Blockchain
区块链

2018.04.10

比特币平台、生态系统和未来

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

课程项目

下次课汇报

比特币平台

加密货币生态系统

比特币未来

比特币作为平台

比特币平台

- 比特币已经work，基于比特币能做什么？

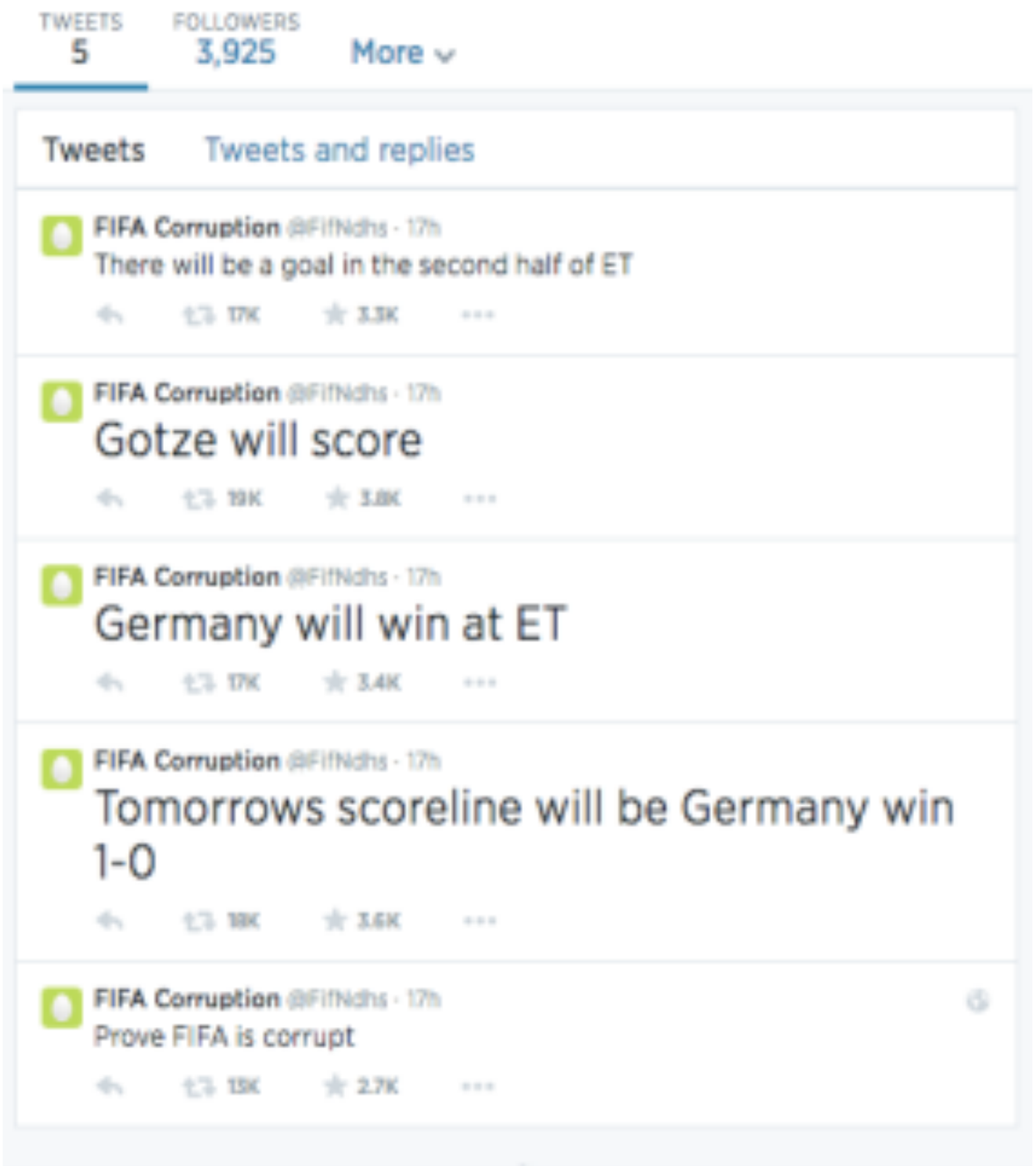
- 作为一个只能增加的记录
- 作为一个智能资产
- 建立博彩系统
- 建立公共随机数源
- 建立预测市场

安全时间戳

- 时间TI公布H(r, x)，TI后可以公布r和x

- 证明创意的有限性
- 证明一些事件的先后顺序

预测未来



FIFA2014　腐败指责

离线时间戳


26
guardtime
guardtime.com
15 July 2009 00:00:00 UTC
AAAAAA-CKLUOA-AAI7FX-EHPAMP
VRUBSC-7DQE7O-TZBCP4-MS5S65
UBOSEC-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、需要矿工一只追踪

- 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

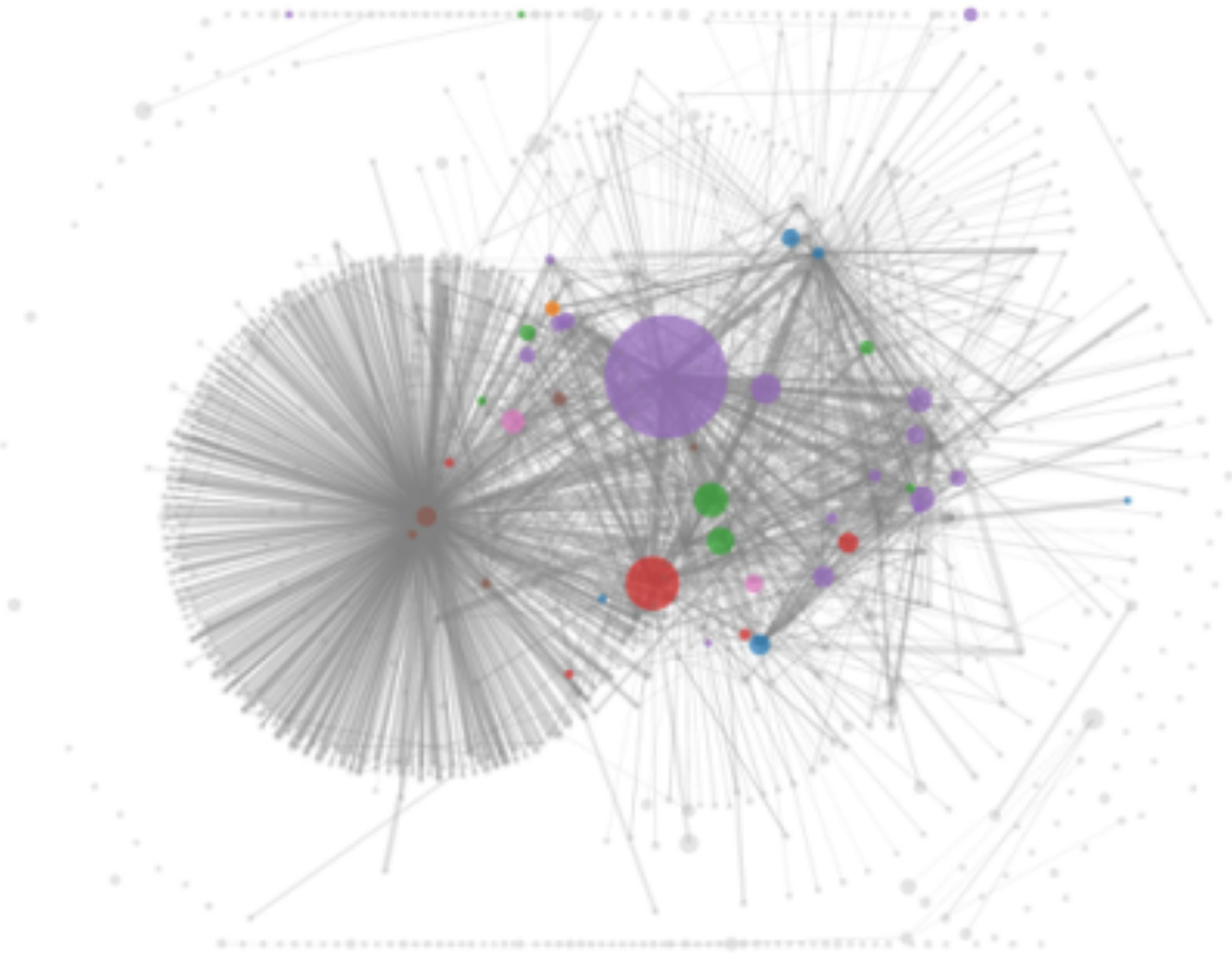
可以提高代价，P2SH

技术归技术

管理归管理

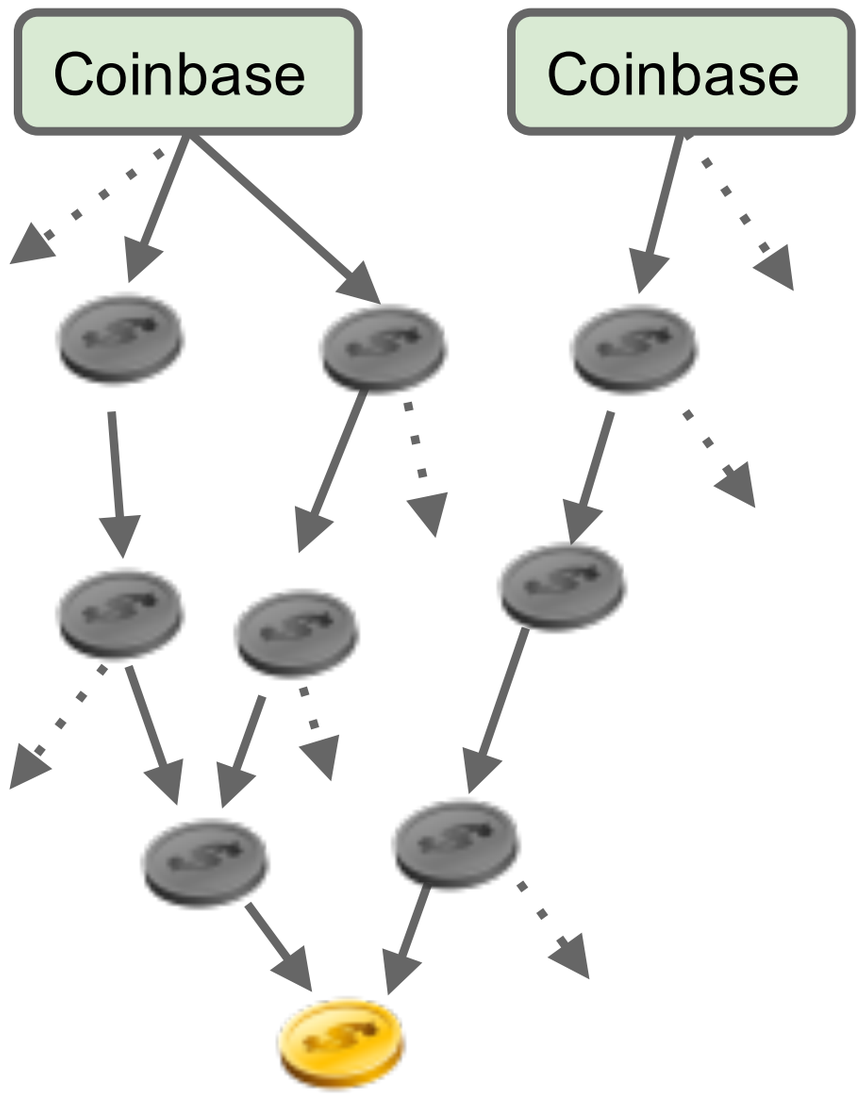
法律归法律

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

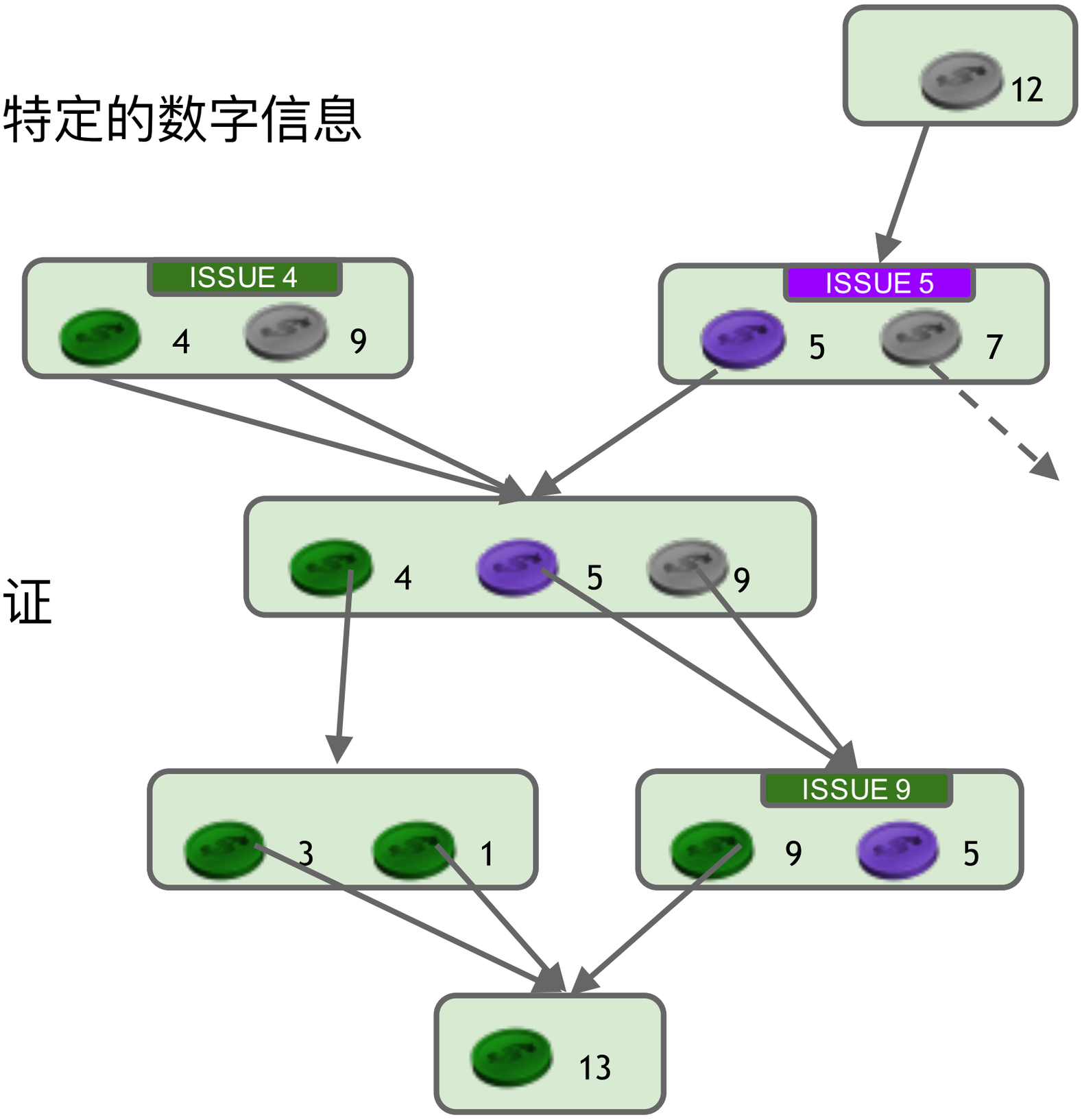
认证应用

"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

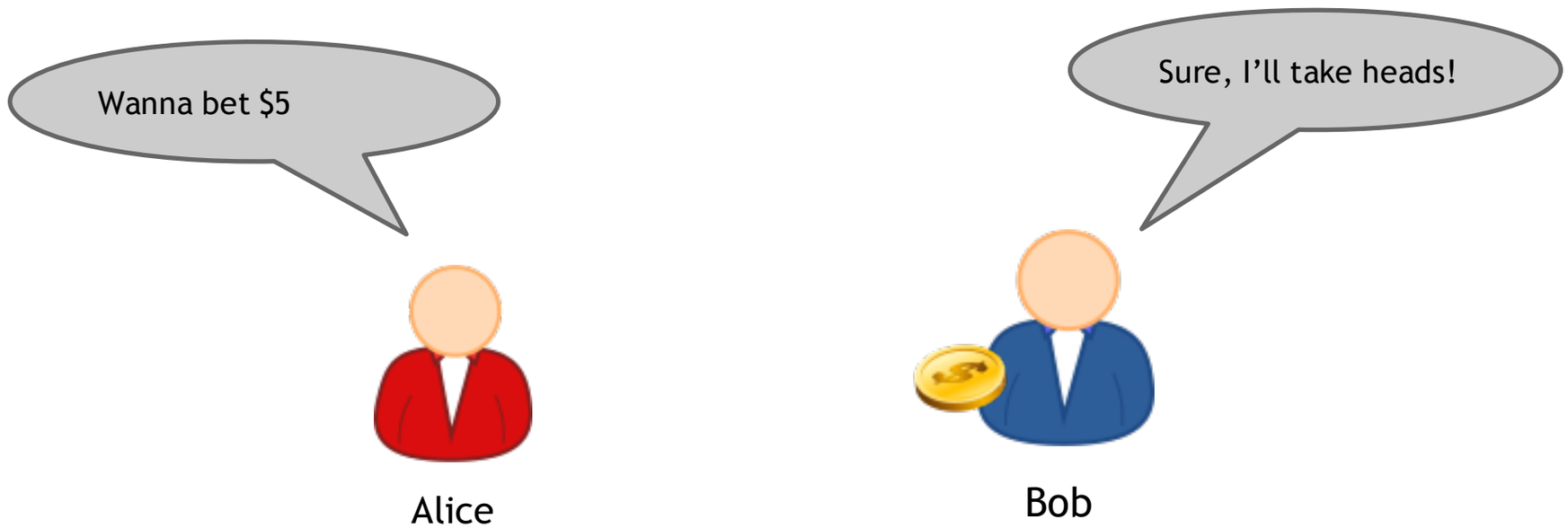
数字资产

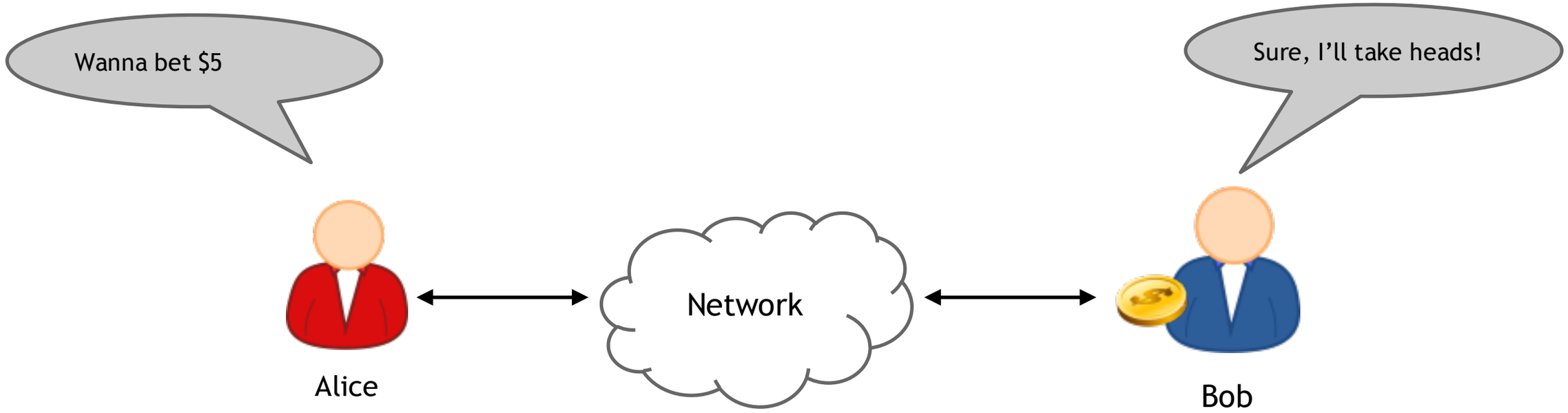
物理资产

股票

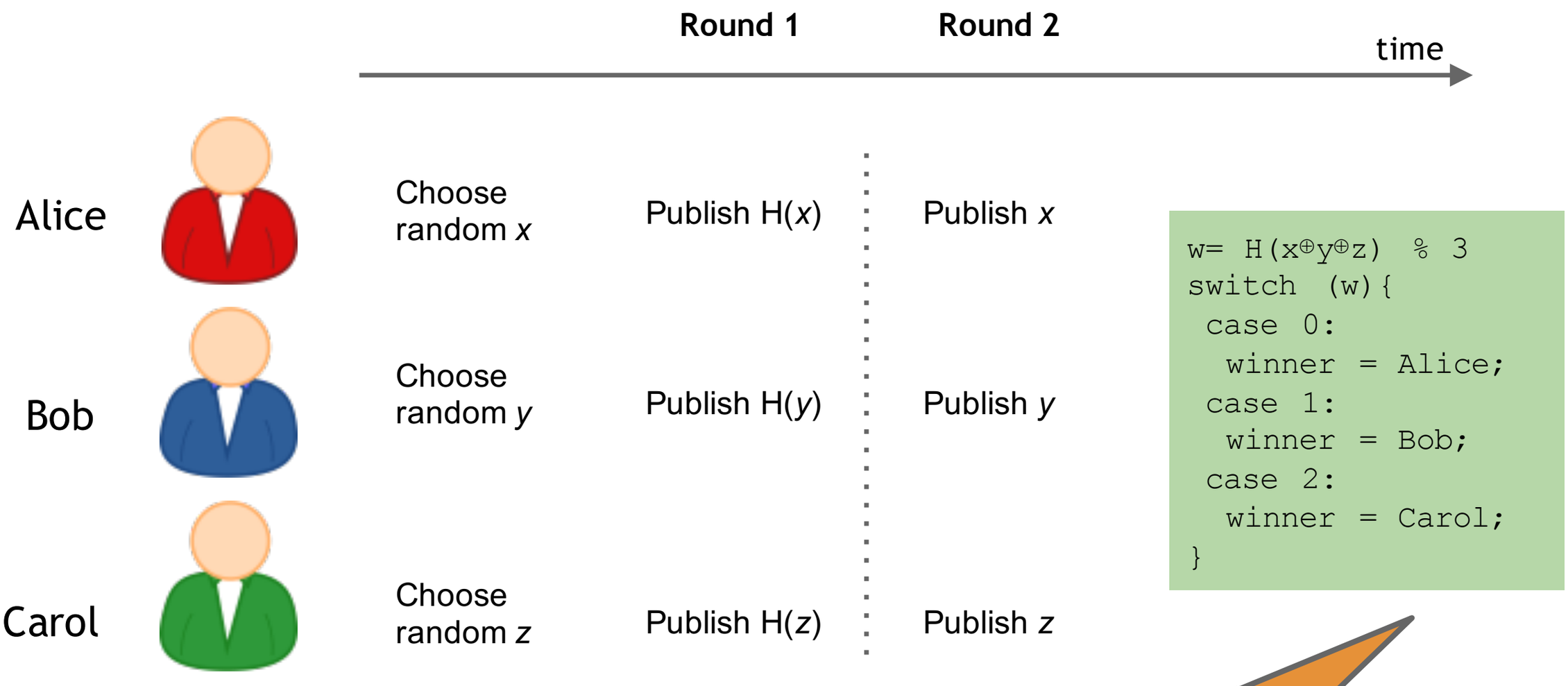
域名币

博彩

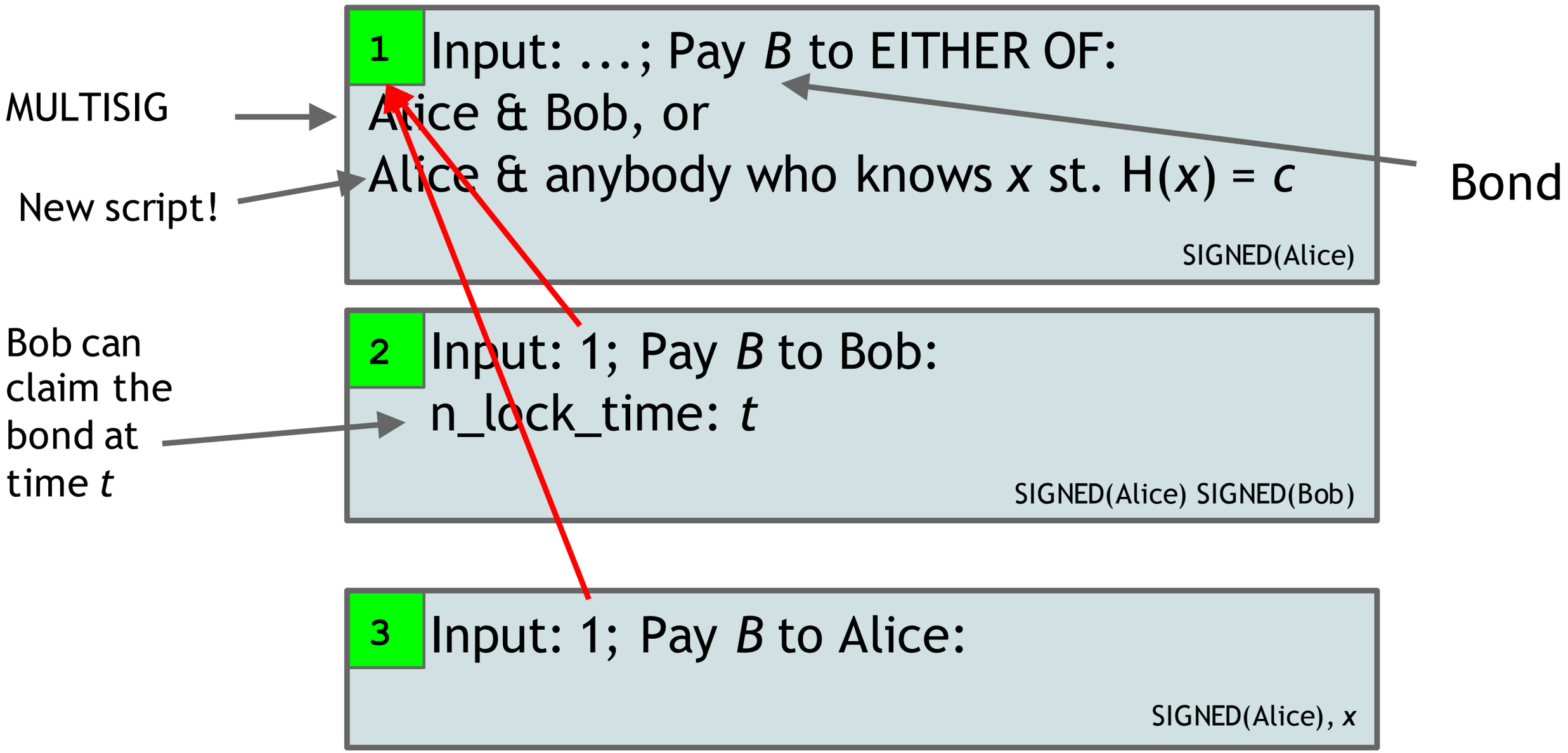

Wanna bet $5
Sure, I'll take heads!
Alice
Bob


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

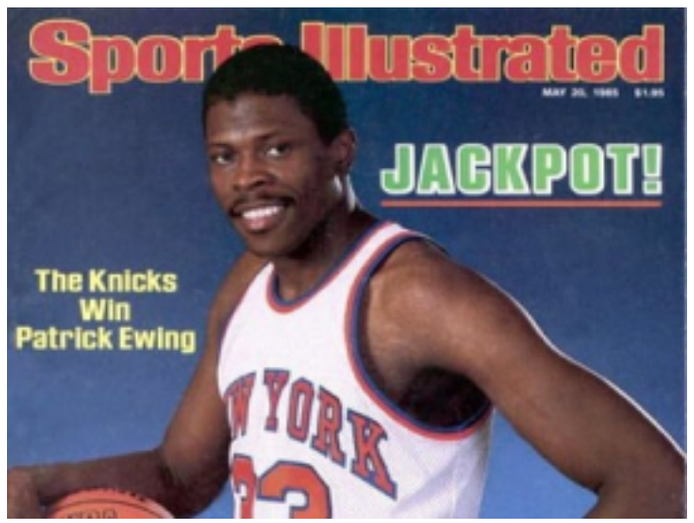
时间约束的在线博彩



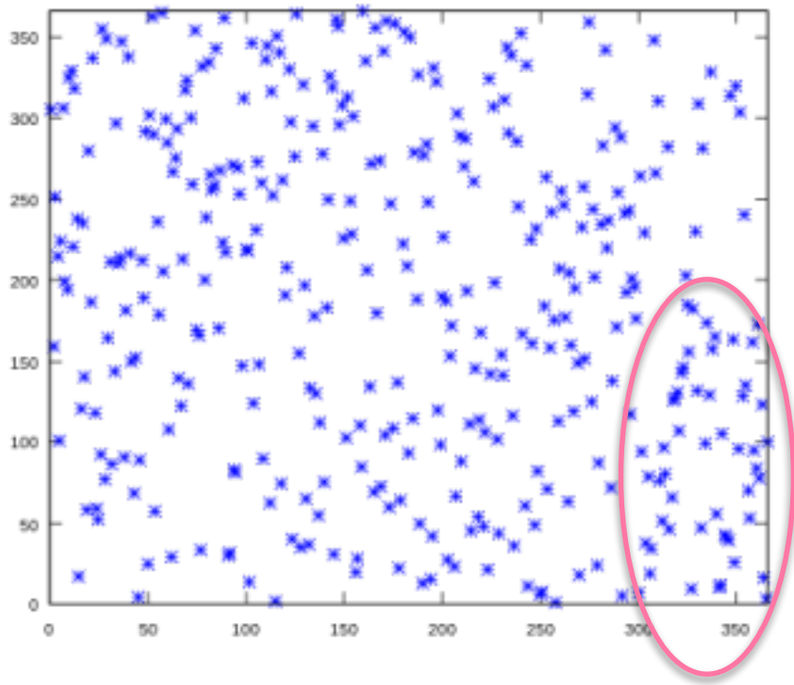
x revealed if Alice reclaims her bond

随机源

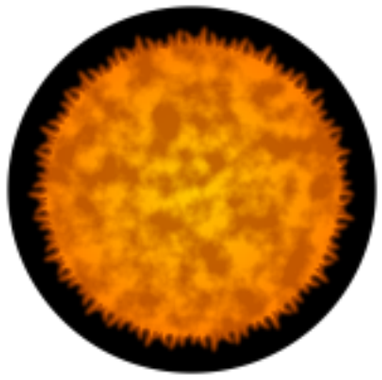

NBA
DRAFT
LOTTERY


Sports Illustrated
JACKPOT!
The Knicks
Win
Patrick Ewing

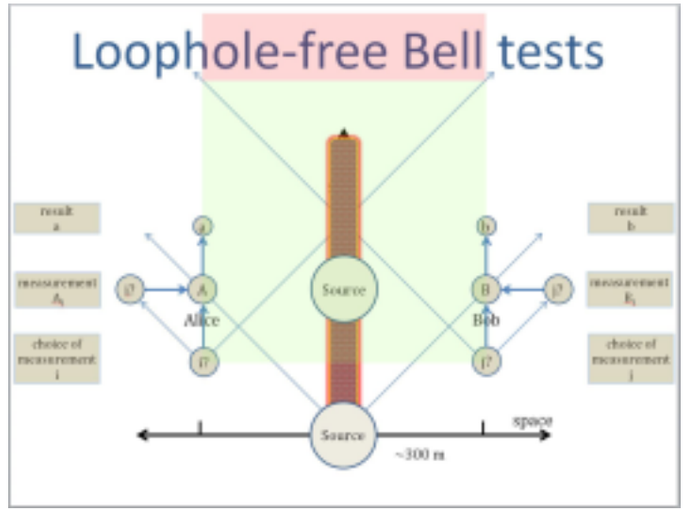

Bent Corner

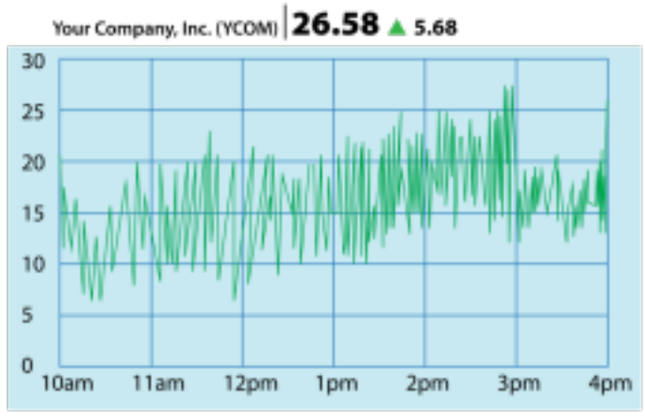

350
300
250
200
150
100
50
0
0
50
100
150
200
250
300
350

随机源

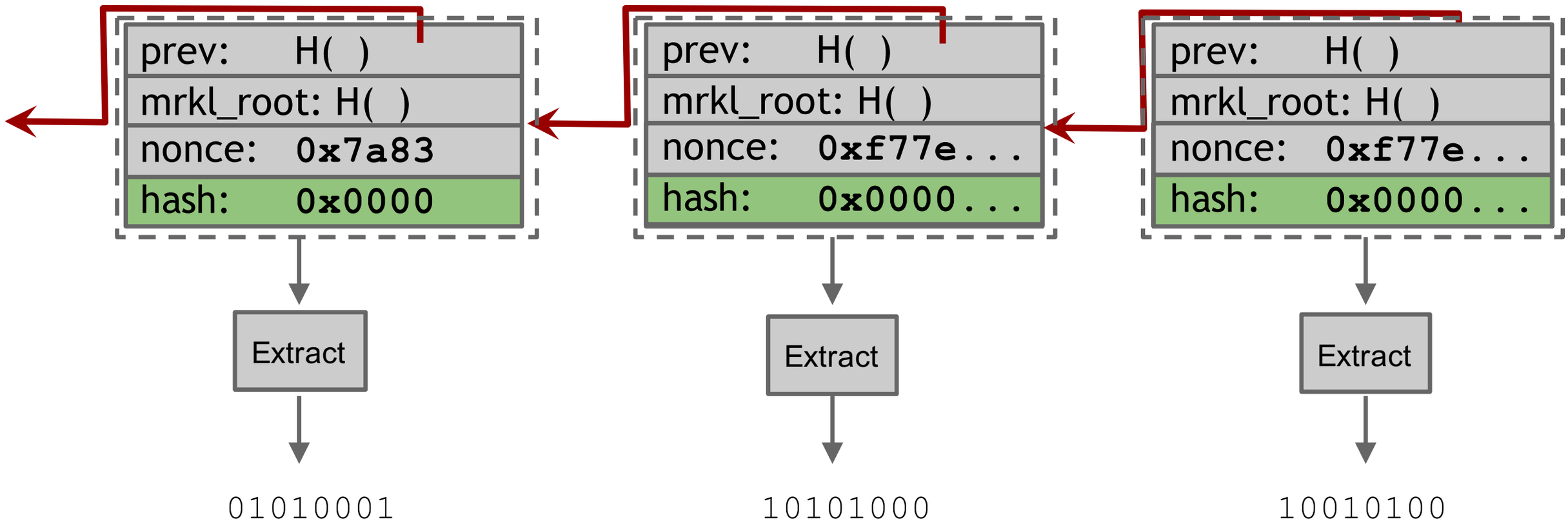



BINGO


Loophole-free Bell tests
result a
measurement A_x
choice of measurement x
result b
measurement B_y
choice of measurement y
a
A
Alice
x
x'
Source
b
B
Bob
y
y'
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

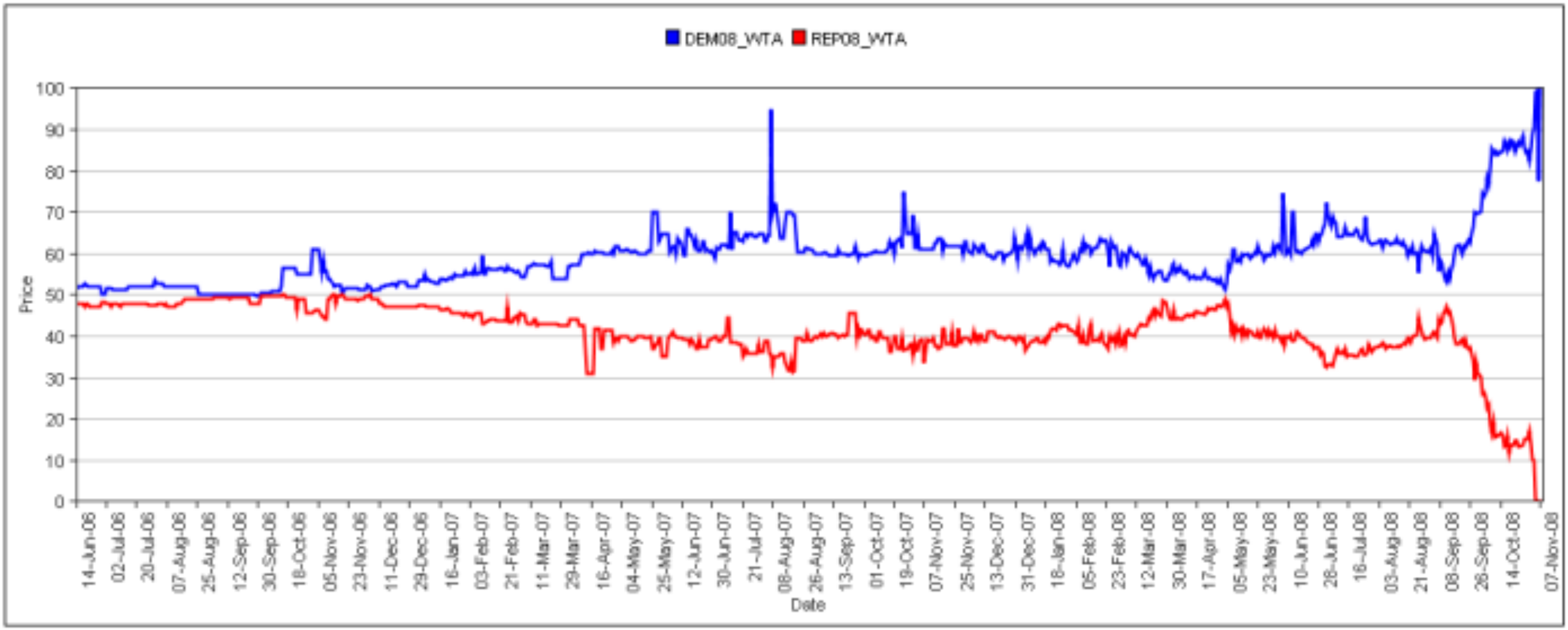
比特币作为随机源


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

REALITY KEYS Pricing Developers Legal Privacy About

Facts about the future, cryptographic proof when they come true.

39 million topics

Follow a Freebase fact

Will Hillary Clinton become US President?

Will Edward Snowden win a Nobel Peace Prize?

You can follow facts about any of the 39 million topics in the Freebase open directory.

Exchange rates

Follow an exchange rate

Will a Dollar be worth more than a Euro?

Will Bitcoin hit $1000 again?

We track the exchange rates of traditional currencies and crypto-currencies.

Blockchain addresses

Follow a transaction

I'm selling Litecoins for Bitcoins. Have I been paid?

Are the bitcoins seized from Silk Road still there?

You can follow any transaction in the blockchain of Bitcoin or any crypto-currency we monitor.

优缺点

Scottish independence referendum results to be for the independence

A month left

Sell at **0.50**

Buy at **1.40**

Scottish independence referendum results to be against the independence.

A month left

Sell at **8.60**

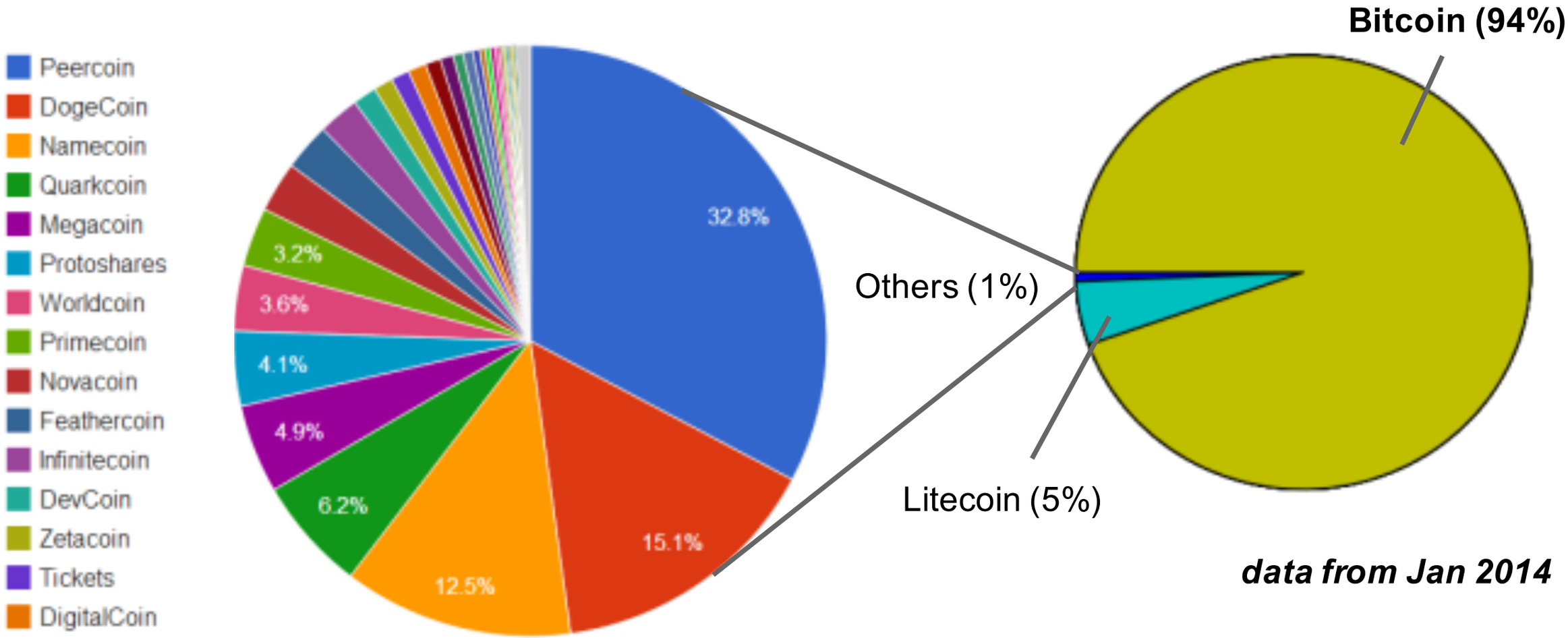
Buy at **9.50**

Orange?

Yellow?

加密货币生态系统

加密货币


Peercoin
DogeCoin
Namecoin
Quarkcoin
Megacoin
Protoshares
Worldcoin
Primecoin
Novacoin
Feathercoin
Infinitecoin
DevCoin
Zetacoin
Tickets
DigitalCoin
32.8%
15.1%
12.5%
6.2%
4.9%
4.1%
3.6%
3.2%
Bitcoin (94%)
Others (1%)
Litecoin (5%)
data from Jan 2014

一些代币

为什么发行

如何发行

吸矿工

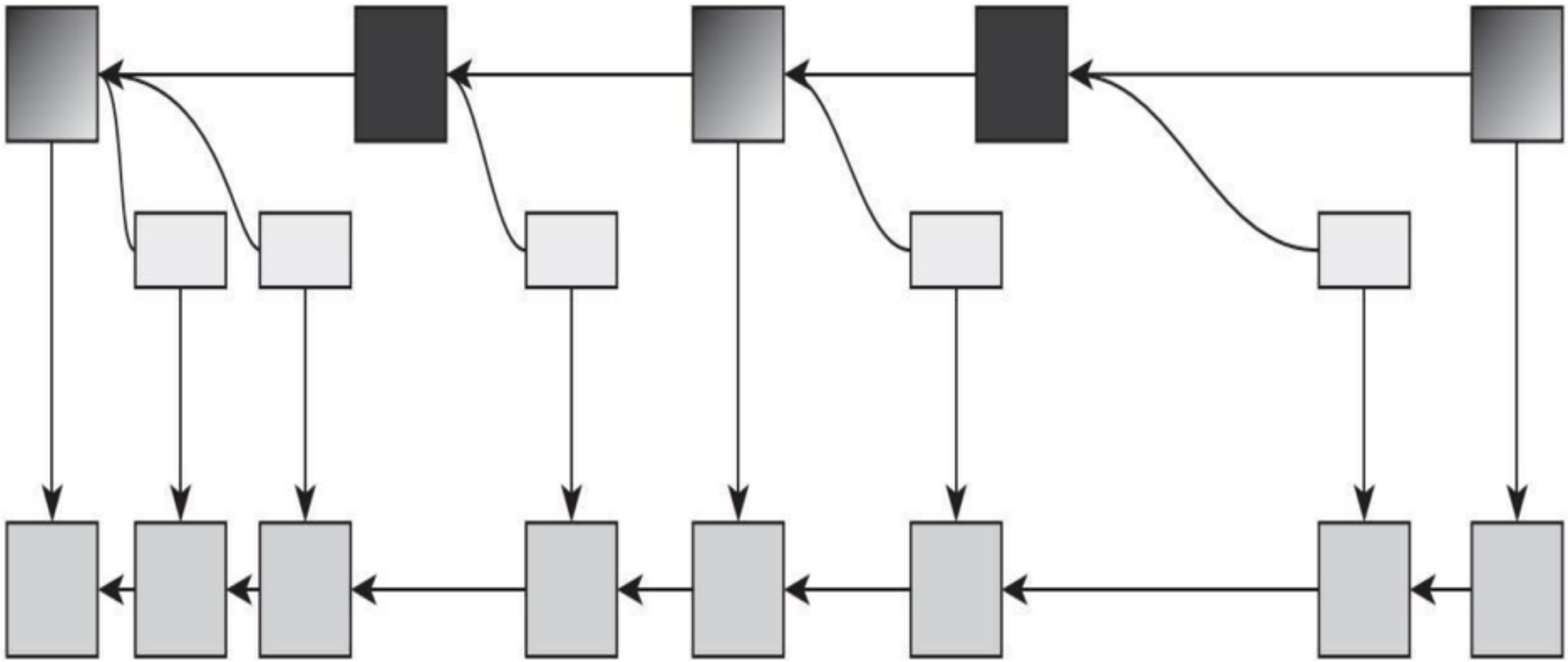
拉高出货

初始分配

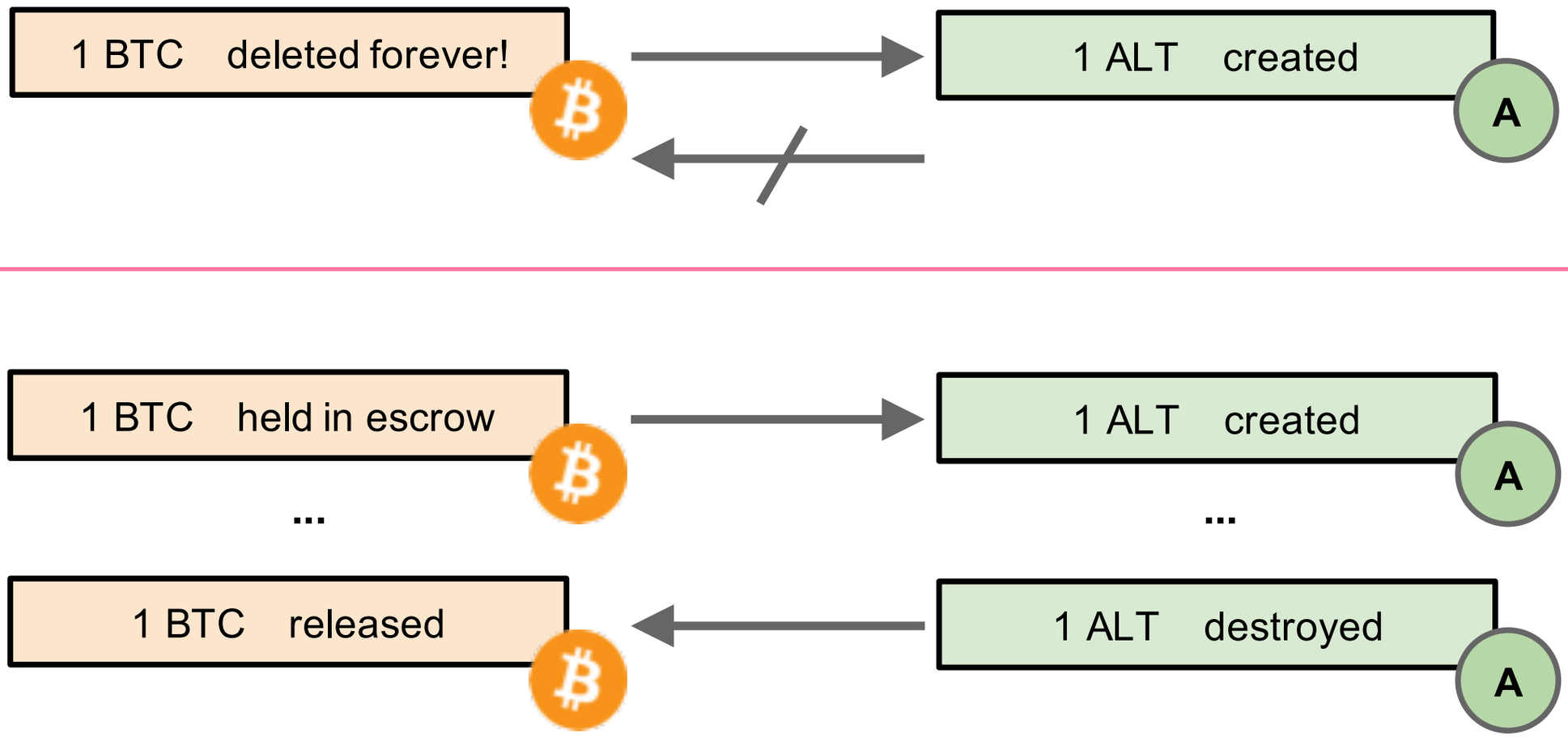
挖矿攻击

共同挖矿

共同挖矿



侧链


1 BTC deleted forever!
1 ALT created
A
1 BTC held in escrow
...
1 ALT created
A
1 BTC released
1 ALT destroyed
...
A


00001010
00000010
00001110
00000110

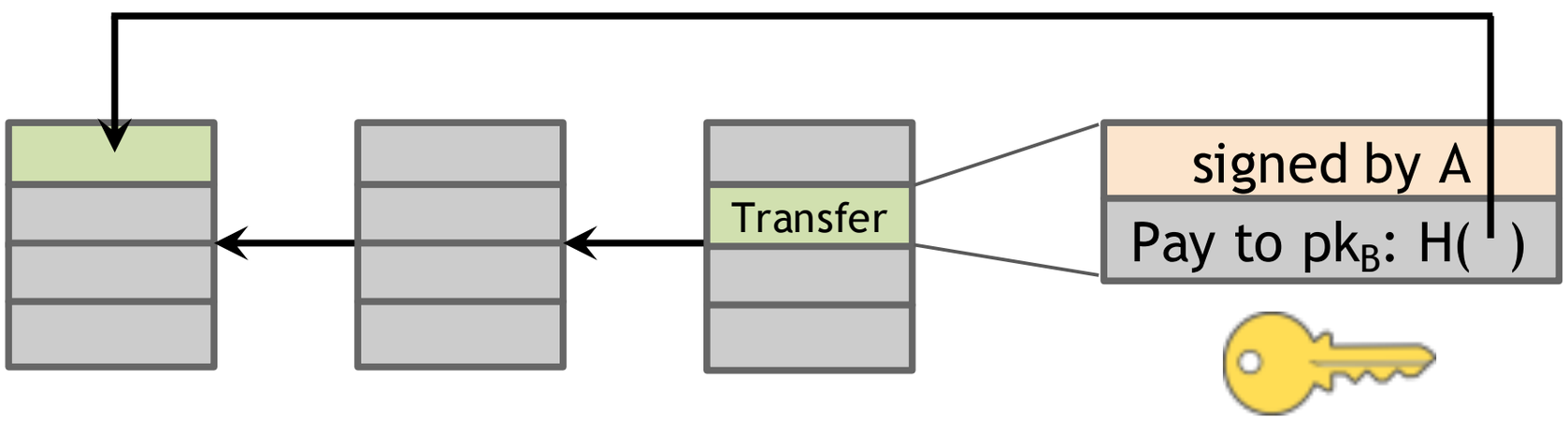
更多的链正在路上

ethereum

HYPERLEDGER

比特币未来

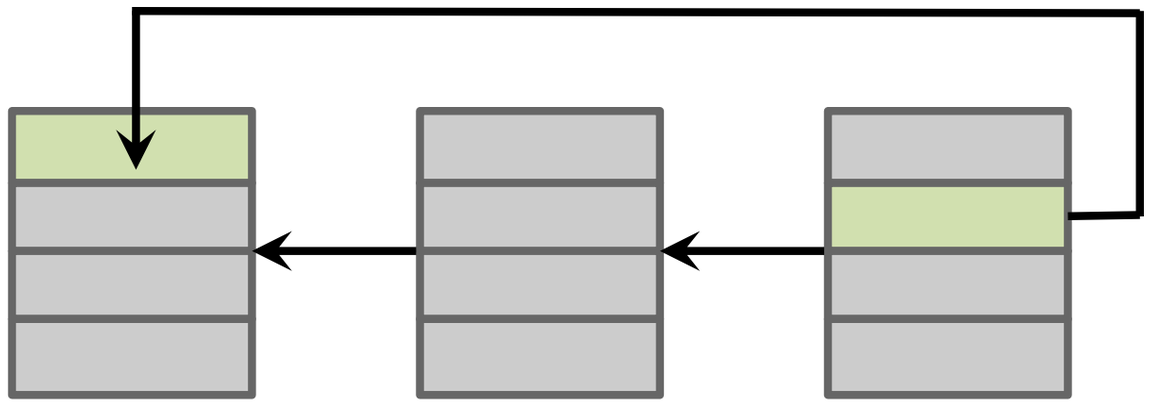
去中心化工具

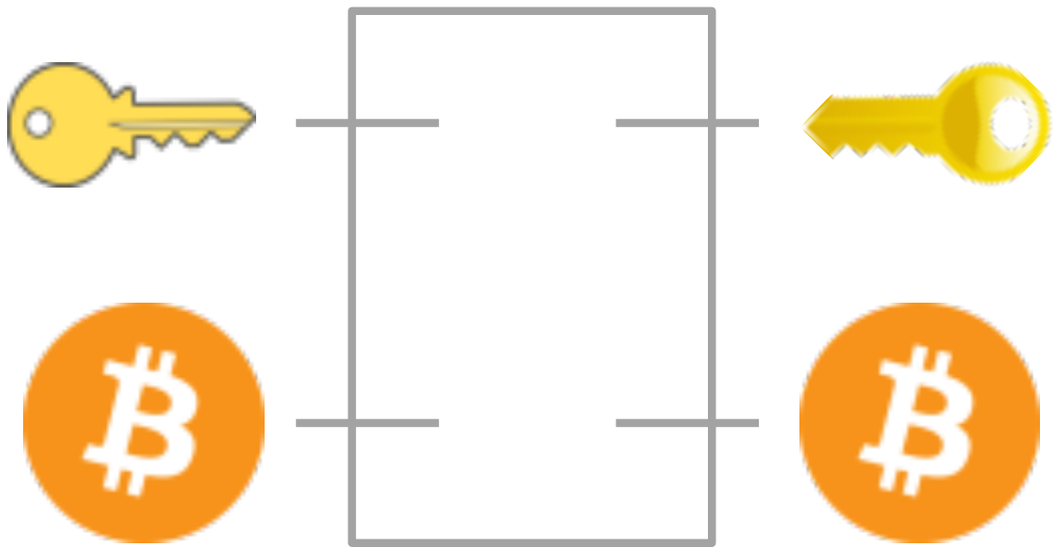


Now Bob's key activates car

智能资产

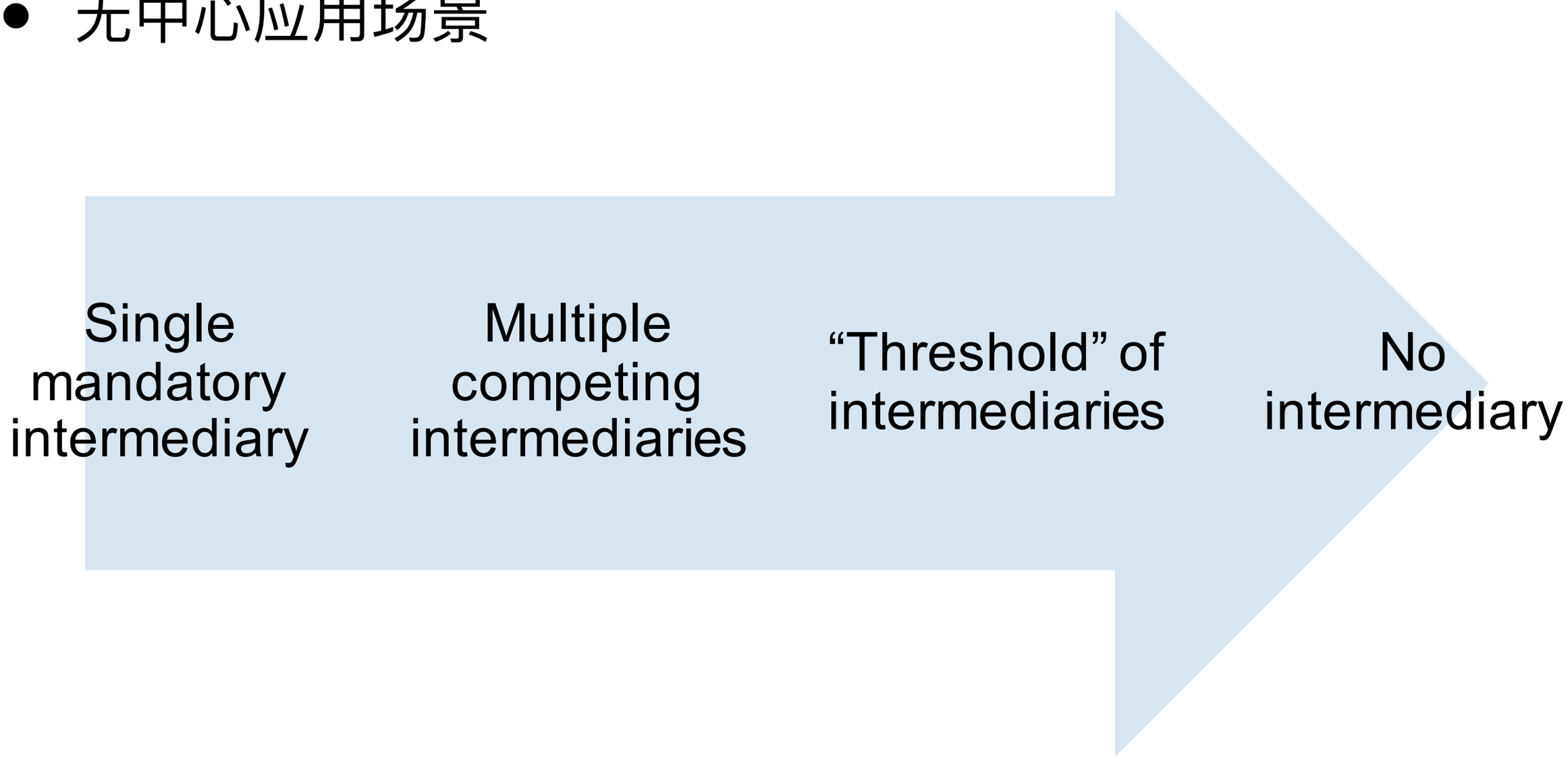

STATE OF CALIFORNIA
CERTIFICATE OF TITLE
AUTOMOBILE
1997 CHRY
03/08/2007
AN 2006 MR
04/02/06
03/01/2006
ACTUAL MILEAGE
Name and address of owner(s) appear here
Today's date
X Write owner's signature here.
X If the title list's 2 owners, the second owner signs here.
Odometer reading here
I certify under penalty of perjury under the laws of the State of California that the foregoing is true and correct.
Today's date
X Owner's signature here
Do not write in these spaces. Leave them blank.
Do not write in these spaces. Leave them blank.
IMPORTANT READ CAREFULLY
If a lien holder is listed here, an original of the Lien Release letter from the lien company will be required for title processing.
X Do not sign here.
CA 9444
VOID WITHOUT BEAR WATERMARK, HOLD TO LIGHT TO VIEW





去中心

- 中心化机构
- 多中心应用场景
- 无中心应用场景



谢谢！

孙惠平

sunhp@ss.pku.edu.cn