SPESC:面向法律的智能合约设计与实践

王迪，秦博涵，宋伟静，朱岩
（北京科技大学计算机与通信工程学院，北京 100083）

摘 要： 智能合约是近年来随着区块链技术兴起而发展起来的一种程序设计、部署及运行的新构架，但目前仍缺少较为完备的面向法律智能合约语言。据此，文章对一种面向法律的智能合约描述语言——SPESC的规范化方法进行了详细介绍，它以类似于现实合同的结构、类似自然语言的语法设计实现智能合约的编撰，明确定义了当事人的义务和权利，制定了时间表达式规范及加密货币的交易规则，达到了提高合约法律性、便于法律人士与计算机人员协作合约开发、易于理解和使用的目的。

关键词： 智能法律合约；SPESC；规范；区块链
中图分类号： TP312 **文献标识码：** A

SPESC: Design and practice of smart legal contracts

Wang Di, Qin Bohan, Song Weijing, Zhu Yan
(*School of Computer & Communication Engineering, University of Science and Technology Beijing, Beijing 100083*)

Abstract: Smart contract is presented as a new infrastructure for programming, deployment and execution with the rapid pace of blockchain technology in recent years. However, there is still a lack of more comprehensive languages for law-oriented smart contract. This paper introduces a formalized method to specify law-oriented smart contract description languages, called SPESC. This method supports the composition of smart contracts with structure similar to real-world contract and grammar similar to natural language. Moreover, the proposed SPESC clearly defines the obligations and rights of the contracting parties, the time expression specifications and the transaction rules for cryptocurrencies. Based on them, our work improves the legality of the SPESC contract, facilitates the cooperation development between legal specialists and computer experts, and makes the contract easy to understand and use.

Key words: smart legal contracts; SPESC; specification; blockchain

1 引言

智能合约是近年来随着区块链技术[1]兴起而发展起来的一种程序设计、部署及运行的新构架，由于具有按照参与方约定自动执行的能力，也被认为是第二代区块链的核心技术。更为重要的是，智能合约技术[2]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，成功地解决了区块链应用开发困难的问题，代表着未来区块链技术发展的方向。

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

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

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[3]。

在智能合约语言方面，大多数智能合约语言皆从计算机编程人员的角度出发进行定义[4]，其合约的创建与维护需要依赖于计算机专业领域人士方能完成，对于跨学科领域的用户缺乏易读性、友好性[5]，也同时限制了智能合约在多领域协作中的应用。近年来高级智能合约语言（ASCL）已被一些学者提出来解决上述问题，如文献[6,7]重点在于验证智能合约的代码验证和语义确认，文献[8~10]从法律角度讨论智能合约，文献[10]从自然语言的角度分析了智能合约。

针对目前缺少较为完备的面向法律智能合约语言的现状，本文改进了智能合约描述语言（SPESC）[11]使其成为一种更加接近于法律合同的高级智能合约语言，给出了从传统静态文本合同到动态可自动执行的计算机程序的语法规范。它包含以提高合约法律性、便于法律人士与计算机人员协作合约开发、易于理解和使用为目的智能合约规范。SPESC语言采用了与现实合同类似的结构来规范智能合约，并使用了类似自然语言的语法，明确定义了当事人的义务和权利、加密货币的交易规则，对于促进智能合约法律化和协作开发智能合约具有很大的潜力。

2 SPESC语言整体结构

SPESC语言是介于现实法律合约与现有智能合约通用语言之间的一种过渡性语言，因此，在SPESC语言中智能合约被视为计算机技术、法律与金融的结合性文档。在语法结构上，SPESC语言既有法律合约的结构和语法，同时又具有一定的计算机形式化语言的特征，从而避免自然语言所有的二义性和不确定性。

SPESC语言结构和实例如图1所示，合约分为合约框架、合约参与方、合约条款和附加信息四部分。SPESC合约采用英文进行写作，合约框架用于规范合约名称、合约签名、签约时间等信息；合约参与方则对所有合约参与方进行说明（以关键字party表示）；合约条款则按照现实合约形式表达各参与方的行为、权力和义务（以关键字term表示）；附加信息则对合约涉及的其它信息进行定义（以关键字type表示）和说明。

在图1中商品买卖合约例子中，所定义条款对下面行为进行了规范：

（1）先由卖家创建合约，在买家下订单后通过调用post()动作进行邮寄；

（2）买家通过调用pay()动作将资金转到合约中作为货款；

（3）当买家调用receive()动作表示已收到货物，卖家才可调用collect获取前述资金。

从图1中不难看出，SPESC语言具有结构简单、表述上易于理解、代码量低等特点。而且，与传统通用编程语言相比，该语言具有全新定义的时序逻辑以及情态动词，用于更准确地表述合约参与方的行为。此外，SPESC语言还包含合约中需要记录的重要属性，如被出售货物的数量和价格等。

在SPESC语言执行上，由SPESC语言编写

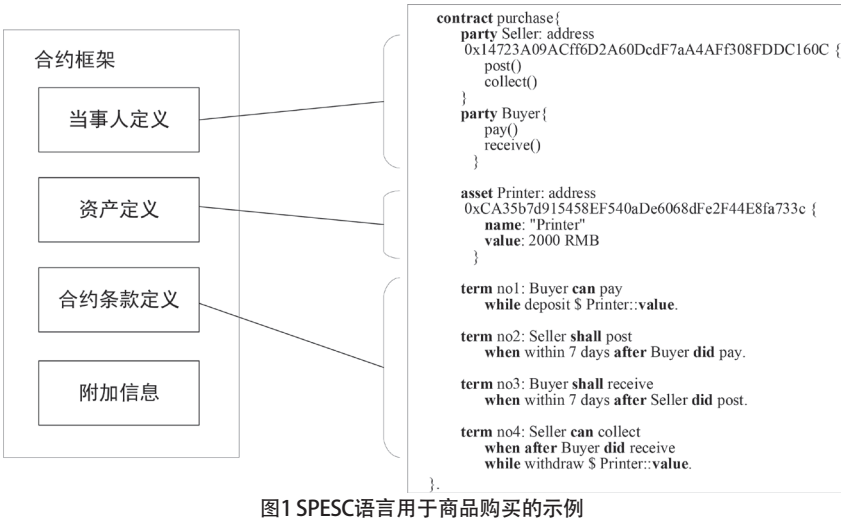

图1 SPESC语言用于商品购买的示例

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

的智能合约并不限定具体的智能合约编程语言和实现环境，可支持将其转化为任何现有区块链智能合约语言程序代码和平台上运行。需要说明的是，SPESC语言编写的合约并不与最终的可执行合约程序完全等价，SPESC语言是智能合约的高层且抽象表示，它重点对合同中的当事人、货币支付流程、时间序列等进行转换，其余补充信息亦可由计算机人员进行后期编程补充。

因此，高级智能合约语言作为一种面向法律规范的智能合约高层语言，它的语言结构和计算机本身的硬件以及指令系统无关，它的可阅读性更强，能够方便地表达合约功能和权利与义务表述。同时，所编写的智能合约也更容易被理解，也更方便被初学者所掌握和学习。

3 SPESC合约参与方规范

在SPESC语言中合约参与方被定义在合约框架的前部，这与现实合约相似。合约参与方将逐一被定义，每一名参与方由party结构进行定义，它由一个作为标识的名称、一些当事人属性和动作构成，其中，这些属性和行为是必须记录在区块链上的信息和一组动作组成。

SPESC中的参与方有四个特点：

（1）一个合约中可以有多个参与方；

（2）一个用户个体可以属于多种参与方；

（3）一个参与方可以包含多个用户个体（被称为群组）；

（4）参与方代表的用户是可以变动的。

合约参与人中定义的每项动作都代表该合约当事人可以或必须履行的某项行为。每个动作通过后面的括号进行声明，例如图1中的post()表示销售方发货行为，pay()表示购买方的付款行为等，这些行为在现实合约中可存在多种实现方法，并已能被合约参与方接受的情况下无需在合约中予以进一步说明。图2展示了三个比较简单的合约参与人的例子：卖家（Seller）、买家（Buyer）和投票者（Voters）。卖家可以行使放弃abort和收集资金collect两个行为；买家具有付款pay和接收receive两个行为；在选举合约中，投票者的定义使用了关键词group表示该参与方对应不止一个个体（由多个个体构成的成员列表表示），且每个投票者包含一个字符串类型的名字属性，还有一个属于投票者的动作——投票。上述定义的参与方及其属性和行为将可在后续合约条款中被使用。

4 SPESC合约条款规范

作为一种法律文书，SPESC语言的主体和内容是通过合约的各项条款（Contract Terms）体现的，在法律上合约条款是当事人合意的产物、合同内容的表现形式，是确定合同当事人权利义务的根据。合约条款也是合同条件的表现和固定化，是确定合同当事人权利和义务的根据。因此，合约条款定义在SPESC语言中具有核心性地位。

在SPESC规范中，合约条款是由关键字term、条款名称，以及其后跟随的一组语句构成，用以表达某个或几个合约参与方在什么条件下需要或可能履行的行为。从SPESC语法上讲，在参与方声明一个动作之后，该动作何时（必须或可以）履行则需要通过使用合同条款来进行规范。

一条SPESC合约条款涉及一个参与方和该参与方的动作，并包含该动作执行的前置、后置条件和资产转移。具体而言，一条条款包含的元素为：

（1）角色：条款内容描述的参与方；

（2）分类：这条条款是属于权利还是义务；

（3）动作：条款中的动作；

（4）前置条件：描述角色在什么条件下可以执行条款；

（5）资产转移：动作的执行时伴随的资产转移情况；

```
party Seller {
abort()
collect()
}
```

```
party Buyer {
pay()
receive()
}
```

```
party group Voters {
name : String
vote()
}
```

图2 参与方示例

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

（6）后置条件：执行结果需要满足的要求。

尽管对计算机人员而言，合约条款的定义通常可以类比为计算机语言中过程或函数的定义，但SPESC中条款定义更加抽象化和明确化，只用于规范资产的转移条件和过程；另一方面，对法律人员而言，SPESC中条款的定义采用计算机中形式化模型加以描述，更加规范化和标准化。

为了增加可读性，SPESC采用类似自然语言的语法来定义合同条款。条款的具体语法在EBNF中定义为：

term name : party (must|may) action
(**when** preCondition)?
(**while** transactions+)?
(**where** postCondition)? .

其中，在SPESC的初始模型中定义的概念以斜体显示，关键字以粗体显示。

按照动作的履行方式，SPESC条款分为权利条款和义务条款两类。

（1）义务条款：规定参与方在一定先决条件下必须执行该动作，通过条款中动作前的关键字must加以定义。

（2）权利条款：定义了参与方在一定先决条件下可以执行该动作，通过条款中动作前关键字may加以定义。

需要说明的是，当执行时条件不成立，两类条款中参与方都不能实施该行动。

条款中行为所需要满足的条件可由前置、后置和伴随条件来表达，具体为：

（1）PreCondition表示执行条款的前置条件；

（2）TransferOperation表示执行该条款的过程中伴随的资产转移；

（3）PostCondition表示该条款执行结束后该满足的后置条件。

图3给出了三条SPESC条款的示例，具体内容为：

（1）第一个条款（no1）是买卖中的例子，意思是卖家可以在买家确认购买前终止合约，并取回自己购买商品两倍价格的保证金。

（2）第二个条款（no2）是投票中的例子，意思是投票者在投票开始后，如果他还没进行过投票，那么他可以委托别人代他投票，并且将他标记为已投票状态。

（3）第三个条款（no3）是拍卖中的例子，意思是竞拍者在主持人开启竞拍且在竞拍结束前可以竞拍，同时要向合约账户转入比目前最高价高的价格，然后把当前最高价返还给当前最高者，最后记录这个竞拍者及新的最高价。

由此可见，SPESC条款具有较强而简洁的当事人行为表达能力。

5 SPESC中时间表达式规范

SPESC中表达式是指由数字、算符、符号、变量等已有意义排列方法所得的组合，它是构成语句的基础。SPESC语言表达式大致分为五类：逻辑表达式、关系表达式、运算表达式、常数表

```
term no1 : seller can abort
    when before buyer did confirmPurchase
    while withdraw $ xxxDescription::price*2.
term no2 : voters can delegate
    when voting is true and his::voted is false
    where his::voted is true.
term no3 : bidders can Bid,
    when after chairPerson did StartBidding and before BiddingStopTime
    while
        deposit $ value > highestPrice
        transfer $ highestPrice to highestBidder
    where highestPrice = value and highestBidder = this bidders.
```

图3 SPESC合约条款示例

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

达式、时间表达式。前四类与其它程序语言大致相同，但具有特有的时间表达式来描述合约中行为/动作之间的相互时序关系，下面将重点对时间表达式规范加以介绍。

在现实合约中，条款中的权利与义务往往是通过时间限制的，比如，买家必须在签订合约后的三天内付款。所以时间表达对于合约条款条件的限定是非常重要的，因此，SPESC中建立了一系列时间表达式来更方便以及更准确地表达时序关系。更严格地说，在SPESC语言中时间表达式是为了支持前置条件、后置条件和资产转移的表达，并包含时间常量、动作完成时间、当时时间等形式。

首先，SPESC智能合约语言在定义时间点（timepoint）的表示基础上将时间表达式分为四种，分别为时间变量、时间常量、全局查询、动作完成时间查询四类：

（1）时间变量指类型为时间（date/time）的变量。

（2）时间常量指一些固定的时间的值，比如3小时20分钟。

（3）全局查询指对系统和合约中某一时间相关信息的获取，比如，获取合约创建时间（start）、获取当前时间（now）（有时限于区块链而只能获取当前区块的时间）。

（4）动作完成时间查询表示某个角色完成某项动作的时间。

对动作完成时间查询而言，由于被查询方（被称为角色）可能表示一个或多个当事人，情况相对复杂，因此定义其表达式格式为：

(all | first | this)? party did action

它的返回值为一个时间点。

具体而言，动作完成时间查询根据当事人的角色不同，可分为两种情况。

首先，如果角色属于单个个体，即只有一个当事人，那么假如这个当事人没有完成这项动作，表达式将返回一个无限大的值；当这个当事人完成了这个动作，表达式返回这个角色完成这项动作的时间。

其次，如果角色是一组人的话，那么需要在动作时间查询表达式中使用全称或特称量词，这种量词分为all、first、this三种：

（1）量词all表示所有用户个体都完成该动作的时间，如all Voters did Vote。

（2）量词first表示第一个用户个体完成该动作时间，如first bidders did Bid。

（3）量词this表示当前用户完成时间，如this bidders did Bid。

除了时间表达式之外，SPESC中定义了两个基本的时间谓词：before和after来限制当事人行为完成的时间范围并定义事件触发的时间条件，其中，谓词返回值是布尔值——真或假。上述两个时间量词定义为：

(before | after) timepoint

其中，timepoint表示前面定义的时间点，before和after分别表示在这个时间点之前和时间点之后，例如before BiddingStopTime、after all Voters did Vote。

时间谓词表达式可转化为关系表达式，before timepoint等价于now < timepoint，after timepoint等价于now > timepoint，其中，now为当前时间。

谓词表达式和其它表达式相结合可以组成时间范围，例如，在买家付款后的三天内可以表示为：

(after buyer **did** pay**) and**

(before buyer **did** pay + 3 day**)**

其中，时间点可进行简单的代数运算。但这种表达比较冗杂，既不方便书写也不方便阅读。SPESC拓展了时间范围谓词的表达方式，定义为：

(within)? boundary **(before | after)** base

其中，boundary表示其边界范围，例如，within 3 day after buyer did pay。

此外，SPESC语言所支持其它表达式形式简单定义为：

（1）逻辑表达式，包含and（与）、or（或）、not（非）以及implies（蕴含）。

（2）关系表达式，包含>、>=、<、<=、=、!=和belong to（属于）。

（3）运算表达式，包含＋、－、*、/、**（乘方）。

（4）常量表达式，包含整型常量、浮点常量、布尔常量等。

总之，通过上述SPESC语言的表达式规范，

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

可以对合约中各方行为加以限定，达到易于表达和理解的目的。

6 SPESC中的货币支付功能

为了支持智能合约中交易的支付款功能，SPESC提供了一种简单的货币支付功能，能够与现有区块链系统中的数字货币相衔接，实现简单而高效的支付款功能。限于智能合约的区块链功能，在SPESC中所有转账交易都是通过交易进行的，不存在用户与用户之间直接的转账操作。

SPESC智能合约语言中的交易分为三种操作：

（1）deposit：调用者向合约账户存入一定量资产。

（2）withdraw：按照合约中的规则，合约账户向调用者转一定资产。

（3）transfer：按照合约中的规则，合约账户向某账户转一定资产。

与后两者不同，deposit是用户主动的行为，是在调用时发生的；而后两者是按照合约规定强制执行的行为，是在执行时发生的。因此，后两者只是按照合约描述执行，而deposit应作为调用动作时的限制条件表达。

具体而言，三种资产转移行为的语法：

deposit (= | > | >= | < | <=)? $amount

withdraw $amount

transfer $amount to target

为了理解上述语句的使用方法，图4给出了三种资产转移行为交易条款的两个示例，并在语句中使用了前述中时间表达式。

第一个条款表示，如果买家收到货了要调用接收（receive）操作解冻货款转给卖家，并取回保证金。

第二个条款表示，如果过了发货后15天后买家仍没有确认到货且没有申诉（其它条款表示），就按未收到货物处理，卖家就可将买家定金从合约中解冻返还给买家，并取走合约中的余额，即他自己的定金和货款。

7 SPESC实例应用

为了验证SPESC语言的有效性，本节将综合应用前述SPESC语法规范，以“打印机售卖合同”为例，展现SPESC语言在编写面向法律合同所具有的便捷性、易用性以及可读性。

（1）合约当事人定义：包括买方和卖方。

卖方拥有一个作为唯一标识的地址，并且可以执行获取交易收益、邮寄打印机的动作。

买方为群体用户，可以执行订购打印机、确认接收打印机的动作。

```
party Seller: address 0x14723…60C {
credentials:String
deliever()
collectPayment ()
}
party group Buyer{
order()
confirmReceive()
}
```

（2）资产描述：一台价值2000元人民币的打印机。

```
asset Printer: address 0xCA35b…733c {
name: "Printer"
value: 2000 RMB
}
```

（3）合约条款定义：

条款1：买方可以向卖方订购一台打印机，

```
term No1: Buyer must receive
        when within 15 day after Seller did post
        while transfer $info::price to Seller
        withdraw $info::price.
term No2: Seller may collect when 15 day after Seller did post
        while transfer $info::price to Buyer
        withdraw balance.
```

图4 三种资产转移行为交易条款示例

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

并向合约存入订金。

term no1: Buyer **may** order
while deposit $ Printer::value.

条款2：如果买方向卖方订购了一台打印机，合约生效，卖方应该在7天内将打印机寄送给买方。

term no2: Seller **must** deliver
when within 7 days after Buyer did order.

条款3：到货后买方应在7天内确认收货。

term no3: Buyer must confirmReceive
when within 7 days **after** Buyer **did** receive.

条款4：在买方确认收货后，卖方可以获取收益并结束交易。

term no4: Seller **may** CollectPayment
when after Buyer **did** confirmReceive
while withdraw $ Printer::value.

（4）合约附加信息Additional定义——添加两方当事人签名。

SellerSignature : String
BuyerSignature : String

综上，形成售卖合同对应的SPESC程序如图5所示。在合约中，Seller为个体用户，Buyer为群体用户，定义用户时便声明其所关联执行的动作，如Seller相关联动作为deliver ()和collectPayment()，动作具体内容由同名条款进行定义。

合同转化后的条款共有4个，包含两个义务条款term no2: Seller must deliver和term no3: Buyer must confirmReceive，以及两个权力条款term no1: Buyer may order和term no4: Seller may collectPayment，并依照第4节所述，定义其各自的前置、后置和伴随条件。

此外，在term no2中，规定卖家必须在买家下单后7天内执行寄出操作，此处使用when表示条款前置条件，并使用within 7 days after Buyer did order的时间表达式对事件发生时间进行约束。

在term no1中，买方订购打印机的同时需向合约存入订金，因为是买方主动的行为，采用deposit进行存入操作。term no4中规定买方确认收货后，卖方可以获取收益，此处是指当前置条件成立后，按照合约中的规则，合约账户向调用者转移资产，因此使用withdraw关键词表示货币支付。

```
contract purchase{
    party Seller: address 0x14723A09ACff6D2A60DcdF7aA4AFf308FDDC160C {
        deliver()
        collectPayment ()
    }
    party group Buyer{
        order()
        confirmReceive()
     }
    asset Printer: address 0xCA35b7d915458EF540aDe6068dFe2F44E8fa733c {
        name: "Printer"
        value: 2000 RMB
     }
     SellerSignature : String
     BuyerSignature : String
    term no1: Buyer may order
        while deposit $ Printer::value.
    term no2: Seller must deliver
        when within 7 days after Buyer did order.
    term no3: Buyer must confirmReceive
        when within 7 days after Seller did deliver.
    term no4: Seller may collectPayment
        when after Buyer did confirmReceive
        while withdraw $ Printer::value.
}.
```

图5 由买卖合同生成SPESC合约示例

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

8 结束语

本文介绍了一种类自然语言的高级智能合约语言SPESC，系统介绍了SPESC的整体结构和语法规则，详述了参与方和条款的撰写规范，并以具体实例的方式介绍了SPESC实现智能合约基础功能——货币支付的方式。SPESC具有更加接近于现实合约的特征，也易于非计算机专业人士理解和使用，代表了未来智能合约发展的趋势，具有较大的应用空间和使用价值。

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] Nakamoto S. A peer-to-peer electronic cash system[J]. Bitcoin. – URL: https://bitcoin. org/bitcoin. pdf, 2008.

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

[3] 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(03):44-49.

[4] Coblenz M . Obsidian: A Safer Blockchain Programming Language[C] In proceedings of 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C). ACM, 2017.

[5] Bhargavan K, Delignat-Lavaud A, Fournet C, et al. Formal verification of smart contracts: Short paper[C]// Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security. ACM, 2016: 91-96.

[6] Hirai Y. Defining the ethereum virtual machine for interactive theorem provers[C]//International Conference on Financial Cryptography and Data Security. Springer, Cham, 2017: 520-535.

[7] Kasprzyk K. The Concept of Smart Contracts from the Legal Perspective[J]. Review of Comparative Law, 2018, 34(3).

[8] Goldenfein J, Leiter A. Legal Engineering on the Blockchain: 'Smart Contracts' as Legal Conduct[J]. Law and Critique, 2018, 29(2): 141-149.

[9] Gomes S S. Smart Contracts: legal frontiers and insertion into the Creative Economy[J]. Brazilian Journal of Operations & Production Management, 2018, 15(3): 376-385.

[10] Allen J G. Wrapped and Stacked: 'Smart Contracts' and the Interaction of Natural and Formal Language[J]. European Review of Contract Law, 2018, 14(4): 307-343.

[11] 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.

作者简介：

王迪（1998-），女，汉族，河南开封人，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。

秦博涵（1995-），男，汉族，北京人，北京科技大学，在读硕士；主要研究方向和关注领域：智能合约、区块链。

宋伟静（1997-），女，汉族，河北邯郸人，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。

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。

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net