星火链网数字证书可信数据集规范

1. 摘要

本文介绍星火链网上可信数据集的协议标准和设计。

2. 原理

可信数据集由管理员进行维护和管理，往往通过智能合约的形式进行，系统初始化时写入管理员列表，维护管理员数据。可信数据集维护发证方、证书模板、吊销证书等模块。证书发证方通常为权威机关，可以通过密码学技术签名来进行数字证书的颁发。发证方提供标准的证书模板，方便发证方和插件钱包对证书进行格式化处理，插件钱包根据模板信息提交发证申请。发证方提交吊销的数字证书保存到可信数据集中，维护证书的吊销变更状态。

3. 规范

可信数据集合约包含执行接口函数、查询接口函数、合约入口。根据不同的业务请求调用不同的执行接口，调用过程会创建不同的交易日志数据整理交易的数据并对外反馈合约数据。插件钱包可以通过查询接口查看合约内的数据信息。

可信数据集合约需要对参数进行校验，保证数据的安全性。

3.1 交易日志定义

在执行发证方注册申请、审核等交易操作时，会触发交易日志（也可以称为'事件'。详情请见各函数说明），调用tlog接口，在区块链上记录一条交易日志，该日志记录了函数调用详情，方便用户阅读。

tlog定义如下:

```
tlog(topic, args...);
```

变量	类型	描述
tlog	function	会产生一笔交易写在区块上
topic	String	日志主题，必须为字符串类型,参数长度(0,128]
args	String[]	可变参数，最多可以包含5个参数，参数类型可以是字符串、数值或者布尔类型,每个参数长度(0,1024]

3.2 业务接口

3.2.1 发证方注册

企业机构使用自己的bid向可信数据集合约进行发证方的注册，提供发证方的资质数据、服务endpoint等信息。管理员对发证方资质验证后对注册申请进行审核操作。

```
    /**
     *  发证方注册申请.
     * @param params-发证方企业和服务信息.
     */
    function issuerApply(params)
```

请求参数

```
{
    "endpoint":"",
        "website":"",
        "companyName":"",
        "publicKey":"",
    "desc":""
}
```

- endpoint：发证方提供发证服务的URL。
- companyName：公司名称。
- publicKey：企业bid公钥。
- website： [选填]企业网站，用于审查企业数据
- desc： [选填]注册描述。

交易日志

```
tlog('issuerApply', applyNo,bid,endpoint,companyName);
```

- applyNo: 注册申请编号（合约内唯一）。
- bid: 发证方bid。
- endpoint：提供凭证服务的URL。
- companyName：公司名称。

3.2.2 模板申请

发证方根据业务需要创建证书模板，向可信数据合约发送创建申请。

```
    /**
     *  注册审核.
     * @param params-申请ID等信息.
     */
    function templateApply(params)
```

请求参数

```
{
        "templateId": "",
    "templateName":"",
    "industryId":"",
        "certType":"",
        "userType":"",
    "version":"",
        "remark":"",
      "vcFormat": "",
      "applyFormat": ""
}
```

- templateId: 模板唯一key。
- templateName：模板名称。
- industryId：行业分类。参考行业分类
- certType：证书类型。参考证书类型章节
- userType：面向用户类型。1-个人，2-企业
- version：版本。
- remark：[选填]备注。
- vcFormat：凭证元数据模板结构。jsonld context字符串数据，如以下结构：

  ```
  [{
      "format": "",
      "label": "",
      "key": "",
      "desc": ""
    }, {
      "format": "",
      "label": "",
      "key": "",
      "desc": ""
    }
  ]
  ```

  属性为如下结构：

  - key：属性的关键字。
  - format：关键字的类型。包括String、int、boolean等
  - label：关键字标签。
  - desc：其它描述。
- applyFormat：凭证申请数据模板结构。同上vcFormat的属性结构、

交易日志

```
tlog('templateApply',applyNo,issuerBid,templateId,templateName);
```

- applyNo:　模板创建申请编号。
- issuerBid:　发证方bid。
- templateId:　模板唯一key。
- templateName：模板名称。

3.2.3 吊销数字证书

发证方对需要吊销的数字证书进行吊销处理，吊销处理结果保存在可信数据集中。

```
//吊销数字证书
function revoke(params);
```

请求数据

```
{
      "credentialId":"",
      "reason":""
}
```

- credentialId:　证书id。参见星火链网可信数字证书颁发规范-证书申请状态查询获取证证书，或者直接从证书原文得到。
- reason：[选填]原因描述。

交易日志

```
tlog('revoke',issuerBid,credentialId,reason);
```

- issuerBid:　发证方bid。
- credentialId:　证书id。
- reason:　原因描述。

3.3 管理接口

3.3.1 审核发证方

管理员对发证方资质验证后对注册申请进行审核操作(待审核数据在发证方注册交易日志获取)。审核成功后，可信数据集合约会调用DDO合约创建发证方bid文档信息(企业)。

```
    /**
     * 审核发证方注册申请.
     * @param params-审核数据.
     */
    function approveIssuer(params)
```

请求参数

```
{
        "applyNo":"",
        "status":""
}
```

- applyNo: 申请编号（合约内唯一）。
- status: 0不通过，1通过。

交易日志

```
tlog('approveIssuer', applyNo,status);
```

3.3.2 审核模板

管理员对模板申请进行审核操作。

```
    /**
     * 审核发证方注册申请.
     * @param params-审核数据.
     */
    function approveTemplate(params)
```

请求参数

```
{
        "applyNo":"",
        "status":""
}
```

- applyNo: 申请编号（合约内唯一）。
- status: 0不通过，1通过。

交易日志

```
tlog('approveTemplate', applyNo,status);
```

3.3.3 吊销发证方

管理员对可信数据集中的发证方信息记录进行吊销操作，更新发证方的状态。

```
    /**
     * 吊销发证方.
     * @param params-发证方bid信息.
     */
    function revokeIssuer(params)
```

请求参数params

```
{
        "issuerBid":"",
    "reason":""
}
```

- issuerBid:　发证方bid。
- reason：[选填]吊销原因。

交易日志

```
tlog('revokeIssuer', issuerBid,reason);
```

3.3.4 吊销模板

管理员对可信数据集中的模板信息记录进行吊销操作，更新模板的状态。

```
    /**
     * 吊销模板.
     * @param params-模板信息.
     */
    function revokeTemplate(params)
```

请求参数params

```
{
        "templateBid":"",
    "reason":""
}
```

- templateBid:　模板bid。
- reason：[选填]吊销原因。

交易日志

```
tlog('revokeTemplate', templateBid,reason);
```

3.3.5 更新管理员列表

管理员可以更新管理员列表数据，增加或减少管理员列表。

```
    /**
     * 更新管理员.
     * @param params-管理员列表信息.
     */
    function updateManagers(params)
```

请求参数params

```
{
   "params": {
        "managersList":[]
   }
}
```

- managersList: bid数组， 管理员列表。

交易日志

```
tlog('updateManagers', managersList);
```

3.4 查询接口

3.4.1 查询发证方

查询发证方在可信数据集中的信息。

请求数据示例

```
{
  "method": "queryIssuer",
  "params": {
    "bid": "did:bid:2zNUZJ3bd97WJZ1Wv67axYB67W9cp8M"
  }
}
```

- bid: 发证方bid。

返回数据

```
{
  "bid":"",
    "endpoint":"",
    "website":"",
    "companyName":"",
    "publicKey":"",
    "auditBid":"",
    "status":"",
    "desc":""
}
```

- bid：发证方bid。
- endpoint：提供凭证服务的URL。
- website：企业网站，用于审查企业数据
- companyName：公司名称。
- publicKey：企业bid公钥。
- auditBid: 审核管理员bid。

- status：(1待审核 2已通过 3未通过 4已吊销)
- desc：注册描述。
- reason：被吊销的原因。

3.4.2 查询模板数据

查询验证方在可信数据集中的信息。

请求数据示例

```
{
  "method": "queryTemplate",
  "params": {
    "bid": "did:bid:2zNUZJ3bd97WJZ1Wv67axYB67W9cp8M"
  }
}
```

- bid:　模板bid。

返回数据

```
{
    "issuerBid": "",
      "status": "",
    "templateName":"",
    "industryId":"",
        "certType":"",
        "userType":"",
    "version":"",
        "remark":"",
      "vcFormat": "",
      "applyFormat": ""
}
```

- issuerBid:　发证方bid。
- status：(1待审核 2已通过 3未通过 4已吊销)
- templateName：模板名称。
- industryId：行业分类。
- certType：证书类型。
- userType：面向用户类型。
- version：版本。
- remark：备注。
- vcFormat：凭证元数据模板结构。
- applyFormat：凭证申请数据模板结构。

3.4.3 查询证书吊销状态

查询证书在可信数据集中的吊销信息。

请求数据示例

```
{
  "method": "queryCredentialRevokeStatus",
  "params": {
        "issuerBid": "",
    "credentialId": "did:bid:2zNUZJ3bd97WJZ1Wv67axYB67W9cp8M"
  }
}
```

- issuerBid: 发证方bid。
- credentialId: 证书bid。

返回数据

```
{
    "status": ""
}
```

- status: 0未吊销1已吊销。

3.5 合约开发

参考星火链网javascript合约开发。其中init、main、query接口由以下定义：

3.5.1 init

合约的初始化函数，创建合约时填入参数调用。初始化管理员列表

```
function init(input)
```

初始化参数input

```
{
   "params": {
       "managersList":[]
   }
}
```

- managersList: bid数组， 管理员列表。

交易日志

```
tlog('init', managersList);
```

3.5.2 main

合约执行的入口函数.。包含业务接口和管理接口

3.5.3 query

执行合约数据查询操作。包含查询接口

4 附录-类型码表

4.1 证书类型

值	描述
201	可信认证
202	学历认证
203	资质认证
204	授权认证
...	待扩展

4.2 行业分类

值	描述
A	农、林、牧、渔业
B	采矿业
C	制造业
D	电力、热力、燃气及水生产和供应业
E	建筑业
F	批发和零售业
G	交通运输、仓储和邮政业
H	住宿和餐饮业住宿和餐饮业
I	信息传输、软件和信息技术服务业
J	金融业
K	房地产业
L	租赁和商务服务业
M	科学研究和技术服务业
N	水利、环境和公共设施管理业
O	居民服务、修理和其他服务业
P	教育
Q	卫生和社会工作
R	文化、体育和娱乐业
S	公共管理、社会保障和社会组织
T	国际组织