doi :10.3969/j.issn.1671-1122.2018.01.006

基于 Merkle 哈希树结构的区块链第二原像攻击

王卯宁，段美姣
（中央财经大学信息学院，北京 100081）

摘　要：区块链是一种新兴的 IT 技术，具有去中心化、高效、透明等优势，被广泛认为具有颠覆性的应用前景。而应用场景的广泛性和应用层面的底层性决定了区块链的安全性必须得到保障。Hash 函数是保证区块链可用性和安全性的重要基础之一。文章从区块链中的 Hash 函数角度出发，基于密码分析原理，针对区块链的特有结构和工作流程，利用区块链中 Merkle 树 Hash 函数叶子节点的 Hash 值具有相同地位这一性质，构造一类对已存在区块发起的第二原像攻击。理论分析证明此类第二原像攻击的复杂度低于平凡搜索攻击，在此基础上，描述了基于 Hellman 原理的攻击实例构造算法。结论表明，Merkle 树 Hash 函数本身的数学结构和区块链交易记录的数据格式是影响区块链安全性的重要因素，今后在设计区块链系统时应当考虑此类因素。

关键词：区块链；Merkle 树；第二原像攻击；Hellman 时空平衡原理
中图分类号：TP309 **文献标识码：**A **文章编号：**1671-1122（2018）01-0038-07

中文引用格式：王卯宁，段美姣 . 基于区块链 Merkle 哈希树结构的第二原像攻击 [J]. 信息网络安全，2018（1）：38-44.

英文引用格式：WANG Maoning，DUAN Meijiao. The Second-preimage Attack to Blockchain Based on the Structure of Merkle Hash Tree[J].Netinfo Security,2018(1):38-44.

The Second-preimage Attack to Blockchain Based on the Structure of Merkle Hash Tree

WANG Maoning，DUAN Meijiao
(*Department of Information*, *Central University of Finance and Economics*, *Beijing* 100081, *China*)

Abstract: Blockchain technology is a kind of emerging information technology model. It is widely regarded as a promising concept because of its advantages such as decentralization, high efficiency, and transparency. The breadth of application scenarios and the underlying layer of application determine that the security of the blockchain must be guaranteed. Hash functions are one of the most important foundations for providing the blockchain's usability and security. Starting from Hash functions in the blockchain and based on the principle of cryptanalysis, this paper presents a type of second preimage attack on the existing blocks by employing the structure and workflow of the blockchain. Specially, the attack constructed in this paper uses the fact that the Hash values in the leaf nodes of a Merkle tree have the same status. After theoretical analysis

收稿日期：2017-10-20
基金项目：国家自然科学基金重点项目 [U1509214]；国家自然科学基金青年科学基金 [61702570]
作者简介：王卯宁（1987—），女，山东，讲师，博士，主要研究方向为密码算法的分析与设计；段美姣（1985—），女，河北，讲师，博士，主要研究方向为网络安全。
通信作者：王卯宁 13854139297@139.com

of proving that the complexity of such an attack is lower than that of trivial brute-force, the attack's concrete steps based on Hellman's time-memory tradeoff principle are also described. The conclusion of the attack shows that both the mathematical structure of the Hash function itself and data format of blockchain transaction records are important to the security of the blockchain. This should be considered in the future when we design blockchain systems.

Key words: blockchain; Merkle tree; second-preimage attack; Hellman's time-memory tradeoff

0 引言

区块链（Blockchain）是一种新兴的 IT 技术，其概念起源于 2008 年中本聪提出的分布式密码数字货币系统——比特币 [1]。区块链技术的实质是由多方参与并共同维护一个持续增长的分布式数据库，也被称为分布式共享总账，其优势在于去中心化、高效、透明、成本低。目前，区块链技术被广泛认为具有颠覆性的应用前景，已经在数字货币以及银行、证券、保险、投融资等金融科技领域得到应用 [2]。进一步而言，区块链技术的发展也为解决云数据存储、物联网等领域中一些问题开拓了新的思路，成为学术界和工业界关注的热点 [3–7]。

应用场景的广泛性和应用层面的底层性决定了区块链的安全性必须得到保障。安全性威胁是区块链如今所面临的最重要问题之一。从安全性角度进行分析，根据目前已公开的研究结果 [8,9]，区块链面临着算法安全性、协议安全性、使用安全性、实现安全性和系统安全性等方面的挑战。目前学术领域的研究者已经给出一些针对上述类型挑战的讨论。例如，KIAYIAS[10] 等人从协议安全性角度出发，在区块链可证明安全性和交易处理速度之间进行权衡，引入一种新的区块链协议（链式增长）来处理这一矛盾问题，得到了更稳健的区块链系统；SASSON[5] 等人从使用安全性角度出发，探讨了比特币中用户的隐私保护问题，给出了基于零知识协议的匿名区块链数字货币方案；GERVAIS[11] 等人从实现安全性角度出发，考虑现有比特币的理论安全分析是否适用于其他实现场景，特别是这些实现是通过不同的共识或网络参数进行实例化的情形，为此，引入一种新的定量框架，用以分析区块链中工作量证明 (Proof–of–Work, PoW) 共识机制对网络参数安全性和高效性的影响，同时，在这一文献中，还测试和讨论了区块链系统安全性的一个例子——eclipse 攻击的影响。

除上述一些研究方法外，另一个重要的研究手段是基于密码学原理，即将区块链系统看做是一个包含多种密码体制的应用系统，应用密码分析和设计原理，从机理上分析这种系统的安全性。特别地，密码分析学对整个系统的安全性评估具有重要意义。密码分析学的研究内容主要包括密码算法中易被攻击的结构弱点分析、密码方案的安全强度与密码数学问题困难性的关系、密码体制在实际环境中可能存在的缺陷、密码体制相互叠加会造成使用条件受限制等问题。此类研究方法也已于近年来出现在其他包含密码方案的系统安全性评估中。例如，STEVENS[12–14] 等人构造满足前缀指定条件的 MD5 碰撞，并基于这一方法构造了对 CA 证书、X.509 证书、pdf 文档的伪造，BHARGAVAN[15] 等人利用类似的原理构造了脚本碰撞攻击，用于攻击 TLS、IKE、SSH 中的认证环节。而区块链系统由于大量应用了各种密码学技术，属于算法高度密集工程，往往更容易出现问题。因而，若要全面地对区块链系统的安全性进行分析，密码分析技术是必不可少的。

更进一步地，在保证区块链可用性和安全性的密码学原理中，Hash 函数是一项重要基础。GIECHASKIEL[16] 等人具体讨论了当最经典的 Hash 函数安全准则，即抗原像性、抗第二原像性、抗碰撞性被打破时，整个区块链体系安全性将受到的冲击。其结论具有原创性的理论意义，但遗憾的是并不全面，

抗原像性等 3 个安全准则是对 Hash 函数本身的安全强度的描述，而对于一个应用于实际场景中的 Hash 函数，其安全性除了取决于本身的函数数学结构外，还与其使用环境的特殊性有关，一般来说，应用场景往往会带来一些限制，使得原本 Hash 函数安全性成立的必要条件发生改变。

在区块链中，Hash 函数的树状链式结构与 ECDSA 签名等其他密码部件的叠加使用，以及消息具有指定的数据结构等限制条件的存在，使得由 Hash 函数确保区块链的安全性这一看似直观的论断需要更多、更严格且更新颖的理论分析。本文着重探讨上述区块链中 Hash 函数面临的安全问题，利用区块链中 Merkle 树 Hash 函数存在的结构性特点和区块链存储交易记录数据格式的限制，构造了一类伪造型攻击。

本文的结构如下：第 1 章介绍区块链的基本知识，着重介绍本文提出的攻击方法中涉及的交易记录的数据结构和区块的形成原理；第 2 章介绍 Merkle 树 Hash 的性质，以及如何利用这一性质发起对已存在区块的第二原像攻击；第 3 章基于 Hellman 时空平衡原理，给出攻击实例的具体构造算法；第 4 章给出关于上述攻击的几点结论。

1 背景知识

1.1 区块链的基本原理

首先，以比特币为例，介绍区块链的基本工作原理。比特币是一类热门的分布式账本密码数字货币，其由中本聪于 2008 年提出。比特币最主要的技术之一是区块链结构的应用。区块链可以被看做是一个公共的日志，在这个日志里记录了所有已经发生的比特币交易 (Transactions)，其形式是将这些交易组成区块。具体来说，每个交易使用脚本语言描述本交易涉及的比特币的所有者，并且由矿工 (Miners) 保证只有有效交易能够被收录到区块链中。为了保证已经发生的交易不能被改变或者被移除，矿工会求解困难计算问题以证明其工作量。

从交易参与者的视角来看，区块链的工作流程可以概括为：一条交易的发起者将本交易涉及的信息按指定的数据结构填入交易记录，并将该交易记录发送给矿工节点；矿工节点验证交易记录，并求解困难问题以完成 PoW 机制来将该交易记录包含到区块链中，形成一个新的区块，将该区块广播至整个网络；交易的接收者看到网络中的区块并验证区块中的信息。

简单地说，比特币通过“挖矿”机制保证了不能任意造币，通过分布式网络和 Hash 链机制解决双重支付问题。实际上，比特币系统中不存在独立的电子货币，而只存在交易记录，货币值是依附于交易记录存在的，所以比特币系统中用户账户里电子货币的数量变化由交易账单所记录。同时，这也意味着，在比特币这样一种数字货币系统中，包含不同用户之间货币转移信息的交易记录就成为影响比特币结构安全性的重要部分。

1.2 交易记录的数据结构

为分析区块链中涉及的密码部件的安全性，寻找可能存在的安全问题的关键，我们着重探讨上述交易记录的数据结构及其中涉及密码部件的部分。一个交易记录可以被看做是一系列的输入和输出，其中，输入是一些可以被使用的，即未被花费的交易记录；输出是一些将要被转入货币的地址。通过观察比特币源代码 [17]Pay-to-Public-Key-Hash（P2PKH）协议中定义的交易记录类 CTransaction（位于 \bitcoin-master\src\primitives\transaction.h 文件中）可知，一条交易记录应按次序包含如下一些成分：

1）整数型变量 nVersion。占 32 比特空间，存放当前使用的区块链系统版本号。

2）数组 vin。包含本条交易使用的比特币的来源，数组中元素的个数即为交易发起者选择的作为本条交易的来源交易的个数。数组中每个元素为一个 CTxIn 类对象，每个对象所占空间为 1344 比特，具体包含如下部分：（1）一个 COutPoint 类对象 prevout，所占空间为 288 比特，标识来源交易具体

是哪一笔（其中包含一个 256 比特的 Hash 值，用以标识来源交易，一个 32 比特的整数用于指明该来源为某一交易记录中的哪一笔）。（2）一个 CScript 类对象 scriptSig，所占空间为 1024 比特，其中包含交易发起者的签名和公钥，由于数字签名算法使用的是 ECDSA（椭圆曲线数字签名算法、secp256k1 曲线），且公钥采用非压缩版，故 scriptSig 中签名 signature 和公钥 pubkey 各占 512 比特的空间。（3）一个 32 比特的整数 nSequence，作为一个固定的标识字来显示是否启用锁定时间。

3）数组 vout。指明本笔交易中比特币将要被转入的账户地址和数额，数组元素的个数即为目的地址的个数。数组中每个元素为一个占 224 比特空间的 CTxOut 类对象，具体来说，其包含一个 32 比特的整数 nValue 和一段脚本 scriptPubKey。脚本 scriptPubKey 的形式为如下伪代码所示：*DUP HASH*160 *addr EQV CHKSIG*，用以解析后续操作，其中 *DUP*、*HASH*160、*EQV*、*CHKSIG* 为 OP 操作码，每个操作码为一个 char 型常数，占 8 比特空间；*addr* 为公钥地址的 160 比特 Hash 值，即脚本 scriptPubKey 占 192 比特空间。

4）整数型变量 nLockTime。占 32 比特空间，一般被置为 0，当交易记录被广播到网络的时间大于该值时，交易才被认为是有效的。

一条交易记录的生成过程即为交易发起者根据需要将上述结构填写完整的过程。

1.3 区块的数据结构

矿工在接收到交易发起者填写的交易记录之后，将把从整个网络收集到的交易记录汇总，形成一个公开的、面向全局的、只能增加的账本，即区块链。这样，货币被保证不能重复使用。具体来说，每个区块将通过 Merkle 树组合交易记录，而新的区块通过挖矿过程形成整个区块链的一部分，即矿工需要找到一个随机数 nonce，使得一个区块头部的 Hash 值小于一个给定的目标值，用公式表示为：

$$Hash(header\|nonce) < target \quad (1)$$

其中区块头部 header 包括如下部分。

1）整数型变量 nVersion：版本号，所占空间为 32 比特。

2）hashPrevBlock：前一个区块的 Hash 值，即表明区块的标识，所占空间为 256 比特。

3）hashMerkleRoot：由所有交易记录的 Hash 值再经过 Merkle 树 Hash 运算得到，所占空间为 256 比特。

4）nTime：时戳，所占空间为 32 比特。

5）nBits：上限目标值，所占空间为 32 比特。

此外，通过 Merkle 树组合交易记录的具体流程为：首先计算每个交易记录 T_j 的 Hash 值，$h_j^0=Hash(T_j)$（当前版本使用的 Hash 函数为两次计算 SHA256 函数，即 SHA256(SHA256(T))），将这些 Hash 值作为 Merkle 树的叶子节点；之后，为计算第 i 层第 j 个节点，将第 i–1 层第 $2j$、$2j$+1 个节点的 Hash 值 h_{2j}^{i-1}、h_{2j+1}^{i-1} 级联作为消息进行 Hash 运算，即 $h_j^i=Hash(h_{2j}^{i-1}\|h_{2j+1}^{i-1})$，特别地，当第 i–1 层具有奇数个节点时，最后一个节点将被重复与其自身组成一个节点组作为消息进行下一层 Hash 运算；重复上述循环直到计算出一个根节点 hashMerkleRoot。

上述流程的机理为 PoW 机制，即生成一个新区块的概率正比于矿工的计算能力，并且由于矿工可以从中获得交易手续费，矿工被激励而进行这些操作，从而生成有效的区块以确认交易信息。

2 利用 Merkle 树结构的第二原像攻击

根据 1.3 节对 Merkle 树根节点计算过程的描述，可以发现如下一个性质：每个位于 Merkle 树叶子节点的 Hash 值具有相同的地位，即不同交易记录的 Hash 值 $h_j^0=Hash(T_j)$ 与 $h_k^0=Hash(T_k)$ 的区别仅是它们位于树的同一层的不同位置而已，成功攻击其中任意一个即可成功攻击整个 Merkle 树。利用这条性质，可以找到一种潜在的、对已存在的区块的攻击，并可以证明其复杂度低于平凡搜索攻击。

定理 1 对于一个包含 $L=2^l$ 个交易记录的区块链（l 可以不为整数），存在复杂度为 2^{n-l} 的第二原像攻击，其中 n 为 Merkle 树中所用 Hash 函数输出的长度。

证明：区块链中包含 $L=2^l$ 个交易记录，意味着在区块链的 Merkle 树中有 L 个叶子节点 Hash 值，这 L 个 Hash 值 $h_0^0,h_1^0,\cdots,h_{L-1}^0$ 均可作为目标，如果敌手能求出其中任何一个 Hash 值的第二原像，则根据 Merkle 树的计算流程，用计算出的这个值替代原有区块链的交易记录中对应的一个，将得到整个区块链的一个不同于原交易记录列表的交易记录列表。

要求一个 n 比特输出长度的 Hash 函数的第二原像，一个简单的方法是直接穷举 2^n 个消息（即交易记录），因为根据 Hash 函数的随机性，一个消息能够计算出某一个 Hash 函数输出值的概率为 $1/2^n$。故某一个消息能够计算出的 Hash 值属于包含 L 个元素的集合 $\{h_j^0,j=0,1,\cdots,L-1\}$ 的概率为：

$$1-(1-\frac{1}{2^n})^L \approx 1-(1-\frac{L}{2^n})=1-(1-\frac{1}{2^{n-l}})=\frac{1}{2^{n-l}} \quad (2)$$

故穷举 2^{n-l} 个随机生成的交易记录，将得到一个 Merkle 树的第二原像，即一个区块链的第二原像交易记录，结论得证。

此外，根据目前比特币的结构设置，有 $n=256,l\leqslant 72$，而交易记录中可供填写的部分能够保证 2^{n-l} 这一自由度的随机数量，故证明了存在复杂度小于平凡搜索（复杂度为 2^n）的伪造型攻击。如 GIECHASKIEL[16] 等人所指出的，这一类型攻击带来的威胁包括：区块链的分叉、破坏区块链的不可篡改性、攻击者可以因此质疑区块链中已经保存的交易等。同时，上述定理的结论可作为对 GIECHASKIEL 等人的分析的一个补充，即区块链中第二原像攻击的复杂度并不是 2^n，而是 2^{n-l}。

3 基于 Hellman 时间 – 空间平衡原理的攻击实例构造方法

更进一步地，基于上述分析结果，本章将展示采用 Hellman 时间 – 空间平衡原理，在允许预计算的前提条件下，构造有意义的第二原像交易记录的方法。

Hellman 时间 – 空间平衡原理 [18,19] 是密码分析学的基本原理之一，其面向的是无结构的搜索问题，即在搜索的过程中并没有运用具体的密码体制或密码算法的特殊结构性质，而是通过进行预计算并存储预计算结果（增加空间复杂度）的方式，将攻击开始后搜索目标的时间复杂度降低。目前，这一原理已广泛应用于密码分析学中很多具体的问题上 [20–22]，同时针对这一原理的理论分析和更有效的实现方式也一直是密码学领域的热门课题之一 [23–27]。

对区块链的应用背景进行研究可以看出，首先，Hellman 时间 – 空间平衡原理中允许预计算这一前提条件是满足的——区块链中存储的交易记录是只允许增长的，并且整个区块链协议中使用的交易记录格式和具体 Hash 函数是分析者（敌手）可见的。其次，由于区块链中需要构造的第二原像并不是随机的，该第二原像应当是满足交易记录格式的，也就是有意义的元素，因此，在本文的攻击方法中，针对区块链结构特性，构造了 Hellman 时间 – 空间平衡原理中所使用的链函数。

将对区块链的第二原像攻击分为如下两个阶段：

1）预计算阶段。分析者首先选取 m 个不同的起点：$SP_1, SP_2,\cdots,SP_m$，其中每个 SP_i 为一个随机交易记录（即符合交易记录数据结构，输出地址和金额为随机数的交易记录）。之后，分析者计算图 1 所示链接中的每个值。

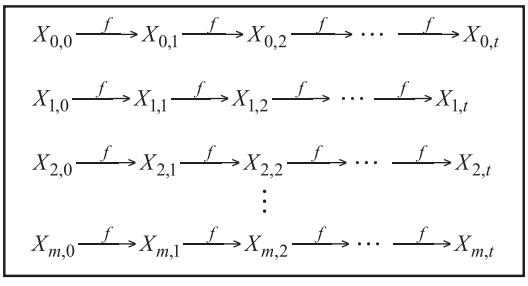

图 1 预计算阶段链式结构计算过程

图 1 中，$X_{i,0}=SP_i$，$S_{i,j}=f(X_{i,j-1})$，$1\leqslant j\leqslant t$；$X_{i,j}$ 为一

个交易记录，f 函数的计算包含 Hash 计算与格式填充两个步骤；m 为链接的条数，t 为每条链接中需要计算的消息记录的个数，m 与 t 应满足 $mt=\frac{2^n}{L}$，L 为 Merkle 树中已包含的交易记录的个数，n 为区块链协议中使用的 Hash 函数的消息摘要长度，例如，对于比特币，Hash 函数选取为 SHA256(SHA256(.))，n=256。对于所有的 i=0,1,⋯,m，j=0,1,⋯，t，$X_{i,j}$ 为有意义的交易记录，即其满足交易记录的格式。此外，为完成序列运算，$X_{i,j}$ 还应符合如下条件：首先，此记录对应的交易输入应当具有足够的金额。为此，提前选取一笔或多笔金额足够的源交易输出，连同其他位于交易输入部分之前的指定数据结构记为前缀 P。其次，选取一个整数 n' 整除 n，并且 $\frac{n}{n'}=s\leqslant 32$，这里 n=256，如上所述为 Hash 函数输出的比特长度。选取 n' 个有效地址 $addr_1,addr_2,\cdots,addr_{n'}$，即每个 $X_{i,j}$ 形式如下：$P\|(value_1,addr_1)\|(value_2,addr_2)\|\cdots\|(value_{n'},addr_{n'})\|(value_{n'+1},P')\|S$，其中，符号 $\|$ 表示级联；$value_1,value_2,\cdots,value_{n'}$ 是转入对应地址的金额，需要根据上一步中 f 函数的计算进行填充；$value_{n'+1}$ 是剩余的需要转入最后一个地址（即源交易所属人地址）的金额；S 为交易记录中结尾字段。

下面对 f 函数即一条链中相邻两个值的计算过程进行介绍。对于一个给定的输入交易记录 $X_{i,j}$，首先计算其 Hash 值（256 比特）$h_{i,j}=Hash(X_{i,j})$。之后，将 $h_{i,j}$ 分割为 n' 段，每段 s 比特，将这 n' 个 s 比特的数分别填入 $value_1,value_2,\cdots,value_{n'}$，再计算相应的 $value_{n'+1}$ 值。这样，就构造了另一个有意义的交易记录，将其作为 $X_{i,j+1}$。依次计算后续每个链中的值。

为减少存储空间的需求，分析者仅需要存储每条链的开始点和结束点的 Hash 值，即 $SP_i=X_{i,0}$，$Hash(EP_i)=Hash(X_{i,t})$。之后，依 $Hash(EP_i)$ 对 $\{SP_i,Hash(EP_i)\}_{i=1}^{m}$ 进行排序，并存储在一个数据结构表（记该表为 *Table*）中，作为预计算的结果。

2）在线攻击阶段。分析者获得存在于 Merkle 树中的 L 个交易记录 $T_1,T_2,\cdots,T_L$，依次计算：$f(T_1),f(T_2),\cdots,f(T_L),f^2(T_1),f^2(T_2),\cdots,f^2(T_L),f^3(T_1),f^3(T_2),\cdots,f^3(T_L),\cdots$。其中，$f$ 为预计算阶段中的 f 函数；f^a 符号表示连续 a 次作用 f 函数，其中 a 取 2，3，4，⋯。在计算出每一个 $f^a(T_b)$ 之后，检测是否有 $i\in\{0,1,\cdots,m\}$ 使得 $Hash(f^a(T_b))=Hash(EP_i)$，即 $Hash(f^a(T_b))$ 是否等于表 *Table* 中的某一个索引值。如果该条件不成立，则继续计算 $f^a(T_b)$ 的下一个值；如果该条件成立，则标记使得条件成立的 i 值，利用存储在表 *Table* 中的起始点 $SP_i=X_{i,0}$，计算到第 $t-a$ 步，即得到交易记录 $X_{i,t-a}$，根据计算过程，$X_{i,t-a}$ 满足 $Hash(X_{i,t-a})=Hash(T_b)$，即分析者找到 Merkle 树某一叶子节点 T_b 的第二原像，根据定理 1 的结论，发起了对整个区块链的第二原像攻击。

从上述攻击阶段的描述可以看出，在预计算阶段，需要计算 $mt=\frac{2^n}{L}$ 次 f 函数，其时间复杂度为 $\frac{2^n}{L}$，空间复杂度为 m；在在线攻击阶段，由于一定存在某个 b，使得 $f^a(T_b)$ 位于 m 条链中的某一条中，所以这一阶段的时间复杂度为 Lt，空间复杂度可忽略。根据目前比特币中的参数设定（n=256,$L=2^{72}$）可知，上述过程复杂度为 2^{184}。

4 结束语

针对区块链中 Merkle 哈希树的特有结构，本文提出了一类第二原像攻击，其复杂度低于区块链中 Hash 函数安全强度设定标准，且存在实际应用场景，因而具有理论意义。本文的研究结论是，对于区块链设计者，使用 Merkle 哈希树或其他密码部件时，应全面考虑应用环境，注意其实际应用场景与理论安全强度成立的条件是否匹配，进而更合理地评估整个区块链系统的安全性。（责编 李臻）

参考文献：

[1] NAKAMOTO S. Bitcoin: A Peer-to-peer Electronic Cash System[EB/OL]. https://bitco.in/pdf/bitcoin.pdf，2008-9-1.

[2] SWAN M. Blockchain: Blueprint for a New Economy[M]. Sebastopol: O'Reilly Media, Inc., 2015.

[3] KOSBA A, MILLER A, SHI E, et al. Hawk: The Blockchain Model of Cryptography and Privacy-preserving Smart Contracts[EB/OL]. http://www.cs.umd.edu/sites/default/files/scholarly_papers/Kosba.pdf,

2016-8-18.
[4] EYAL I, GENCER A E, SIRER E G, et al. Bitcoin-NG: A Scalable Blockchain Protocol[EB/OL]. http://www.usenix.org/sites/default/files/conference/protected-files/nsdi16_slides_eyal.pdf, 2017-8-20.
[5] SASSON E B, CHIESA A, GARMAN C, et al. Zerocash: Decentralized Anonymous Payments from Bitcoin[EB/OL]. http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf, 2014-5-18.
[6] ZHANG Y, WEN J. The IoT Electric Business Model: Using Blockchain Technology for the Internet of Things[J]. Peer-to-peer Networking Application, 2017, 10(4): 983-994.
[7] CHRISTIDIS K, DEVETSIKIOTIS M. Blockchains and Smart Contracts for the Internet of Things[J]. IEEE Access, 2016, 4: 2292-2303.
[8] bitcoinwiki. Common Vulnerabilities and Exposures[EB/OL]. https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures, 2017-5-25.
[9] bitcoinwiki. Weaknesses[EB/OL]. https://en.bitcoin.it/wiki/Weaknesses, 2017-7-4.
[10] KIAYIAS A, PANAGIOTAKOS G. Speed-security Tradeoff s in Blockchain Protocols[EB/OL]. https://eprint.iacr.org/2015/1019, 2015-12-1.
[11] GERVAIS A, KARAME G O, WÜST K, et al. On the Security and Performance of Proof of Work Blockchains[C]//ACM. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, October 24 - 28, 2016,Vienna, Austria. Myers and Shai Halevi. New York, USA: ACM, 2016: 3-16.
[12] STEVENS M, LENSTRA A K, De Weger B. Chosen-prefix Collisions for MD5 and Applications[J]. International Journal of Applied Cryptography, 2012, 2(4): 322-359.
[13] STEVENS M, SOTIROV A, APPELBAUM J, et al. Short Chosen-prefix Collisions for MD5 and the Creation of a Rogue CA Certificate[EB/OL].http://pdfs.semanticscholar.org/086d/25b00cb1d3534335eafdf9cc20e1092e5629.pdf,2009-8-16.
[14] STEVENS M. New Collision Attacks on SHA-1 Based on Optimal Joint Local-collision Analysis[EB/OL]. http://www.marc-stevens.nl/research/papers/EC13-S.pdf,2017-8-29.
[15] BHARGAVAN K, LEURENT G. Transcript Collision Attacks: Breaking Authentication in TLS, IKE, and SSH[EB/OL]. https://www.mitls.org/downloads/transcript-collisions.pdf, 2016-2-21.
[16] GIECHASKIEL I, CREMERS C, RASMUSSEN K B. On Bitcoin Security in the Presence of Broken Cryptographic Primitives[EB/OL]. https://eprint.iacr.org/2016/167.pdf, 2017-8-29.
[17] bitcoincore.org. Bitcoin Core[EB/OL]. https://github.com/bitcoin/bitcoin, 2017-8-18.
[18] HELLMAN M. A Cryptanalytic Time-memory Trade-off[J]. IEEE Transactions on Information Theory, 1980, 26(4): 401-406.
[19] QUISQUATER J J, STANDAERT F X. Time-memory Tradeoffs[M]// Henk C.A.v. Tilborg. Encyclopedia of Cryptography and Security. New York:Springer,2005: 614-616.
[20] BIRYUKOV A, SHAMIR A. Cryptanalytic Time/memory/data Tradeoffs for Stream Ciphers[EB/OL]. http://pdfs.semanticscholar.org/ae2e/3e5508409c10f6cce483b468fc2995db2285.pdf,2017-9-11.
[21] BIRYUKOV A, SHAMIR A, WAGNER D. Real Time Cryptanalysis of A5/1 on a PC[EB/OL]. http://pdfs.semanticscholar.org/9028/b0223c918a9a135cd0de074f05e1ca842166.pdf,2010-4-10.
[22] SASAKI Y. Recent Applications of Hellman's Time-memory Tradeoff[EB/OL]. www1.spms.ntu.edu.sg/~ask/2015/slides/07_YuSasaki.pdf, 2015-9-1.
[23] OECHSLIN P. Making a Faster Cryptanalytic Time-memory Trade-off[EB/OL]. https://lasec.epfl.ch/pub/lasec/doc/Oech03.pdf,2017-9-15.
[24] BARKAN E, BIHAM E, SHAMIR A. Rigorous Bounds on Cryptanalytic Time/memory Tradeoffs[EB/OL]. http://cs.tau.ac.il/~tromer/SKC2006/tm40.pdf, 2017-9-15.
[25] QUISQUATER J J, STANDAERT F X, ROUVROY G, et al. A Cryptanalytic Time-memory Tradeoff: First FPGA Implementation [EB/OL].https://perso.uclouvain.be/fstandae/PUBLIS/3.pdf,2017-9-20.
[26] HONG J, KIM B I. Performance Comparison of Cryptanalytic Time Memory Data Ttradeoff Methods[J]. Bulltin of the Korean Mathematical Society, 2016, 53(5): 1439-1446.
[27] DINUR I, DUNKELMAN O, KELLER N, et al. Memory-efficient Algorithms for Finding Needles in Haystacks[EB/OL]. https://eprint.iacr.org/2016/560.pdf,2017-10-9.