后量子区块链与密码货币

张方国

中山大学数据科学与计算机学院

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

主要内容

- 密码货币：从电子现金到比特币
- 量子计算到后量子区块链
- 公钥后量子签名代替传统签名
  1，格签名替换ECDSA
  2，基于格的可链接环签名的密码货币
- 纯哈希的抗量子账本
- 基于量子的抗量子账本
- 结束语

货币形态

实物货币

金属货币

纸币

货币是人类文明发展过程中的一大发明，最重要的职能包括价值尺度、流通手段、贮藏手段。

数字货币或电子货币

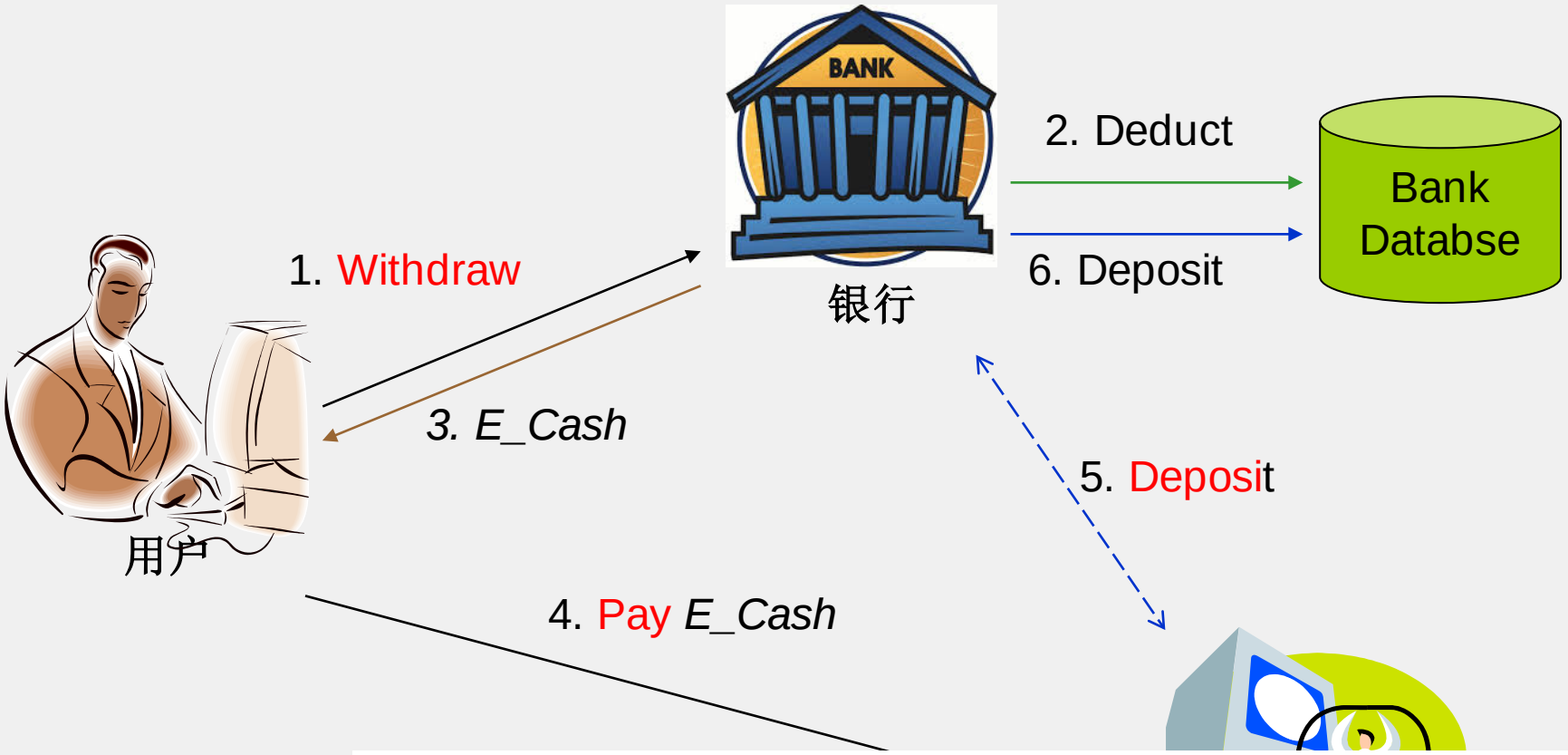
- 储值卡型
- 信用卡应用型
- 电子支票
- 电子钱包
- **电子（数字）现金**

David Chaum ecash

- 1983 年，David Chaum 最早提出 ecash
- 1989 年创建了 Digicash 公司；
- DigiCash公司位于阿姆斯特丹，1994年5月开发了E-Cash网上支付。

- ecash 系统是首个匿名化的数字密码货币

电子现金支付系统



借助盲签名技术

第 24 卷 第 5 期
2001 年 5 月

计 算 机 学 报
CHINESE J. COMPUTERS

Vol 24 No. 5
May 2001

多银行电子现金系统

张方国[1] 张福泰[2] 王育民[1]

Chaum's e-cash

- 匿名的（anonymous）
- 安全的(防伪造，没有重花no double-spending)
- 依赖于存在一个中心：银行或中心化的中介机构。
- 不具备可分性

…1999年，Chaum的公司破产

比特币

Bitcoin: A Peer-to-Peer Electronic Cash System

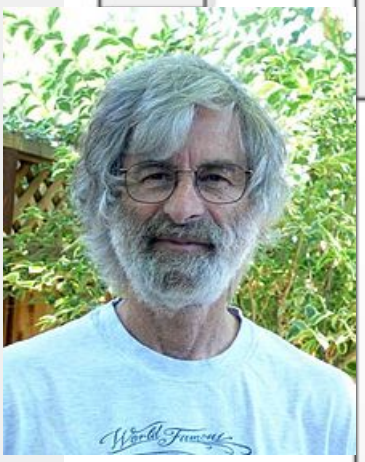
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

2008.
11.01

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.

- 2009年1月，创世区块诞生。
- 一种完全基于点对点（P2P）的电子现金系统，使得全部支付都可以由交易双方直接进行，完全摆脱了第三方，创造了一种全新的货币体系。

区块链！



区块头

前一区块 Hash

时间戳

随机数

目标Hash

POW

前一区块

后一区块

Merkle根

区块体

Hash1234

Hash12

Hash34

Hash1

Hash2

Hash3

Hash4

.....

D1

D2

D3

D4

.....

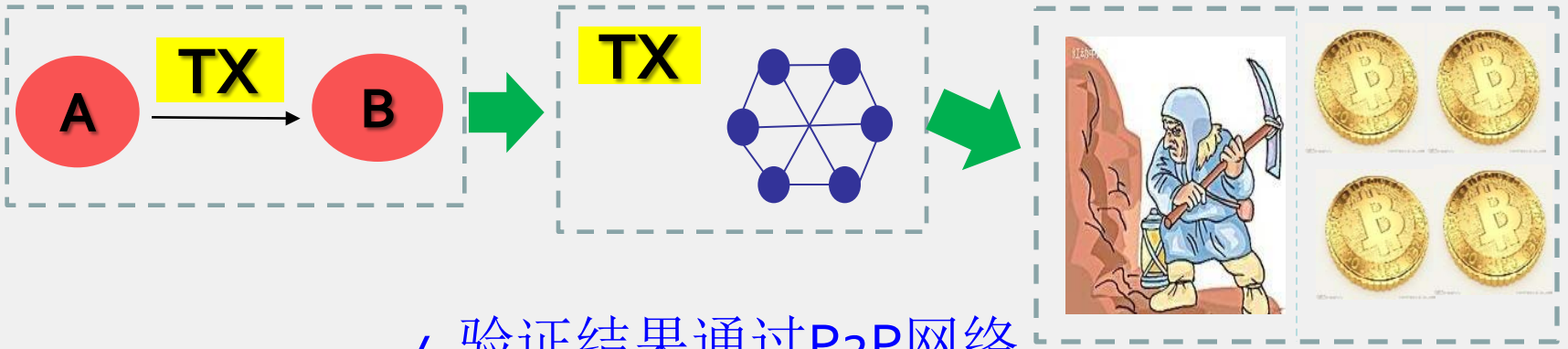
区块链的最早应用：密码货币

- 区块链就变成了**公开账本**!

1.新交易创建

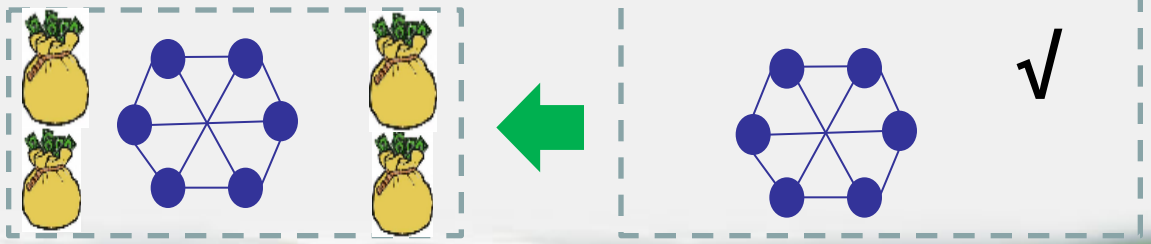
2.交易通过P2P网络传播

3. 交易验证



4.验证结果通过P2P网络传播

5.交易写入账本



一个具体的交易描述Tx

- 主要部分：版本号，输入，输出，锁定时间等

metadata

input(s)

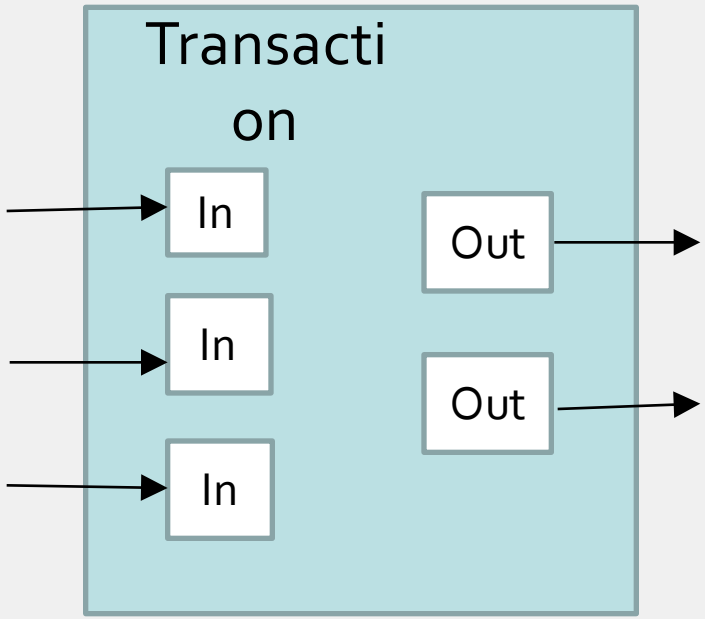
output(s)


```
{
  "hash":"5a42590fbe0a90ee8e8747244d6c84f0db1a3a24e8f1b95b10c9e050990b8b6b",
  "ver":1,
  "vin_sz":2,
  "vout_sz":1,
  "lock_time":0,
  "size":404,
  "in":[
   {
    "prev_out":{
     "hash":"3be4ac9728a0823cf5e2deb2e86fc0bd2aa503a91d307b42ba76117d79280260",
     "n":0
    },

      "scriptSig":"30440....3f3a4ce81"
   },
   {
    "prev_out":{
     "hash":"7508e6ab259b4df0fd5147bab0c949d81473db4518f81afc5c3f52f91ff6b34e",
     "n":0
    },
    "scriptSig":"304602210....3f3a4ce81"
   }
  ],
  "out":[
   {
    "value":"10.12287097",
    "scriptPubKey":"OP_DUP OP_HASH160 69e02e18b5705a05dd6b28ed517716c894b3d42e OP_EQUALVERIFY OP_CHECKSIG"
   }
  ]
}
```

UTXO交易模式

UTXO是未花费的交易输出，是比特币交易过程中的基本单位。



I. 每个交易可以有多个输入，但是输出值最多有两个。

II. 输出值中一个是用于付账，另一个是找零。

III. 创世区块和矿工产生区块所得的交易中没有输入值。

基于区块链的新密码货币（特别是比特币）为什么能活（火）？

- 匿名的（独立于钱包的假名系统）
- 安全的：
  - 不可伪造（数字签名不可伪造性+Hash的抗碰撞性）
  - 没有重花 (公共账本记录不可修改的交易历史)
- 有效的解决了可分性(找零)
- 不依赖于中心(银行或中心化的中介机构)

- 缺点：交易慢，扩容差！

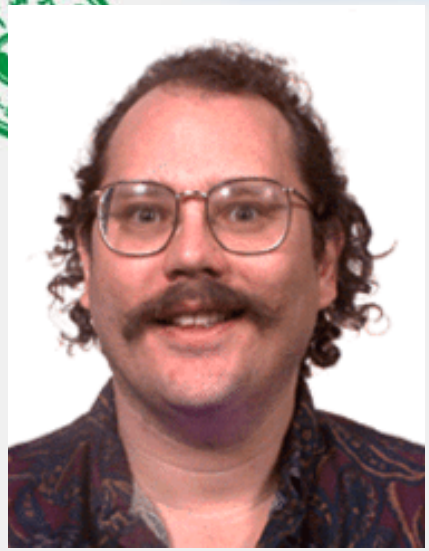
区块链的各种新应用

- 去中心化：替换第三方
- 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

量子计算到后量子区块链

- 量子算法与量子计算机
- P≠NP的假设
- 为什么需要后量子区块链和密码货币
- 候选的抗量子密码体制(非量子)



1994 Shor's algorithm: Factoring is easy with a quantum computer!

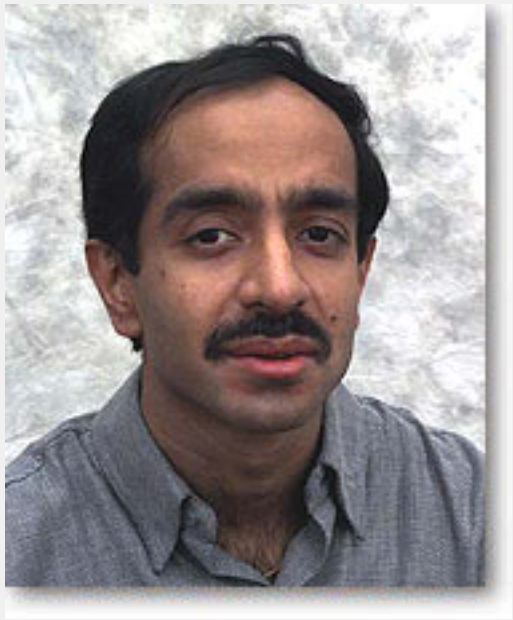
(Peter Shor)

1994年，Peter Shor的量子算法[S1994]：

- 多项式时间解决整数分解(IF)与离散对数(DLP)
- 关键技术，量子傅里叶变换

[S1994] Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring[C]//Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on. Ieee, 1994: 124-134.

Grover‘s Algorithm



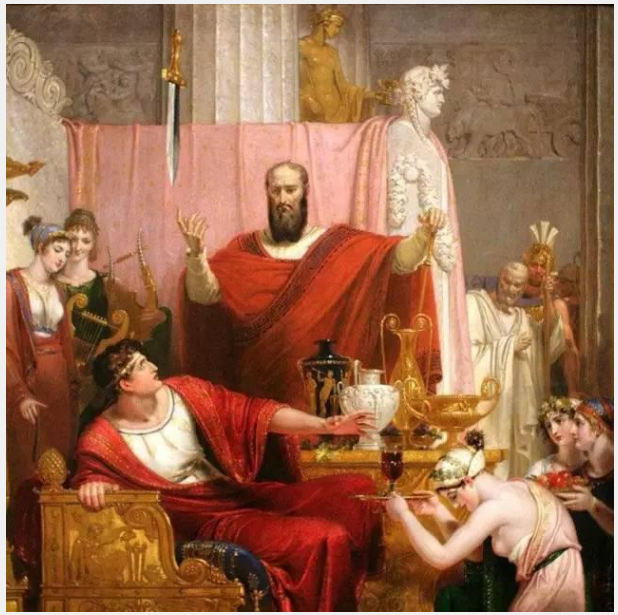
Lov Kumar Grover (born 1961)

1995年, 无序数据库的搜索算法

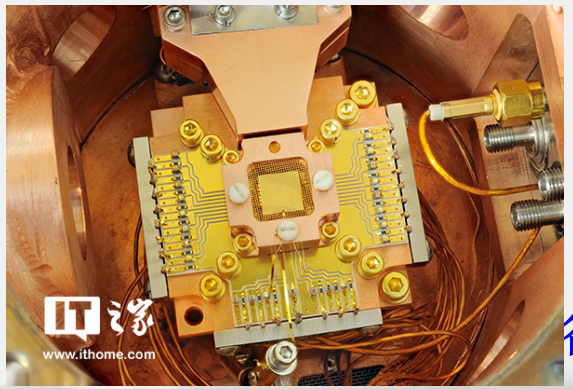
在O(sqrt(n))时间内搜索大小为n的数据库

256比特的AES的安全性变成了128比特级别

快速发展的量子计算机



- 区块链的达摩克里斯之剑
  - 悬顶之剑，超强的计算能力
  - 破坏密码方案的安全性
- 量子计算机的快速发展
  - Google, NASA与D-Wave合作
  - 阿里巴巴与中科院合作
  - 2012年之后，关键技术获得接连突破
  - ……



微软宣布在半导体和超导体材料组成的线缆中生成马约拉纳费米子

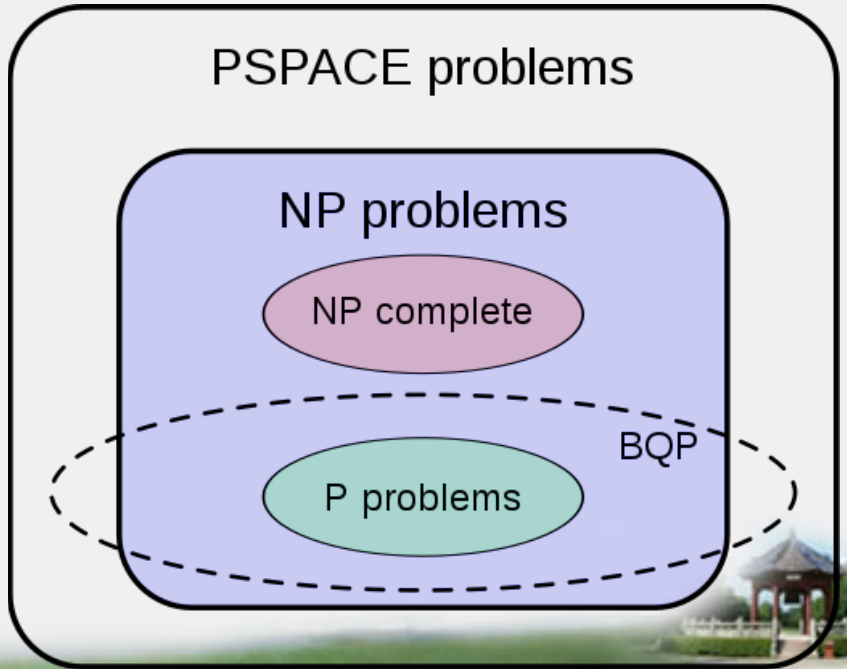
谷歌发布世界第一72位量子计算机芯片

P≠NP的假设

- 量子计算模型不一定等于非确定型图灵机
  - NP，非确定型图灵机多项式时间判定的判定性问题类
  - 普遍猜想BQP（“Bounded-error Quantum Polynomial time”）与NPC无交集

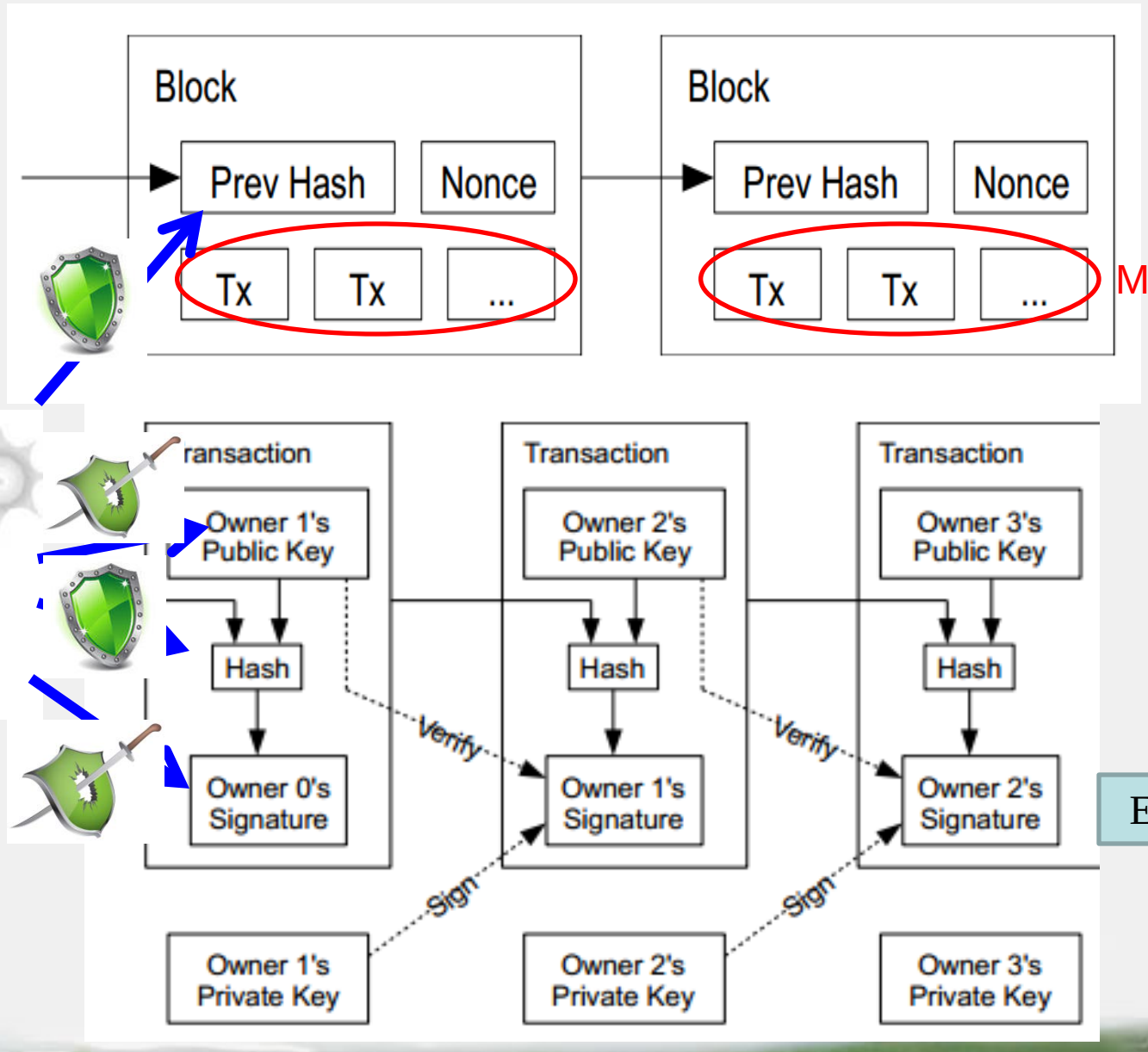
IF, DLP∈BQP

- 尚有大量计算困难问题可用于现代密码学



Cryptography is not over yet!

Why Post-quantum cryptocash?



National Institute of Standards and Technology

NISTIR 8105

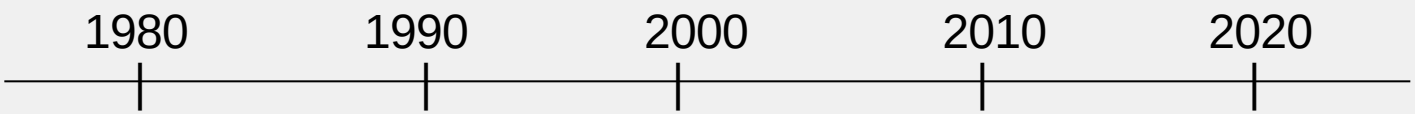
Report on Post-Quantum Cryptography

Lily Chen
Stephen Jordan
Yi-Kai Liu
Dustin Moody
Rene Peralta
Ray Perlner
Daniel Smith-Tone

基于Hash的密码
基于编码（纠错码）的密码(NPC)
基于格的密码(NPC)
基于多变量多项式的密码(NPC)
私钥加密，如AES
其他类：椭圆曲线同源密码，辫群等

2017.11.30，NIST后量子密码密码标准完成征集

公钥密码学的研究热点



RSA (整数分解问题)

ECC(短的密钥, 离散对数问题困难)

基于配对的密码体制(IBE)

后量子密码体制(格, 纠错码问题等)

后量子区块链和密码货币

- 对于区块链，如果是只考虑存储，或区块链只是用到了哈希函数，那么这是的区块链本身就是抗量子的了。
- 如果是考虑一些具体应用，如密码货币，就需要交易中所用到的签名也是要抗量子的。

  对于此类，就是把非后量子区块链中的签名方案替换成后量子签名！

公钥后量子签名代替传统签名

- 格签名替换ECDSA
- 基于格的可链接环签名

主要的后量子签名方案

- 基于格的
  - 1997 Goldreich Goldwasser Halevi
  - 2003 NTRUSign
  - 2008 Lyubashevski, Micciancio
  - 2013 BLISS(Bimodal Lattice Signature Scheme)
- 基于纠错码的
  - 2001 The CFS signature
  - 1997 The KKS signature
- 基于多变量的
- 基于椭圆曲线同源的
- 基于Hash的

Bitcoin→Post-quantum Bitcoin

- 任何有效的抗量子签名方案替换ECDSA

为什么选择格

格的ISIS与群的DLP的相似之处：

困难问题的形式
$\mathbf{Ay = b}$

$\|y\|<\delta$

困难问题的形式
$g^y = b$

Implementation	Security	Signature Size	SK Size	PK Size	Sign (ms)	Sign/s	Verify (ms)	Verify/s
BLISS-0	$\leqslant$ 60 bits	3.3 kb	1.5 kb	3.3 kb	0.241	4k	0.017	59k
BLISS-I	128 bits	5.6 kb	2 kb	7 kb	0.124	8k	0.030	33k
BLISS-II	128 bits	5 kb	2 kb	7 kb	0.480	2k	0.030	33k
BLISS-III	160 bits	6 kb	3 kb	7 kb	0.203	5k	0.031	32k
BLISS-IV	192 bits	6.5 kb	3 kb	7 kb	0.375	2.5k	0.032	31k
RSA 1024	72-80 bits	1 kb	1 kb	1 kb	0.167	6k	0.004	91k
RSA 2048	103-112 bits	2 kb	2 kb	2 kb	1.180	0.8k	0.038	27k
RSA 4096	$\geqslant$ 128 bits	4 kb	4 kb	4 kb	8.660	0.1k	0.138	7.5k
ECDSA[1] 160	80 bits	0.32 kb	0.16 kb	0.16 kb	0.058	17k	0.205	5k
ECDSA 256	128 bits	0.5 kb	0.25 kb	0.25 kb	0.106	9.5k	0.384	2.5k
ECDSA 384	192 bits	0.75 kb	0.37 kb	0.37 kb	0.195	5k	0.853	1k

Table 1. Benchmarking on a desktop computer (Intel Core i7 at 3.4Ghz, 32GB RAM) with `openssl` 1.0.1c

格签名替换ECDSA

Lyubashevsky格签名

私钥: **S**

公钥: **A, b=AS**

Sign:
1. 随机选择 **y**←$D_{Z^m,\sigma}$
2. 计算 **c**←H(**Ay**, msg)
3. 计算 **z**←**Sc**+**y**
4. 以特定的概率输出签名(**z, c**)

Verify:
1. 验证 z的范数满足一定界限
2. **验证是否 c=H(Az-bc**, msg)

Schnorr签名

私钥: S

公钥: g, $b=g^S$

Sign:
1. 随机均匀地选择 y←Z_q
2. 计算 c←H(g^y, msg)
3. 计算 z←Sc+y mod q
4. 输出签名(z, c)

Verify:
验证是否 c=H(g^z,/b^c msg)

标准签名VS环签名

- Bitcoin——标准签名
  - 较弱的匿名性[OKJ2013], [RS2013]
  - 允许密钥对复用
- Monero——环签名
  - 较强的匿名性
  - 密钥对强制使用一次
  - 匿名性与效率此消彼长
- Zerocash——零知识证明
  - 最强的匿名性
  - 最弱的效率

Anonymous Post-Quantum Cryptocash

Huang Zhang[1,2], Fangguo Zhang[1,2] ⋆, Haibo Tian[1,2], and Man Ho Au[3]

[1] School of Data and Computer Science, Sun Yat-Sen University, Guangzhou 510006, China
[2] Guangdong Key Laboratory of Information Security, Guangzhou 510006, China
[3] Department of Computing, The Hong Kong Polytechnic University, Hong Kong, China

Abstract. In this pa
cryptocash protocol w
In order to achieve tha
is proposed. The size
the number of partici
system follows that of
the logarithmic size q
protocol is efficient an
verifying and signing
ly. With these techni
transactions are prote
ledger.

IFCA International Financial Cryptography Association

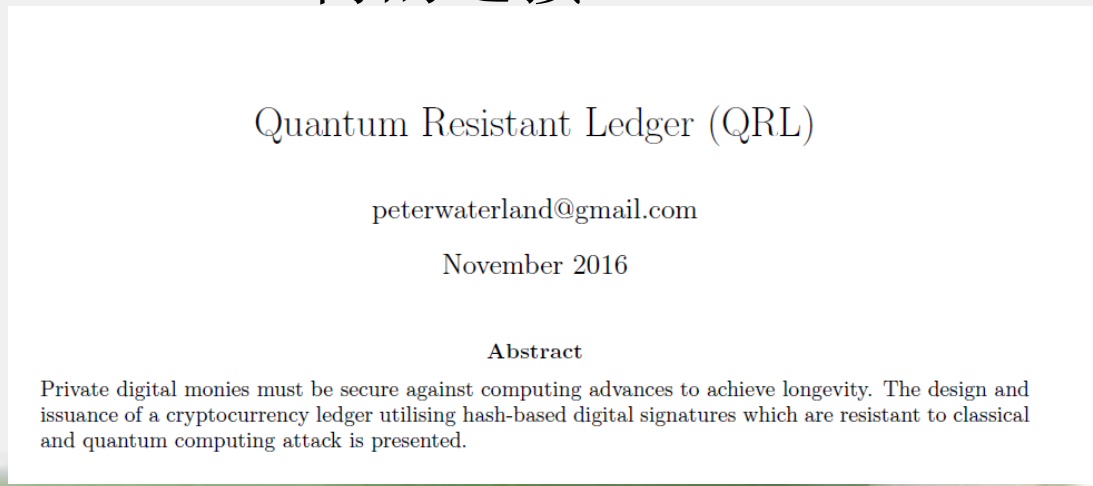
Financial Cryptography and Data Security 2018

Twenty-Second International Conference
February 26–March 2, 2018
Santa Barbara Beach Resort
Curaçao

Cryptology ePrint Archive: Report 2017/716

纯Hash的抗量子账本

- Lamport一次性签名(OTS)
- Winternitz一次性签名(OTS)
- Merkle签名(MSS)
- Hypertree：Merkle树的连接



Quantum Resistant Ledger (QRL)

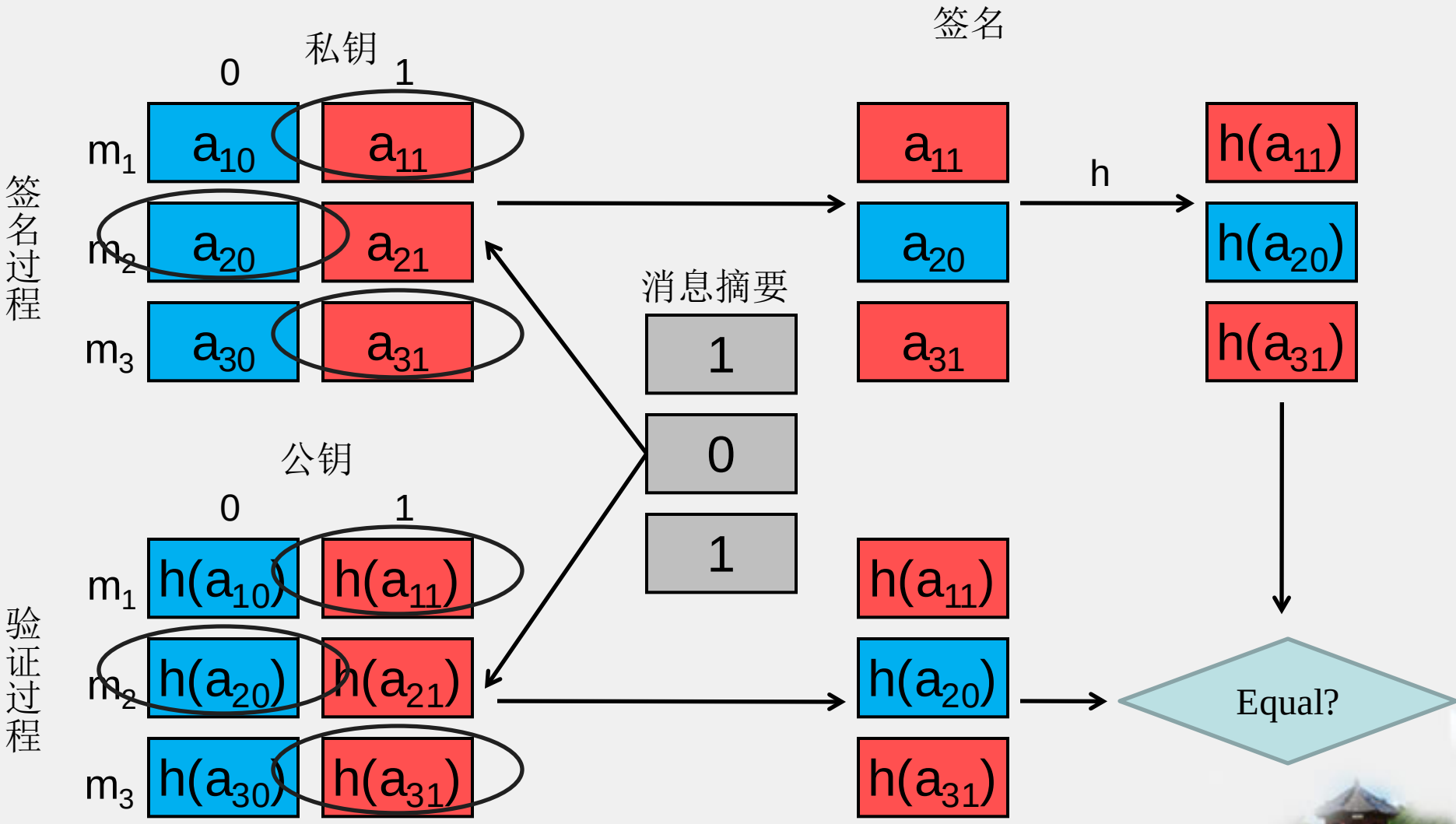
peterwaterland@gmail.com

November 2016

Abstract

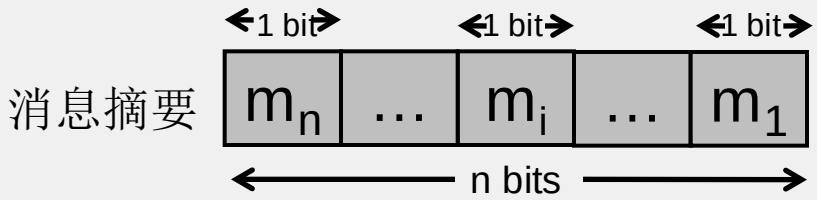
Private digital monies must be secure against computing advances to achieve longevity. The design and issuance of a cryptocurrency ledger utilising hash-based digital signatures which are resistant to classical and quantum computing attack is presented.

Lamport一次性签名(OTS)

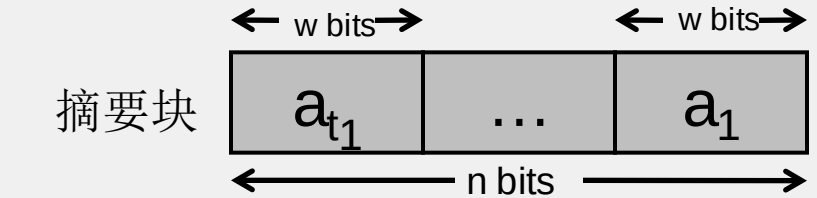


Winternitz一次性签名(OTS)

一次处理w个比特是降低签名尺寸的思路



补0再分块

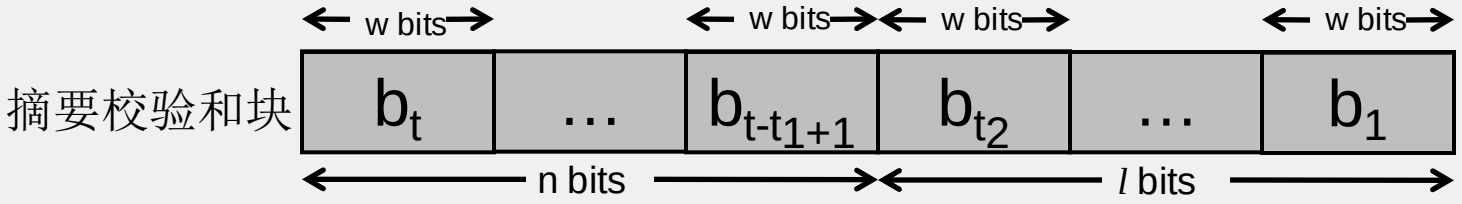


$$t_1 = \lceil n/w \rceil$$

计算摘要校验和

$$\text{校验和 } c = \sum_{i=1}^{t_1} \left(2^w - a_i\right) \le t_1 \cdot 2^w$$

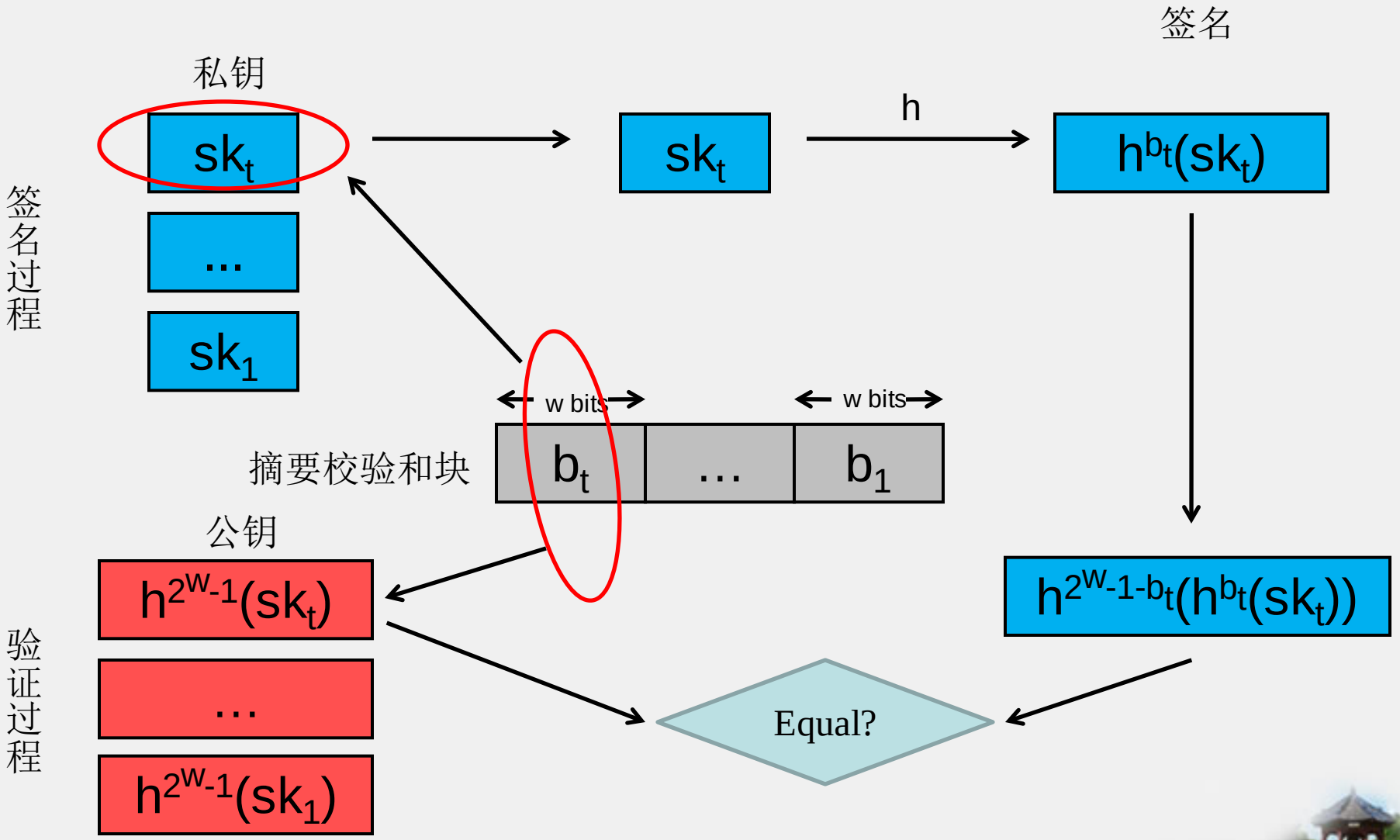
追加校验和的分块



$t = t_1 + t_2$

$$l = \lfloor \log_2 (t_1 \cdot 2^w) \rfloor + 1 = \lfloor \log_2 t_1 \rfloor + 1 + w \qquad t_2 = \lceil l/w \rceil$$

Winternitz一次性签名(OTS)



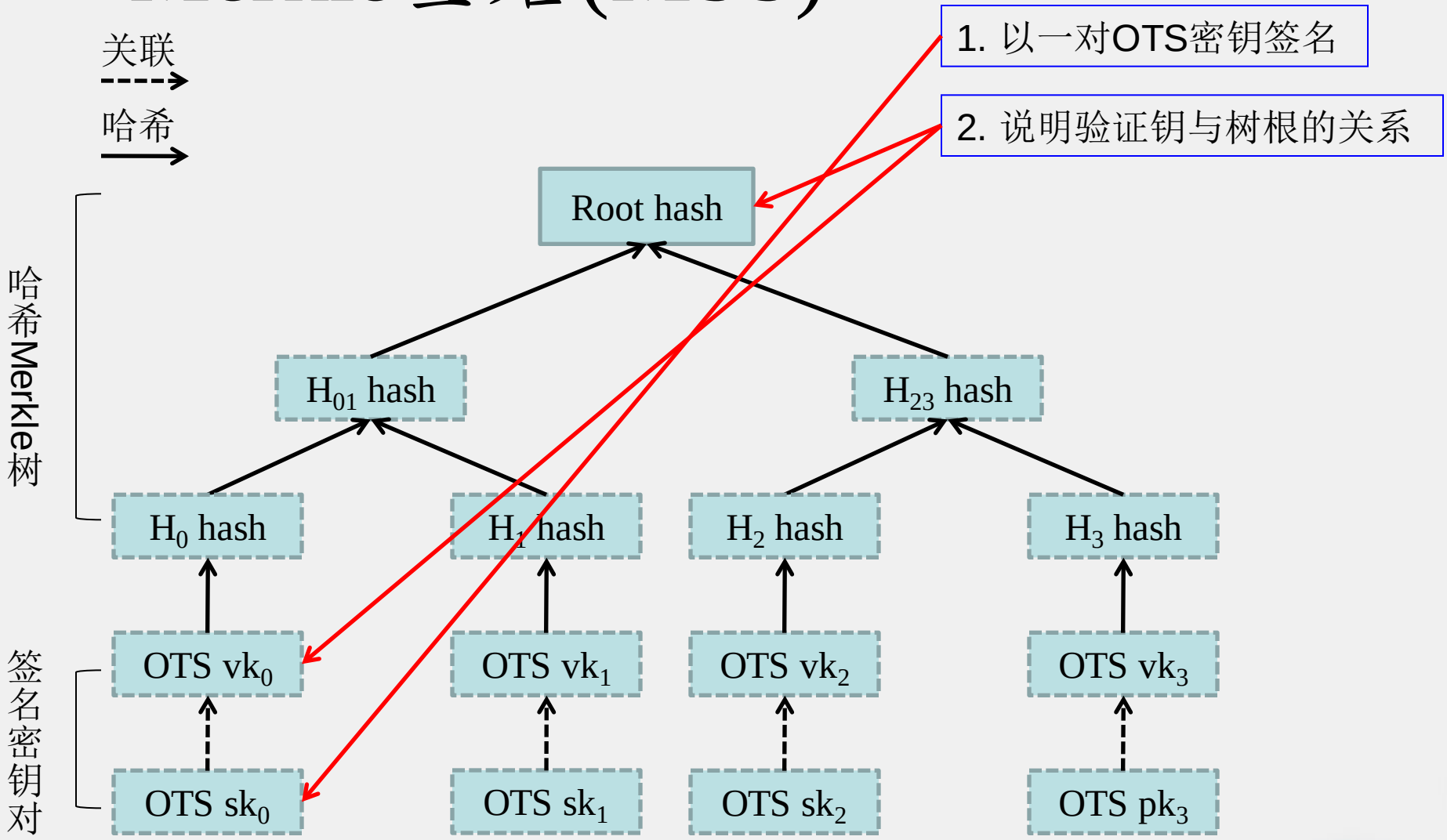
OTS的缺点

- 需要维护大量的密钥而不实用
  - 例如，银行对大量文件签名，用户验证文件需要寻找对应公钥
  - 例如，密码货币中以验证密钥（或其哈希函数值）作钱包地址。每次必须将钱包的钱全部转出
- 解决办法：统一公钥
  - 签名\验证密钥依然不能复用
  - 利用多个验证密钥生成一个统一的公钥
  - Merkle签名(MSS) [M1989]
  - 扩展的Merkle签名(XMSS) [BDH2011]

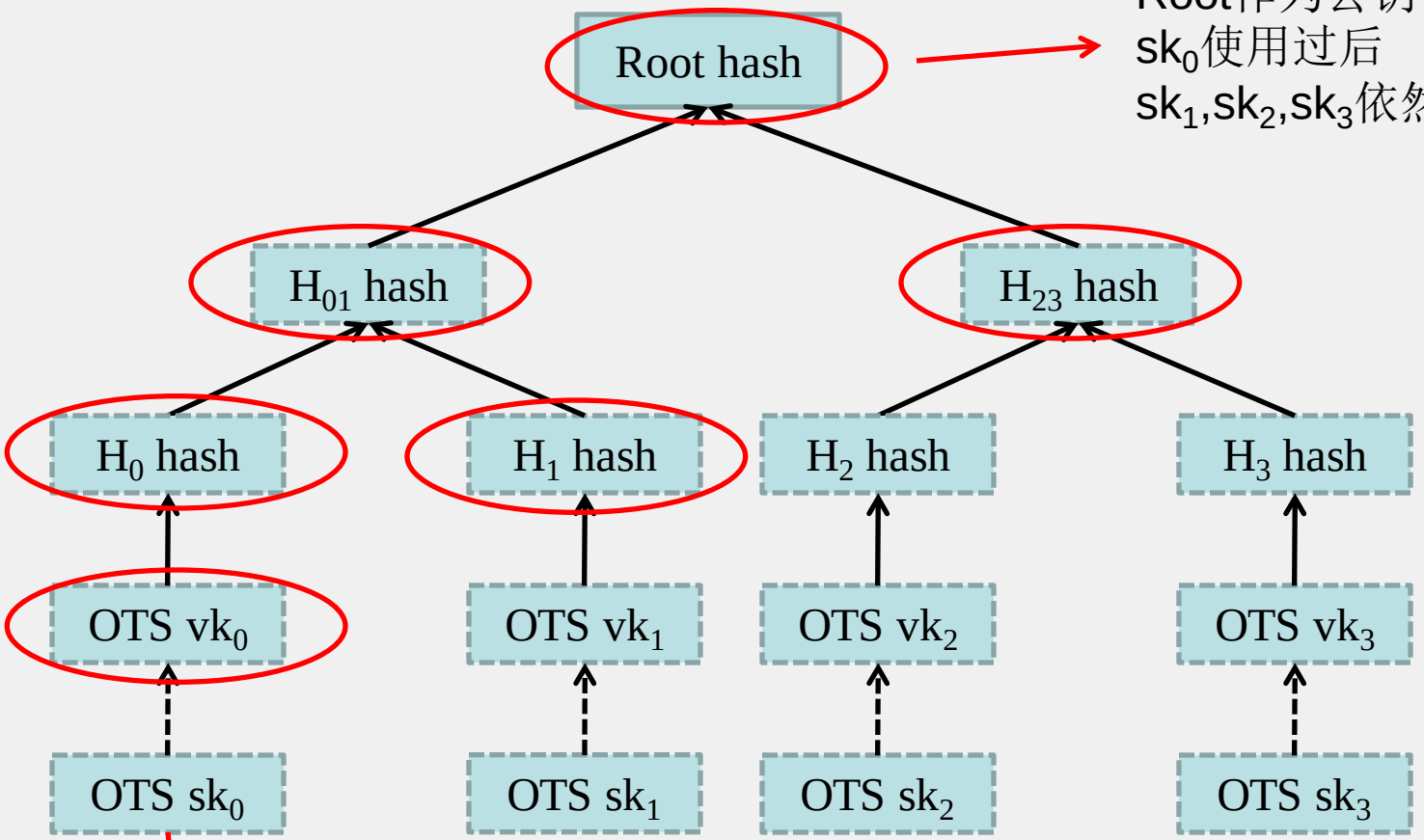
Merkle签名(MSS)

- 组合任意的抗碰撞哈希函数和OTS
  - 哈希函数用于构造Merkle树
  - OTS用于处理消息摘要
- 预先确定的Merkle树
  - 满二叉树
  - 叶子为OTS验证密钥的哈希值
  - 父节点是孩子结点的哈希值
  - 根节点为该用户的公钥
- 有限的签名次数（不同于ESCDSA等）
  - 若m是树的深度，最多签名2^m次(即叶子个数)

Merkle签名(MSS)



Merkle签名(MSS)



sk0的签名包含：{sign(m,sk0), s=0, vk0, ~~H0~~, H1, ~~H01~~, H23, Root}

由于H0，H01可由其它点算出

Merkle签名(MSS)

- Merkle签名是EU-CMA安全的
  - 如果构造Merkle树的哈希函数是抗碰撞的
  - 并且使用的OTS签名是EU-CMA安全的
- 扩展的Merkle签名(XMSS)
  - 亦是利用Merkle树，设计上与MSS大体相似
  - 孩子节点哈希成父节点前，分别与随机的bitmask异或
  - XMSS的EU-CMA安全性对哈希函数的要求降低，仅需要抗第二原像

缺点：

1. OTS密钥对的个数需事先确定，树的深度多大才合适？
2. OTS密钥对越多，构造树的时间越长

Hypertree：Merkle树的连接

- 想要解决的问题
  - 更加灵活地生成OTS密钥对，不需要一次性将往后需要使用的密钥对全部生成
- 解决思路
  - 预先生成适当数量OTS密钥对，构造Merkle树A
  - 签名时，生成适当数量OTS密钥对，构造Merkle树B_i
  - B_i对消息进行OTS签名，A对B_i的树根进行OTS签名
  - 联合形成完整的消息签名
  - B_i的密钥对使用完后,构造B_j并以A的另一对密钥签名B_j

量子账本

- 量子密码学
- 基于量子密码学的货币

量子密码学(量子签名)

- 著名的BB84
  - 量子秘钥分配(秘钥交换)
  - 旨在构建无条件安全的秘密信道
  - 一次一密的MAC和对称加密
- Arbitrated quantum-signature[ZK2002]

[ZK2002] Zeng G, Keitel C H. Arbitrated quantum-signature scheme[J]. Physical review A, 2002, 65(4): 042312.

量子密码学(量子签名)

- Arbitrated quantum signature scheme with message recovery [LHK+2004]
  - 利用持有的秘密从签名中恢复消息
  - 安全性是否依赖于entanglement和GHZ triplet states受到质疑 [WZL+2005]
- Weak blind signature[WNJ+2008]
  - 签名者不知道签名的具体消息是什么
  - 签名者可以追踪到消息的持有人是谁

量子密码货币的发展历程

- Quantum Banknotes: 第一个基于量子原理的量子货币方案，属于私钥系统，只能由铸币方验证真伪。
- Quantum Subway：第一个公钥量子密码货币系统，只允许一张钱花一次，因此称为地铁票。
- Quantum Coins：第一个满足货币可流通（transferable）而且匿名的方案。所有等额的货币具有相同的量子态，货币比特态在通过验证后不会改变，进而可以多次流通使用，而且使得无法追踪货币的使用人或地点。
- Quantum Bitcoin: 第一个去中心化的分布式量子货币系统。

参考文献

- Bennett C H, Brassard G, Breidbart S, et al. **Quantum cryptography, or unforgeable subway tokens**[C]//Advances in Cryptology'82. Springer US, 1983: 267-275.

- Wiesner S. **Conjugate coding[J**]. ACM Sigact News, 1983, 15(1): 78-88.

- Jogenfors J. **Quantum bitcoin: An anonymous and distributed currency secured by the no-cloning theorem of quantum mechanics**[J]. arXiv preprint arXiv:1604.01383, 2016.

- 贾恒越, 武霞, 朱建明. 量子加密货币研究进展概述[J]. 网络与信息安全学报, 2017, 3(2): 1-8.

量子区块链系统测试成功

- 俄罗斯国家量子研究中心，2017.06

Evgeny Kiktenko

Hash函数+量子秘钥分发

结束语

- 为什么要研究抗量子区块链和密码货币？
- 怎么实现？
  哈希函数+后量子公钥签名（环签名）
  哈希函数+哈希函数基于的一次性签名
  量子区块链与量子密码货币