

中华人民共和国金融行业标准

JR/T 0066.1—2019

代替 JR/T 0066—2011

---

银行间市场业务数据交换协议  
第 1 部分：语法、结构与会话层

Interbank market information exchange protocol—  
Part 1: Syntax, structure and session layer

2019 - 01 - 08 发布

2019 - 01 - 08 实施

---

中国人民银行 发布



## 目 次

前言 .....	II
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 报文语法与结构 .....	2
5 会话传输 .....	14
6 会话管理 .....	15
7 会话类报文与组件 .....	24
附录 A（规范性附录） 域字典 .....	32
参考文献 .....	37

## 前 言

JR/T 0066《银行间市场业务数据交换协议》分成3部分：

- 第1部分：语法、结构与会话层；
- 第2部分：应用层；
- 第3部分：适流表示层。

本部分为JR/T 0066的第1部分。

本部分依据GB/T 1.1—2009给出的规则起草。

本部分代替JR/T 0066—2011《银行间市场业务数据交换协议》的协议语法结构、会话机制和会话层消息相关内容，未被代替的内容纳入JR/T 0066的第2部分。本部分与JR/T 0066—2011的替代部分相比，除编辑性修改外主要技术变化如下：

- 增加了规范性引用文件（见章节2）；
- 修改和新增了部分术语和定义（见章节3，2011版的章节2）；
- 修改了报文语法与结构的内容（见章节4，2011版的第4章节和5.1、5.2、5.3）；
- 修改了会话传输的内容（见章节5，2011版的章节3.1、3.2、3.3、3.4、3.5、3.6和3.7）；
- 修改了会话管理的内容（见章节6，2011版的3.8和3.9）；
- 修改了会话类报文与组件的内容（见章节7，2011版的5.4）；
- 增加了区块链扩展应用以适应国际技术发展（见4.7和7.2.2）。

本部分由中国外汇交易中心暨全国银行间同业拆借中心提出。

本部分由全国金融标准化技术委员会（SAC/TC 180）归口。

本部分负责起草单位：中国外汇交易中心暨全国银行间同业拆借中心。

本部分参与起草单位：中国人民银行科技司。

本部分主要起草人：许再越、姚前、杨富玉、朱荣、叶胜国、姜才康、王成勇、胡剑、李正、陈彬、胡卫平、沈峻、崔崑、郦永达、余波、曲维民、孙小林、沈薇薇、茅廷、杨帆、夏志江、孙英昊、包晓晶、赵俊锋、卢艳民、崔奇、邓钢铁、严璐祎、沈叶。

JR/T 0066于2011年6月2日首次发布，本次为第一次修订。

# 银行间市场业务数据交换协议

## 第1部分：语法、结构与会话层

### 1 范围

JR/T 0066的本部分规定了银行间市场参与方之间进行银行间交易所需的会话层通讯协议（Interbank Market Information Exchange Protocol Transport，简称IMIXT），包括报文语法与结构、会话可靠传输规范、会话管理规范、会话类报文与组件等。

本部分适用于银行间市场参与方之间的基础会话通讯数据交换。本部分应用于银行间市场机构间的业务数据交换协议（Interbank Market Information Exchange Protocol，简称IMIX）报文传输交互，银行间市场机构包括且不限于中介服务机构、会员机构、使用本部分的其他机构等。

### 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 2659 世界各国和地区名称代码

GB/T 12406 表示货币和资金的代码

JR/T 0066.2—2019 银行间市场业务数据交换协议 第2部分：应用层

### 3 术语和定义

下列术语和定义适用于本文件。

#### 3.1

**域界定符** field separator

报文中所有的域都有一个分隔符来界定分隔。

注：分隔符为ASCII码0x01，JR/T 0066中域界定符以<SOH>表示。

#### 3.2

**重复组** repeating group

由重复次数和若干组同类数据组成的域集合。

#### 3.3

**组件** component

会话报文和应用报文中，按照一定业务逻辑组成的域集合。

#### 3.4

**报文序号** message sequence number

报文传输过程中，用于监测报文传输连续性的数值。

注：通过该数值判断交换数据是否丢失。

### 3.5

**心跳 heart beat**

报文发起方和接收方在报文交换空闲期，通过产生规律性心跳报文保持通讯连接的场景。

### 3.6

**重复发送 possible duplicate**

因响应一个重发请求或者不确定对方是否收到已发报文，导致重复发送报文的场景。

注：该场景下的报文应设置“可能重复标志”（PossDupFlag=Y）。

### 3.7

**重新发送 possible resend**

因发送方或接收方应用需要，由报文发送方重新生成报文并发送的场景。

注：该场景下的报文应设置“可能重发标志”（PossResend=Y）。

### 3.8

**序号重设 sequence reset**

发送方用于设置预期报文序号的报文。序号重设报文有两种模式：序号重设-缺口填补（SeqReset-Gap Fill）、序号重设-重置（SeqReset-Reset）。

注：序号重设-重置（SeqReset-Reset）仅在灾难恢复情况下使用。

### 3.9

**有效IMIX报文 valid IMIX message**

按照IMIX协议正确生成的报文。

### 3.10

**发起方 initiator**

登录报文的发送方。

### 3.11

**接收方 acceptor**

登录报文的接收方。

### 3.12

**区块链 blockchain**

一种在对等网络环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理事务处理的模式。

## 4 报文语法与结构

### 4.1 数据类型

#### 4.1.1 说明

数据类型用于定义数据域的取值类型，JR/T 0066使用的数据类型由几个基本的数据类型（整数、浮点数、字符、字符串、数据）和在此基础上扩展的数据类型组成。除“数据”数据类型外，其他数据类型均以ASCII码字符串表示。

#### 4.1.2 整数 int

无逗号和小数位的数值，可表示正负（ASCII码字符“-”，“0”至“9”组成）。符号占据一个字符位置。前置字符可置零（例如“00023”=“23”）。

整数类型的扩展定义：

- a) 长度 Length：以整数表示字节为单位的数据长度，正数；
- b) 重复数 NumInGroup：以整数表示重复组的个数，正数；
- c) 报文序号 SeqNum：以整数表示报文序号，正数；
- d) 域号 TagNum：以整数表示的域号（或称 Tag），正数，首位不能为零；
- e) 月日期号 DayOfMonth：以整数表示的月份中第几天，取值 1 至 31。

#### 4.1.3 浮点数 float

含有可选的小数部分，可表示正负（ASCII码字符“-”，“0”至“9”和“.”组成）。前置字符可置零（例如“0023”=“23”），小数部分后置字符可置零（例如“23.0”=“23.0000”=“23”）。

浮点数类型的扩展定义：

- a) 量 Qty：股份数量、资产数量等，可有小数部分；
- b) 价格 Price：小数位数可变；
- c) 价格偏移量 PriceOffset：代表价格偏移量的浮点域；
- d) 金额 Amt：典型的价格与数量相乘结果，如成交金额；
- e) 百分比 Percentage：小数表示方法，例如.05代表5%。

#### 4.1.4 字符 char

除界定符外所有字母字符和标点字符，区分字母大小写。

字符类型的扩展定义是布尔 Boolean：该域取值有两个字符（“Y”=True/Yes，“N”=False/No）。

#### 4.1.5 字符串 String

除界定符外由数字、字母、符号组成的一串字符，区分字母大小写。

字符串类型的扩展定义：

- a) 多元值字符串 MultipleValueString：用空格分隔（例如 10243=D2 M3 Y3）；
- b) 国家 Country：取值范围见 GB/T 2659（例如 470=CHN）；
- c) 字符串货币类型 Currency：取值范围见 GB/T 12406（例如 15=CNY）；
- d) 交易所或市场编号 Exchange：字符串（例如 1301=2）；
- e) 年月 Month-year：格式 YYYYMM，YYYY=0000-9999，MM=01-12（例如 200=201710）；
- f) 国际标准时时间戳 UTCTimestamp：格式 YYYYMMDD-HH:MM:SS（秒）或 YYYYMMDD-HH:MM:SS.sss（毫秒），YYYY=0000-9999，MM=01-12，DD=01-31，HH=00-23，MM=00-59，SS=00-59（秒），sss=000-999（毫秒）（例如 60=20171012-11:40:00 或 20171012-11:40:00.123）；
- g) 国际标准时时间 UTCTimeOnly：格式 HH:MM:SS 或 HH:MM:SS.sss，HH=00-23，MM=00-59，SS=00-59（秒），sss=000-999（毫秒）（例如 10318=11:40:00 或 11:40:00.123）；

- h) 本地市场日期 LocalMktDate: 格式 YYYYMMDD, YYYY=0000-9999, MM=01-12, DD=01-31 (例如 916=20171012);
- i) 国际标准时日期 UTCDate: 格式 YYYYMMDD, YYYY=0000-9999, MM=01-12, DD=01-31 (例如 75=20171012)。

#### 4.1.6 数据 Data

无格式和内容限制的原始数据,包含长度域和数据域两个部分,数据域数据可包含域界定符(SOH)、特殊符号等,长度域指明数据域的字节数(注意:该字节数的计算不计域界定符(SOH))。

示例: 1401 为长度域, 1402 为数据域。

数据样例: 1401=5 1402=XX<SOH>=X

### 4.2 域

#### 4.2.1 域的定义

域是基本的数据元素。传输过程中,域由域号、等号、域值组成,即域号=域值。域字典部分详细定义了本部分所涉及到的所有域的数据类型和取值范围,见附录A。

#### 4.2.2 域的使用

在报文中,域的使用有三种方式:必需的、非必需的、条件限制选择(即根据其他相关域的存在与否或取值来决定)。

条件限制选择域的示例见表1。当628、629、630存在取值时,则627应有值;当628、629、630不存在取值时,则627也可为空。627即为条件限制选择域。

表1 条件限制选择域的示例

域号/嵌套组件名	域名	必需域
627	NoHops	
--> 628	HopCompID	Y
--> 629	HopSendingTime	
--> 630	HopRefID	

#### 4.2.3 自定义域

如JR/T 0066中定义的域无法满足使用,可扩展定义新的域,即自定义域。

JR/T 0066使用者之间可自行约定自定义域,自定义域的域号不应与JR/T 0066中定义的域号重复,且应大于10000。

#### 4.2.4 域界定

报文中所有的域(包含data类型数据域)都有一个分隔符来界定分隔,该分隔符就是ASCII码0x01(以<SOH>表示)。

任何报文应由多个“域号=值”的基本结构组成,用域界定符<SOH>分隔。报文组成结构见图1。



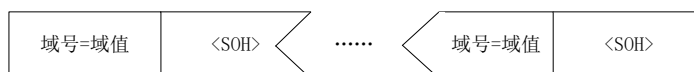


图1 报文组成结构

### 4.3 IMIX 报文组成规则

报文由报文头、报文体和报文尾组成。每个组成部分都由一系列“域号=值”组成，应遵循以下规则：

- 开始部分应是报文头，随后是报文体，最后是报文尾；
- 报文头的前3个域的次序不应改变：起始串(Tag#8)、报文体长度(Tag#9)、报文类型(Tag#35)；
- 报文尾的最后一个域应是校验和域(Tag#10)；
- 重复组中，域出现的顺序应遵循该重复组在报文或组件中定义时的次序；
- 除重复组域外，任一域号在一条报文内只能出现一次，否则视为错误。

报文格式示例见图2。

```

8=IMIX1.0<SOH>9=xxx<SOH>35=8<SOH>49=CFETS<SOH>56=29000881100000000000<SOH>57=MHBJ.D
EALER@MHBJ<SOH>34=13<SOH>52=20070913-10:20:59<SOH>347=UTF-8<SOH>11=MHBJ_ORDER_002<SOH
>15=AUD<SOH>17=5.1.3293<SOH>31=0.771<SOH>32=50000<SOH>54=1<SOH>60=20061122-10:21:34<S
OH>63=0<SOH>64=20061124<SOH>75=20061122<SOH>120=AUD<SOH>150=F<SOH>194=0.771<SOH>1056=
38550<SOH>10176=12<SOH>10038=22<SOH>10042=MT<SOH>10317=5<SOH>10315=2<SOH>10296=200611
24<SOH>1028438547.5<SOH>22=5<SOH>48=AUDUSD=CFHA<SOH>55=AUD.USD<SOH>453=2<SOH>448=1190
0004301000000000<SOH>452=I14<SOH>802=3<SOH>523=CCCB.DEALER@CCCB<SOH>803=101<SOH>523=
CCCB<SOH>803=102<SOH>523=ChangshaCityCommercialBank<SOH>803=5<SOH>448=290008811000000
000000<SOH>452=I13<SOH>802=3<SOH>523=MHBJ.DEALER@MHBJ<SOH>803=101<SOH>523=MHBJ<SOH>80
3=102<SOH>523=Mizuho Corporate Bank Beijing<SOH>803=5<SOH>10=XXX<SOH>

```

图2 报文格式示例

### 4.4 重复组

重复组是由重复次数和若干组同类数据组成的域集合。

重复组内，同类数据域集合的第一个域是必需的。如果域名起始为“No”字符、用于指明重复次数的域的域值大于0，则该域后所列的第一个域为必需域。

重复组示例见表1。628为必需域，根据628判断新的628、629、630组成的域集合的开始。

JR/T 0066通过缩进的符号“-->”对报文定义内的重复组进行标注。重复组可嵌入其他重复组。JR/T 0066通过重复组结构中增加被嵌套的重复组名称，对被嵌套的重复组进行标注。

### 4.5 安全与加密

由于报文可能在公共网络或不安全的网络上传输交换，因此对相关的敏感数据宜进行加密处理。具体加密的方法由连接双方达成的协议而定，同时加密方法应符合国家密码管理机构的规定。报文内除某些需要公开识别的域以明文传输外，其他任何域都可加密放置在密文数据域(SecureData)内。这些被

加密的域也可同时保留明文的表示方式。如果报文的重复组内有部分数据需要加密，则应对整个重复组加密。本部分还提供一些域用以支持数字签名、密钥交换和正文加密等安全技术。

加密方案有三种：

- a) 将安全敏感的域加密后移至 SecureData 域；
- b) 将所有可加密的域加密后移至 SecureData 域；
- c) 将所有可加密的域加密后移至 SecureData 域，同时这些域以明文在报文中重复出现。

#### 4.6 数据完整性

数据的完整性通过两个方法保证：报文体长度以及校验和的验证。

报文体长度以BodyLength域来表示，其值是计算出的报文长度域后面的字符数，包含紧靠校验和域“10=”之前的域界定符<SOH>。校验和是把每个字符的二进制值从报文开头“8=”中的“8”开始相加，一直加到紧靠在校验和域“10=”之前的域界定符，然后取按256取模得到的结果。校验和域位于报文的最末，校验和的计算是在加密之后进行的。为便于传输，校验和应按可打印字符进行发送，所以应转换为以ASCII码编码的3个值。

示例：如果校验和计算出来是 274，则按 256 取模就得到 18，即  $(256+18) \bmod 256=18$ 。这个值将会以|10=018|传输，其中“10=”是校验和域的标志。

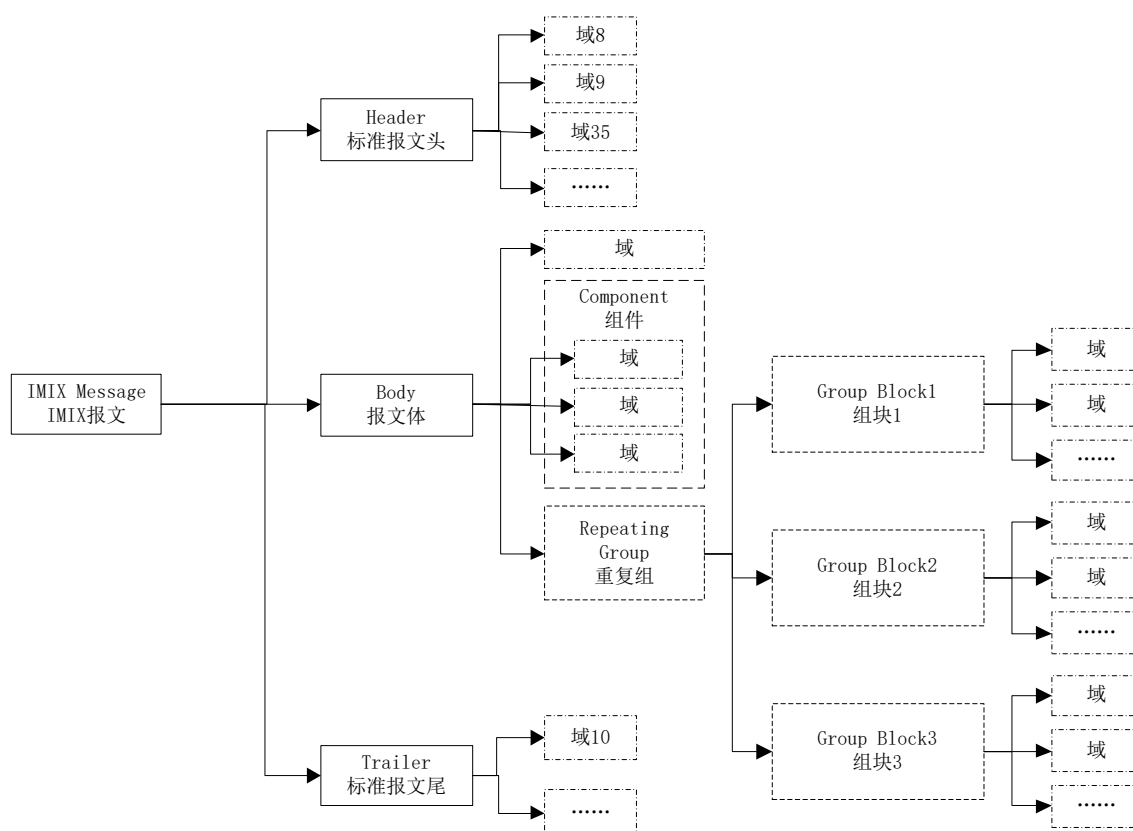
产生校验和域的一个示范代码片段见图3。

```
char *GenerateChecksum(char *buf, long bufLen)
{
    static char tmpBuf[4];
    long idx;
    unsigned int cks;
    for( idx = 0L, cks = 0; idx < bufLen; cks += (unsigned int)buf[ idx++ ] );
    sprintf( tmpBuf, "%03d", (unsigned int)( cks % 256 ) );
    return( tmpBuf );
};
```

图3 校验和域示范代码片段

#### 4.7 IMIX 报文结构

对于每一条IMIX报文，它的报文结构分解见图4。



说明:

- 域 ——表示某个域;
- 重复组 ——表示重复组, 可由多个重复组块组成;
- 组块 ——表示重复组中每块重复部分, 也是由域块组成;
- 组件 ——表示多个域的集合, 这些域所代表的含义之间具有关联性。

图4 IMIX 报文结构

面向区块链技术运作的数据整体结构见图5。

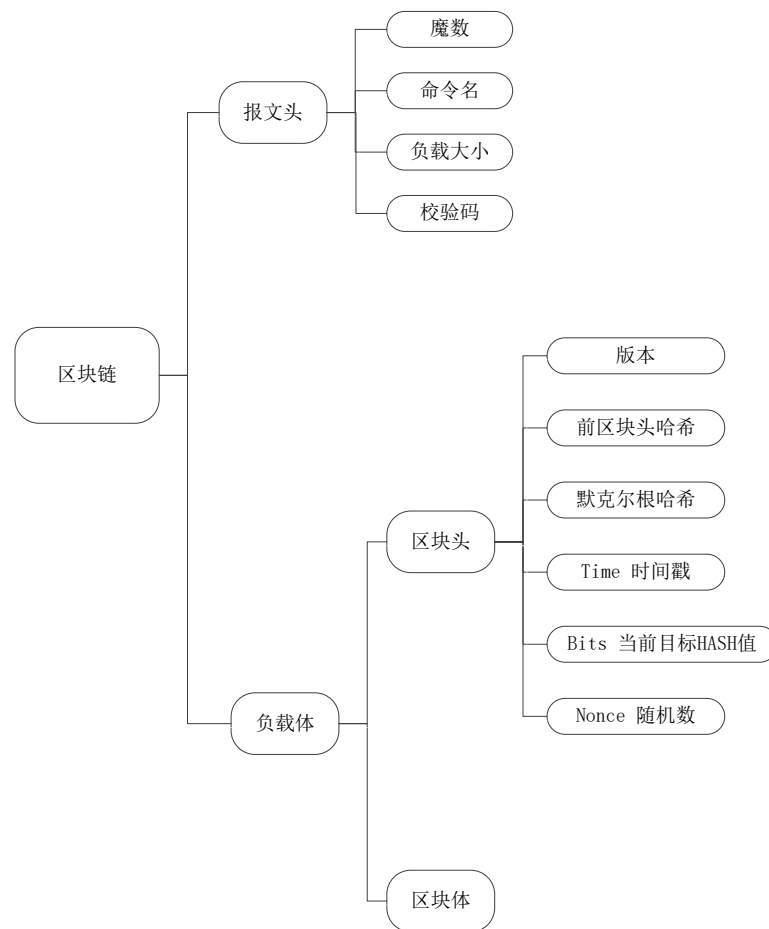
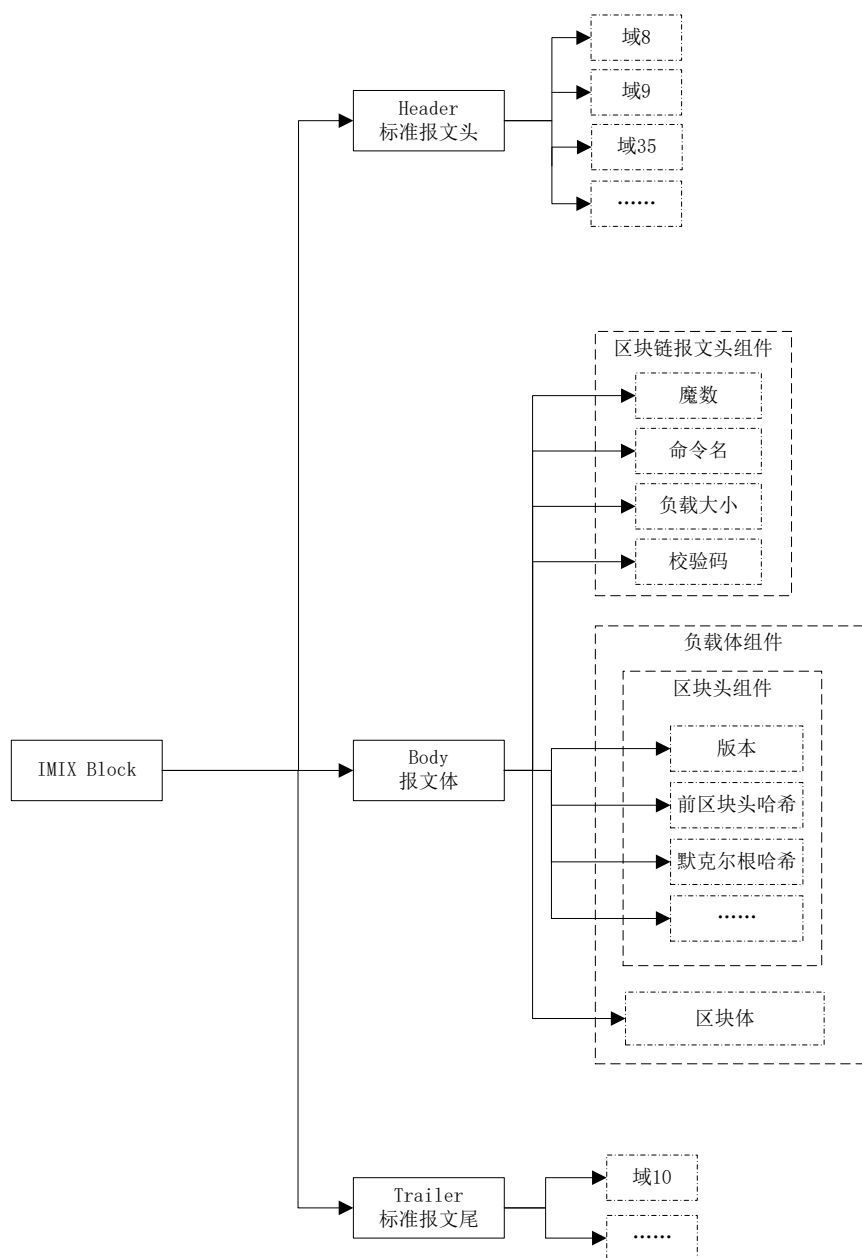


图5 区块链整体结构

区块链整体结构包括报文头和负载体。不同的负载体类型可满足各类场景传输的需求，如获取区块、获取数据、交易单等。图5为传输区块头和交易单的区块链时的区块链整体结构。当负载体无数据定义时，可仅传输报文头。

根据区块链的数据结构定义，其数据类型和组织方式并未超出现有IMIX体系范畴。按照图4给出的IMIX报文结构，应用区块链技术的IMIX报文结构见图6。



说明:

域 ——表示某个域;

组件 ——表示多个域的集合, 这些域所代表的含义之间具有关联性。

图6 应用区块链技术的 IMIX 报文结构

图6为传输区块头和交易单区块时的IMIX报文结构。根据具体场景应用需求, 可使用不同负载体类型的组件。

IMIX协议中, 固定分配20000—21000域号段用于区块链数据内容的表达。

#### 4.8 标准报文头

## 4.8.1 概述

每个会话报文或应用报文都有一个报文头，该报文头指明报文类型、报文体长度、发送目的地、报文序号、发送起始点和发送时间。

## 4.8.2 标准报文头格式

标准报文头见表2。

表2 标准报文头

域号/嵌套组件名	域名	必需域	备注
8	BeginString	Y	起始串定义报文的协议版本（不应加密，报文的第一个域）。
9	BodyLength	Y	报文体长度（不应加密，应是报文的第二个域）。
34	MsgSeqNum	Y	报文序号（可加密）。
35	MsgType	Y	报文类型（不应加密，应是报文的第三个域）。
43	PossDupFlag		可能重复标志，重复发送时，作此标记（可加密）。
49	SenderCompID	Y	发送方标识符（不应加密）。
50	SenderSubID		发送方子标识符（可加密）。
52	SendingTime	Y	发送时间（可加密）。
56	TargetCompID	Y	接收方标识符（不应加密）。
57	TargetSubID		接收方子标识符（可加密）。
90	SecureDataLen		用于标识报文加密部分的长度时必需（不应加密）。
91	SecureData		报文体加密时必需。紧跟在 SercureDataLen 域之后。
97	PossResend		可能重发标志（可加密）。
115	OnBehalfOfCompID		最初发送方标识符（可加密），用于经第三方发送。
116	OnBehalfOfSubID		最初发送方子标识符（可加密）。
122	OrigSendingTime		原始发送时间（可加密）。
128	DeliverToCompID		最终接收方标识符（可加密），用于经第三方发送。
129	DeliverToSubID		最终接收方子标识符（可加密）。
142	SenderLocationID		发送方的 LocationID（如：地理位置和（或）席位（desk））（可加密）。
143	TargetLocationID		接收方 LocationID（如：地理位置和（或）席位（desk））（可加密）。
145	DeliverToLocationID		最终接收方的 LocationID（如：地理位置和（或）席位（desk））（可加密）。
212	XmlDataLen		当标识 XmlData 报文体长度时必需（可加密）。
213	XmlData		包含 XML 格式的报文块（如 IMIXML）；总紧跟在 XmlDataLen（可加密）之后。
347	MessageEncoding		在报文的“Encode”域中使用的报文编码格式（非 ASCII 编码），使用编码域时必需。
369	LastMsgSeqNumProcessed		最后处理报文序号（可加密）。
1128	ApplVerID		使用 SP 标识方法标明应用版本，ApplVerID 用于一个特定报文的场景。

域号/嵌套组件名	域名	必需域	备注
1129	CstmApplVerID		用于支持客户共同协商认可的功能。
1156	AppIExtID		
组件<HopGrp>			为历史跳跃信息重复组，记录报文经第三方发送的历史。每次经第三方发送为一个跳跃，仅当 OnBehalfOfCompID 使用时有效，主要用于跟踪报文的的路径。注意：一些市场条例或者对手方可能要求追踪 hops 报文。

### 4.8.3 标准报文头在报文传输的应用

#### 4.8.3.1 点对点传输

表3和表4展示了在两个市场参与方之间的单个点对点IMIX会话中如何使用SenderCompID、TargetCompID、SenderSubID、TargetSubID域。SenderSubID为SenderCompID的子机构，TargetSubID为TargetCompID的子机构。

两个主机机构之间的单个点对点IMIX会话传输示例见表3。假设A为卖方主机机构，B为买方主机机构。

表3 点对点传输示例表（主机机构之间）

	SenderSubID	SenderCompID	TargetCompID	TargetSubID
A 到 B		A	B	
B 到 A		B	A	

两个子机构之间的单个点对点IMIX会话传输示例见表4。假设A1为卖方子机构，A为卖方主机机构，B1为买方子机构，B为买方主机机构。

表4 点对点传输示例表（子机构之间）

	SenderSubID	SenderCompID	TargetCompID	TargetSubID
A1 到 B1	A1	A	B	B1
B1 到 A1	B1	B	A	A1

#### 4.8.3.2 报文转发

由于两端之间的报文通过第三方进行转发，第三方可与其他第三方连接，在报文发起方和最终的接收方间形成多点的链条。SenderCompID、SenderSubID、TargetCompID、TargetSubID、DeliverToCompID、DeliverToSubID、OnBehalfOfCompID和OnBehalfOfSubID域用于报文路由。这些域的使用方法见表5，其中A为卖方，B和C为买方，Q为第三方。

表5 报文转发示例表

	SenderCompID	OnBehalfOf CompID	TargetCompID	DeliverTo CompID	HopCompID	HopSendingTime
从 A 通过 Q 到 B						
1	A 到 Q	A	Q	B		
2	Q 到 B	Q	B		Q	A 的发送时间
B 通过 Q 响应 A						

	SenderCompID	OnBehalfOfCompID	TargetCompID	DeliverToCompID	HopCompID	HopSendingTime
1	B 到 Q	B		Q	A	
2	Q 到 A	Q	B	A		Q 的发送时间
A 通过 Q 发送到 B 和 C						
1	A 到 Q	A		Q	B	
2	Q 到 B	Q	A	B		Q 的发送时间
3	A 到 Q	A		Q	C	
4	Q 到 C	Q	A	C		Q 的发送时间
B 和 C 通过 Q 发送到 A						
1	B 到 Q	B		Q	A	
2	Q 到 A	Q	B	A		Q 的发送时间
3	C 到 Q	C		Q	A	
4	Q 到 A	Q	C	A		Q 的发送时间
<p>注：由于在一个给定的IMIX会话中，一些域（如在一个新Order指令中的C10rdID）应是唯一的。因此，当使用OnBehalfOfCompID域（或DeliverToCompID域）进行寻址时，应在OnBehalfOfCompID域（或DeliverToCompID域）之后加上原值。这样，如果A发送报文到Q的C10rdID为“123”，则Q将“A-123”作为C10rdID的值发送到C，以确保唯一性。</p>						

报文转发场景示例见表6。

表6 报文转发场景示例

示例	条件/触发条件	预期行为
支持第三方机构编码	收到报文中，OnBehalfOfCompID 和 DeliverToCompID 域值与会话配置中的 OnBehalfOfCompID 和 DeliverToCompID 域值相同。	接收报文。
支持第三方机构编码	收到报文中，OnBehalfOfCompID 或 DeliverToCompID 域值与会话配置中的 OnBehalfOfCompID 和 DeliverToCompID 域值不同。	发送拒绝报文，描述无效的 OnBehalfOfCompID 或 DeliverToCompID 域值（sessionRejectReason= “CompID problem”）。

#### 4.8.4 接收标准报文头场景示例

接收标准报文头场景见表7。

表7 接收标准报文头场景示例

示例	条件/触发条件	预期行为
接收标准报文头	接收预期的 MsgSeqNum 域值。	接收报文的 MsgSeqNum 域值。
	MsgSeqNum 域值比预期高。	发起重发请求报文。
	MsgSeqNum 域值比预期低并且 PossDupFlag 域没有设置为 Y。 例外：SeqReset 被重置。	a) 发送序号重设-重置报文，将对端下一个预期的报文序号重置成1； b) 本方将下一个预期接收报文序号重置成



示例	条件/触发条件	预期行为
		1。
	接收到异常的报文 <sup>a</sup> 。	发送拒绝报文。
	PossDupFlag 设置为 Y, OrigSendingTime 少于或等于 SendingTime, 并且 MsgSeqNum 域值低于预期。 注意: OrigSendingTime 应早于 SendingTime。	接收并处理该报文。
	PossDupFlag 设置为 Y, OrigSendingTime 大于 SendingTime, 并且 MsgSeqNum 与预期相同。 注意: OrigSendingTime 应早于 SendingTime 除非该报文在同一秒被重新发送。	a) 发送拒绝报文, 描述错误的 SendingTime (SessionRejectReason=“SendingTime accuracy problem”); b) 发出登出报文, 等待登出报文响应, 接收到登出报文响应后断开连接。
	PossDupFlag 设置为 Y 且 OrigSendingTime 值未被指定。 注意: 响应重发请求报文时, 由于报文的最初发送时间不是当前 SendingTime 值, 因此应发送 OrigSendingTime, 并且设置 PossDupFlag=“Y”。	发送拒绝报文, 描述错误的 OrigSendingTime (SessionRejectReason=“Required tag missing”)。
	接收 BeginString 的值与会话指定值匹配。	接收报文的 BeginString 域值。
	接收到的 BeginString 的值与会话指定值不匹配。	a) 忽略该报文; b) 设置下一个报文序号自增1; c) 断开连接。
	接收 SenderCompID 和 TargetCompID 的值与会话指定值匹配。	接收报文的 SenderCompID 和 TargetCompID 域值。
	接收到的 SenderCompID 和 TargetCompID 值与会话指定值不匹配。	a) 忽略该报文; b) 断开连接。
	接收到正确的 BodyLength 值。	接收报文中的 BodyLength 域。
	接收到错误的 BodyLength 值。	重新计算 BodyLength 值, 并赋值。
	接收的 SendingTime 的值符合规定时间 <sup>b</sup> 。	接收报文的 SendingTime 域。
	接收的 SendingTime 的值不符合规定时间。	a) 发送拒绝报文, 描述不准确的 SendingTime (SessionRejectReason=“SendingTime accuracy problem”); b) 发送附有错误 SenderCompID 或 SendingTime 值的登出报文; c) (非必需) 等待登出报文响应 (注意: 可能传来有错误的 SendingTime 值)。
	接收到有效的 MsgType 的值 (数据字典定义)。	接收报文的 MsgType 域。
	接收到无效的 MsgType 的值 (数据字典未定义)。	a) 忽略该报文; b) 设置下一个报文序号自增1。
	BeginString、BodyLength 和 MsgType 是报文的前三个域。	接收报文。
	BeginString、BodyLength 和 MsgType 不是报	a) 考虑报文存在异常, 忽略该报文;

示例	条件/触发条件	预期行为
	文的前三个域。	b) 设置下一个报文序号自增1。
<p><sup>a</sup> 异常报文是指下述情况：</p> <p>a) BeginString (tag#8) 非报文中的第一个域，或不符合 8=IMIX*.n.m. 的格式；</p> <p>b) BodyLength (tag#9) 非报文中的第二个域，或字节数不正确；</p> <p>c) MessageType (tag#35) 非报文中的第三个域；</p> <p>d) Checksum (tag#10) 非最后一个域，或其值非有效值。</p> <p><sup>b</sup> 规定时间指的是两边的系统时间一致并且 SendingTime 应为当前时间。</p>		

## 4.9 标准报文尾

### 4.9.1 概述

每一个会话报文或应用报文都有一个报文尾，并以此终止。报文尾可用于分隔多个报文，包含有3位数的校验和值。

### 4.9.2 标准报文尾格式

标准报文尾格式见表8。

表8 标准报文尾

域号/嵌套组件名	域名	必需域	备注
89	Signature		数字签名（不可加密）。
93	SignatureLength		数字签名长度（不可加密）。
10	Checksum	Y	校验和，报文的最末域（不可加密）。

### 4.9.3 标准报文尾场景示例

接收标准报文尾场景示例见表9。

表9 接收标准报文尾场景示例

示例	条件/触发条件	预期行为
接收标准报文尾	有效的 CheckSum 域值。	接收报文。
	无效的 CheckSum 域值。	a) 考虑报文存在异常，忽略该报文； b) 设置下一个报文序号自增1。
	异常的报文。	a) 考虑报文存在异常，忽略该报文； b) 发送拒绝报文，其中Text域描述错误情况。
	Checksum 在报文的末尾域，域值的长度是 3 且以<SOH>为结尾。	接收报文。
	Checksum 不在报文的末尾域，或域值的长度不是 3，或不以<SOH>为结尾。	a) 考虑报文存在异常，忽略该报文； b) 设置下一个报文序号自增1。

## 5 会话传输

## 5.1 会话机制

IMIX会话由一个或多个IMIX连接(IMIX Connection)组成。IMIX连接由三部分组成:登录(logon)、报文传输(message exchange)和登出(logout)。一个IMIX会话可多次登录。

## 5.2 报文序号

任何一条报文都被分配一个唯一的报文序号来加以标识。报文序号在每次会话过程中从1开始,在整个会话过程中连续递增,直到该会话过程全部结束。

## 5.3 心跳

在报文交换的空闲期间,连接双方将在规定的时间间隔内发出心跳报文。通过心跳报文可监测通讯连接的状态。

## 5.4 报文丢失

报文接收方应监测报文是否丢失并加以处理。

## 5.5 报文重复发送

报文发送方响应一个重发请求而重复发送报文时应在被重发报文内加上可能重复标志(PossDupFlag=Y),应重新计算校验和。报文接收方检查该报文,如果曾经接收过,则忽略报文;如果未曾收到过,则按正常步骤处理。

## 5.6 报文重新发送

报文发送方应设置可能重发标志(PossResend=Y),设置新的报文序号,重新计算校验和,重新发送报文。报文接收方收到该类报文后,应通过查询报文内的域(如订单编号等)来确定此前是否收到过该报文。

## 5.7 报文确认

报文接收方通过监测报文序号缺口来识别正常传送过程中的错误,IMIX应用层报文确认处理见JR/T 0066.2—2019。

# 6 会话管理

## 6.1 概述

连接双方各自维护一组连续的报文序号实现会话维持。会话过程分为三个部分:登录、报文交换、登出。

## 6.2 报文分类管理

报文分成会话层报文和应用层报文,根据附录A域字典中的域号35区分报文类型。

## 6.3 会话流程

### 6.3.1 数据交互时序图

会话流程数据交互时序图见图7。

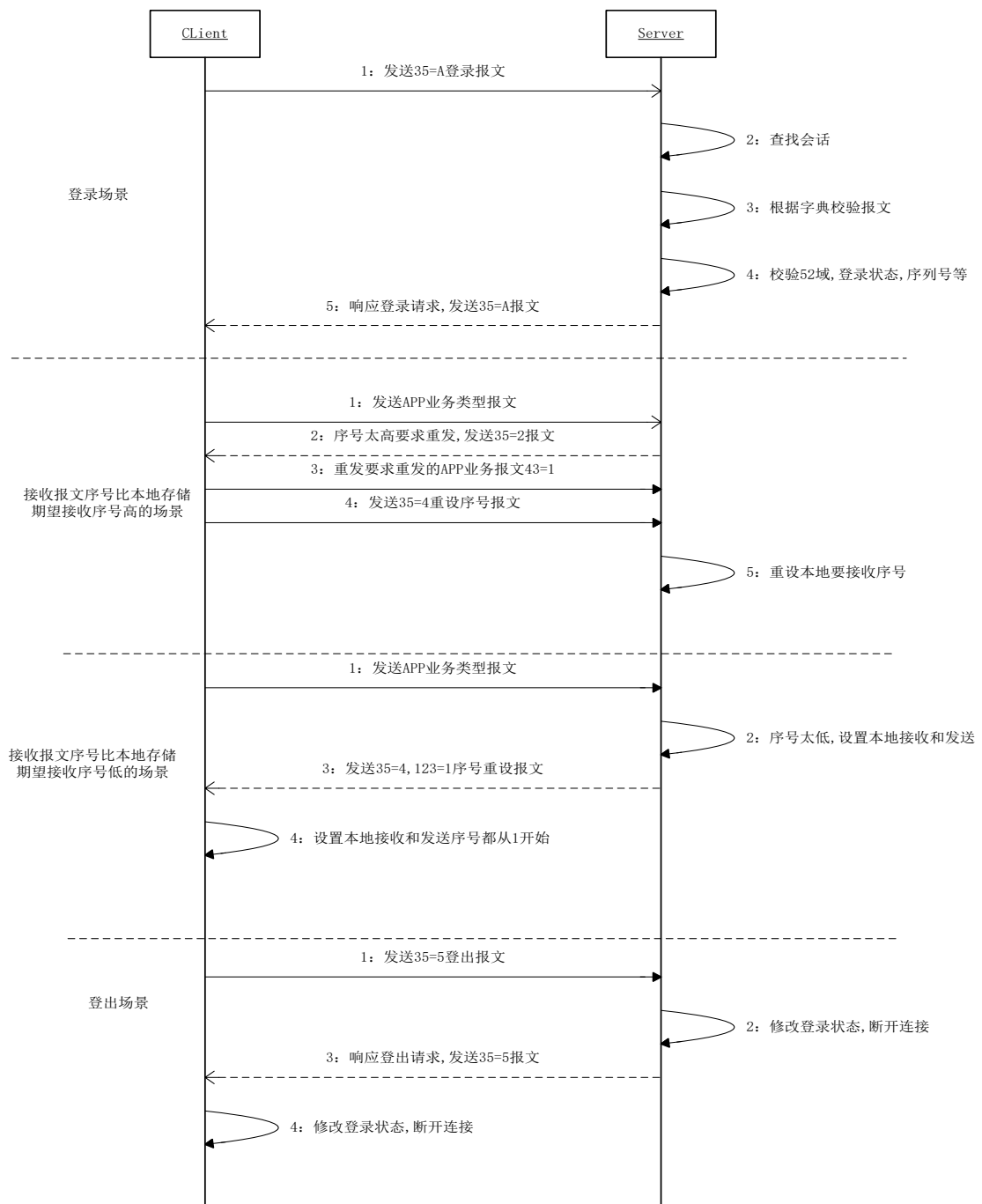


图7 数据交互时序图

## 6.3.2 会话流程状态

会话流程状态说明见表10。

表10 IMIX 会话流程状态

序号	状态	发起方	接收方	描述
1	断开-未登录	Y	Y	当前处于断开状态，当日未进行连接尝试，将不会占用 MsgSeqNum 报文序号（当日下一个连接的 MsgSeqNum 域值起始值为 1）。
2	监测到网络连接中断	Y	Y	尝试连接时，监测到网络连接中断（如 TCP socket 关闭）。断开网络连接并关闭该会话。
3	等待连接	N	Y	会话接收方等待对端连接。
4	发起连接	Y	N	会话发起方向对端建立连接。
5	网络连接建立	Y	Y	双方建立网络连接。
6	发送登录报文	Y	N	会话发起方登录并发送登录报文。
7	收到登录报文	N	Y	会话接收方登录并收到对端登录报文。
8	响应登录报文	N	Y	会话接收方使用登录报文与对端握手，响应对端登录报文。
9	处理重发请求报文	Y	Y	接收对端发送的重发请求报文，响应请求报文中要求重发的 MsgSeqNum 域值范围序号（请求报文的 BeginSeqNo 域到 EndSeqNo 域值）的报文。接收方根据请求报文范围，返回丢失报文。发送完毕后，向对手方发送序号重设-重置报文。
10	收到 MsgSeqNum 值过高	Y	Y	若收到报文序号比预期报文序号高，则向对方发送重发请求报文（请求报文的序号范围为预期报文序号至本次接收到的报文序号）。
11	收到 MsgSeqNum 值过低	Y	Y	若收到报文序号比预期报文序号高，则向对方发送序号重设-重置报文。
12	等待/处理重发请求响应	Y	Y	处理 MsgSeqNum 范围内的报文，设置 PossDupFlag=“Y”进行重发，并处理序号重设-缺口填补报文。
13	在时间间隔内未收到报文	Y	Y	在心跳超时周期内，非异常情况下未收到报文，应发送测试请求报文。
14	等待或处理对测试请求报文的响应	Y	Y	处理入队列报文。
15	接收登出报文	Y	Y	接收对端发送的登出报文。无论 MsgSeqNum 域值如何，都会在发送登出报文响应后，断开与对端的网络连接。
16	发出登出报文	Y	Y	识别正常断开或有原因的断开时，发送登出报文给对端，并等待合理时间间隔以接收登出报文响应。注意：某些登出原因（如，数据入库/存储失败），应在登出报文发送后，立即断开该会话的网络连接并关闭会话。
17	活跃/正常会话	Y	Y	网络连接建立后，双方成功交换登录报文后，符合预期地依次接收和发送 MsgSeqNum 域的报文序号，并且在心跳超时周期内能正常接收心跳报文或其他报文。
18	等待登录确认	Y	N	会话发起方等待会话接收方发送登录确认报文。

注：发起方和接收方的“Y”表示发起方或接收方参与当前会话流程，“N”表示不参与当前会话流程。

## 6.3.3 登录过程会话状态转换

登录过程中的会话状态转换见表11。

表11 IMIX 登录过程会话状态转换

会话发起方(如:买方)行为	会话接收方(如:卖方)行为	会话发起方(如:买方)状态	会话接收方(如:卖方)状态
开始。		初始状态:断开—未登录。	初始状态:等待连接。
连接。		发起连接; (可能)监测到网络连接中断。	等待连接。
	接收连接。	建立网络连接。	建立网络连接。
开始登录。		发送登录报文。	建立网络连接。
	收到登录报文。	发送登录报文。	接收登录报文。
	发送登录报文的响应。	发送登录报文。	登录报文的响应; (可能)发送序号重设报文 (如:如果MsgSeqNum过低); (可能)收到的MsgSeqNum域 值过高。
	(可能)发送重发请求 报文。		登录报文的响应; (可能)接收到的MsgSeqNum 域值过高。
接收登录报文的响应。		(可能)活跃/会话正常; (可能)发送序号重设报文 (如:MsgSeqNum域值过低)。	登录报文的响应。
(可能)发送重发请求 报文。		(可能)活跃/会话正常; (可能)收到的MsgSeqNum域 值过高。	(可能)活跃/会话正常; (可能)处理重发请求报文。
		活跃/会话正常。	活跃/会话正常。

## 6.3.4 登出过程会话状态转换

登出过程中的会话状态转换见表12。

表12 IMIX 登出过程会话状态转换

登出发起方行为	登出接收方行为	登出发起方状态	登出接收方状态
开始		初始状态: a) 活跃/会话正常; b) 在时间间隔内未收到报文; c) 等待/处理测试请求报文的响应。	初始状态: a) 活跃/会话正常; b) 在时间间隔内未收到报文; c) 发送初始登录报文; d) 等待/处理测试请求报文的响应; e) 等待登录生效; f) 收到的MsgSeqNum域值过高;

登出发起方行为	登出接收方行为	登出发起方状态	登出接收方状态
			g) 等待/处理重发请求报文的响应; h) 发起登出报文处理; i) 等待登录报文的反馈。
发送登出报文。		登出等待中。	
	接收登出报文。	登出等待中。	(可能) 收到的 MsgSeqNum 域值过高。
	发送登出报文的响应。	登出等待中。	等待断开连接。
	(可能) 发送重发请求报文。	登出等待中。	(可能) 等待/处理去响应重发请求。
(可能) 接收到重发请求报文。		(可能) 等待/处理去响应重发请求报文。	(可能) 等待响应重发请求报文。
接收登出报文的响应。		断开—未登录。	等待断开连接。
断开连接。		断开—未登录。	断开—未登录。

#### 6.4 登录

登录包含三个步骤:

- 建立TCP连接, 会话发起方与会话接收方建立TCP连接;
- 连接双方的确认/认证, 会话发起方发送35=A的登录报文请求认证, 会话接收方认证通过, 回复一个35=A的登录响应报文, 会话接收方认证不通过, 回复一个包含失败说明35=5的登出报文;
- 报文序号同步。

买方(会话发起方)登录及开始会话示例见表13。

表13 买方(会话发起方)登录及开始会话示例

示例	条件/触发条件	预期行为
连接并发送登录报文	建立网络连接。	与对手方成功建立 TCP socket 连接。
	发送登录报文。	发送登录报文。
	收到经过登录认证成功的登录响应报文。	可正常发送应用业务报文。
	收到经过登录认证失败的登录响应报文。	a) 发送拒绝报文, 其中Text域描述错误情况; b) 发出登出报文。
	登录前, 收到除登录报文以外的其他报文。	断开连接。

卖方(会话接收方)登录及开始会话示例见表14。

表14 卖方(会话接收方)登录及开始会话示例

示例	条件/触发条件	预期行为
接收登录报文	收到登录报文。	响应登录报文。
	收到相同信息的登录报	拒绝本次登录。

示例	条件/触发条件	预期行为
	文（即：BeginString, SenderCompID, TargetCompID 等连接已经存在的情况）。	
	接收到的登录报文, 经过认证失败。	发送登出报文。
	不符合 IMIX 协议的登录报文。	a) 发送拒绝报文, 其中Text域描述错误情况; b) 发送登出报文。
接收到登录报文以外的任何报文	收到的第一个报文非登录报文。	断开连接。

## 6.5 报文交换

完成初始化过程后, 开始正常的报文交换。会话类报文与组件见第7章, 应用层报文的格式细节参见JR/T 0066.2—2019。

## 6.6 登出

### 6.6.1 概述

连接双方互相发送登出报文视作会话的正常结束。若结束时没有收到回送的登出报文（Logout），则把对方视作已登出。除此之外的其他方式的会话结束应视为非正常, 并按错误来处理。

登出不影响任何已收到的业务报文的处理。所有已收到的有效业务报文都可在登出（Logout）之后处理。

### 6.6.2 登出与断开连接

一般情况下, 一个登出报文应在结束连接前发送。异常情况下, 会话双方发出可随时发出登出报文, 并在Text域对错误原因进行描述。这里有两个例外, 不应发送登出报文:

- 在登录阶段, 会话双方物理网络断开或会话超时, 则应立即终止会话, 不发送登出报文;
- 在登录阶段, 有效的 IMIX 会话收到来自相同 SenderCompID 的第 2 次连接尝试时, 会话接收方应立即中断该第 2 次连接尝试, 不发送登出报文。

在其他情况下, 发送登出报文不会产生风险和冲突的安全问题。

## 6.7 报文恢复

收到的报文序号与预期的报文序号不符时, 应进行报文恢复。

如果收到的报文序号比预期的报文序号小, 而且没有设置可能重复标志（PossDupFlag），则收发双方重置序号。如果收到的报文序号比预期的大, 则表明有报文被遗漏, 应通过发送重发请求申请填补缺口。

当收到重发请求时, 重发方可选择下列一种方式作出回应:

- 作为正常回应, 重发方按顺序发送被请求的报文, 这些报文的报文序号仍为原报文序号, 并且将可能重复标志（PossDupFlag）置为“Y”;
- 作为正常回应, 重发方发送序号重设-缺口填补（SeqReset-GapFill）报文, 可能重复标志（PossDupFlag）置为“Y”, 以表示删除过时或多余的报文;



- c) 作为非正常回应，重发方发送序号重设-重置 (SeqReset-Reset) 报文，可能重复标志 (PossDupFlag) 置为“Y”，以强制报文序号同步。

当接收到的报文序号大于预期报文序号时应采取的措施见表15。

表15 当接收到的报文序号大于预期报文序号时应采取的措施

报文类型	针对报文序号错误所采取的措施
登录	连接双方发送的第一条报文，用于认证和确认连接。如果发现登录报文中存在缺口，则应在回送登录确认报文之后立即发送重发请求。
登出	如果发现有缺口，应发送重发请求报文以重新接收所有丢失的报文，然后再发送登出报文作为对登出请求的确认。注意：严禁在有缺口情况下结束会话。并由登出的最初发起方负责结束会话，因此登出发起方有责任回应所有的重发请求。
重发请求	首先处理完对方的重发请求，随后发送自己的重发请求以填补报文序号错误而发生的报文缺口。
序号重设-重置	可忽略报文序号错误。因为在序号重设-重置 (SeqReset-Reset) 报文中的新报文序号 (NewSeqNo) 强制为下一发送报文的报文序号。
序号重设-缺口填补	应立即向对方发送重发请求。但是，应确保没有无意间跳过任何报文，这意味着缺口填补报文应按次序被接收到，如果次序不对，则表示出现了非正常的情况。
业务报文	执行正常的缺口填补。
<p>注：在任何情况下，除了序号重设-重置报文外，如果收到的报文序号比预期的报文序号小，而且可能重复标志 (PossDupFlag) 没有被设置，则应立即终止会话过程，并应在结束会话之前，向对方发送带有错误原因描述的登出 (Logout) 报文。</p>	

## 6.8 会话可靠性

会话可靠性通过“下一个预期的报文序号” (NextExpectedMsgSeqNum) 来保证。

## 6.9 会话场景处理

会话场景处理见表16。

表16 会话场景处理

序号	示例	必需/非必需	条件/触发条件	预期行为
1	接收会话层或应用层报文	必需	收到未在规格中定义的域 (域号)。 例外：用户自定义域。	发送拒绝报文，描述错误的域号。 (SessionRejectReason=“Invalid tag number”)。
			收到的报文中，必需域 (域号) 丢失。	发送拒绝报文，描述错误的域号。 (SessionRejectReason=“Required tag missing”)。
			收到的报文中，出现当前报文类型下未定义域。 例外：当前报文类型中，使用用户自定义域。	发送拒绝报文，描述当前报文类型下未定义域。 (SessionRejectReason=“Tag not defined for this message type”)。
			收到报文中，域值不符合定义	发送拒绝报文，描述域值不符合规定。

序号	示例	必需/非必需	条件/触发条件	预期行为
			规定（如：“55=<SOH>”和“55=IBM<SOH>”）。	（SessionRejectReason=“Tag specified without a value”）。
			收到报文中，域的域值有错误（超出范围或不在有效枚举数值列表中）。 例外：用户自定义枚举值。	发送拒绝报文，描述域的域值有错误（超出范围或不在有效枚举数值列表中）。 （SessionRejectReason=“Value is incorrect (out of range) for this tag”）。
			收到报文中，域的数据格式不正确。	发送拒绝报文，描述域的数据格式不正确。 （SessionRejectReason=“Incorrect data format for value”）。
			收到报文中，报文格式混乱：标准报文头+报文体+标准报文末的顺序不正确。	发送拒绝报文，描述不正确的报文结构。 header+body+tailer（SessionRejectReason=“Tag specified out of required order”）。
			收到报文中，非重复组的域值出现次数超过一次。	发送拒绝报文，描述域重复出现。 （SessionRejectReason=“Tag appears more than once”）。
			收到带有重复组的报文中，重复组的重复次数的域值不正确。	发送拒绝报文，描述重复次数的域值不正确。 （SessionRejectReason=“Incorrect NumInGroup count for repeating group”）。
			收到带有重复组的报文中，该重复组中域的顺序不符合规范。	发送拒绝报文，描述域顺序不正确的重复组。 （SessionRejectReason=“Repeating group fields out of order”）。
			收到报文中，域值包含一个或多个域界定符（<SOH>），而非正常数据。	发送拒绝报文，描述嵌有<SOH>的域（域号）。 （SessionRejectReason=“Non ‘data’ value includes field delimiter ( SOH character)”）。
			（非必需）当应用级处理或者系统不可用时，收到报文。	发送 Business Message Reject 报文，描述应用层报文处理不可用。 （BusinessRejectReason=“Application notavailable”）。
			收到报文中，条件必需域丢失。	发送 Business Message Reject 报文，描述报文的条件必需域缺失。 （BusinessRejectReason=“Conditionally Required Field Missing”）。
			收到报文中，同一个域同时出现在明文和加密部分中，但值不相同。	发送拒绝报文。（SessionRejectReason=“Decryption problem”）。
2	发送应用和会话信息来测试正常或者不正常的行为/回	必需	发送多个相同报文，域值相同（排除有顺序限制的）。	报文能被正常接收，后续报文的 MsgSeqNum 能被正常接收。

序号	示例	必需/非必需	条件/触发条件	预期行为
	应			
3	报文出入队列	必需	断开连接时，报文出队或入队的处理。	报文入队，但报文不出队。
4	支持加密	非必需	收到支持且有效的 EncrypMethod 域值的登录报文。	a) 接收报文； b) 执行适用的解密算法和快速的加密算法； c) 用相同的加密算法响应登录报文。
			收到无效或未被支持的 EncrypMethod 域值的登录报文。	a) 发送拒绝报文，描述无效或未被支持的 EncrypMethod 域值 (SessionRejectReason=“Decryption problem”)； b) 发送登出报文，描述无效或未被支持的加密算法； c) (非必需的) 等待登出报文的响应 (可能由于解密问题导致无法收到响应)； d) 断开会话。
			收到 SignatureLength 和 Signature 域值有效的报文。	接收报文。
			收到 SignatureLength 域值无效的报文。	发送拒绝报文，描述 SignatureLength 域值无效。(SessionRejectReason=“Signature problem”)。
			收到 Signature 域值无效的报文。	发送拒绝报文，描述 Signature 域值无效。(SessionRejectReason=“Signature problem”)。 或者，考虑解密错误或报文乱序问题，忽视该报文 (设置下一个报文序号自增 1)，继续接收报文。
			收到报文，其中 SecureDataLen 域值有效，并且 SecureData 域值能被解密为有效的可解析的明文。	接收报文。
			收到 SecureDataLen 域值无效的报文。	考虑到解密错误或报文乱序问题，忽视该报文，设置下一个报文序号自增 1，继续接收报文。
			收到报文中，SecureData 域值无法被解密为有效的可解析的明文。	发送拒绝报文，描述无效的 SecureData 域值 (SessionRejectReason=“Decryption problem”)。

序号	示例	必需/非必需	条件/触发条件	预期行为
			接收的报文中，有一个或多个域不在未加密部分，而双方约定这些域应属于“必须未加密”部分。	发送拒绝报文，描述未加密部分域缺失（SessionRejectReason=“Decryption problem”）。
			接收的报文中，存在不符合EncryptMethod规定，错误操作导致残留字符问题（比如：加密部分之前的明文长度不符合8的倍数）。	发送拒绝报文，描述在加密时错误操作导致残留字符问题（SessionRejectReason=“Decryption problem”）。

## 7 会话类报文与组件

### 7.1 会话类报文

#### 7.1.1 心跳报文（Heartbeat MsgType=0）

心跳用于监测通信连接的状况，并可确认是否接收到最后一条报文。

心跳报文作为测试请求报文的响应，应包含在测试请求报文中的TestReqID域值，用于验证心跳报文是测试请求报文的响应而不是常规超时的响应。

心跳报文格式见表17。

表17 心跳报文格式

域号/嵌套组件名	域名	必需域	备注
StandardHeader 标准报文头		Y	MsgType=0。
112	TestReqID		测试请求标识符，如是对测试请求而响应的心跳，则应包含本域。
StandardTailor 标准报文尾		Y	

心跳报文场景示例见表18。

表18 心跳报文场景示例

示例	条件/触发条件	预期行为
发送心跳报文	预设的心跳间隔期间（HeartBtInt 域）。	发送心跳报文。
接收心跳报文	有效的心跳报文。	接收心跳报文。

#### 7.1.2 登录报文（Logon MsgType=A）

登录报文能证实用户是否已建立与对方系统的连接。登录报文应是在会话开始时的连接双方发送的第一个报文。

在接收登录报文时，登录接收方将验证登录发起方身份的合法性，并发出登录报文或响应登录报文以确认连接请求已被接收。

登录报文格式见表19。

表19 登录报文格式

域号/嵌套组件名	域名	必需域	备注
StandardHeader 标准报文头		Y	MsgType=A。
58	Text		当用作接收方发回给登录发起方的登录确认报文时，能提供登录反馈。
95	RawDataLength		无格式数据长度，用于认证。
96	RawData		无格式数据，用于认证。
98	EncryptMethod		加密方法。
108	HeartBtInt	Y	心跳间隔。
141	ResetSeqNumFlag		序号重设标志。
354	EncodedTextLen		如果 EncodedText 被指定，EncodedTextLen 应设置并且优先级最高。
355	EncodedText		通过 MessageEncoding 域用指定的加密格式来加密该文本域。
383	MaxMessageSize		最大报文长度，单条报文的最大字节数。
464	TestMessageIndicator		测试标志，指明该会话是测试连接或正常运行连接，用于防止意外。
553	Username		用户名。
554	Password		密码。
789	NextExpectedMsgSeqNum		非必需，双方监测和恢复报文缺口的候选协商方法参照 6.8 条会话可靠性。
925 (10193*) <sup>a</sup>	NewPassword		为 IMIX 登录指定一个新的密码，在接下来的登录中使用该密码。
1137	DefaultAppIVerID		IMIX 报文的默认版本在这个会话中使用。
1400	EncryptedPasswordMethod		
1401	EncryptedPasswordLen		
1402	EncryptedPassword		
1403	EncryptedNewPasswordLen		
1404	EncryptedNewPassword		加密新密码-通过在域 EncryptedPasswordMethod (1400) 中指定的方法加密。
1407	DefaultAppIExtID		IMIX 报文的默认扩展包在这个会话中使用。
1408	DefaultCstnAppIVerID		IMIX 报文的默认自定义应用版本（字典）在这个会话中使用。
1409	SessionStatus		登录时间的会话状态。当登录报文是来自于会话接收方的确认登录时，该域被使用。
StandardTailor 标准尾部		Y	
<sup>a</sup> ( ) 中带*的域号为 JR/T 0066—2011 版本对应的域号，与本部分版本域号兼容，下同。			

登录报文场景示例见表20。

表20 登录报文场景示例

示例	条件/触发条件	预期行为
发起登录过程	发起登录请求。	发送登录报文。
接收登录反馈	接收到登录反馈。	a) 登录成功, 接收登录成功反馈, 正常发送业务报文; b) 登录失败, 接收到登录反馈, 断开连接。

## 7.1.3 测试请求报文 (Test Request MsgType=1)

测试请求报文用于检查对方报文序号或检查通信线路的状况。接收方需使用带有测试请求标识符 (TestReqID) 的心跳进行应答。宜使用时间戳用作测试请求标识符 (TestReqID) 的值。

测试请求报文格式见表21。

表21 测试请求报文格式

域号/嵌套组件名	域名	必需域	备注
StandardHeader 标准报文头		Y	MsgType=1。
112	TestReqID	Y	测试请求标识符, 不能加密。
StandardTailor 标准报文尾		Y	

测试请求报文场景示例见表22。

表22 测试请求报文场景示例

示例	条件/触发条件	预期行为
发送测试请求报文	预设的心跳超时周期内, 未收到报文。	a) 发送测试请求报文; b) 追踪并核实收到的测试请求报文响应中TestReqID 一致 (可能不是下一条接收的报文)。

## 7.1.4 重发请求报文 (Resend Request MsgType=2)

当报文接收方发现报文序号缺口或丢失报文时, 可发出重发请求, 向报文发送方申请报文重复发送。重发请求可用于请求重新发送单个报文、一系列的报文或在某一特定报文之后的所有报文。

重发请求有以下几种表示方式:

- 请求重发一条报文: 起始报文序号 (BeginSeqNo) = 结束报文序号 (EndSeqNo);
- 请求重发某个范围内的报文: 起始报文序号 (BeginSeqNo) = 该范围中的第一条报文, 结束报文序号 (EndSeqNo) = 该范围中的最后一条报文序号;
- 请求重发某一特定报文之后的所有的报文: 起始报文序号 (BeginSeqNo) = 该范围中的第一条报文, 结束报文序号 (EndSeqNo) = 0。

重发请求报文的格式见表23。

表23 重发请求报文格式

域号/嵌套组件名	域名	必需域	备注
StandardHeader 标准报文头		Y	MsgType=2。
7	BeginSeqNo	Y	

域号/嵌套组件名	域名	必需域	备注
16	EndSeqNo	Y	
StandardTailor 标准报文尾		Y	

重发请求报文场景示例见表24。

表24 重发请求报文场景

示例	条件/触发条件	预期行为
发送重发请求	发送重发请求报文，来请求丢失的报文。	收到重发的报文。
收到重发请求	收到对端发来的重发请求。	对被请求的报文，执行重发处理。

### 7.1.5 会话拒绝报文 (Reject MsgType=3)

当报文接收方收到非法报文时，应发出会话拒绝报文。会话拒绝原因见表25。

表25 会话拒绝原因

会话拒绝原因
0=存在无效域号。
1=所需域号丢失。
2=该报文类型未定义域号。
3=未定义域号。
4=指定的域号没有赋值。
5=具有错误值（不在范围内）的域号。
6=值的错误数据格式。
7=加密问题。
8=签字问题。
9=参与方标识符问题 (CompID problem)。
10=发送时间准确性问题。
11=无效报文类型 (Invalid MsgType)。
12=XML 确认错误 (Validation error)。
13=域号出现一次以上。
14=指定的域号不符合要求的次序。
15=重复组的域次序颠倒。
16=重复组内的“组内计数号”计数不正确。
17=非“数据”型的值包含域界定符<SOH>。
99=其他。
注：可能存在其他违反会话层规则的情况，在这种情形下，可应用99=其他，详尽的原因可存于正文 (text) 域内。

会话拒绝报文应写入日志，同样会话拒绝报文序号也应依次递增。

会话拒绝报文格式见表26。

表26 会话拒绝报文格式

域号/嵌套组件名	域名	必需域	备注
StandardHeader 标准报文头		Y	MsgType=3。
45	RefSeqNum	Y	引用报文序号,即被拒绝的报文序号。
58	Text		文本,可作解释拒绝的原因。
354	EncodedTextLen		编码文本长度,如果报文使用 EncodedText 域,则 EncodedTextLen 必需且 EncodedText 应紧跟在 EncodedTextLen 之后。
355	EncodedText		编码文本(非 ASCII 码)。
371	RefTagID		相关错误域号。
372	RefMsgType		相关错误报文类型。
373	SessionRejectReason		会话拒绝原因编号。
1130	RefAppIVerID		登录报文应使用 DefaultAppIVerID 域(1137)指定默认应用版本。当应用类报文未指定 AppIVerID 域(1128)时,宜在会话拒绝报文中,使用该域指定版本。
1131	RefCstmAppIVerID		登录报文应使用 DefaultCstmAppIVerID 域(1408)指定自定义应用版本。当应用类报文未指定 CstmAppIVerID 域(1129)时,宜在会话拒绝报文中,使用该域指定自定义应用版本。
1406	RefAppIExtID		登录报文应使用 DefaultAppIExtID 域(1407)指定应用扩展版本。当应用类报文未指定 AppIExtID 域(1156)时,宜在会话拒绝报文中,使用该域指定版本。
StandardTailer 标准报文尾		Y	

接收拒绝报文场景示例见表27。

表27 接收拒绝报文场景示例

示例	条件/触发条件	预期行为
接收拒绝报文	有效的拒绝报文。	接收该拒绝报文。

### 7.1.6 序号重设报文 (Sequence Reset MsgType=4)

序号重设报文是报文发送方用于告知报文接收方下一个报文的报文序号。

序号重设报文有两种模式: 序号重设-缺口填补 (SeqReset-Gap Fill) 和序号重设-重置 (SeqReset-Reset), 用GapFillFlag域来标识。当GapFillFlag=Y时, 该报文为序号重设-缺口填补 (SeqReset-Gap Fill); 当GapFillFlag=N或没有设置时, 该报文为序号重设-重置 (SeqReset-Reset)。



序号重设报文格式见表28。

表28 序号重设报文格式

域号/嵌套组件名	域名	必需域	备注
StandardHeader 标准报文头		Y	MsgType=4。
36	NewSeqNo	Y	新报文序号。
123	GapFillFlag		缺口填补标识。
StandardTailor 标准报文尾		Y	

序号重设报文场景示例见表29。

表29 序号重设报文场景示例

示例	条件/触发条件	预期行为
接收重发请求报文	有效的重发请求报文。	a) 接收对端发送的重发请求报文，响应请求报文中要求重发的MsgSeqNum域值范围序号（请求报文的BeginSeqNo域到EndSeqNo域值）的报文； b) 接收方根据请求报文范围，返回丢失报文； c) 发送完毕后，向对手方发送序号重设-重置报文。
序号同步	申请失败。	发送序号重设-重置报文，或手动重置MsgSeqNum值为1。
收到序号重设-缺口填补报文	收到序号重设-缺口填补报文，满足NewSeqNo大于MsgSeqNum，且MsgSeqNum大于预期的序列值。	为填补最后预期接收MsgSeqNum值和实际接收MsgSeqNum值之间的缺口，发送重发请求报文。
	收到序号重设-缺口填补报文，满足NewSeqNo大于MsgSeqNum，且MsgSeqNum与预期序列值相同。	设置下一个报文的报文序号（NextExpectedMsgSeqNum）值等于NewSeqNo。
收到序号重设-缺口填补报文	收到序号重设-缺口填补报文，满足NewSeqNo大于MsgSeqNum，且MsgSeqNum小于预期序列值，且PossDupFlag="Y"。	a) 忽略报文； b) 设置下一个报文序号（NextExpectedMsgSeqNum）自增1。
	收到序号重设-缺口填补报文，满足NewSeqNo大于MsgSeqNum，且MsgSeqNum小于预期序列值，且PossDupFlag的值不是"Y"。	a) 应发送含有"MsgSeqNum过低，预期序号值为X但接收到的是Y"描述的登出报文； b)（非必需）等待登出报文响应（注意：可能有错误的MsgSeqNum）。
	收到序号重设-缺口填补报文，满足NewSeqNo小于等于MsgSeqNum，且MsgSeqNum等于预期序列值。	发送拒绝报文，描述信息"尝试降低序号，错误值MsgSeqNum=<X>"。
收到序号重设-重置报文	收到序号重设-重置报文，满足NewSeqNo大于预期要接收报文的序列值。	重置接收下一个报文序号预期值为本次重置报文中的NewSeqNo的值。
	收到序号重设-重置报文，满足NewSeqNo等于预期要接收报文的序	a) 忽略报文； b) 设置下一个报文序号自增1。

示例	条件/触发条件	预期行为
	列值。	
	收到序号重设-重置报文，满足 NewSeqNo 小于预期的数字序列。	a) 接收序号重设-重置报文，忽略其MsgSeqNum值； b) 发送拒绝报文，描述错误的MsgType值 (SessionRejectReason=“Value is incorrect (out of range) for this tag”)； c) 不调低预期序列值。
PossResend 域的处理	收到非序号重设-重置的报文，其中 PossResend=“Y”。	a) 忽略此报文； b) 设置下一个报文序号自增1。

### 7.1.7 登出报文 (Logout MsgType=5)

登出报文是会话一方发起或确认会话终止的报文。  
登出报文格式见表30。

表30 登出报文格式

域号/嵌套组件名	域名	必需域	备注
StandardHeader 标准报文头		Y	MsgType=5。
58	Text		文本。
354	EncodedTextLen		编码文本长度，如果使用 EncodedText 域，必需且 EncodedText 应紧跟在该域之后。
355	EncodedText		使用编码文本（非 ASCII 码）。
1409	SessionStatus		登出时的会话状态。
StandardTailor 标准报文尾		Y	

登出报文场景示例见表31。

表31 登出报文场景示例

示例	条件/触发条件	预期行为
发送登出请求	发送登出请求。	a) 发送登出报文； b) 等待对方响应登出报文（注意：如果会话存在问题，可能接收不到响应）； c) 断开连接。
收到登出报文	收到的有效登出报文，视为响应登出请求处理。	断开连接，不发送报文。
	接收到主动发起的有效登出报文。	a) 发送登出响应报文； b) 断开连接。

## 7.2 会话类组件

### 7.2.1 HopGrp 重复组

重复组<HopGrp>记录报文经第三方发送的历史，主要用于跟踪报文的路径。  
<HopGrp>组件结构见表32。

表32 &lt;HopGrp&gt;组件结构

域号/嵌套组件名	域名	必需域	备注
627	NoHops		
-->	628	HopCompID	Y
-->	629	HopSendingTime	
-->	630	HopRefID	

## 7.2.2 区块链组件

### 7.2.2.1 BlockChainHeader 组件

区块链报文头包含魔数、命令名、负载大小和校验码。

<BlockChainHeader>组件结构见表33。

表33 &lt;BlockChainHeader&gt;组件结构

域号/嵌套组件名	域名	必需域	备注
20000	MagicNumber		魔数。
20001	CommandName		命令名。
20002	LoadSize		负载大小。
20003	CheckCode		校验码。

### 7.2.2.2 BlockHeader 组件

区块头包含前区块哈希值、区块产生时间戳、区块中所有交易的Merkle树根等。

<BlockHeader>组件结构见表34。

表34 &lt;BlockHeader&gt;组件结构

域号/嵌套组件名	域名	必需域	备注
20004	Version		版本。
20005	HashPrevBlock		前区块头哈希。
20006	HashMerkleRoot		默克尔根哈希。
20007	Time		Time 时间戳。
20008	HashBits		Bits 当前目标 HASH 值。
20009	Nonce		Nonce 随机数。

附 录 A  
(规范性附录)  
域字典

域字典见表A.1。

表A.1 域字典

域号	域名	数据类型	有效值	注释
7	BeginSeqNo	SeqNum		
8	BeginString	String		
9	BodyLength	Length		
10	Checksum	String		校验和, 报文的最末域(不可加密)。
16	EndSeqNo	SeqNum		
34	MsgSeqNum	SeqNum		
35	MsgType	String	0、1、2、3、4、5、A、U203、U204、U205、U206、U207、U208、U209、U210、U211、U212、U213、U214、U215	报文类型。 每条 IMIX 报文都有自己的报文类型编码, 即 MsgType。系统根据 MsgType 的值来确定收到的是何种 IMIX 报文。
36	NewSeqNo	SeqNum		
43	PossDupFlag	Boolean	N-ORIGINAL_TRANSMISSION Y-POSSIBLE_DUPLICATE	N、Y。
45	RefSeqNum	SeqNum		
49	SenderCompID	String		
50	SenderSubID	String		报文发送方子标识。
52	SendingTime	UTCTimestamp		
56	TargetCompID	String		报文接收方标识。
57	TargetSubID	String		
58	Text	String		
89	Signature	Data		
90	SecureDataLen	Length		
91	SecureData	Data		Actual encrypted data stream。
93	SignatureLength	Length		
95	RawDataLength	Length		
96	RawData	Data		
97	PossResend	Boolean		报文可能重新发送的标志。
98	EncryptMethod	Int		
108	HeartBtInt	Int		心跳间隔。

域号	域名	数据类型	有效值	注释
112	TestReqID	String		测试请求标识符，如是对测试请求而响应的心跳，则应包含本域。
115	OnBehalfOfCompID	String		最初发送方标识符（可加密），用于经第三方发送。
116	OnBehalfOfSubID	String		最初发送方子标识符（可加密），用于经第三方发送。
122	OrigSendingTime	UTCTimestamp		
123	GapFillFlag	Boolean	N-SEQUENCE_RESET_IGNORE_MSG_SEQ_NUM Y-GAP_FILL_MESSAGE_MSG_SEQ_NUM_FIELD_VALID	N、Y。
128	DeliverToCompID	String		
129	DeliverToSubID	String		最终接收方子标识符（可加密）。
141	ResetSeqNumFlag	Boolean		报文序号重置标志。
142	SenderLocationID	String		
143	TargetLocationID	String		
145	DeliverToLocationID	String		
212	XmlDataLen	Length		
213	XmlData	Data		
347	MessageEncoding	String		
354	EncodedTextLen	Length		
355	EncodedText	Data		
369	LastMsgSeqNumProcessed	SeqNum		
371	RefTagID	Int		
372	RefMsgType	String	0-HEARTBEAT 1-TEST_REQUEST 2-RESEND_REQUEST 3-REJECT 4-SEQUENCE_RESET 5-LOGOUT A-LOGON	0、1、2、3、4、5、A。
373	SessionRejectReason	Int	0-INVALID_TAG_NUMBER 1-REQUIRED_TAG_MISSING 2-TAG_NOT_DEFINED_FOR_THIS_MESSAGE_TYPE 3-UNDEFINED_TAG 4-TAG_SPECIFIED_WITHOUT_A_VALUE 5-VALUE_IS_INCORRECT	

域号	域名	数据类型	有效值	注释
			6-INCORRECT_DATA_FORMAT_FOR_VALUE 7-DECRYPTION_PROBLEM 8-SIGNATURE_PROBLEM 9-COMPID_PROBLEM 10-SENDINGTIME_ACCURACY_PROBLEM 11-INVALID_MSGTYPE 12-XML_VALIDATION_ERROR 13-TAG_APPEARS_MORE_THAN_ONCE 14-TAG_SPECIFIED_OUT_OF_REQUIRED_ORDER 15-REPEATING_GROUP_FIELDS_OUT_OF_ORDER 16-INCORRECT_NUMINGROUP_COUNT_FOR_REPEATING_GROUP 17-NON_DATA_VALUE_INCLUDES_FIELD_DELIMITER 18-INVALID_UNSUPPORTED_APPLICATION_VERSION 99-OTHER	
383	MaxMessageSize	Length		
464	TestMessageIndicator	Boolean	N-FALSE Y-TRUE	N、Y。
553	Username	String		
554	Password	String		
627	NoHops	NumInGroup		
628	HopCompID	String		
629	HopSendingTime	UTCTimestamp		
630	HopRefID	SeqNum		
789	NextExpectedMsgSeqNum	SeqNum		
925 (10193)	NewPassword	String		兼容 925 和 10193。
1128	AppIVerID	String	0-V2_0_5	0、1、2、3、4。
1128	AppIVerID	String	1-V2_0_6 2-V2_0_7 3-V2_0_8 4-V2_0_9	0、1、2、3、4。

域号	域名	数据类型	有效值	注释
1130	RefApplVerID	String	0-V2_0_5 1-V2_0_6 2-V2_0_7 3-V2_0_8 4-V2_0_9	0、1、2、3、4。
1131	RefCstmApplVerID	String		
1137	DefaultApplVerID	String		
1156	ApplExtID	Int		
1400	EncryptedPasswordMethod	Int		
1401	EncryptedPasswordLen	Length		
1402	EncryptedPassword	Data		
1403	EncryptedNewPasswordLen	Length		
1404	EncryptedNewPassword	Data		
1406	RefApplExtID	Int		
1407	DefaultApplExtID	Int		
1408	DefaultCstmApplVerID	String		
1409	SessionStatus	Int	0-SESSION_ACTIVE 1-SESSION_PASSWORD_CHANGED 2-SESSION_PASSWORD_DUE_TO_EXPIRE 3-NEW_SESSION_PASSWORD_DOES_NOT_COMPLY_WITH_POLICY 4-SESSION_LOGOUT_COMPLETE 5-INVALID_USERNAME_OR_PASSWORD 6-ACCOUNT_LOCKED 7-LOGONS_ARE_NOT_ALLOWED_AT_THIS_TIME 8-PASSWORD_EXPIRED	0、1、2、3、4、5、6、7、8。
20000	MagicNumber	Int		魔数。
20001	CommandName	Char		命令名。
20002	LoadSize	Int		负载大小。
20003	CheckCode	Char		校验码。
20004	Version	Int		版本。
20005	HashPrevBlock	Char		前区块头哈希。
20006	HashMerkleRoot	Char		默克尔根哈希。
20007	Time	UTCTimestamp		Time 时间戳。
20008	HashBits	Int		Bits 当前目标 HASH 值。

域号	域名	数据类型	有效值	注释
20009	Nonce	Int		Nonce 随机数。



参 考 文 献

- [1] CBD-Forum-001—2017 区块链 参考架构
-