcoin-NG
Ghost
闪电网络
雷电网络
侧链机制
经典共识算法
PoS
DPoS
经典区块链性能拓展机制
新型区块链性能拓展机制
分片机制
跨链机制
新型共识算法
PoA
PoET
Algorand

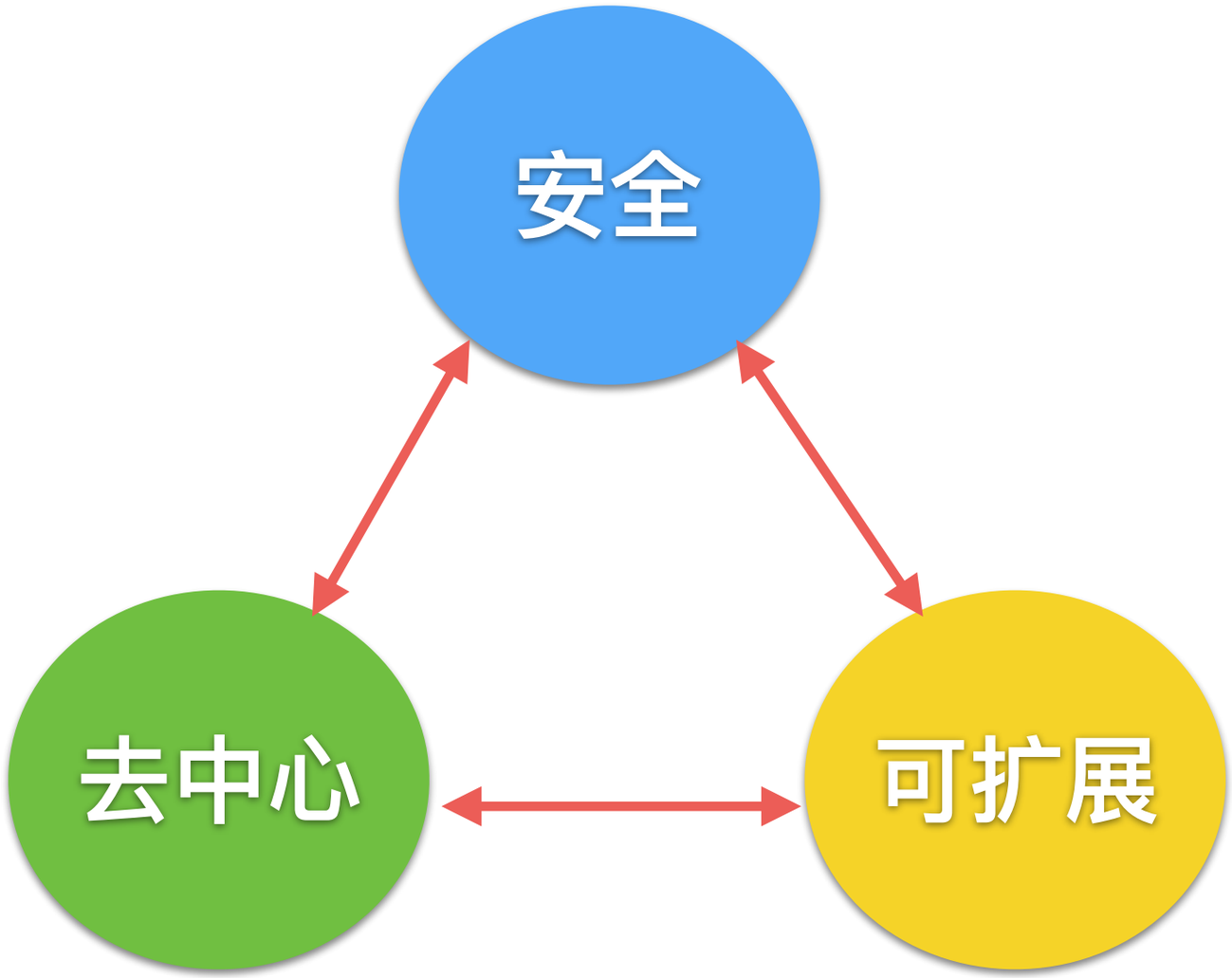
另一种分类

Layer	Categories	Solutions
Layer2: *Non On-Chain*	Payment channel	Lightning Network [20], DMC [26] Raiden Network [27], Sprites [28]
	Side chain	Pegged Sidechain [29], Plasma [21] liquidity.network [30]
	Cross-chain	Cosmos [22], Polkadot [31]
	Off-chain computation	Truebit [32], Arbitrum [33]
Layer1: *On-Chain*	Block data	SegWit [34], Bitcoin-Cash [9] Compact block relay [10], Txilm [35] CUB [36], Jidar [37]
	Consensus	Bitcoin-NG [15], Algorand [16] Snow white [17],Ouroboros [18] [19]
	Sharding	Elastico [11], OmniLedger [12] RapidChain [13],Monoxide [14]
	DAG	Inclusive [38], SPECTRE [39] PHANTOM [40], Conflux [41] Dagcoin [42], IOTA [43] Byteball [44], Nano [45]
Layer0	Data propagation	Erlay [46], Kadcast [47] Velocity [48],bloXroute [49]

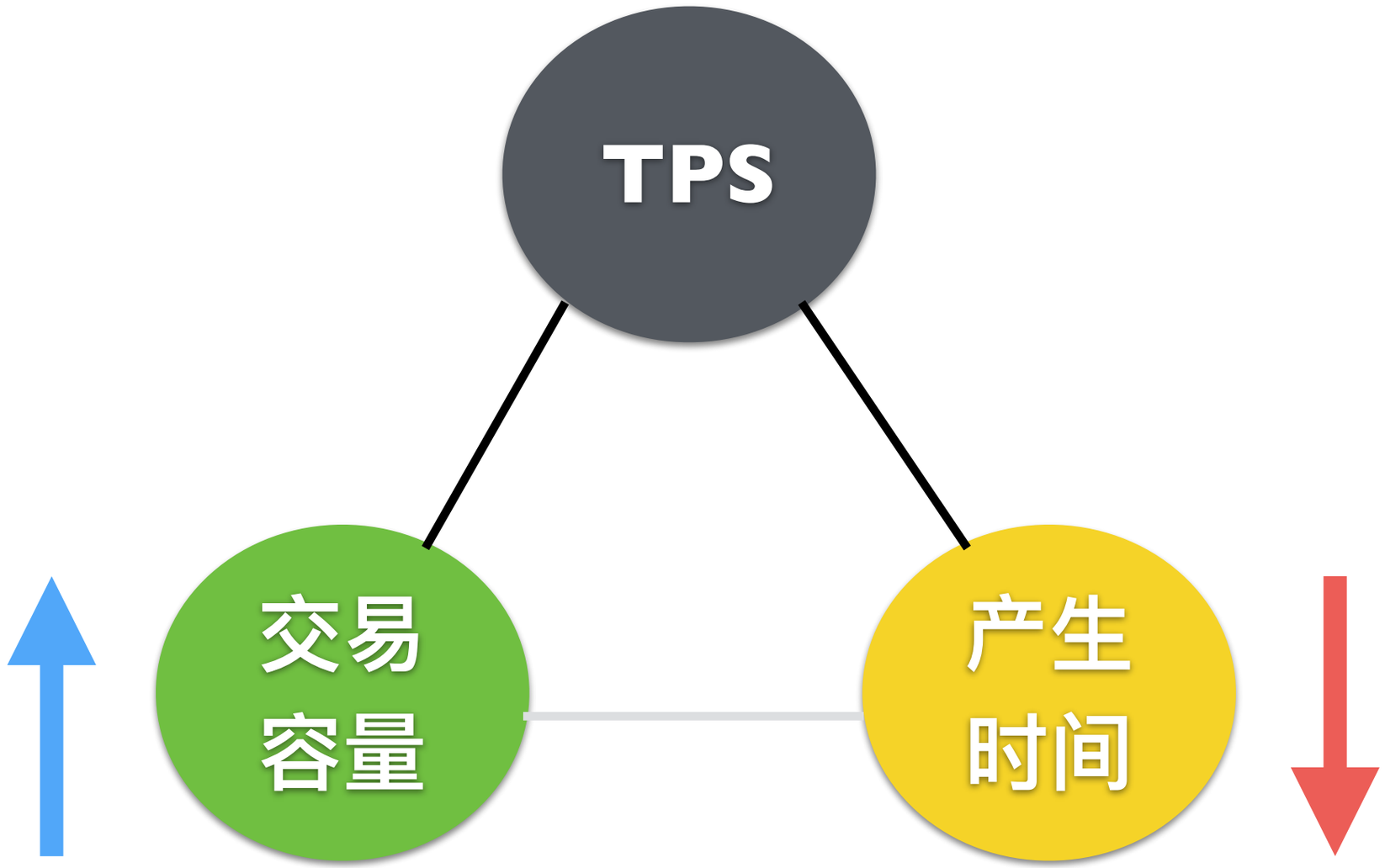
区块链可扩展性

交易容量

产生块时间



可扩展性



交易大小　　块的大小

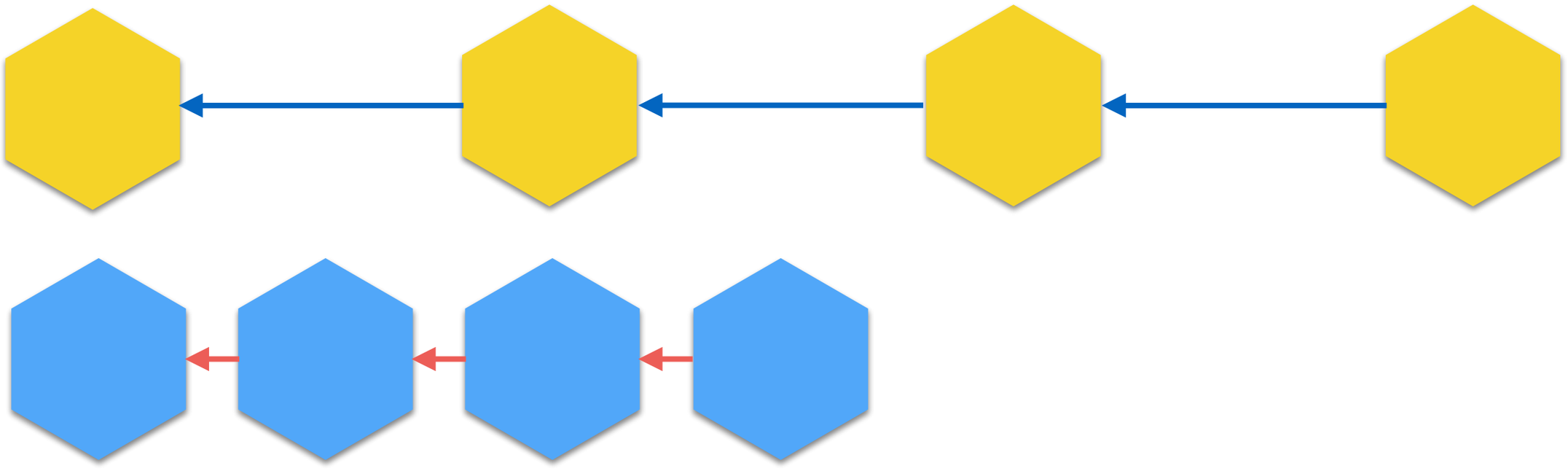
减少块产生时间

块传播时间

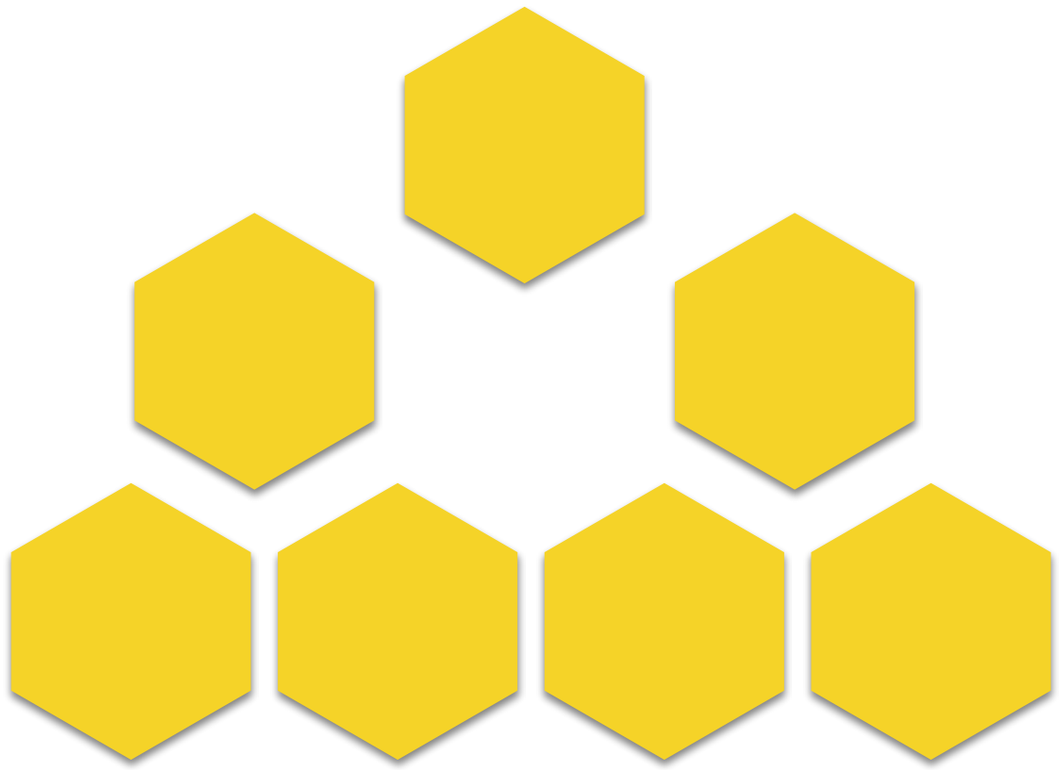
块产生时间

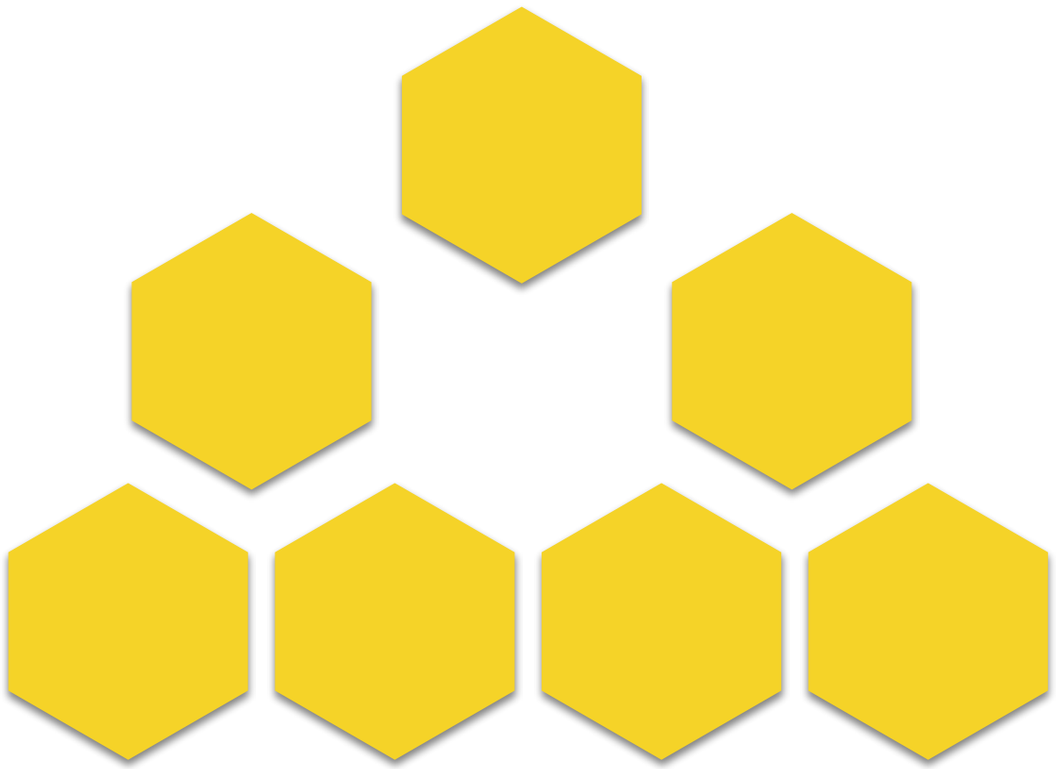
块传播时间

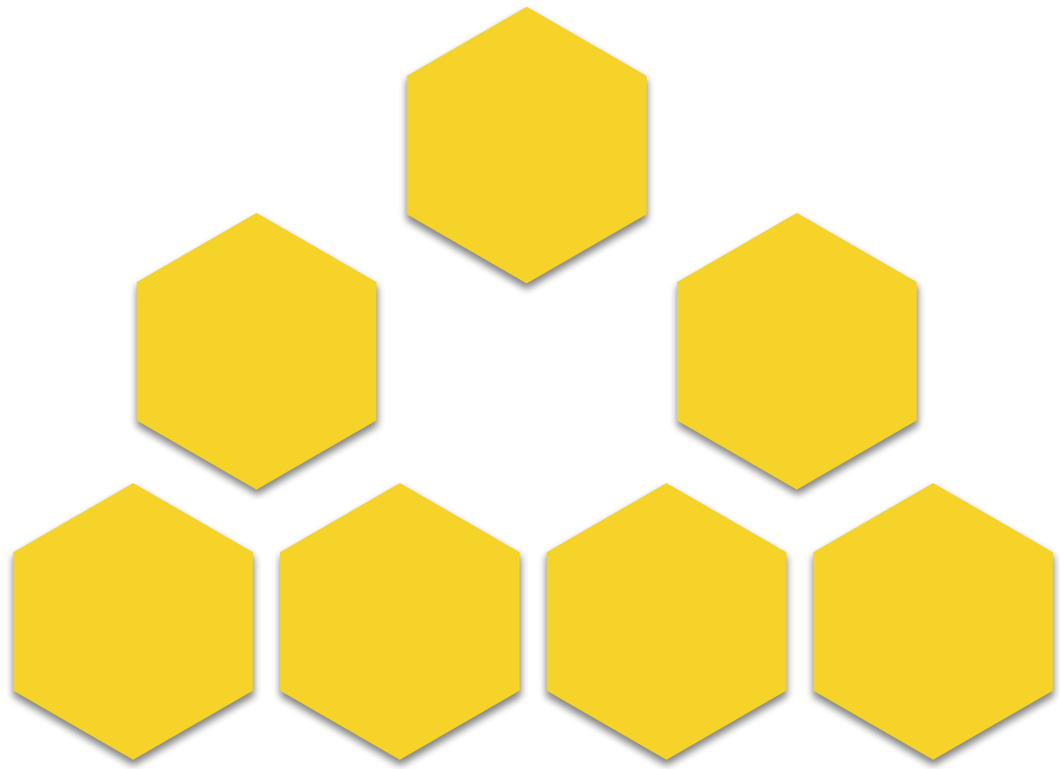
块产生时间



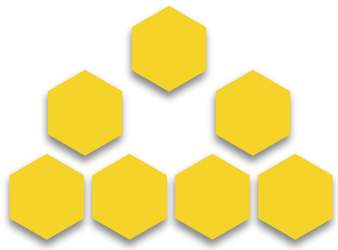
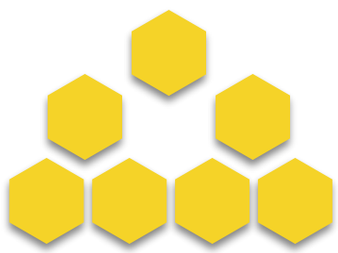
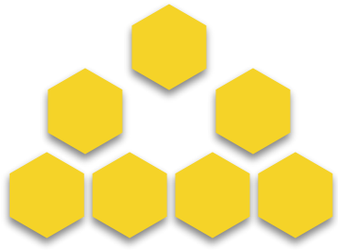
增大块大小







增大块大小

容易执行

更低的成本

矿工同意即可

硬分叉

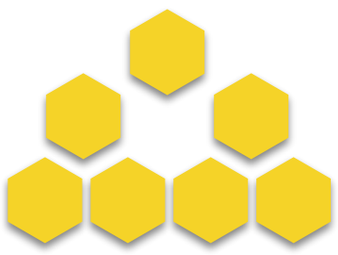
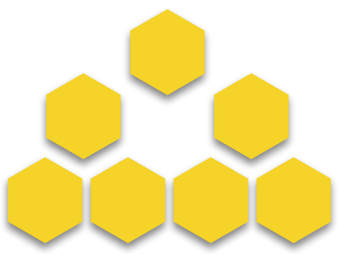
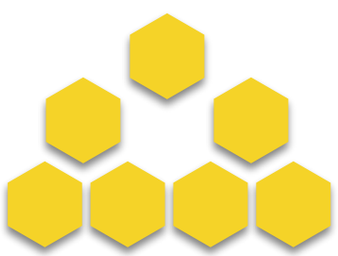
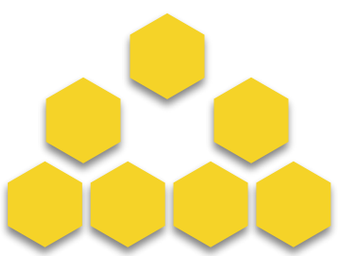
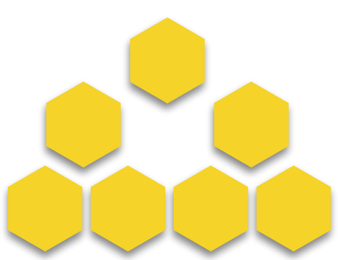
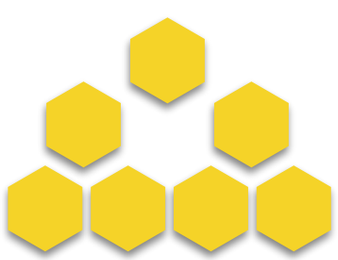
计算能力

更长的传播时间

大小增长快

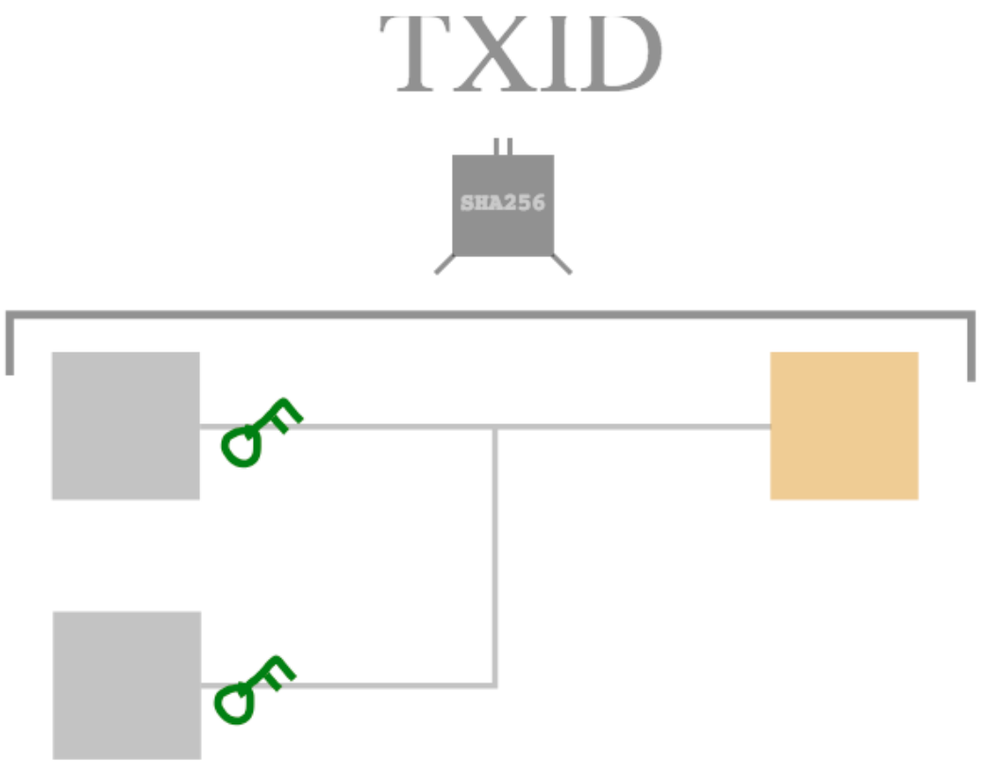
挖矿设备

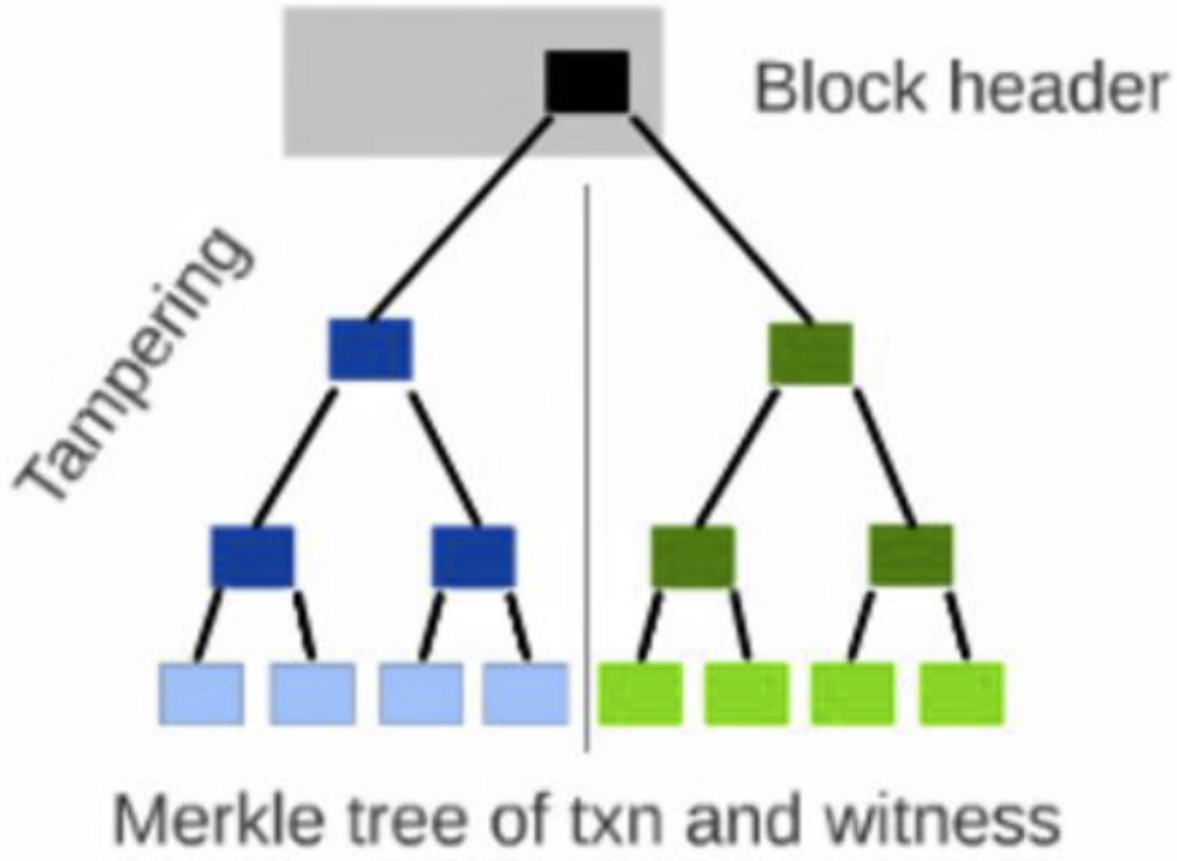
安全性

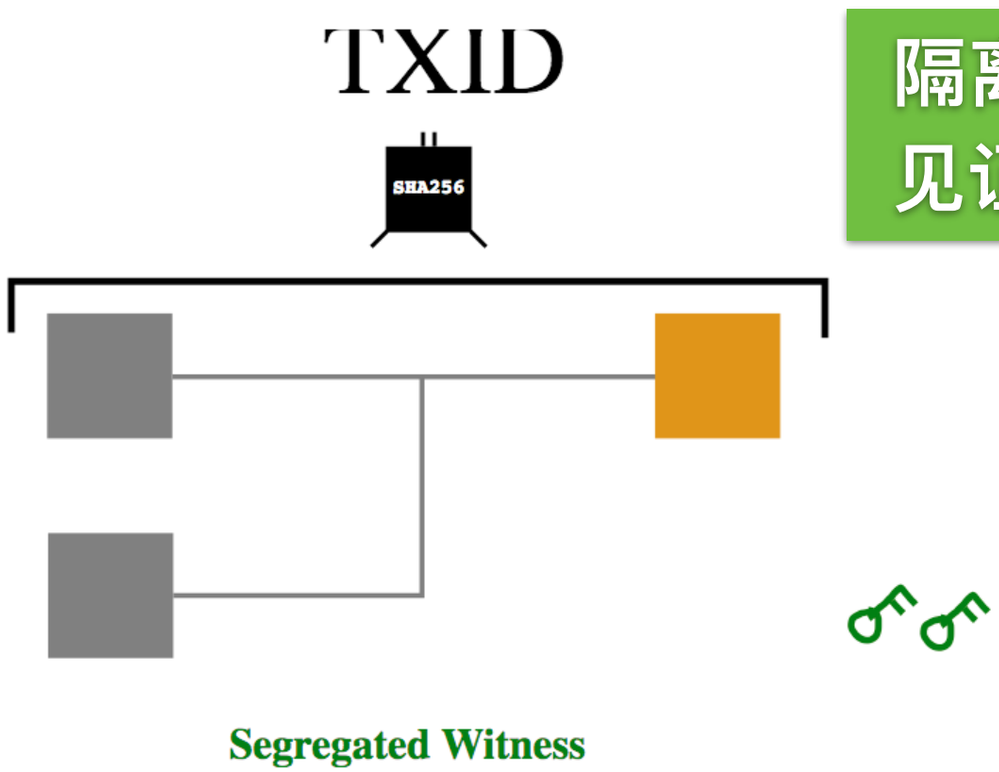
减少交易大小

http://learnmeabitcoin.com/faq/segregated-witness





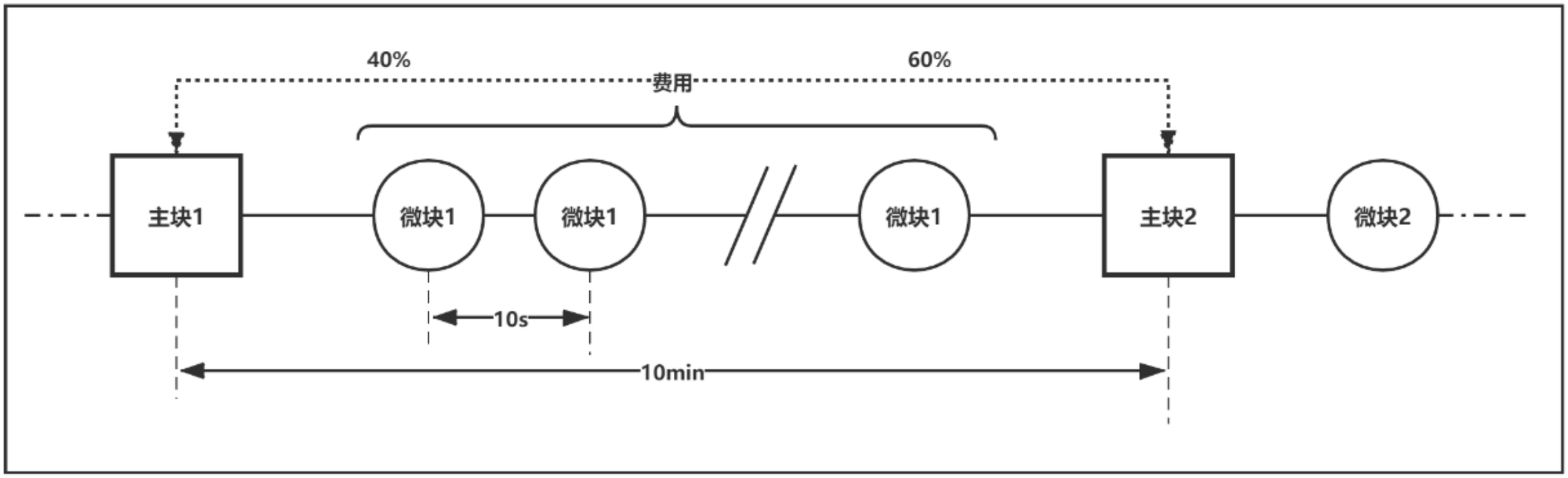
隔离见证



优点

缺点

减少挖矿频率

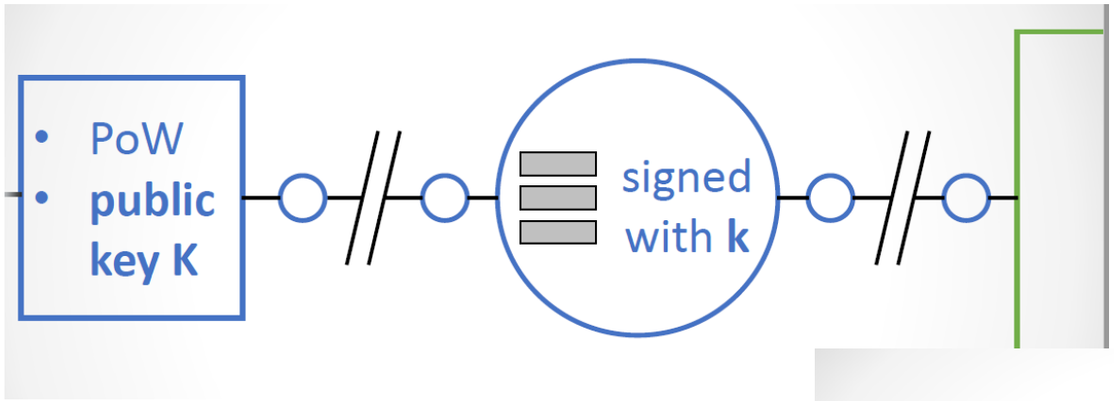


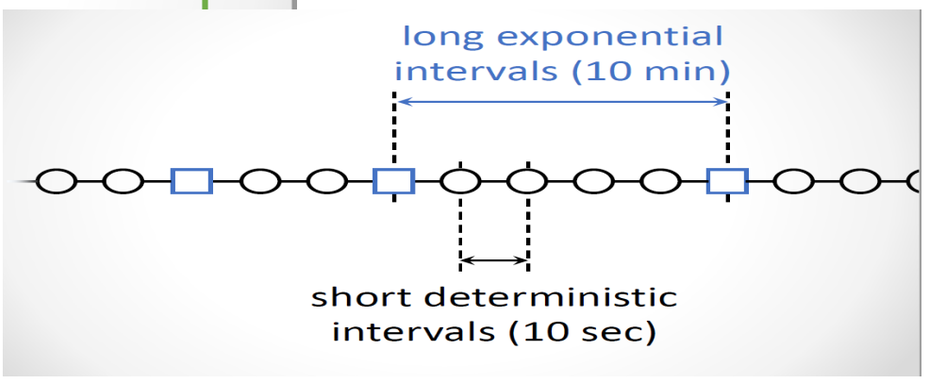
主块:

- 无交易
- Leader选举

微块:

- 只有交易





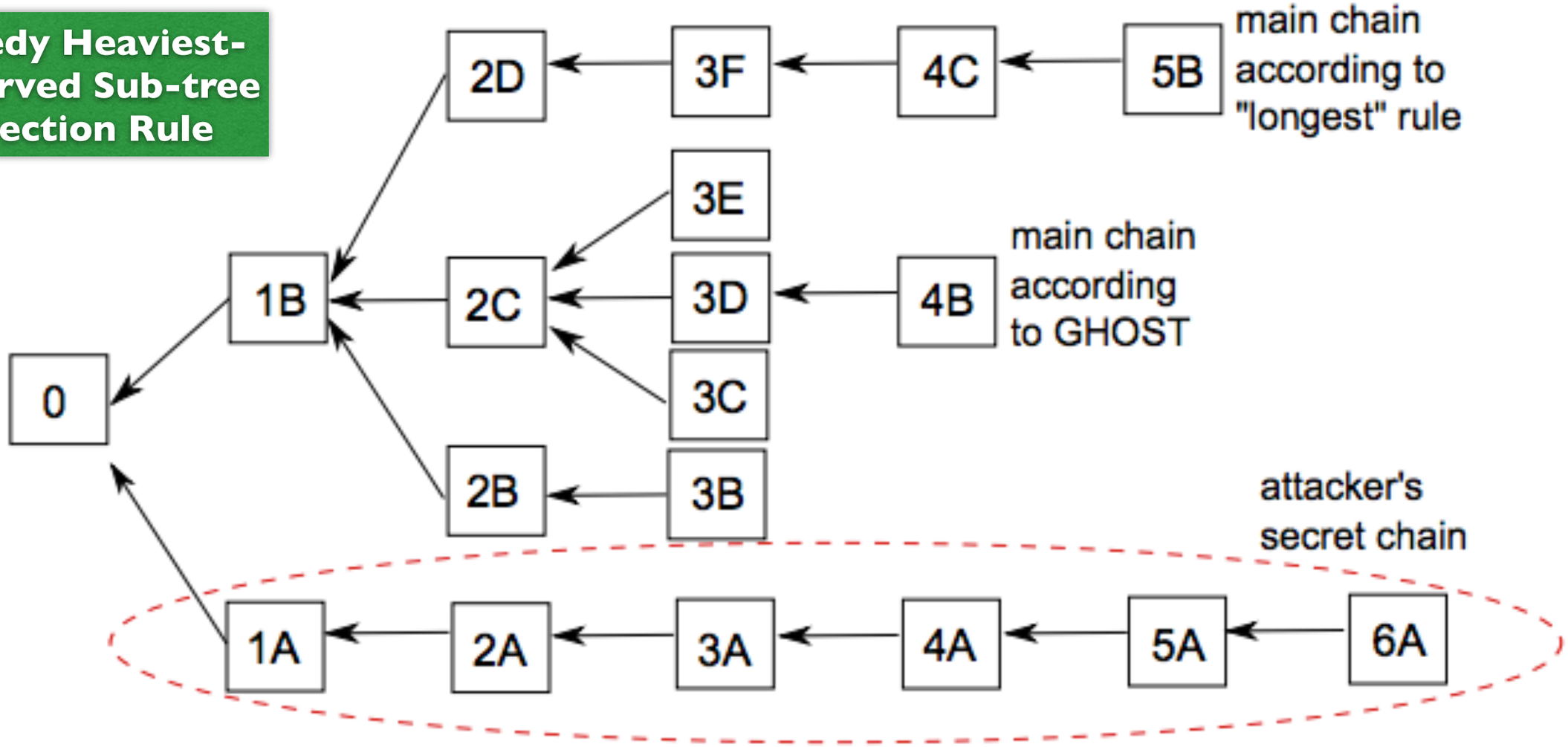
GHOST协议

http://www.avivz.net/pubs/15/btc_ghost_full.pdf

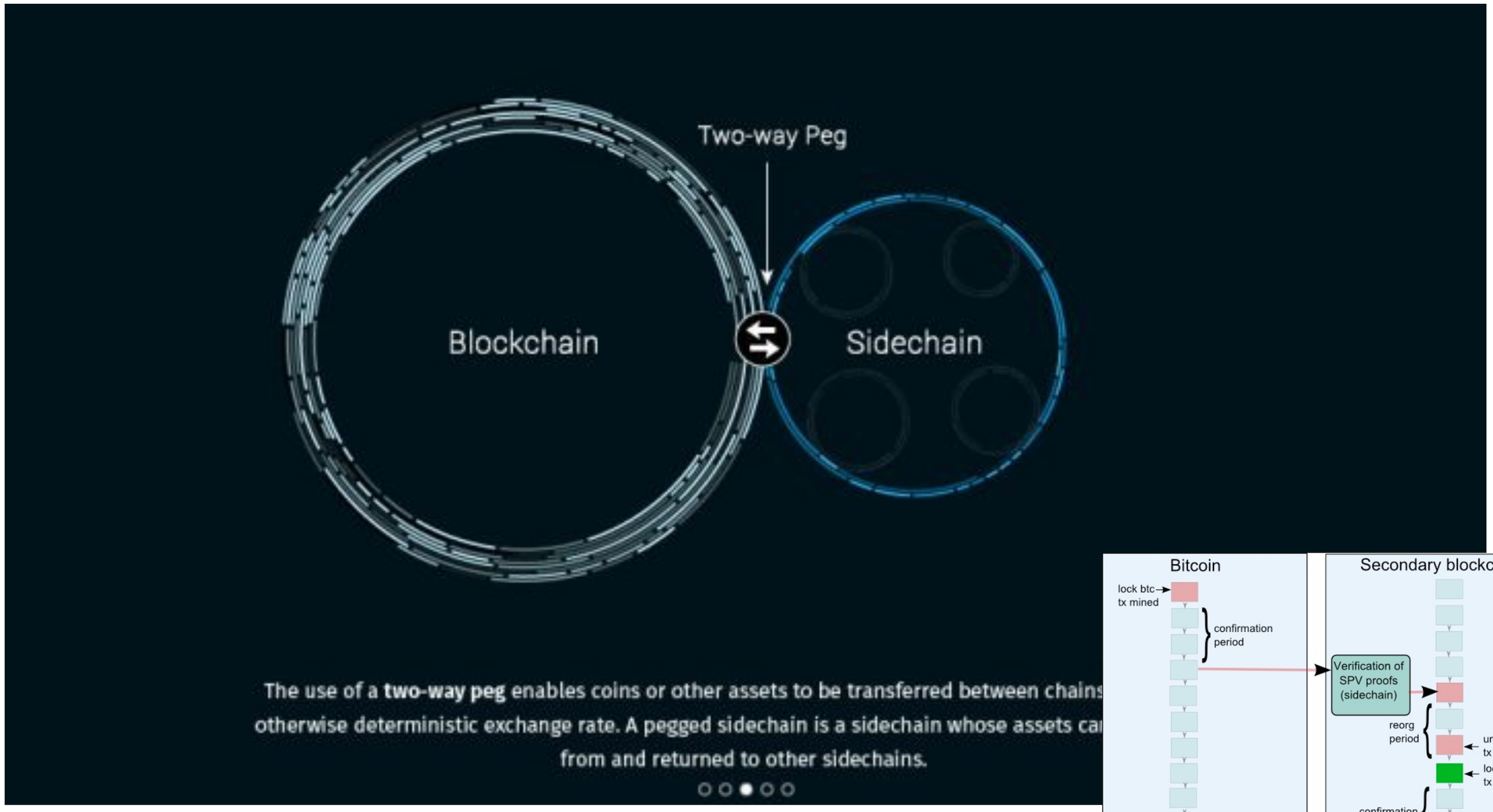
Secure High-Rate Transaction Processing in Bitcoin

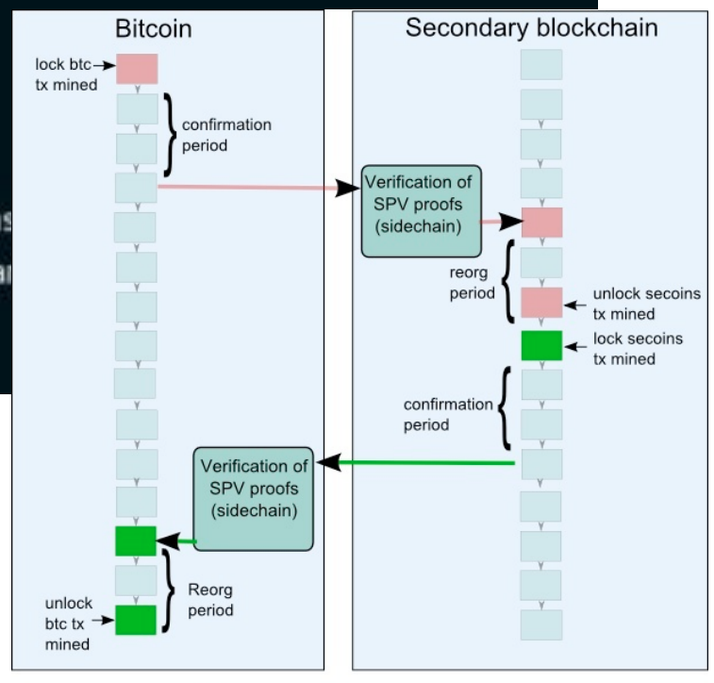
Financial Cryptography and Data Security 2015

Greedy Heaviest-Observed Sub-tree selection Rule

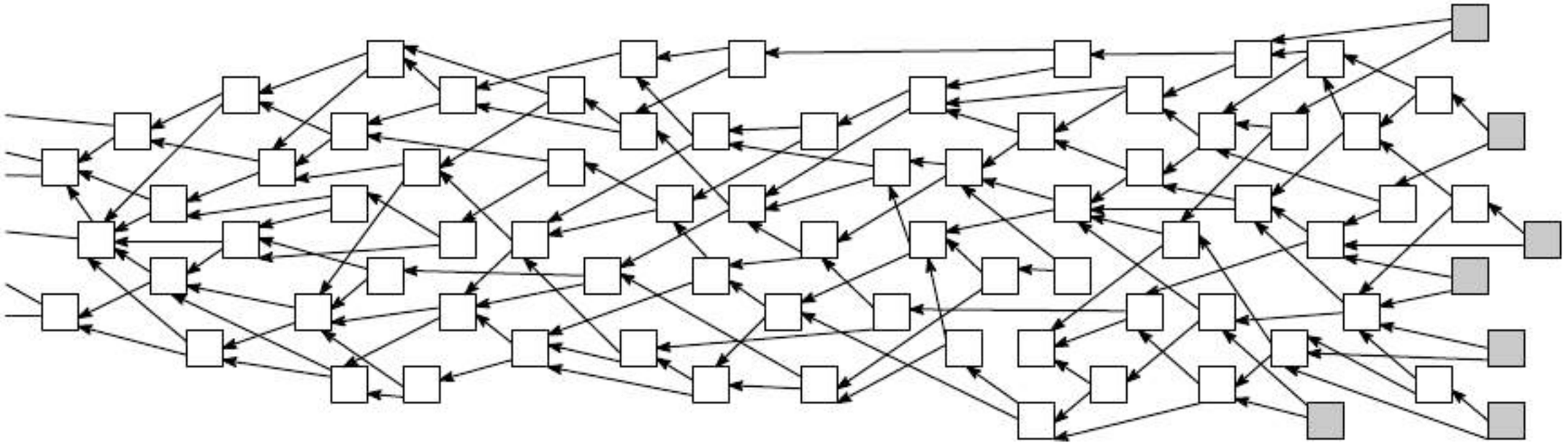


侧链

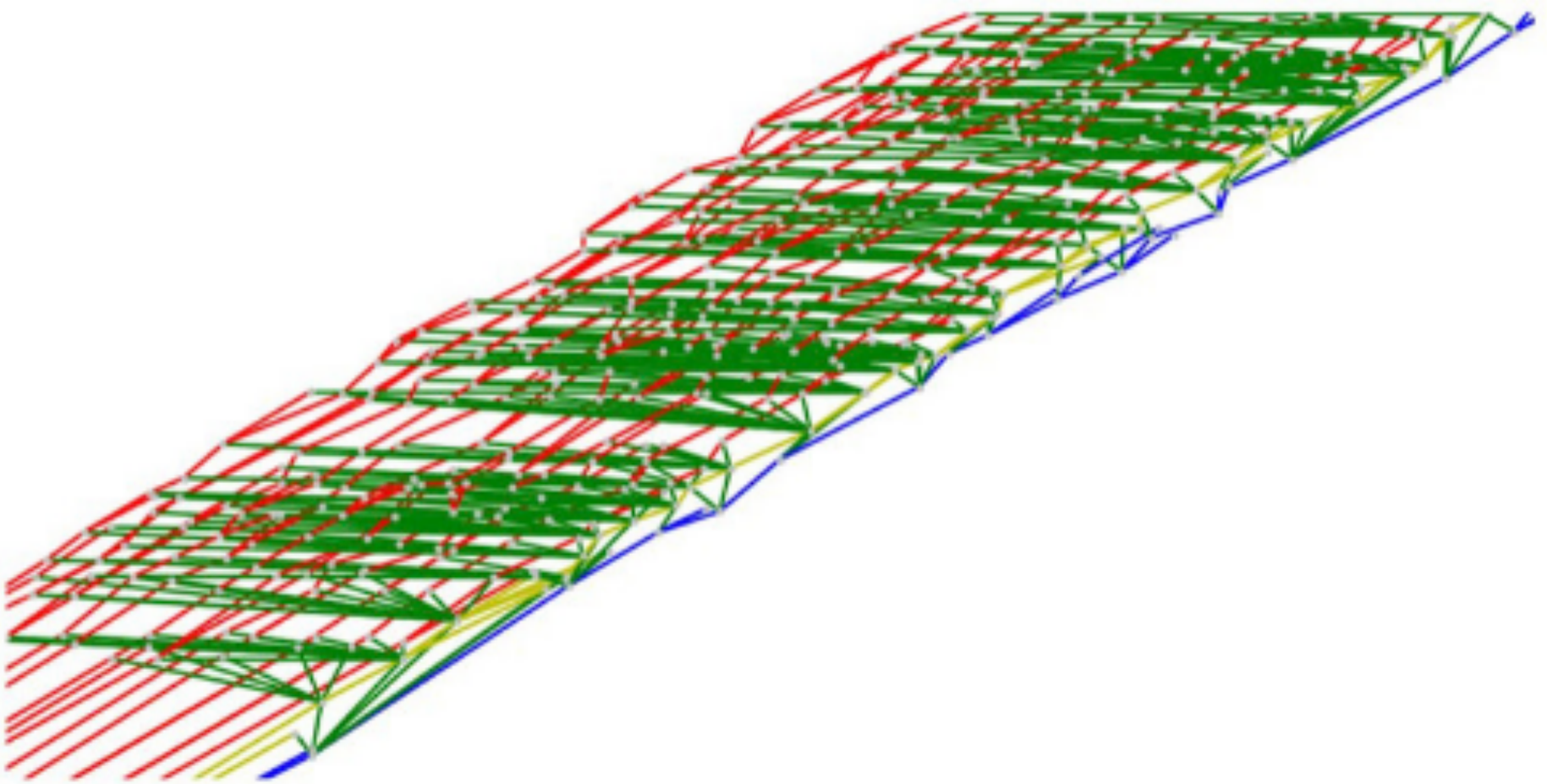

Two-way Peg
Blockchain
Sidechain
The use of a **two-way peg** enables coins or other assets to be transferred between chains
otherwise deterministic exchange rate. A pegged sidechain is a sidechain whose assets ca
from and returned to other sidechains.


Bitcoin
Secondary blockchain
lock btc tx mined
confirmation period
Verification of SPV proofs (sidechain)
reorg period
unlock secoins tx mined
lock secoins tx mined
confirmation period
Verification of SPV proofs (sidechain)
unlock btc tx mined
Reorg period
Affected blocks in secoins ->BTC transfer

DAG



分片



分片

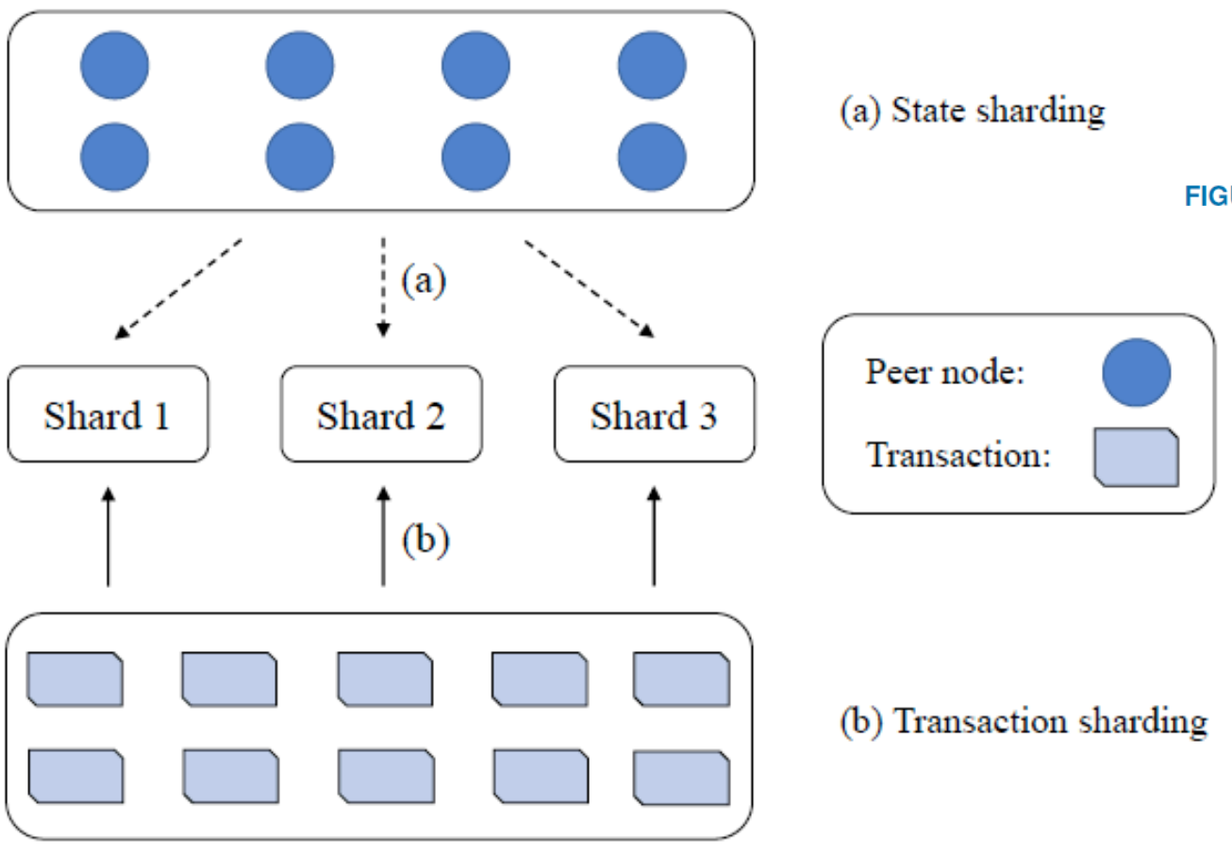


FIGURE 4. Illustration of Sharding. The initial network contains eight nodes (blue circle). After (a), nodes are assigned to different shards. (b) Transactions are distributed to different shards and be processed in parallel.

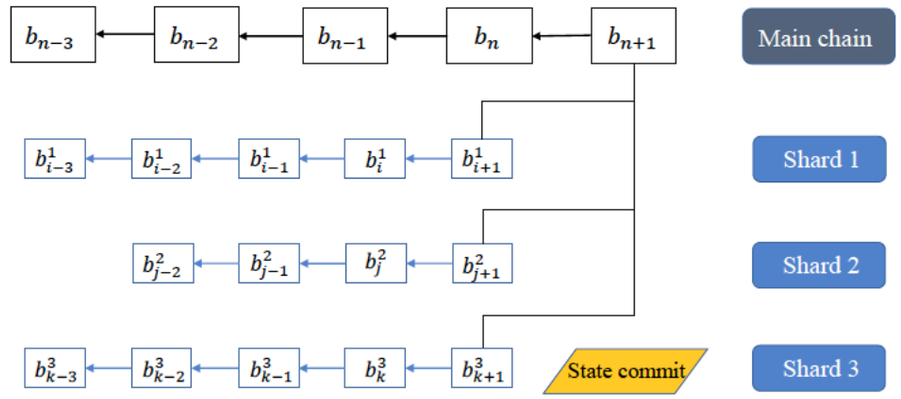
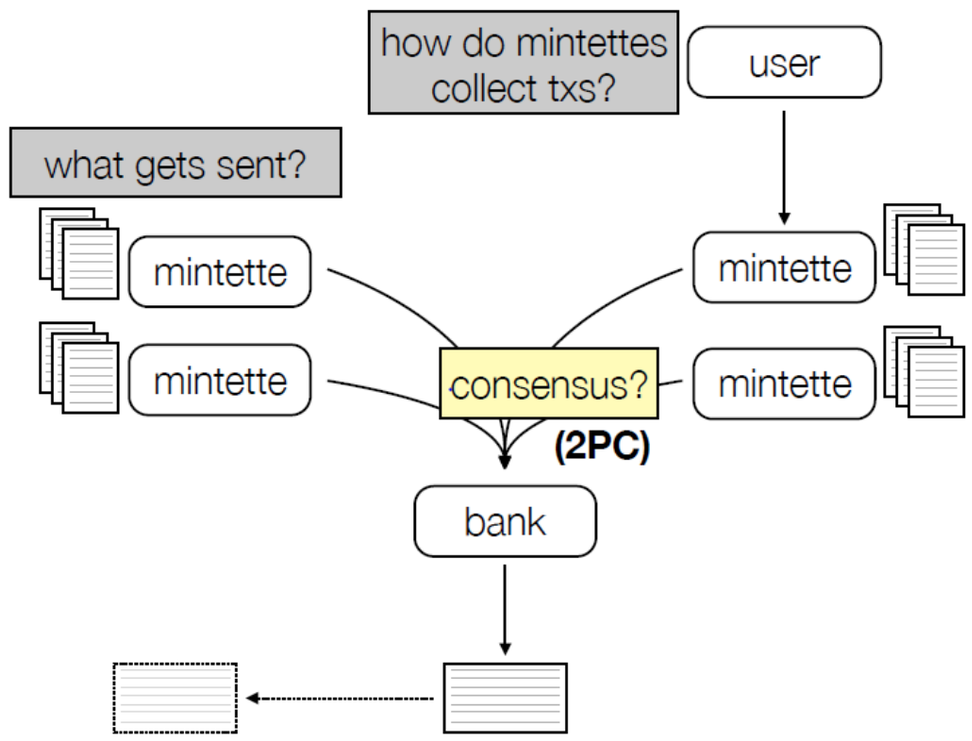
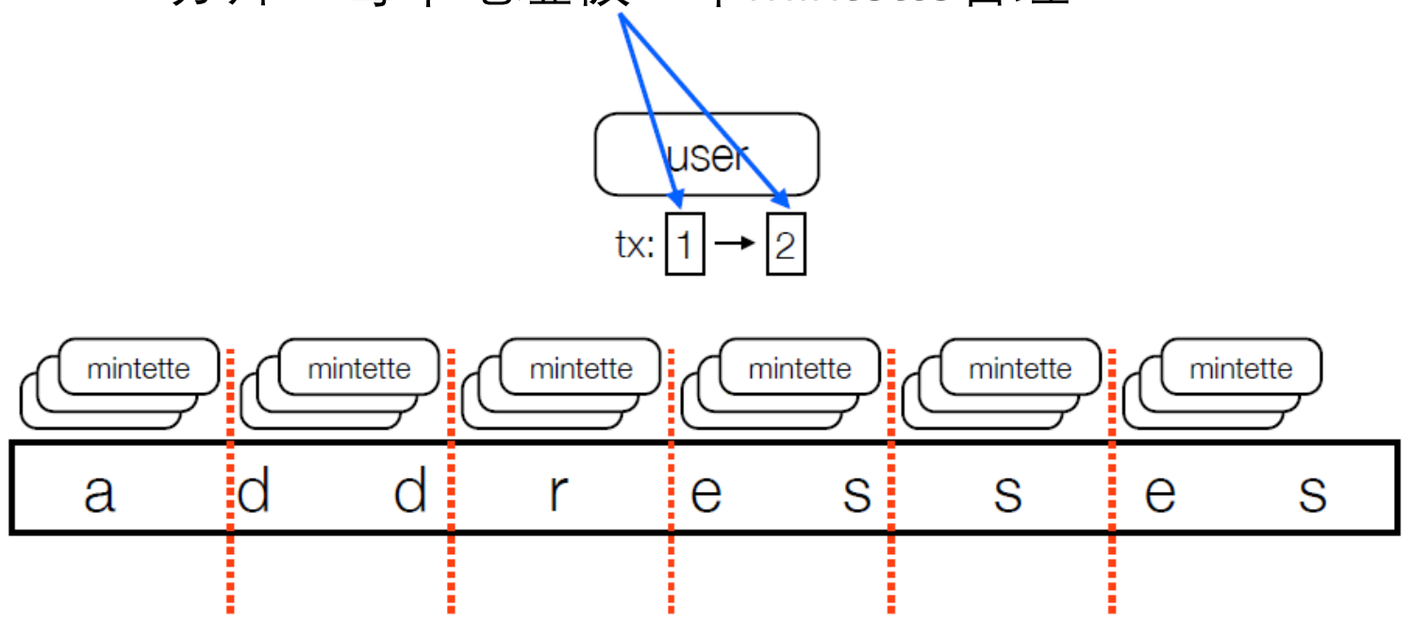


FIGURE 5. Architecture of the Sharding protocol with a Main chain

RSCoin



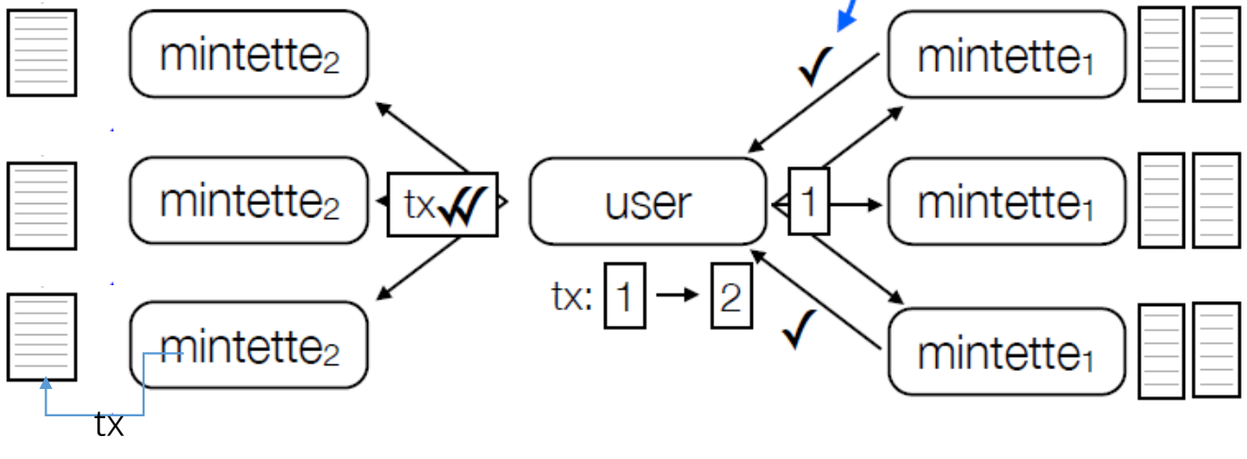
分片：每个地址被一个mintette管理



投票

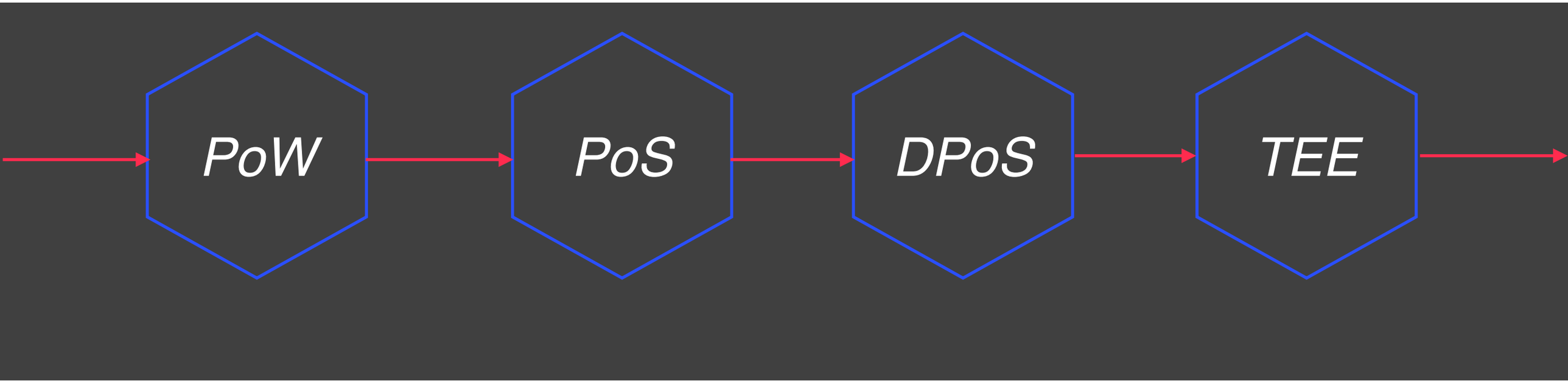
mintettes通过检查授权的mintette的签名来决定交易的有效性

mintette维护一个UTXO列表并负责双重支付的检查



如果签名满足条件，被提交到账本并返回收据

共识算法



共识模型

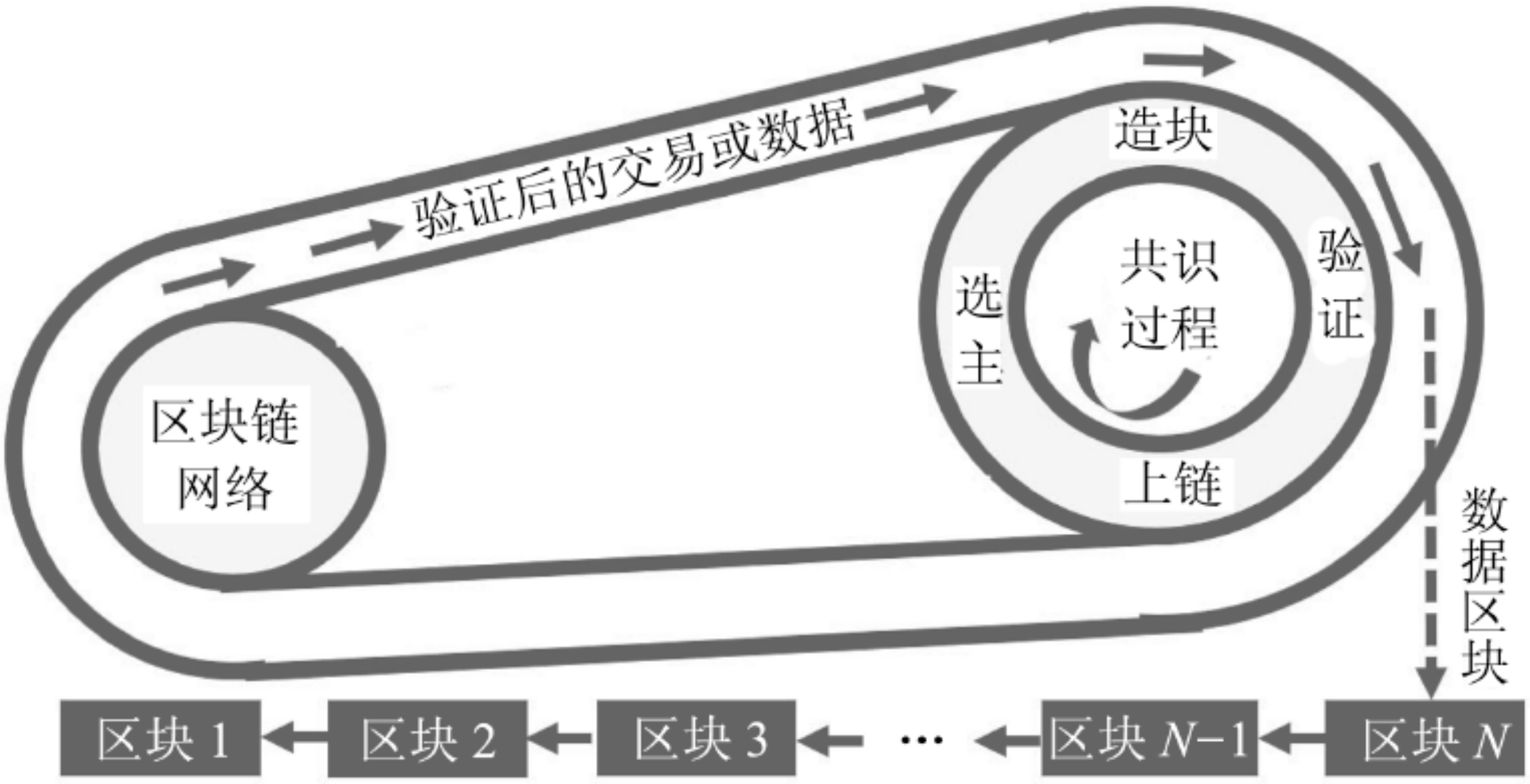


图 1　区块链共识过程的基础模型

共识算法

目的：在特定的**网络模型和故障模型**前提下，如何在缺乏中央控制和协调的分布式网络中确保**一致性**。（群龙无首）

基础理论：拜占庭将军问题

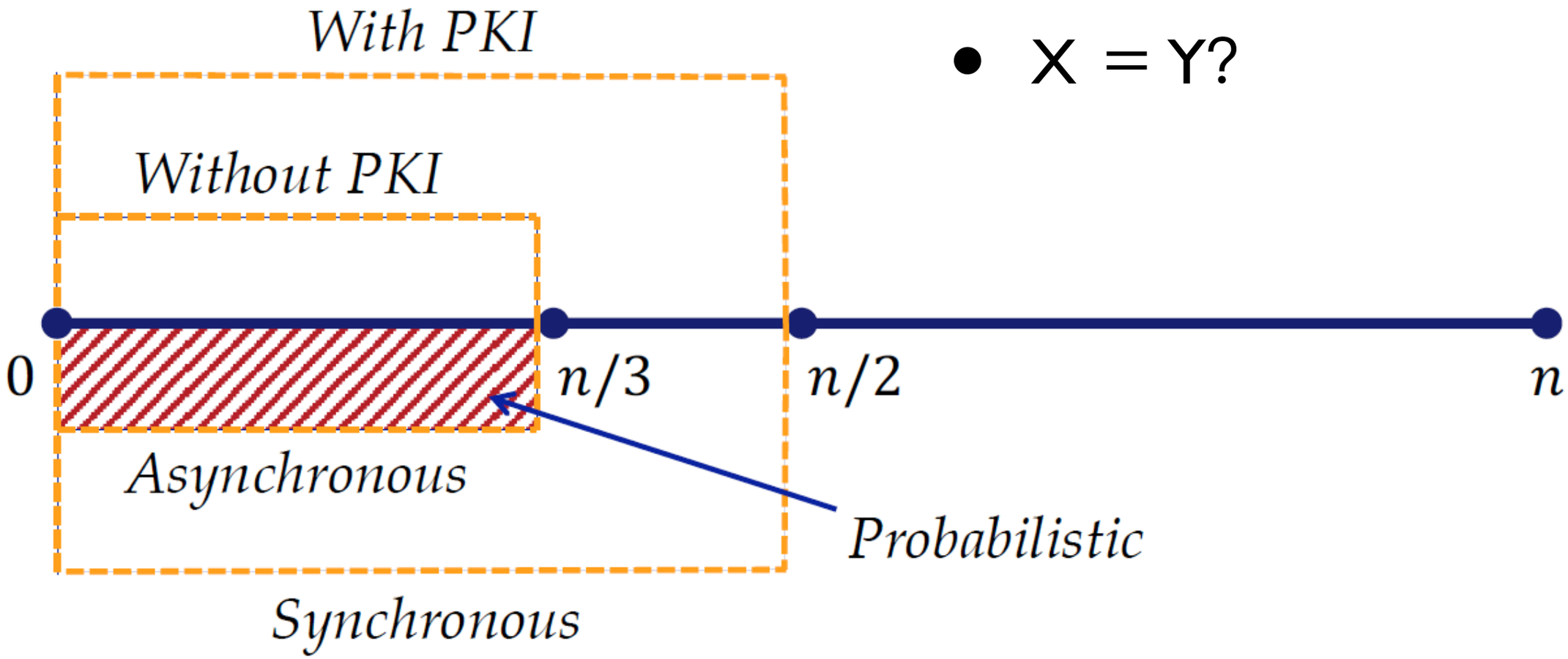
过程：选举 、出块、验证 、上链

根据选举策略分类：选举类（Paxos）、证明类（pow）、随机类（PoET）、联盟类（DPoS）和混合类（pow+pos）

根据演进方向分类：pow,pos,pow+pos,传统分布式一致性算法的改进及其他有明显的创新之处，具有一定的大规模应用的前景。

传统的共识

- N个节点，T个拜占庭节点
- 广播X
- 所有诚实节点输出Y
- X = Y?



PoW类

Pow类基本思想：矿工节点在每一轮共识过程中必须证明自己具有 某种特定的能力, 证明方式通常是竞争性地完成某 项难以解决但易于验证的任务, 在竞争中胜出的矿工节点将获得记账权

改进方向：扩容或者降低能耗以提高效率和公平。

典型代表：

- Proof Of Work（pow）
- Proof Of Elapsed Time（poet）
- Proof Of Luck(pol)
- Proof Of Useful Work（pouw）

PoUW

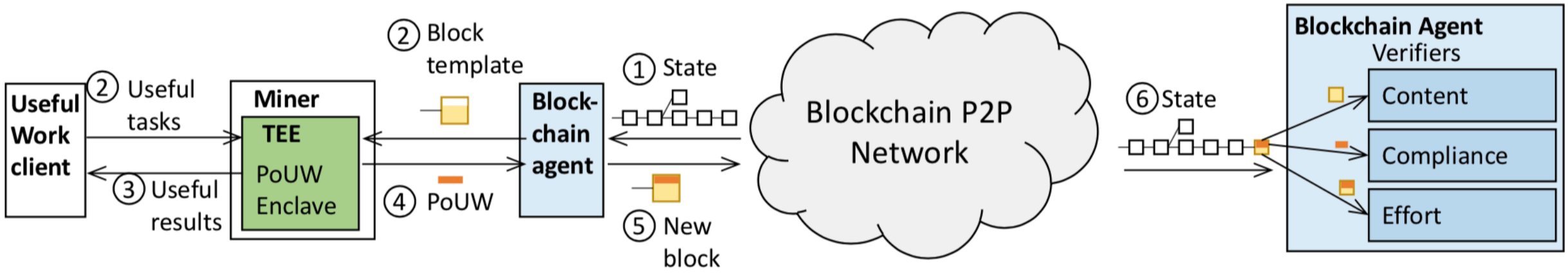
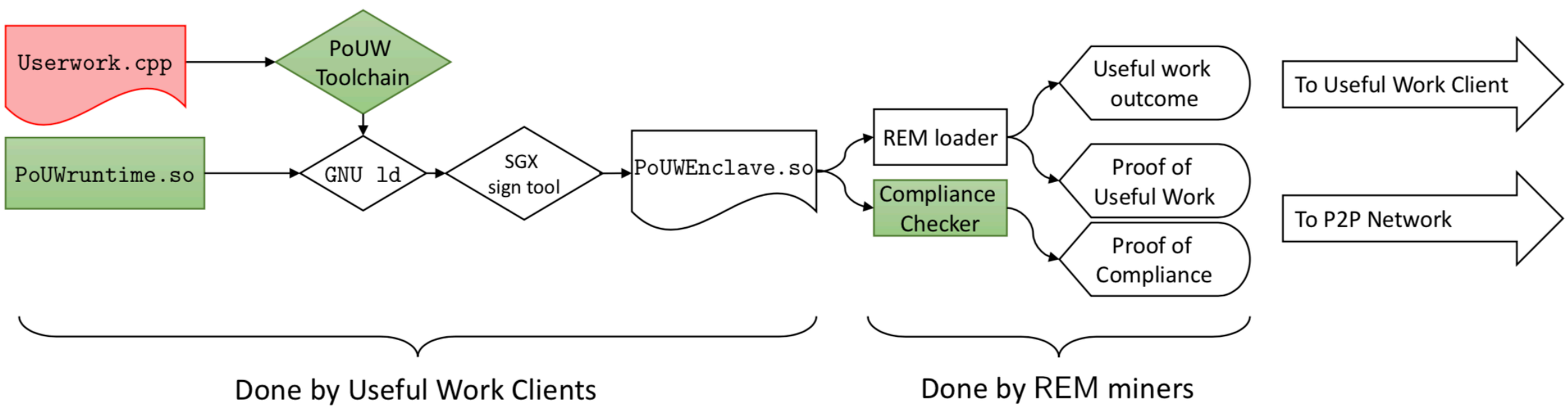


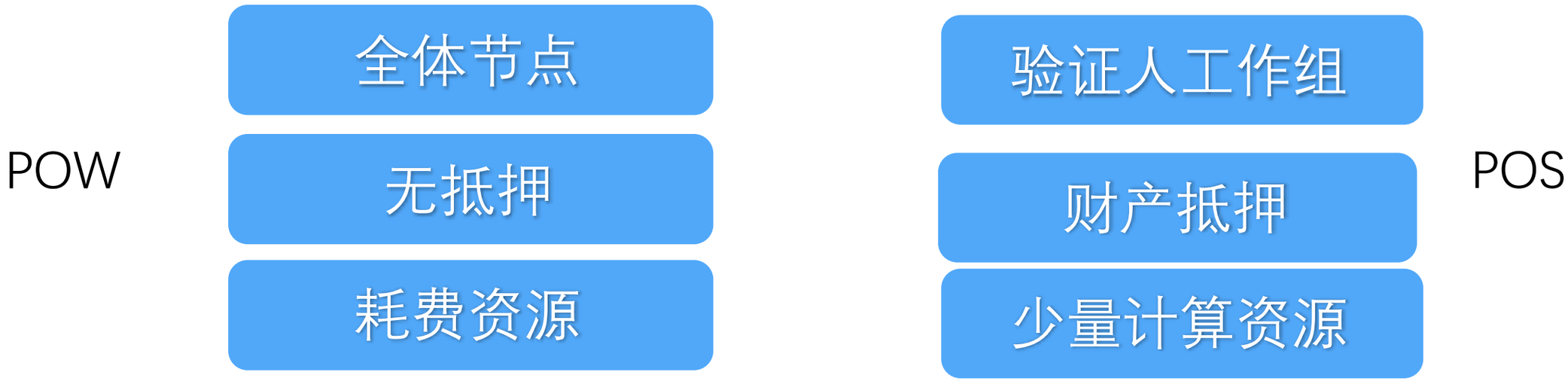
Figure 1: Architecture overview of REM



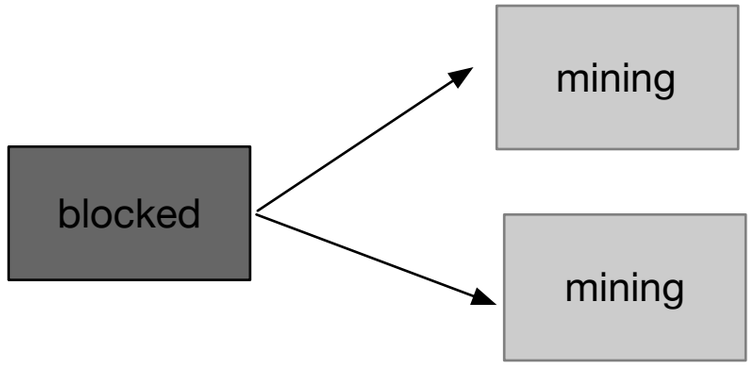
PoS

每个领导者被选出的概率与持有股份数量成比例，被选出的领导者可以生成区块。

—Janno Siim：Proof-of-Stake Research Seminar in Cryptography

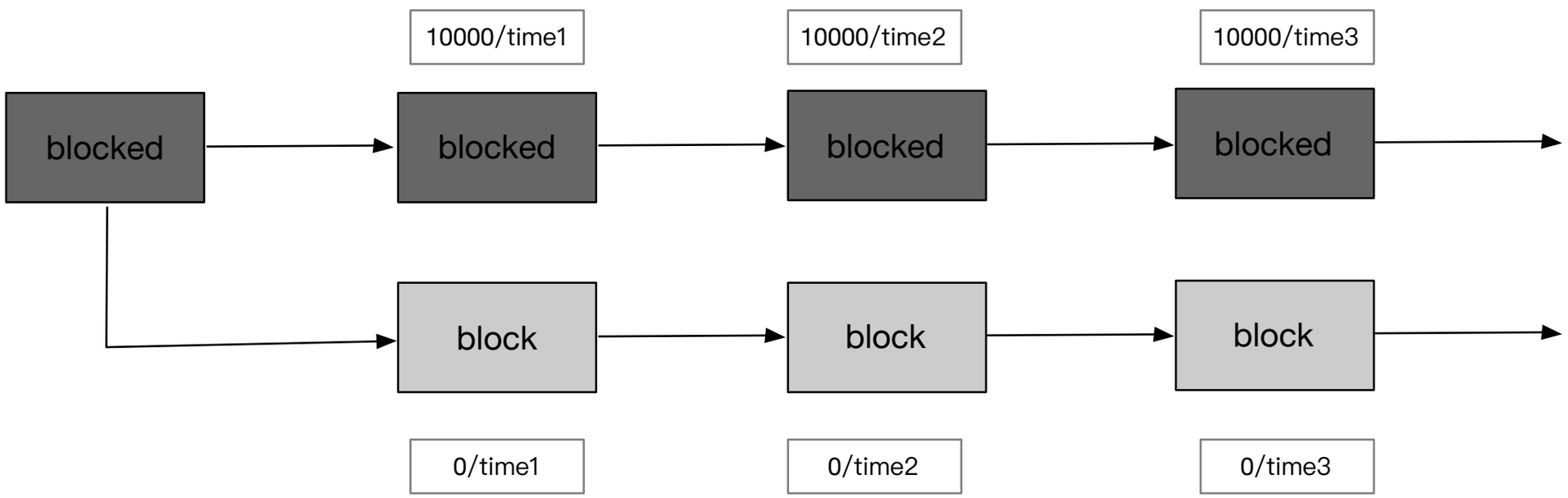


PoS攻击



- POS挖矿资源消耗的低
- 矿工在分叉链上挖矿消耗少
- 矿工可以同时挖分叉链
- 没有相应的限制和惩罚

- Deposit-based PoS



TEE + PoS

TEE： Trusted Execution Environments

1）独立于操作系统的一个执行区

2）提供一些密码函数和限制操作系统内存读写

3） **montonic counter 单调计数器**

TEE-based Pos

1) 资格证明和块签名由TEE产生。

2）用单调计数器保障每个高度最多产生一个快

3）两个单调计数器CTRep和CTRbs

4) CTRep记录已经提交的资格签名的块高度，CTRep记录已经提交的区块签名的块高度

5) 块高度H的出块资格条件 CTRep<H

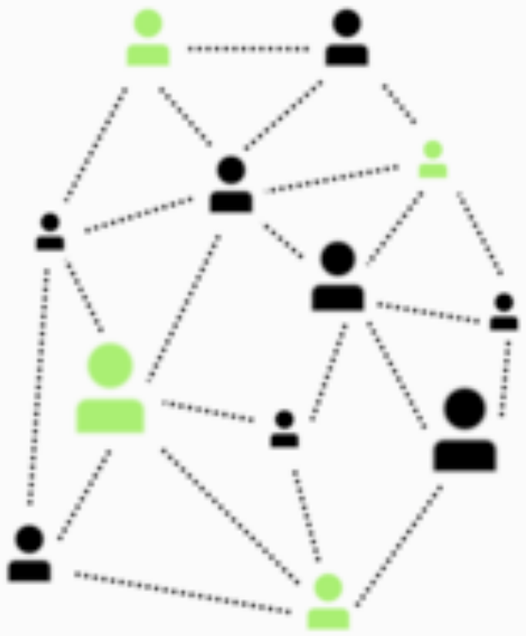
6）验证器签名块的条件 CTRbs<H

DPoS

Electing witnesses in a Delegated Proof-of-Stake network

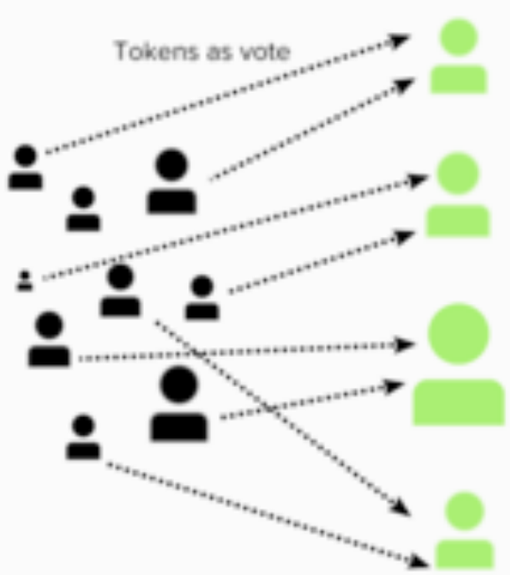
nichanank.com

1.



Nodes express interest in becoming a witness and begin lobbying, making positive contributions to the network and engaging the community.

2.



People in the network allocate their tokens as **votes** for witnesses

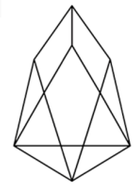
The more tokens they have, the higher their voting weight - hence *proof of stake**

3.

We end up with a ranking of nodes with the most votes (# tokens allocated to them).

The top N of these will become members of the elected witness panel. N depends on the network.

*Participants are NOT *giving* tokens to their witnesses. They are merely *alloting* funds to their choices as an expression of their vote. They can reassign their tokens to another witness at any time.



EOS

共识 + TEE

= inside TEE

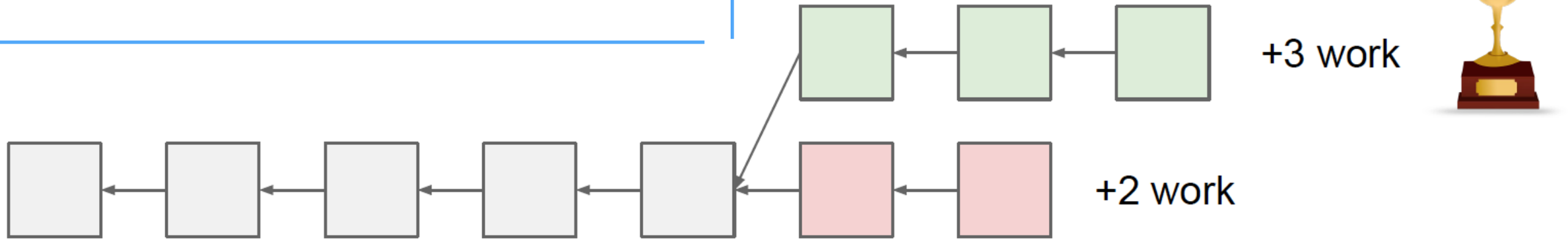
Start PoW

Do original proof of work (nonce, difficulty)

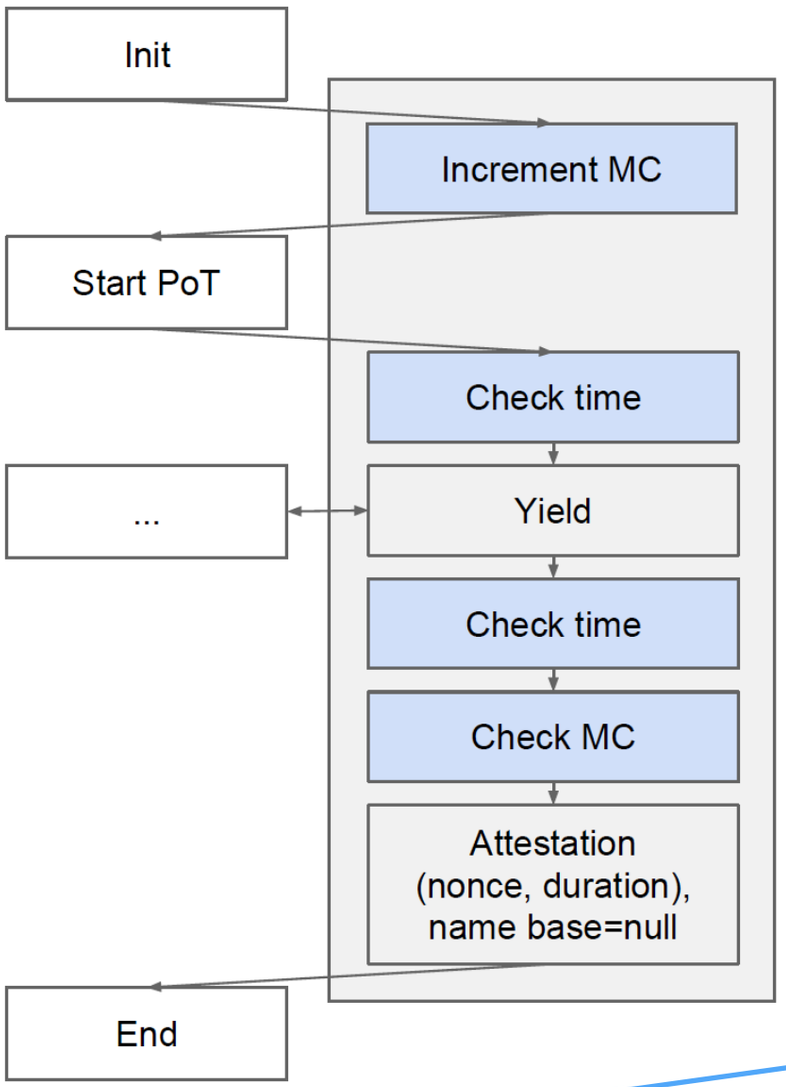
Attestation (nonce, difficulty), name base=null

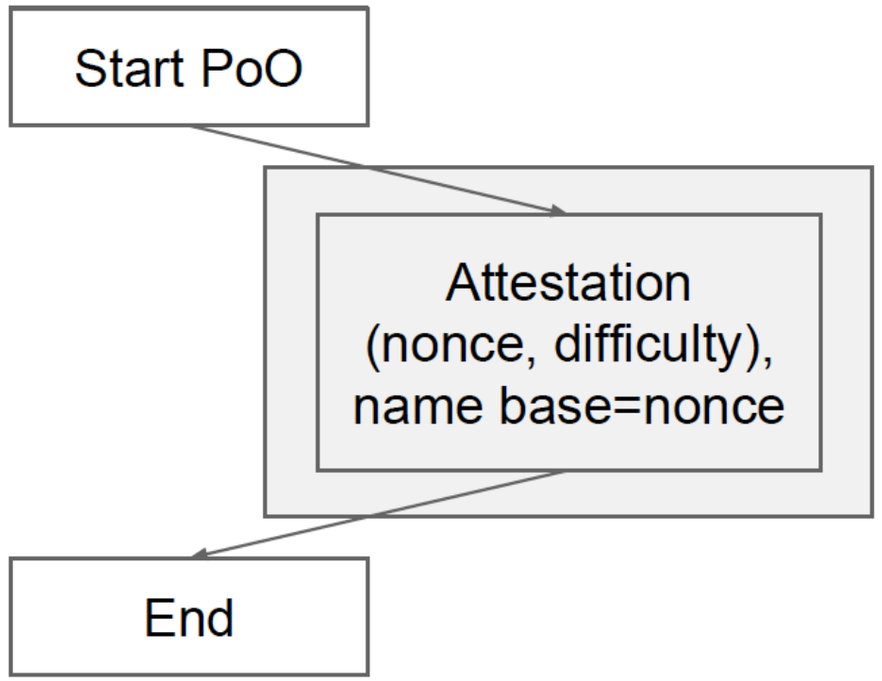
A pays B

A pays C



共识 + TEE

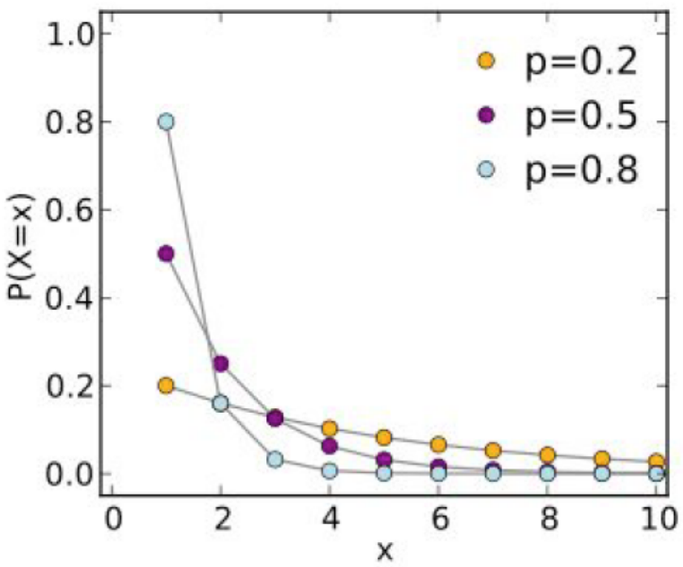




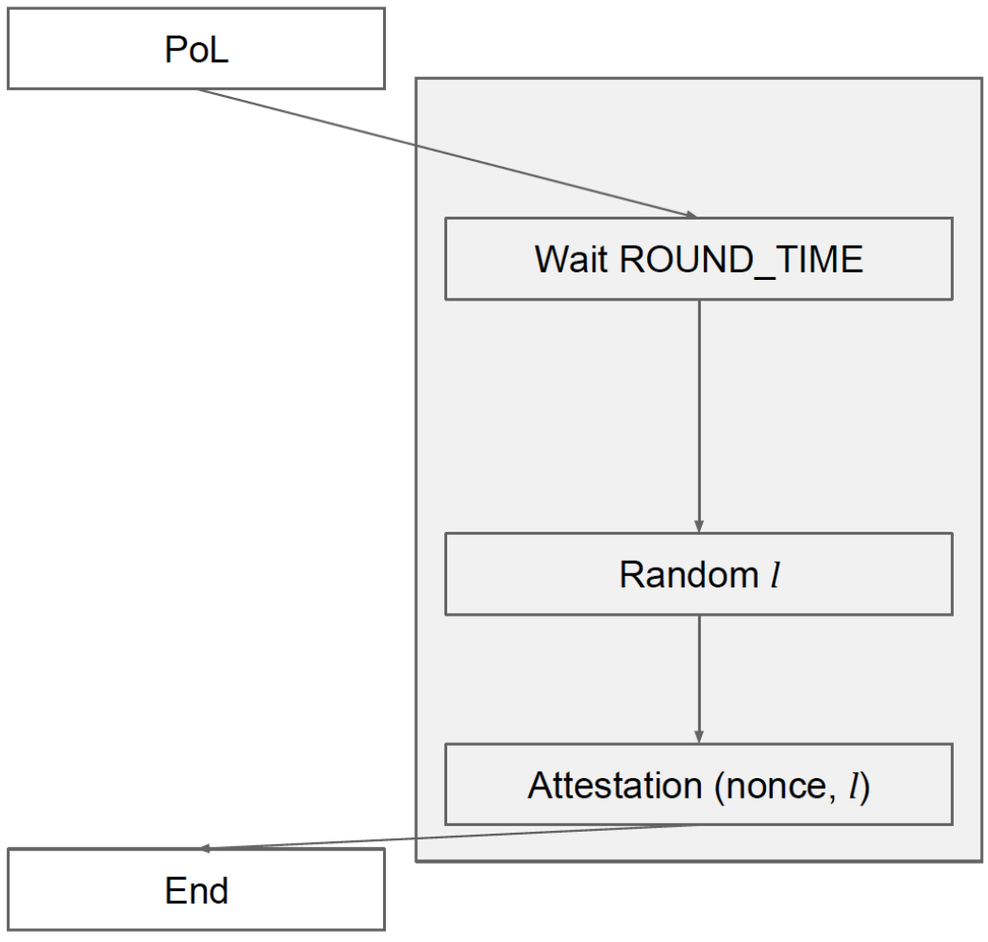

```
598fc24b...
c052d575...
d824325d...
fd3f6615...
f2c4d943...
d9799954...
fb2eb5e0...
439696f5...
c7882894...
00000000...
```

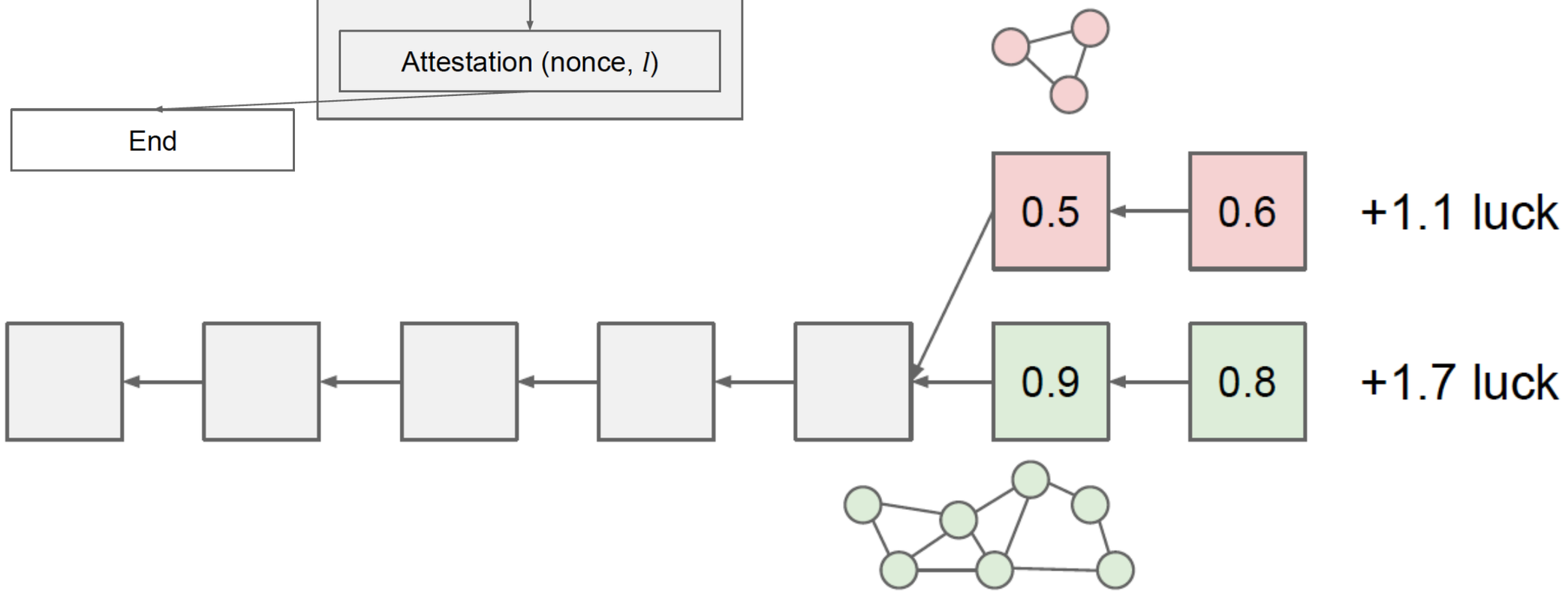
X ~ geometric distribution

$$\Pr[X = x] = (1-p)^{k-1}p$$

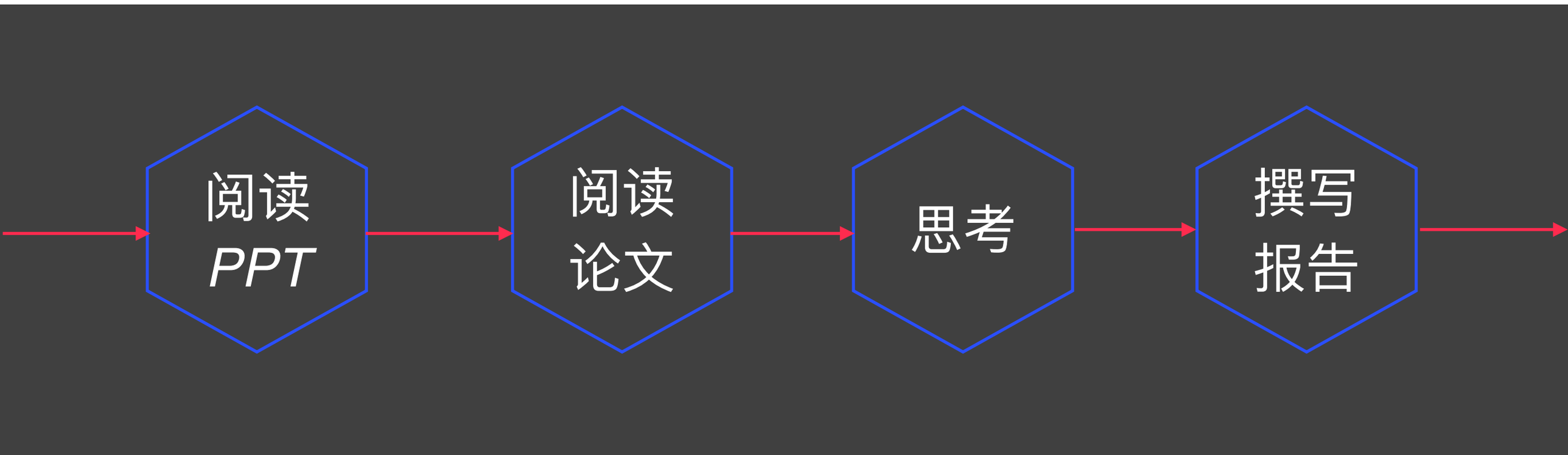


PoL


PoL
Wait ROUND_TIME
Random l
Attestation (nonce, l)
End

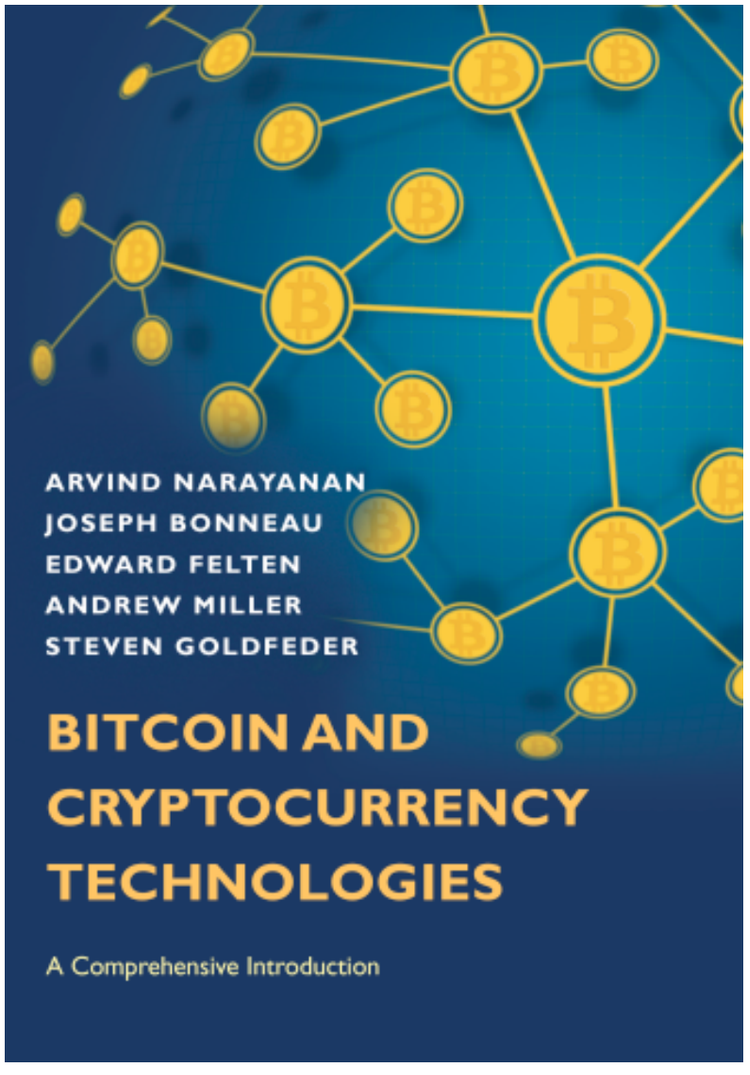

0.5
0.6
+1.1 luck
0.9
0.8
+1.7 luck

课后作业



Homework

阅读教材



阅读第6、7、8、9章

Homework

课后作业

要求阅读如下文章，写阅读报告

自己选择和课程项目相关的一篇论文

说明课程项目涉及哪些论文
这篇论文的作用

1、文章概述
2、主要收获
3、存在疑问
4、所思所感
5、一篇论文

周日晚上12点前提交

谢谢！

Huiping Sun

sunhp@ss.pku.edu.cn

https://huipingsun.github.io