区块链与隐私保护

张方国

中山大学数据科学与计算机学院

E-mail: isszhfg@mail.sysu.edu.cn

2018.06.09，华东师大

主要内容

一 隐私性与区块链的兴起

二 区块链中的隐私保护

用户身份隐私保护技术　　数据隐私保护技术

三 利用区块链技术实现隐私保护

数据隐私；隐蔽通信。。。

四 结束语

隐私

- 隐私，顾名思义，隐蔽、不公开的私事。
- 隐私的种类：
  个人事务、个人信息、个人领域。
- 隐私权是指自然人享有的私人生活安宁与私人信息秘密依法受到保护，不被他人非法侵扰、知悉、收集、利用和公开的一种人格权，而且权利主体对他人在何种程度上可以介入自己的私生活，对自己是否向他人公开隐私以及公开的范围和程度等具有决定权。

隐私泄露问题日趋严重!

Facebook数据泄露

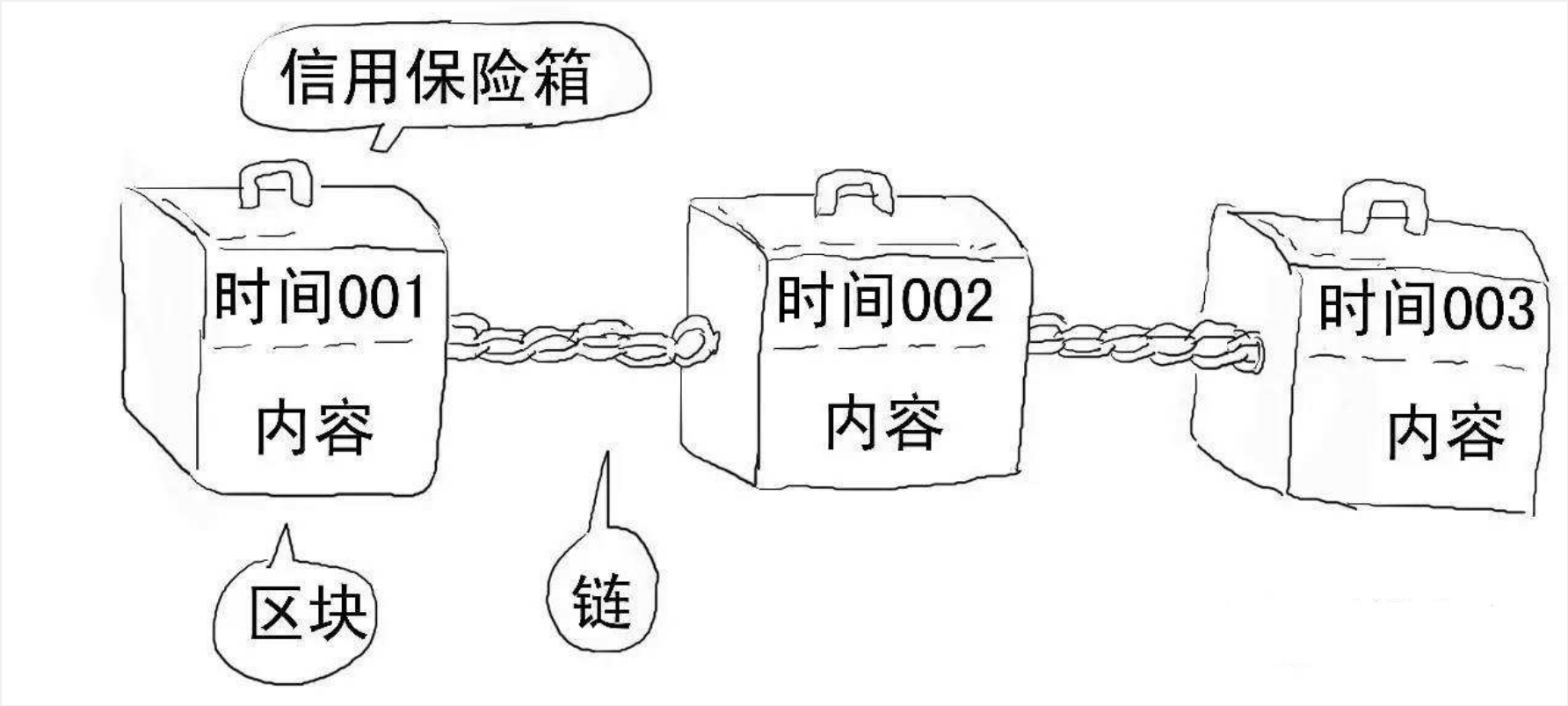
美总统大选邮件门

隐私泄露不只要钱，还能要命！

12306用户信息外泄

区块链的兴起

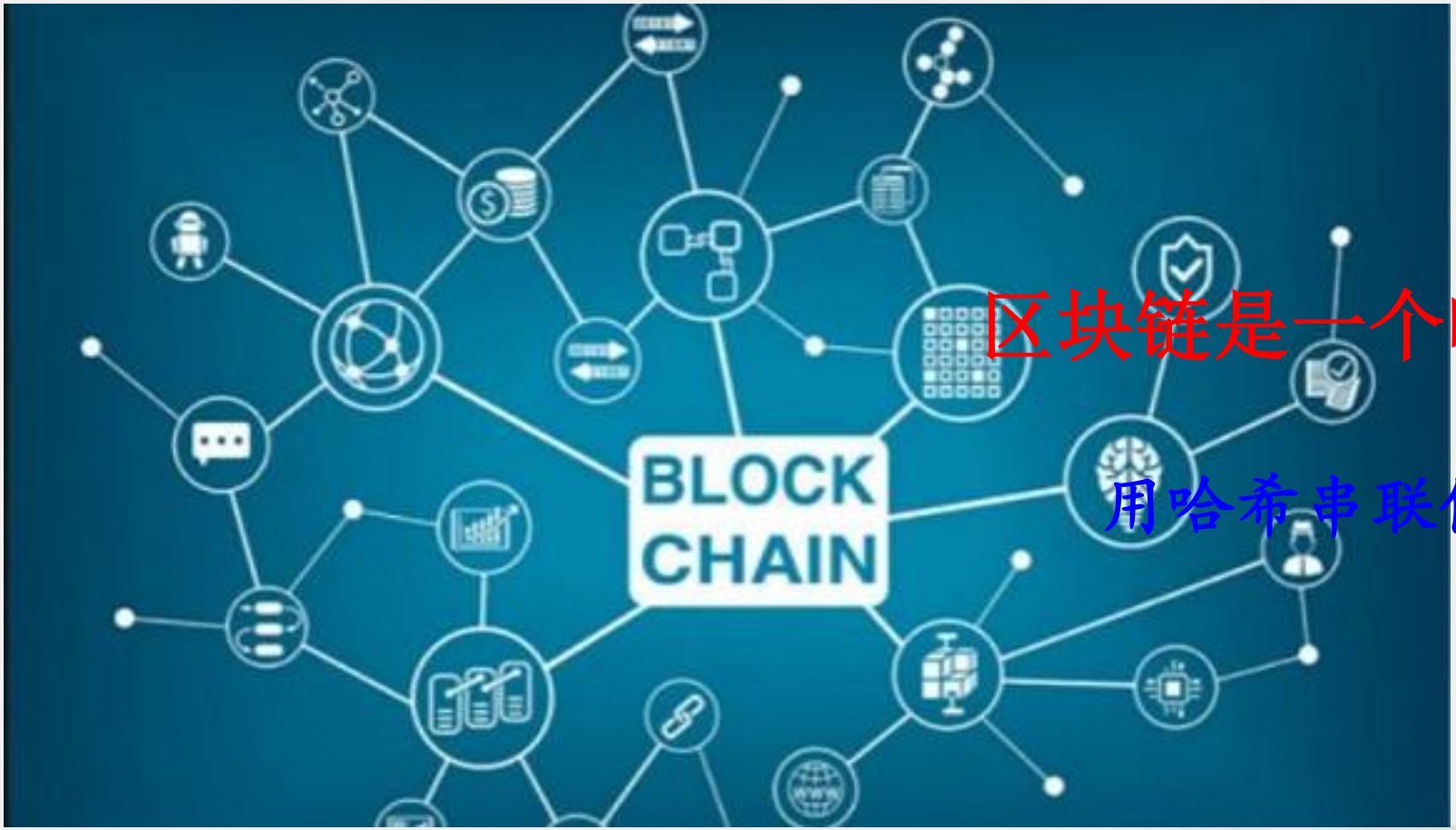
区块链是为了信任！



区块链还可以提供隐私保护！！！

什么是区块链?

- 区块链是比特币的底层技术，先比特币，后区块链

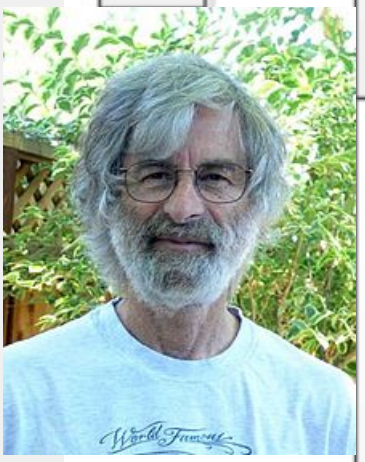


区块链是一个哈希链

用哈希串联信息

区块链就变成了这样！

DAG



区块头

前一区块 Hash

时间戳

随机数

POW

目标Hash

Merkle根

区块体

Hash1234

Hash12

Hash34

Hash1

Hash2

Hash3

Hash4

D1

D2

D3

D4

前一区块

后一区块

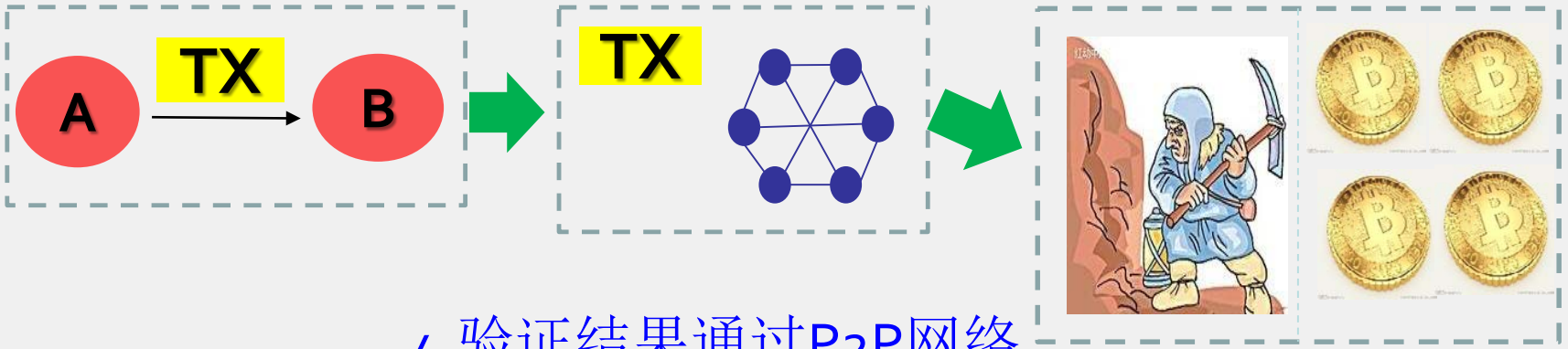
区块链的最早应用：密码货币

- 区块链就变成了**公开账本**!

1.新交易创建

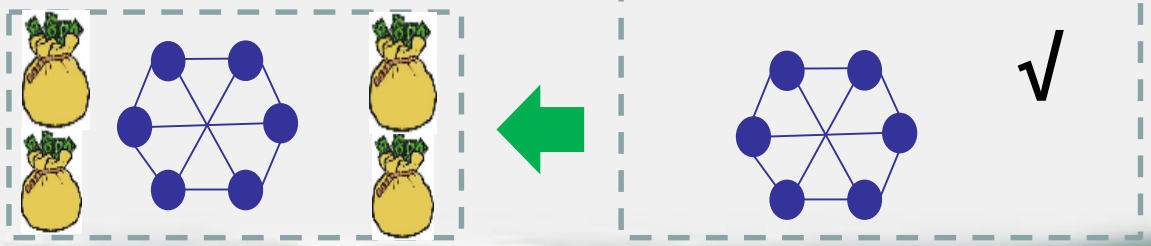
2.交易通过P2P网络传播

3. 交易验证



4.验证结果通过P2P网络传播

5.交易写入账本



区块链的各种新应用

- 替换第三方：审计、认证、仲裁等功能
- 防伪：公开可验证和不可篡改
- 智能合约：数据可编程
- 。。。

区块链就是分布式数据库
数据的多少决定块的大小，
数据的性质决定应用的领域

区块链隐私需求（密码货币）

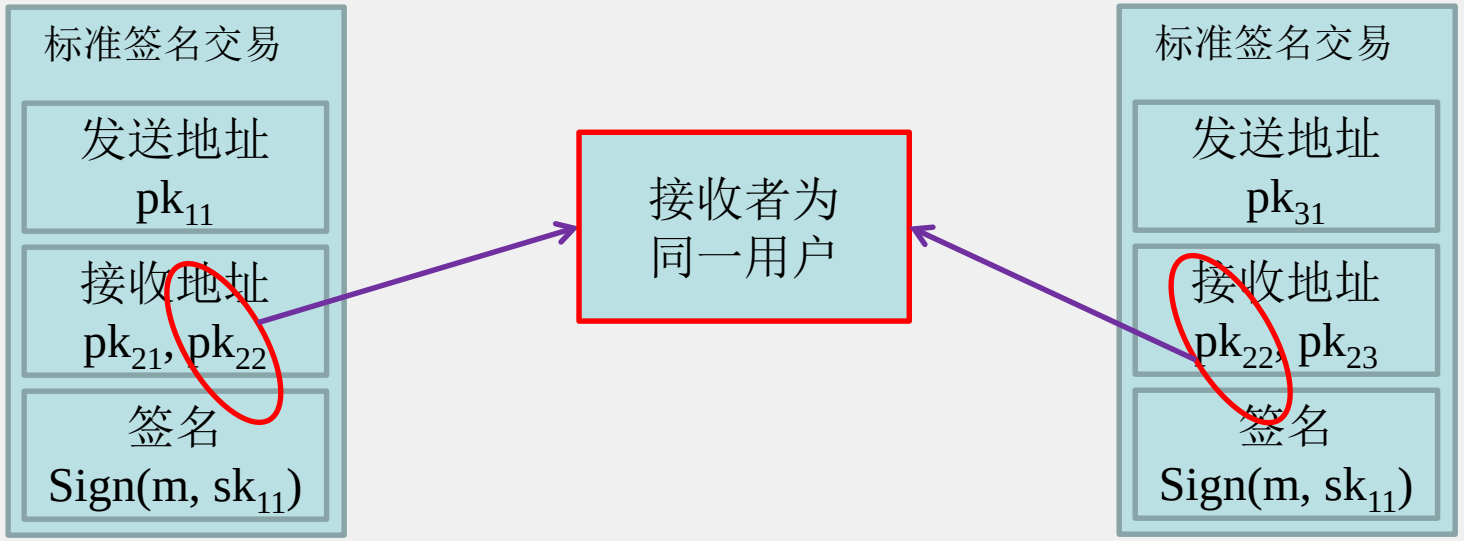
- **交易匿名性**
  - 对于任何交易，无法确认其发送方或接收方对应的真实身份
- **地址不可关联性**
  - 给定任意两个地址，无法判断其是否由统一个用户拥有
- **交易金额机密性**
  - 无法确定交易金额，仅能验证输入输出金额相等

发送者隐私保护（密码）

- **普通签名（纯假名）—— Bitcoin**
  - 已确认较弱的匿名性[OKJ2013], [RS2013]
  - 开销小
- **环签名——Monero ,CryptNote**
  - 理论上中庸的匿名性
  - 开销中等
- **零知识证明——Zerocoin, Zerocash**
  - 理论上最强的匿名性
  - 最强的扩展能力
  - 开销最大

Bitcoin的接收者隐私

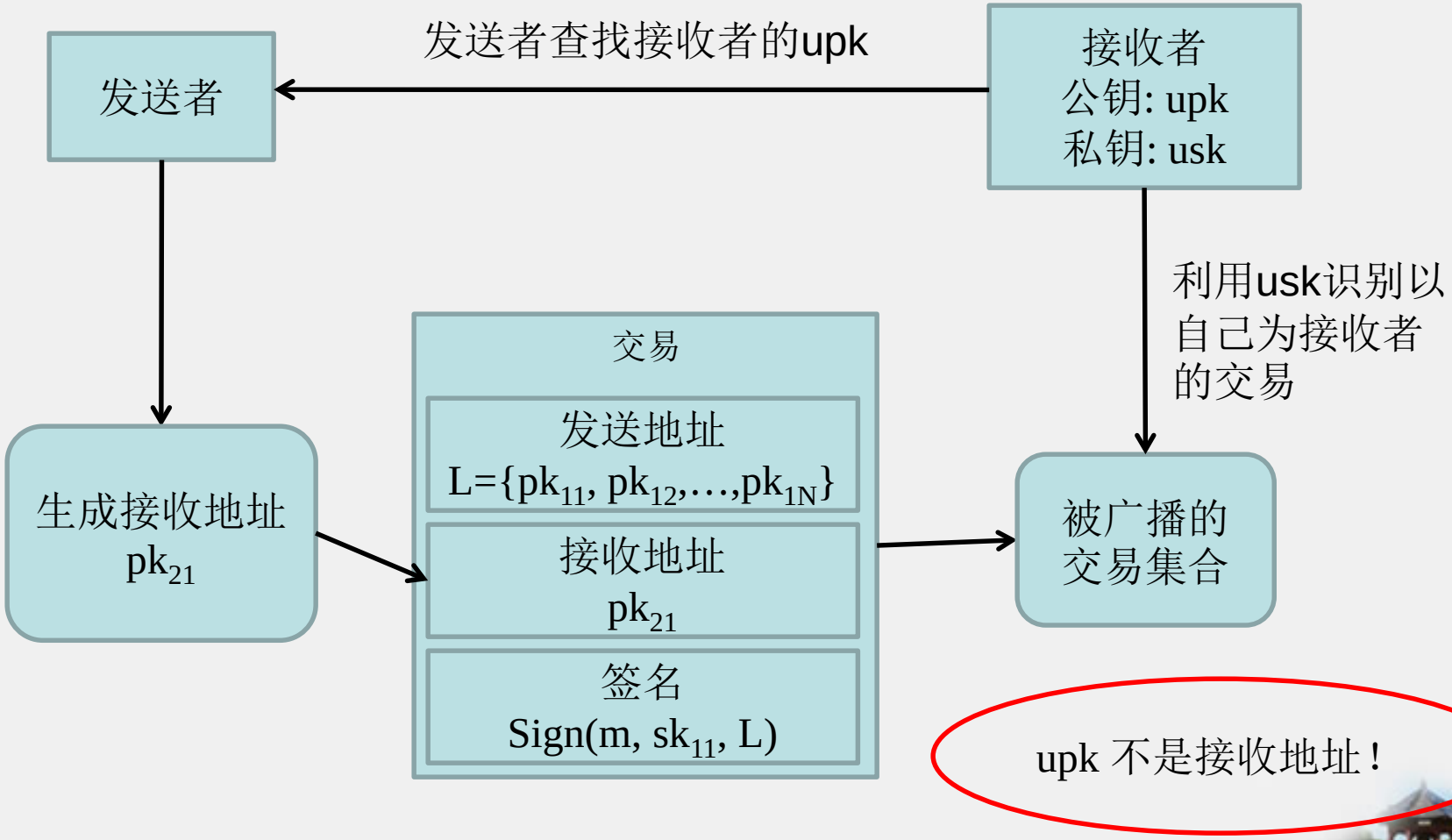
- 公开账本分析



- 解决思路
  - 不重复使用接收地址（隐蔽地址）
  - 不显式出现接收地址（零知识证明）

接收者隐私保护

- **隐蔽地址(Stealth addresses)**



数据隐私保护

- 隐藏交易金额
  - 不影响交易的合法与公平
- 秘密交易
  - Confidential Transaction [M2015]
  - RingCT [N2015]
  - RingCT 2.0 [SALY2017]
- 零知识证明
  - Zerocash
- （全）同态加密

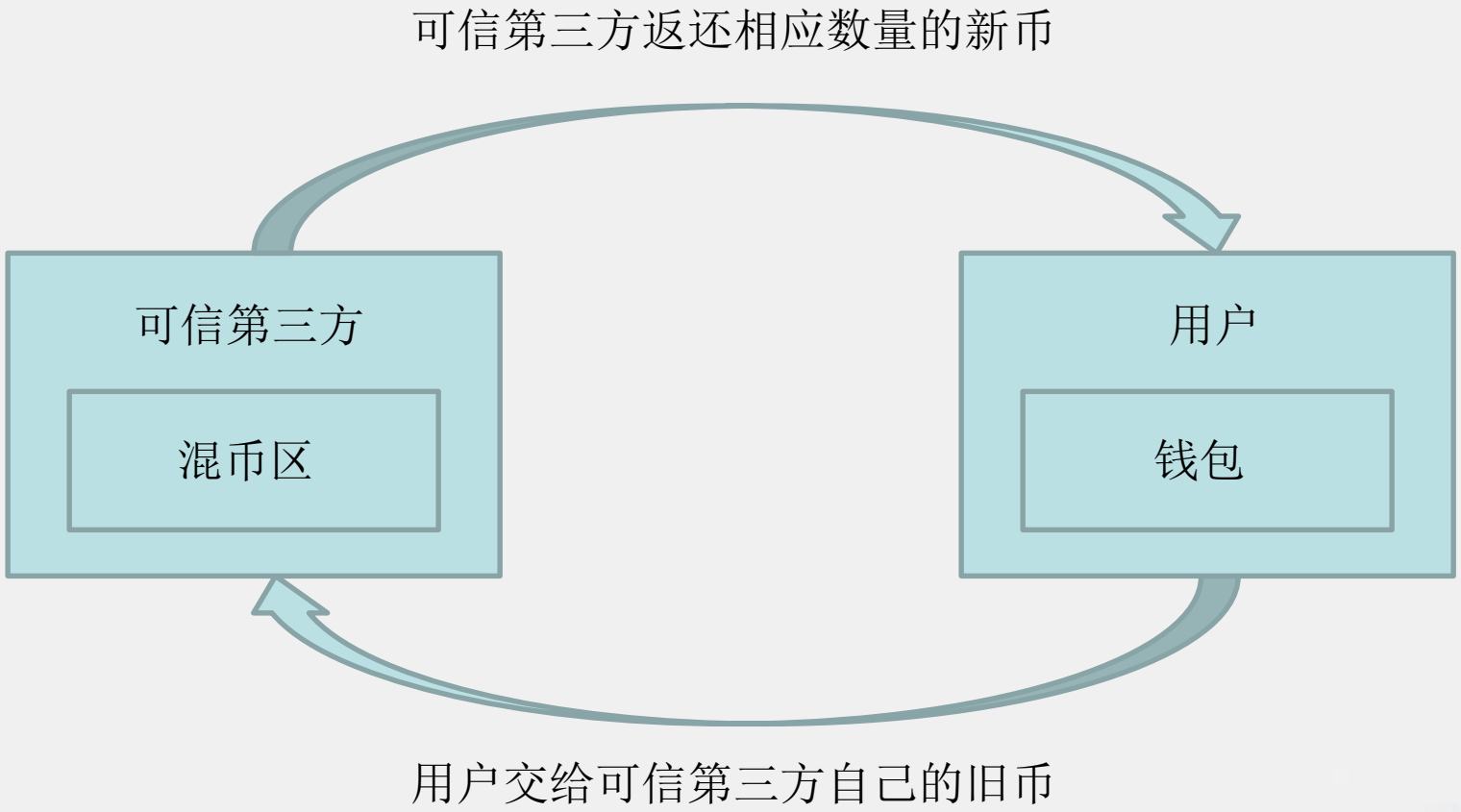
隐私保护手段（密码货币）

名称	可实现功能	缺点	代表应用
纯假名	发送、接收者匿名	最弱匿名性	Bitcoin
有中心混币	强化发送者匿名	中心	BitLaundry
环签名	发送者匿名	开销大，可扩展性差	CryptoNote, Monero
零知识证明	发送、接收者匿名，数据隐私	计算、存储开销大	Zerocoin, Zerocash
隐蔽地址	接收者匿名		CryptoNote, Monero
秘密交易	数据隐私		Bitcoin,Monero

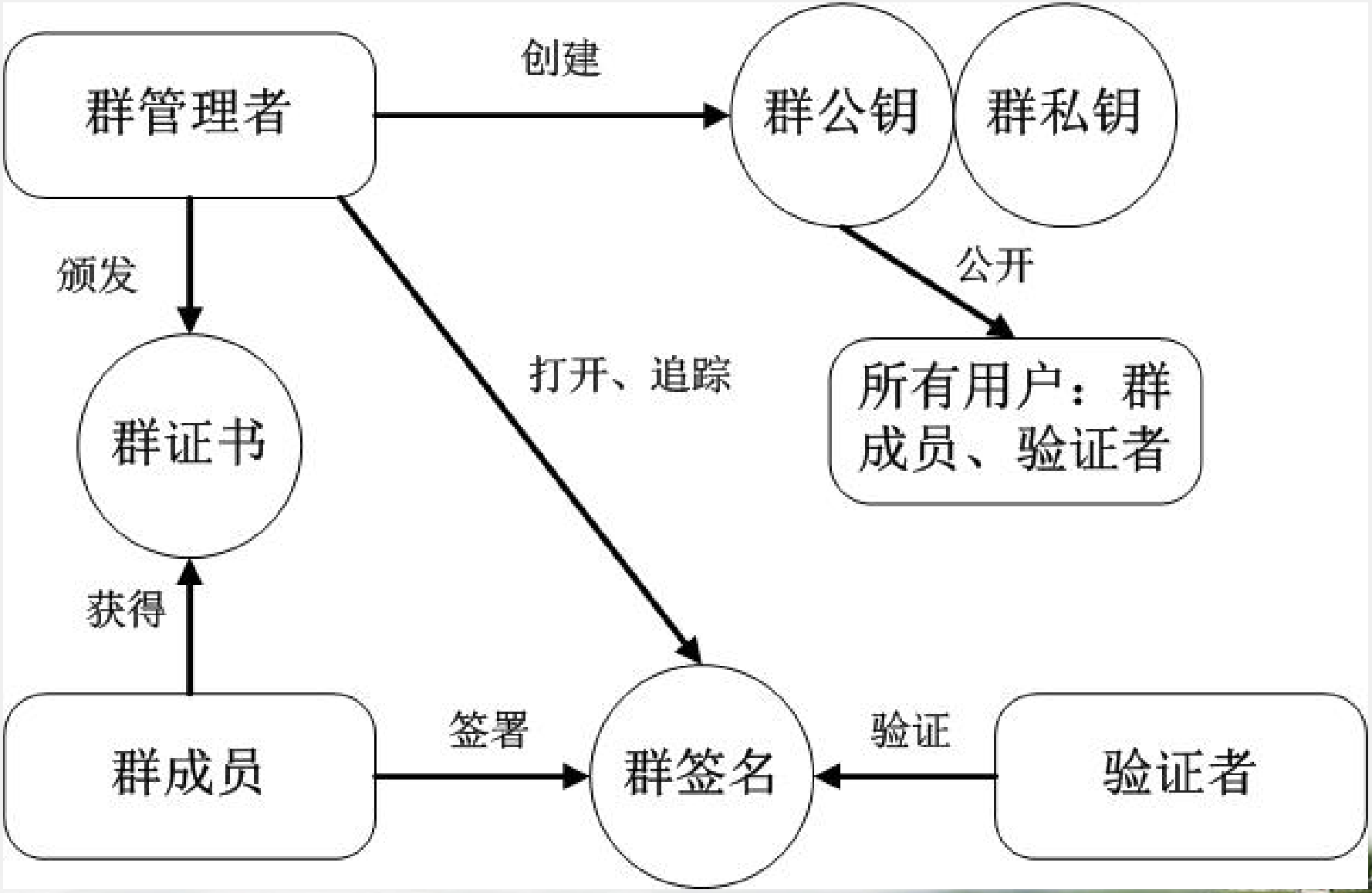
推荐阅读文献[LNW+2017]，以获取更全面的总结

发送者隐私保护（非密码）

- 中心混合、分发货币（Laundering）



可控隐私的实现–群签名



利用区块链技术实现隐私保护

- 实现数据隐私保护
  SSE

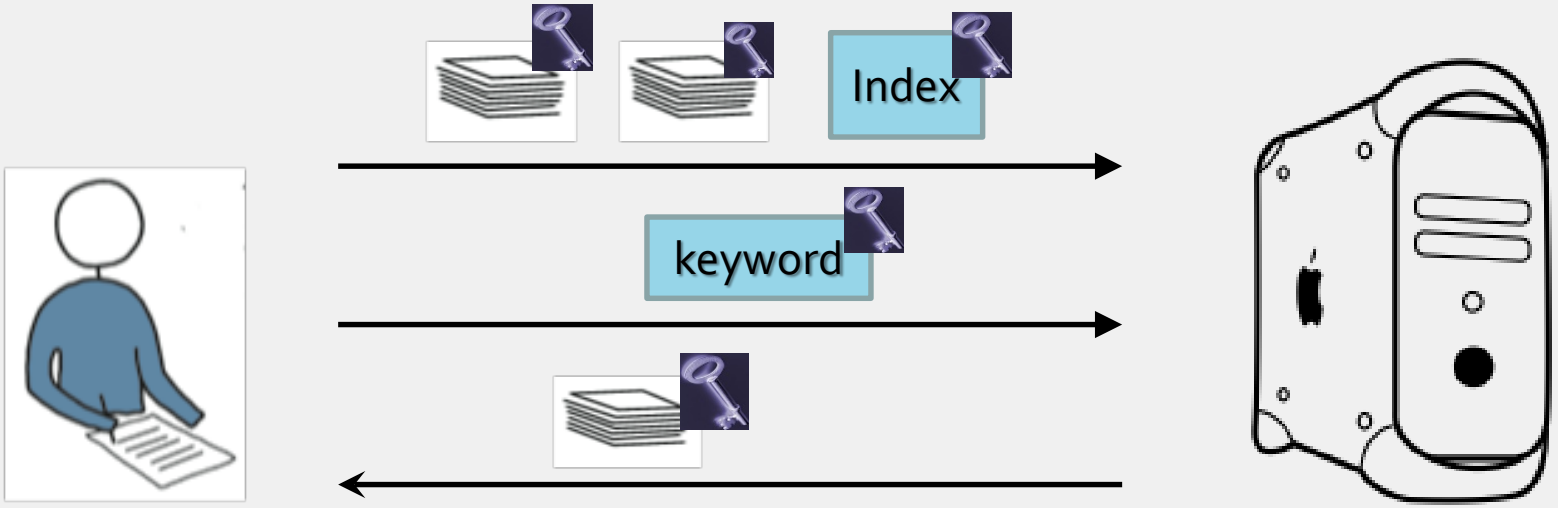
- 利用区块链实现隐蔽通信
  潜信道
  其他。。

数据加密

- 解决数据泄露的办法：对云端**数据加密**

加密后的数据如何搜索？

SSE（特别是基于索引的SSE）



利用区块链实现SSE

Data owner U

Share K

User U'

Receiver:S'
Sender: U
Embeded info:C_1
Value:d $
Transaction1

Receiver:S'
Sender: U
Embeded info:C_2
Value:d $
Transaction 2

,…,

Receiver:S'
Sender: U
Embeded info:C_n
Value:d $
Transaction n

Step 1

Step 2

Receiver:R
Sender: U
Embeded info:I
Value:d $
Transaction *Inx*

Block chain

Receiver:Q
Sender: *Q*
Embeded info:$\{Cij\}^{j=n}_{j=1}$,MAC($C_{i1}||C_{i2}||\cdots||C_{in}$)
Value:d $
Transaction s

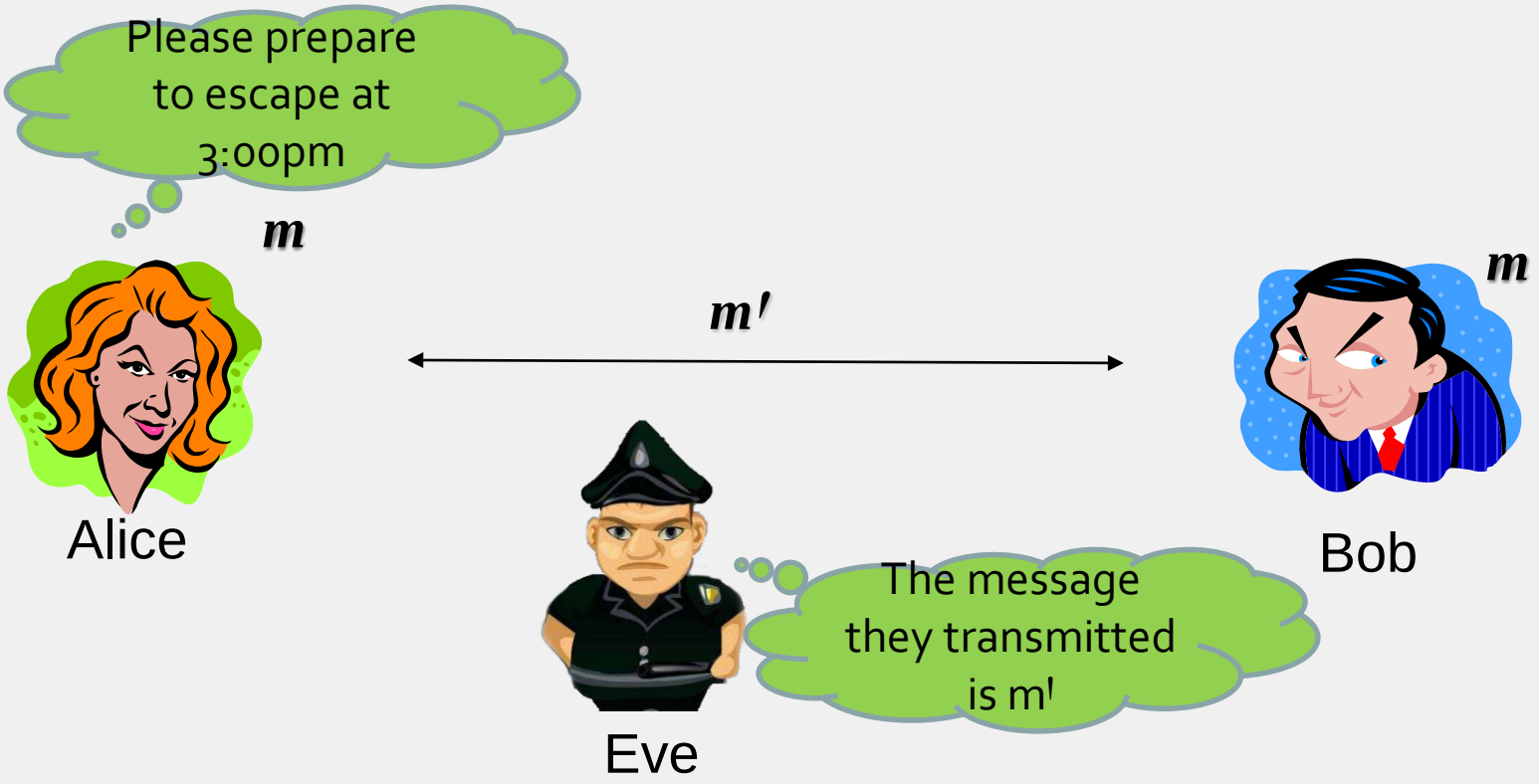
Step 4

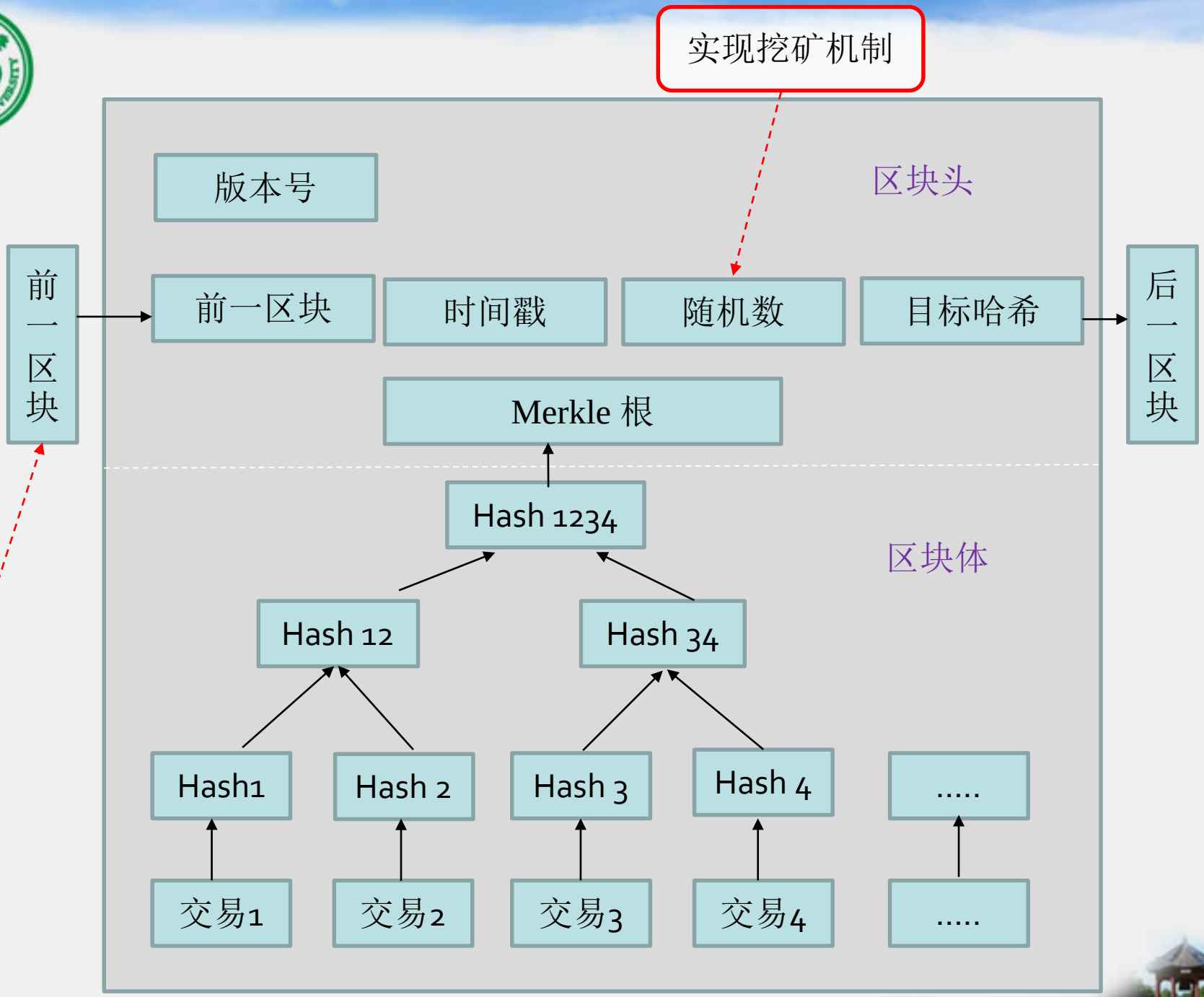
Step 3

Receiver:U' ∨ Q
Sender: U'
Embeded info: ϕ （*t(w),Inx*）
Value:d $
Transaction t

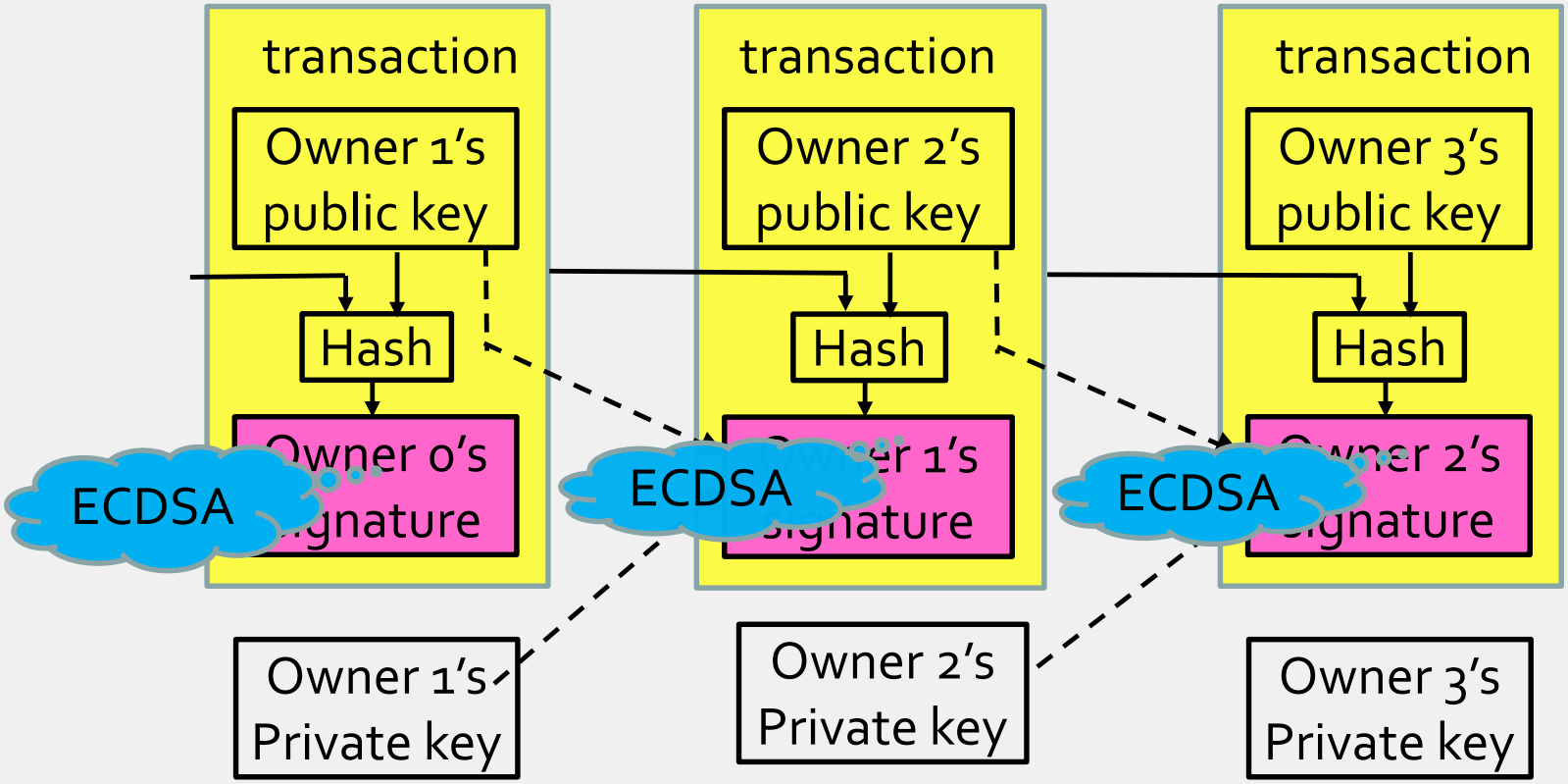
Huige Li, Fangguo Zhang, Jiejie He and Haibo Tian, A Searchable Symmetric Encryption Scheme using BlockChain, http://arxiv.org/abs/1711.01030

阈下信道的背景


Please prepare to escape at 3:00pm
m
Alice
m′
m
Bob
Eve
The message they transmitted is m′


实现挖矿机制
区块头
版本号
前一区块
时间戳
随机数
目标哈希
前一区块
后一区块
Merkle 根
区块体
Hash 1234
Hash 12
Hash 34
Hash1
Hash 2
Hash 3
Hash 4
.....
交易1
交易2
交易3
交易4
.....

基于签名算法的区块链系统下的阈下信道的构造



交易中使用的签名算法往往含有随机数，因此可以构建阈下信道

基于其它算法的区块链下的隐蔽信道

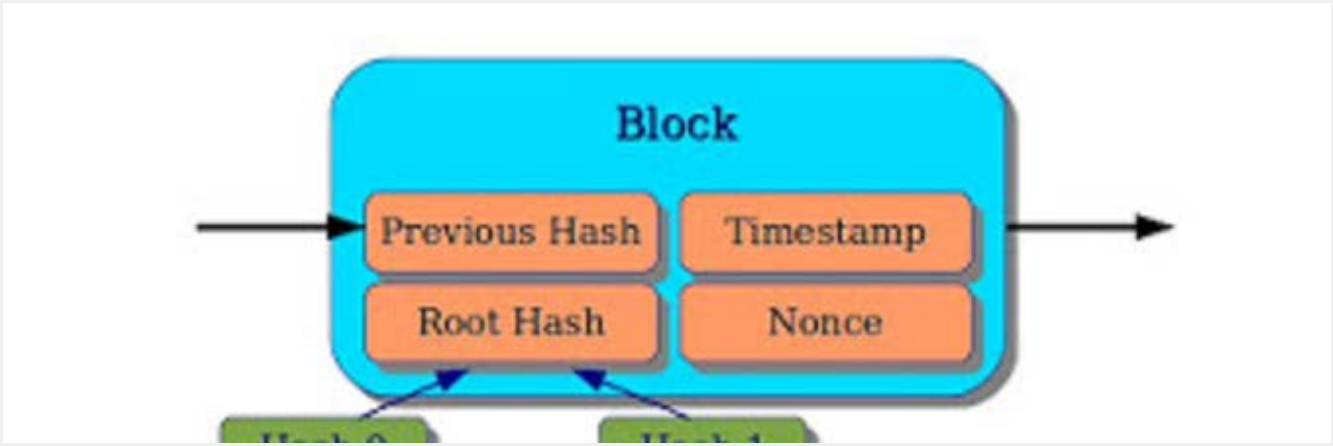
区块链系统可以使用其它的算法来保证电子货币的流通

- Zerocoin
- Zerocash

利用非交互式的零知识证明来保证电子密码货币的流通

R=AES_k(m||i), i=0,1,2…

区块链下的隐蔽信道



K

K

User U

User O

结束语

- 隐私泄露日益严重
- 区块链是哈希链
- 区块链中的隐私保护技术
- 利用区块链实现隐私保护

感谢您的聆听!