Computer Science and Application 计算机科学与应用, 2021, 11(12), 3012-3018
Published Online December 2021 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2021.1112304

Hans汉斯

基于区块链的安全微支付协议

王星凯

天津工业大学计算机科学与技术学院，天津

收稿日期：2021年11月24日；录用日期：2021年12月20日；发布日期：2021年12月27日

摘　要

原有的基于PayWord的微支付方案存在第三方经纪人掌握支付双方信息并与某一方合谋攻击另一方的问题，使支付的安全性得不到保证。本文结合双支付链思想，基于区块链提出了一种新的微支付协议，用智能合约代替原有方案中的第三方经纪人，实现了去中心化，保证了支付的安全性；利用双支付链，支持多个元支付一次性执行，提高了支付的效率，同时设计了仲裁子协议，保证方案的公平性。通过对协议的分析表明，该协议不仅可以保证支付的安全性、公平性，同时具有较高的支付效率。

关键词

区块链，微支付，哈希链，智能合约

Secure Micro Payment Protocol Based on Blockchain

Xingkai Wang

School of Computer Science and Technology, Tiangong University, Tianjin

Received: Nov. 24th, 2021; accepted: Dec. 20th, 2021; published: Dec. 27th, 2021

Abstract

The original micro payment scheme based on PayWord has the problem that the third-party broker grasps the information of both parties and colludes with one party to attack the other party, so that the security of payment cannot be guaranteed. Combined with the idea of double payment chain and based on blockchain, this paper proposes a new micro payment protocol, which uses smart contract to replace the third-party broker in the original scheme, realizes decentralization and ensures the security of payment; the double payment chain is used to support the one-time execution of multiple unit payments, which improves the efficiency of payment. At the same time, the arbitration sub protocol is designed to ensure the fairness of the scheme. The analysis of the

文章引用: 王星凯. 基于区块链的安全微支付协议[J]. 计算机科学与应用, 2021, 11(12): 3012-3018.
DOI: 10.12677/csa.2021.1112304

protocol shows that the protocol can not only ensure the security and fairness of payment, but also has high payment efficiency.

Keywords

Blockchain, Micro Payment, Hash Chain, Smart Contract

1. 概述

传统的支付过程是纸质的，往往在买家、卖家和银行三方之间进行。但随着互联网和电子商务的飞速发展，电子支付也随之发展成熟。在电子支付中，不可避免地会出现很多小额支付，如购买在线音乐、按页购买资料、按次付费等场景，这些支付金额可能是很小的，这种情况下，电子支付本身的计算成本可能已经超过本次支付的价值了。为了解决这个问题，人们提出了许多微支付协议或方案，其中人气较高且使用较广泛的微支付协议是由 Rivest 和 Shamir 提出的 PayWord [1]。许多有效的微支付方案都是基于 PayWord 思想进行研究和改进的，这些微支付方案都需要可信的第三方经纪人，但实际情况是我们不得不考虑第三方经纪人的诚实性。经纪人往往掌握着支付双方的个人信息且负责资金结算，如果经纪人有恶意，很容易就能和买卖双方中其中一方合谋攻击另一方，造成被攻击方个人信息泄露或利益受损。

近年来，随着区块链技术的发展，许多行业都在积极探索并推进区块链技术与本行业进行结合，如供应链[2] [3]，医疗保健[4] [5]，数据交易[6] [7]等。同样的，区块链技术也为原有微支付方案中存在的问题提供了新的解决思路。

本文提出了一种基于区块链的新型微支付协议，该协议基于区块链，借鉴双支付链[8]的思想，使用智能合约代替传统方案中的经纪人，实现了去中心化，保证了支付的安全性和匿名性。同时，双支付链机制也保证了支付的公平性和高效性。

2. 相关理论与研究

2.1. PayWord 微支付协议

PayWord 是基于信用的离线微支付协议，该协议使用非对称加密算法实现数字签名，来保证顾客的可靠性。利用哈希函数运算速度快和单向性的特点，保证了高效性和安全性。

PayWord 协议共有三个实体参与：顾客(U)，经纪人(B)，供应商(V)，其中 B 一般由银行来担任。其交互过程如图 1 所示，主要步骤如下：

① U 向 B 提交自己的信息，建立账户。

② B 向 U 颁发数字签名证书。

③ 通过②中获得的证书，U 被授权生成用于当作支付凭证的以 w_0 为根哈希值的哈希链 $w_0, w_1, \cdots, w_N$。哈希链生成方法为：用户随机选取一个哈希值 w_N，通过 w_N 以相反顺序计算前一个哈希值，即 $w_{i-1} = h(w_i), i = N, N-1, \cdots, 1$。其中 h 为单向哈希函数。同时 U 生成支付承诺并连同本次支付凭证 (w_i, i) 一同发送给 V。

④ U 向 V 提供本次支付的支付凭证 w_i。

⑤ V 向 U 提供服务或商品。

⑥ 在支付结束后，V 可以向 B 提交 U 的支付承诺和最后一次收到的支付凭证(w_i, i)，B 验证支付凭证，若验证通过，则将前 i 次支付的资金从 U 的账户转到 V 的账户中。

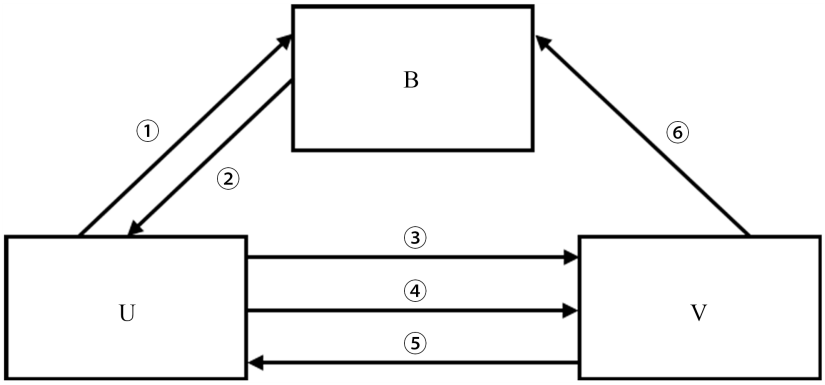

Figure 1. PayWord protocol interaction process
图 1. PayWord 协议交互过程

2.2. 区块链与智能合约

区块链技术来源于一种 P2P 电子支付系统——比特币(Bitcoin) [9]，是一个去中心化、点对点的分布式分类账。它的状态并非由某个或某些特权节点来决定，而是由各个节点共同决定。其具有去中心化、可验证性、透明化和不变性等显著特性。区块链由一系列块组成，新生成的块通过引用前一个块的哈希值来锁定前一个块，通过共识机制来确定有效的块，从而确定主链。

智能合约[10]是在互不信任的各方之间以数字方式执行特定协议的合约。通常在区块链上执行，通过区块链的特性来保证即使是智能合约的部署者也无法在部署后对合约进行更改或者使合约异常执行。目前发展较好且较受欢迎的智能合约平台为以太坊(Ethereum) [11]，其提供了一种图灵完备的语言供用户自己编写和定义智能合约，并运行在以太坊虚拟机(EVM)之上。

2.3. 相关研究

PayWord 作为一个经典的微支付协议，有许多微支付方案都是基于其思想进行的研究与改进。

樊利民等[8]在分割 PayWord 链中哈希值的思想上，提出了双 PayWord 链的概念，同时实现了非单元支付的功能。依靠数据业务管理平台和双 PayWord 链提出了一种新的小额支付协议，保证了支付的完全公平性和高效性。Mona Hosseinkhani 等[12]提出了一种基于 PayWord 的小额支付系统，其使用户使用一个哈希链就可以从不同的 V 处购买商品，同时使用通用货币使支付方案成为匿名的，提高了方案的效率同时保证了匿名性，保护了支付双方的隐私。Tao-Ku Chang 等[13]提出了一种针对移动支付的微支付方案，保证了买家、卖家和银行三方相互不可抵赖，且买家可以在多个设备上使用一条哈希链进行支付，提高了微支付方案的安全性、可用性和高效性。Aye Mi San 等[14]提出了一种离线的多卖家的微支付协议，买家、卖家和银行三方传递信息全部用对称加密进行加密，保证了良好的安全性和效率。

以上基于 PayWord 思想的微支付方案研究，同大多数方案一样，都需要第三方经纪人参与，恶意经纪人一旦与双方当中的某一方串通，会给另一方造成极大的利益损失。本文提出的方案使用智能合约代替经纪人，保证支付的安全性。使用双支付链，支持多个元支付一次性执行，提高了支付的效率，同时配合本文的仲裁子协议，保证方案的公平性。

3. 协议设计与说明

本文提出的协议中同样有三个实体：顾客(U)、供应商(V)、仲裁机构(ARB)，一个非实体：智能合约(SC)，且包含五个子协议。为方便描述，文中后续部分都使用表 1 中定义的符号。

Table 1. Symbols and their meanings
表 1. 符号及其含义

符号	说明
$Addr_P$	P 的账户地址
PK_P	P 的公钥
SK_P	P 的私钥
w_{mi}	支付意向链的第 i 个哈希值
w_{si}	支付凭证链的第 i 个哈希值
N	商品个数
$UnitPrice$	支付单位金额
$Deadline$	支付期限
SN_V	V 已经结算的支付单位个数
G_i	第 i 个商品
$\{M\}SK_P$	消息 M 本身及其签名

微支付协议的整体模型如图 2 所示。

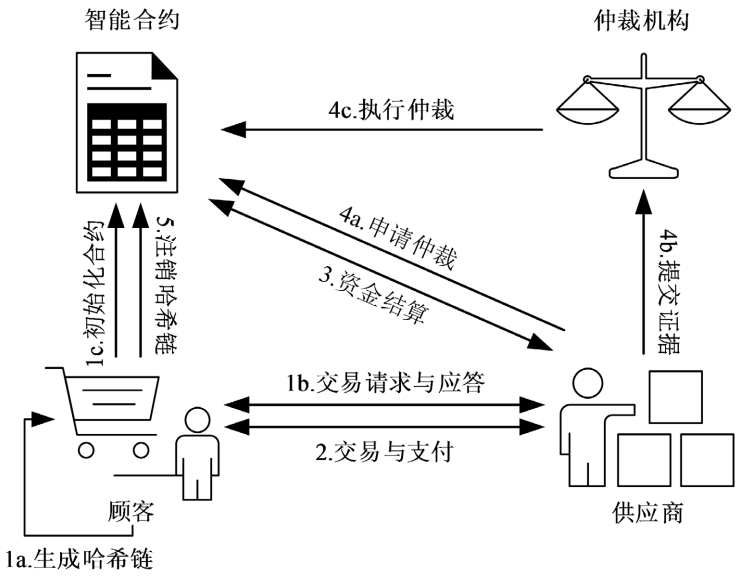

Figure 2. Overall protocol model
图 2. 协议整体模型

3.1. 初始化子协议

U 随机选择一个二元组 (w_{mN}, w_{sN})，并利用强抗碰撞的单向哈希函数，利用公式(1)(2)生成两条长度为 N+1 的哈希链，支付意向链 $w_m(w_{m0}, w_{m1}, w_{m2}, \cdots, w_{mN})$ 和支付凭证链 $w_s(w_{s0}, w_{s1}, w_{s2}, \cdots, w_{sN})$。

$$w_{mi} = h\left(w_{m(i+1)}\right), i = N-1, N-2, \cdots, 0 \tag{1}$$

$$w_{si} = h\left(w_{s(i+1)}\right), i = N-1, N-2, ..., 0 \tag{2}$$

随后 U 将 $\{Addr_U, Addr_V, PK_U, w_{m0}, w_{s0}, Price, UnitPrice, N, Deadline\}SK_U$ 发送给 V。V 收到后首先进行签名验证，若验证通过，对商品序列 $G(G_1, G_2, \cdots, G_N)$ 进行哈希运算，生成哈希值序列 $w_G\left(w_{G_1}, w_{G_2}, \cdots, w_{G_N}\right)$ 并签名得到 $\{w_G\}SK_V$，随后将 $\left(PK_V, \{w_G\}SK_V\right)$ 发送给 U。

U 收到 $\left(PK_V, \{w_G\}SK_V\right)$ 后首先验证签名，若验证通过，则使用信息 $\{Addr_U, Addr_V, PK_U, PK_V, w_{m0}, w_{s0}, N, UnitPrice, Deadline\}SK_U$ 部署并初始化 SC，并向 SC 中存入大于等于 $UnitPrice * N$ 的资金，支付流程开始。

3.2. 支付子协议

设支付金额和购买的商品均为 1 个单位的支付为元支付，每次支付至少进行一个元支付或将多个元支付合成一个支付组，一次性执行。

U 先向 V 发送支付意向 $\left(w_{m(i+j)}, i+j\right)$，V 收到后验证 $w_{m(i+j)}$，即验证 $w_{m(i+j)}$ 经过 j 次哈希运算是否等于最后一次收到的支付意向 (w_{mi}, i)。若验证通过，V 向 U 发送第 i 到第 $i+j$ 个商品 $\left(G_{i+1,i+j}, i+1, i+j\right)$，U 收到并进行签名验证后，将支付凭证 $\left(w_{s(i+j)}, i+j\right)$ 发送给 V，V 收到后依旧按上述方法进行验证，若验证通过，$\left(w_{s(i+j)}, i+j\right)$ 便是合法的支付凭证。

3.3. 资金结算子协议

SC 使用 SN_V 记录已经结算的支付单位个数。在某次支付结束后，V 可以将最后一次收到的支付凭证 (w_{si}, i) 提交给 SC 发起结算申请。SC 验证 (w_{si}, i)，若验证通过且 $i - SN_V > 0$，则 SC 将 $i - SN_V$ 个支付单位的资金总额转入 $Addr_V$，同时更新 SN_V，令 $SN_V = i$。若 $i - SN_V \le 0$，表示 V 提交的支付凭证在之前已经结算过，则本次结算视为重放攻击，SC 将拒绝结算。

3.4. 仲裁子协议

若在支付过程中，U 收到 V 发送的 $\left(G_{i+1,i+j}, i+1, i+j\right)$ 后，拒绝向 V 本次支付的支付凭证 $\left(w_{s(i+j)}, i+j\right)$，则 V 可以根据仲裁子协议，向 SC 提起仲裁。

V 向 SC 申请仲裁并向 ARB 提供证据 $\left(w_{m(i+j)}, i+1, i+j, \{G_{i+1,i+j}\}SK_V\right)$，U 也需要向 ARB 提交证据 $\left(\{w_G\}SK_V\right)$ 令 ARB 验证 $\{G_{i+1,i+j}\}$ 是否为本次支付 U 应得的数据。

仲裁机构首先验证所有签名以及 $w_{m(i+j)}$ 的正确性，随后对商品 $G_{i+1,i+j}$ 进行哈希运算，将得到的哈希值与 w_G 进行比对，判断 $G_{i+1,i+j}$ 是否为 U 应得商品。若上述验证通过或 U 拒绝提供证据，则 V 仲裁成功，ARB 将 $\{G_{i+1,i+j}\}SK_V$ 发送给 U，并调用 SC 将总额为 $(i+j-SN_V) * UnitPrice$ 的资金从 U 存储的资金中扣除并转入 V 的账户；若上述验证失败，则本次仲裁失败，ARB 调用 SC 结束仲裁。

3.5. 注销子协议

在支付结束前，U 可以随时注销尚未使用的支付凭证。U 首先向 SC 申请注销支付凭证，随后 V 使用最后一次收到的支付凭证向 SC 申请资金结算，得到自己应得的利益。结算后，SC 将不再接受任何资金结算请求，尚未使用的支付凭证自动注销。

4. 协议分析

4.1. 安全性分析

使用 SC 代替原有协议中的经纪人的地位，由于 SC 一旦部署双方均不能更改，必须按照 SC 的规定执行，所以避免了原协议中恶意经纪人与 U 或 V 合谋攻击另一方的情况。同时，由于使用 SC，双方无需像原协议一样向经纪人提交信息并在经纪人处开设账户，只需要拥有一个加密货币账户即可。双方只需要自行生成各自账户，顾客将支付所需的资金存入 SC，然后向 SC 提交 V 的账户地址 $Addr_V$，在 V 结算阶段 SC 直接将资金转入 $Addr_V$ 即可，保证了支付的匿名性。

在 SC 部署时就已经规定了支付次数与单次支付金额，V 每次结算前 SC 都会验证当前支付凭证 (w_{si}, i) 并比较当前已结算支付单位数 i 与 SC 中记录的上次结算的支付单位数 SN_V，若当前支付次数超过 SC 规定的总支付次数，则视为恶意透支，拒绝结算；若当前支付次数小于等于 SC 记录的 SN_V，则视为重放攻击，拒绝结算。

综上，该协议可保证双方的匿名性，同时可防止顾客进行恶意透支和重放攻击，保证了支付的安全性。

4.2. 公平性分析

协议采用双支付链的形式进行支付，U 和 V 交替发送各自的信息给对方，若支付双方完全按协议执行，直至支付结束，那么协议本身是公平的，所以整个支付过程是公平的。若有恶意的 U 在收到 V 发送的 $\left(G_{i+1,i+j}, i+1, i+j\right)$ 后，不发送支付凭证 $\left(w_{s(i+j)}, i+j\right)$ 给 V，则 V 可根据仲裁子协议向 SC 申请仲裁，使用仲裁子协议保证支付的公平性。

另外，若 V 长时间无应答或恶意拖延时间，则 U 的资金会被长时间冻结在 SC 中无法使用和取回，这必将导致 U 的利益受损。SC 中设置了支付期限 *Deadline*，若当前时间超过 *Deadline*，则 U 可向 SC 申请结束支付并取回 SC 中剩余的所有资金，支付结束。这可以保证 U 的资金不会被长时间冻结在 SC 中，保证了支付的公平性。

4.3. 效率分析

本协议虽然使用了 SC，但具体的交易和支付过程及 U 和 V 针对对方信息的验证过程均是在链下进行，SC 并不参与，避开了区块链吞吐量低，存储及计算代价昂贵的缺点，保证了 SC 不会拉低支付速度，避免 SC 成为效率瓶颈。

U 和 V 在已经建立信任的基础上，可以将多个元支付打包为支付组进行支付。这便完成了一组元支付一次性执行，极大提升了支付效率。

5. 结束语

本文分析了原有微支付方案的缺陷，基于区块链提出了一种的新的安全且公平的微支付协议。该协议采用 PayWord 的思想，用智能合约代替原有方案中的经纪人，实现去中心化，避免恶意经纪人与某一方合谋攻击另一方，同时防止顾客恶意透支和重放攻击，保证了支付的安全。借鉴了双支付链思想[8]，保证了支付公平性，同时支持一组元支付的一次性执行，提升了支付效率。下一步研究工作，需要尽量减少非对称加密次数以及签名次数，以进一步提高支付效率。

参考文献

[1] Rivest, R.L. and Shamir, A. (1996) PayWord and MicroMint: Two Simple Micropayment Schemes. *Security Protocols, International Workshop*, Cambridge, United Kingdom, 10-12 April 1996, 69-87.

[2] Raj, Y. and Sowmiya, B. (2021) Study on Supply Chain Management Using Blockchain Technology. 2021 6*th International Conference on Inventive Computation Technologies* (*ICICT*), Coimbatore, 20-22 January 2021, 1243-1247. https://doi.org/10.1109/ICICT50816.2021.9358768

[3] Niya, S.R., Dordevic, D., Nabi, A.G., *et al*. (2019) A Platform-Independent, Generic-Purpose, and Blockchain-Based Supply Chain Tracking. 2019 *IEEE International Conference on Blockchain and Cryptocurrency* (*ICBC*), Seoul, 14-17 May 2019, 11-12. https://doi.org/10.1109/BLOC.2019.8751415

[4] Daraghmi, E.Y., Daraghmi, Y.A. and Yuan, S.M. (2019) MedChain: A Design of Blockchain-Based System for Medical Records Access and Permissions Management. *IEEE Access*, **7**, 164595-164613. https://doi.org/10.1109/ACCESS.2019.2952942

[5] Yang, W.K., Chen, J.S. and Chen, Y.S. (2020) An Electronic Medical Record Management System Based on Smart Contracts. 2019 12*th International Conference on Ubi-Media Computing* (*Ubi-Media*), Bali, 5-8 August 2019, 220-223. https://doi.org/10.1109/Ubi-Media.2019.00050

[6] Zhou, J., Tang, F., Zhu, H., *et al*. (2019) Distributed Data Vending on Blockchain. 2018 *IEEE International Conference on Internet of Things* (*iThings*) *and IEEE Green Computing and Communications* (*GreenCom*) *and IEEE Cyber, Physical and Social Computing* (*CPSCom*) *and IEEE Smart Data* (*SmartData*), Halifax, NS, 30 July-3 August 2018, 1100-1107. https://doi.org/10.1109/Cybermatics_2018.2018.00201

[7] Dai, W., Dai, C., Choo, K., *et al*. (2020) SDTE: A Secure Blockchain-Based Data Trading Ecosystem. *IEEE Transactions on Information Forensics and Security*, **15**, 725-737. https://doi.org/10.1109/TIFS.2019.2928256

[8] 樊利民, 廖建新. 公平的移动小额支付协议[J]. 电子与信息学报, 2007(11): 2599-2602.

[9] Nakamoto, S. (2019) Bitcoin: A Peer-to-Peer Electronic Cash System. Manubot.

[10] Kemmoe, V.Y., Stone, W., Kim, J., *et al*. (2020) Recent Advances in Smart Contracts: A Technical Overview and State of the Art. *IEEE Access*, **8**, 117782-117801. https://doi.org/10.1109/ACCESS.2020.3005020

[11] Wood, G. (2014) Ethereum: A Secure Decentralised Generalised Transaction Ledger. *Ethereum Project Yellow Paper*, **151**, 1-32.

[12] Hosseinkhani, M., Tarameshloo, E. and Shajari, M. (2011) AMVPayword: Secure and Efficient Anonymous Payword-Based Micropayment Scheme. 2010 *International Conference on Computational Intelligence & Security*, Nanning, 11-14 December 2010, 551-555. https://doi.org/10.1109/CIS.2010.126

[13] Chang, T.K., Yangw, C.N. and Yeh, F.H. (2016) Using the Same PayWord Chains of a Single Account from Multiple Devices. 2016 13th *International Joint Conference on Computer Science & Software Engineering*, Khon Kaen, 13-15 July 2016, 1-4. https://doi.org/10.1109/JCSSE.2016.7748926

[14] San, A.M. and Sathitwiriyawong, C. (2016) Efficient Offline Micropayment Protocol for Multi-Vendor. 2016 *International Computer Science and Engineering Conference* (*ICSEC*), Chiang Mai, 14-17 December 2016, 1-4. https://doi.org/10.1109/ICSEC.2016.7859938