FCSP-Blockchain:基于区块链技术的公平合约交换协议的实现*

于 雷[1], 孙毅[1], 张珺[3], 赵晓芳[1], 金 岩[1], 胡 斌[1,2]

[1)]（中国科学院计算技术研究所 北京 100190）

[2)]（中国科学院大学，北京 100049）

[3)]（内蒙古大学，内蒙古 呼和浩特 010021）

通讯作者：于雷, E-mail: yulei@ncic.ac.cn

摘 要: 本文给出了无可信第三方的、基于区块链技术的、确定性的公平合约交换协议的实现，改变了目前交易类型区块链技术的单向信任关系，通过附加协议，在区块链参与节点之间建立了多向信任关系。将交易类型区块链的交易内容转换为待签合约，通过多方之间发送“转账”交易单，实现多方之间对合约的签名确认。本协议规定：多方在链接的交易单之中完成随机顺序签名确认后，为合约生效的唯一确认。由于区块链交易数据的公开性、不可篡改性和不可否认性，避免了合约任何一方的作弊行为，保证了合约交换过程的公平性，也保证了合约交换完毕之后的均势。同时，为多方合约提供了实时动态管理功能，包括合约内容的追加、更新和删除。最后讨论了该协议的公平性、隐私性及共识机制的选择问题。

关键词: 公平合约交换协议；区块链；双向信任；合约更新；隐私

中文引用格式: 于雷,孙毅, 张珺,赵晓芳,金岩,胡斌. FCSP-Blockchain:基于区块链技术的公平合约交换协议的实现.软件学报. http://www.jos.org.cn/1000-9825/ 0000.htm

英文引用格式: Yu L, Sun Y, Zhang J, Zhao XF, Jin Y, Hu B. FCSP-Blockchain: Implementation of Fair Contract Signing Protocol Based on Blockchain Technology. Ruan Jian Xue Bao/Journal of Software, 2016 (in Chinese). http://www.jos.org.cn/1000-9825/0000.htm

FCSP-Blockchain: Implementation of Fair Contract Signing Protocol Based on Blockchain Technology

YU Lei[1], SUN Yi[1], ZHANG Jun[3], ZHAO Xiaofang[1], JIN Yan[1], HU Bin[1,2]

[1)](Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190)

[2)] (University of Chinese Academy of Sciences, Beijing 100049)

[3)] (Inner Mongolia University, Hohhot, China 010021)

Abstract: This paper presents the realization of deterministic fair Contract Signing protocol based on blockchain technology without trusted third party, which changes the one-way trust relationship of the transaction blockchain technology and establishes a multi-way trust relationship between the nodes participating in the blockchain through an additional protocol. The transaction content in blockchain is replaced by the contract to be signed, then, conduct "transfer" transactions between multiple parties, to achieve multi-party sign the contract in the random order. It is the only confirmation that the contract is effective when multiple parties complete the sequential signature among the linked tickets. Due to the openness, tampering and non-repudiation of the blockchain transaction data, the cheat of any party in the contract is avoided, the fairness of the contract exchange process is guaranteed, and the balance between multiple parties is completed after the contract exchange. At the same time, this protocol provides real-time, dynamic management of multi-party contracts, including the addition, renewal and deletion of contract content. Finally, the paper discusses the fairness, privacy and the choice of blockchain consensus.

Key words: fair contract signing protocol; blockchain; two-way trust; contract renewal; privacy

1 引言

1.1 公平合约交换协议

在社会生活中涉及多方经济利益及法律责任的数据，最终呈现为多种形式的合约（保险合同、银行存单等）。在以纸质材料为存证要素时，通常情况下，利益和责任各方相互留存纸质材料作为存证是可行，因为纸质材料包含了各方的签名、指纹、印章、身份证复印件等内容，并且，在线下可以保证双方同时公平获得对方签署的纸质合约，这样即可作为具有法律效力的存证数据。在数字化深入发展今天，只有将纸质合约电子化、数字化、去纸化，才能利用目前信息技术和大数据技术优势，提高存证数据管理的效率。

涉及“多方利益及责任”的合约数据数字化之后，通过 PKI/CA 体系的非对称秘钥数字签名机制，可以实现对合同内容的安全加密传输及单方确认签字；通过单向哈希摘要算法可以验证合约数据的

基金项目：面向无线网络的节点行为建模及安全技术研究基金（61202413），国家自然科学基金（61772502，61672499）

This work is supported by the National Science Foundation of China (61202413, 61772502, 61672499)

CNKI 在线出版时间: 0000-00-00

完整性、并且可以提高数字签名的效率。除此之外，确保电子合约的公平交换协议（Fair Contract Signing Protocol, FCSP）是实现线上电子合约签署的必要条件。公平交换协议指的是，双方通过网络相互发送经过己方数字签名的合约数据，合约内容对双方来说都是公平的（公平指的是合约内容即包括双方的“利益”，也包括双方的“责任”），数字签名都是可由对方验证的，在双方互不信任的情况，合约的交换过程要保证公平性，也就是说，不管交换过程成功与否（可能网络故障意外终止交换过程、也可能某一方恶意终止交换过程），都应该使得交换的双方处于均势。如果合约签署交换过程正常进行，双方都能得到各自所需的数据（对方的数字签名），如果交易过程异常终止（包括协议某一方的恶意终止），任何一方（包括恶意终止的一方）都不占优势。公平合约交换协议要解决的不仅仅是节点异常或网络异常的行为，而是要解决任何一方作弊时（为了逃避合约“责任”，或是为了获得不公平“利益”），在被诚实的一方举证后，经过第三方仲裁，都不能否认诚实方的合约利益，也不能否认己方的合约责任。实现公平合约交换协议，可以划分为两种类型：1)有可信第三方（Trusted Third Party, TTP）的实现方式；2）无可信第三方的实现方式。

1.2 区块链技术

近年，以比特币[1]为代表的数字货币实践获得广泛关注，数字货币的底层技术平台是区块链（Blockchain）技术，区块链的核心协议可以概括为以下几个技术术语的组合：P2P 网络、基于非对称秘钥机制的签名验证、全网共同遵守的当前时间段交易信息共识、基于单向 HASH 算法的交易历史链式数据结构，这在“中本聪”的论文《Bitcoin: a peer-to-peer electronic cash system》进行了详细的描述。可以将区块链技术的本质视为分布式数据库，该数据库保存历史交易数据，这个数据库被所有节点通过分布式一致协议共享[9]。区块链技术的核心价值包括去中心化，分布式共识、非对称秘钥的签名和加密、时间戳，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，从而为解决中心化机构普遍存在的高成本、信用垄断、可靠性依赖等问题提供了解决方案。具体的区块链的定义可描述如下：区块链是一种按照时间顺序将数据区块用类似链表的方式组成的数据结构，并以分布式共识和密码学方式保证区块链的数据全局一致、不可篡改和不可伪造的分布式去中心化账本，能够安全存储简单的、有先后关系的、能在系统内进行验证的数据[2]。区块链的出现解决了数字货币的两大问题：双重支付问题以及拜占庭将军问题[3-8]。区块链技术在金融、保险、支付、公证等领域有广阔的应用前景。

一般而言，目前的区块链类型可以分为两类：

1．记录交易单链接类型的区块链，以下简称交易类型的区块链。

2．记录账户变化信息的区块链，简称账户类型的区块链。

本文只利用交易类型的区块链协议，账户类型的区块链不在本文进行讨论，本文以下内容都是基于交易类型的区块链协议进行的描述及讨论。

当前，交易类型区块链技术并没有形成行业标准，基本的区块链的数据结构如下图所示：

Fig. 1 Basic data structure of blockchain.

图 1 区块链的基本数据结构

区块链协议中的链式结构、交易信息的 Merkle 树和共识机制，保证了历史交易数据极难被篡改，其中的交易数据为本段时间内的交易单信息，其中的交易单的逻辑结构如下图所示：

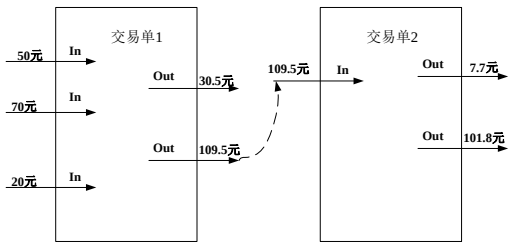

Fig. 2 Logical link of the transactions in blockchain.

图 2 交易型区块链交易单的逻辑链接

以比特币为例，从创世区块开始，区块链历史账本数据中，包含了数字资产的首尾相接转账交易单构成的交易链条，上一个交易单的输出（out）成为当前交易单的输入（in），当前交易单的 out，又可以作为下一个交易单的 in，每个交易单的具体数据结构如下：

```
{
  hash:[代表本交易单的哈希值],
  in:  //收入来源项内容
  {
      prev_out:  //前置交易信息
      {
          hash:[代表前置交易的哈希值],
          n:[代表输出项 out 的索引值]
      },
      scriptSig:  <sig>  <pubKey>  //拥有者的签名和公钥
  },
```

out: //支出去向项内容

{

value:[付款金额],

address: [代表收款方地址的哈希值],

scriptPubKey:脚本内容

验证使用者的公钥地址与当前指向的公钥地址哈希值匹配（基于非对称秘钥机制）;

验证使用者的数字签名与使用者的公钥匹配（基于非对称秘钥机制）;

},

}

首尾相接的交易单数据（包含交易发送方的数字签名）经过脚本内容的验证为合法后，被不同时间戳的区块进行记录，构成首尾相接的区块链的数据主体。区块链网络的节点通过共识过程，竞争交易单的记账权，避免“双花”问题，避免历史交易数据被轻易篡改。

基于去中心化的点对点交易需求以及系统可靠性方面的考虑，区块链技术普遍基于 P2P 网络，网络中的每个节点以扁平式拓扑结构相互连通和交互，不存在任何中心化的特殊节点、不存在层级结构，每个节点均会承担网络路由、验证交易单、验证区块数据、传播区块数据、发现新节点等功能。

本文的主要贡献如下:

1) 利用区块链技术，实现了多方的、无 TTP 的、确定性的 FCSP 协议，并且提供了公平合约的追加、更新和删除管理功能。

2) 改变了区块链的“单向信任”模式，为区块链网络建立了双向信任（或称多向信任）。

3) 分析了方法的公平性、有效性和隐私性。

本文第 2 节对 FCSP 协议的研究进行总结。第 3 节对本文实现的协议进行综述，包括区块链协议改造、系统搭建、公平合约的交换过程和更新过程。第 4 节对本文实现的协议进行公平性、隐私性和共识方面的讨论。第 5 节描述了本协议的概要内容并总结。

2 相关工作

线上公平合约交换协议（Fair Contract Signing Protocol，简称 FCSP）可以被划分为两种类型：1)有可信第三方（Trusted Third Party, TTP）的实现方式，包括在线和离线两种情况；2）无可信第三方的实现方式。

1.无 TTP 的协议：文献[20]中已经证明，如果没有第三方参与，利用数字签名方法，两方之间是不存在确定的 FCSP 协议的，原因在于双方之间发送签名的顺序，双方无论经过多少轮的顺序签名，被提前终止发送顺序签名的一方都会被质疑是否向对方传递顺序数字签名，而使得自身保存的顺序数字签名无法主张权利。基于此，Even[11]，Goldreich[12]等人也给出了无 TTP 的、近似的 FCSP 实现，他们的方案是将己方的数字签名数据分散为多份，每份进行一个确定难度的加密运算，将加密的签名数据分片传递给对方之后，双方同步相互发送己方的数字签名加密分片的解密秘钥，己方获得一份秘钥之后，发送己方的一份秘钥给对方，如此往复，直到双方都收到全部的分片秘钥，显而易见，这不是一个确定性的无 TTP 方案，因为，当一方收到最后一份秘钥之后，他可能拒绝发出自己最后的一份己方秘钥，另一方只能通过解密的方式求解最后一份秘钥，虽然假定加密算法的难度是确定的，但是他仍然可能在有效的时间内无法破解最后一份秘钥，从而使得自己处于被动劣势地位。

2.基于在线 TTP 的协议：文献[13]的 FCSP 协议需要半信任的第三方来保证每一次交换的公平性，并且保证第三方在内的任何一方提前终止数据交换，都不会是获得任何益处，也不会使得利益不均衡，但是需要确保的前提是第三方不会与任何一方同谋。Alawi 等人在文献[14]中给出了名为 Halevi-Micali“承诺”方案，要求准备签署合同的双方把合同交给第三方做备案记录，这需要在线 TTP 的支持。该方案可以应用到互联网上。该方案实现的公平交换协议保证了“乐观，公平和无滥用”等安全特性，并且，该方案使用无碰撞哈希函数，即建立在基础的计算机密码学之上，使得该方案很实用。而且，只需要四轮数据交换即可完成协议过程，通信和计算成本相对较低。Wan 等人在文献[15]号称实现了无任何 TTP 的 FCSP，但是实际上，该文献提到的可信时间戳服务充当了 TTP 角色。

3.离线 TTP 协议：[16-19]分别利用数字签名技术的不同方面提出了 FCSP，它们都需要第三方离线 TTP 在争议时提供验证服务和仲裁。

区块链技术以“去中心化”为核心特征，对应了 FCSP 的无 TTP 需求，其中文献[21]给出了基于区块链技术的 FCSP 的三方实现，其核心思想是三方在对合约进行数字签名之后，在比特币网络上发布对赌交易，没有传递自身签名的一方会被惩罚失去对应的比特币，此方案是基于区块链技术首次尝试实现 FCSP，此方案的缺点也是明显的，此方法依赖比特币一类的公有链数字货币，并且，当对赌的数字货币的价值低于公平协议包含的价值时，此方案将会失效。

文献[23]利用以太坊区块链的智能合约实现了公平合约交换协议的部分第三方功能，其实现的基本方法是将待签协议以交易单的形式发布在以太坊的区块链网络内，等待对手方的签名确认或由己方签名废弃。此方法的缺陷是在公有链的线上环境暴露了合约内容，这在真实的商业场景是不能接受的；其实现的交换协议只适用于两方，不能推广到多方的合约场景；并且只适用于交换“利益”，不能适用交换“责任”。

文献[25]在比特币网络上实现了公平交换混合器

（fair-exchange mixer），通过公平交换混合器实现比特币与“收据”之间的公平交换，但是，交换过程效率低下，通常需要几个小时完成，这不适用于在线合约交换的应用场景。文献[24]和[26]也使用公平交换混合器作为中介机构保证发送双方匿名发送比特币，公平交换混合器是无法窃取中间资金的，与[25]相比，在效率上做了优化，同样，这三个方案都是建立在比特币网络之上的有“中心”机构公平交换，并且只能适用于交换“利益”，即以比特币（转账比特币是不包含责任的）为交换媒介。

文献[22]使用比特币网络实现了数字货币与线上数据之间的公平交换。大概过程分为三个步骤，**1)数据证明，**数据卖方 S 将售卖数据分成多份，S 产生非对称秘钥对 $\{PK, SK\}$，用公钥 PK 分别将拆分为多份的数据加密传递给买方 B，同时将 PK 传递给 B，B 随机将部分数据分片要求 S 提供解密证据，证明数据的正确性，S 将 B 提供的部分数据用 SK 解密之后返回给 B，B 可以验证解密数据的正确性，并可证明解密数据与原加密数据一致。**2)签名承诺，**B 提交一个当前消息给 S，请求 S 用 SK 进行签名，S 将签名之后的数据返回给 B，B 用 PK（上一步骤得到）可以验证 SK 的正确性。**3)私钥交换，**B 在比特币网络创建一个私钥锁定交易（private key locked tRanRaction）Tx_1 用于执行原子性的私钥交换，在该交易中提交购买数据所需的比特币，Tx_1 被记入新区块并经过确认后，S 看到了 Tx_1 之后，使用自己的私钥 SK 和 Tx_1 构建新的交易 Tx_2，将 Tx_1 的比特币转账进入 S 的新公钥地址，Tx_2 被广播到网络之后，B 即可获得 SK 的信息，使用 SK 解密购买的数据。通过以上过程，实现了 B 和 S 之间的公平交换，此方法需要区块链内的智能合约脚本支持私钥锁定交易，适用于比特币及其它线上数据之间的公平交换，且 B 和 S 之间交易的数据需要能被分片验证正确性（例如利用视频片段或图像片段验证完整数据的正确性）。目前该方法基于在比特币区块链实现，依赖比特币的脚本语言。此方法只适用于交换 “利益”的场景，不适用于交换“责任”的场景，不能适用于公平交换合约（合约中既包含双方的“利益”，也规定了双方的“责任”）的场景，也就是说，当“责任”数据交换成功之后，当责任事件发生后，某一方为逃避责任，可以通过藏匿自身收到的数据，声明没有收到过对手方发送的“责任”，此时，基于公平原则，对手方收到的数据也不能在声明权利（因为比特币网络是完全匿名的，无法证明对手方发送了自身签名的数据），从而造成了交换“责任”的失效。

3 基于区块链技术的线上公平合约交换

目前，学术界和工业界还未出现基于区块链技术体系的公平合约（合约中包括利益、也包括责任划分）交换协议实现，区块链核心协议中实现了在不信任的网络节点之间建立“去中心的”信任，但是这种信任是百分之百单向的、不公平的，以比特币支付为例，A 向 B 支付了一笔比特币后，B 可以信任 A 的支付行为，但是 A 仍然无法信任 B，并且数字货币的支付只包含了“利益”的交换，没有包含“责任”的交换，基于此，本文将区块链的核心协议进行了改造，建立 A 和 B 之间的双向信任关系，实现“利益与责任”的公平交换。

3.1 合约目标

首先，将交易类型的区块链网络交易的内容从“数字”货币，转变为待双方（或多方，本文以下以两方 A 和 B 的形式讨论，最后给出多方的推广方法）签署合约内容 m 的哈希摘要 $H(m)$，在双方 A 和 B 的交易过程中，完成交易双方对 $H(m)$ 的顺序三轮签名，假设 A 和 B 的签名分别为 $Ra(H(m))$ 和 $Rb(H(m))$，由于签名的交易数据广播到网络内，经过全网共识记账之后，链入全局一致的区块链数据结构中，这保证了签名在双方传递的过程及各自的签名过程是无法抵赖、无法藏匿的。为了达到 FCSP 的公平性，需要确保双方都能获得对方的签名合约，只需在协议中规定：顺序的三次签名交易 $Ra(H(m))$、$Rb(Ra(H(m)))$ 和 $Ra(Rb(Ra(H(m))))$ 都被记账，才使双方最终确认合约生效（Ra 和 Rb 的签名没有严格的起始顺序要求，只需相互间隔即可），除此之外的情况，都认为合约是无效的；在顺序签名过程的未完成时，任何一方都可在当前签名链条的末尾链接一个“合约废止”签名，使得当前公平合约交换过程正常终止。此种方法源于无 TTP 时顺序数字签名的“递归质疑公平性”[116]。在区块链的技术体系下，任何一方的签名都会被广播到全网，通过全网的共识、记账、验证过程，将签名顺序记入共享区块链账本，这保证了任何一方都无法通过藏匿最后一次获得的签名数据而逃避合

约规定的责任，因为签名顺序是公开记录在共享区块链账本中的，因此双方获得了同等的权益和责任保证。以下给出基于交易类型的区块链协议实现 FCSP 的具体方法。

3.2 线上公平合约的建立机制

3.2.1 系统架构及数据结构

以交易类型（例如比特币）区块链协议和系统为原型，进行针对公平合约交换协议 FCSP 的改造，搭建专用区块链网络，称为：FCSP-Blockchain，这个区块链系统内，将交易类型的区块链系统内的交易单的交易内容从“数字”货币，转变为文本内容的公平合约 m，具体的组网方式如下图所示：

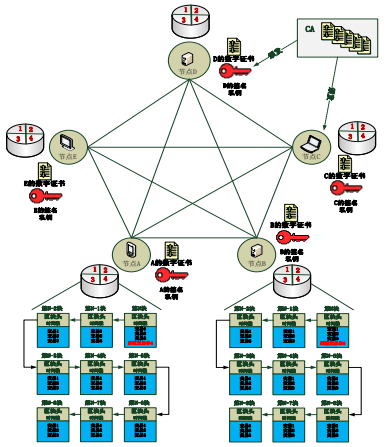

Fig. 3 Networking between nodes of FCSP-Blockchain.

图 3 FCSP-Blockchain 的参与节点 P2P 组网方式

本方案中包含 CA 中心，用于向参与节点颁发实名绑定的数字证书，每个节点用数字证书对应的公私钥完成交易过程和交换合约内容的签名、验签，由于交换的合约既包括“利益”，还包括“责任”，实名数字证书用于避免节点为逃避“责任”，而否认己方的公私钥。本方案中引入 CA 中心并非是向中心化的退化，更非传统的可信第三方的角色（TTP）。可以通过其它更简单的方式取消 CA，例如，要求参与 FCSP-Blockchain 的所有节点在区块链之外公开自己的公钥信息，即可不再需要 CA。

首先将待签合约内容数字化为数据 m，将交易单的交易有效内容从“数字”货币替换为 m 或 A、B 双方对 m 的签名确认。将公平合约交换协议中包含的各方签名确认转变为区块链网络的交易单“转账”过程。合约交换过程未完成时，允许任何一方终止交换过程，合约 m 的终止消息为 dm。

一般情况下合约的线上签署过程分为发起方和确认方，由于合约的多轮签署及确认是一个动态的过程，因此为了保证存证数据的权威性，基于区块链技术的 A 和 B 双方合约签署过程，既要实现合约内容由双方（发起方和确认方）进行数字签名确认，也要实现合约多轮的签署过程由双方签名并确认，不妨设 A 为发起方，B 为确认方。具体的初始化流程如下：

3.2.2 双方公平合约的创建及确认

1）首先由 A 发起合约 m 的签署确认的初始化过程，A 将包含 m 的初始化信息形成以下内容的交易单结构，

{

hash:[代表本交易单的哈希值（例如：abc）],

in: //来源项内容

{

prev_out: //前置交易信息

{

hash:[为空 NULL],

n:[为空 NULL],

},

scriptSig: <sig> <pubKey> //拥有者的签名和公钥）(为空 null)

},

out: //去向项内容

{

content:[内容 m],

contentHash:[m 的单向哈希摘要信息 H(m)],

contentHashSigA:[A 对 H(m)的数字签名 Ra(H(m))],

contentHashSigB:[为空：null],

addressB: [代表 B 地址的哈希值],

scriptPubKey:脚本内容如下:

{

验证确认方（B）的公钥地址与当前指向的公钥地址哈希值匹配 （基于非对称秘钥机制）;

验证确认方（B）的数字签名与当前指定的的公钥匹配（基于非对称秘钥机制）;

}

},

{

content:[内容 dm],

contentHash:[m 的单向哈希摘要信息 H(dm)],

contentHashSigA:[A 对 H(m)的数字签名 Ra(H(dm))],

contentHashSigB:[为空：null],

addressA: [代表 A 地址的哈希值],

scriptPubKey:脚本内容如下:

{

验证发起方（A）的公钥地址与当前指向的公钥地址哈希值匹配 （基于非对称秘钥机制）；

验证发起方（A）的数字签名与当前指定的的公钥匹配（基于非对称秘钥机制）；

}

}

}

A 将以上数据结构封装为区块链网络的交易单信息，广播到区块链网络，表示 A 已经确认签名确认了 m ，且等待 B 的签名确认（或等待 A 链接终止交易单）；

2）区块链网络的共识节点接收到该交易单信息后，共识判断该交易单为 A 发起的合约签署初始化过程，因此不需对交易单的来源项进行验证，经过区块链网络的共识过程和共识验证，将本交易单写入区块链的历史区块中；

3）B 客户端通过区块链历史数据，发现有指向自己公钥地址的待确认合约签署请求，B 通过查询获得 A 提交的交易单数据，通过该交易单构造新的交易单如下：

{

hash:[代表本交易单的哈希值（例如：def）],

in: //来源项内容

{

prev_out: //前置交易信息

{

hash:[代表前置交易的哈希值：abc],

n:[代表输出项 out 的索引值：0]

},

scriptSig: <sig> <pubKey> //拥有者 B 的签名和公钥

},

out: //去向项内容

{

content:[为空：NULL],// //节省空间

contentHash:[为空：NULL], //节省空间

contentHashSigA:[A 对 H(m)的数字签名 Ra(H(m))],

contentHashSigB:[B 对 H(m)的数字签名 Rb(H(m))],

addressA: [代表 A 地址的哈希值]

scriptPubKey:脚本内容如下:

{

验证 A 的公钥地址与当前指向的公钥地址哈希值匹配（基于非对称秘钥机制）；

验证 A 的数字签名与当前的公钥匹配（基于非对称秘钥机制）；

}

},

{

content:[为空：NULL],// //节省空间

contentHash:[为空：NULL], //节省空间

contentHashSigA:[A 对 H(m)的数字签名 Ra(H(m))],

contentHashSigB:[B 对 H(dm)的数字签名 Rb(H(dm))],

addressB: [代表 B 地址的哈希值],

scriptPubKey:脚本内容如下:

{

验证确认方（B）的公钥地址与当前指向的公钥地址哈希值匹配 （基于非对称秘钥机制）；

验证确认方（B）的数字签名与当前指定的的公钥匹配（基于非对称秘钥机制）；

}

}

}

B 将该交易单广播到区块链网络，表示 A 对合约 m 的签名已经被 B 确认，并且 B 也对合约 m 进行了签名；

4）区块链网络共识节点接收到该交易单，共识节点验证该交易单的合法性（验证 B 的公钥地址与前置交易单的输出公钥地址是否匹配，验证 B 的数字签名与公钥地址是否匹配），验证通过后，经过区块链网络的共识过程和验证过程，将该交易单写入区块链网络的历史区块中；

5）A 客户端通过区块链历史数据，发现有指向自己公钥地址的待确认合约签署请求，A 查询获得 B 提交的交易单数据，通过该交易单构造新的交易单如下：

{

hash:[代表本交易单的哈希值（例如：ghi）],

in: //来源项内容

{

prev_out: //前置交易信息

{

hash:[代表前置交易的哈希值：def],

n:[代表输出项 out 的索引值：0]

},

scriptSig: <sig> <pubKey> //拥有者 A 的签名和

公钥

},

out: //去向项内容

{

content:[为空：null],//节省空间

contentHash:[为空：null], //节省空间

contentHashSigA:[A 对 H(m)的数字签名 Ra(H(m))],

contentHashSigB:[B 对 H(m)的数字签名 Rb(H(m))],

addressA: [代表 A 地址的哈希值],

scriptPubKey:脚本内容如下:

{

验证 A 的公钥地址与当前指向的公钥地址哈希值匹配（基于非对称秘钥机制）;

验证 A 的数字签名与当前的公钥匹配（基于非对称秘钥机制）;

}

},

{

content:[为空：null],//节省空间

contentHash:[为空：null], //节省空间

contentHashSigA:[A 对 H(m)的数字签名 Ra(H(m))],

contentHashSigB:[B 对 H(m)的数字签名 Rb(H(m))],

addressB: [代表 B 地址的哈希值],

scriptPubKey:脚本内容如下:

{

验证 B 的公钥地址与当前指向的公钥地址哈希值匹配（基于非对称秘钥机制）;

验证 B 的数字签名与当前的公钥匹配（基于非对称秘钥机制）;

}

}

}

A 将以上数据结构封装为区块链网络的交易单信息，广播到区块链网络;

6）区块链网络的共识节点接收到该交易单信息后，共识节点验证该交易单的合法性(验证 A 的公钥地址与前置交易单的输出公钥地址是否匹配，验证 A 的数字签名与公钥地址是否匹配)，验证通过后，经过区块链网络的共识过程和验证过程，将该交易单写入区块链网络的历史区块中;

经过以上的过程，确认了两项内容：1)A 和 B 双方对合约内容 m 的数字签名；2)A 和 B 对合约的顺序数字签名确认。这个过程保证了合约内容的可信性、不可抵赖性和合约签署过程的可信性、不可抵赖性（不可藏匿）；当三次顺序签名的交易单被区块链网络记入区块链数据结构以后，双方之间的公平合约即建立。此后，合约内容是无法单方撤销的，需要双方的再次三次签名确认过程才能撤销已建立的公平合约（后面将会叙述）。

在前两个交易单的数据结构中，双方都在交易单的输出 out 的第二项内容中，加入了本方的交易地址，目的是，在合约交换还未完成时，允许任何一方终止还在交换过程中的公平合约。区块链的共识机制避免了“分叉”现象，因此，交换过程中的公平合约，当任何一方发布链接“终止合约”交易单，对手方同时发布“确认”合约交易单时，区块链的全网共识机制，保证了只能有一种一个交易单被成功记入区块链全局账本数据中，这保证了公平合约交换过程的全局数据一致性。无论公平合约成功建立，还是某一方终止合约交换过程，都不影响其公平性、不可抵赖性和不可撤销。由其在区块链网络内形成的交易单链接图如下所示：

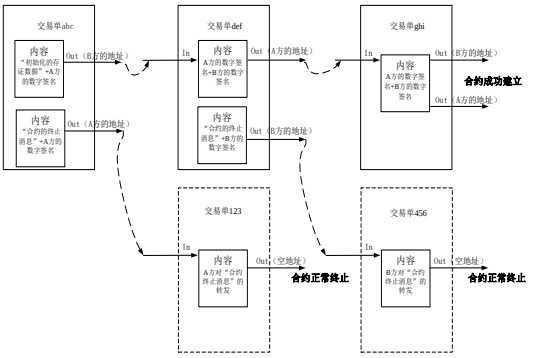

Fig. 4 Creating contract and signature transfer process between A

图 4 合约创建及 A 和 B 双方的签名确认过程

其合约终止交易单可有 A、B 中的任何一方发起，数据结构如下所示：

{

hash:[代表本交易单的哈希值（例如：123）],

in: //来源项内容

{

prev_out: //前置交易信息

{

hash:[代表前置交易的哈希值：abc,

```
                n:[代表输出项 out 的索引值：1]
            },
            scriptSig:  <sig>  <pubKey>  //拥有者 A 的签名和公钥
        },
        out:  //去向项内容
        {
            content:[为空：null],//节省空间
            contentHash:[为空：null],  //节省空间
            contentHashSigA:[A 对 H(dm)的数字签名 Ra(H(dm))],

            address: [Null],
            scriptPubKey:脚本内容如下:
            {
                无法获得有效的验证（由于输出指向地址为 Null，此交易单的输出项将无法被使用）
            }
        },
        {
            content:[为空：null],//节省空间
            contentHash:[为空：null],  //节省空间
            contentHashSigA:[A 对 H(m)的数字签名 Ra(H(m))],

            contentHashSigB:[B 对 H(m)的数字签名 Rb(H(m))],

            addressB: [代表 B 地址的哈希值],
            scriptPubKey:脚本内容如下:
            {
                验证 B 的公钥地址与当前指向的公钥地址哈希值匹配（基于非对称秘钥机制）;
                验证 B 的数字签名与当前的公钥匹配（基于非对称秘钥机制）;
            }
        }
}
```

不难发现，图 5.2 中的交易单链接关系，为了保证合约交换过程的数据一致及状态一致，避免造成“合约正常终止”与“合约成功建立”同时发生而出现的矛盾，其区块链全网节点的交易单合法性验证，与目前的交易类型区块链交易单合法性验证略有不同，即每个交易单，输出项 Out 索引中不论包含多少个有效输出项，只能有一个输出项能被后续交易单使用，交易单的某个输出项被后续交易单使用之后，此交易单其它输出项同时变为无效状态，即某个交易单的多个输出项被后续交易单使用时，会被其它节点验证交易单输入项不合法。在区块链网络的共识协议保证下，避免了交易单的“分叉”现象，多个矛盾的交易单同时在区块链网络发布时，只能有其中一个交易单被成功记入区块链网络，这使得合约交换过程要么被双方确认成功，要么被某一方确认终止，不会产生矛盾的交易单分叉情况。

3.2.3 双方公平合约的追加、更新和删除

在上述过程中，在末尾交易单 ghi 构造新的交易单，可以在合约公平交换协议中实现合约内容的追加、更新和删除过程。“追加”指的是在合约内容 m 之后补充新的条款 m'；“更新”指的是在合约内容 m 之后补充新的条款 m'，且 m' 中包含与原 m 相矛盾的内容时，以最新的补充条款 m' 为准；“删除”指的是在合约内容 m 之后补充新的条款 m'，且 m' 的内容为对 m 的失效声明。由此可知，合约内容 m 的追加、更新和删除都表现为在交易单 ghi 之后链接新的交易单，且新交易单的双方待签内容为 m'，因此，以下将追加、更新和删除过程抽象为相同的过程：在合约内容 m 之后追加新的合约内容 m' 并确认 m'。合约更新的交换过程未完成时，允许任何一方终止合约更新过程，合约更新内容 m' 的终止消息为 dm'。

其在区块链网络内形成的合约更新过程交易单链接示意图如下所示：

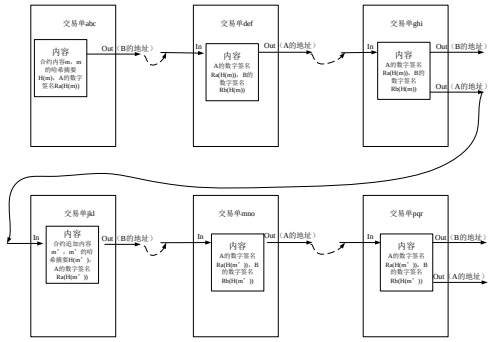

Fig. 5 When the contents of the contract are added, signature transfer process between A and B.

图 5 合约内容追加时的 AB 双方签名确认过程（省略了交换过程被

正常终止的展示）

3.3 多方公平交换协议的推广

以上的讨论中，只涉及 A 和 B 两方进行合约的公平交换过程，不难发现，可以将以上的实现过程推广到 N 方之间，即将以上的三次交易单链接过程，推广为 $N+1$ 次交易单链接过程，每个链接的交易单是 N 方之一进行数字签名确认过程，新链接的交易单的输出地址指向 N 方中剩下所有未签名确认的参与方，剩下所有未签名确认的每个参与方，通过竞争在交易单链条末尾链接自己的签名确认交易单，区块链网络的共识机制会保证对这些竞争的交易单其中之一（同时在某个交易单链条末尾竞争签名的交易单在同一时间是相互矛盾的，只能有一个交易单被成功记入当前新生成的区块中）进行记账，未被成功记账的参与者会选择在新的交易单链条末尾竞争记账，直到 N 方中的所有参与者都将自己签名确认的交易单链接到本次合约的交易单链条中，合约签署的发起方最后会链接一个指向 N 方所有地址的交易单在此交易链条的末尾作为截止，以便 N 方中任何一方都可发起合约内容的追加、更新和删除请求。区块链网络的共识协议避免了签名交易单链条的分叉，最终保证了只有唯一的一个签名顺序会被记入全网一致的区块链数据结构中，如图 5.4 所示：

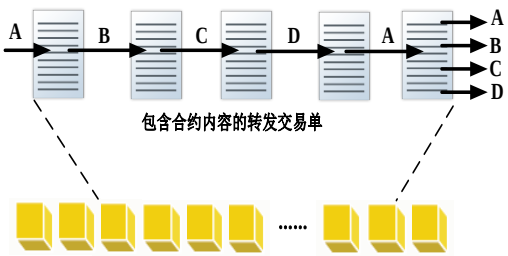

Fig 6 The unique signature order between N parties is recorded in the blockchain data structure

图 6 N 方之间的唯一签名顺序记入区块链数据结构（省略了交换过程被正常终止的展示）

通过以上过程，形成的 N 方之间的签名顺序是随机的，这通常是现实中的合约所需要的，这也是合约的线上交换过程的公平性体现之一。

同样的，在 N 方之间的合约交换和更新过程中，可由 N 方中的已完成交易单链接的任何一方提前终止合约交换过程，这与两方之间的合约正常终止过程类似，不再赘述。

4 特性分析

4.1 公平性

本文中合约交换过程的公平性讨论如下：

1）本协议规定，只有经过 $N+1$ 次链接的交易单被记入区块链数据结构之后，N 方数字签名确认的合约内容才是生效的状态，除此之外，都是无效状态。因此，任何一方提前终止 $N+1$ 次交换过程，既不会使得本方获益，也不会使得对手方受害；

2）$N+1$ 次链接的交易单被成功记入区块链全局账本之后，因为区块链全局账本的公开透明性，所以任何一方都无法否认某一次签名确认的行为（公钥是提前公开的，或者采用 CA 颁发的数字证书），从而避免了通过藏匿签名数据而逃避责任的行为，因此，区别于原始区块链技术的单向信任关系，本文的协议改造方案使得区块链的节点之间建立了多方之间的任意双方的双向信任关系。

4.2 隐私性

在上节的讨论中，为便于说明，将合约内容原文 m 写入了交易单 abc 中，显然，将交易单 abc 中的合约内容 m 去掉，只保留 $H(m)$，不会影响本协议的正确性和可验证性，从而实现针对合约内容的隐私性。

但是，由于采用公开的公钥信息（或 CA 颁发的数字证书）进行合约内容和交换过程的数字签名，因此，这样的信息：“实体 A 和 B 之间发生了一次交换合约行为”仍然是公开的，实现这个信息的隐私是本文未来的工作，零知识证明是可选择的方案之一。

4.3 共识协议的选择

本协议依赖的区块链技术来源于交易类型的区块链（例如比特币）。改造的主要内容是：1)交易的有效数据从“数字货币”变成了待签合约（或待签合约的哈希摘要）；2)参与节点必须公开自己的公钥信息（或是采用 CA 颁发的数字证书），用公开的公钥信息对应的公私钥完成数字签名和验签。除以上两点之外，本协议可完全继承交易类型区块链协议的其它部分。但是，出于对效率的考虑，

可以替换基于算力竞争的共识协议，采用更加合适的共识协议，以便在效率和安全性上做恰当的折中。

5 结论

无 TTP 的 FCSP 协议还未有确定性的实现，有 TTP 的 FCSP 协议实现的缺点是明显的，包括信用单点、可靠性单点、额外的第三方成本等。本文提出了基于区块链核心协议的、无 TTP 的、确定性的 FCSP 协议实现。将交易类型的区块链的交易内容替换为合约内容，公平合约交换的参与方依次构造 $N+1$ 次的链接交易单，结合区块链的共识协议实现了合约内容的依次签名确认，并且避免了合约签名链条的分叉。本实现协议规定：$N+1$ 次的顺序交易单都被记入区块链全局账本数据中以后，视为唯一合约生效的确认，除此之外的情况都为无效的合约交换。合约交换过程中，任何一方都可以提前终止交换过程。此方法实现的 FCSP 避免了任何一方在合约交换过程中、合约交换完成之后的作弊行为，实现了确定的公平性。此方法利用区块链的交易单链接可以实现合约内容的公平追加、更新和删除。此外，本文实现了区块链参与节点之间的双向信任关系。避免“A 和 B 之间发生了一次合约交换行为”的信息泄露是未来研究的待解问题。

References:

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. https://bitcoin.org/bitcoin.pdf: bitcoin,2008

[2] 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

[3] Lamport L, Shostak R, Pease M, The Byzantine Generals problem[EB/OL]. https://www.microsoft.com/en-us/research/wp-content/uploads/2016/12/The-Byzantine-Generals-Problem.pdf: microsoft,1982

[4] FAN J, YI L T, SHU J W. Research on the technologies of Byzan-tine system[J]. Journal of Software, 2013, 24(6):1346-1360

[5] NELSON M. The Byzantine General’s problem:an agreement protocol for distributed system[EB/OL]. http://www.drdobbs.com/cpp/the-byzantine-generals-problem/206904396: drdobbs,2008

[6] LAMPORT L. The weak byzantine generals problem[J]. Journal of the ACM (JACM), 1983, 30(3): 668-676.

[7] FEDOTOVA N, VELTRI L. Byzantine generals problem in the light of P2P computing[C] The International Conference on Mobile & Ubiquitous Systems: Networking & Services. 2006:1-5.

[8] REISCHUK R. A new solution for the byzantine generals problem[J]. Decision Support Systems, 1985, 1(2):182.

[9] Swan M. Blockchain Thinking: The Brain as a DAC (Decentralized Autonomous Organization. In Texas Bitcoin Conference, pp. 27-29.2015.

[10] BLUM M. How to Exchange (Secret) Keys[J]. ACM Transactions on Computer Systems, 1983, 1(2): 175-193.

[11] EVEN S. A Protocol for Signing Contracts[J]. ACM SIGACT News, 1983, 15(1): 34-39.

[12] GOLDREICH O. A Simple Protocol for Signing Contracts[C]//Advances in Cryptology. New York,USA :Springer , 1984: 133-136.

[13] FRANKLIN M K, REITER M K. Fair Exchange with a Semi-trusted Third Party[C]//Proceedings of the 4th ACM Conference on Computer and Communications Security. New York:ACM, 1997: 1-5.

[14] AL-SAGGAF A A, GHOUTI L. Efficient Abuse-free Fair Contract-signing Protocol Based on an Ordinary Crisp Commitment Scheme[J]. IET Information Security, 2015,9(1): 50-58.

[15] WAN Z, DENG R H, LEE D. Electronic Contract Signing without Using Trusted Third Party[C]//International Conference on Network and System Security. New York , USA:Springer International Publishing, 2015: 386-394.

[16] BEN-OR M, GOLDREICH O, MICALI S, et al. A Fair Protocol for Signing Contracts[J]. IEEE Transactions on Information Theory, 1990, 36(1): 40-46.

[17] ASOKAN N, SHOUP V, WAIDNER M. Optimistic Fair Exchange of Digital Signatures[J]. IEEE Journal on Selected Areas in Communications, 2000, 18(4): 593-610.

[18] HUANG X, MU Y, SUSILO W, et al. Preserving Transparency and Accountability in Optimistic Fair Exchange of Digital Signatures[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(2): 498-512.

[19] WANG G. An Abuse-free Fair Contract-signing Protocol Based on the RSA Signature[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(1): 158-168.

[20] Even, S., and Yacobi, Y., "Relations among Public Key Signature Systems", Technical Report # 175, Comp. Sci. Oept., Technion, Haifa, Israel, March, 1980.

[21] Huang H, Li K C, Chen X. A Fair Three-Party Contract Singing Protocol Based on Blockchain[J]. S. Wen et al. (Eds.): CSS 2017, LNCS 10581, pp. 72–85, 2017.

[22] Delgado-Segura S, Pérez-Solà C, Navarro-Arribas G, et al. A fair protocol for data trading based on Bitcoin transactions[J]. Future Generation Computer Systems, 2017.

[23] LIU J, LI W, KARAME G O, et al. Towards fairness of cryptocurrency payments[J]. arXiv preprint arXiv:1609.07256, 2016.

[24] Ethan Heilman, Foteini Baldimtsi, and Sharon Goldberg. Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions. In Jeremy Clark et al., editors, Financial Cryptography and Data Security – FC 2016 International Workshops, BITCOIN, VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers, volume 9604 of Lecture Notes in Computer Science, pages 43–60. Springer, 2016.

[25] George Bissias, A Pinar Ozisik, Brian N Levine, and Marc Liberatore. Sybil-resistant mixing for bitcoin. In Workshop on Privacy in the Electronic Society, pages 149–158. ACM, 2014.

[26] Gregory Maxwell. Coinswap: transaction graph disjoint trustless trading, 2013.