一种基于散列链的高效微支付系统*)

程文青[1] 郎为民[1,2] 杨宗凯[1] 谭运猛[1]

(华中科技大学电子与信息工程系 武汉430074)[1] (通信指挥学院 武汉430010)[2]

摘 要 本文提出了一种基于散列链的微支付系统,它是一种离线的预支付系统,数字货币的可转移性,允许用户将未花费的数字货币转让给其它用户。同时,本方案是公平的,它使交易双方的利益都得到了很好的保护。与其它微支付方案(如PayWord)相比,由于本系统完全没有使用公开密钥算法,因而效率大大提高。此外,系统还为用户提供了有限的匿名性。

关键词 微支付,散列链,PayWord

An Efficient Micropayment System Based on Hash Chain

CHENG Wen-Qing[1] LANG Wei-Min[1,2] YANG Zong-Kai[1] TAN Yun-Meng[1]

(Department of Electronic and Information Engineering, Huazhong University of Science and Technology, Wuhan 430074)[1]

(University of Communication Commanding, Wuhan 430010)[2]

Abstract In this paper, we propose an off-line, prepaid micropayment system based on hash chain, which supports transferability of digital coins in a simpler way. Moreover, in our system, a hash chain remaining unspent can be transferred by one user to the other and the profits of both consumers and merchants are protected, so the fairness of our system is high. Compared with other micropayment schemes, e.g. PayWord, no public-key operation is required, which improves the efficiency of our system. In addition, restricted anonymity is provided in our system.

Keywords Micropayment, Hash chain, PayWord

1 引言

微支付作为数字货币的一种支付形式,是目前电子支付发展的一个新方向,它能够较好地满足信息商品或服务的需求。与大额支付相比,它的每一笔交易额非常低,在满足安全性的前提下要求系统简单高效。按照付款类型,微支付可分为基于借记(预付)和基于信用(或后付)两种模式。预付模式要求用户首先在经纪人处购买一定数量的数字货币(一般是针对特定商家的),在交易时用户将该货币支付给商家,最后由商家通过与经纪人执行存款协议完成交易的清算和转账。这种形式的微支付方案包括MicroMint[3,7]和Millicent[5,8],等。而PayWord[2,7]和Mini-Pay[1]则是两个典型的基于信用(或后付)的微支付方案。在这种支付模式中,由于用户在付款之前已获取了商家所提供的信息商品或服务,因而对于用户的重复花费(同一数字货币在不同商家使用多次)和超支消费(所购买信息商品或服务的总价值超过其真实账户的余额或信用上限)没有良好的防范措施。Buttyán[4]提出了一种去除微支付欺诈行为商业动机的方案,但该方案没有提供真正的公正性,只是使得进行欺诈行为的用户或商家变得无利可图,且在同样支付条件下,该方案需要的散列链长度是PayWord的两倍,用户生成散列链及商家和经纪人验证散列链时的计算量也比PayWord多一倍,因而效率不高。Yen等[9]提出一个能够保证客户公正性的微支付系统PayFair,它是一个预付方案,通过经纪人在线验证每次交易中支付指令的合法性来防止用户进行重复花费和超支消费,但经纪人可能会成为系统性能的瓶颈,且由于该系统经纪人是在商家向用户提供商品或服务之前进行转账的,因而存在着商家欺诈的可能。ADACHI等[6]在对PayWord方案的安全问题进行分析后,给出了防止欺诈行为的限制条件,但并没有从根本上解决原方案存在的问题。

本文提出了一种基于散列链的新型公正微支付系统,它是一种离线的预支付系统,支持数字货币的可分性,并允许用户使用同一个散列链与多个商家进行交易。与其它微支付方案(如PayWord)相比,其显著特征就是由于本系统完全没有使用公开密钥算法,因而其效率比较高。此外,系统还为用户提供了部分的匿名性。

本文第2节介绍相关的符号及其定义;第3节全面描述我们所提出的基于散列链的新型公正微支付系统;第4节详细分析了系统的有关性能;最后对全文进行总结并给出结论。

2 符号描述和基本定义

本文所涉及到的符号和参数的意义描述如下:

$\|$:字符串连接运算符;ID_B:经纪人的身份标识;IDU:用户的匿名标识;Av:商家V的网址;ID_{V_k}:商家V_k的身份标识;K_{UB}:用户和经纪人共享的秘密密钥;K_{UV}:用户和商家共享的一次性秘密密钥;K_{M_kB}:商家M_k和经纪人共享的秘密密钥;$\{M\}k_{ij}$:使用秘密密钥K_{ij}对消息M进行加密;$H(\cdot)$:碰撞自由的单向散列函数;$H^r(W_N)$:对W_N进行r次散列运算

*)基金项目:国家自然科学基金资助项目(90104033)。程文青 副教授,研究方向为网络安全和下一代互联网。郎为民 博士研究生,讲师,研究方向为电子支付、信息安全和应用密码学。杨宗凯 教授,博士生导师,研究方向为电子商务、远程教育和网络安全。谭运猛 博士,副教授,研究方向为电子支付、信息安全和应用密码学。

的结果，即 $H^r(W_N)=\underbrace{H(H(\cdots(H(W_N))\cdots))}_{r次}$。

3 基本模型和协议

微支付的特征是能够处理任意小量的钱，通常用于特别小的网络交易，精确度甚至可以达到十分之一美分，适合于因特网上“不可触摸商品”(或虚拟商品)的交易。本文所提出的微支付模型如图1所示，它涉及到用户(User)、商家(Vendor)和经纪人(Broker)三方。

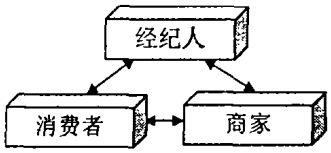

图1 微支付系统模型

其中，用户 U 是使用数字货币购买信息商品或服务的主体，商家 V 是为消费者提供商品或服务并接受消费者支付的网上商店，经纪人 B 在方案中相当于经纪人的角色，它作为用户和商家之间的中介，能够为用户和商家开立并维护账户、认证交易双方的身份、进行货币销售和交易结算，并协调解决可能引起的争端。

微支付系统的主要特点是：交易额非常小，交易成本低，在满足一定安全性的前提下，要求它有尽可能少的信息传输、较低的管理和存储需求，即速度和效率要求比较高。其安全性主要是通过审计或管理策略来保证，一般适用于交易费用相当低或手续简便的系统。

3.1 开户协议

用户选择一个匿名标识 ID_U，该标识与用户的真实身份没有必然联系。用户将 ID_U 发送给经纪人，同时向经纪人出示其身份证或护照等来唯一标识其身份。经纪人验证其证明，为其开立并维护一个账户，然后在用户账户数据库中存储该用户的身份识别信息及 ID_U，从而将 ID_U 与用户的身份信息绑定在一起。同时，用户与经纪人共享一个秘密密钥 K_{UB}。

商家也必须在经纪人处开户，他将 ID_V 作为其身份标识发送给经纪人，同时向经纪人出示其营业执照和网址 A_V 等来唯一标识其身份。经纪人验证其证明，为其开立和维护一个账户，并在商家账户数据库中存储该商家的身份识别信息 ID_V 和网址 A_V，从而将 A_V 与商家的身份识别信息 ID_V 绑定在一起。同样，商家也与经纪人共享一个秘密密钥 K_{VB}。

3.2 取款协议

为使用户具有一定的支付能力，用户的账号上必须具有足够的余额，并保证其账户处于良好的状态且没有任何使用限制。

(1)用户通过浏览商家的站点选择需要购买的商品或服务，并记录商家的网址 A_V 及商品或服务的价格，生成订单信息 OI，它包含购买商品或服务的种类、数量和总金额等信息。用户发送一个取款请求给经纪人，取款请求的格式如下：

$(ID_U, ID_B, A_V, OI)K_{UB}$

(2)经纪人首先验证取款请求的合法性(他知道秘密密钥 K_{CB})，并根据订单信息中的总金额决定生成散列链的长度 N。如果交易额为40美分且每个散列值代表的面额为1美分，则需要产生一个长度为40的散列链。经纪人选择一个随机数 W_N(称为散列链的根)，根据公式

$W_i=H(W_{i+1})$

对 W_N 进行 N 次散列计算，其中 $i=N-1, N-2, \cdots, 1, 0$。这样经纪人就生成了一个散列链 $\{W_N, W_{N-1}, \cdots, W_1, W_0\}$，$W_0$ 称为该散列链的锚，其中每个散列值代表一个货币单位。

(3)经纪人产生一个取款响应，同时为用户和商家产生一个一次性会话密钥 K_{UV}，并将其发送给用户，消息格式如下：

$(K_{UV}, N, W_N, W_0, Expiry)_{K_{UB}}$

其中 $Expiry$ 为数字货币的有效期。经纪人将 N，W_0，$Expiry$ 和 W_N 存储数据库中，并从用户账户上扣除与散列链数额相当的资金。

(4)经纪人发送如下授权消息给商家。

$(ID_U, ID_B, K_{UV}, N, W_0, OI, Expiry)_{K_{VB}}$

商家验证授权消息的合法性，并保存 N，W_0，$Expiry$，OI 和 ID_U。

3.3 支付协议

当用户从经纪人处取得足够的数字货币时，他通过如下支付协议与商家进行交互，共同完成整个交易过程。

(1)用户根据公式 $W_i=H(W_{i+1})$，对 W_N 进行 N 次散列计算，其中 $i=N-1, N-2, \cdots, 1, 0$。并将结果与 W_0 比较，验证数字货币的合法性，并发送如下支付指令给商家：

$\{ID_U, ID_B, N, W_N, OI\}_{K_{UV}}$

(2)商家首先进行支付指令合法性的检查，然后遍历其数据库，根据支付指令中的 ID_U 检查是否存在对应于该用户的经纪人授权信息，观察该数字货币是否过期，并验证

$H^N(W_N)\stackrel{?}{=}W_0$

若验证通过，商家将信息商品或服务提供给用户。

3.4 存款协议

商家通过执行如下的存款协议可以将用户提交的数字货币在经纪人处进行兑现。

(1)一段时间(如一天)后，商家将根据用户的支付指令生成存款请求信息：

$(ID_C, ID_M, W_N, N)_{K_{VB}}$

(2)经纪人首先检查数字货币是否过期，并通过将存款请求信息中的元素与数据库中存储的相应数据项对比和计算，验证其合法性。如果验证通过的话，则经纪人将与散列链数额相当的资金转移到商家的账户上，并将数据库中用户条目中的 W_0，$Expiry$ 和 W_N 删除。

4 系统性能分析

在本节中，我们将 PayWord 方案同本文提出的系统进行详细的比较，以说明系统的实用性和高效性。

4.1 可转移性

在本文提出的微支付方案中，数字货币是可以转移的。用户可将花费剩余的数字货币转让给其他人。假设经纪人生成的 N 个散列值被用户花费后，还剩余 N' 个，需要转让的用户 C 身份标识为 ID_C(用户 C 在经纪人处开立了账户且与经纪人共享一个秘密密钥 K_{CB})，用户 C 准备使用此散列链与商家进行交易，则用户 U 将发送如下货币转让请求给经纪人，其格式如下：

$\{ID_U, ID_C, N', W_N \cdots, ID_V \cdots, W_0\}_{K_{UB}}$。

经纪人为用户和商家产生一个一次性会话密钥 K_{CV}，并将其作为货币转让响应消息发送给用户 C，其格式如下：

(下转第91页)

县的电子政务构架中得到了验证和应用，并取得了良好的效果。

参考文献

1 张清浦. 西部大开发与政府 GIS[J]. 测绘科学，2000，25(2)：37～42
2 陈拂晓. 电子政务与标准化一我国电子政务建设面临的机遇与挑战. 信息技术与应，2003，(1-2)：14～17
3 张震. 网格技术及其在电子政务平台中的应用[J]. 电子技术，2003，7：22～23
4 王卫军，付晓江. 基于三层体系结构电子政务系统的 JSP 技术[J]. 吉林大学学报(信息科学版)，2003，21(1)：87～91
5 曾喻江，谢自美，盛翊智. 电子商务网站中的三层体系结构[J]. 信息技术，2001，11：32～34
6 王映辉，冯德明. 大规模软件构架技术[M]. 科学出版社，2003
7 王映辉. 分布构件模型技术比较研究[J]. 计算机应用研究，2003(7)
8 王映辉. 基于 Web 的应用程序构造模式比较研究[J]. 计算机科学，2003(7)

(上接第87页)

$(K_{CV}, N', W_{N'}, W_0, Expiry)_{K_{CB}}$

经纪人将 N'，W_0，$Expiry$ 和 $W_{N'}$ 存储在数据库中，并从用户 C 账户上扣除与散列链数额相当的资金，并将其转移到用户 U 的账户上。同时，经纪人发送如下支付授权消息给商家。

$(ID_C, ID_B, N', W_0, K_{CV'}, Expiry, OI)_{K_{V'B}}$

商家验证授权消息的合法性，并保存 N'，W_0，$W_{N'}$，$Expiry$，OI 和 ID_C。支付与存款过程可参照前节有关协议。

PayWord 方案中没有提及可转移性，消费者生成的 PayWord 链通常都是针对特定商家的，且不能将其转让给其他用户。

4.2 公平性

本文所提出的系统预付系统，它假定经纪人是诚信的，消费者在获得商品或服务之前将相应的资金支付给经纪人，因而商家和经纪人的利益得到了很好的保障。交易所需散列链是由经纪人产生的，消费者的超支消费问题也得到解决。同时，由于在和消费者进行交易前商家需要经纪人的授权信息，并能够通过遍历数据库验证消费者支付指令的合法性，在支付结束时删除对应于该消费者的经纪人授权信息，从而有效地防止了消费者进行重复花费。综上所述，本文所提出的系统对于客户和商家都是公平的。

而 PayWord 方案并没有为参与交易的各方提供真正的公正性。在 PayWord 方案中，由于它是基于信用的，消费者在付款之前已获取了商家所提供的信息商品或服务，因而存在着消费者的重复花费和超支消费等欺诈行为，对于经纪人和商家都是不公平的。

4.3 安全性

由于每次支付执行时，交易信息都是使用共享密钥进行加密的，因此攻击者无法获取相关的敏感信息，也无法伪造合法的电子现金。同时，商家无法进行重复存储，由于存款协议执行结束时，经纪人已将数据库中用户条目中的 W_0，OI，$Expiry$ 和 W_N 删除且商家不知道 C 和 B 共享的秘密密钥 K_{CB}，因而无法通过经纪人的合法性检验。由前面的分析可知，本系统同样能够防止用户进行重复花费和超支消费。

PayWord 系统中支付承诺是使用用户的私钥进行签名的，且由于散列函数具有单向不可逆性，因而能够有效防止攻击者的伪造和非法花费。经纪人通过数据库的形式存储某一支付承诺及其对应的已花费的 PayWord，能够有效地防止用户重复花费和商家的重复存储。

4.4 效率分析

在本系统中，用户不需要经纪人签名的证书，而仅仅需要与经纪人共享一个秘密密钥 K_{CB}，用户的支付承诺(用户对支付指令的签名)转换为用户使用对称密钥对支付指令进行加密。在协议执行过程中，散列运算的次数基本上与 PayWord 相同，且商家和经纪人保存的信息也很简单，并在协议执行完成后即可进行删除，因而计算开销和存储开销大大减少。在 PayWord 方案中，每个用户需要一个由经纪人签名的数字证书，且在每次支付时，都需要用户签名生成一个支付承诺，用户、经纪人和商家都需要进行 N 次散列运算。为防止用户进行重复花费，经纪人和商家需要记录和保存最后一次消费的有效 PayWord、支付承诺及数字证书等信息，计算开销和存储开销较大。所以，本文所提出的微支付系统，由于完全没有采用公钥密码算法，其效率大大提高。

4.5 有限的匿名性

由于只有经纪人知道用户的匿名标识和真实身份之间的对应关系，因而在与商家进行交易时，商家不能获知用户的身份信息，所以系统为用户提供了有限的匿名性。在 PayWord 方案中，由于经纪人颁发给用户的数字证书中包含了用户的身份信息，因而系统没有提供匿名性服务。

结论 本文设计了一个基于散列链的高效微支付系统。该系统是一个离线的预付系统，它采用秘密密钥加密体制及相关的安全手段来防止用户的重复花费、超支消费和商家的重复存储，为参与交易的各方提供了安全保障。与现有的微支付方案相比，由于它完全没有采用公钥密码算法，且协议执行中所需保存的信息比较简单，因而系统的计算开销和存储开销大大减少。此外，由于系统允许用户在开户时使用匿名标识，该标识与用户的真实身份没有必然联系，在进行交易时，商家无法获知用户的身份信息，因而系统提供了有限的匿名性。

参考文献

1 Herzberg A, Yochai H. Mini-Pay: charging per click on the Web. In: Proc. of the 6th Intl. World Wide Web Conf. Santa Clara, California, April 1997. 301～307
2 Azbel. PayWord micro-payment scheme: strengths, weaknesses and proposed improvements. Department of Computer Science, University of Cape Town, South Africa, 1997
3 Burstein J. An implementation of MicroMint: [M. Sc thesis]. Massachusetts Institute of Technology, Cambridge, Massachusetts, May 1998
4 Buttyán L. Removing the Financial Incentive to Cheat in Micropayment Schemes. IEE Electronics Letters, 2000, 36(2): 132～133
5 Manasse M. The Millicent protocols for Electronic Commerce. In: Proc. 1st USENIX Workshop on Electronic Commerce, New York, 1995. 117～123
6 Adachi N, Aoki S, Komano Y, et al. The Security Problems of Rivest and Shamir's PayWord Scheme. In: Proc. of the IEEE Intl. Conf. on E-Commerce (CEC'03), 2003. 126～129
7 Rivest R L, Shamir A. PayWord and MicroMint: two simple micropayment schemes. Lecture Notes Comput. Sci., 1997, 1189: 69～87
8 Glassmann S, Manasse M, Abadi M, et al. The Millicent protocol for inexpensive electronic commerce. In: Proc. of the 4th Intl. World Wide Web Conf. Boston, MA, 1995. 603～608
9 Yen S, Lee C, Ho L. PayFair: a prepaid Internet micropayment scheme promising customer fairness. In: IEE Proc. of Comput. Digit. Tech., 2001, 148(6): 207～213