

团 体 标 准

T/CIE 095—2020

区块链智能合约形式化表达

Formal expression of blockchain smart contract

2020-12-21 发布

2021-01-01 实施

中国电子学会 发 布

中国电子学会 (内部)

目 次

前言 I

引言 II

1 范围 1

2 术语和定义 1

3 符号和关键词 1

 3.1 符号 1

 3.2 关键词 2

4 表示形式 3

5 构成要素 3

6 要素的表述 4

 6.1 合约框架 4

 6.2 合约名称 4

 6.3 当事人描述 4

 6.4 标的 6

 6.5 合约条款 6

 6.6 权利和义务 7

 6.7 资产操作 8

 6.8 表达式符号 9

 6.9 时间表示 9

 6.10 附加信息 10

 6.11 合约订立 10

附录 A（资料性） 智能法律合约及智能合约示例 12

 A.1 智能法律合约示例 1 12

 A.2 智能法律合约示例 2 14

 A.3 智能合约示例 16

附录 B（资料性） 智能法律合约签订流程 18

参考文献 19

图 1 合同转换关系示意图 II

图 2 智能合约签订流程示意图 3

图 3 智能法律合约构成要素关系图 4

表 1 关键词及其含义 2

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由北京科技大学提出。

本文件由中国电子学会区块链分会技术归口。

本文件起草单位：北京科技大学、北京大学、北京市经济和信息化局、北京市社会公信建设促进会、天津蛟图信息科技有限责任公司、北京航空航天大学、中化能源股份有限公司、北京文章无忧信息科技有限公司、贝壳找房(北京)科技有限公司、京东数字科技集团。

本文件主要起草人：朱岩、秦博涵、何啸、王迪、孙贻滋、郭倩、宋伟静、王晟典、洪京一、姚前、蒋国庆、李冀宁、刘国伟、伊然、冯荣权、张韬、胡凯、徐双泉、韩心慧、英伟、甘国华。

引言

区块链是采用密码手段保障、只可追加、链式结构组织的分布式账本系统。智能合约允许开发者利用编程语言在区块链上编写自动执行程序,实现价值交换等应用并存证。随着数字经济的发展,区块链智能合约的规范化需求日益强烈,然而现有智能合约面临专业性强、可读性差、生产效率低等实际问题,现实法律合同到可执行程序代码之间的高效转化难以实现。这既影响了行业应用与计算机及法律界人士的跨领域合作,也阻碍了智能合约的法律化进程。

本文件通过提供一种适用法律合同的智能合约框架及语法规则,使所开发的智能法律合约成为一种介于现实法律合同与智能合约之间的过渡性法律文档。如图 1 所示,现实法律合同以自然语言为载体,可翻译成由智能法律合约语言撰写的智能法律合约,进而转化为由智能合约语言编写的智能合约。

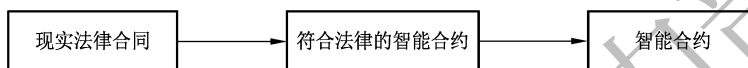


图 1 合同转换关系示意图

智能法律合约以程序代码表达合同条款,将现实法律合同与网络空间的程序代码相衔接,保证智能法律合约既有现实合同的法律特征和易理解性,又有计算机程序代码的规范性,促进计算机、法律等专业人员的跨领域协作。在区块链确权基础上,智能法律合约将物理世界资产,如房子、健康数据和版权等表达为数字资产,并与可编程数字货币相结合,使其在区块链网络上自由使用和流通,推动数字经济快速健康发展。

本文件的发布机构提请注意,声明符合本文件时,可能涉及第 6 章与智能法律合约语法相关的专利的使用。

本文件的发布机构对于该专利的真实性、有效性和范围无任何立场。

该专利持有人已向本文件的发布机构承诺,他愿意同任何申请人在合理且无歧视的条款和条件下,就专利授权许可进行谈判。该专利持有人的声明已在本文件的发布机构备案。相关信息可以通过以下联系方式获得:

专利:202010381549.5 一种法律合约的智能可执行合约构造与执行方法和系统

专利持有人姓名:北京科技大学

地址:北京市海淀区学院路 30 号

请注意除上述专利外,本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别专利的责任。

区块链智能合约形式化表达

1 范围

本文件规定了智能合约语言的结构和语法,界定了有关术语和定义。

注:本文提供的智能法律合约示例及智能合约示例,见附录 A。

本文件适用于通用智能合约设计、开发和使用,也可为区块链厂商和用户构建智能合约平台参考。

2 术语和定义

下列术语和定义适用于本文件。

2.1

智能合约 smart contract

部署在区块链上、在满足预定条件时可自动执行并存证的计算机程序。

2.2

符合法律的智能合约 smart contract complying with law

一种含有合同构成要素、涵盖合同缔约方依据要约和承诺达成履行约定的计算机程序。

注:在不引起混淆的情况下,本文件中简称为“智能法律合约”。

2.3

智能合约语言 smart contract language

用于定义智能合约、包含词汇和语法规则的形式化表达规范。

2.4

符合法律的智能合约语言 smart contract language complying with law

可实现符合法律的智能合约的编程语言。

注:在不引起混淆的情况下,本文件中简称为“智能法律合约语言”。

2.5

智能合约平台 smart contract platform

支持智能合约可执行程序开发、生成、部署、运行、验证的信息网络系统。

2.6

账户 account

具有一定的格式和结构,用于描述当事人、操作和反映标的等智能法律合约要素的增减变化情况及结果的载体。

2.6.1

用户账户 party account

当事人所拥有账户。

2.6.2

合约账户 contract account

智能法律合约在智能合约平台上所拥有账户。

3 符号和关键词

3.1 符号

下面符号适用于本文件:

@@	中文意思表示的前缀
::=	表示定义,即“被定义为”
?	前置关键词任选
	同级元素的“或”关系
{ } ()	可供选择的语句集合
.	语句结束符
+	零条或多条语句
//	注释符
‘ ’, “ ”	字符串类型
0x	十六进制数的前缀
, 空格	同级元素的并列与分割

3.2 关键词

本文件中所用关键词及其对应的含义如表 1 所示。

表 1 关键词及其含义

关键词	含义
he, she, his, her, himself, herself, this, the	当前的,相当于程序语言中 this
=, is	相等
:	分隔符
::	属性信息引用
! =, <>, isn't	不相等
all, for all, some, exist	全称量词和存在量词
can, must, cannot	权利限制,应当限制,禁止限制
origin	动作执行前账户的值
after, before, within	在……之后(前、内)
did	常与 after 连用,表示某当事人做过某事
true, false	布尔值
value	当事人所转移的资产数目
and, or, not, implies	逻辑符号
>, >=, <, <=, belongsTo	关系符号
Cname, Pname, Aname, Tname, Bname, Dname	名称表示的合约、当事人、资产、一般条款、违约条款、附加信息等实体,统称为 Entity
year, month, date, hour, minute, second, now	时间符号
String, Money, Date, Integer, Float, Boolean, Right, Time	变量类型的符号
when, while, where	条款中的条件标识保留字
transfer, withdraw, deposit	资产操作保留字
contract, info, right, party, group, asset, term, breach term, arbitration term, contract conclusion, signature of party, addition, serial number, of, to, institution	其他保留字

4 表示形式

4.1 智能法律合约属于数据电文。当事人订立智能法律合约,采取要约、承诺方式。

4.2 智能法律合约遵循《中华人民共和国民法典》《中华人民共和国电子签名法》及有关法律法规相关条文,具有与现实法律合同相同的法律效力,智能法律合约和现实法律合同使用的词句推定具有相同含义,两者使用的词句不一致时,应根据合同的相关条款、性质、目的以及诚信原则等予以解释。

4.3 智能法律合约可转化为数据电文表示的可执行程序,经智能法律合约签订后,在智能合约平台自动执行并存证。

4.4 智能法律合约可根据应用场景采用中文、英文或中英文混合形式编写。

4.5 智能法律合约生命周期包括以下三个阶段。

- 生成阶段:当事人达成合意后撰写智能法律合约,经翻译形成计算机可执行程序;
- 订立阶段:将智能法律合约与计算机可执行程序整合后部署至区块链,由当事人各自调取并签名确认后写回区块链存证,订立后的智能合约可随时被调取查用,签订流程应参照图 2 中示例(参见附录 B);
- 执行阶段:在满足预定条件时由区块链节点调取并运行相关代码,修改合约状态并写回区块链存证,直至合约终止。

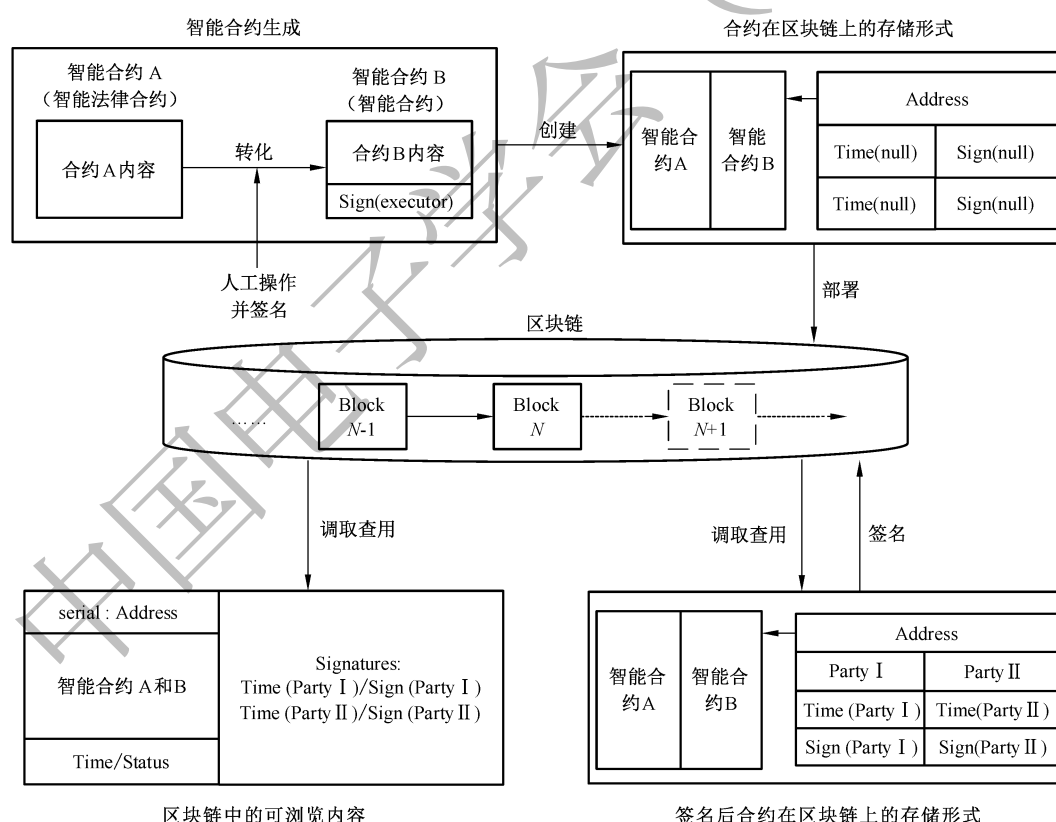


图 2 智能合约签订流程示意图

5 构成要素

智能法律合约可涵盖当事人信息、标的、数量、质量、价款或者报酬、履行期限和方式、违约责任、解

决争议的方法等内容。智能法律合约框架内的构成要素宜包括合约名称、当事人描述、标的、合约条款、附加信息、合约订立等,其中,合约条款可包括一般条款、违约条款、仲裁条款等。智能法律合约编写过程中可涉及权利和义务、资产操作、表达式、时间表示等语法规范。上述要素之间关系如图3所示。

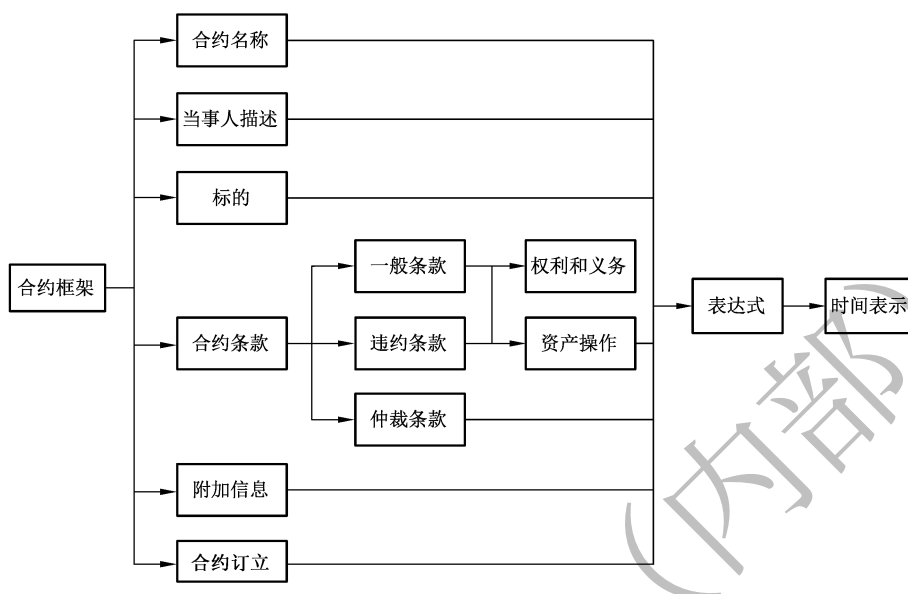


图3 智能法律合约构成要素关系图

6 要素的表述

6.1 合约框架

智能法律合约由合约名称及合约内容构成。合约内容通常包括:当事人描述、资产描述、合约条款、附加信息、合约订立。

$Contracts ::= Title \{ Parties + Assets + Terms + Additions + Signs + \}$

6.2 合约名称

合约名称可由合约标题和合约序号构成。语法如下:

@@ 合约标题:合约序号

$Title ::= contract \ Cname (; \ serial \ number \ Chash) ?$

注:合约序号是指智能法律合约经哈希运算所求取的唯一性编号。

示例:

@@买卖合同;0x827198...ab193

contract purchase; serial number 0x827198...ab193

6.3 当事人描述

当事人描述可包含当事人的名称、姓名、住所、账号等当事人所拥有的属性及属性值,可采用当事人身份认证等技术措施保证其身份唯一性。语法如下:

@@ 当事人 群体? 名称 {属性域 + }

$Parties ::= party \ group ? \ Pname \{ field + \}$

其中,属性域用于描述当事人所拥有的属性及属性值,由使用冒号分割的二元组表示,左部为属性

名称,右部为属性值,表示如下:

@@ 属性:(常量 | 变量类型)

field := attribute : (constant | type)

注: 属性值可分为常量或变量类型,当属性值为变量类型时,其初始值为空。

实体属性值的引用使用 Entity:: attribute 形式表达,其结果为该属性的值。

示例 1:

@@当事人信息:卖家,登记信息包括:当事人账号:0x7c84e8...2934;姓名:张三。

party Seller { account: 0x7c84e8...2934 name: 'Zhang San' }

注: 当事人账号指该当事人在区块链中所拥有的用户账户地址。

示例 2:

@@群组当事人信息:竞标人,登记信息包括:当事人账号。

party group Voters{ account: Integer }

注: 群组当事人可表示为动态加入的当事人列表。

6.4 标的

合约标的指当事人权利和义务共同指向的对象,一般分为物、行为、智力成果等,在智能法律合约中用资产加以表示,在区块链中应存在该资产的描述。语法如下:

@@ 资产 资产名称 {资产描述{属性域+} 资产权属{属性域+}}

Assets ::= **asset** Aname{ **info**{ *field* + } **right** { *field* + } }

注: 资产的定义应包含资产的名称、资产的属性及资产的权属。

info 用以描述该资产拥有的属性及属性值。**right** 用于明确资产的权属,通常包括:所有权(ownershipRight)、使用权(useRight)、占有权(possessRight)、收益权(usufructRight)、处分权(disposeRight),可作为类型使用,用户可根据实际需要自行添加权属。

示例 1:

@@资产:房屋,属性信息包括:产权编号:0x71a2f8...78d93;面积:50;用途:商业;价格:货币资产;权属信息包括:收益权、使用权。

```
asset House{
    info{ sn: 0x71a2f8...78d93 area : 50 usage : "business" price : Money }
    right{ houseBenefitRight: usufructRight houseUse : useRight }
}
```

注: usufructRight 与 useRight 类型用于记录权属信息;Money 用于表示货币资产。

资产表达式用于条款中资产的调用,定义如下:

@@ 资产表达式: \$ (具体数量)? (具体权属)? 资产名称

AssetExpressions ::= \$ (amount)? (right of)? Aname

注: Aname 为智能法律合约中声明的资产。right 是指对该资产定义时声明的权利,如果无权属说明,则默认为所有权。

示例 2:

@@20 元。

\$ 20 RMB

注: 系统中预定义的货币资产包括:人民币(RMB)、美元(USD)等。

示例 3:

@@在智能法律合约中声明房屋资产。

\$ House

示例 4:

@@本金的 120%。

\$ 120% * principal

注：本金为 Money 类型的资产。

示例 5：

@@在智能法律合约中声明资产 House 的 50% 所有权。

\$ 50% ownershipRight of House

6.5 合约条款

合约条款包括一般条款、违约条款、仲裁条款等类型。

Terms ::= **GeneralTerms** | **BreachTerms** | **ArbitrationTerms**

6.5.1 一般条款

一般条款包含条款名称、条款当事人、当事人权利和义务(必须、可以或禁止履行的行为)、条款执行条件、资产转移以及条款执行后应满足的后置条件。语法如下：

@@ 条款名:当事人(必须 | 可以 | 禁止) 行为(属性域+)

(执行所需的前置条件)?

(伴随的资产操作+)?

(执行后需满足的后置条件)?

GeneralTerms ::= **term** Tname: Pname (**must** | **can** | **cannot**) action(*field* +)

(**when** preCondition)?

(**while** transactions+)?

(**where** postCondition)?.

注：条款声称某当事人在何种前置条件下必须、可以或禁止采取何种行为，同时伴随着何种资产操作，完成后应满足何种后置条件。其中，行为是对其后属性列表的操作，它由智能合约平台的程序实现。具体包括：

——preCondition 由表示前置条件的表达式构成，在条款执行前进行检测，如果满足前置条件，则可执行条款；如果不满足，不能执行条款。

——transactions 表示条款执行过程中伴随的资产操作。

——postCondition 由表示后置条件的表达式构成，在条款执行完后进行检测，如果满足后置条件，则本条款执行成功；如果不满足，则执行失败。

示例：

@@条款 1: 竞拍者可在竞拍开始后出价竞拍，向合约账户转入大于当前最高价的资金，出价最高者为得主。

term no1: bidder **can** bid()

when after bidBegin

while deposit value > highestPrice

where winner = **this** bidder.

6.5.2 违约条款

违约条款是指双方约定的当事人不履行智能法律合约中规定的义务或履行义务不符合约定时，应承担的法律责任。即在指定条款的后置条件未得到满足且此违约条件的前置条件得以满足时，当事人必须或可以执行违约处理，可伴随相应的资产转移，执行后应满足违约条款的后置条件。

@@ 违约条款 条款名(针对 条款名+)? : 当事人(必须 | 可以) 违约处理(属性域+)

(执行所需的前置条件)?

(伴随的资产操作+)?

(执行后需满足的后置条件)?

BreachTerms ::= **breach term** Bname (**against** Tname+)? : Pname (**must** | **can**) action(*field* +)

(**when** preCondition)?

(**while** transactions +)?

(**where** postCondition)?.

注：违约条款通常可规定违约者必须执行的动作或受害者可以执行的动作。

示例：

@@如果买家在预定了购买房屋之后，房屋主人把房屋租出去了，那么房屋主人应该赔偿买家违约金。

breach term no6 **against** no4 : houseOwner **must** compensate()

when houseOwner **did** lend **after** buyer **did** order

while transfer default **to** buyer.

6.5.3 仲裁条款

智能法律合约中以仲裁条款形式规定解决争议的方法，具体争议可由自然语言陈述，并可指定仲裁机构，语法如下：

@@(所声明之争议)? 由某仲裁机构进行裁决。

ArbitrationTerms :: = **arbitration term** : (The statement of any controversy)?

administered by **institution** : instName.

注：可选择区块链网络中具有司法管辖权的节点作为仲裁机构。

示例：

@@凡因本智能法律合约引起的或与其有关的一切劳动争议，均由北京劳动仲裁委员会按照仲裁规则进行裁决。

arbitration term : Any labor controversy or claim arising out of or relating to this contract, or the breach thereof, shall be settled by arbitration administered by **institution** : Beijing Labor Arbitration Commission.

6.6 权利和义务

6.6.1 权利

权利限制应使用关键词 **can**，用于在满足前置条件时当事人可执行该条款或不执行。

示例：

@@条款 2：投票者可在主席发表提案后开始投票。

term no2: voter **can** vote (target)

when after chairPerson **did** propose.

注：投票属于权利，投票者可行使自己的权利为提案投票，或不行使自己的权利，放弃投票。

6.6.2 义务

义务限制包括应当限制与禁止限制。

——应当限制应使用关键词 **must**，用于在满足前置条件时当事人必须执行该条款。

示例 1：

@@条款 3：借贷者需要在借贷后两年内归还借款。

term no3: borrower **must** return (loan)

when within 2 year **after** borrower **did** lend.

注：归还属于义务，当事人需要在规定期限内履行自己的义务。

——禁止限制应使用关键词 **cannot**，用于在满足前置条件时当事人不能执行该条款。

示例 2：

@@条款 4：房屋所有者在买家预定后，不能再把房屋租出去。

term no4: houseOwner **cannot** rent()

when after buyer **did** order.

某一禁止条款可设置多种限制方式，既可按执行条件进行限制，也可直接对执行结果进行限制，

示例 3:

对于“投票者不可给自己投票”,如果直接投票给候选人,有如下两种表述方式:

@@条款 5_1:如果选举人的投票对象是自己(执行条件),选举人不能执行投票。

term no5_1: voter **cannot** elect (target)

when target = **this** voter.

@@条款 5_2:如果选举人投票结果是使自己选票加一(执行结果),选举人不能投票。

term no5_2: voter **cannot** elect(target)

where this voter:: candidate = **this** voter :: **origin** candidate + 1.

注:对条款 5_1,如果投票者将选票给代理人,再由代理人投给投票者,这种行为将被许可;而用条款 5_2 直接对执行结果进行限制则可避免上述行为。

6.7 资产操作

资产操作是指智能法律合约执行过程中对资产的不同操作方式,通常用来实现标的物在不同账户之间的转移,资产操作包含以下三类。

6.7.1 存入

当事人主动由其用户账户向合约账户存入资产,作为条款的执行条件使用,可直接指定存入的资产或根据价值关系进行限制,后者在关系满足时才能转移指定的资产,语法如下:

@@ 存入(满足某种价值关系的)? 资产描述。

Deposits ::= **deposit** (value RelationOperator)? **AssetExpression**

示例 1:

@@存入大于当前最高价的金额

deposit value > highestPrice

注:在竞拍条款中要求存入金额大于目前最高价才能执行竞拍操作,其中 highestPrice 表示当前最高价,为货币类型(Money)资产。

示例 2:

@@存入大于 10 元的金额。

deposit value > \$ 10 RMB

6.7.2 取回

当事人执行条款过程中从合约账户中取回一定资产,语法如下:

@@ 取回 指定资产。

Withdraws ::= **withdraw** **AssetExpression**

示例:

@@取回本金和利息(资产表达式中数额 * (1+息率))。

withdraw principal * (1+rate)

注:在执行取款条款时,可取回本金和利息。

6.7.3 转移

当事人执行条款过程中从当前合约账户向其他当事人转移一定资产,语法如下:

@@ 转移指定资产到某当事人。

Transfers ::= **transfer** **AssetExpression** **to** target

示例 1:

@@向卖家转移保证金。

transfer welfare **to** seller

注：welfare 是买家事先存入的保证金，为 Money 类型，在买方确认收货时，会将事先存入合约账户的保证金转给卖家。

条款可有多条资产操作语句。

示例 2：

@@条款 6：借贷者可抵押自己的房子，将房屋的所有权存入合约账户，同时取出约定好的资金。

term no6: borrower can mortgage ()

while deposit \$ House and withdraw HousePrice.

6.8 表达式符号

智能法律合约中采用表达式规范合约内容，其中条款条件表达式结果为布尔值。表达式中使用的符号包括：

- 逻辑符号，包括：and、or、not、implies；
- 关系符号，包括：>、>=、<、<=、=、!=、belongsTo；
- 算术符号，包括：+、-、*、/、%；
- 常量符号，包括：数字、字符串、true、false；
- 时间符号，包括：month、day、year、hour、minute、second、now；
- 类型符号，包括：String、Money、Date、Integer、Float、Boolean、Right、Time。

6.9 时间表示

时间表示由时间点表达式和时间段表达式构成。

6.9.1 时间点表达式

时间点表达式分为四种：时间变量、时间常量、全局查询、动作完成时间查询。

- 时间变量是指日期(Date)类型的变量。
- 时间常量是指固定时间的值，比如 2019 年 11 月 18 日。
- 全局查询是指获取与智能法律合约运行相关的时间数值，如获取区块链智能合约生效时间(effective_date)、获取当前时间(now)，由智能合约平台提供。
- 动作完成时间查询指当事人完成某项动作的时间，语法如下：

@@ 动作完成时间查询：(任意 | 存在 | 当前)? 当事人执行某动作的时间。

ActionEnforcedTimeQuery ::= (all | some | this)? party did action

注：根据当事人为个体或群体情况，可将时间查询分为如下两种情况：

- 当事人为个体时，不必添加冠词 all、some、this。

示例 1：

@@买家支付完成的时刻。

buyer did pay

- 当事人为群体时，可通过添加冠词 all、some、this 查询特定时间。

- 冠词 all：表示群体当事人中最后一个完成某动作的时间，若存在任意个体未完成，则查询结果为未完成。

示例 2：

@@所有投票者投票完成的时刻。

all voter did vote

- 冠词 some：表示群体当事人最近一个完成某动作的时间，若群体中无个体完成动作，则查询结果为未完成。

示例 3：

@@竞标者群体中最近一个完成拍卖动作的时刻。

some bidder did bid

- 冠词 **this**:表示当前条款执行人若属于该群体,则查询结果为该个体的完成时间。

示例 4:

@@本人投票完成的时刻。

this voter **did** vote

6.9.2 时间段表达式

时间段分为时间变量和时间常量两类。

——时间变量是指时间类型(**Time**)的变量;

——时间常量是指固定长度的时间,如 1 天、2 小时等。

时间段表达式定义如下:

@@(目标时间)? (是 | 否) 在基础时间点(之前 | 之后)

TimePredicate ::= (targetTime)? (is | isn't) (before | after) baseTime

注: targetTime 和 baseTime 都是时间点,如果没有设定目标时间点,则默认与当前时间进行比较。

示例 1:

@@本人投过票之后且所有人投票完成之前。

(after this voter did vote) and (before all voter did vote)

示例 2:

@@本人投票完成时刻是在有效期之后。

this voter **did** vote **is after** effective_date

边界时间段表达式定义如下:

@@ 边界时间点(之前 | 之后) 一段时间(内)?

BoundedTimePredicate ::= (within)? boundary (before | after) baseTime

注: boundary 为时间段,baseTime 为时间点。

示例 3:

@@在拍卖结束前的三天内。

within 3 day **before** auctionEnd

示例 4:

@@在拍卖结束前的三天以前。

3 day **before** auctionEnd

6.10 附加信息

附加信息给出智能法律合约所需的其他补充条件的定义,包括:合约属性、合约标的、当事人签名、保证人信息及签名、附加条款、程序变量、数据结构定义等,可置于智能法律合约任何位置,语法如下:

@@(属性域 +) 或(附加信息 附加信息名 { 属性域 +})

Additions ::= field + | (addition Dname { field + })

注: 附加信息引用采用 (Cname::) ? **attribute** 或 Dname::**attribute** 的形式。

示例:

@@最高拍卖金额和拍卖停止时间。

highestPrice : **Money**

biddingStopTime : **Date**

6.11 合约订立

@@ 合约订立 : (所有当事人的约定)?

Signs ::= **Contract conclusion** : (The statement of all parties.)?

{ **Signature of party** Pname (当事人签字):

```

    {   printedName(打印名):String,
        signature(法定代表人签字): String,
        date(签订日期): Date
    },+
}

```

示例：

@@合约订立：本智能法律合约当事人不得以任何形式修改本合同，除非以书面形式并经双方签字。本合同及其附件构成合约双方的完整协议。本合同对当事各方及其继承人、受让人均具有约束力。通过签署本协议，各方同意上述条款。双方各收到一份本协议，并负责维护其条款。双方同意将本合同转化为智能合约平台上的计算机程序，并同意该程序及其执行具有相同法律效力。

Contract conclusion: This contract may not be modified in any manner unless in writing and signed by both parties. This document and any attachments hereto constitute the entire agreement between the parties. This Contract shall be binding upon the parties, their successors and assigns. By signing this agreement, all parties agree to the terms as described above. Each of parties will receive one copy of this agreement, and will be responsible for upholding its terms. Both parties agree with conversion from this contract to computer programs on smart contract platform, and approve that the programs' implementation has the same legal effect.

Signature of party auctioneer(拍卖人签字)：

```

{   printedName(打印名):Yao San,
    signature(法定代表人签字):0x2319...8DE393,
    date(签订日期):2020/7/12
}

```


附 录 A
(资料性)
智能法律合约及智能合约示例

A.1 智能法律合约示例 1

示例：一种网络竞买合同对应的智能法律合约。

@@网络竞买合同协议书

contract SimpleAuction{

@@甲方信息：拍卖人，登记信息包括：用户账户信息：0x712379218...C4E80。

party auctioneer{

account : 0x712379218...C4E80

}

@@乙方信息：竞买人，属于群体，登记信息包括：用户账户信息：[0x93A8BCD...793968, 0x48BD38... 92AC93]；
账户曾出价累计值：货币资产。

party group bidders{

account : [0x93A8BCD...793968, 0x48BD38...92AC93]

amount : Money

}

@@当前最高价、最高出价的竞拍者、竞拍结束时间。

highestPrice : Money

highestBidder : bidders

biddingStopTime : Date

@@标的物：竞拍货品，拍卖人需要提供拍卖物的物品名称、数量等相关信息。

asset good{

info{

name : Name //物品名称

quantity : Integer //物品数量

price : Money //价格

package : String //运送包装

}

}

@@条款 1：拍卖人可发起竞拍，在动作执行后，当前最高价应为拍卖人输入的底价，结束时间为当前时间加上输入的竞拍持续时间。

term no1 : auctioneer **can** StartBidding(reservePrice : Money, auctionDuration : Date)

when before auctioneer **did** StartBidding

where highestPrice = reservePrice **and** biddingStopTime = auctionDuration + **now**.

@@条款 2：竞买人可在拍卖人发起竞拍后至竞拍结束前进行出价，如果出价大于目前所给最高价格，则出价成功。

term no2 : bidders **can** Bid

when after auctioneer **did** StartBidding **and before** biddingStopTime

while deposit value > highestPrice

where highestPrice = value **and** highestBidder = **this** bidder **and this** bidder::amount = **this** bidder::

origin amount + value.

@@条款 3_1:若竞买人不是最高出价者,且当前合约账户中存有其押金,竞买人可取回无效押金,此后该竞买人押金清零。

```
term no3_1 : bidders can WithdrawOverbidMoney
  when this bidder::amount > 0 and this bidder isn't highestBidder
  while withdraw this bidder::amount
  where this bidder::amount = 0.
```

@@条款 3_2:若竞买人是当前最高出价者,且当前合约账户中存有其之前的失败押金,竞买人可取回无效押金,并登记成为当前竞拍最高价。

```
term no3_2 : bidders can WithdrawOverbidMoney
  when this bidder::amount > highestPrice and this bidder is highestBidder
  while withdraw this bidder::amount-highestPrice
  where this bidder::amount = highestPrice.
```

@@条款 4:拍卖人可在竞拍时间结束后,收取拍卖成交款。

```
term no4 : auctioneer can StopBidding
  when after biddingStopTime and before auctioneer did StopBidding
  while withdraw highestPrice.
```

@@仲裁条款:凡因本智能法律合约引起的或与其有关的一切争议,均由北京互联网法院管辖。

Arbitration term : Any controversy or claim arising out of or relating to this contract, or the breach thereof, shall be settled by arbitration administered by **institution** : BeijingInternetCourt.

@@合约订立:本智能法律合约当事人不得以任何形式修改本合约,除非以书面形式并经双方签字。本合约及其附件构成合约双方的完整协议。通过签署本协议,各方同意上述条款。双方各收到一份本协议,并负责维护其条款。双方同意将本合约转化为智能合约平台上的计算机程序,并同意该程序及其执行具有相同法律效力。

Contract conclusion: This contract may not be modified in any manner unless in writing and signed by both parties. This document and any attachments hereto constitute the entire agreement between the parties. This Contract shall be binding upon the parties, their successors and assigns. By signing this agreement, all parties agree to the terms as described above. Each of parties will receive one copy of this agreement, and will be responsible for upholding its terms. Both parties agree with conversion from this contract to computer programs on smart contract platform, and approve that the programs' implementation has the same legal effect.

Signature of party auctioneer(拍卖人签字):

```
{
  printedName(打印名): Yao San,
  signature(法定代表人签字): 0x23198de...393,
  date(签订日期): 2020/7/12
}
```

Signature of party bidders(竞拍人签字):

```
{
  printedName(打印名): 柳湾,
  signature(法定代表人签字): 0x877238...201,
  date(签订日期): 2020/7/12
}
{
  printedName(打印名): 秦源,
  signature(法定代表人签字): 0x9340593...495,
  date(签订日期): 2020/7/12
}
```

```
}
```

A.2 智能法律合约示例 2

示例：一种房屋租赁合同对应的智能法律合约。

@@房屋租赁合同协议书

contract HouseLease{

@@甲方信息:出租人,登记信息包括:用户账户信息:0x82384a68...90e72。

party Landlord{

 account : 0x82384a68...90e72

 }

@@乙方信息:承租人,登记信息包括:用户账户信息:0x9845a6b...73c4e。

party Tenant{

 account : 0x9845a6b...73c4e

 }

@@合约属性:出租人押金、承租人押金、房屋租金、总租金、合约起始时间、合约终止时间、支付租金的时间、租金支付周期。

addition infos {

 renterBail:Money

 renantBail:Money

 rental:Money

 totalRental:Money

 startLeasingTime:Date

 endLeasingTime:Date

 payDate:Date

 payDuration:Date

 }

@@标的物:房屋,出租人应提供产权号、地址、面积、用途、价格等信息。

asset House{

info{ /* 房屋的具体信息 */

 ownershipNumber: Integer

 location: Address

 area: Integer

 usage: String

 price: Money

 }

right{ /* 所有者可对该资产行使的 4 种权利 */

 houseUseright : useRight

 houseUsufruct : usufructRight

 dispositionRight: Right

 ossessionRight: Right

 }

 }

@@条款 1:出租人可通过交纳出租人押金来注册房屋信息。

term term1: Landlord can registerHouse

while deposit infos::renterBail.

@@条款 2:承租人可在出租人注册房屋之后,通过交纳承租人押金来确认租赁,动作执行之后要求自动记录当前时间为合约的开始时间、且计算截止时间并设置合约执行有效期和承租人支付租金的时间。

term term2: Tenant can confirmLease

when after Landlord did registerHouse

```

while deposit infos::tenantBail
where infos::startLeasingTime = now and infos::endLeasingTime = endLeasingDuration+now
and infos::payDate = payDuration+now and infos::payDuration = payDuration.
@@条款 3: 承租人确认承租 7 天内, 出租人必须将房屋使用权转移给承租人。
term term3: Landlord must transferHouse
when within 7 day after Tenant did confirmLease
while deposit $ houseUseright of house.
@@条款 4: 在承租人确认承租后, 在规定的支付租金日期之前, 承租人必须支付租金。
term term4: Tenant must payRent
when before infos :: payDate and after Landlord did transferHouse
while deposit infos ::rental.
@@条款 5: 租赁合同到期后且承租人检查房租之前, 承租人应归还房屋, 即将房屋使用权转回出租人。
term term5: Tenant must returnHouse
when after infos :: endLeasing Time and before Landlord did checkHouse
while transfer $ houseUseright of house to Landlord.
@@条款 6: 出租人在承租人确认归还房屋后可对房屋进行检查。
term term6: Landlord can checkHouse
when after Tenant did returnHouse.
@@条款 7: 出租人在检查房屋之后的 15 天内, 可收取全部租金, 即取出租金。
term term7: Landlord can collectRent
when within 15 day after Landlord did checkHouse
while withdraw infos::rental.
@@条款 8_1: 在检查房屋之后的 15 天内, 出租人可取出出租人押金。
term term8: Landlord can collectBail
when within 15 day after Landlord did checkHouse
while withdraw infos :: renterBail.
@@条款 8_2: 在检查房屋之后的 15 天内, 承租人可取出承租人押金。
term term9: Tenant can collectBail
when 15 day after Landlord did checkHouse
while withdraw infos :: tenantBail.

```

@@仲裁条款: 凡因本智能法律合约引起的或与其有关的一切争议, 均由北京互联网法院管辖。

Arbitration term : Any controversy or claim arising out of or relating to this contract, or the breach thereof, shall be settled by arbitration administered by **institution** : BeijingIneternetCourt.

@@合约订立: 本智能法律合约当事人不得以任何形式修改本合约, 除非以书面形式并经双方签字。本合约及其附件构成合约双方的完整协议。通过签署本协议, 各方同意上述条款。双方各收到一份本协议, 并负责维护其条款。双方同意将本合约转化为智能合约平台上的计算机程序, 并同意该程序及其实施具有相同法律效力。

Contract conclusion: This contract may not be modified in any manner unless in writing and signed by both parties. This document and any attachments hereto constitute the entire agreement between the parties. This Contract shall be binding upon the parties, their successors and assigns. By signing this agreement, all parties agree to the terms as described above. Each of parties will receive one copy of this agreement, and will be responsible for upholding its terms. Both parties agree with conversion from this contract to computer programs on smart contract platform, and approve that the programs' implementation has the same legal effect.

Signature of party Landlord(出租人签字):

```

{
  printedName(打印名):Mike Micheal,
  signature(法定代表人签字): 0x9045f7a...80d4,
  date(签订日期): 2020/8/20
}

```

Signature of party Tenant(承租人人签字):

```

{
  printedName(打印名):姜爽,
  signature(法定代表人签字): 0x46b9d3e...a983,
  date(签订日期): 2020/8/20
}

```

```

}

```

A.3 智能合约示例

示例：A.1 中智能法律合约示例对应 Solidity 语言编写的智能合约。

```
pragma solidity >=0.5.0 <0.6.0;

import "./bidders.sol";
import "./auctioneer.sol";

contract SimpleAuction {

    biddersT bidders;
    auctioneerT auctioneer;

    uint highestPrice;
    address highestBidder;
    uint biddingStopTime;

    constructor() public{
        bidders = new biddersT();
        auctioneer = new auctioneerT();
        auctioneer.regist(msg.sender);
        auctioneer.name = "Yao San";
        auctioneer.signature = "0x23198de...393";
        auctioneer.signDate = 2020/7/12;
        bidders.add("柳湾", "0x877238...201", 2020/7/12);
        bidders.add("秦源", "0x9340593...495", 2020/7/12);
    }

    modifier onlybidders{
        require(bidders.contains(msg.sender));
        _;
    }

    modifier onlyauctioneer{
        require(auctioneer.getAddress() == msg.sender);
        _;
    }

    function StartBidding(uint reservePrice, uint auctionDuration) onlyauctioneer() public {
        //RECORD
        auctioneer.StartBiddingDone();
        //USER CODE HERE
        highestPrice = reservePrice;
        biddingStopTime = auctionDuration + now;
    }
}
```

```

//CHECK
assert(highestPrice == reservePrice && biddingStopTime == auctionDuration + now);
}

function Bid() public payable {
    if(! bidders.contains(msg.sender))
        bidders.add(msg.sender);
    //REQUIRE
    require(now > auctioneer.StartBiddingTime() && now < biddingStopTime);
    require(msg.value > highestPrice);
    uint this_bidder_Ori_amount = bidders.getamount(msg.sender);
    //USER CODE HERE
    highestPrice = msg.value;
    highestBidder = msg.sender;
    bidders.setamount(msg.sender, bidders.getamount(msg.sender) + msg.value);
    //CHECK
    assert(highestPrice == msg.value && highestBidder == msg.sender &&
        bidders.getamount(msg.sender) == this_bidder_Ori_amount + msg.value);
}

function WithdrawOverbidMoney() onlybidders() public payable {
    //REQUIRE
    if(msg.sender != highestBidder && bidders.getamount(msg.sender) > 0){
        //USER CODE HERE
        msg.sender.transfer(bidders.getamount(msg.sender));
        bidders.setamount(msg.sender, 0);
        //CHECK
        assert(bidders.getamount(msg.sender) == 0);
    }
    //REQUIRE
    else if(msg.sender == highestBidder && bidders.getamount(msg.sender) > highestPrice) {
        //USER CODE HERE
        msg.sender.transfer(bidders.getamount(msg.sender) - highestPrice);
        bidders.setamount(msg.sender, highestPrice);
        //CHECK
        assert(bidders.getamount(msg.sender) == highestPrice);
    }
    else{
        revert();
    }
}

function CollectPayment() onlyauctioneer() public payable {
    //REQUIRE
    require(now > biddingStopTime && now < auctioneer.CollectPaymentTime());
    //RECORD
    auctioneer.CollectPaymentDone();
    //USER CODE HERE
    msg.sender.transfer(highestPrice);
}
}

```

附 录 B

(资料性)

智能法律合约签订流程

智能法律合约签订流程可包括智能法律合约到生成、部署、签名和存证等处理。在智能法律合约经当事人协商撰写完成后,通过翻译器转化为可执行的计算机程序,进而部署到智能合约平台中并由当事人签名确认。签订后的智能合约可随时被查阅与审查。

智能法律合约存储形式既包含智能法律合约、演化形态、用户定义信息,也包含智能法律合约自身的基本属性与状态信息,如合约地址 Address、签名信息 Sign、时间戳 Time 等。

图 2 中智能合约签订编程具体描述如下:

- a) 使用本文件语言编写智能法律合约 A 时,A 中所有缺省属性值为空;
- b) 由 A 生成可执行区块链智能合约 B 时,如需人工操作,操作者应进行签名;
- c) 在部署 B 时,生成 Address 作为 B 的唯一编号;部署成功后,当事人,如 PartyI,加入 Time (PartyI)记录签名时间,并对 A 和 B 进行签名得到 Sign(PartyI);
- d) 当事人完成签名后,任何时间可通过调取查用将合约属性填充回智能合约 A,生成可浏览的合约内容。

参 考 文 献

- [1] GB/T 35285—2017 信息安全技术 公钥基础设施 基于数字证书的可靠电子签名生成及验证技术要求
 - [2] YD/T 3204—2016 网络电子身份标识 eID 体系架构
 - [3] 中华人民共和国民法典
 - [4] 中华人民共和国电子签名法
-

中国电子学会 (内部)