电子支付协议的原子性研究综述*)

刘义春　张焕国　王丽娜

(湖南理工学院　岳阳414006)　(武汉大学软件工程国家重点实验室　武汉430072)

摘　要　原子性是设计电子支付协议时应考虑的重要性质。文章介绍了电子支付系统的原子性概念,分析了一些重要电子支付协议的原子性,论述了原子性电子支付协议的实现策略,描述了两个著名的原子性电子支付协议——NetBill和Anonymous Atomic Transaction Protocol的协议实现,基于两阶段提交策略提出了一种新的原子性实现方法并用于构造原子性电子合同签署协议,就复杂电子交易模式的原子性支付问题进行了探讨,指出了电子支付原子性研究的最新发展和亟待解决的公开问题。

关键词　电子支付,原子性,两阶段提交,匿名性

Survey of Atomicity in Electronic Payment Protocol

LIU Yi-Chun　ZHANG Huan-Guo　WANG Li-Na

(Hunan Insitute of Science and Technology, Yueyang 414006)

(State Key Laboratory of Software Engineering, Wuhan University, Wuhan 430072)

Abstract　Atomicity is one of the most important property of electronic commerce payment. In this paper, the basic concept of atomicity in electronic commerce transaction is introduced. The atomicity of some important payment protocols is analysed. The technical strategies of implementing atomic electronic payment protocol are discussed. The implementation of two famous atomic payment protocol, NetBill and Anonymous Atomic Transaction Protocol, are described detailedly. A new method for realizing atomicity is presented and used to design a atomic electronic contract signing protocol utilizing two-phase commitment with introduction of Trsted Third Party. The atomicity problem about complex electronic exchange mode is explored. The new developments about researches of atomicity of electronic payment are pointed out.

Keywords　Electronic payment, Atomicity, Two-phase commitment, Anonymity

1　引言

随着Internet在全球的普及,电子商务的普遍应用成为大势所趋,电子支付技术已成为电子商务发展的主要瓶颈。近年来,人们根据不同电子支付方式,运用密码学等先进技术,提出了诸多支付协议。加密解密技术用于保障电子商务交易时信息流的秘密性;签名技术和Hash方法用于保障交易信息流的真实性、完整性;时间戳或临时值用于保障交易的时效性;D. Chaum[1]提出的盲签名技术则满足了一些电子商务交易中用户的匿名性要求。

Carnegie Mellon大学的J. D. Tygar于1996年正式提出电子支付的原子性概念[2],以进一步规范电子支付中的资金流、信息流和物流,并提出用模型检测工具FDR和CSP逻辑对电子支付协议进行原子性分析[3]。B. Cox和J. D. Tygar引入一个可信第三方,提出了具有原子性电子支付协议NetBill[4]。针对DigiCash等匿名数字现金协议不能满足原子性,J. Camp和J. D. Tygar引入可信第四方——交易日志L,给出了兼有匿名性和原子性的电子支付协议Anonymous Atomic Transaction Protocol[5]。G. Wang和A. Das提出了复杂交易模式中的原子性问题[6]。针对多个商家的交易情形,H. Schuldt和A. Popovici进一步提出了分布式购买原子性[7]的概念。K. Adi和M. Debbabi针对借记/贷记卡交易提出了一种形式化逻辑[8],以分析电子支付协议的原子性。国内一些学者也针对电子支付的原子性,从不同侧面进行了很多研究。

2　电子商务交易的原子性

2.1　原子性的概念

原子性概念源于数据库理论,指对数据库操作的一个逻辑单元,由一系列操作组成,事务将数据库从一个一致的相容状态(Consistent State)转换为另一个一致的相容状态:

```
〈Transaction Begin〉
  State-changing operation 1;
  State-changing operation 2;
  ……
  State-changing operation n;
〈Transaction End〉
```

这组操作执行时,要么n个操作全部成功执行,状态一致发生变化;要么整个操作都不会引起任何状态变化,似乎n个操作全都从未发生。

分布式系统中,原子性已成为分布式事务处理的标准机制。分布式事务成功进行当且仅当所有子事务成功执行,以避

*)国家自然科学基金重点项目(No. 90104005, No. 90204011, No. 60373087);教育部博士点基金(No. 200220486046);湖北省自然科学基金重点项目(No. 2002AB0039)。刘义春　博士研究生,研究方向为网络安全和电子商务;张焕国　博士生导师,研究方向为计算机通信安全;王丽娜　教授,研究方向为计算机网络安全。

免整个系统处于不确定的中间状态。

保障分布式处理的基本方法是两阶段提交协议(two-phase commit)。在两阶段提交协议中,由一个事务协调者,知道并记录事务中各方身份。每一方在事务开始前记录自身状态。事务进行后,各方完成各自的计算或通信子事务。各方在改变自身状态前,给协调者发出一准备提交的消息。如果协调者收到了所有参与方的提交请求,协调者将给各方广播事务提交命令,各方均改变自身状态;如果有某一方给协调者发送中止事务请求,或协调者与其中某一方失去联系,则协调者通过广播中止事务命令取消整个事务,各方回到事务发生前的状态。

2.2 电子商务中的原子性

J. D. Tygar 于1996年把原子性概念引入电子商务[2],并把电子支付的原子性分为三级,呈向上兼容,后者包含前者。

① 钱的原子性(Money Atomicity):电子商务交易发生前后资金守恒,资金在电子支付中既不会创生也不会消失,客户钱的减少等于商家的增加。

② 商品原子性(Goods Atomicity):首先,满足商品原子性的协议一定满足钱原子性;其次,保证客户收到商品当且仅当对应商家获得付款。

③ 确认发送原子性(Certified Delivery):首先,满足确认发送原子性的协议一定满足钱原子性和商品原子性。其次,需要对客户从商家购得的商品和商家付给客户的商品分别进行确认,保证客户得到他所订购的商品(包括品质)。如果有争议,拥有仲裁依据来证实到底何种商品被传送。

容易看出,J. D. Tygar 的三种原子性没有涵盖电子合同的范畴。为了进一步规范电子合同的签署,我们提出合同原子性的概念。

④ 合同原子性(Contract Atomicity):合同签署结束后,合同中的双方要么都得到了有效签署的合同,要么都未得到有效签署的合同,不存在一方得到有效签署的合同而另一方不能得到有效签署的合同的情况发生。

2.3 非原子性电子支付协议

2.3.1 Digicash 是著名的电子现金系统。Digicash 基于 D. Chaum 提出的盲签名协议[1],保证电子现金的匿名性。协议如下:

① 客户从银行得到盲签名的代币,去盲因子。

② 客户把代币传送给商家。

③ 商家检验客户提交的代币,确认此前未使用。

④ 商家发货给客户。

⑤ 商家把代币传送给银行。

⑥ 银行检验该代币的唯一性。若唯一,则付款;否则顾客身份将被暴露。

上述协议中若执行第②步时出现通信故障,客户无法知道商家是否已收到代币。如果客户将代币退回银行或在其他商家另行购物,而商家实际上已收到代币并兑现存款,则客户身份将被揭露并受到指控。反之,如果客户不用此代币再次购物或在银行兑现,而商家又从未收到此币,则顾客将损失此代币。由此看出,DigiCash 协议不能满足钱的原子性。

2.3.2 SSL SSL 协议采用 DES、MD5等加密技术实现数据机密性和完整性,并采用 X.509数字证书实现鉴别,可保证信息传输中的安全。基于银行卡的 SSL 支付中钱币仅在银行间流动,因而满足钱的原子性。但缺少客户对商家认证,商家获得货款后可能抵赖而不肯发货,或发出品质不符的商品,SSL 不满足商品原子性。

2.3.3 SET 是 Visa 和 Master 开发的信用卡交易标准,有很好的安全性能,能保证支付信息的机密性、完整性、对商户及持卡人的身份验证。SET 交易中钱的流动由支付网关通知发卡行转账付款完成,交易前后资金守恒,因而满足钱的原子性。SET 协议不提供不可抵赖性,当客户付款后商家不发货或所发货物品质不符,协议无法退回(Roll-Back)至执行之初的状态,因而不支持商品原子性。

3 电子商务支付协议的原子性设计

3.1 构造协议原子性的基本方法

J. Su 给出了两种构造原子性电子支付协议的基本方法[9]:基于加密的原子性实现;基于授权的原子性实现。

在下面的描述中:S 为信息发送方,R 为接受方,A 为可信第三方,$\{goods\}_k$ 为用对称密钥 k 加密的信息产品,协议针对数字产品的交易。

3.1.1 *基于加密的原子性实现方法*

① $S \rightarrow R: \{goods\}_k, TID$

② $R \rightarrow S: Sig\{goods\}_k, TID$

③ $S \rightarrow A: k, TID$

④ $S \rightarrow R: k, TID$

如果第③步或之前出现通信故障,S 未将 k 传送给 R,R 无法得到 goods,相当于交易未发生。如果第③步之后出现通信故障,R 将可从 A 处获得 k。第②步中传送的 $Sig\{goods\}_k$ 实际上是 R 收到 goods 的收据。若此后出现争议,可用 $Sig\{goods\}_k$ 向第三方证明 goods 的真实性。

3.1.2 *基于授权的原子性实现方法* 基于授权的原子性实现使用可信第三方 A 作为通信代理,从而实现交易原子性。

① $S \rightarrow A$: goods, R, TID

② $A \rightarrow R$: "message available", TID

③ $R \rightarrow A$: "send me the goods", TID

④ $A \rightarrow R$: goods, TID

J. Su 的两种原子性实现方法用于数字商品交易,不适宜于合同签署等事务。基于授权的原子性实现要求支付服务器保存整个商品的内容,负荷远大于基于加密的原子性协议。

3.1.3 *基于单向函数值提交的原子性实现方法* 在一个公平的电子合同签署中,交易双方常常相互发送含有单向函数值作为公共提交(Public Commitment)的信息,而后发送作为函数变量的随机值以保障合同签署的公平性和不可抵赖性。前面 J. Su 的两种方法不能有效实现电子合同的原子性。为保证电子合同签署的原子性,我们提出如下基于单向函数值提交方法的原子性实现策略:

① $S \rightarrow R: com_1 = F(N_1)$

② $R \rightarrow S: com_2 = F(N_2)$

③ $S \rightarrow A: com_2, N_1$

$R \rightarrow A: com_1, N_2$

④ $A \rightarrow S: N_2$

$A \rightarrow R: N_1$

本实现方法只需可信第三方(协调者)用单向函数 F 验证随机值的正确性,计算负荷较小。

与 J. Su 的两种原子性实现方法不同,这种新的方法可用来有效解决电子合同的原子性问题。

3.2 NetBill 协议

B. Cox 和 J. D. Tygar 于1995年提出电子支付协议 NetBill[4]，该协议基于加密的原子性方法，引入一个可信第三方——支付服务器 NetBill Server，代替两阶段提交协议中的协调者。

NetBill 协议流程如下：

① 客户 C 向商家 M 发出购物请求。

C→M：T_{CM}(Identity)，E_{CM}(Credentials，，PRD，Bid，RequestFlags，TID)

② M 向 C 报价(价格清单)

M→C：E_{CM}(ProductID，Price，RequestFlags，TID)

③ C 表示接受该报价，并请 M 传送商品

C→ M：T_{CM}(Identity)，E_{CM}(TID)

④ M 发送加密的数字商品 Goods

M→C：E_K(Goods)，E_{CM}(CC(E_K(Goods))，EPOID)

⑤ C 生成一个电子采购订单 EPO，数字签名后发送给 M

C→ M：T_{CM}(Identity)，E_{CM}($[EPO]_C$)

⑥ M 对收到的$[EPO]_C$及密钥 K 进行数字背书并发送至支付服务器 N

M→N：T_{MN}(M)，E_{MN}($[[EPO]_C$，MAcct，Mmemo，K$]_M$)

⑦ N 确认 EPO 信息有效性，检验客户账号，然后生成一个含有结果码、各方身份、交易价格、商品描述、EPOID、密钥 K 的收据，使用 DSA 签名后发送给商家，并将客户购款划拨商家账户。

N→M：E_{MN}($[Recipt]_{N\text{-}DSA}$，E_{CN}(EPOID，CAcct，Bal，Flags))

⑧ M 验证收到的信息，并将⑦中收到的信息转发 C。

M→C：E_{CM}($[Recipt]_{N\text{-}DSA}$，E_{CN}(EPOID，CAcct，Bal，Flags))

⑨ C 解密$[Recipt]_{N\text{-}DSA}$，得到 K，用其对先前收到的 E_K(Goods)解密，得到信息商品。

步骤①、②可重复多次直至客户和商家达成一致价格。

NetBill 协议中，利用一个各方都信任的支付服务器，客户与商家账户均存于支付服务器中，资金转移均发生在支付服务器中，因此保证了钱的原子性。

NetBill 协议的资金转移和数字商品密钥发送均发生在第⑦步。若之前支付系统出现故障，则不会发生资金转移，客户也不会获得解读数字商品所需的密钥。若此后出现故障，则商家已获得货款，而客户也可以后从商家或支付服务器处获得密钥。商品原子性得到保证。

若客户认为商品品质与所订不符，可将 E_K(Goods)递交支付服务器。EPO 经客户及商家先后背书，并已存于服务器处，EPO 中含 CC(E_K(Goods))项，仲裁者可由此用密钥 K 解密 E_K(Goods)并裁定商品是否为客户所订商品。协议满足确认发送原子性。

3.3 匿名原子交易协议

J. Camp 于1996年提出了匿名原子交易协议(Anonymous Atomic Transactions)[5]，该协议基于加密的原子性策略，引入除客户 C、商家 M、银行 B 外的第四方——交易日志服务器 L(Transaction Log)，代替两阶段提交协议中的协调者，解决数字商品交易中的原子性问题。

交易协议如下：

① M→C：$(n,contract,E_k(goods))_m$

② C→B：$(n,expiration,M,L,Q^*)_q$

③ B→M：$(n,expiration,M,L,value)_b$

④ M→L：$(n,expiration,k)_m$

⑤(a) L：$((n,expiration,k)_m)_L$或

(b) L：$((n,expiration,M,failed)_m)_L$。

代币 Q^*经过银行盲签名。(Q,q)为客户的公钥/私钥对。

第①步商家发送已签名交易号 n、商品描述 contract 及用对称钥 K 加密的 goods 给客户。

第②步中银行检验 Q^*的有效性和是否被重用，银行和商家有权否决客户对截止日期 expiration 和 L 的选择。

第③步中银行通知商家准备提交，商家确认 n、L、expiration。Value 为 Q^*的币值。

第④步中商家向 L 发送 K、expiration 和 n，进行交易提交。L 验证是否已超时。

第⑤步为系统的提交阶段，L 记录商家的提交当且仅当在有效期内收到商家提交。提交时向客户、商家和银行发送提交消息 Commit。任何一方均可使用交易日志的记录。如果出现超时，L 向客户、商家和银行发送夭折消息 Abort。

客户收到 Commit 消息后可用 K 解密数字商品。若收到 Abort 消息，代币可重用。

银行收到 Commit 消息后将代币置为已花费，其值划拨至商家账户。若收到 Abort 消息，代币解锁置为未花费。

商家若收到 Abort 消息，客户得不到解密钥 K，无法得到 Goods，商家账户未获得货款。

如果客户解密后的 Goods 不符合要求，用户用(n，contract，E_k(goods))$_m$ 和 Commit(内容为$((n,expiration,k)_m)_L$)向商家索赔或投诉。

协议满足钱的原子性、商品原子性和单向确认发送原子性。

3.4 原子性电子合同签署协议

电子合同是电子商务的一个重要方面。一个典型的传统电子合同签署协议如下：

① A→B：m_1=SigA(A，B，text，com_A)

其中 com_A= h(N_A)

② B→A：m_2=Sig_B(m_1，com_B)

其中 com_B= h(N_B)

③ A→B：m_3=N_A

④ B→A：m_4=N_B

A、B 为签订电子合同的双方；text 为电子合同内容；临时值 N_A、N_B 分别由 A、B 随机产生；一个有效合同为多元组｛m_1，N_A，m_2，N_B｝。

如果第③步、第④步中 A 或 B 发送错误的 N_A、N_B，其中一方将得到有效的电子合同，而另一方将不能得到有效的电子合同。

利用基于单向函数值提交方法的原子性实现策略，引入可信第三方 T 作为协调方，我们给出如下原子性电子合同签署协议：

① A→B：m_1=Sig_A(A，B，T，text，com_A)

② B→A：m_2=Sig_B(m_1，com_B)

③ A→T：m_3= A，B，N_A，com_B

B→T：m_4= B，A，N_B，com_A

④ If com_A= h(N_A) and com_B= h(N_B) then

T→A：m_5=B，N_B

T→B：m_6=A，N_A

Else

T→A,B:canceled

协议执行时,不存在仅有某一方得到有效合同或一方进行欺诈的结果,要么双方均能得到有效签署的合同,要么都不能得到合同的签署。协议满足原子性。

上述原子性电子合同协议满足原子性,且此原子性因不涉及钱的原子性,因而不同于 J. D. Tygar 所提出的三种原子性。

4 复杂电子商务支付的原子性分析

目前多数电子支付协议皆针对较为简单的交易情形,如单一的客户、商家、银行、第三方或第四方,与传统贸易中交易的多样性要求甚远,不能适应较为复杂的交易情形。前面涉及的几种支付协议均针对简单情形的电子商务交易。

4.1 复杂电子商务交易模式

G. Wang 和 A. Das 对复杂情形电子商务交易进行了分析[6],提出了如下几类交易模式:

① 链型交易模式 CTM(Chained Transaction Model):理论上有无限参与方参与整个交易。这些参与方中,存在一个作为最终买主的客户和一个终端供应商。其他参与方皆为中间经纪人,他们买入商品然后再卖出该商品。

② 组合交易模式 ATM(Aggregate Transaction Model):客户从不同销售商处购买多种商品,因缺少某些商品而导致的商品的不完整交易对客户而言没有价值。客户要么购买所有商品要么一件也不购买。

③ 可选交易模式 OTM(Optional Transaction Model):客户从若干可选的销售商处购买一件商品。客户可并发地进行多项交易,但最终只有其中之一能提交。

④ 捆绑交易模式 BTM(Bundled Transaction Model):交易时厂商捆绑一些其他厂商的产品和服务,如广告、商品、包装或产品递送。在电子商务中,这种捆绑常常通过一个相对固定的合同而实现。

上述四类模式中,交易不仅仅在买卖双方间进行。一个完整的交易常包含若干子交易。

4.2 复杂电子商务交易的原子性

考虑复杂交易中的原子性,应避免出现下列问题:

① 中间经纪商从前一个卖主手中买入商品后不能卖给下一个买主,而出现交易风险。这种情形常出现在 CTM 和 BTM 中。

② 买主需要得到几种商品的组合,得到其中部分商品对他没有价值,但交易时却只能得到不完全的组合。这种情形可能出现在 ATM 中。

③ 买主希望从几个可选卖主中的一个卖主那里购入商品,结果同时向满足要求的几个卖主支付了货款。这种情形可能出现在 OTM 中。

为了避免这三种情形,我们对复杂电子商务交易的提交和终止给出如下原子性规则:

① 在所有子交易提交前,父交易不能提交。本规则防止在 ATM 中买主只买入部分商品,即不完全购买。

② 如果父交易中止,那么所有子交易应该被中止。此规则防止在 CTM 和 BTM 中问题①的出现。

③ 在 OTM 中,如果没有子交易被提交,那么父交易亦不能提交;如果有一个子交易已提交,那么整个交易提交。如果所有子交易夭折,那么整个交易才夭折。

④ 在 OTM 中,如果有任意一个子交易被提交,所有其他子交易应该被中止。此规则消除了 OTM 中问题③出现的可能性,保护买主以免重复付款。

为确保复杂交易系统的原子性,为每个操作定义两个提交阶段:局部提交状态和最终提交状态。为完成某交易的所需所有数据项被存储到一个可靠的硬件,能使交易能随时被最终提交或安全中止,此时为局部提交状态;买卖双方就商品和货款相互达成一致时,状态为最终提交状态。当且仅当所有所需的子事务局部提交时,一个事务就绪等待最终提交。

4.3 复杂电子支付协议

在复杂交易系统中,为确保协议原子性,语义上将支付流程分为3个阶段:

支付阶段:信息从买方流向卖方。卖方必须提供商品发送担保,而买方必须为交易的最后阶段背书。

商品发送阶段:有条件的商品发送保证信息沿交易树从卖方上溯至买方,每一级都有对应 TTP 作为担保者。商品发送阶段结束时,子交易被局部提交。在顶级交易的所有子交易已局部提交后,客户可决定最终提交整个交易,进入最终提交阶段。

最终提交阶段:所有子交易被从根结点到叶结点最终提交。对每一个操作,相关 TTP 把支付保证或商品发送保证转变为实际支付或商品发送。

实际生活中的电子商务交易大都不是简单的电子商务交易模式,复杂电子商务交易中的原子性问题是一个非常重要的研究课题,但从 G. Wang 和 A. Das 提出相关问题后,这方面尚未见到更多的研究。

我们认为,由于群签名允许组中合法用户以用户组的名义签名,具有签名者匿名、只有权威才能辨认签名者等特点,采用群签名技术设计原子性电子支付协议,可用于解决捆绑交易、组合交易、多客户团购、多银行支付等交易模式,还可确保客户对商家和银行的匿名性和不可追踪性。有序多重签名采用链状签名模式,链中每一节点验证前一节点签名的有效性后再签名,因而该技术也可用于实现链型模式的原子性支付。此外,代理签名技术亦可用于设计满足原子性的有条件匿名的电子支付协议。

5 进一步的研究方向

近年来,电子支付的研究发展非常迅速,各种支付协议层出不穷。与电子支付的匿名性、公平性等方面研究相比,电子支付的原子性研究仍显逊色。NetBill 协议和原子性的电子支付协议 Anonymous Atomic Transaction Protocol 只限于数字商品的简单交易模式,且受限于 NetBill Server 和交易日志 L,不能在较大范围内使用。其他的研究大都只提出了一些研究思路,未能给出有效的实现协议。

电子支付的原子性研究还有许多工作尚待进行,其中包括:

- 除钱原子性、商品原子性和发送确认原子性外,新的原子性概念的提出
- 如何将针对数字商品的原子性支付协议拓展至有形商品交易
- 针对借记/贷记卡交易的原子性研究
- 针对多银行和多个可信协调方的电子支付协议的原子性研究
- 针对多客户团购的电子支付协议的原子性研究

(下转第113页)

Publishing Co.,1993
3 Garlan D,Allen R,Ockerbloom J. Exploiting style in architectural design environments. ACM SIGSOFT Software Engineering Notes,1994,19(5): 175～188
4 Medvidovic N,Rosenblum D S,Taylor R N. A language and environment for architecture-based software development and evolution. In:Proc. of the 21st Intl. Conf. on Software Engineering (ICSE '99),1999. 44～53
5 Robbins J E,Redmiles D F. Software architecture design from the perspective of human cognitive needs. In:Proc. of the California Software Symposium (CSS'96),Los Angeles,CA,1996
6 Magee J,Kramer J. Dynamic structure in software architectures. In:Proc. of ACM SIGSOFT'96: Fourth Symposium on the Foundations of Software Engineering (FSE4), San Francisco, CA, 1996. 3～14
7 Honeywell. MetaH language and tools. http://www.htc.honeywell.com/projects/ dssa_tools/dssa_tools_mh.html
8 Luckham D C. Rapide: a language and toolset for simulation of distributed systems by partial ordering of events. DIMACS Partial Order Methods Workshop IV,Princeton University,1996
9 Shaw M,DeLine R,Klein D V,et al. Abstractions for software architecture and tools to support them. IEEE Trans. on Software Engineering,1995,21(4):314～335
10 Allen R. A formal approach to software architecture:[Technical Report,CMU-CS-97-144]. Carnegie Mellon University,1997
11 Garlan D,Monroe R,Wile D. ACME: an architecture description interchange language. In:Proc. of CASCON '97,Nov. 1997
12 朱雪阳,唐稚松. 基于时序逻辑的软件体系结构描述语言 XYZ/ADL. 软件学报,2003,14(4):713～720
13 梅宏,陈锋,冯耀东,杨杰. ABC:基于体系结构、面向构件的软件开发方法. 软件学报,2003,14(4):721～732
14 Jacobson I,Booch G,Rumbaugh J. The unified software development process. MA: Addison-Wesley,1999
15 Garlan D. Software architecture. Wiley Encyclopedia of software engineering,Marciniak J (Ed.),John Wiley & Sons,Ltd. 2001
16 Towards an ADL ToolKit. http://www-2.cs.cmu.edu/～acme/adltk/
17 Vestal S. A cursory overview and comparison of four architecture description languages:[Technical Report]. Honeywell Technology Center, 1993. http://www.htc.honeywell.com/projects/dssa/ftp/papers/four_adl.ps
18 Clements P C. A survey of architecture description languages. Eighth International Workshop on Software Specification and Design,Germany,Mar. 1996
19 Medvidovic N,Rosenblum D S. Domains of concern in software architectures and architecture description languages. In:Proc. of the 1997 USENIX Conf. on Domain-Specific Languages, Santa Barbara,California,1997
20 Medvidovic N, Taylor R N. A classification and comparison framework for software architecture description languages. IEEE Trans. on Software Engineering,2000,26(1):70～93
21 Kruchten P B. The 4+1 view model of architecture. IEEE Software,1995,28(11):42～50
22 Garlan D,Kompanek A. Reconciling the needs of architecture description with object-modeling notations. In:Proc. of the Third Intl. Conf. on the Unified Modeling Language - 《UML》2000, York,UK,Oct. 2000
23 Hofmeister C,Nord R L,Soni D. Describing software architecture with UML. In:Proc. of Working IFIP Conf. on Software Architecture,1999. 145～160
24 Robbins J E,Medvidovic N,Redmiles D F,et al. Integrating architecture description languages with a standard design method. In: Proc. of the 20th Intl. Conf. on Software Engineering,1998. 209～218
25 Medvidovic N,Rosenblum D S,Redmiles D F,et al. Modeling software architectures in the Unified Modeling Language. ACM Trans. on Software Engineering and Methodology (TOSEM), 2002,11(1): 2～57
26 OMG. UML2.0 superstructure specification. http://www.omg.org/cgi-bin/doc?ptc/2003-08-02 /03-08-02.pdf
27 Shaw M,Garlan D. Software architecture: perspectives on an emerging discipline. Prentice Hall,1996
28 Shekaran C,Garlan D,Jackson M,et al. The role of software architecture in requirements engineering. In: Proc. of the First Intl. Conf. on Requirements Engineering,Apr. 1994. 239～245
29 International Workshop. From Software Requirements to Architectures(STRAW'2003). http://se.uwaterloo.ca/～straw03/

(上接第96页)

·针对复杂电子商务交易模式,如何设计有效的原子性支付协议

·如何实现支付协议中匿名性和原子性的相容

·电子拍卖交易模式中的原子性研究

·证券交易和期货交易中的原子性研究

·电子慈善事务中的原子性研究

·利用原子性实现电子支付系统的容侵

·电子支付协议原子性的形式化分析

结论 原子性是电子支付协议中应考虑的一个重要特性,国内外已进行一些重要的探讨和研究,提出了一些解决思路和方法,但仍有待人们进行深一步研究。

本文介绍了电子支付的原子性概念,分析了一些重要电子支付协议的原子性,就原子性电子支付协议实现策略进行了探讨,提出了一种新的原子性实现方法并用于构造一个原子性电子合同签署协议,阐述了电子支付原子性研究的最新发展和亟待解决的问题。

参考文献

1 Chaum D. Blind Signatures for Untraceable Payments. In: Proc. Crypto'82, LNCS,Springer-Verlag,1983. 199～203
2 Tygar J D. Atomicity in Electronic Commerce. In: Proc. of the 15th Annual ACM Symposium on Principles of Distributed-Computing, May 1996. 8～26
3 Heintze N,Tygar J D,Wing J,Wong H C. Model Checking Electroinc Commerce Protocols. In:Proc. of the 2nd USENIX Workshop on Electronic Commerce, Nov,1996. 147～164
4 Cox B,Tygar J D,Sirbu M. NetBill Security and Transaction Protocol. In: Proc. of the First USENIX Workshop on Electronic Commerce, July 1995. 77～88
5 Camp L J,Harkavy M,Tygar J D,Yee B. Anonymous Atomic Transactions. In:Proc. of the 2nd USENIX Workshop on Electronic Commerce, 1996. 123～133
6 Wang G,Das A. Models and Protocol Structures for Software Agent Based Complex E-Commerce Transactions. Journal of Electronic Commerce 2001 , LNCS 2115, Berlin. Springer-Verlag, 2001. 121～131
7 Schuldt H,Popovici A,Schek H. Execution Gurantees in Electronic Commerce Payments. In:Proc. of the 8th USENIX Workshop on Transaction and Database Dynamics, LNCS 1773,Berlin. Springer-Verlag,2000. 193～202
8 Adi K,Debbabi M,Mejri M. A New Logic for Electronic Commerce Protocols. AMAST 2000, LNCS, 2000, 1816: 499～513
9 Su J,Tygar J D. Building Blocks for Atomicity in Electronic Commerce. In: Proc. of the 6th USENIX Security Symposium, July 1996. 97～104