Computer Science and Application 计算机科学与应用, 2021, 11(11), 2700-2704
Published Online November 2021 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2021.1111273

Hans汉斯

基于区块链的公平合同签订方案

陈俊屹

天津工业大学计算机科学与技术学院，天津

收稿日期：2021年10月8日；录用日期：2021年11月5日；发布日期：2021年11月12日

摘　要

合同签订是一个基于信任的服务，传统的合同签订方案往往需要引入中心化的可信第三方来保证公平性，合同签订参与者公平的交换他们的数字签名，并由中心化的可信第三方来解决出现的争端。合同签订依赖于中心化第三方的可靠性，如果中心化的第三方与合同签订的一方合谋或者受到攻击，则会对公平性和隐私性造成巨大影响。区块链技术为我们提供了一个去中心化的可信第三方，可以避免中心化带来的种种问题。本文提出了一个基于区块链的合同签订方案，聚焦于合同签订的过程，只在链上进行签名的确认，而将签名的交换和验证过程放在链下进行。

关键词

区块链，合同签订，智能合约

Fair Contract Signing Scheme Based on Block Chain

Junyi Chen

School of Computer Science and Technology, Tiangong University, Tianjin

Received: Oct. 8th, 2021; accepted: Nov. 5th, 2021; published: Nov. 12th, 2021

Abstract

Contract signing is a truth-based service. Traditional contract signing schemes often need to introduce a centralized trusted third party to ensure fairness. Participants in contract signing can exchange their digital signatures fairly, and the centralized trusted third party can solve disputes. Contract signing depends on the reliability of the centralized third party. If the centralized third party conspires with the contract signing party or is attacked, the fairness and privacy will be greatly affected. Block chain technology provides us with a decentralized, trusted third party that can avoid the problems of centralization. This paper proposes a contract signing scheme based on

文章引用: 陈俊屹. 基于区块链的公平合同签订方案[J]. 计算机科学与应用, 2021, 11(11): 2700-2704.
DOI: 10.12677/csa.2021.1111273

block chain, focusing on the process of contract signing, only confirming the signature on the chain, and putting the exchange and verification process of signature under the chain.

Keywords

Block Chain, Contract Signing, Smart Contract

1. 概述

现如今，合同签订已经不仅仅局限在线下，在线的合同签订方案也越来越多的被人们所使用。目前，这些合同签订方案根据对可信第三方的使用情况大致分为两类：一类不需要第三方的参与，采用逐步交换等方案，这种方案不仅存在不公平性，还需要复杂的交换过程。

另一类需要第三方的参与，但是中心化的可信第三方由于可能会收到内部外部攻击，单点故障等问题，同时中心化的可信第三方也限制了电子合同签订的扩展。而基于区块链技术的合同签订协议可以在满足合同签订要求的同时，既保证了公平性隐私性，又消除了中心化的可信第三方的存在。

Josep-Lluis 等人[1]提出，合同的电子签名是一组服务的一部分贴上公平交换价值，合同双方都能得到对方签名或者都不能得到，这种类型的例子有认证电子邮件，付款收据等，可以考虑通过电子邮件等方面的方案来尝试解决合同签订的问题。文献[2]提出了使用区块链的多方认证电子邮件的解决方案，给本文的基于区块链的合同签订方案提供了一种可能，其中交换双方的不可否认证据为认证的电子邮件解决方案的关键。

在文献[3]提出了一种基于区块链的公平合同签订协议，合同发起人将合同加密并通过智能合约使接收方能够破解加密合同，接收方决定是否签订，在截止时间后进行判断，但是这篇文章给出的方案在截止时间前无法对不诚信方进行约束且合同接收方只能决定是否签署并不能协商合同内容。

文献[4]提出了通过使用可验证的加密签名(VES)的基于区块链的公平合同签订方案，该方案通过四个智能合约将合同签订分为上传参数，提交押金，验证 VES 签名，判断四个过程，能整体上实现合同签订的过程，但本文的签名验证过程只能通过链下模拟来进行，目前以太坊智能合约缺少双线性配对的验证计算函数库，所以文中提出的 VES 的签名验证过程在智能合约上的实现存在困难。

目前已有的大多数基于区块链的公平合同签订方案都是聚焦于合同签订双方签名的交换，但是合同签名在智能合约的验证存在困难。本文提出合同签订方案聚焦于合同签订的过程，而不是签名交换和验证。本文提出的这个基于区块链的公平合同签订方案中，避免了第三方的存在，只通过使用一个合同签订智能合约来完成合同的签订过程，而将签名的交换与验证过程都放到链下进行。

本文第 2 节概述了相关理论。第 3 节对本文的方案进行了描述。第 4 节从公平性和隐私性的基础上进行了分析。第 5 节总结了本文的方案并进行了展望。

2. 相关理论

2.1. 区块链

区块链技术起源于 2008 年化名为“中本聪”的学者提出的《比特币：一种点对点电子现金系统》[5]。区块链是以比特币为代表的数字加密货币体系的核心支撑技术。区块链技术的核心优势是去中心化，能

够通过运用数据加密、时间戳、分布式共识和经济激励等手段在节点无需互相信任的分布式系统中实现基于去中心化信用的点对点交易、协调与协作[6]。比特币是一个点对点的电子现金系统，通常被当作一个记账的账本，人们把他叫作区块链 1.0 (简单的记账转账)。而以以太坊[7]为代表的带有智能合约的区块链被我们称作区块链 2.0 (不仅可以记账转账还可以包含其他功能)。近几年，以高性能大吞吐量，开发者友好和用户友好为目标的区块链 3.0 被提出，有 EOS 等不同的解决方案。

2.2. 智能合约

智能合约本质上是一个数字化的合同，通过代码代替人来仲裁和执行合约，智能合约允许在没有第三方的情况下进行可信交易，智能合约本质是一个部署在以太坊区块链上的程序。智能合约具有确定性，一致性，可终止性，可观察和可验证性，去中心化，高性能和实时性等一系列优点[8]。通过 solidity 语言编写智能合约代码，在 Remix 编译器中部署和测试智能合约，一经编写完成发布在链上后，便不能再进行修改。

3. 基于区块链的公平合同签订方案

3.1. 系统设计

本文的方案中，合同签订智能合约只对合同的有效性进行操作，合同签订双方在收到并验证对方签名成功之后，可以通过自己的以太坊地址在合同签订智能合约中进行确认操作。在规定的时间内只有双方都进行了确认操作，合同才变为有效合同。由于不需要在链上进行押金和签名验证环节，合同签订的过程大大简化。

3.2. 系统流程

基于区块链的公平合同签订方案模型如下图 1 所示，具体的流程有以下几步：

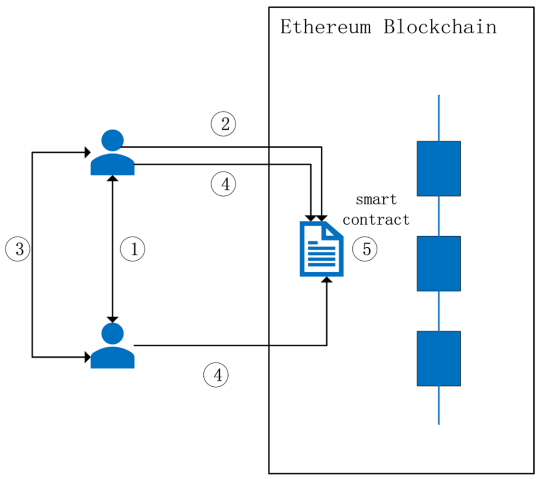

Figure 1. Blockchain-based contract signing scheme model
图 1. 基于区块链的合同签订方案模型

1) 合同签订双方 Alice 和 Bob 在链下协商合同的内容，协商好的合同 c，双方选定加密算法，Alice 和 Bob 生成签名密钥对(Pka，Ska)，(Pkb，Skb)，其中 Pka 为 Alice 的公钥，Ska 为 Alice 的私钥。Pkb 为 Bob 的公钥，Skb 为 Bob 的私钥。之后双方使用自己的签名密钥对对合同 c 进行签名。双方交换对该合同的公钥 Pka，Pkb。并生成合同的哈希值 H(c)。

2) 合同签订的一方发布合同签订智能合约。

3) 双方在链下交换对该合同 c 的签名。

4) 如果合同签订方 Alice 使用 Bob 的公钥 Pkb 验证 Bob 的签名成功，则调用合同签订智能合约进行确认。如果合同签订方 Bob 使用 Alice 的公钥 Pka 验证 Alice 的签名成功，则调用合同签订智能合约进行确认。

5) 到截止时间后合同签订智能合约进行判断，如果合同签订双方 Alice 和 Bob 都在合同签订智能合约上确认，则合同生效。如果一方或者两方都没确认，则合同依然是无效合同。

3.3. 算法设计

算法：合同签订智能合约算法

1) 输入：合同签订双方的地址 adda，addb，双方协商好的合同的哈希 H(c)，合同签订截止时间 t。合同布尔值设置为 0，目前签订的合同为无效合同。

2) 当合同签订一方收到对方的签名并验证成功后，可以调用智能合约，进行确认操作。

3) 在截止时间前合同签订双方都调用智能合约进行确认操作后，合同布尔值为 1。

4) 截止时间后，有一方未确认或者双方都未确认，合同布尔值为 0

5) 输出：合同的布尔值，若为 1 则合同签订成功，合同生效，若为 0，则为无效合同，合同签订失败。

4. 方案分析

4.1. 公平性分析

1) 如果合同双方都诚信，那么他们收到签名验证成功后都确认，使合同变为有效合同。则可以在区块链中看到双方成功签订了合同。

2) 如果有一方不诚信，那么合同就无法成功签订，不诚信方能拿到诚信方对该合同的签名，但是由于合同签订失败，诚信方对该合同的签名也失效，不诚信方拿到的签名也没有意义。

3) 如果合同双方都不诚信，则双方都没有在智能合约上进行确认操作，则合同依然是无效合同。

4.2. 隐私性分析

合同签订智能合约中包括合同内容的哈希 H(c)，通过 H(c)无法得到合同的内容 c，从而实现了合同内容的隐藏。由于合同签订双方对合同签订智能合约进行确认操作使合同生效，则合同签订双方对哈希值为 H(c)的合同签订成功是记录在区块链中的，是公开可查的。

5. 总结与展望

本文的方案只将合同签订智能合约上传到区块链中，其余的协商合同、交换验证签名等过程都在链下执行，避免了合同内容的泄露，极大的简化了合同签订的过程。本文基于区块链技术的公平合同签订方案，在没有第三方参与的同时满足了公平性。通过一个合同签订智能合约使合同签订过程聚焦于合同签订上而非签名的交换。本文的方案由于不需要在智能合约上验证签名，所以可实现性方面有着很大的优势。但由于本文的方案没有押金来约束合同签订双方，所以合同签订双方违约的成本也会降低，今后考虑通过添加信誉积分系统来对合同签订者的信誉进行评估，如果出现恶意违规的情况将被降低信誉，并在后面的合同签订过程中被标识出来。

参考文献

[1] Ferrer-Gomila, J.-L. and Francisca Hinarejos, M. (2020) A 2020 Perspective on “A Fair Contract Signing Protocol with Blockchain Support”. *Electronic Commerce Research and Applications*, **42**, Article ID: 100981.

https://doi.org/10.1016/j.elerap.2020.100981

[2] Francisca Hinarejos, M. and Ferrer-Gomila, J.-L. (2020) A Solution for Secure Multi-Party Certified Electronic Mail Using Blockchain. *IEEE Access*, **8**, 102997-103006. https://doi.org/10.1109/ACCESS.2020.2998679

[3] Ferrer-Gomila, J.-L., Francisca Hinarejos, M. and Isern-Deyà, A.-P. (2019) A Fair Contract Signing Protocol with Blockchain Support. *Electronic Commerce Research and Applications*, **36**, Article ID: 100869. https://doi.org/10.1016/j.elerap.2019.100869

[4] Zhang, L., Zhang, H.L., Yu, J. and Xian, H.Q. (2020) Blockchain-Based Two-Party Fair Contract Signing Scheme. *Information Sciences*, **535**, 142-155. https://doi.org/10.1016/j.ins.2020.05.054

[5] Satoshi, N. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[6] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.

[7] Buterin,V. (2014) White Paper: A Next-Generation Smart Contract and Decentralized Application Platform. https://www.ethereum.org/pdfs/EthereumWhitePaper.pdf

[8] 贺海武, 延安, 陈泽华. 基于区块链的智能合约技术与应用综述[J]. 计算机研究与发展, 2018, 55(11): 2452-2466.