第 13 卷 第 5 期
2024 年 9 月
集 成 技 术
JOURNAL OF INTEGRATION TECHNOLOGY
Vol. 13 No. 5
Sep. 2024

引文格式：
郭海凤, 杜心童, 张羽兮. 区块链智能合约应用与安全问题研究 [J]. 集成技术, 2024, 13(5): 93-102.
Guo HF, Du XT, Zhang YX. Research on blockchain smart contract application and security issues [J]. Journal of Integration Technology, 2024, 13(5): 93-102.

区块链智能合约应用与安全问题研究

郭海凤[1] 杜心童[2*] 张羽兮[2]

[1]（西南财经大学金融学院 成都 611130）
[2]（哈尔滨工业大学经济与管理学院 哈尔滨 150001）

摘 要 独有的金融特性使得广泛嵌套于各种区块链平台上的智能合约成为区块链技术最成功的应用之一。由于承载着大量的资产及虚拟货币，具有极高的经济价值，因此，智能合约不断受到各种安全攻击。此外，匿名与自动执行等特点使得智能合约被用于多种违法交易与恶意应用。基于此，作者首先介绍智能合约在区块链相关技术方面的运行机制和原理，探讨智能合约技术的应用场景及发展中存在的潜在安全漏洞，以及可能引发的安全问题，然后根据对现有研究工作的总结，探讨智能合约漏洞检测领域面临的挑战，并结合深度学习技术展望智能合约的未来研究方向。

关键词 区块链；智能合约；比特币；以太坊；超级账本；有害信息
中图分类号 TP309.2 **文献标志码** A doi: 10.12146/j.issn.2095-3135.20240128001

Research on Blockchain Smart Contract Application and Security Issues

GUO Haifeng[1] DU Xintong[2*] ZHANG Yuxi[2]

[1](*School of Finance*, *Southwestern University of Finance and Economics*, *Chengdu* 611130, *China*)
[2](*School of Management*, *Harbin Institute of Technology*, *Harbin* 150001, *China*)
[*]*Corresponding Author*: 19b910032@*stu.hit.edu.cn*

Abstract The unique financial characteristics make smart contract, which are widely nested in various blockchain platforms, one of the most successful applications of blockchain technology. Due to the high economic value of carrying large amounts of assets and virtual currencies, smart contracts are constantly subject to various security attacks. In addition, features such as anonymity and automatic execution make smart contracts used in a variety of illegal transactions and malicious applications. Based on this, the paper firstly introduces the operation mechanism and principle of smart contracts in blockchain-related technologies,

收稿日期：2024-01-28 **修回日期**：2024-08-01
基金项目：四川省重点研发计划项目（2024YFHZ0161）
作者简介：郭海凤，教授，研究方向为区块链、金融科技等；杜心童（通讯作者），博士研究生，研究方向为企业战略、金融科技等，E-mail：19b910032@stu.hit.edu.cn；张羽兮，博士研究生，研究方向为区块链、金融科技等。

discusses the application scenarios of smart contract technology and the potential security vulnerabilities and security problems that may be triggered by the development of smart contract technology, and then, based on the summary of the existing research work, discusses the challenges faced by the field of smart contract vulnerability detection, and looks forward to the future research direction of smart contracts in combination with deep learning technology.

Keywords blockchain; smart contract; Bitcoin; Ethereum; Hyperledger; hazardous information
Funding This work is supported by Key Research and Development Program of Sichuan Province (2024YFHZ0161)

1 引 言

区块链技术的大规模普及不仅极大地改变了传统的交易模式[1]，还催生了一批依托区块链技术的各种应用，其中，智能合约(smart contract)无疑是最成功的应用之一。作为一种运行在区块链上的分布式应用[2-3]，智能合约本质上是部署在区块链上的一些可执行代码，可不依赖中心机构自动代表各签署方执行合约[4]。因此，智能合约可灵活嵌入各种数据和资产，帮助实现安全高效的信息交换、价值转移和资产管理。

目前，许多区块链平台(如以太坊(Ethereum)❶、EOS❷、维特链(VNT chain)❸等)均支持运行智能合约。据统计，目前，各类区块链平台上均已部署了数以万计的智能合约，且仍在持续增长中。在众多平台中，以太坊是规模最大，并最具影响力的区块链平台[5]，该平台广受好评主要是因为它的图灵完备，并且可以允许开发人员编写任意智能合约和去中心化应用(decentralized application，DAPP)。DAPP 是一些可以在区块链上运行，由一个或多个智能合约组成，包括前端、后台等构件的应用程序[6]。如果承载一个 DAPP 运行的区块链是无许可型区块链，则这个 DAPP 就可以在无须中心化媒介控制和干预的情况下自动运行。目前，一些信息通信技术公司和国家政府已开始关注区块链与智能合约的发展、应用及监管情况[7]，大部分国家政府对推动区块链技术的发展持积极态度。

然而，在智能合约为人们工作和生活带来便利的同时，它所引发的安全问题也同样不容小觑。由于智能合约是一段由用户自主编写的程序代码，因此，其在设计和开发过程中可能出现代码安全问题[8-9]。此外，嵌套在区块链上的智能合约通常暴露在开放网络环境中，进一步增加了智能合约使用过程中的安全隐患[10]。同时，区块链及智能合约的去中心化和匿名特性助长了恶意合约的产生，违法者可通过发布恶意的智能合约对区块链系统和用户发起攻击，也可利用合约实现匿名的犯罪交易，导致机密信息泄露、密钥窃取或各种真实世界的犯罪行为。

2 智能合约概述

早在 1996 年，智能合约的概念就已被 Szabo[11]提出，他将智能合约定义为执行合约条款的可计算交易协议，并设想“智能合约可通

注❶：Etherscan. 2014. https://etherscan.io/
注❷：EOS Official Portal. 2019. https://eos.io/
注❸：VNT chain. 2018. https://scan.vntchain.io/

过使用协议和用户接口促进合约的执行”。与此同时，他还给出智能合约应具有的性质：可见性、强制执行性、可验证性和隐私性。1997年，Szabo[12]进一步将智能合约定义为一套数字形式的承诺，含有合约参与方可在上面执行这些承诺的协议。这些承诺定义了合约的本质和目的，包括用于执行业务逻辑的合约条款和基于规则的操作，而协议则是参与方必须遵守的一系列规则。因此，智能合约是具备状态的、由事件驱动的、部署于可共享的分布式数据库上的计算机程序。现存智能合约的工作原理类似于其他计算机程序的 if-then 语句[13]，当一个预先设定的条件被触发时，智能合约便可相应执行合同条款。智能合约正是以这种方式与真实世界的资产进行交互。

从本质上讲，智能合约是由计算机代码构成的一段程序，它的数字形式表明这类合约由代码组成，他们的输出可以被预测并自动执行。作为一种嵌入式程序化合约，计算机专家将各方事先协商确定的权利义务事项通过计算机的程序语言转换为代码，并设计算法，计入区块链中，只要条件成熟，便自动执行，无须第三方督促，也不会发生合同双方拒不履行现象，实现了从权利义务设定、签署到执行的一体化，从而使智能合约具有数据透明、不可篡改、永久运行等特性[14]。

由此可见，智能合约在设计之初的构想是以数字形式定义一个合同，当参与方达成合同所需的条件时，计算机便可自动执行该合同。然而，受限于技术水平，这一构想直到近年来区块链技术逐渐成熟，以及加密货币的快速发展才得以实现[15]。区块链的去中心化、所存储数据的防篡改特性使得智能合约适合依附在区块链上运行。因此，近年来，区块链技术的发展，尤其是以太坊平台的出现，为智能合约的发展提供了更广阔的前景。由于区块链的种类和运行模式存在差异，所以在不同平台上，智能合约的运行机制也有所不同。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最具代表性。

以太坊和超级账本的智能合约缔结过程如下：

第一步，参与缔约的双方或多方用户商定后将共同协议制定成一份智能合约；

第二步，该智能合约通过区块链网络向全球各个区块链的支点广播，并存储；

第三步，构建成功的智能合约等待条件达成后自动执行合约内容。

普通、标准的合同涵盖当事人之间协议的条款，常通过法律强制执行；而智能合约是数字化的，存储在区块链中，通过加密代码强制执行，即智能合约是根据以太坊中的计算机编程语言来编写和运行的软件程序，与所有程序一样，只要一段代码中所编写的要求被满足，合约中的义务和条款将完全按照程序员的意图自动执行。

3　智能合约的应用及潜在危险

3.1　智能合约的应用

智能合约不同于传统意义上的手写合同，也不是民法意义上的合同，而是一种智能软件，只要各方具备先前设置的各种条件，并满足预定条件，即可控制或记录，甚至产生特定的法律相关活动，并依赖软件技术自动完成交易[16]。作为一种可自动运行的计算机协议，智能合约一旦部署，就能实现自我执行和自我验证，因此在物联网和分布式计算等领域的应用上都具备广阔前景[17]。

目前，智能合约已被广泛应用于去中心化金融(decentralized finance，DeFi)服务。DeFi 是一种基于区块链的金融基础设施，通常指建立在公共智能合约平台上的开放、无须许可且具有较高的可互操作性的协议栈，是目前以太坊上最热门的智能合约应用类型。为提升可互操作的性能，

如在区块链上转移虚拟货币或资产，许多从以太坊开始的较新协议提供嵌入脚本代码片段的机会，在理论上可以进行任何计算。由于智能合约能依托计算机在网络空间运行，以信息化方式传播，由计算机读取、验证、执行，具备用户自助操作的特点[8]，因此智能合约可以以更开放、透明的方式复制现有的金融服务[18]，不依赖中介机构和中心化机构，而是基于开放协议和去中心化应用程序。基于此，智能合约已成为新 DeFi 架构的另一个基本层。

在此基础上，区块链系统提供一种去中心化的方法，利用网络上的多个节点来集体验证并记录数据，这种分布式存储和验证数据的共识机制可确保数字记录的完整性，并可为传统的集中式数据库提供令人信服的替代方案。基于区块链的身份系统的核心在于利用加密技术，如哈希函数、数字签名和零知识证明等，安全地共享和验证敏感信息。具体来说，哈希算法可将文档转换为唯一的数字指纹，防止智能合约中存储的信息被轻易篡改。政府机构或受信任的实体可通过数字签名进一步提高文档的有效性。零知识证明可在不泄露敏感细节的情况下进行身份验证，从而提供了一种在不损害隐私的情况下证明身份属性的方法。

此外，智能合约的应用还可赋予用户定义自我主权身份的权利，包括个人数字信誉和数字资产等。这些数据可存储在个人钱包中(类似于加密钱包)，并可指定哪些数据可以或不可以与他人共享。在这种情况下，人们可以决定何时及如何共享他们的信息。例如，智能合约的用户可将他们的信用卡凭据存储在个人钱包中，然后利用他们的私钥签署发送该信息的交易。这能证明他们是该信用卡的真正所有者。

总的来说，区块链技术虽然主要用于存储和交换加密货币，但也可用于共享和验证个人文档和签名。

3.2 智能合约的潜在危险

3.2.1 自动识别与执行

智能合约的义务通常以“if-then”的形式写入代码，例如，“如果 A 完成任务一，那么，来自 B 的付款会转给 A”。通过这样的协议，智能合约允许各种资产交易等合同义务的履行，每个合约被复制和存储在分布式账本中。这样，所有信息都不能被篡改或破坏，数据加密确保参与者之间的完全匿名。智能合约具有自动识别与执行功能，自动识别的对象是用于启动智能合约的条件信息，自动执行的对象是与智能合约相关联的履约标的物，如数字货币。当智能合约设置成功时，合约交易方就会自动履行自身义务。当合同义务履行完毕后，智能合约就会通过自行解释数据验证合约中的条件、判断义务完成与否，并根据已完成的前置条件执行应执行给付的财产义务。智能合约的自动识别与执行功能极大地减少了犯罪分子之间的实质性接触。

3.2.2 匿名性

犯罪分子希望通过隐匿踪迹逃脱处罚，因此，智能合约的匿名性功能受到犯罪分子的青睐。智能合约的交易方虽然是自然人，但在以太坊等区块链平台上通常是数字货币账户。数字货币账户所代表的自然人之间的联系是由私钥沟通的。然而，私钥具有不记名性，不仅使侵害私钥的行为具有严重危害性，还隐匿了账户所有者的主体身份。因此，智能合约的匿名性功能导致犯罪更加便利，使罪犯更容易逃脱处罚。

3.2.3 去中心化跨区域犯罪

智能合约所处的区块链网络世界能跨越区域限制，实现远距离的即时沟通与交流。与传统中心化网络不同，区块链具有去中心性。在去中心化系统下，个人与个人之间的交互摆脱了中心节点的控制。但目前主流平台中基于智能合约的互联网投融资与交易模式并未实现完全去中心化，投资者对网络信贷的信任主要是对平台的信任[19]。

这种不完全的去中心化反而更容易结合线下的宣传，吸引人们使用某种合约进行相关的投融资交易。同时，结合跨区域性，智能合约必然为犯罪提供极大便利，依靠一个国家的刑事力量将难以摧毁全球化的犯罪团伙。

4　智能合约的安全问题

由于智能合约存在不可篡改特性，因此，在部署它们之前确保其设计良好和没有错误至关重要。此外，智能合约的不可篡改特性可让区块链平台上的用户很容易建立起信任，然而这也使得不法分子以恶意合约为工具谋利，引发各种安全隐患。目前，智能合约所引发的安全问题主要指其存在的安全漏洞所导致的用户加密资产被盗或损失。此外，智能合约还可能会存在一定的合约缺陷(contract defect)，通常是智能合约编写过程中的错误、缺陷或故障，导致它产生不正确或意外的结果，或以非预期的方式行事。为更好地了解智能合约存在的缺陷和潜在安全问题，Chen等[20]收集了与智能合约相关的帖子，并进行分析，最终定义了 20 种合约缺陷。本文将智能合约的安全问题分为两类：合约本身存在的安全漏洞与具有不良目的的恶意合约。

4.1　安全漏洞

目前，智能合约上的安全漏洞导致的经济损失已超过数十亿美元[21]。2022 年，加密货币全行业公开报道的安全事故至少有 189 起，造成至少 76 亿美元的加密资产损失[22]。其中，在 181 起 DAPP 类的安全事故中，80% 的 DAPP 安全事故缘于智能合约漏洞。基于此，若智能合约本身存在漏洞，则不法分子可利用这些漏洞为自己牟利。更严重的是，很多犯罪分子以智能合约为载体，实现集资、诈骗等违法行为。由于区块链上的所有用户都可看到智能合约的具体内容，所以包括安全漏洞在内的所有合约漏洞对所有用户可见，且无法迅速修复。

以太坊中的智能合约存在的安全问题包括合约编程语言 Solidity 自身设计的缺陷[23]、编译器错误、以太坊虚拟机错误、对区块链网络的攻击、程序错误的不变性、开发者在开发过程中引入的错误，以及其他尚无文档记录的攻击[24]。

著名的 The DAO 攻击是因为代码中的一个错误允许攻击者反复抽走资金，导致 360 万个以太币被从 The DAO 资产池中分离出来(2019 年 2 月，1 以太币≈150 美元)，投资者失去了价值约 5 000 万美元的加密货币[25-26]。

如图 1 所示，类似的智能合约安全漏洞还有整数溢出问题。在计算机编程中，当算术运算试图编写一个超出可用位数表示范围的数值时，就会发生整数溢出错误。例如，2018 年 4 月，一款名为 BEC 的代币遭受溢出攻击，攻击者在短时间内利用乘法溢出向外部账户转入海量合约代币，并进行抛售，导致该代币的价格迅速缩水归零。在攻击手法被披露的 24 h 内，还有多达 30 个合约遭受类似攻击。这一漏洞的发生原因是：在 Solidity 语言中，int 类型的数据变量被规定了长度，如 uint8 代表的是无符号的 8 位整数，即 0～255。因此，若传入的参数是一个 uint8 类型的变量，则它的范围在 0～255；若输入值是 255，则返回值是 0；若输入值是 256，则返回值是 1。上述现象的原因主要与数据在计算机中的存储有关，计算机只给 uint8 类型的变量分配了长度为 8 的空间，最大值为 255，若超过 255，则会出现进位之后被截断，导致存储的 8 位全是 0 的现象，并因此造成整数溢出。

在 BEC 智能合约中，图 2 中的代码是为了实现批量转账。其中，receivers 为接受者的数组；value 为转账金额。如图 2 所示，定义一个 uint256 类型的变量 amount 来接收转账的总金额，并通过比较总金额和用户所发送的金额判断用户是否能够发送这么多代币。如

```
01. 1. // SPDX-License-Identifier: GPL-3.0-or-later
02. 2. pragma solidity ^0.7.0;
03. 3.
04. 4. contract Overflow{
05. 5.
06. 6.     mapping(address => uint256) public balances;
07. 7.     //Record the caller's deposit amount
08. 8.     function deposit() public payable{
09. 9.         balances[msg.sender] += msg.value;
10. 10.     }
11. 11.     //Withdraw the caller's deposit amount
12. 12.     function withdraw(uint256 amount) public{
13. 13.         require(balances[msg.sender] - amount >= 0);
14. 14.                     //Unsafe addition, subtraction, multiplication,
15. 15.         msg.sender.transfer(amount);
16. 16.         balances[msg.sender] -= amount;
17. 17.     }
18. 18.     //View contract account balance
19. 19.     function accountBalance() public view returns (uint256){
20. 20.         return address(this).balance;
21. 21.     }
22. 22. }
```

图 1 整数溢出问题导致的智能合约安全漏洞

Fig. 1 Smart contract security vulnerabilities due to integer overflow issues

```
function batchTransfer(address[] _receivers, uint256 _value) public whenNotPaused returns (bool) {
  uint cnt = _receivers.length;
  uint256 amount = uint256(cnt) * _value;
 require(cnt > 0 && cnt <= 20);
 require(_value > 0 && balances[msg.sender] >= amount);

 balances[msg.sender] = balances[msg.sender].sub(amount);
 for (uint i = 0; i < cnt; i++) {
     balances[_receivers[i]] = balances[_receivers[i]].add(_value);
     Transfer(msg.sender, _receivers[i], _value);
 }
 return true;
}
```

图 2 代码编写不当导致的智能合约安全漏洞

Fig. 2 Smart contract security vulnerabilities caused by poorly written code

果 uint256(cnt)*_value 的值超过 uint256，则产生溢出。智能合约的攻击者正是通过传递两个账户 _value 为 2^{255}，人为加长了 uint8 类型变量的长度，从而利用计算机的存储问题达成 $2\times2^{255}=2^{256}$ 的效果，最终完成了溢出，在此条件下，amount 的值为 0。这就允许 amount 能够通过后面的所有校验，最后发送给两个账户 2^{255} 个代币。

图 1 所示的智能合约主要实现了用户与合约间的交易转账功能，类似于银行的存取款功能，函数 deposit()用于调用者向合约账户存入以太币；函数 withdraw()用于调用者提取自己在合约账户中的以太币；函数 accountBalance()用于查看合约账户余额。由于红框中的代码编写不当，因此，当智能合约遭遇攻击导致减法溢出时，会失去对用户的限制，当合约账户余额不为 0 时，攻击者可无限次调用 withdraw()函数，窃取合约账户中的代币资产。

4.2 恶意合约

由于智能合约部署在区块链上，如以太坊或其他分布式账本等基础设施，侦听来自预言机(oracle)的加密安全数据源的事件和更新。因

此，智能合约通常控制大量高价值数据的流动，如转移资金、提供服务和解锁受保护的内容等。这使智能合约成为极具吸引力的攻击目标。

在设计和开发智能合约时，安全必须是重中之重。一旦智能合约部署到区块链上，就很难甚至无法修补，如发现漏洞，就必须删除、重新创建和重新部署。此外，一旦智能合约上链，则任何人都可以访问智能合约中的漏洞。在编写智能合约时，开发团队需特别注意一些可能存在的漏洞。常见的恶意合约问题是重入攻击，即每一行代码都必须在下一行代码开始之前执行。这就意味着，当合约对另一个合约进行外部调用时，调用合约的执行将暂停，直到调用返回。这使被调用的合约能暂时控制接下来发生的事情，从而创造了无限循环的可能性。重入攻击的本质是合约内部调用的函数未能恰当地处理合约状态的更改。攻击者利用这个漏洞，将攻击代码插入到合约执行流程中，使得攻击者可以在合约还未完成之前再次调用某个函数，从而让攻击者在合约中获得额外的资产或信息。例如，恶意合约可以递归回原始合约以提取资源，而无须等待第一次调用完成。重入攻击有多种形式，包括单功能、跨功能、交叉收缩和只读重入攻击。

Juels 等[27]分析了一种名为 Pwdtheft 的恶意智能合约，其可被用于盗取用户密码，并保证立契者和违法者之间的公平交易。另有学者指出，类似“丝绸之路”的匿名国际线上市场同样存在恶意合约问题。该非法物品交易网站允许用户自由交易违禁药品、毒品和枪支等，许多不法分子通常利用嵌套在该网站上的智能合约作为一个隐藏服务，并使用比特币作为支付媒介。智能合约的应用将使这些地下市场交易更加便捷，最终对社会造成危害[28]。

4.3　基于智能合约的违法犯罪行为

区块链智能合约存在去中心化、匿名性、自动执行等特性[29]，一些犯罪分子利用智能合约的真实身份与实际交易的弱关联性，以虚拟货币为中介实施违法犯罪活动。由于虚拟货币可匿名、现金交易，通常导致难以进行身份溯源，因此可能会助长黑色市场交易、逃税、洗钱及恐怖组织资助[30]。

目前，许多人利用智能合约买卖毒品、枪支等违禁品。在对 2022 年虚拟货币的相关文书进行分析后发现，2022 年，诈骗类虚拟货币案件高发，主要涉及诈骗、网赌、传销、洗钱、盗币、黄播、信息贩卖、涉密等犯罪类型。其中，诈骗案的数量占比最大，约占 29%，其次是网赌、传销和洗钱。诈骗类案件依然是 2022 年国内涉虚拟货币犯罪案件的重灾区。其中虚拟货币投资骗局尤为突出。

智能合约也可能被用于赌博、色情等违反公序良俗以致犯罪的交易。根据中国裁判文书网数据，2022 年，在与虚拟货币相关的文书中，刑事案共 161 件，其中帮助信息网络犯罪活动罪、掩饰隐瞒犯罪所得以及犯罪所得收益罪、诈骗罪、开设赌场罪占比最多。与 2021 年相比，2022 年的帮助信息网络犯罪活动罪依然是占比最大的；掩饰隐瞒犯罪所得以及犯罪所得收益罪案件的占比由 22% 上升至 30%；诈骗案件的占比由 22% 下降至 17%。

目前，众多区块链平台普遍缺乏一个中心化的机构来承担监管责任，交易双方甚至可以在不了解对方真实身份的情况下完成交易，如果交易中包含违法活动或者交易信息内含有有害信息，通过区块链平台的智能合约，犯罪分子甚至难以受到法律追究。对于区块链平台上的普通用户而言，能够获取的智能合约信息较少且真假难辨，因此难以在使用前对智能合约的安全性有所预知。此外，各类违法犯罪所得资金利用传统洗钱模式的“洗白”难度加大。为逃避打击，不法分子转移非法所得资金的方式逐渐转向更为隐蔽的虚拟货币。不法分子利用虚拟货币进行洗钱的

操作和手段不断更新，例如：将虚拟货币洗钱与各类犯罪活动交织渗透，区块链新技术、新应用(如智能合约)被快速广泛应用于洗钱，包括通过DeFi、混币平台和泰达币(USTD)跑分等方法洗钱。据行业相关报告数据，我国参与网络赌博的用户超过千万，每年境内流出涉赌资金超一万亿元。由于跨境网络赌博的门槛低、玩法多，支持多种支付方式，因此，大量人员被吸引参赌，单起案件的涉案赌资动辄上亿元，甚至数十亿元。

首先，智能合约在区块链上的执行方式从根本上改变了传统合约的执行过程[31]，一旦开始被执行，智能合约的分布式性质就使得其不可能单方面停止或逆转执行过程，除非某些能约束或终止合约的条件被事先写入程序。其次，智能合约的代码存在不确定性和不一致性的可能，这会导致合约本身存在漏洞，且合约的执行过程存在复杂的时间依赖和次序依赖关系，进而导致合约执行结果的不确定性[32]。最后，由于区块链存在匿名性，因此，即使在交易纠纷发生后，交易方试图起诉另一交易方，最终也会导致法律责任的不确定性[33]。

5 结论与展望

随着区块链技术的普及和应用不断深入，新兴的智能合约技术引起了学术界和产业界的广泛关注。智能合约去中心化、去信任、自治自足、不可篡改等特性允许合约各方在无须任何信任基础或第三方可信权威的情况下完成交易。同时，其可嵌入的数字形式正在深入变革金融、管理、医疗、物联网等诸多传统领域，有望促成各类可编程的智能资产、系统和社会。在大量商业应用不断涌现的同时，与智能合约有关的学术研究，特别是基础理论研究，却仍处于早期阶段，智能合约的相关研究领域内尚缺乏方向性研究框架和共同的话语体系。为此，本文对智能合约技术的运行机制、主流平台、关键技术、应用领域与风险挑战进行了全面的梳理，归纳了智能合约的缺陷问题与安全漏洞问题，并以此为序提出了智能合约的监管要求，讨论了智能合约的发展趋势，充分体现了智能合约的核心研究方向。

在大数据时代，央行应通过大数据监测区块链业务，增强风险监测能力，防范技术风险与金融风险。与此同时，央行与商业机构、市场主体也要强化信息共享、资源共用，增加监管者与被监管者之间的联系，充分利用金融科技企业的技术优势，开展战略合作，共同研发智能合约监管沙盒测试工具，加强对智能合约技术试点的监测，避免瑕疵代码与漏洞。此外，设定智能合约发生代码故障的应对机制，减少技术风险的发生。同时，数币智能合约也会受金融市场风险的影响，易引发系统性风险。因此，央行要考虑金融服务与其他模块的兼容性，创设符合风险特征的共识协议，构建全面化的防控网络，以应对网络攻击等突发事件。

虽然存在上述挑战，但区块链在彻底改变数字身份管理和数字货币方面的潜力是不可否认的。随着世界变得越来越数字化，人们对数字身份解决方案的日益关注，对安全高效的身份管理系统的需求从未像现在这样迫切。未来，区块链技术在身份管理和验证领域上的前景无疑会帮助我国塑造安全和可信的数字交互渠道。

本文对智能合约存在的漏洞和安全问题进行综述，对智能合约开发者存在一定价值，并为未来智能合约研究提供有益的启发与参考。目前，智能合约尚处于试点阶段，还未达到推广应用的程度。为发挥智能合约的积极作用，重塑相关领域的应用与信用机制，需要处理好智能合约与信用交互之间的关系，协调科技创新、隐私保护与金融监管之间的关系，密切关注智能合约技术的瓶颈，防范各类安全风险，实现监管科技与金融科技积极互动。

参 考 文 献

[1] Wang R, Lin ZX, Luo H. Blockchain, bank credit and SME financing [J]. Quality & Quantity: International Journal of Methodology, 2019, 53(3): 1127-1140.

[2] Buterin V. A next-generation smart contract and decentralized application platform [EB/OL]. [2024-08-01]. https://github.com/ethereum/wiki/wiki/White-Paper.

[3] 欧阳丽炜, 王帅, 袁勇, 等. 智能合约: 架构及进展 [J]. 自动化学报, 2019, 45(3): 445-457.
Ouyang LW, Wang S, Yuan Y, et al. Smart contracts: architecture and research progresses [J]. Acta Automatica Sinica, 2019, 45(3): 445-457.

[4] 马春光, 安婧, 毕伟, 等. 区块链中的智能合约 [J]. 信息网络安全, 2018, (11): 8-17.
Ma CG, An J, Bi W, et al. Smart contract in blockchain [J]. Netinfo Security, 2018, (11): 8-17.

[5] Fu ML, Wu LF, Hong Z, et al. Research on vulnerability mining technique for smart contracts [J]. Journal of Computer Applications, 2019, 39(7): 1959-1966.

[6] Jyothi C, Supriya M. Decentralized application (DApp) for microfinance using a blockchain network [C] // Proceedings of the Lecture Notes in Networks and Systems, 2022: 95-107.

[7] UK Government Chief Scientific Adviser. “Distributed ledger technology”: beyond block chain [EB/OL]. (2016-01-19)[2024-08-01]. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

[8] Unsworth R. Smart contract this! An assessment of the contractual landscape and the herculean challenges it currently presents for “self-executing” contracts [M] // Legal tech, smart contracts and blockchain. Perspectives in law, business and innovation. Singapore: Springer, 2019.

[9] Brent L, Grech N, Lagouvardos S, et al. Ethainter: a smart contract security analyzer for composite vulnerabilities [C] // Proceedings of the 41st ACM SIGPLAN Conference on Programming Language Design and Implementation, 2020: 454-469.

[10] Wohrer M, Zdun U. Smart contracts: security patterns in the ethereum ecosystem and solidity [C] // Proceedings of the 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), 2018: 2-8.

[11] Szabo N. Smart contracts: building blocks for digital markets [EB/OL]. [2024-08-01]. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

[12] Szabo N. Formalizing and securing relationships on public networks [J/OL]. First Monday, 1997, 2(9) [2024-08-01]. https://firstmonday.org/ojs/index.php/fm/article/view/548/469.

[13] 何蒲, 于戈, 张岩峰, 等. 区块链技术与应用前瞻综述 [J]. 计算机科学, 2017, 44(4): 1-7+15.
He P, Yu G, Zhang YF, et al. Survey on blockchain technology and its application prospect [J]. Computer Science, 2017, 44(4): 1-7+15.

[14] 工业和信息化部信息中心. 2018 年中国区块链产业白皮书 [EB/OL]. [2024-08-01]. https://www.miitxxzx.org.cn/n955454/n955459/c977029/part/977032.pdf.
Information Center, Ministry of Industry and Information Technology. 2018 China Blockchain Industry White Paper [EB/OL]. [2024-08-01]. https://www.miitxxzx.org.cn/n955454/n955459/c977029/part/977032.pdf.

[15] 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.
Yuan Y, Wang FY. Blockchain: the state of the art and future trends [J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[16] Giancaspro M. Is a ‘smart contract’ really a smart idea? Insights from a legal perspective [J]. Computer Law & Security Review, 2017, 33(6): 825-835.

[17] 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.
He HW, Yan A, Chen ZH. Survey of smart contract

technology and application based on blockchain [J]. Journal of Computer Research and Development, 2018, 55(11): 2452-2466.

[18] 乔海曙, 谢姗珊. 区块链金融理论研究的最新进展 [J]. 金融理论与实践, 2017, (3): 75-79.
Qiao HS, Xie SS. The latest extension on block chain finance theory research [J]. Financial Theory and Practice, 2017, (3): 75-79.

[19] 郑迎飞, 陈晓静, 辛苑. 中国 P2P 网贷利率决定: 基于跨平台横截面数据的实证研究 [J]. 当代财经, 2017, (4): 47-56.
Zheng YF, Chen XJ, Xin Y. The determination of interest rate of China's P2P online lending: an empirical study based on cross-section data of cross-platform [J]. Contemporary Finance and Economics, 2017, (4): 47-56.

[20] Chen JC, Xia X, Lo D, et al. Defining smart contract defects on Ethereum [J]. IEEE Transactions on Software Engineering, 2020, 48(1): 327-345.

[21] 钱鹏, 刘振广, 何钦铭, 等. 智能合约安全漏洞检测技术研究综述 [J]. 软件学报, 2022, 33(8): 3059-3085.
Qian P, Liu ZG, He QM, et al. A review of smart contract security vulnerability detection techniques [J]. Journal of Software, 2022, 33(8): 3059-3085.

[22] 成都链安. 2022 年全球 Web3 区块链安全态势报告及加密行业监管政策总结 [EB/OL]. (2022-07-09)[2024-08-01]. https://mp.weixin.qq.com/s?__biz=MzU2NzUxMTM0Nw==&mid=2247498777&idx=1&sn=35f5cfbd2e262bed6f8ebc279e3853df&chksm=fc9eac45cbe9255328207b84dd536a97c69cd469429ba4742b6b90aca4dd2167775f10a1cb96.
Chengdu Chain Security. 2022 global Web3 blockchain security landscape report and summary of regulatory policies for the crypto industry [EB/OL]. (2022-07-09)[2024-08-01]. https://mp.weixin.qq.com/s?__biz=MzU2NzUxMTM0Nw==&mid=2247498777&idx=1&sn=35f5cfbd2e262bed6f8ebc279e3853df&chksm=fc9eac45cbe9255328207b84dd536a97c69cd469429ba4742b6b90aca4dd2167775f10a1cb96.

[23] He DJ, Deng Z, Zhang YX, et al. Smart contract vulnerability analysis and security audit [J]. IEEE Network, 2020, 34(5): 276-282.

[24] Wang ZL, Jin H, Dai WQ, et al. Ethereum smart contract security research: survey and future research opportunities [J]. Frontiers of Computer Science, 2021, 15(2): 152802.

[25] Mehar MI, Shier CL, Giambattista A, et al. Understanding a revolutionary and flawed grand experiment in blockchain: the DAO attack [J]. Journal of Cases on Information Technology, 2019, 21(1): 19-32.

[26] Siegel D. Understanding the DAO attack [EB/OL]. (2023-01-14)[2024-08-01]. https://www.coindesk.com/understanding-dao-hack-journalists.

[27] Juels A, Kosba A, Shi E. The ring of Gyges: investigating the future of criminal smart contracts [C] // Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016: 283-295.

[28] Christin N. Traveling the silk road: a measurement analysis of a large anonymous online marketplace [C] // Proceedings of the 22nd International Conference on World Wide Web, 2013: 213-224.

[29] Saxena A, Misra J, Dhar A. Increasing anonymity in bitcoin [C] // Proceedings of International Conference on Financial Cryptography and Data Security, 2014: 122-139.

[30] Kiviat TI. Beyond bitcoin: issues in regulating blockchain transactions [J]. Duke Law Journal, 2015, 65: 569-608.

[31] Werbach K, Cornell N. Contracts Ex Machina [J]. Duke Law Journal, 2017, 67: 313-382.

[32] Werbach K. The blockchain and the new architecture of trust [M]. Cambridge: MIT Press, 2018.

[33] Savelyev A. Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law [J]. Information & Communications Technology Law, 2017, 26(2): 116-134.