软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, [doi: 10.13328/j.cnki.jos.000000]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

区块链：基于以太坊平台的电子合同系统

王业超[1]，姚芝俏[2]，严瑾瑜[2]

[1](华南理工大学 软件学院本科生,广东 广州 510006)

[2](华南理工大学 法学院本科生,广东 广州 510006)

摘 要: 随着法制社会的建设，合同的签署愈来愈成为人们社会生活一项重要活动。而为了使人们能更有效率地签署法律合同，电子合同应运而生，但是电子合同又带来如何保证中心化节点可信，如何防止造假等问题。基于此，我们应用区块链技术，构造了一个全新的系统，该系统能够异地签署合同，保留当下电子合同的优点；同时去中心化、保护隐私并能防止篡改，有极大安全性；同时利用智能合约能自动验证合同真伪，大大降低合同验证真伪的成本.

关键词: 电子合同;区块链;以太坊;智能合约

中图法分类号: TP311

中文引用格式: 陈翔,顾庆,刘望舒,刘树龙,倪超.静态软件缺陷预测方法研究.软件学报. http://www.jos.org.cn/1000-9825/0000.htm

英文引用格式: Chen X, Gu Q, Liu WS, Liu SL, Ni C. State-of-the-Art survey of static software defect prediction. Ruan Jian Xue Bao/Journal of Software, 2016 (in Chinese). http://www.jos.org.cn/1000-9825/0000.htm

Blockchain: an electronic contract system based on Ethernet platform

WANG Ye-Chao[1], YAO Zhi-Qiao[2], YAN Jin-Yu[2]

[1](South China University of Technology Undergraduate of Software College, Guangzhou 510006, China)

[2](South China University of Technology Undergraduate of Law College, Guangzhou 510006, China)

Abstract: With the construction of a legal society, the signing of contracts plays an important part in people's social life. In order to make people sign legal contracts more efficiently, electronic contracts arise at the historic moment. However, electronic contracts bring about problems such as how to ensure the credibility of centralized nodes and how to prevent forgery. Based on this, we construct a new system by using blockchain technology, which retains the advantages of current electronic contract system and can meet the needs of users to sign contracts fast and conveniently in different places; at the same time, it has great security by decentralizing, protecting privacy and preventing tampering. The automatic execution of intelligent contract can greatly reduce the error of human operation, improve the accuracy and efficiency of operation, and greatly reduce the cost of the court to verify the authenticity of the contract.

Key words: electronic contracts; blockchain; Ethereum; intelligent contracts

1 简介

区块链是由包含交易信息的区块从后向前有序链接起来的数据结构。区块链可以想象成地质构造中的地质层。表层可能随着季节而变化，如被风吹走了。但是越往深处，地质层就变得越稳定。到了几百英尺深的地方，你看到的将是保存了数百万年但依然保持历史原状的岩层。在区块链里，最近的几个区块可能会由于区块链分叉所引发的重新计算而被修改.最新的六个区块就像几英寸的深的表土层.但是,超过这六块后,区块在区块链中的位置越深,被改变的可能性就越小.

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式,其拥有去中心化、开放性、自治性、信息不可篡改、匿名性等特征[2].

在区块链中,任意节点的权利和义务都是均等的,整个系统中具有维护功能的节点共同维护系统,这便是去

中心化的含义.而其开放性是指区块链的数据中,除了交易各方的私有信息是加密的,其他都是明文对所有人公开.区块链上的自治让多参与方、 多中心的系统按照公开的算法、规则形成的自动协商一致的机制基础上来运行,以确保记录在区块链上的每一笔交易的准确性和真实性[3].

区块链的信息是不可篡改的,一旦信息被验证成功添加上区块链,除非你能够控制整个系统 51%的节点,否则你是无法篡改区块链的数据的,故区块链有着极强的数据稳定性.最后,区块链的匿名指的是非实名,即区块链上你的身份与你的真实身份无关,而系统各节点之间的交换遵循固定算法,并且区块链上的程序会自行判断活动是否有效,故交易双方无需公开身份便可以得到对方信任.

2 背景

当下合同的形式主要是纸质合同,但在互联网金融快速发展的形势下,网上交易量呈井喷式递增,纸质合同的签署形式难以满足当下的快节奏签署效率[4].

为了提高合同的签署效率等,电子合同应运而生.《中华人民共和国合同法》第 11 条规定“书面形式是指合同书、信件和数据电文 （包括电报、电传、传真、电子数据交换和电子邮件）等可以有形地表现所载内容的形式.”表明我国法律认可合同的签订包括电子数据的形式,承认了电子合同的法律地位[5].电子数据与纸面形式相比具有易消失性、作为证据的局限性和易改动性等.操作不当可能抹掉所有数据,可能受到计算机病毒攻击,以键盘输入,用磁性介质保存、改动或伪造可以不留痕迹等[6].

区块链技术的不可篡改、可追溯等特点正好可以改革电子合同的技术,实现更加安全的“电子合同”签署模式.《合同法》第 25 条规定:“承诺生效时,合同成立”,这意味着电子合同在签署时必须能够准确无误记录时间并防止时间被伪造篡改等,而区块链的时间戳恰好能记录交易的时间并无法篡改,是解决该问题的一个可行方案.

在 2018 年 9 月 3 日由最高人民法院审判委员会第 1747 次会议通过的《最高人民法院关于互联网法院审理案件若干问题的规定》中第十一条提到：当事人提交的电子数据,通过电子签名、可信时间戳、哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存证平台认证,能够证明其真实性的,互联网法院应当确认.这是我国首次以司法解释形式对区块链技术电子存证进行法律确认.这也意味着运用区块链技术来签署合同产生的凭证将具有法律效力,这同样意味着区块链合同的开发并运用来解决实际问题是完全可行的.

3.基于以太坊平台的电子合同系统

3.1相关工作

文献[7]中提出了一个无需可信第三方的公平合同签署协议,该系统借助一个时间戳服务器实现,而时间戳正好是区块链的一个特性,同时该文献中提出：合同签字人 Alice 和 Bob 首先协商签订合同的最后期限,然后在合同中声称只有在合同双方在最后期限签署合同,合同才是有效的.

目前的比特币跟以太坊的交易数据几乎都是明文的,因此基于区块链设计安全协议需要考虑区块链的公开验证和隐私保护之间的矛盾[8].文献[8]提出了一种盲的可验证加密签名（BVES）,但由于区块链的假名性,这种加密签名也存在泄漏身份的可能性.同时,如果要在智能合约嵌入这种加密函数,会让智能合约变得臃肿,并耗费过多的 gas[9].

针对比特币的可链接性、可追踪性等,其他学者也提出不同的隐私保护方案.比如 Maxwell 提出的 CoinJoin 混币原理,简单说就是一个交易中包含大量输入输出,以至于很难找到输入与输出的对应关系.而文献[10]提出的 Zerocoin 则是使用零知识证明,通过割裂输入地址和输出地址的关系来达到目的.文献[11]基于 Zerocoin 引入的零知识证明,进一步发展了 Zerocoin 的协议.

文献[12]提出了一个基于超级账本的区块链合同设计,该文利用超级账本架构,设计了一个可以满足合同签署与撤销、可以实现签名与盖章等功能的系统,但该文对如何保护合同数据的隐私并没有给出相应的方案.

现有工作中并没有发现既满足电子合同签署需求同时又考虑到保护用户隐私的区块链合同方案,故本文基于以太坊平台,并在中国法律《电子合同在线订立流程与规范》的指导下,设计了一个满足电子合同签署需求并同时考虑到保护用户隐私的区块链合同方案.

3.2基于以太坊平台的电子合同系统

基于以上研究,我们设计了一种基于以太坊平台的新型合同签署系统,该系统通过引入了中心化的数据库保证了数据的隐私,并利用区块链的数据完整性校验快速准确检验数据是否被篡改;同时区块链的智能合约自动化执行,实现合同在甲乙方之间的传递与相关数据的自动记录并上链.该系统的框架图如图 1 所示.

该框架图主要由司法机构、数据库、区块链、以及用户（合同甲乙方）组成.其中:

1） 司法机构:司法机构是智能合约发布者,是整个系统的开端.它的主要功能有:

（1）完成区块链的创世;

（2）对用户（合同甲乙方）的身份认证并将认证结果上传写入区块链;

（3）对数据库的合同进行数据完整性校验.

2） 用户（合同甲乙方):用户分为甲乙方,甲乙方对应于法律合同签署的甲乙方,是整个系统的服务对象.其中甲方的主要功能是:

（4）向司法机构进行身份认证;

（5）拟定合同,并将合同内容上传至数据库,得到数据库返回的索引;

（6）将数据库的合同索引以及其他与数据完整性校验相关的参数上传至区块链.

乙方的主要功能是:

（1） 当乙方收到区块链的合同签署请求时,查看、检验合同内容,并决定是否签署,签署的结果将记录在区块链上.

3） 数据库:数据库是系统的一个存储中心.它的主要功能有:

（1）存储用户的合同数据;

（2）数据需要控制访问权限,这将是用户隐私的重要保障;

4） 区块链:区块链是此系统的核心技术,区块链上的智能合约是整个系统功能开发的核心部分.区块链完成的主要功能包括以下几方面:

（1） 存储合同签署甲乙方的相关信息及对应合同的索引、校验参数等;

（2） 智能合约自动化判断签署时间的有效性,自动化存储签署结果.

整个系统框架的流程可分为 3 个子流程:

（1） 用户认证流程:用户在司法机构申请进行身份认证→司法机构认证完成将结果上传至区块链,以用于将来出现合同纠纷时对相关方身份的确认.

（2） 合同签署流程:合同甲方拟定合同上传至中心数据库,并将对应索引、数据完整性验证、以及乙方签署截止时间上传至区块链→智能合约被触动,自动向合同乙方发动要约→乙方确认是否签署并将结果上传至链→智能合约再次被触动,检验签署时间是否在甲方设定时间内,并将签署结果上传至链,反馈给甲乙方.

（3） 合同真假验证流程:司法机构利用区块链的相关参数,对合同的数据进行快速地完整性校验,检验合同内容是否被篡改,确认合同甲乙方的身份.

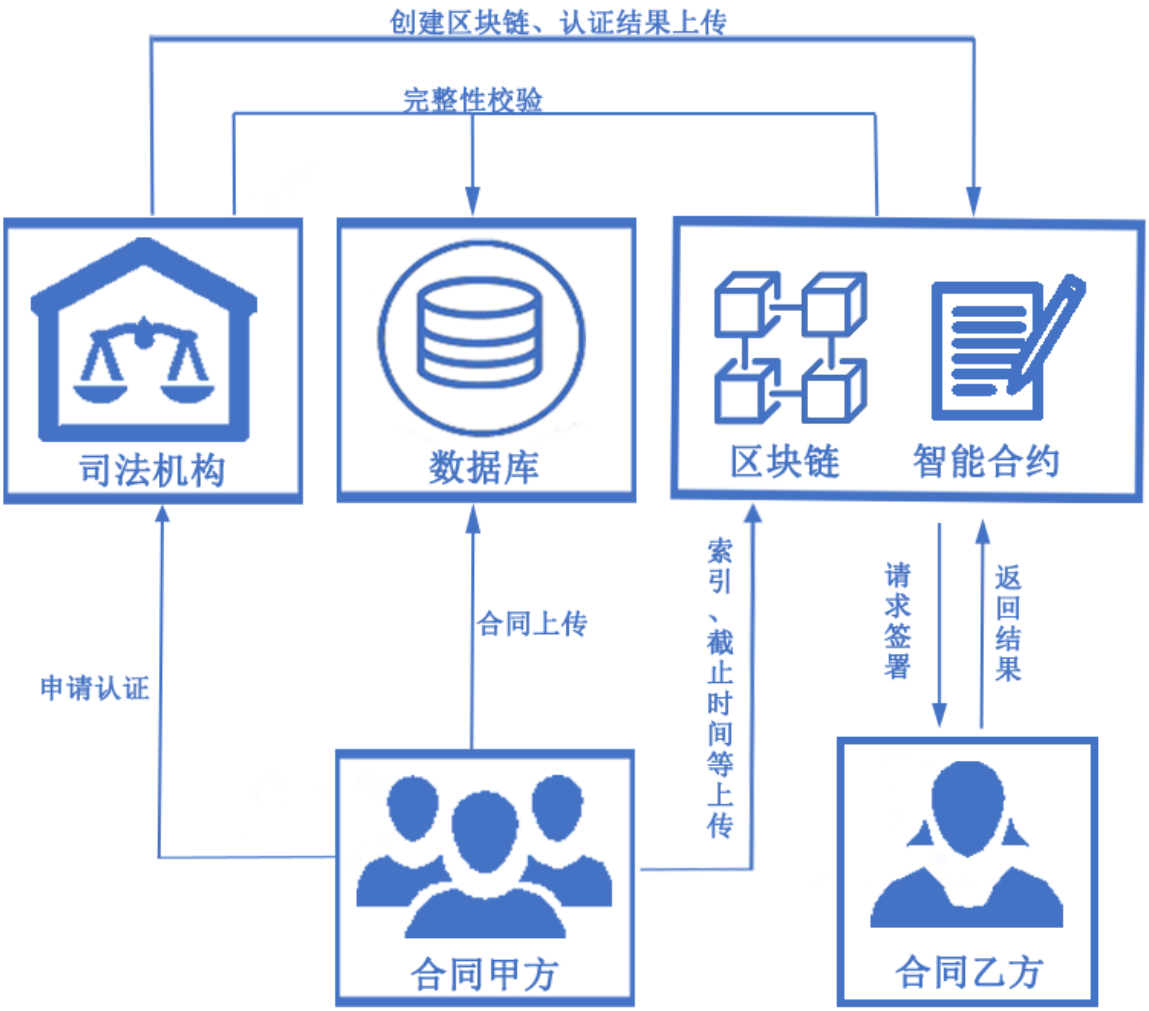

Fig.1 Framework of electronic contract system based on Ethereum

图 1 基于以太坊的电子合同系统框架

3.3系统优缺点以及同其他现有成果的比较

该系统保护了用户隐私,提高签署效率并大大降低真假的检验流程、成本等,满足了当下用户签署电子合同的大部分需求.但是基于目前以太坊平台的限制,该系统在保护用户隐私时需要引入中心化数据库,存在数据库被攻破而出现数据的大规模泄漏问题.但由于合同签署的甲乙方等隐私信息存在区块链上,而智能合约控制只有合同甲乙方等才有权力查看合同数据索引,所以哪怕存在大规模的数据泄漏,要想根据每份合同的索引一一对应找到合同的甲乙方等信息也不是一件易事.

文献[8]、[10]、[11]基于比特币平台提出了对应的一些保护隐私的方案,而文献[12]的区块链合同设计则是基于超级账本平台,平台间有着共同的理论技术作支撑,但是也有着性能,架构等的巨大差别,进而带来了不同的性能差异,更具体的差异对比可参考文献[12],其较为全面的比较了比特币、以太坊、超级账本三个平台.

以太坊的 gaslimit 等限制,一份合同的数据过大,把合同数据记录进链会导致过多的 gas,代之以将合同存储于中

心化数据库,而其索引、完整性校验数据等上链的方式,将大大降低 gas 的耗费.文献[8]、[10]、[11]所提出的的加密方案如果嵌入智能合约也是不可行的,这也是受限于目前的以太坊限制,会带来合约臃肿等问题.我们的系统通过控制用户访问存储合同数据的中心数据库来保护隐私,避免了以太坊平台的限制,虽然无法避免数据库被攻击而带来的数据被篡改等问题,但通过数据完整性校验（相关参数是在区块链上的,无法篡改）等保证了可以快速检验出数据是否被篡改,这对合同签署的场景是有效可行的.文献[12]基于超级账本平台所设计的系统较好实现了合同签署与撤销、实现签名与盖章等功能但是并没有过多阐述如何保护合同数据的方案,而我们的系统则通过隐私数据上链,对应合同入数据库上链,两者通过索引相连,并控制只有相关方有权访问索引、隐私数据、合同数据的方案,对用户隐私进行保护.

4 结语与展望

该系统实现了对合同的隐私保护,同时实现了用户可异地签署合同,极大提高合同签署的速度与便捷性；同时利用智能合约的自动执行,数据记录、上传至区块链等自动执行,极大简便了用户的操作又保证了操作的正确性.利用该系统,我们较好解决了当下合同签署存在的一些问题,对社会的合同签署改进提供了一个可行的新方案.

该系统在未来应该再结合人工智能、大数据等,在用户上传合同时自动进行检验合同是否有效并给出如何修正等意见.同时智能合约要实现自动判罚,合同到期时根据结果自动执行合同的相应条款,将来甚至可以取代法院的大部分工作.文献[14]提出了一种使用可信度评分的新共识机制,这种机制不同于以太坊平台的共识机制,可以给本文系统的改良提供一个新的改良方案.

References:

[7] Zhiguo Wan, Robert H. Deng and David Lee. Electronic Contract Signing without Using Trusted Third Party[J]. ‘International Conference on Network & System Secu’, 2015:386-394.

[9] Haibo Tian, Jiejie He, and Liqing Fu. Contract Coin: Toward Practical Contract Signing on Blockchain[J]. ’International Conference on Information Security’, 2017:43-61.

[10] Miers I, Garman C, Green M, et al. Zerocoin: Anonymous Distributed E-Cash from Bitcoin[J]. 'IEEE Symposium on Security & Privacy', 2013:397-411.

[11] Eli Ben-Sasson , Alessandro Chiesa, Christina Garman , Matthew Green , Ian Miers, Eran Tromer, Madars Virza. Zerocash: Decentralized Anonymous Payments from Bitcoin[J]. 'Security & Privacy’,2014:459-474.

[14] Hiroki Watanabe, Shigeru Fujimura, Atsushi Nakadaira, Yasuhiko Miyazaki, Akihito Akutsu and so on. Blockchain Contract: Securing a Blockchain Applied to Smart Contracts[J]. ‘IEEE International Conference on Consumer Electro’, 2016:467-468.

附中文参考文献:

[1] Andreas M Antonopoulos.精通比特币[M].杭州:巴比特图书.

[2]区块链.URL：
https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/13465666?fr=aladdin#8.

[3] 百科：如何理解区块链的自治性？ URL:
http://3g.163.com/dy/article/DHUDV43R0519V75E.html

[4] 恰似.以信立业，一诺签金.互联网周刊,2017(14):56-56.

[5] 葛婷.在线电子合同签订的存证证明力探析[J].科技与法律，2018(1).

[6] 赵金龙,任学靖.论电子合同[J].当代法学, 2003(8):43-48.

[8] 田海博,何杰杰,付利青.基于公开区块链的隐私保护公平合同签署协议[J].《密码学报》,2017,4(2):187-198.

[12]尹稚淳.基于区块链技术的电子合同系统设计与实现[D].《沈阳师范大学》,2018.

[13] 董宁,朱轩彤. 区块链技术演进及产业应用展望[J].《信息安全研究》,2017,3(3):200-210.