基于区块链的智能合约技术研究进展

朱岩[1]，王静[1]，郭倩[1]，刘国伟[2]
（1.北京科技大学计算机与通信工程学院，北京 100083；
2.北京市经济和信息化局，北京 100744）

摘 要：智能合约被认为是第二代区块链的技术核心，它是区块链从虚拟货币、金融交易协议到通用工具发展的必然结果。然而，目前智能合约技术尚不完善，对智能合约概念及内涵缺乏较为系统的分析，对基于区块链的智能合约软件系统也缺少体系上的归纳与总结。有鉴于此，文章从智能合约的基本定义入手，介绍了智能合约的发展历史、分类、规范等概念，进而从抽象计算模型角度出发给出了智能合约的通用架构，并对智能合约语言与编译机制、合约部署机制与合约运行过程予以详尽分析，上述结果将有利于把握智能合约未来研究方向。

关键词：智能合约；语言；框架；部署；运行机制
中图分类号： TP312 **文献标识码：** A

Research progress of smart contracts based on blockchain

Zhu Yan[1], Wang Jing[1], Guo Qian[1], Liu Guowei[2]
(*1.School of Computer & Communication Engineering, University of Science and Technology Beijing, Beijing 100083;
2.Beijing Municipal Bureau of Economy and Information Technology, Beijing 100744*)

Abstract: Smart contracts are considered to be the technical core of the second-generation blockchain, which is the inevitable result of the development of blockchain from virtual currency, financial transaction protocols to general tools. However, the current smart contract technology is not perfect, and there is a lack of a systematic analysis of the concept and connotation of smart contracts, as well as a systematic induction and summary of the smart contract software system based on blockchain. In view of this, this paper starts with the basic definition of smart contract, introduces the development history, classification, specification and other concepts of smart contract, and then gives the general framework of smart contract from the perspective of abstract computing model. Moreover, we provided a detailed analysis of the smart contract language and compilation mechanism, contract deployment mechanism and contract operation process. The above results will help to grasp the future research direction of smart contracts.

Key words: smart contracts; language; frame; disposition; operating mechanism

1 引言

智能合约（Smart Contract）被认为是第二代区块链的技术核心，它是区块链从虚拟货币、金融交易协议到通用工具发展的必然结果。目前几乎所有的区块链技术公司都已在其产品中支持智能合约产品，例如，以太坊基于虚拟机的智能合约平台、基于Bitcoin区块链的RSK平台、IBM公司提出的企业级HyperLeger Fabric平台等，这些产品的推出极大的丰富了智能合约技术的内涵和范围，为区块链技术在不同领域的现实应用奠定了基础，也代表了区块链未来发展的方向。

目前智能合约技术尚不完善，对智能合约概念及其内涵缺乏较为系统的介绍，对基于区块链的智能合约软件系统也缺少体系上的归纳与总结。有鉴于此，本文从智能合约的基本概念入手，介绍智能合约的历史、分类、规范等基本概念，进而对智能合约的框架、语言与编译、部署与运行进行阐述。本文研究结果将为相关领域研究提供系统的指导，有利于更好地把握智能合约未来研究方向。

2 智能合约概念

合约是特定人之间签订的契约，在生活中随处可见，是一个使未取得彼此信任的各参与方具有安排权利与义务的商定框架。而智能合约在广义上讲是指任何符合多方之间约定的计算机协议。首先，智能合约是一种可由计算机处理的协议，与通常由单台计算机执行的算法不同，它需要两名或多名参与者共同协作来完成计算任务；其次，计算机协议的运行必须满足参与者事先的约定，这既体现了协议遵循的可信性与合规性（或合法性），又体现了为了保证协议合规性所必需的技术手段，包括协议验证、存证、争议解决等[1]。此外，与传统纸质协议相比较，多方协议的计算机化以及相应保障技术的采纳间接体现了智能合约的智能化。

上述定义较为广泛，几乎能够将所有的计算机协议囊括其中。据此，维基百科中给出了另一个针对法律合约的智能合约定义："一种旨在以数字方式促进、验证、加强合约协商和履行的计算机协议（Smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract）"。这一定义体现了智能合约的对象是法律合约，计算机协议是保障合约协商和履行的手段，该手段的目的是促进、验证、加强合约协商和履行，而数字方式是手段的表现形式。

由此可知，智能合约是一个较为宽泛的概念，更加准确地定义是"存储在区块链上并可在满足预定条款和条件时自动执行的计算机代码（Smart contracts are lines of computer code that are stored on a blockchain and automatically execute when predetermined terms and conditions are met）"，因此也被称为区块链智能合约。从这一定义可以看出，智能合约的载体是区块链，它本质是一种自动执行的计算机代码。该代码描述了买卖双方之间的协议条款，并被直接写入区块链的代码行中，满足预定条款和条件是代码被执行的触发条件。由于代码的执行不需要人为干预，因此被称为自动执行。

需要说明的是，智能合约作为一种计算机程序，它是应用软件的一部分，是一种数字表示的程序，虽然是合约条款的代码表示，但不是法律意义上的合同或合约。此外，区块链智能合约由计算机网络执行，并且执行不需要可信方的参与运行，而由共识协议保证合约代码执行的正确性。因此，智能合约也可以理解为一种无需中介、自我验证、自动执行合约条款的计算机交易协议[2]。当然，目前智能合约系统功能与上述概念之间还存在巨大差异。

3 智能合约历史

智能合约概念最早可追溯到1994年由Nick Szabo撰写的论文《Smart Contracts: Building Blocks for Digital Markets》[3]。在该论文中，Nick Szabo期望将智能合约定义为执行合约条款的计算机化交易协议，创新性地提出"智能合约不涉及人工智能，它是一组由代码方式外在表示的要约和承诺，并能够涵盖双方依据的要约和承诺达成履行约定的自动行为"，并希望将诸如POS（销售点）之类的电子交易方法的功能扩展到智能合约领域。他在1998年发明了一种叫作"Bit Gold"的虚拟货币，比比特币发明早了10年。

此后，Nick并没有停止对智能合约的探索，例如，他的后续论文还提出了对合成资产（如衍生工具和债券）执行合同的建议[4]。Szabo写道："这些新证券是通过多种方式将证券（例如债券）和衍生品（期权和期货）组合在一起而形成的。非常复杂的付款期限结构现在可以构建为标准化合同，以较低的交易成本进行交易，并对这些付款期限结构进行了计算机分析"。

由于缺少可信的执行环境，Nick提出的智能

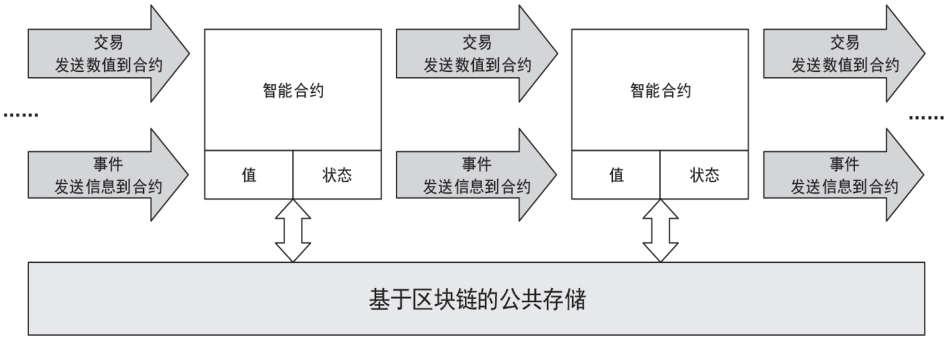

图1 区块链智能合约抽象模型

合约并没有被应用到实际产业中。到2008年比特币诞生后，人们才认识到比特币的底层技术（即区块链）可以为智能合约提供可信的执行环境[5]。以太坊首先意识到区块链和智能合约的契合，发布了白皮书《以太坊：下一代智能合约和去中心化应用平台》，并重新使用了智能合约这一概念，并建立了一整套智能合约的规范与架构，为智能合约这一概念带来了生机。

在以太坊实现并发布了面向智能合约的区块链系统后，智能合约被普遍认为是第二代区块链技术，其它区块链开发公司也都进行了智能合约的开发与创新。以太坊和超级账本是目前应用最广泛的两种智能合约开发平台，它们的智能合约运行机制也最具代表性。

4 智能合约架构

智能合约的构建来源于通常的区块链框架。区块链作为一种公共记账单系统，打开了点对点数字化价值转移模式的大门，实现了在不需要信任第三方的情况下异地间的安全价值转移，但也存在功能单一的问题[6]。智能合约则通过支持更加强大的编程语言和运行环境，允许开发者在其上面开发任意价值交换相关的应用，成功的解决了区块链应用单一的问题。

智能合约不仅仅是区块链上的一段可执行代码，而是构建在区块链上包含智能合约语言、运行环境、执行方法等的一个完整计算系统[7]。为了理解这一复杂系统，本节首先从抽象计算模型角度来加以介绍，进而给出智能合约的通用架构。

图1描绘了在程序状态机模型下的区块链智能合约抽象模型。从计算模型的观点来看，公共记账本能够作为一种状态转换系统[8]，它能够记录任何账户所持有货币的所有权状态以及预先定义好的“状态转换函数”。当该系统接收到一个（可以由交易或可信外部事件引发）含有状态改变的事物时，它将依据“状态转换函数”输出一个新的状态，并将该输出状态（以一种所有人都信任的方式）写入到公共记账本，这一过程可以往复进行。例如，在银行系统中状态是一个资产负债表，交易是一个将资产x从账户A移动到B的请求，状态转换函数将账户A中的资产值减少x，将账户B中的值增加x。如果账户A中的值事先小于x，则状态转换函数返回一个错误。

在上述智能合约抽象模型中，“状态转换函数”可理解为一段已预定义的智能合约代码，它以交易形式被分享和部署在区块链中，但该合约代码仅限于对所在交易中资产数值和运行状态进行改变。其次，智能合约系统能够接收外部发来的事件或来自其它账户发来的交易，通过“状态转换函数”预制的条件来激活合约代码的运行，从而控制自身的资产和对接收到的外界事件进行回应，而且这一过程是自动执行的，无需外界干预。

为了支持上述抽象计算模型的实现，图2表述了一种区块链智能合约的通用架构。该框架涉及到智能合约的程序设计、代码生成、部署与执行等多个阶段，该框架由三个主要部分构成。

（1）智能合约编程环境

为智能合约开发提供代码开发环境，包括支持生成智能合约的编程语言规范、开发和编译工具，能够帮助开发者撰写智能合约程序并编译成为可执行代码。例如，由高级智能合约语言提供更加专业化的智能合约编写和验证，由通用智能合约语言提供标准化语言下的跨平台代码生成。

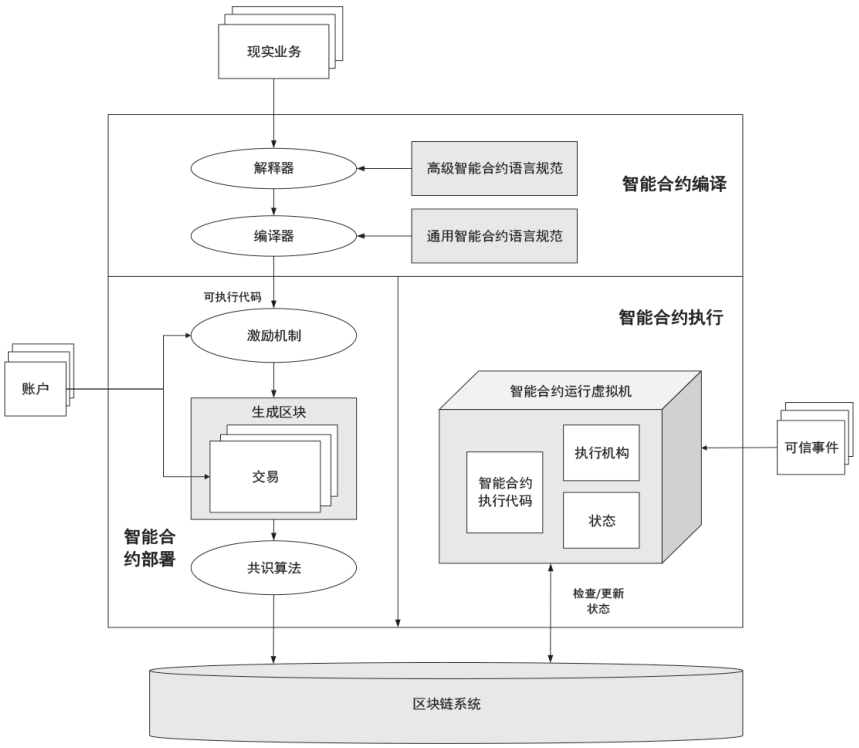

图2 区块链智能合约通用架构

（2）智能合约部署环境

提供智能合约可执行代码部署区块链中所需要的工具，包括将可执行代码与合约参与者账户及激励机制进行绑定、并以区块链可接受的方式（包括规范化格式、合约状态、共识机制等）将其部署到区块链中，同时也记录由合约代码运行所带来的合约属性值和合约状态的改变。

（3）智能合约运行环境

提供一种可信运行环境来运行智能合约代码，包括接收外部发来的可信事件或内部交易，建立可信智能合约运行虚拟机或沙箱，下载相关区块链交易中的合约代码，触发通过执行机构和指令系统执行合约代码对事件或交易进行响应，并将输出结果以交易方式写入区块链。

随着智能合约技术的发展，已经出现越来越多的工具辅助智能合约完成程序设计、代码生成、部署与执行等功能，也使得智能合约构架日趋完善。

5 智能合约运行机理

为了更好地理解智能合约的原理，下面将分别对智能合约语言与编译、智能合约的区块链部署、以及合约代码运行的机理分别加以介绍。

5.1 智能合约语言与编译机制

智能合约语言是现实应用中各种业务与智能合约平台之间的中介，也是帮助智能合约的使用者快速生成智能合约程序和代码的重要工具[9]。各智能合约平台都已推出自己的智能合约语言，例如，比特币使用较为底层的栈式脚本语言、以太坊的智能合约目前支持Serpent和Solidity两种编程语言（Serpent类似于Python语言，而Solidity类似于JavaScript语言）、超级账本支持如Go、Java等语言直接编写；此外，其它平台也以传统编程语言（如C、C++、Java）基础上给出了智能合约开发工具。从语言形式和运行环境上讲，目前的智能合约可分为三类。

（1）脚本型智能合约：通过区块链中定义好的脚本指令和栈式类Forth语言完成基本的计算与条件控制，例如，比特币脚本系统。

（2）通用型智能合约：其语言直接采用传统程序语言，部署在虚拟机（VM）或容器（Docker）里，通过规定好的接口与区块链进行交互。例如，超级账本平台中的链码采用Java、

Go等语言，Neo平台支持将C#、Java和Python等多种语言编译为NeoVM支持的指令集。

（3）专用型智能合约：模仿传统程序语言并添加了与区块链交互的特殊元素，如以太坊的Solidity语言，同时该语言含有gas计费等特殊功能。

智能合约是一个跨学科的概念，涉及商业、金融、合同法和信息技术，设计和开发智能合约也需要来自不同领域的专家的密切合作。然而，上述三种智能合约仍然建立在计算机编程语言基础上，对于非计算机专业人员依然难以理解和掌握。

针对这一问题，近年来一种被称为高级智能合约语言已引起学术界的广泛关注，例如，面向现实合约的智能合约描述语言（SPESC）[10]。这种语言以现实合约的语法结构为基础，采用近似自然语言的形式进行编写，明确定义了当事人的义务和权利，以及加密货币的交易规则，便于法律人士与计算机人员协作合约开发，对于促进智能合约的专业性、易用性、可理解性，以及协作开发等方面能力有重要意义。

5.2 智能合约的区块链部署

区块链是智能合约得以实施的基础，智能合约的自动化执行、运行结果的有效性，以及合约代码的安全都依赖于区块链[11]，因此智能合约与区块链的有效结合与部署成为智能合约实施的关键[12~13]。为了便于被理解和掌握，智能合约通常将区块链转化为几个抽象概念：共享数据库、交易和区块。下面将分别对其进行介绍。

首先，区块链对智能合约而言可被视为全球共享的交易数据库，其中，交易被用来描述每一次通过智能合约语言接口执行的行为。全球共享则意味着每个人都可以通过智能合约网络接口来读取交易数据库中存储的条目。

其次，交易可理解为更改共享数据库中某些内容的行为，而且保证该行为必须被数据库网络中其它参与方所接受。后者也被称为“all-or-nothing”原则，如果交易要同时更改两个值，要么根本没有完成，要么完成所有修改。此外，在将交易完成后，没有其它交易可以更改这一过程。

再次，交易从安全性来看始终需要由发起方（创建者）进行签名，这可保护访问共享数据库的特定修改必须经过授权。从已有的数字货币交易可知，签名机制可保证简单的检查即可确保只有持有该账户密钥的人才能从该账户中转移资金。

此外，智能合约所生成的交易将被捆绑到一个所谓的“区块”中，然后将它被分发到共享数据库的所有参与节点。如果两笔交易相互矛盾，那么最后一笔交易将被拒绝，并且不会成为交易的一部分，因此，区块被理解在时间上形成线性关系的存储单元，并为智能合约选择一个全球公认的交易顺序，以解决冲突。总之，区块链为智能合约提供了一种安全和一致性的共享交易数据库。

最后，对于智能合约的使用者和编程人员而言，当前智能合约平台已经能够屏蔽掉区块链中的很多技术细节，使得区块链中的各种复杂机制（哈希、对等网络、共识、挖矿等）变成了智能合约平台提供的承诺。因此，开发和使用人员只需要关注自己的业务需求，充分利用智能合约平台提供的部署工具，而不需要考虑如何将智能合约执行代码转化为区块链数据的具体实现。

5.3 合约代码运行

当满足触发条件时，被部署在区块链上的智能合约代码将被区块链系统自动执行，并依照合约规定完成各种资产的转移。这一过程需要货币激励、执行机构、指令系统和触发条件等机制相互协调，才能保证合约代码自动和无差错地被执行。

首先，奖励机制是合约代码执行的必备条件，原因在于智能合约代码是在区块链节点内（虚拟机、容器等）被执行的，必然带来存储、计算、带宽等方面的开销，因此需要智能合约发布者预付一定量的货币（如以太网gas）作为奖励。如果预付金额太小了，不足以执行所有的操作，那么操作就会失败，状态将会回滚。

其次，执行机构是指智能合约代码运行的环境，目前主要有脚本、容器、虚拟机等三种运行方式，具体特征为：

（1）脚本（Script）方式

最早在比特币系统中被采用，是一种类似Forth语言的指令体系，由脚本解释器解释执行，用于验证该笔交易的合法性。交易一般会包

括输入脚本和输出脚本两个部分，分别用于解锁上一笔交易的输出以及设置该笔交易金额的解锁条件。

（2）容器（Docker）方式

是不同于虚拟机的一种新型虚拟化技术，它只需要将智能合约所需要的依赖软件打包即可独立运行，而不需要一个附加的虚拟操作系统环境。它比虚拟机方式更为独立和灵活，可调用的资源也更多。Hyperledger Fabric是典型使用容器方式的智能合约平台。

（3）虚拟机（VM）方式

它通过在用户程序和底层环境中增加的一层中间环境，提供一个完全对底层透明的执行环境：屏蔽区块链节点自身执行环境的区别，在所有节点上运行均一致。它按照执行方式分为两种：基于栈（Stack）和基于寄存器（Register）的虚拟机，其中，基于栈的虚拟机是目前实现智能合约最多的方式，也演化出多种智能合约运行方法。

此外，指令系统在智能合约中也是较重要的概念。指令是智能合约发给运行环境的命令，智能合约的执行代码是由一系列的指令组成的，而指令系统是智能合约运行环境提供的语言系统，是全部指令的集合，反映了运行环境所拥有的基本功能。因此，智能合约指令系统是由所采用的运行方式决定的。

最后，智能合约代码中预置了合约条款的相应触发场景和响应规则，运行环境需要根据可信外部事件和内部交易状态，自动地判断当前所处场景是否满足合约触发条件，严格执行响应规则并向区块链发送更新合约状态的交易，经共识算法认证后链接到区块链中，使更新生效。

6 结束语

智能合约作为普遍认为的“第二代区块链技术”，任何人都可接入其中，不需要事先审查或者预付成本，又可以移除经济交易中对第三方机构的信任必要。本文对智能合约的研究进展进行了归纳总结，介绍了智能合约的发展历史以及基本概念、并详细阐述了智能合约语言现有的分类和不同的编译机制、智能合约在区块链上的部署方式以及运行机制。

目前几乎所有的区块链技术公司都已在其产品中支持智能合约产品，例如，以太坊基于虚拟机的智能合约平台、基于Bitcoin区块链的RSK平台、IBM公司提出的企业级HyperLeger Fabric平台等。这些产品的推出极大的丰富了智能合约技术的内涵和范围，为区块链技术在不同领域的现实应用奠定了基础，也代表了区块链未来发展的方向。但同时智能合约跨领域合作、标准统一、法律化结合等多个研究方向都尚不完善，这些问题的存在囿限着智能合约的市场普及和应用广度，是现在智能合约研究极具挑战性的方向。

基金项目：

1.国家科技部重点研发计划（项目编号：2018YFB1402702）；

2.国家自然科学基金（项目编号：61972032）。

参考文献

[1] Bartoletti M, Pompianu L. An empirical analysis of smart contracts: platforms, applications, and design patterns[C]// International conference on financial cryptography and data security. Springer, Cham, 2017: 494-509.

[2] Szabo, Nick. "Smart contracts: Building blocks for digital markets[N]. 1996." (2001).

[3] Szabo N. Smart contracts in essays on smart contracts, commercial controls and security (1994) [EB/OL].http://www. fon. hum. uva. nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best. vwh. net/smart. contracts. html.

[4] Beaumont P H. Fixed-income Synthetic Assets: Packaging, Pricing, and Trading Strategies for Financial Professionals[M]. John Wiley & Sons, 1992.

[5] 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.

[6] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the internet of things[J]. Ieee Access, 2016, 4: 2292-2303.

（下转第54页）

论, 2019.
[5] 谢勇. 电子交易中的合同法规则[M]. 北京：人民法院出版社, 2015.
[6] 陈吉栋. 智能合约的法律构造[J]. 东方法学, 2019, 69(03):20-31.
[7] 吴烨.论智能合约的私法构造[J].法学家, 2020(2):1-13.
[8] 柴振国.区块链下智能合约的合同法思考[J].广东社会科学,2019(4):236-246.
[9] 郭少飞.区块链智能合约的合同法分析[J].东方法学, 2019(3):4-17.
[10] 倪蕴帷. 区块链技术下智能合约的民法分析、应用与启示[J].重庆大学学报（社会科学版）, 2019(3):170-181.
[11] 蔡一博.智能合约与私法体系契合问题研究[J].东方法学, 2019(2):68-81.
[12] 魏昂, 黄忠义, 周鸣爱. 智能合约安全与实施规范研究[J]. 网络空间安全, 2020, 11(3): 9-.
[13] 王延川.智能合约的构造与风险防治[J].法学杂志, 2019(2):43-51.

作者简介：

张韬（1980-），男，汉族，黑龙江伊春人，中国政法大学，硕士，北京华讯律师事务所，主任律师。主要研究方向和关注领域：电子商务法、科技法、网络法、知识产权法。

（上接第24页）

[7] 朱岩, 甘国华, 邓迪, 等. 区块链关键技术中的安全性研究[J]. 信息安全研究, 2016, 2(12): 1090-1097.
[8] Frantz C K, Nowostawski M. From institutions to code: Towards automated generation of smart contracts[C]//2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W). IEEE, 2016: 210-215.
[9] 何小东, 易积政, 陈爱斌. 区块链技术的应用进展与发展趋势[J]. 世界科技研究与发展, 2018, 40(6): 615-626.
[10] He X, Qin B, Zhu Y, et al. Spesc: A specification language for smart contracts[C]//2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). IEEE, 2018, 1: 132-137.
[11] Sklaroff J M. Smart contracts and the cost of inflexibility[J]. U. Pa. L. Rev., 2017, 166: 263.
[12] Watanabe H, Fujimura S, Nakadaira A, et al. Blockchain contract: Securing a blockchain applied to smart contracts[C]//2016 IEEE international conference on consumer electronics (ICCE). IEEE, 2016: 467-468.
[13] 王继辉.区块链与智能合约图谱分析[J].网络空间安全, 2019,10(11):1-6+25.

作者简介：

朱岩(1974-)，男，汉族，黑龙江大庆人，哈尔滨工程大学，博士，北京科技大学，教授；主要研究方向和关注领域：信息安全、密码学。

王静（1995-），女，汉族，山西阳泉人，北京科技大学，在读硕士；主要研究方向和关注领域：区块链、智能合约。

郭倩（1997-），女，汉族，山西临汾人，北京科技大学，在读硕士；主要研究方向和关注领域：区块链、智能合约。

刘国伟（1980-），男，汉族，山东肥城人，北京市经济和信息化局，大数据标注与安全处处长，高级工程师；主要研究方向和关注领域：大数据安全、网络安全、大数据标准。