Financial Technology
腾讯支付基础平台与金融应用线

TrustSQL
对接开发指南

腾讯科技（深圳）有限公司

目 录

第1章　对接方法

1.1 总体描述

TrustSQL 的接入方法与 mysql 类似，指定 IP、端口、用户名和密码，通过 mysql5.5+的客户端连接。

TrustSQL 提供 insert 和 select 两种 SQL 接口：交易通过 insert into t_transaction 交易流水来实现；查询通过 select * from t_transaction(t_account、t_block)来实现。

与 Mysql 的区别：

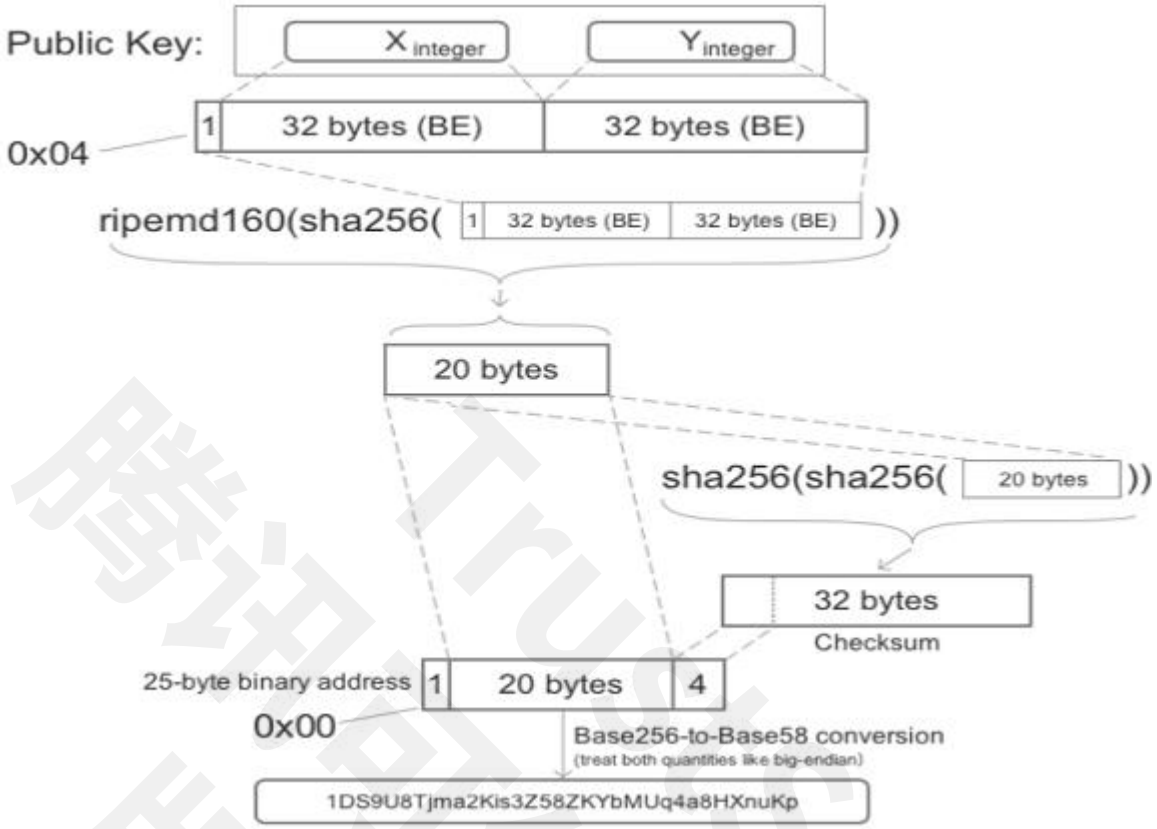
项目	Mysql	TrustSQL	描述
协议	Mysql 协议	兼容 Mysql 协议	
支持的操作	CURD	仅仅支持 Insert 和 select	区块链入链数据不可修改，所以只支持 Insert 操作
插入操作	可以随意插入数据	所有入链的数据需要使用私钥进行签名	
查询操作	可以随意查询	兼容 Mysql 查询	

1.2 公私钥、地址与签名

TrustSQL 统一采用 ECDSA 进行数字签名，曲线选择与比特币相同：secp256k1。

公私钥：采用 secp256k1 椭圆曲线生成一对，或者通过私钥可以算出公钥。在 TrustSQL 中公私钥的编码格式为 Base64。

地址：通过私钥可以算出公钥，通过公钥可以算出地址，地址使用。在 TrustSQL 中地址的编码格式为 Base58。



签名：使用 secp256k1 椭圆曲线签名，签名后的 r/s 使用 der 编码。在 TrustSQL 中签名的编码格式为 Base64。

1.3 TrustSQL 提供的接口

1、 建立连接：

Trustsql 提供兼容 Mysql5.5+协议的连接方式，可以使用 libmysql 库，libmysql++库，mysql 客户端等进行对接，使用 mysql 连接举例如下：

--mysql -hip -P8066 -uuser -ppassword -Dtrustsql

- ✓ ip：Trustsql 服务所在 ip 地址
- ✓ user：Trustsql 服务的用户名
- ✓ password：Trustsql 服务的密码

2、 交易接口：

a) 字段说明：

序号	字段名称	字段类型	参与签名	字段说明
1.	Fseqno	String	Y	交易单号是
2.	Fsrc	String	Y	源账户地址
3.	Fdst1	String	Y	目的账户地址 1
4.	Fdst1_amount	Int	Y	转出份额 1
5.	Fdst2	String	Y	目的账户地址 2
6.	Fdst2_amount	Int	Y	转出份额 2
7.	Fattach	json	Y	附加字段，每次交易可以附带上的数据
8.	Fassets	json	Y	数字资产 JSON，该字段为不可变类型，相同 Fassets 才可转账
9.	Ftime	datetime	Y	记账时间
10.	Fsign	String	N	Fsrc 私钥的签名
11.	Fpubkey	String	Y	Fsrc 的公钥 BASE64 格式

b) 操作例子：

交易接口直接需要按照如下例子拼接 insert 语句进行操作，举例如下：

```
-- insert into t_transaction
-- Fseqno='xxxxxxxxxxxx',                                    //交易单号
-- Fsrc='3KA86SffUFYXZcbPfdEc4UX1F8z95PdGob',    //源帐户地址
-- Fdst1='1CeZ4EZamNQixcgPQ6tTXbgYkNfc5dDErB',  //目的帐户地址 1
-- Fdst1_amount=100,                                        //转账份额 1
-- Fdst2='1CeZ4EZamNQixcgPQ6tTXbgYkNfc5dDErB',  //目的帐户地址 2
-- Fdst2_amount=100,                                        //转账份额 2
-- Fattach='{JSON String}',                                 //附加字段，覆盖 src 地址中 Fattach 的内容
-- Fassets='{JSON String}',          //数字资产 JSON，该字段为不可变类型，相同 Fassets 才可转账
-- Ftime='2017-01-01 00:00:00',                             //记账时间
-- Fsign='304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446',    //Fsrc 私钥的签名
--
Fpubkey='BHSgdFFuE8p0FQ5+Ge1AO5XAj8su5B8UpAtWo9zNXifUk9+6T4L5rVxhxRWU7t83zek7
EYTYap6EY1LWl2Qc/Ro=',                                    //Fsrc 的公钥 BASE64 格式
```

✓ 例子中代表 Fsrc 向 Fdst1 和 Fdst2 分别转账 100 份额。

✓ 需要注意转账双方的 Fassets 必须一致才能转账，即同一类资产才可转账。

✓ Fassets，Fattach 必须有值。

✓ 当(Fsrc==Fdst1)&&(Fdst1_amount=0)&&(Fdst2==NULL)时，等同于只修改资产的状态，只更新 src 中 Fattach 的内容。

状态的变更看作是一种特殊交易，通过 insert into t_transaction 把输入和输出地址设置为相同帐户，交易金额设置为 0 来实现，实际达到更新 t_account 中 Fattach 字段的效果。

c) 签名规则

insert 操作时需要使用 Fsrc 的私钥对请求串进行签名。签名算法如下：

1) 参与签名字段如下（字段名的 ASCII 码从小到大排序）：

Fattach；Fassets；Fdst1；Fdst1_amount；Fdst2；Fdst2_amount；Fpubkey；Fseqno；Fsrc；Ftime

2) Fassets 和 Fattach 的 json 字段排序，生成规则：

- ✓ json::object 中每个字段按照 key=value 形式展开，并按照 key 的 ASCII 码从小到大排序后 以&号分隔；
- ✓ json::array 中每个字段按照 value1,value2,...形式展开，并按照 index 排序后以,号分隔；
- ✓ 当 json::object 嵌套时 按照 key=key=value 形式展开，并按照 key 的 ASCII 码从小到大排序后以&号分隔；

例如：{"a":1,"b":"2","c":false,"d":{"d1":"v1","d2":2},"e":[1,2,3,{"e4":4}]}

转成 a=1&b=2&c=false&d=d1=v1&d2=2&e=1,2,3,e4=4 再参与签名串的拼接，其中 key 和 value 都不包含 json 字段开头和结尾的"（双引号）。

3) 拼接签名原字符串规则：

原字符串按照参数字段名的 ASCII 码从小到大排序后使用 QueryString 的格式（即 key1=value1&key2=value2…）拼接而成。签名时字段名和字段值都采用 UTF-8 编码，但不进行 URL 编码。

例如上面交易接口中对应的签名原串为：

Fassets=json 字段排序&Fattach=json 字段排序&Fdst1=1CeZ4EZamNQixcgPQ6tTXbgYkNfc5dDErB&Fdst1_amount=100&Fdst2=1CeZ4EZamNQixcgPQ6tTXbgYkNfc5dDErB&Fdst2_amount=100&Fpubkey=BHSgdFFuE8p0FQ5+Ge1AO5XAj8su5B8UpAtWo9zNXifUk9+6T4L5rVxhxRWU7t83zek7EYTYap6EY1LWl2Qc/Ro=&Fseqno=xxxxxxxxxxxx&Fsrc=3KA86SffUFYXZcbPfdEc4UX1F8z95PdGob&Ftime=2017-01-01 00:00:00

4) 签名算法描述：

sign = base64（ECDSA (sha256(原字符串))）。签名后的 r/s 使用 DER 编码再转成 base64 表示。

3、 查询接口：

查询接口可以兼容 Mysql 查询类型，直接拼装 select 语句即可，支持使用 Mysql5.7 json 字段进行查询。

a) 交易流水

交易流水查询接口可以得到的字段与交易接口相同，举例如下：

--select Fseqno,Fsrc,Fdst1,Fdst1_amount,Fdst2,Fdst2_amount,Fattach,Fassets,Ftime,Fsign,Fpubkey from t_transaction;

b) 账户信息

帐户信息查询接口可以得到的字段如下表，举例如下：

-- select Famount, Fattach from t_account where Faddress='14qViLJfdGaP4EeHnDyJbEGQys'

字段说明

序号	字段名称	字段类型	字段说明
1.	Faddress	String	账户地址
2.	Famount	Int	账户拥有份额
3.	Fattach	json	附加字段，覆盖成 t_transaction 表中最后一条交易 Fsrc 地址中 Fattach 的内容
4.	Fassets	json	数字资产 JSON，对应 Faddress 产生第一笔交易的 Fassets 的内容，之后所有交易都必须相同
5.	Fmodify_time	datetime	修改时间
6.	Ftrans_hash	String	最后交易 hash 值

c) 区块信息

区块信息查询接口可以得到的字段如下表，举例如下：

-- select Fhight, Fprev_hash,Fcreate_time from t_block where Fhight='0'

字段说明

序号	字段名称	字段类型	字段说明
1.	Fhight	Int	区块高度
2.	Fprev_hash	String	前一个区块 hash 值
3.	Froot_hash	String	根区块 hash 值
4.	Fcreate_time	datetime	创建时间
5.	Fhash	String	本区块 hash 值

4、 系统状态查询：

查询系统运行状态：版本信息，是否 leader，是否在修复数据等，举例如下

-- show @@trustsql_info;

```
mysql> show @@trustsql_info;
+-------------------------------------+----------------------------+-----------------------------------------------------------------------
| NAME                                | VALUE                      | DESCR
+-------------------------------------+----------------------------+-----------------------------------------------------------------------
| trustsql.version                    | trustsql-0.2-20170315044113 | trustsql publish version.
| trustsql.ip                         | [redacted]                 | trustsql service listening ip.
| trustsql.port                       | 8066                       | trustsql service listening port
| trustsql.default_charsert           | utf8                       | trustsql connection default_charsert.
| trustsql.node.id                    | 1                          | trustsql node id
| trustsql.node.count                 | 4                          | trustsql node count
| trustsql.repairing                  | false                      | trustsql reparing status
| trustsql.socket.so_rcvbuf           | 16777216                   | trustsql connection socket receive buffer size
| trustsql.socket.so_sndbuf           | 16777216                   | trustsql connection socket send buffer size
| trustsql.socket.so_timeout          | 600                        | trustsql connection socket so_timeout.
| trustsql.socket.tcp_nodelay         | true                       | trustsql connection socket tcp nodelay.
| trustsql.socket.connect_timeout_millis | 5000                    | trustsql  connection connect timeout millis.
| trustsql.bft-raft.members           | 1,2,3,4                    | bft-raft Members
| trustsql.bft-raft.leader            | 4, raft-id=4               | bft-raft current leader
| trustsql.bft-raft.isleader          | false                      | bft-raft current node isleader(true or false)
| trustsql.bft-raft.majority          | 3                          | bft-raft majority
| trustsql.bft-raft.currentTerm       | 3599                       | bft-raft currentTerm
| trustsql.bft-raft.lastAppended      | 512950                     | bft-raft lastAppended
| trustsql.bft-raft.commitIndex       | 512950                     | bft-raft commitIndex
| system.jvm.version                  | 1.8.0_111                  | Java Runtime Version.
| system.jvm.processors               | 4                          | the number of processors available to the Java virtual machine
| system.jvm.totalMemory              | 2139619328                 | the total amount of memory in the Java virtual machine.
| system.jvm.maxMemory                | 3817865216                 | the maximum amount of memory that the Java virtual machine will
| system.jvm.freeMemory               | 1529236600                 | the amount of free memory in the Java Virtual Machine
```

字段说明

序号	字段名称	字段类型	字段说明
1.	trustsql.version	String	Trustsql 版本号
2.	trustsql.ip	String	当前节点 ip
3.	trustsql.port	Int	当前节点监听端口
4.	trustsql.default_charsert	String	默认连接字符集
5.	trustsql.node.id	Int	当前节点 id
6.	trustsql.node.count	Int	Trustsql 网络总结点数
7.	trustsql.repairing	Bool	当前节点是否在修复数据
8.	trustsql.socket.so_rcvbuf	Int	Socket 接收缓冲区大小
9.	trustsql.socket.so_sndbuf	Int	Socket 发送缓存区大小
10.	trustsql.socket.so_timeout	Int	Socket 超时时间(秒)
11.	trustsql.socket.tcp_nodelay	Bool	IPPROTO_TCP 设置 TCP_NODELAY 标志位
12.	trustsql.socket.connect_timeout_millis	Int	Mysql 连接超时(秒)
13.	trustsql.bft-raft.members	String	Trustsql 网络成员节点列表
14.	trustsql.bft-raft.leader	String	Trustsql 网络主节点 id
15.	trustsql.bft-raft.isleader	Bool	当前节点是否为主节点
16.	trustsql.bft-raft.majority	Int	需要多少节点保持正常运行
17.	trustsql.bft-raft.currentTerm	Int	bft-raft 当前 Term 值
18.	trustsql.bft-raft.lastAppended		最后追加数据的高度
19.	trustsql.bft-raft.commitIndex		最后提交数据的高度
20.	system.jvm.version		jvm 版本号
21.	system.jvm.processors		jvm 运行数量
22.	system.jvm.totalMemory		jvm 总内存大小

23.	system.jvm.maxMemory		jvm 最大使用内存限制
24.	system.jvm.freeMemory		jvm 内存空闲大小