软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, [doi: 10.13328/j.cnki.jos.000000]
©中国科学院软件研究所版权所有.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于“垂直认证”的区块链安全解决方案 *

胡祥义[1,2], 赵桂芬[1,2]

[1](北京市科学技术情报研究所, 北京 100044)

[2](网络密码认证北京市重点实验室, 北京 100044)

通讯作者: 赵桂芬, E-mail: gfzh@hotmail.com

摘 要: 本文对现有区块链安全体系进行分析，公开了其安全架构的技术漏洞，以及不法分子可能对这些漏洞进行攻击的具体方法，阐述了采用公钥体系保证区块链安全不可行的原因。提出了基于“垂直认证”技术建立区块链安全解决方案，是采用单钥算法建立区块链认证体系，亦即：采用组合密钥生成算法，实时产生认证、签名和加密密钥，一次一变，解决了单钥密码算法密钥管理的难题，对比公钥体系大约可提高区块链认证协议速度 100 倍， 大约提高签名验证速度 200 倍，在客户端、节点服务器端和密钥管理服务器端，采用“芯片”对“芯片”的签名协议，且签名密钥一次一变，即：新一代数字签名协议，从而，建立“芯片级”可信区块链安全系统。

关键词: 区块链;垂直认证;组合密钥;加密芯片;单钥算法;公钥算法;新一代签名处理

中图法分类号: TP311

中文引用格式: 胡祥义,赵桂芬. 基于“垂直认证”的区块链安全解决方案.软件学报. http://www.jos.org.cn/1000-9825/0000.htm

英文引用格式: Hu XY, Zhao GF. Solution for Block-chain security based on Vertical Authentication. Ruan Jian Xue Bao/Journal of Software, 2018 (in Chinese). http://www.jos.org.cn/1000-9825/0000.htm

Solution for Block-chain security based on Vertical Authentication

HU Xiang-Yi[1,2], ZHAO Gui-Fen[1,2]

[1] Beijing Municipal Institute of Science & Technology Information, Beijing 100044, China)

[2] Beijing Key Laboratory of Network Cryptographic Authentication (Beijing Municipal Institute of Science & Technology Information), Beijing 100044, China)

Abstract: Analyze the current security architecture of block-chain, weakness, and possible attack method. Set out the reason why public key architecture is unfeasible for block-chain security. A security solution for block-chain is proposed on the basis of vertical authentication technology. It adopts secret key algorithm to set up block-chain authentication architecture, that is adopts combined key generation algorithm and generate real-time authentication, signature and encryption key. Therefore, solve the problem of secret key management, and enhance the authentication speed about 100 times and signature verification speed about 200 times contrast with public key architecture. At client, node server and key management server, chipsets to chipsets signature protocol is used, that is new generation digital signature protocol. Thereby chipsets-level trusted block-chain security system is built.

Key words: Block-chain; vertical authentication; combined key; encryption chipset; secret key algorithm; public key algorithm; new generation signature

目前，国内外的区块链都是采用公钥体系（如：PKI）来实现，但是，由于公钥算法运行效率较低，造

* 基金项目:

收稿时间: 0000-00-00; 修改时间: 0000-00-00; 采用时间: 0000-00-00; jos 在线出版时间: 0000-00-00
CNKI 在线出版时间: 0000-00-00

成现有区块链运行速度较慢，如：比特币每秒只能完成 7 笔交易，这影响并阻碍了区块链实现规模化并发交易的应用，同时，用户的私钥容易被黑客获取，其安全等级较低，造成现有区块链的安全事件频发，如：比特币每半年就出现一次信息安全事件，给用户带来较大损失，总之，现有的区块链技术产品不能满足市场的需求。

近几年，区块链技术也在进行安全升级，陆续为用户客户端提供带 CPU 芯片的 U 盾，带 CPU 芯片的 U 盾是采用价格低廉的加密芯片，将用户的私钥放在 U 盾的芯片里。但是，这些廉价的 CPU 芯片安全等级较低，容易被不法分子通过破坏性解剖拿到用户的私钥，再来克隆用户的 U 盾，盗取用户账户里的资金。即使在客户端为用户提供的是合规的 U 盾，而 PKI 技术的公钥是以明文形式存储在网络公钥服务器中，也容易受到黑客的攻击。

为一劳永逸彻底解决现区块链的安全问题，我们提出一种基于“垂直认证”技术的区块链安全升级方案，其中：“垂直认证”技术是基于“密钥种子”集中生成，集中灌装，集中分发，集中销毁，并采用单钥密码算法（SM1 或 SM4 算法）和组合密钥（CSK，companed single key）生成算法，建立认证、签名和加密协议，在客户端为用户提供合规的加密芯片（如：U 盾或手机端 TF 卡），在加密芯片里写入认证、签名和加密协议，在节点服务器端嵌入加密芯片，在加密芯片里写入认证、签名验证和解密协议，建立“芯片”对“芯片”的签名协议，且签名密钥一次一变，亦即：新一代签名协议，采用单钥算法建立区块链的安全体系，对比公钥体系安全性较高，且并发认证的速度大约能提高 100 倍，并发签验的速度大约能提高 200 倍，可以解决目前存在的区块链安全体系漏洞而带来的资金被盗的问题。

1 区块链系统存在安全隐患

区块链系统存在多种安全隐患，我们这里主要是阐述采用公钥体系建立区块链数字货币系统存在的安全隐患。

区块链数字货币交易系统是采用公钥算法（如：PKI）建立安全架构，PKI 已经问世近 30 年了， PKI 采用公钥体系建立认证体系，即：采用公钥算法（公钥密码算法如： RSA 或 ECC ），实现身份认证、数字签名和密钥交换，并采用单钥密码算法（如：SM1、SM4、AES、3DES、DES 、RC5 等）实现数据的加/解密。

1.1 “软钱包”存在的安全隐患

所谓“软钱包”就是采用软件方式开发的认证协议，如：软件开发的 PKI 认证/签名协议，实现身份认证后登录用户的账号（钱包），通过签名协议对支付单进行签名。软件开发的 PKI 认证/签名协议，存在安全隐患。

1.1.1“软钱包”容易被破解，黑客可以通过病毒获得用户在客户端（PC 机或手机等）中的私钥，再使用盗来的用户私钥登录用户的钱包，从而，盗用数字货币，其中：私钥就是一串数字，如:RSA 算法的密钥对的长度为 1024、2048、4096 比特；ECC 算法密钥对的长度为 256 比特。

黑客还可以篡改数字货币社区公钥服务器中的用户证书，其中：证书含：用户标识、实体证书公钥、中级证书公钥、根证书公钥，以及上一级证书的私钥对下一级证书的数字签名等，即：黑客使用伪造的证书来替代用户存储在公钥服务器中的证书，黑客采用自己的私钥来通过身份认证协议登录用户的钱包。

1.1.2 “软钱包”受攻击的原理，在建立“软钱包”的过程中，公钥密码算法（如：RSA 或 ECC 算法）是公开的，PKI 身份认证协议（双向认证、单向认证、或挑战/应答式认证）是公开的，数字签名的协议是公开的，证书（含：公钥）也是公开的，且能在数字货币社区的证书服务器里下载。 可见，除了用户的私钥，所有的认证/签名协议及其数据黑客都知道。黑客可伪造一组密钥对和证书，在客户端采用伪造的私钥，对证书和一组随机数进行加密（举例：挑战/应答式认证协议），生成认证口令，数字货币社区的证书服务器对应黑客伪造的证书，对口令进行认证，实现黑客登录用户的账户（钱包）。

同时，黑客在客户端，采用伪造的私钥对数字货币的交易单进行签名，数字货币社区的证书服务器对应

黑客伪造的证书（含：公钥），对交易单的数字签名进行签名验证，从而，完成数字货币的交易，盗用用户的数字货币。

通过以上攻击方式，黑客可以实现“张冠李戴”式攻击进入用户的账户（钱包），从而，盗取用户钱包里的数字货币。

1. 2 “硬钱包”存在的安全隐患

1.2.1 所谓“硬钱包”就是采用 PKI 建立认证/签名协议，在用户的客户端使用 U 盾（智能卡加密芯片）或带加密芯片的 SD 卡（插入手机里），将密码算法、摘要算法、私钥、证书、身份认证协议和数字签名协议存放在 U 盾或 SD 卡中，用户使用 U 盾或 SD 卡硬件设备，实现身份认证后可登录用户的账号（钱包）。

数字货币交易所采用“硬钱包”，要比“软钱包”安全等级高的多。但是，为数字货币交易所提供 PKI 服务的开发商，若采用劣质 U 盾芯片，造成智能卡中被封装的芯片容易受到黑客破坏性破解，读出芯片里用户的私钥；或者，用户丢失 U 盾或 SD 卡后，通过设备初始化生成的记忆，重新将相同的私钥写入新 U 盾或 SD 卡的过程中，造成用户的私钥外泄。

总之，劣质的 U 盾或 SD 卡容易被破解，用户的私钥会被读出，无法保证“硬钱包”的安全。

1.2.2 “硬钱包”与“软钱包”一样，存储在数字货币社区公钥服务器上的用户证书容易受到黑客攻击，即使用户不将自己的证书（含：公钥）存储在数字货币社区公钥服务器上，黑客也可容易在节点服务器端获得用户的证书（含：公钥）。黑客通过伪造用户证书（公、私钥），来替代用户的证书（含：公钥）（存储在公钥服务器中），黑客采用自己的私钥来通过身份认证协议登录用户的账户（钱包），并对交易单进行数字签名来盗取用户的数字货币。

2 区块链交易系统效率较低

目前，数字货币交易系统的节点服务器端，处理区块链数字货币交易记录为：7 笔/秒。数字货币交易系统的区块链，是使用公钥算法建立认证体系如：PKI，数字货币社区的证书认证服务器，并发认证或并发签验的速度都较慢，直接制约了数字货币交易系统的效率，无法支撑较大量用户的并发认证，或较大量支付单的并发签验。

IBM 曾经发出豪言壮语：他们公司开发的区块链，节点服务器处理交易记录的速度能达到：10000 笔/秒。但是，每个节点端的设备成本他们没有阐述。

因此，若想提高节点端交易速度，只能不断增加节点端服务器设备的投入，从而，增加了数字货币交易所建立数字货币区块链系统的成本。

3 采用“垂直认证”技术解决区块链数字货币交易的安全问题

3.1 “垂直认证”技术的的定义：密钥集中生成，集中灌装，集中分发，集中注销。

“垂直认证”技术的特征：是采用单钥算法如：SM1、SM4、AES 算法，完成身份认证、数字签名、密钥交换和数据加密 4 个功能。国际通用“第三方认证”技术如：PKI，是采用公钥算法（如：ECC 或 RSA），与单钥算法（如：SM1 或 SM4）相结合，完成身份认证、数字签名、密钥交换和数据加密等 4 项功能。

“垂直认证”技术是在认证中心端使用硬件设备作为仲裁者，使用组合对称密钥生成算法，实现认证、签名和加密密钥，一次一变，解决了单钥算法的密钥更新管理的难题，其中：采用组合密钥生成算法更新密钥，是一种智能合约式密钥更新方式，PKI 是人工更新密钥方式。

3.2 客户端采用获得国家密码管理局颁发商密产品证书的 U 盾或 SD 卡，该 U 盾或 SD 卡通过密码管理局商密产品测试中心的安全检测，认证/签名协议和密钥数据不能被读出，可抗破坏性解刨分析，U 盾或 SD 卡中芯片的安全得到保证。或者，与芯片厂商深入合作，在 U 盾或 SD 卡芯片的 IP 内，写入“垂直认证”技

术的组合密钥生成算法和认证、签名和加密协议（国密算法 SM1、SM2、SM3、SM4 算法，也写入芯片的 IP 核中），其中：采用 SM1 保密算法（算法不公开），芯片的 IP 核可以保证各种密码算法、协议和密钥数据的运行和存储安全。

3.3 基于“垂直认证”技术的区块链数字货币交易系统方案

在客户端嵌入加密芯片如：U 盾或 SD 卡，在客户端加密芯片里写入单钥算法、摘要算法、组合密钥生成算法、一组“密钥种子”表 i 的元素、身份认证协议、签名协议、加密协议、解密协议，从而，建立“芯片级”区块链的客户端。

在区块链系统中建立 j 个节点，在节点的服务器端部署加密芯片硬件设备，写入单钥算法、组合密钥生成算法、一组“存储密钥”K、身份认证协议、签名验证协议、解密协议，在节点服务器端建立“密钥种子”数据库，将全体用户的标识、账号、“密钥种子”表 i 的元素密文，一并存储在节点服务器端的“密钥种子”数据库中,从而，建立“芯片级”的区块链节点（见下图），其中：分别用“存储密钥”K，加密全体用户的“密钥种子”表 i 元素， j=100～10 万，j 为区块链全部节点的总数。

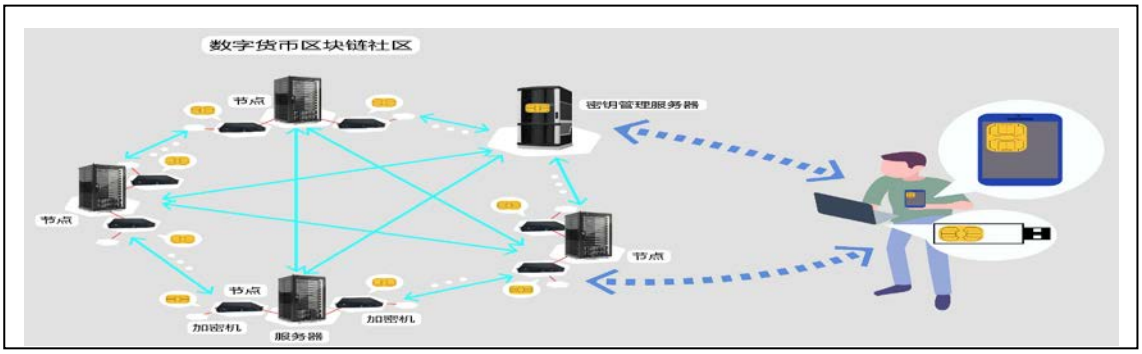

图 1 数字货币交易区块链系统拓扑图

在区块链系统中建立 1～3 个密钥管理服务器，在密钥管理服务器端也部署加密芯片硬件，在加密芯片里写入单钥算法、一组“存储密钥”K、组合密钥生成算法、加密协议，在密钥管理服务器端建立“密钥种子”数据库，将全体用户的标识、账号、对应的 “密钥种子”表 i 的元素密文，一并存储在密钥管理服务器端的“密钥种子”数据库中，从而，建立“芯片级”的区块链的密钥管理服务器（见下图），其中：用“存储密钥”K,分别加密全体用户的“密钥种子”表 i 元素，i=1～n，n≤20 亿，n 为全体区块链用户总数，不同节点服务器端和密钥管理服务器的“存储密钥”K，都两两相同。

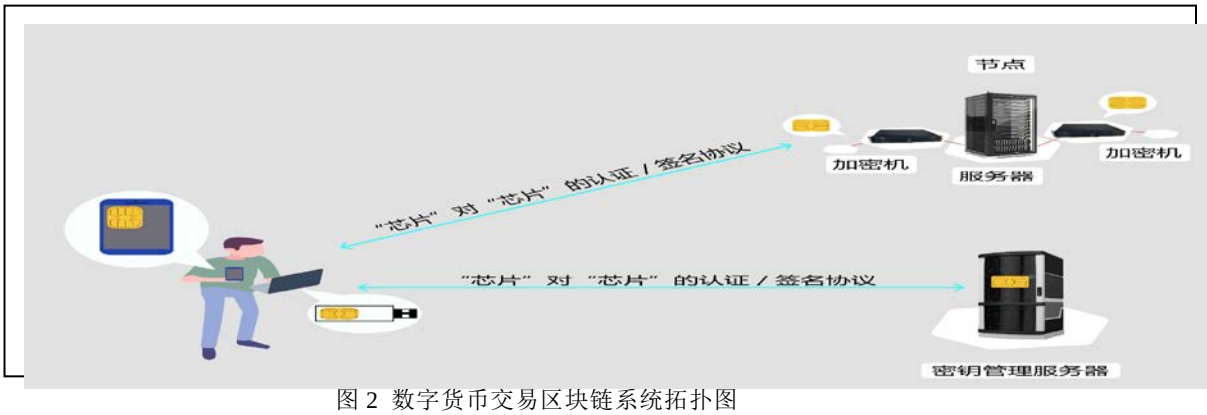

图 2 数字货币交易区块链系统拓扑图

3.3.1 组合密钥生成算法，是由一组时间戳和随机数组成的选取参数，来对一组“密钥种子”表的元素进行选取，将选出的 Y 个元素，并合成一组认证密钥 RK、签名密钥 QK，或加密密钥 JK，因为，区块链加密系统采用单钥算法，则：客户端的认证密钥 RK=节点服务器端的认证密钥 RK，签名密钥 QK=签名验证密钥 QK，加密密钥 JK=解密密钥 JK，其中：Y=16 或 32，认证、签名和加密密钥一次一变。

3.3.2 当用户客户端的加密芯片丢失时，由密钥管理单位负责更新用户客户端加密芯片，在新的加密芯片里写入一组新“密钥种子”表元素，其他内容与原用户客户端加密芯片里内容完全相同，同时，更新密钥管理服务器端的“密钥种子”数据库里对应用户的记录，再由密钥管理服务器端加密系统，对所有节点服务器端的“密钥种子”数据库里对应用户的记录进行自动更新。

3.4 区块链的数字货币交易协议

3.4.1 当用户 A 支付一笔款给用户 B 时，用户 A 和用户 B 客户端加密芯片里的签名协议，根据组合密钥生成算法，分别产生用户 A 的签名密钥 QKa 和用户 B 的签名密钥 QKb，对用户 A 和用户 B 的交易单进行签名，所有节点服务器都将已被用户 A 和用户 B 签名的交易单，分别收入一个区块里，每个节点服务器端加密芯片里，根据组合密钥生成算法，分别生成用户 A 的签名验证密钥 QKa1 和用户 B 的签名验证密钥 QKb1，对已经被用户 A 和用户 B 签名的交易单进行签名验证，若通过签名验证，则各个节点服务器端加密系统，将用户 A 和用户 B 的交易单写入区块中，否则，则用户 A 和用户 B 的交易单无效。

在经过时间 T 后，各个节点服务器端加密系统，根据“共识算法”，确认某个用户对区块进行记账，将时间 T 内所有通过签名验证的交易单登记在一个区块里，智能合约将上一个区块的摘要信息写入本区块“头部”，形成区块链中的一个区块，并对本区块进行摘要得到摘要信息 M，其他节点服务器端加密系统对摘要信息 M 进行验证，通过验证后也在其他所有节点服务器端记录该区块，从而，完成用户之间的交易单在区块链里的登记。

3.4.2 当用户 A 发送一张现金支票给用户 B 时， 用户 A 客户端加密芯片里的签名协议，根据组合密钥生成算法，产生用户 A 的签名密钥 QKa，对用户 A 发送给用户 B 的现金支票进行签名，用户 B 客户端加密芯片里的加密协议，产生用户 B 的加密密钥 JKb，将用户 A 发送给用户 B 的现金支票加密成密文，所有节点服务器都将已被用户 A 签名和用户 B 加密的交易单，分别收入一个区块里，每个节点服务器端加密芯片里，分别生成用户 A 的签名验证密钥 QKa1 和用户 B 的解密密钥 JKb1， 对已经被用户 A 签名的现金支票进行签名验证，若未通过签名验证，则现金支票不可信，若查询通过，则用户 A 发送给用户 B 的现金支票有效，各个节点服务器端加密系统将用户 A 发送给用户 B 的现金支票写入一个区块中；

在经过时间 T 后，各个节点服务器端加密系统，根据“共识算法”，确认某个用户对区块进行记账，将时间 T 内所有通过签名验证的现金支票登记在一个区块里，智能合约将上一个区块的摘要信息写入本区块“头部”，形成区块链中的一个区块，并对该区块进行摘要得到摘要信息 M，其他节点服务器端加密系统，对摘要信息 M 进行验证，通过验证后，也在其他所有节点服务器端记录该区块，从而，完成用户现金支票在区块链的登记。只有用户 B 才能调用自己的密钥，对用户 A 发送给用户 B 的现金支票密文进行解密，并使用该现金支票。

3.5 采用“垂直认证”技术建立区块链安全体系，能实时产生认证、签名和加密密钥，一次一变。同时，在客户端、节点服务器端和密钥管理服务器端，都部署加密芯片里，实现“芯片”对“芯片”的身份认证协议、签名协议和签名验证协议，也是新一代数字签名协议，从而，建立一种“芯片级”可信区块链系统，可大幅度提高区块链数字货币应用系统的安全等级。

4 4.0 采用“垂直认证”技术解决区块链的数字货币交易的效率问题

4. 1 采用单钥算法建立认证/签名协议，效率较高。所有教课书都阐述：在芯片里，单钥算法比公钥算

法的运行速度快 1000 倍，在计算机内存里，单钥算法比公钥算法的运行速度快 100 倍，这是公理。由此可见，采用单钥算法建立认证/签名协议，可充分发挥单钥算法具有加/解密速度快的优势，能大大提高区块链节点服务器端并发签名验证的效率。

4.2 “垂直认证”技术和 PKI 技术的签名和加密协议过程对比

PKI 技术签名和加密协议过程图如下：

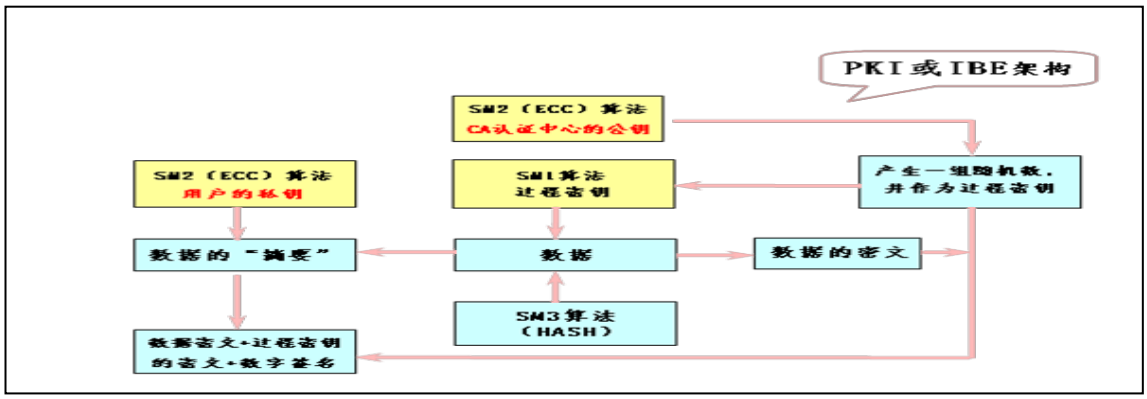

图 3 PKI 技术签名和加密协议过程图

“垂直认证”技术的签名和加密协议过程图如下：

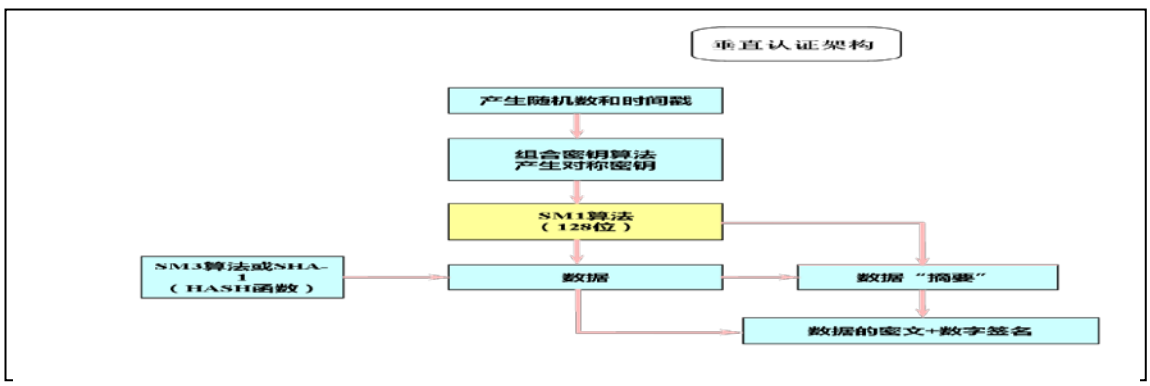

图 4 “垂直认证”技术的签名和加密协议过程图

通过对比“垂直认证”技术与 PKI 的签名和加密协议的流程图，可见：PKI 多调用了 2 次公钥算法，同时，多调用了 2 种公钥，一次是加密数据文件的“摘要”（即：数字签名），一次是加密过程密钥 K，实现过程密钥 K 的交换。而“垂直认证”技术少调用 2 次公钥算法，且少调用了 2 次密钥（私钥和公钥）。

因此，“垂直认证”技术的并发认证/签验对比 PKI，大约能提高区块链认证速度 100 倍，对比 PKI 大约能提高区块链签名验证速度 200 倍（详见 4.3 测试报告数据对比）。采用新一代签名协议，能有效解决现有区块链系统每秒只能完成 7 笔交易，运行效率较低的难题。

4. 3 “垂直认证”技术的并发认证/签验测试报告

经过权威的国内第三方产品性能检测，单座认证中心，可管理 3 亿用户，并发认证达到 1228.50 次/秒，并发签名验证达到 823.93 次/秒。

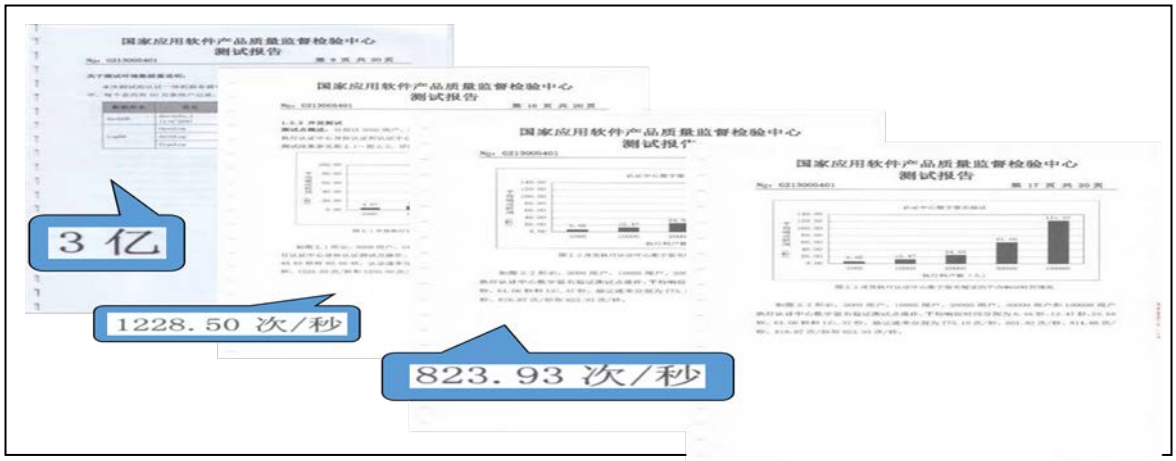

图 5 “垂直认证”技术的认证中心测试报告

由上图可见： “垂直认证” 技术产品，经过第三方权威部门的检测报告：可管理用户规模达 3 亿，并发认证：1228.50 次/秒，并发签验：823.93 次/秒。“垂直认证”技术的技术性能，远远超过 2020 年国家该领域的技术指标（见：“网络空间安全”重点专项 2016 年度项目申报指南）。

用“垂直认证”技术的检测报告，来对比国家《 “网络空间安全”重点专项 2016 年度项目申报指南》中的认证技术指标，其中：并发认证的速度比 PKI 快 3600 倍，远远超过 100 倍。由此可推算出，并发签验的速度比 PKI 快 200 倍以上。【 注：《“网络空间安全”重点专项 2016 年度项目申报指南 》 ……。 3.1 网络可信身份管理技术研究（重大共性关键技术类） 考核指标：1. 身份管理系统应支持亿级规模的身份管理，百万级并发、1000 个应用条件下，单个身份鉴别延时不大于 3 秒，身份鉴别应采用国产密码算法。……。】

5 结束语

总之，采用“垂直认证”技术建立区块链数字货币交易安全系统，通过组合密钥生成算法解决单钥算法密钥管理的难题，可实现认证、签名和加密密钥，一次一变。每个用户对应的“密钥种子”，两两不同，一个用户的“密钥种子”不慎泄露，不影响其他用户“密钥种子”的安全，并通过建立客户端、节点服务器端和密钥管理服务器端的“芯片级”认证、签名和加密协议，能提高区块链的安全等级。不法分子无法攻克新一代签名协议——签名密钥一次一变的“芯片级”签名协议。同时，“垂直认证”技术采用的单钥算法，具有加/解密速度快的优势，能提高区块链数字货币交易的效率，对比 PKI 大约能提高区块链认证速度 100 倍，对比 PKI 大约能提高区块链签名验证速度 200 倍。能解决现有区块链系统每秒只能完成 7 笔交易，运行效率较低的难题。另外，“垂直认证”技术产品已经通过的国家密码管理局颁发的商密产品证书 ——《SRZ06 身份认证系统》和《SRT1101 数据签名验证系统》，技术合规且成熟，能较好应用于区块链领域，保证区块链系统运行安全高效。

References:

附中文参考文献:

[1] Cory Fields， 比特币现金漏洞追踪始末， 猎云网.2018.8.15 ； Cory Fields ， 麻省理工学院媒体实验室，数字货币项目比特币核心钱包开发人员；

[2] 比萨 几乎所有钱包都有致命漏洞，黑客接触手机 2 分钟，就能转走币 一本区块链，2018.*7.21；*

[3] 刘惠莹 区块链安全造成 20 亿美元经济损失，安全问题频发让人防不胜防，IT 时报，2018,8,6；

[4] 胡祥义 一种安全高效的区块链实现方法，专利申请号：201810786886.5 ，2018、7、18；

[5] 胡祥义，赵桂芬，马彦姣.一种可信移动支付解决方案.网络安全与技术[J].2016,4；