



**北京航空航天大学**  
B E I H A N G U N I V E R S I T Y

**第二十八届“冯如杯”学生学术科技作  
品竞赛项目论文**

**物品租赁合同的可信化部署**

——基于区块链和自然语言处理的智能合约自动生成

## 摘要

纸质合同不能适应现代社会的需要，区块链智能合约正在开启一个新的时代……

隔着屏幕的陌生人间租赁还是有很多不确定性，租赁平台第三方的合法性、公正性让人不敢轻易尝试，人工的财产划分也带来了不少损失，租赁流程的透明度不高，司法上交易举证的模糊性使矛盾双方不能达成共识，给推卸责任拒不履行者带来了可乘之机……

租赁是永恒的话题，但租赁机制亟待完善！

本次开发选取物品租赁文本合同的可信部署这一应用场景，演示智能合约客观、提高工作效率和区块链的去中心化和信息不可篡改等多种安全性能保障财产分割安全性等技术优点，优化已有 NLP 技术模型，并自创适用于合同处理的 nlp 算法自动生成 java 智能合约代码并部署到区块链上实时监督交易流程、利用协议和用户接口自动执行合同内容、实时记录行为轨迹，从而保障租借交易安全性、便利性。

开发一个更安全可信、更自动化、更便利的物品租赁平台，是大众的期待，有助于绿色消费观念的养成。更用自动化的视角重新审视了这个时代。

关键词： 智能合约 区块链 自然语言处理 物品租赁

## Abstract

Paper contracts cannot adapt to the needs of the modern society. Blockchain smart contracts are opening a new era...

There is still a lot of uncertainty in the renting of strangers across the screen. The legitimacy and impartiality of third-party leasing platforms make it difficult to try them easily. The artificial property division also brings a lot of losses. The transparency of the leasing process is not high. The vagueness of the evidence in the judicial transaction makes it impossible for the two parties to reach a consensus, which has brought opportunities to the shirk of responsibility and refusal to perform...

Leasing is an eternal topic, but the leasing mechanism needs to be improved!

The application scenario of developing a trusted deployment for the lease document contract of this article demonstrates technical advantages such as the objective of smart contracts, improved work efficiency, decentralization of blockchains, and the inability to tamper with information and other security features to ensure asset segmentation security. Introduce Jieba segmentation, doc2txt, and Stanford Parse, and create an nlp algorithm for contract processing to automatically generate java smart contract code and deploy it to the blockchain to supervise the transaction flow in real time, use the protocol and user interface to automatically execute the contract content, real-time recording The trajectory of the behavior ensures the security and convenience of the lease transaction.

The development of a safer, more reliable, more automated, and more convenient platform for the leasing of goods is the public's expectation and contributes to the development of green consumption concepts. We have re-examined this era with an automated perspective.

### Keywords:

Smart Contract    Blockchain    Natural Language Processing    Item Rental

## 目录

第一章 项目简介.....	3
（一）主要创新点.....	3
（二）项目背景.....	3
（三）区块链合约部署工具开发框架.....	6
第二章 工具主要功能介绍.....	6
（一）合同订制.....	6
（二）代码自动生成.....	6
（三）交易流程详解.....	7
第三章 技术选型.....	9
（一）自然语言处理.....	9
（二）智能合约的生成.....	12
（三）智能合约接入区块链.....	14
（四）Pyqt 5——用户界面简洁、功能集中.....	21
（五）开发初期本地测试工具.....	22
第四章 工具开发设计和方案修正过程.....	23
第五章 工具使用范例.....	25
第六章 改进方向.....	36
第七章 当前工具应用待解决的问题.....	36
结论.....	37
附录.....	37
参考文献.....	43

## 第一章 项目简介

### （一）主要创新点

1、优化已有 NLP 技术，处理合同文本并生成关键字列表。针对租赁合约的撰写特性优化自然语言处理技术，实现个性化定制；

2、据合约逻辑编写可自动运行的 JAVA 代码。

3、在物品租赁财产分割方面智能合约与区块链相结合的具体应用展示。

NLP+智能合约+区块链=自动、安全、便捷的新时代！

### （二）项目背景

#### 1、区块链热门应用概况



图 1 区块链应用场景概览

目前天猫、京东都已经宣布将区块链技术运用在物流、商品等领域上。苏宁金融也建立了国内首个基于区块链技术的金融行业区块链黑名单共享平台。区块链使房屋交易产业链更现代化、智能化、可信化、可视化……

苏宁金融研究院高级研究员洪蜀宁说过，区块链的产生发展是有应用前景、有技术支撑、有成功先例的颠覆性技术革命，它的存在为社会的信任机制筑造了牢固的防火墙，

意义远超互联网。



图2 区块链现状

## 2、智能合约（链上代码）热门概况

凡是讲求诚信的地方，都是智能合约和区块链的舞台。

“代码即合约”，智能合约部署工具也是一种特殊的软件，蕴含法律关系和利益交易，有更复杂的关联，更高的可信要求。

智能合约是区块链未来发展的核心动力，展望未来，智能合约将是需要大规模生产和应用的服务软件。

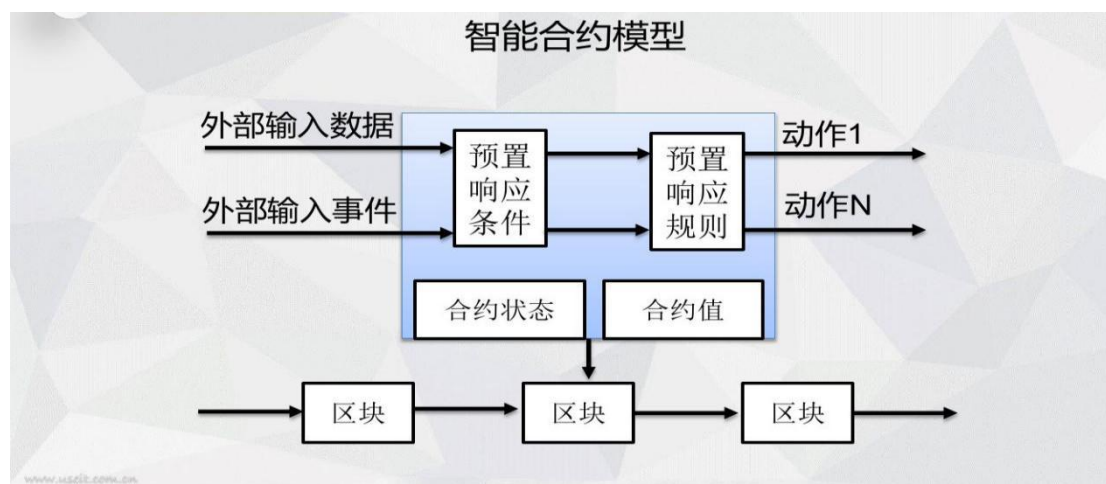


图3 智能合约模型

## 3、自然语言处理应用概况

NLP 的技术发展不断成熟，Dialogue 方面，自然语言对话开创一个新的人机交互时代；Open-domain QA 方面，MRC 取得的进展大家已经有目共睹；再看 Unsupervised

Learning 和 NLG 方面，通过 RNN-language model 来做语言生成已经很成熟了。

但即便如此，针对合约处理的自然语言处理需要具有自己的特点，需要做出个性化改进。

#### 4、合约隐患

作为租出方，除了人为运营的网站数据库外没有可信、无法篡改的证据证明自己发起了交易，作为租入方，也缺乏可靠的平台记录签订的租入合同内容，合约的执行、结束、惩罚都需要人为判别，金钱交易、合法权益难以得到安全保障。面对面签订的租赁合同撰写复杂、不够完善且很可能被损毁、恶意修改，记录合约内容和交易流程的证据随时被单方面控制甚至无处可查，这样的交易也就意味着层出不穷的隐患。

电子商务和现实租赁领域都做的不够完善，而引入区块链这一分布式账本后，在交易双方都确认的情况下生成不可删改的节点，使证据的控制权不在任何一方的手中，无疑是推动交易安全性的成功之选。

### （三）区块链合约部署工具开发框架



图 4 项目开发框架

## 第二章 工具主要功能介绍

### （一）合同订制

录入一份物品租赁合同内容的渠道有二：

①用户根据需要填写已有合同模板（如不填写的内容也有缺省值保证合同逻辑正常运行）

②用户个性化提交纸质合同，自然语言处理分析合同语言逻辑，捕捉关键信息待用户确认

以上如有异常用户可以提出异议并微调。

### （二）代码自动生成

合同关键信息（包括双方身份信息和合约信息字段）+据合约生成 JAVA 逻辑代码部署到区块链。

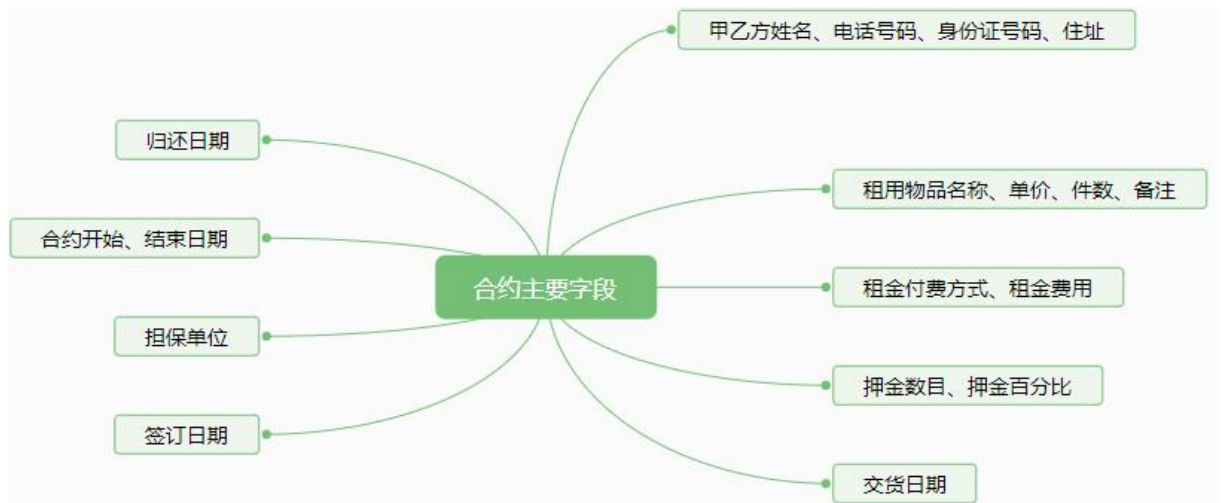


图 5 合约主要抽取字段

### （三）交易流程详解

用户注册→双方签订合同并确认→提取信息生成代码及合同部署→接收外部信息实时自动判定合同触发条件是否满足→执行相关交易操作（如自动转账）、返回相关信息并在区块链记录轨迹→交易结束用户可查



以上交易过程如报异常随时废止合同。

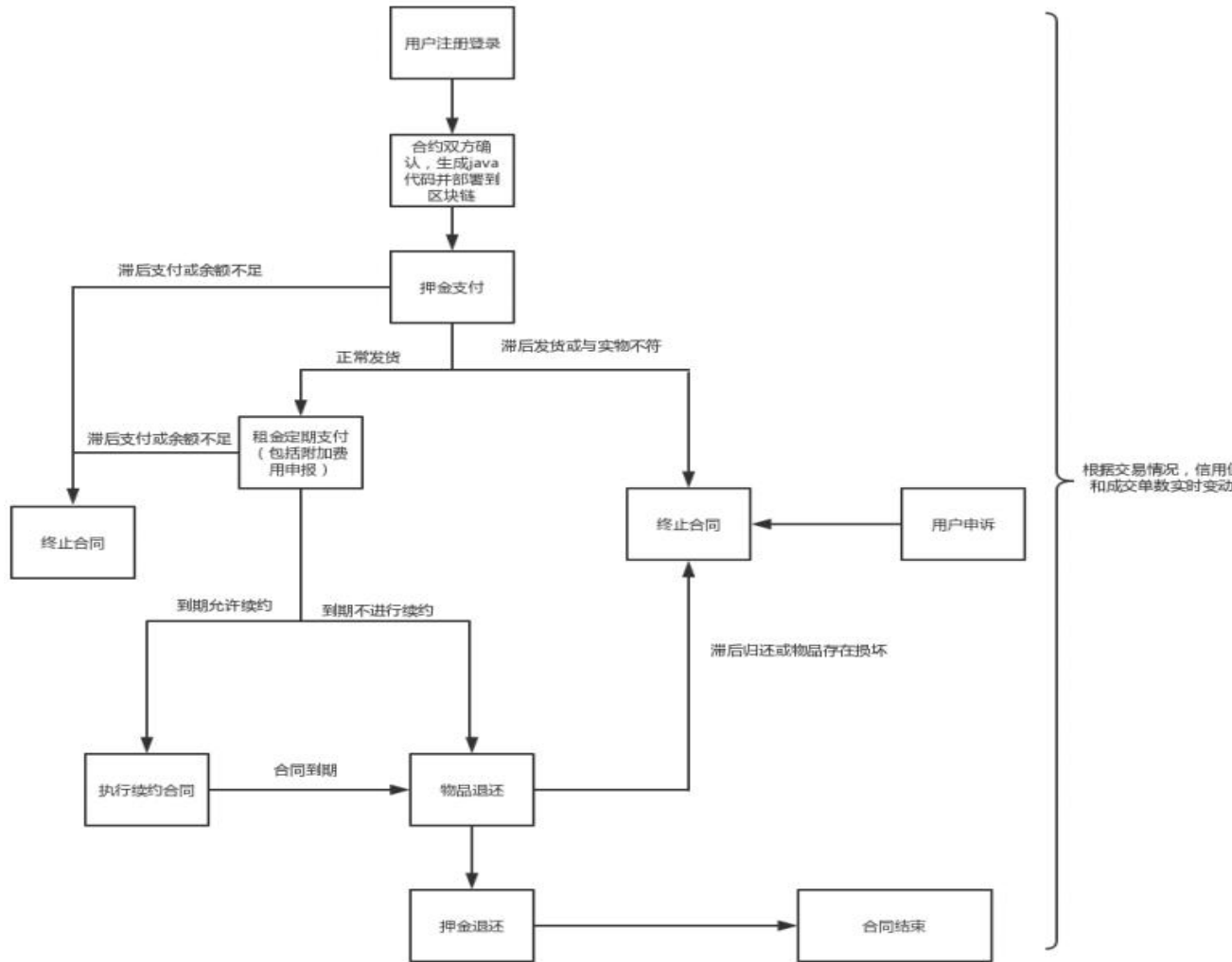


图6 智能合约的逻辑运行简图

## 第三章 技术选型



图 7 项目开发过程简介

### （一）自然语言处理

#### 1、已有 NLP 成果升级优化

租赁合同文本通常具有表述明确的特点，所以许多事实描述都可以使用自然语言处理的方法提取出来，语言模型的结构和组成成分直接地、明显地表示出来，但租赁合同对财产分配的逻辑表达比较复杂，所以需要在现有的自然语言研究成果基础上继续优化、为租赁合同个性化订制信息抽取方法。

语料的准备过程采用精确模式的分词技术。数据清洗前从权威词库上按合同领域的对应主题获取出词条并整理形成词典，经验证可以适用于 80%以上的合同文本，在此基础上依旧可以自定义词典来适应更为精细的用户使用场景。

使用基于统计学的经验主义分析方法训练语言学数据，并自动或半自动地从训练的语言学数据中获取语言统计学知识，可以有效地建立语言统计学模型。这种方法在自动提取合约文本方面效果很好，并且在借助 Stanford Parser 进行句法自动分析和词语消歧时也表现良好。

自然语言处理是智能合约的基础，我们通过对自然语言形式的合同文本的处理，采用同义词多分类检索与匹配技术，运用于复杂合约文本相近语义关键词提取，使之自动部署到区块链上，提高了信息抽取的效率与准确度。同时，可自定义的多维用户词典更加适应用户的实际使用场景，提高了信息检索的效率，且编码的同一性支持多重语言分

析处理。

## 2、项目团队设计适于处理租赁合约的个性 NLP 算法

对于合同文本的自然语言处理，我们设计了一套自己的 nlp 算法，该算法大致分为以下几个步骤：

### 2.1 提取用户填写内容

我们发现，在正式合同中，为便于用户填写，每种合同模板都会需要在需要填写位置预留下划线，如“甲方：\_\_\_\_\_”，在用户填写后，该位置变为“甲方：\_\_\_\_智能问诊项目组\_\_\_\_”，根据这一特点，我们通过对合同中的下划线进行匹配，即可获取用户所填写的内容。

### 2.2 获取用户所填内容的类别

在获取到用户填写的内容后，我们需要知道用户填写内容的类别，比如“甲方：\_\_\_\_智能问诊项目组\_\_\_\_”中，用户填写内容为“智能问诊项目组”，内容类别为“甲方”。为实现这一功能，我们使用了 TF-IDF 算法结合 jieba 分词的词频统计对关键词进行提取，在结合测试结果对词频进行微调、去停用词等一系列优化后，关键词提取正确率已超过 90%。

由于 TF-IDF 算法提取关键词后，会返回词频由高到低的一系列词语，在测试中我们发现，我们需要的关键词一定会出现在返回的前三个词语中，所以当用户对自动提取得到的关键词不满意时，还可以手动从这三个词语中选择关键词，同时我们也会根据用户的选择在后台自动对词频进行微调，以提高今后关键词提取的准确性。

### 2.3 获取除用户填写内容外的其他可能关键词

获得其他可能关键词的原理与获得用户所填内容的类别的原理相近，都是通过 TF-IDF 算法结合 jieba 分词的词频统计功能对关键词进行提取，用户可选择性的使用这些关键词。

### 2.4 责任方归属问题的处理

在获得关键词后，可能会由于责任方不明而产生歧义，如“合同签订后，甲方向乙方缴纳\_原物品价值的\_百分之\_5\_（视为 100）作为押金。”，可能会导致用户不知道“缴纳”这一行为是谁向谁进行的。为解决这一问题，我们进行了句法分析，算法基于 Stanford Parser 实现，目前正确率可达 80%，用户同样可以手动对处理结果进行选择，同时我们会根据用户选择自动进行优化。

## 2.5 处理效果展示

经过 164 份合约的整体性测试，所有使用给定模板的合约都可以正确部署执行，信息提取正确、财产分割无错。平均正确率达到 80.4%。

形式规整、表意浅显、逻辑具有普适性的合约类型基本都能保证财产的正确分割和交流流程详细记录。

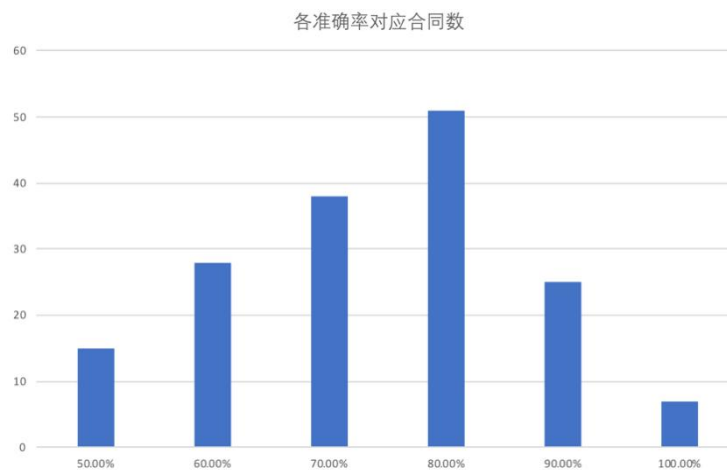


图 8 测试合同的准确率统计

合约举例：（测试用完整合约在附录）

## 物品租赁合同

甲方向乙方租用物品，有关事项经甲乙双方协商后达成如下协议：

甲方（租赁方）

姓名：\_李四\_

电话号码：\_16922833103\_

地址：\_北京市海淀区学院路 37 号对面\_

身份证号码：\_131181199901013523\_

乙方（承租方）

姓名：\_老王\_

电话：\_377481223\_

地址：\_北京市海淀区五道口男子技术学院\_

身份证号码：\_1000000000003213123\_

甲乙双方同意按照下列条款签订本租赁合同(以下简称“合同”)以资共同遵守：

### 第一条 合同依据和租赁物件

1.甲方根据乙方上级主管部门的批准并根据乙方租赁委托书的要求，租赁物件的名称、规格、型号、数量和使用地点详见本合同附表第 1、5 项，该附表为本合同不可分割的组成部分。

2.租赁物品信息：

名称：\_笔记本电脑\_

单价：\_9000\_元

件数：\_1\_ 件

备注：\_本物品为惠普笔记本电脑\_

图 9 待处理合约第一页

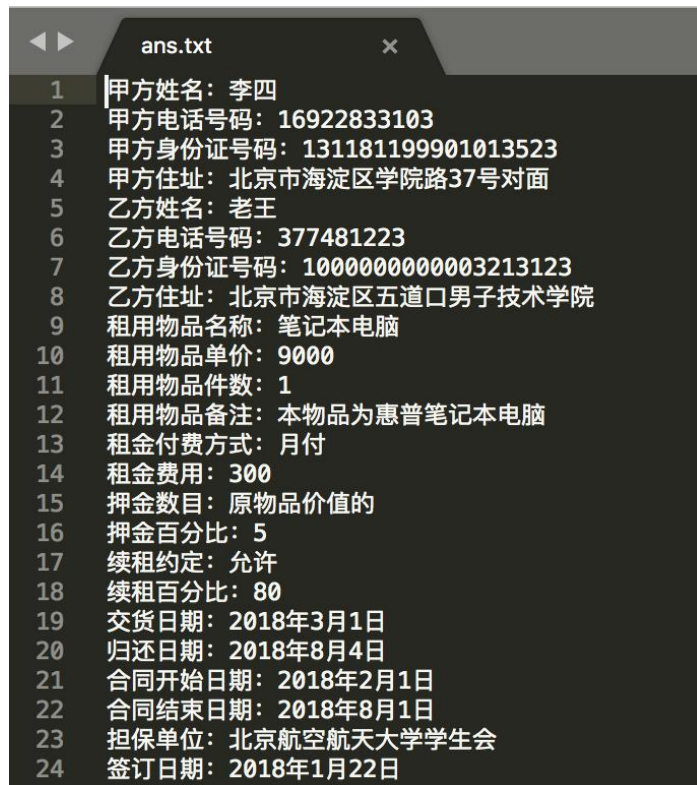


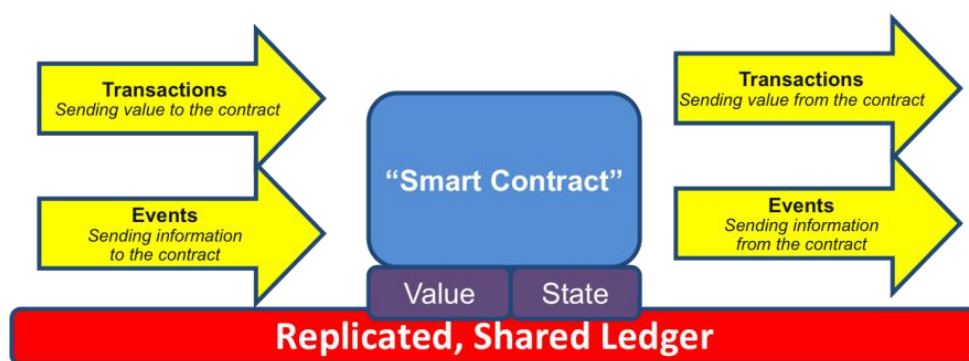
图 10 在 txt 中显示关键词的提取效果

## （二）智能合约的生成

智能合约实质上是基于区块链的合约签订双方都确认执行的资产分割代码。一旦区块链记录了合约代码，合约就不会被更改。代码根据接收到的外界信息和规定好的合约条款实时对比，在恰当的时机执行约定的动作，具有强制性。

合约状态的改变不是由单点决定的，而是由多个节点一起决定的，保证了合约执行的可验证性与可信性，从而可以省去第三方监管的费用。

因为有了智能合约，数字货币的交易被重新注入了生机。



本题就是将现实中的合约逻辑转化为 JAVA 代码部署到区块链上，同时保证授权公开和私人信息加密机制，使合约顺应现代社会的特点，在双方确认的情况下排除人为干扰，保障财产转移安全性、防止恶意篡改、增强了交易可信度。

## JAVA代码

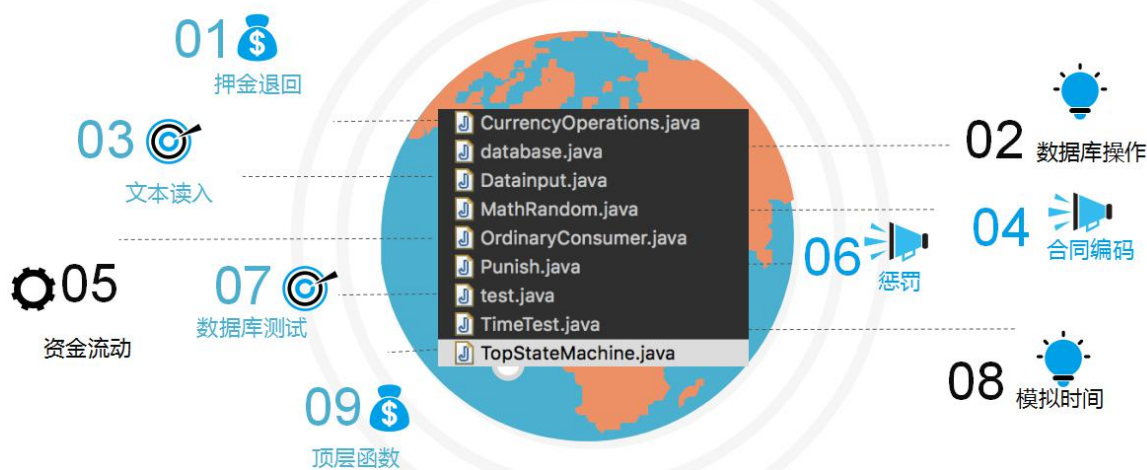


图 12 JAVA 代码

### （三）智能合约接入区块链



图 13 区块链和智能合约的关系结构简图

#### 1、为什么选用区块链

- 1.1 不管是网络世界还是现实生活，我们都难免会遇到信任危机
- 1.2 行业之间的信息通达率不高，信息传递和转移降低了工作效率
- 1.3 私人信息易泄露，权限意识差
- 1.4 历史信息易被单方控制篡改，约定无保障

#### 2、区块链特点

##### 2.1 安全性——不易篡改、很难伪造、可追溯。

分布式数据存储、点对点传输、共识机制、加密算法

• 块链结构：经典的时间戳设计，块和块之间含有哈希加密信息，每次交易信息都能得到确认。

• 多独立拷贝存储：节点都互为备份，节点间信息可以用于互相考证。

• 拜占庭容错：信息只要被记录并加入区块链就会受到保护，永久存储。采用投票机制，只要有少于三分之一的节点被破坏，就可以通过这种印证机制容错，保证存储信息查询结果的正确性。

只有“增加”和“查询”两个操作，数据修改和变更，通过添加新的交易记录来实现。因为账本只会越来越长而不是可以涂改，交易数据的安全性就得到了保障，数据的恶意修改成为不可能。

作为记账本，区块链每经一段周期会将全网内的交易记录按时间顺序打包在一起。

交易数据一致性检验是区块链的特色，完整性验证功能也为交易提供了有力的保障。修改就会被“巡逻的警察”发现通过密码验证实现，各节点中的数据是否具有 consistency 特征用哈希表即可验证，交易全程产生的所有交易数据用节点记录。默克尔树的结构杜绝



了交易信息的恶意篡改， 犯罪检测通过验证到树根路径上的哈希值完成。

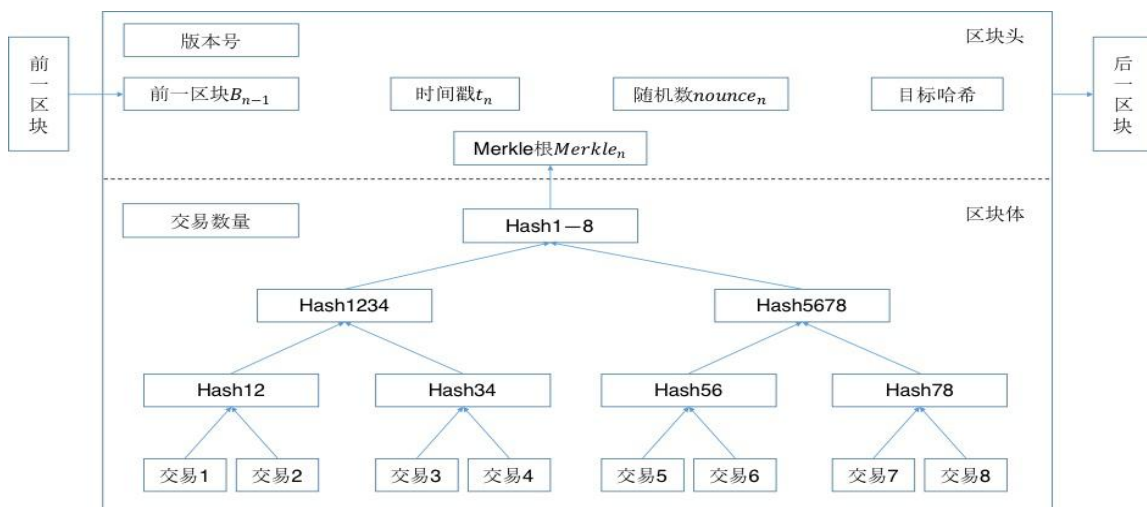


图 14 区块内部结构简图

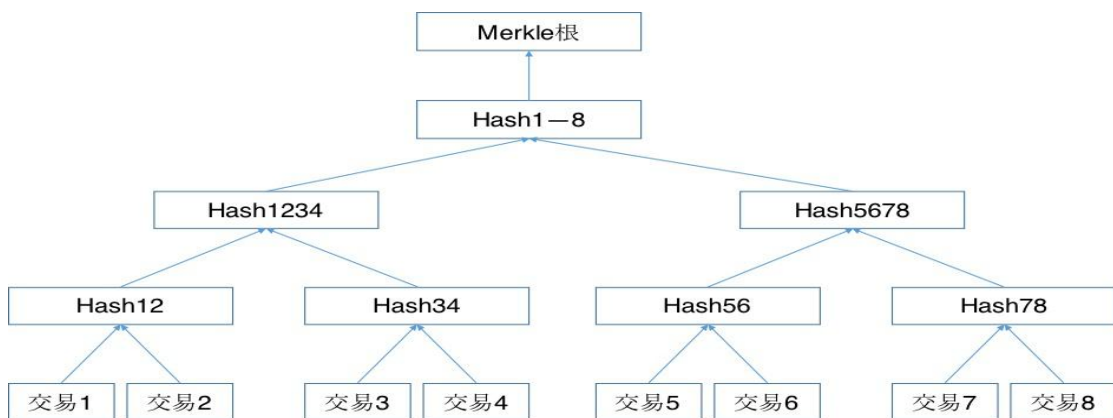


图 15 默克尔树

## 2.2 合理的开放性

适当的系统信息透明，同步、公开，有利于拓展市场，私密信息权限保护。

非对称加密和授权使得交易信息半开放，交易各方的私有信息被加密，其他人不可见，除非用户授权，行业间的有用信息可以有选择的被公开。





图 16 公共总账本链的查看

### 2.3 去中心化，匿名可信

中心化通过分布式核算和存储的方式杜绝。系统由多个节点共同维护，权利的一致性使公平、可信成为可能。

信息交换遵循固定算法，程序规则会自动判断行为的有效性，交易双方不必互相交换更多信息就可以满足可信性，产生的信用积累也是很有说服力的。

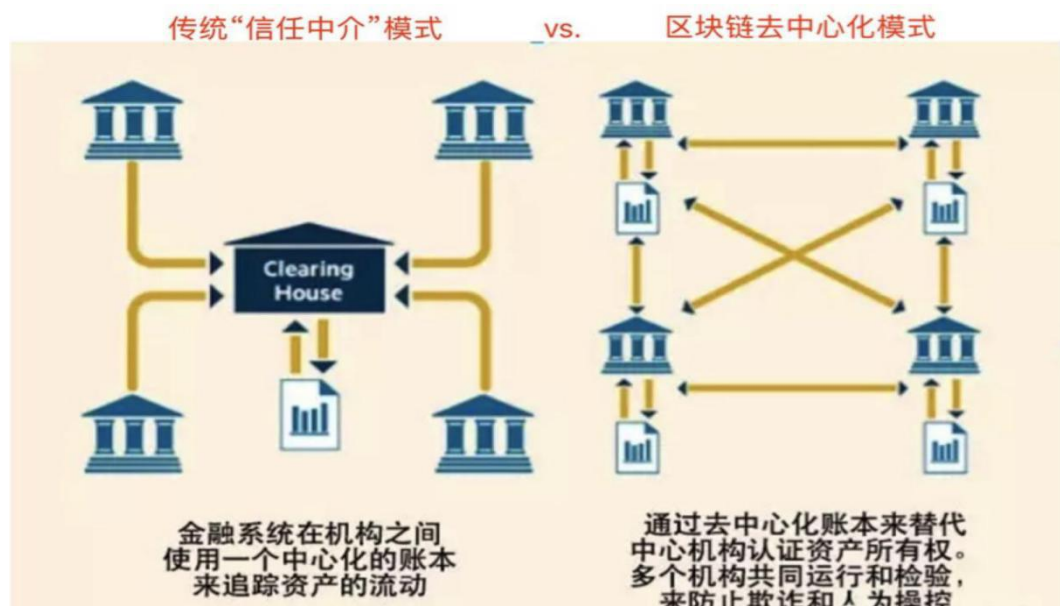


图 17 传统模式与区块链去中心化模式对比

### 2.4 高速性、一致性、可扩展性

区块链信息更同步、公开，有利于拓展市场。

每秒交易可达上万次，建立区块数可以达到多个，块的内部交易也数以万计。创建、上传、更新账户简便有效。

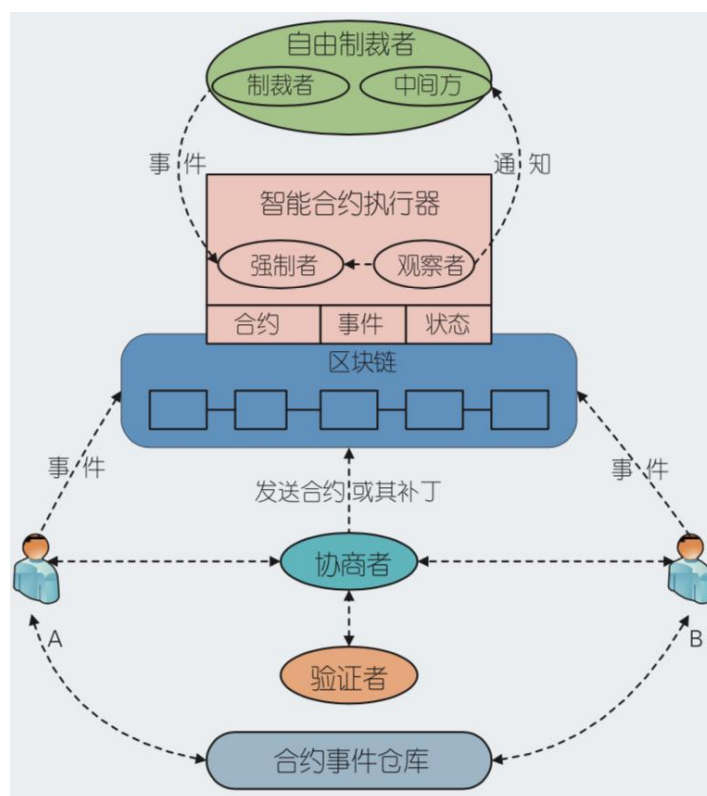


图 18 智能合约与区块链结合的运作模式

## 2.5 智能合约部署到区块链上的部分操作演示

区块链运营方提供对应字段的应用接口 OBCC, 可以使区块链之外的设计者使用区块链的功能畅通无阻, 比如说将交易约定和财产分割流程存入区块链、查询交易信息。put(action, data) 是写入的接口设计原型, action 代表数据操作方式, 包括创建(create)、插入(insert)、更新(update)或删除(delete)。data 包含真正的待存入数据, 为了适应不同的情境, 以上的格式和内容会稍作修改。get(condition) 是查询接口的原型, 信息查询的特征性条件和块的哈希值或交易的哈希值甚至应用有关的关键字都可以作为 condition 使用。倒排索引和大数据分析可以使高价值的查询结果反馈变得快速高效。

## 3、区块链可提供读写接口举例：（在工具优化扩展过程中根据需要随时增加）

Api 链接: <http://60.205.231.159:8080/BUAABlockChain-v0.1/v1/medService>

```

#存款到自己账户
def deposit():
    self.storage[msg.sender] += msg.value
    return(1)

#从自己账户中取款
def withdraw(amount):
#检查账户余额是否充足
    if self.storage[msg.sender] < amount:
        return(-1)
    else:
        #如果有足够的钱，则完成取款
        self.storage[msg.sender] -= amount
        send(0, msg.sender, amount)
        return(1)

#转移资金到别的账户中
def transfer(amount, destination):
    #检查是否有足够的资金
    if self.storage[msg.sender] < amount:
        return(-1)
    else:
        #如果有足够的资金，则完成转帐
        self.storage[msg.sender] -= amount
        self.storage[destination] += amount
        return(1)

#查询余额
def balance():
    return(self.storage[msg.sender])

```

图 19 简单的自动执行的区块链银行智能合约

#### 4、目前上传数据结构如下：（在优化过程中不断修改）

##### i. 写入区块链 API 简述：

字段	值	含义
type	Insert	上传操作
service_type	TradingContract	合约双方信息
service_type	auth	合约授权信息
service_type	transaction	交易记录
Id	任意字符串	代表交易合约唯一 id
content	Json 字符串数组	代表合约和交易流程财产分割情况的账本内容

例如上传 id 为“9527”合约交易记录，简单测试数据如下所示

```
{
  "type": "Insert",
  "service_type": "TradingContract",
  "id": "9527",
  "content": [
    "合约部署日 2018 年 1 月 1 日, 账户 pipilu 因支付押金转账给账户 luxixi 3000 元",
    "2018 年 1 月 7 日, 账户 luxixi 因支付车辆保养附加费用转账给账户 pipilu 1000 元",
    "2018 年 2 月 1 日, 账户 pipilu 因月付租赁费向账户 luxixi 支付 2000 元",
    "2018 年 2 月 16 日, 因本合约支持续租, 账户 pipilu 提出向账户 luxixi 续租 3 个月的请求通过, 合约结束时间由 2018 年 3 月 1 日改为 2018 年 6 月 1 日",
    "2018 年 4 月 8 日, luxixi 对自动扣费提出异议, pipilu 账户余额不足, 未按时支付租金, 合约结束"
  ]
}
```

**PLUS: 插入相同的数据两次, 若插入会显示成功, 但是查询会报错!**

**返回 json 串:**

```
{"result":["101","101","101"],"timestamp":0,"vote":[["101","101","101","101"],["101","101","101","101"],["101","101","101","101"]]}
```

字段	值	含义
result	Json 字符串数组	插入的最终结果, 数组第一个返回码代表第一个处方插入成功, 数组第二个返回码代表第二个处方插入成功, 一次类推
vote	Json 字符串数组	投票信息, 第一个数组代表四台机器对第一个处方的投票结果, 以此类推

**返回码以及含义:**

001: 合约部署成功 002: 合约代码失效 003: 合约执行错误 101: 新增成功 102: 新

增失败 201:查询成功 202:信息被篡改

#### ii. 从区块链里查询 API

查询合约双方信息、授权记录、交易记录，具有共识机制，可用于举证。

字段	值	含义
type	Query	查询操作
service_type	TradingContract	合约双方信息
service_type	auth	合约授权信息
service_type	transaction	交易记录
Id	任意字符串	代表交易合约唯一 id
content	Json 字符串数组	代表合约和交易流程财产分割情况的账本内容

查询测试用例，查询其中一条记录（查询一个记录 content 也要写成 json 数组的形式）：

```
{
  "type": "Query",
  "service_type": "TradingContract",
  "id": "9527",
  "content": [
    "2018 年 1 月 7 日，账户 luxixi 因支付车辆保养附加费用转账给账户 pipilu 1000 元",
  ]
}
```

查询结果：

```
{"result":["201"],"timestamp":0,"vote":[["201","201","201","201"]]}
```

### 查询测试用例，查询其中一个错误的记录

```
{
  "type": "Query",
  "service_type": "TradingContract",
  "id": "9527",
  "content": [
    "2018 年 5 月 1 日, 账户 pipilu 因月付租赁费向账户 luxixi 支付 2000 元",
  ]
}
```

### 查询结果，结果显示没有查到：

```
{"result":["202"],"timestamp":0,"vote":[["202","202","202","202"]]}
```

## （四）Pyqt 5——用户界面简洁、功能集中

GUI 整合了所有在线租赁的基本功能，同时将智能合约的进行过程完整的呈现给用户，给用户直观的租赁流程体验，同时它功能集中显示，简化用户操作，并给予大量提示信息，省去用户的麻烦与困扰。

智能合约本身是后台程序，普通用户无法对其进行了解，对它的真正运行情况更无从知晓，通过提示信息的方式，将后台程序的本质及运行过程表达出来，让用户通过能够理解的方式去接受并信任智能合约。

在编写 GUI 的过程中，出现的主要问题是与后台的衔接，因为编写语言的不同，导致程序之间的互相调用产生了很大困难，最后我们通过内部数据库的信息互换解决了这个问题。

## （五）开发初期本地测试工具

### 1、SQLite 数据库

#### 1.1 SQL 结构化查询语言

一种可以存储数据并且查询、更新和管理关系的数据库系统的经典语言。

## 1.2 使用 SQL 语句操纵 SQLite 数据库记录用户信息



图 20 SQLite 数据库的创建

## 2、Redis 数据库

用来模拟区块链的环境，超大量数据可以通过 Redis 数据库在 PC 服务器集群上处理，键值对的存储形式也有效满足了存储合同字段和前端信息修改的需求。

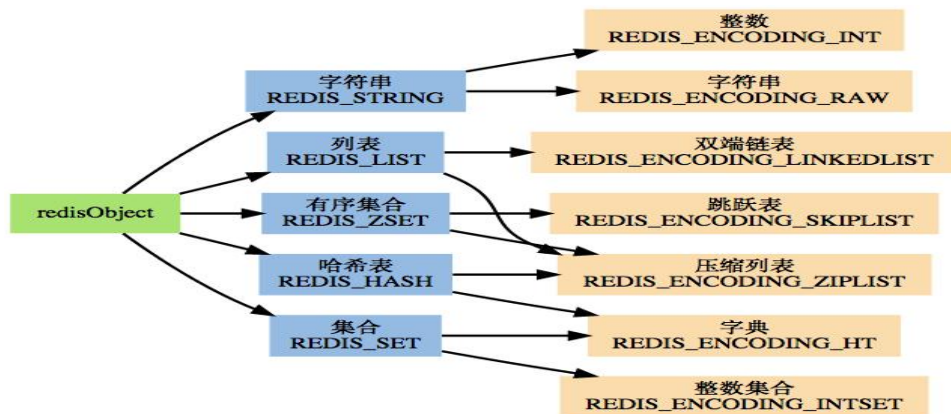


图 21 Redis 库存储类型

## 第四章 工具开发设计和方案修正过程

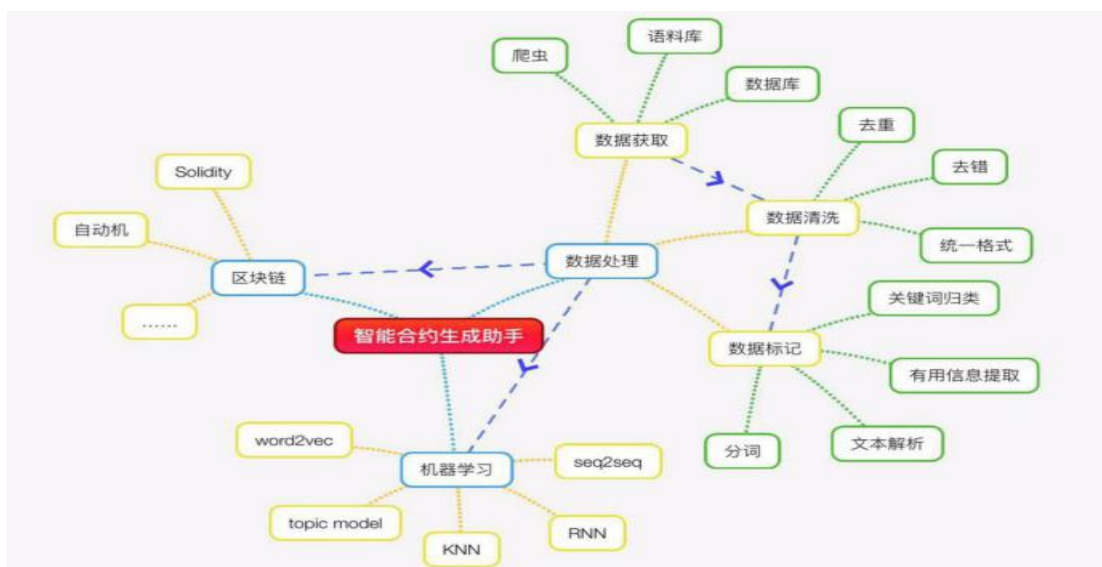


图 22 开发技术思维导图

### （一）阶段一：基于本地数据库测试的工具开发和优化

#### 技术难点与优化：

##### 1、数据处理方面：

Stanford Parser 对中文的句法分析效果差强人意，虽然目前准确率可达 80%，但仍然需要进行优化，提高准确度，减少用户的手动修正。

解决方案：对现有模型进行测试，优化其提取效果。

##### 2、代码函数设计方面：

函数设计时的字段比很多合同的实际字段数多，同时合约逻辑多变，需要在各种情况下保证后台函数运行正确。

解决方案：注意分析多种形式的合同的逻辑关系并在代码中分情况对应、注意函数缺省值的配置、虚拟货币的正确转移和实时记录等。

##### 3、本地数据记录方面：

SQLite 这种小型的嵌入式数据库虽然操作简洁、条理性强但存在锁的问题，即当前后台在实时交互的情况下需要不断同时读写时，由于本身没有提供复杂的锁定机制，无法高效地解决多路并发下的数据操作同步问题，所以在这种情况下外部进行读写锁控制



是必不可少的，否则 SQLite 会返回 SQLITE\_BUSY 错误拒绝相关请求，最后导致工具运行瘫痪。

```
org.sqlite.SQLiteException: [SQLITE_BUSY] The database file is locked (database is locked)
```

图 23 同时读写造成的锁库现象

解决方案：对适合建表存储且改动不大、不需要同时读写的用户注册信息保留 SQLite 库存储形式，为适合采用 key-value 存储的多变合约字段、前后台交互信息块选用支持同时读写而不锁库的 Redis 数据库。

#### 4、测试衔接方面：

智能合约上的代码都是自动触发的，且一般是无法阻止其运行的，合约代码中包含了资产的操作，如果逻辑上出错，会导致很严重的后果。而本工具涉及到的字段数多、信息量繁杂、变动性强、个性化高，不仅要三方面衔接起来，更要做到测试量大而全，找到全部细节问题。

解决方案：

先每两方面衔接，再三方面连接，发现问题并修改代码对接，消除技术断层。

函数运行需要对关键信息进一步的处理，基本功能函数的设计细化，对代码进行基于 excel 和数据库的信息输出比对、货币转移等功能追踪测试与改进。

对每个功能单独测试，测试途径有下载网上数据集、自创数据集和邀请其他用户试用该工具并予以反馈。

设计完备的用户查看信息和反馈机制，当用户提出异常时，合约废止功能被触发，区块链也会记录详细信息，作为日后可信举证。

#### 5、前后端交互方面：

跨平台、跨语言编程，变动信息共享受阻，实时信息交互成为难题。

解决方案：

在 Redis 数据库使用多个交互标记变量，设计“写信——收信——回复”机制，与信息变动一一对应。

## （二）阶段二：区块链部署——区块链存储和查询操作方法的调用

难点：首次接入区块链的代码适应修改工作比较繁杂，需要将之前在本地测试使用

的记录、查询代码删掉而不影响正常功能。且接入区块链后测试难度加大。

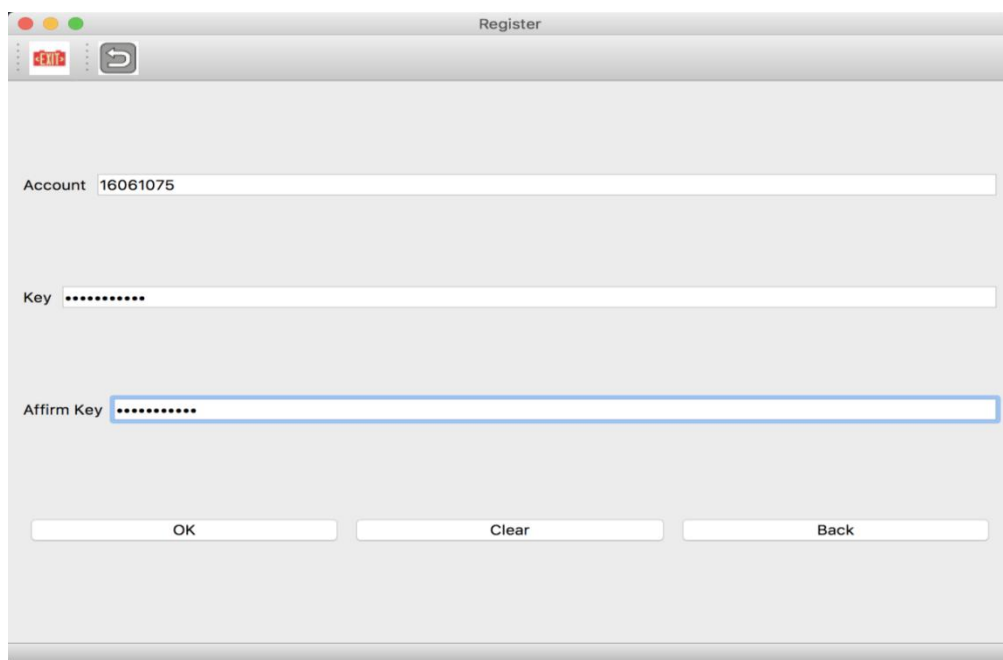
解决方案：在接入前进行大量测试保证代码改进代码生成独立有效且分布集中的区块链接口，调用方法将之前在数据库测试过的信息独立的存入区块链，再次全面测试接入区块链后工具功能的有效性。

## 第五章 工具使用范例

下面以界面图示介绍主要使用流程，值得注意的是，虽然用户界面体验和使用普通数据库的工具区别不大，但实际上信息块记录于不可更改的区块链，查找的信息源是区块链，信息更改并非修改数据库信息而是通过在区块链上增加一条记录完成。

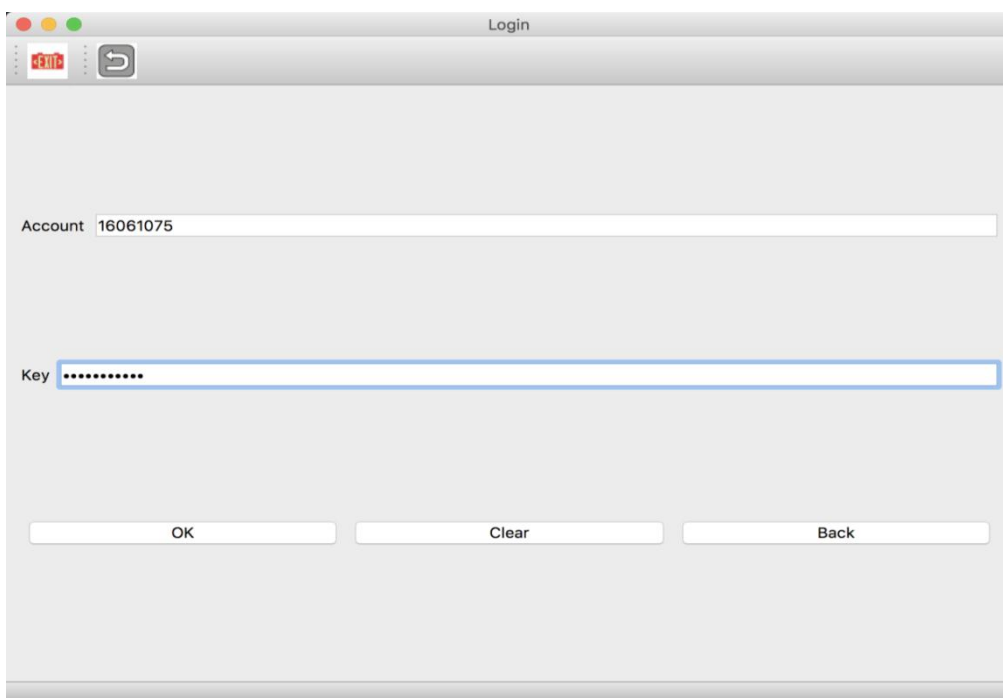


图 24-1 欢迎界面，用户可注册或登录



The screenshot shows a 'Register' window with a title bar containing standard Mac OS window controls (red, yellow, green buttons) and a toolbar with a red icon and a circular arrow icon. The main area contains three text input fields: 'Account' with the value '16061075', 'Key' with masked characters '.....', and 'Affirm Key' with masked characters '.....'. The 'Affirm Key' field is currently selected, indicated by a blue border. At the bottom, there are three buttons: 'OK', 'Clear', and 'Back'.

图 24-2 注册界面



The screenshot shows a 'Login' window with a title bar containing standard Mac OS window controls (red, yellow, green buttons) and a toolbar with a red icon and a circular arrow icon. The main area contains two text input fields: 'Account' with the value '16061075' and 'Key' with masked characters '.....'. The 'Key' field is currently selected, indicated by a blue border. At the bottom, there are three buttons: 'OK', 'Clear', and 'Back'.

图 24-3 登录界面



图 24-4 菜单界面，用户可选择查看账户的个人信息和在系统中的合同信息

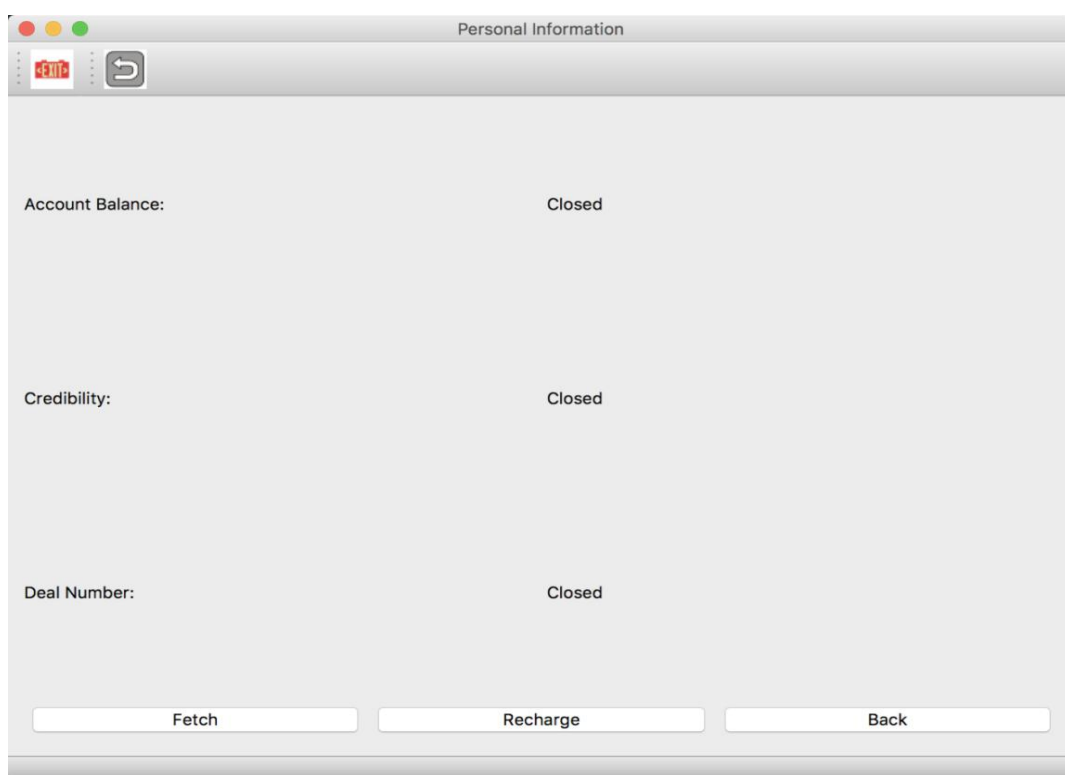


图 24-5 个人信息界面，用户可点击 Fetch 拉取区块链上的个人信息，可通过 Recharge 对账户进行充值

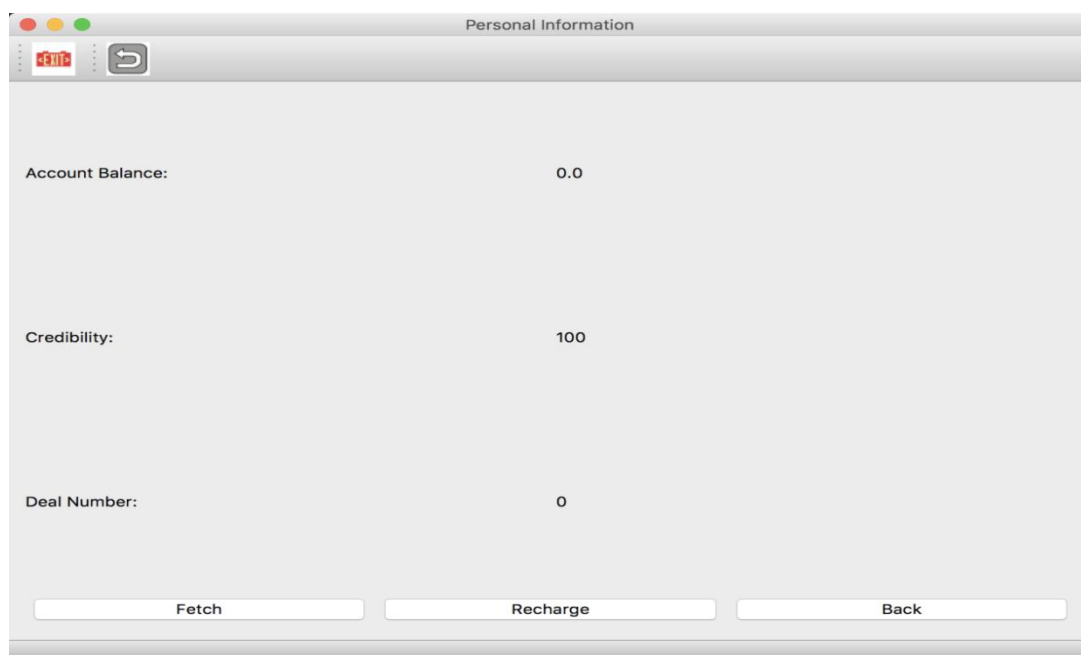


图 24-6 初始信息

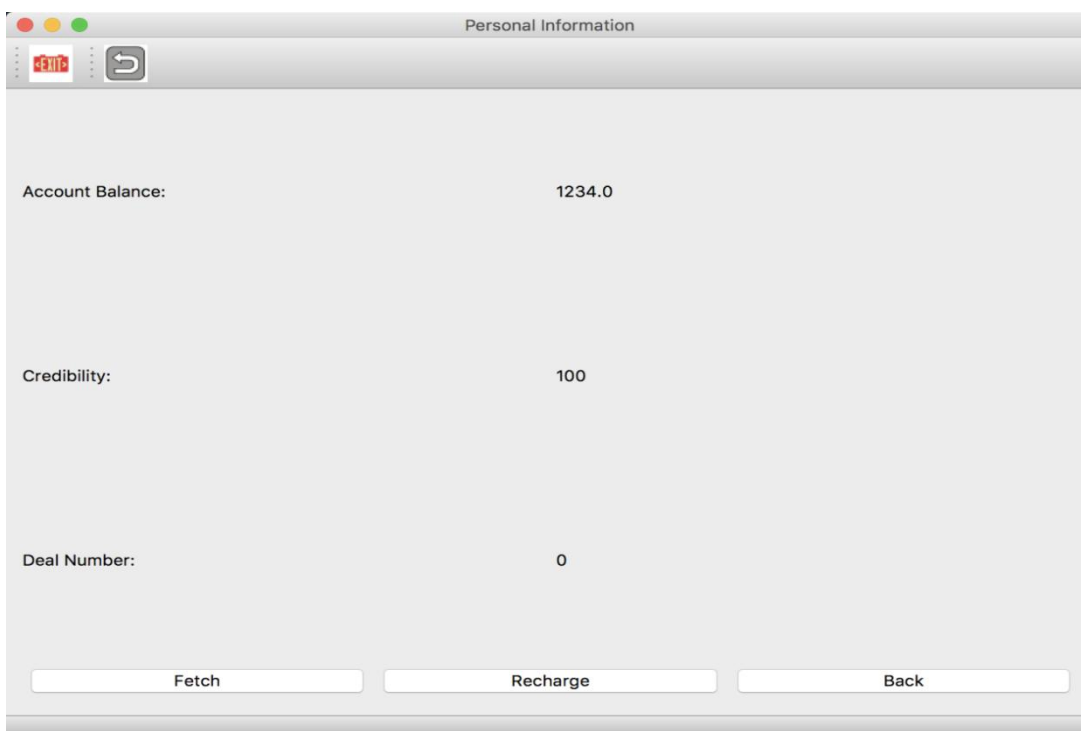
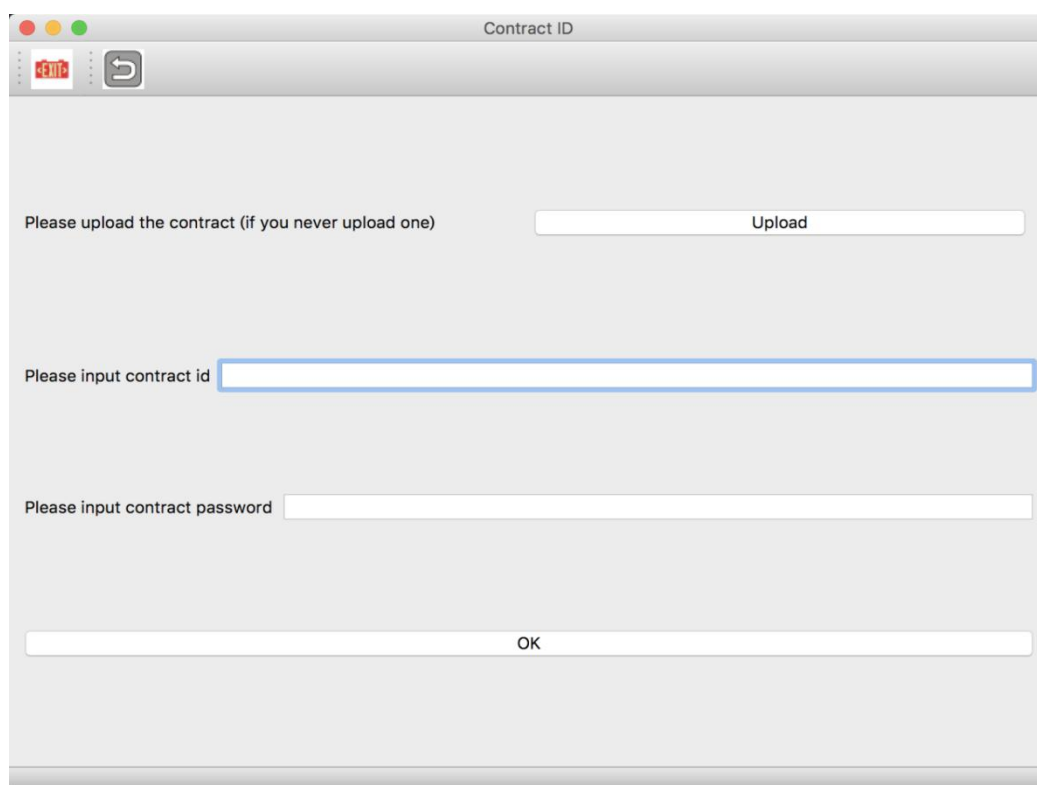
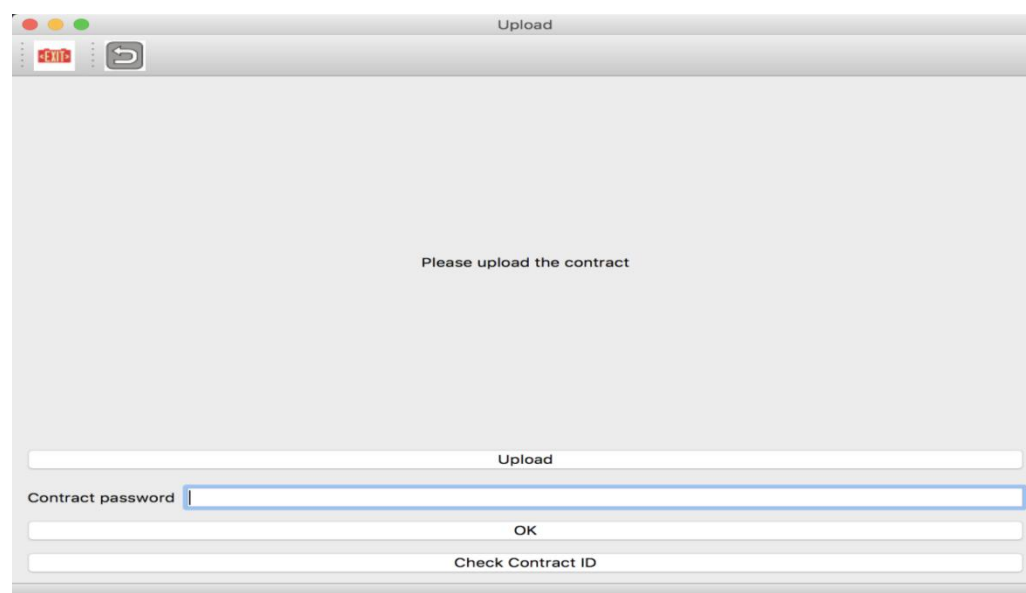


图 24-7 充值 1234 元后信息



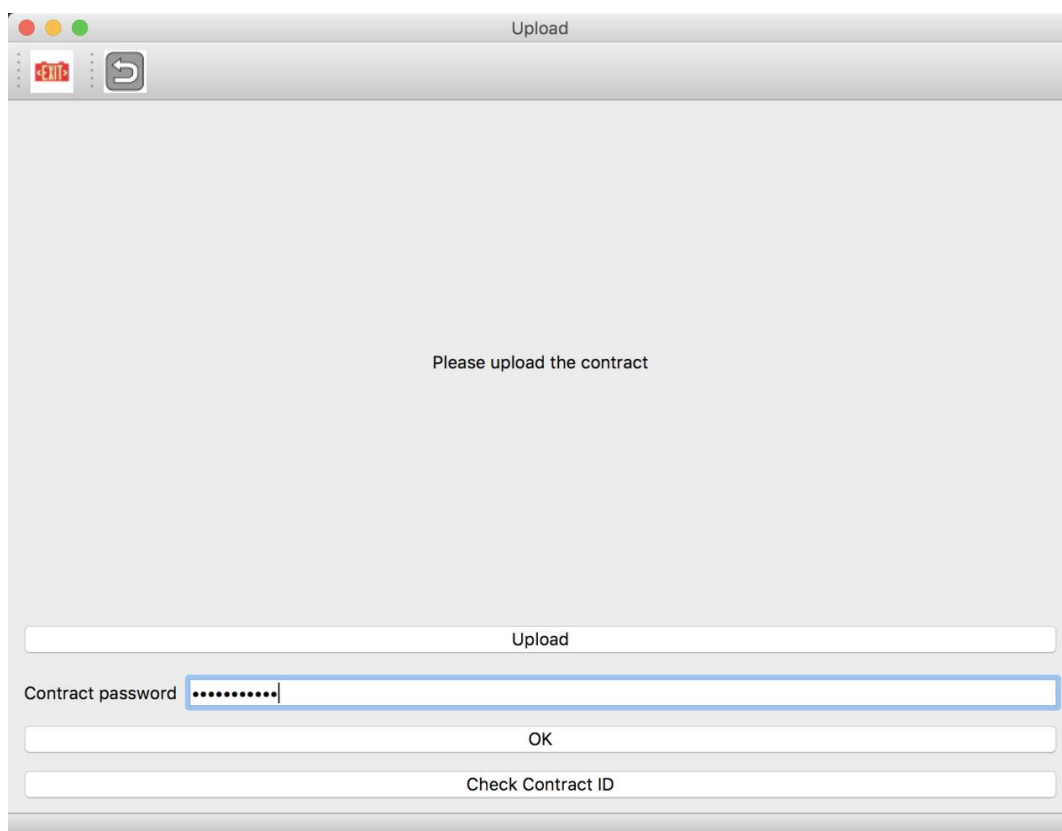
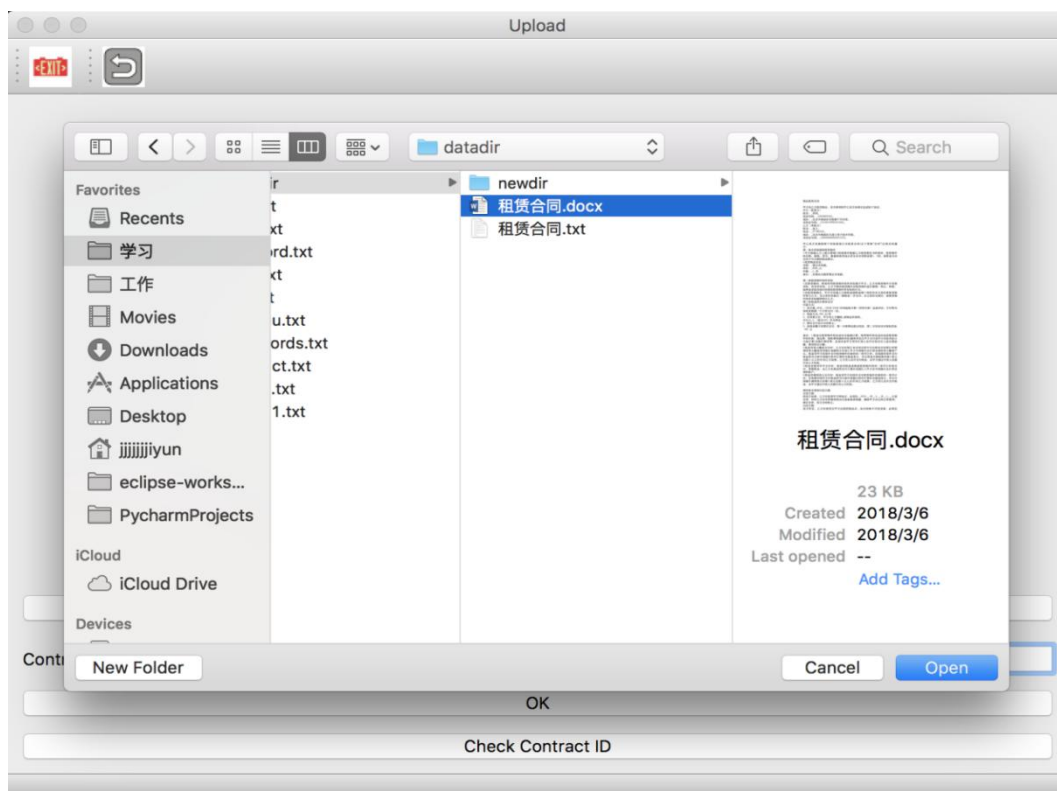
A screenshot of a software window titled "Contract ID". The window has a standard macOS-style title bar with red, yellow, and green window control buttons on the top left. Below the title bar, there are two small icons: a red square with a white "X" and a grey square with a white circular arrow. The main content area is light grey and contains the following elements from top to bottom: a text prompt "Please upload the contract (if you never upload one)" followed by a white "Upload" button; a text prompt "Please input contract id" followed by a white text input field with a blue border; a text prompt "Please input contract password" followed by a white text input field; and a wide white button labeled "OK" at the bottom.

图 24-8 合同上传及合同登录界面，若用户未上传过合同，则上传合同，若上传过，则通过合同的账号密码登录



A screenshot of a software window titled "Upload". The window has a standard macOS-style title bar with red, yellow, and green window control buttons on the top left. Below the title bar, there are two small icons: a red square with a white "X" and a grey square with a white circular arrow. The main content area is light grey and contains the following elements from top to bottom: a text prompt "Please upload the contract" centered; a wide white button labeled "Upload"; a text prompt "Contract password" followed by a white text input field with a blue border; a wide white button labeled "OK"; and a wide white button labeled "Check Contract ID" at the bottom.

图 24-9 上传合同界面，用户选择合同的电子文件，并自行设置合同密码，点击 OK 后系统会生成合同账号返回给用户



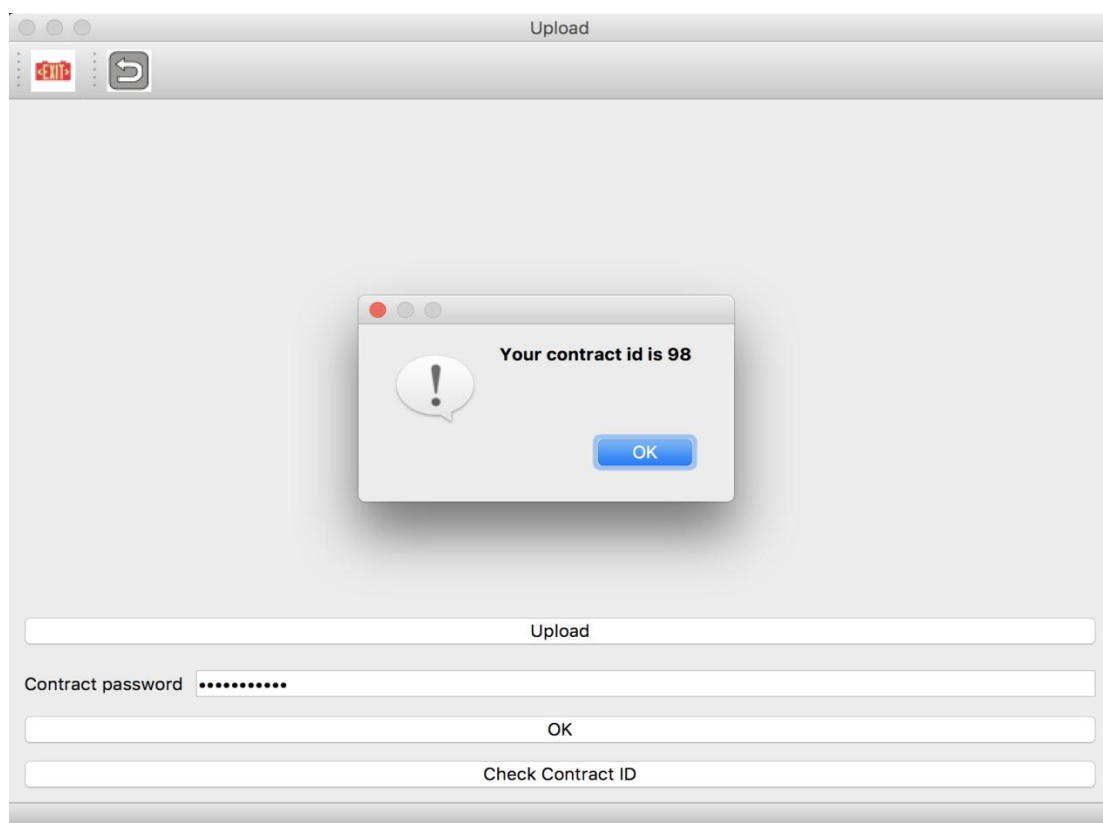


图 24-12 获取合约编号

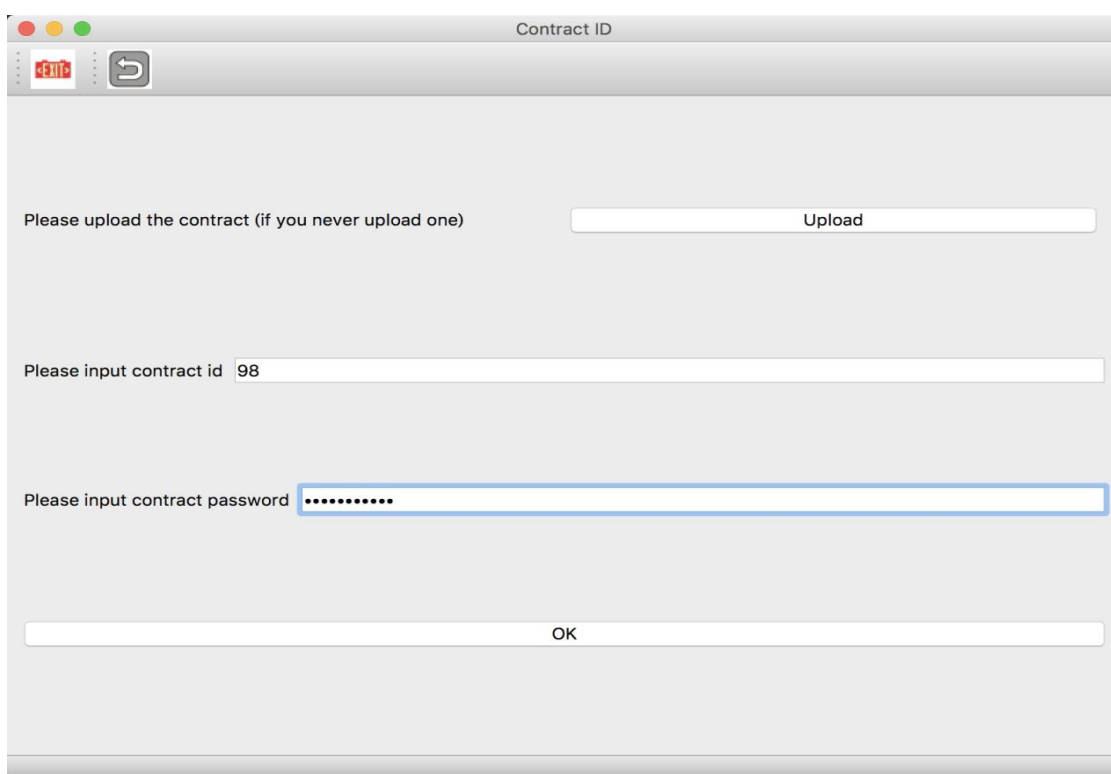


图 24-13 输入账号密码后登陆合同



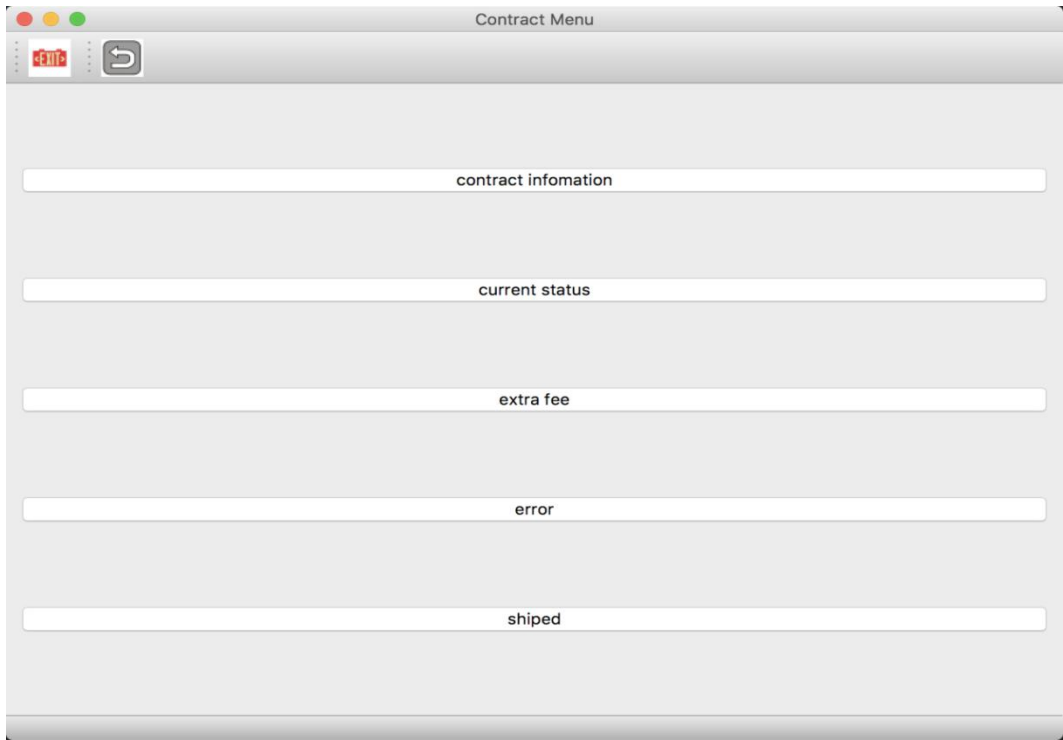


图 24-14 可查看的合同信息菜单

包括合同的基本信息，现在合同的进行状态，附加费用提交，异常状态，以及租赁物品发出按钮，合同基本信息页面会有一个确认信息符合文本合同按钮，当交易双方都按下后才可以使后四个按钮生效。

甲方姓名:	李四	租金付费方式:	月付
甲方电话号码:	16922833103	租金:	300
甲方身份证号码:	131181199901013523	押金数目:	原物品价值的
甲方住址:	北京市海淀区学院路37号对面	押金百分比:	5
乙方姓名:	老王	是否允许续租:	允许
乙方电话号码:	None	续租租金百分比:	80
乙方身份证号码:	1000000000003213123	交货日期:	2018年3月1日
乙方住址:	北京市海淀区五道口男子技术学院	归还日期:	2018年8月4日
租赁物品名称:	笔记本电脑	合同开始日期:	2018年2月1日
租赁物品单价:	9000	合同结束日期:	2018年8月1日
租赁物品件数:	1	担保单位:	北京航空航天大学学生会
租赁物品备注:	本物品为惠普笔记本电脑	签订日期:	2018年1月22日

Buttons: Show INFO, OK, Back

图 24-15 合同基本信息，其中 OK 按钮为上述的确认按钮

Information

甲方姓名: 李四 租金付费方式: 月付

甲方电话号码: 16922833103 租金: 300

甲方身份证号码: 131181199901013523 押金数目: 原物品价值的

甲方住址: 北京市海淀区学

乙方姓名: 老王

乙方电话号码: None

乙方身份证号码: 1000000

乙方住址: 北京市海淀区五

租赁物品名称: 笔记本电脑

租赁物品单价: 9000

租赁物品件数: 1

租赁物品备注: 本物品为惠普笔记本电脑

合同开始日期: 2018年2月1日

合同结束日期: 2018年8月1日

担保单位: 北京航空航天大学学生会

签订日期: 2018年1月22日

OK means that you allow us to use your account balance

No Yes

Show INFO OK Back

图 24-16 确认同意使用账户余额并确认合同信息符合文本合同

Contract ID

Please upload the contract (if you never upload one) Upload

Please input contract id qwepoizxcmb

Please input contract password 12

Wrong Password!

OK

OK

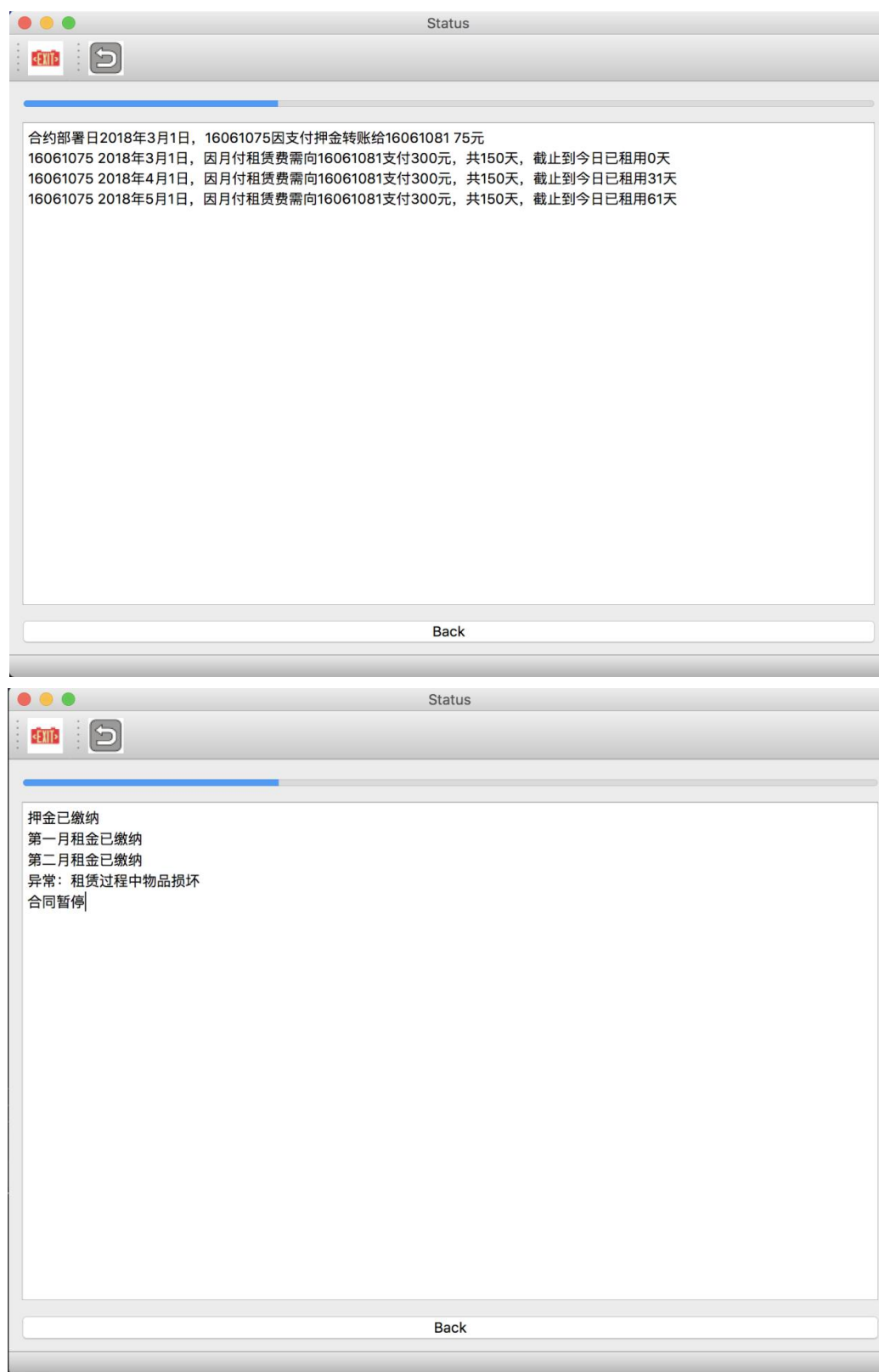


图 24-17 合同运行状态界面，通过进度条告知用户总进度，通过文字信息告知用户合同内容执行情况

Extra Fee

What caused the extra fee

How much

Who to pay

Who to receive

OK

图 24-18 附加费用提交页面

Error

物品与实物不符

租用过程中损坏

XXX

XXX

图 24-19 异常状况提交界面

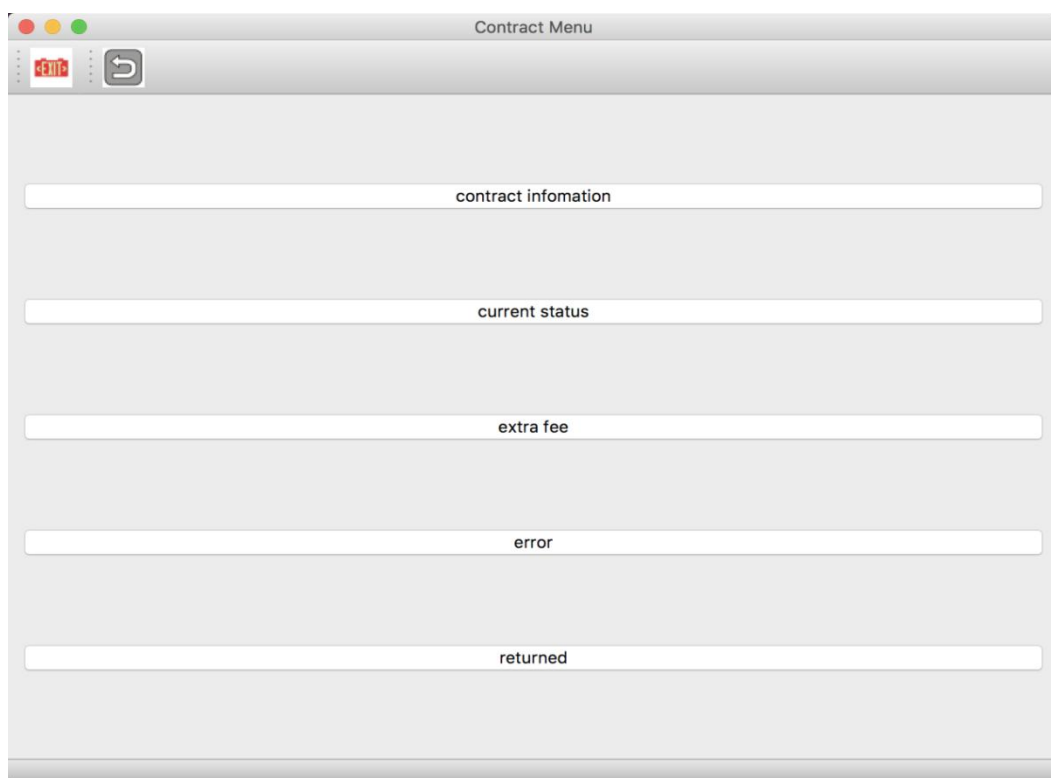


图 24-20 当最后的 returned 按钮被点击后，代表物品已归还，合同自动终止

## 第六章 改进方向

- (1) 进一步优化算法，增强代码的健壮性、多样性和包容性，使之兼容更多类型的合约。
- (2) 增强平台的透明度和整体性，让用户对自己手下的合约有更清晰详细的了解。
- (3) 扩展工具功能和适用合约类型范围，提升应用空间。
- (4) 寒假开发时间有限，作为一个新手开发团队，UI 的美化永不止步。

## 第七章 当前工具应用待解决的问题

### (1) 合法性问题

公众对其了解程度还不够，需要一段时间普及；新的法律法规来确保智能合约的法律效力也是目前需要解决的问题。智能合约不仅会影响到合同法，而且影响力会扩展到整个社会的其他社会性契约。

### (2) 监管监督问题

国家监管因区块链的去中心、自治化等特点而被淡化了。在监管无法触达的情况下

一些，由于市场的逐利等特性区块链技术可能会被不法分子应用于非法领域，为黑色产业提供了庇护所。

### （3）惩罚机制不完善

合约代码仅仅对合同中出现的异常情况进行终止合同执行处理，可以进一步优化，建立一套完整的惩罚机制，包括对延迟发货、延迟付款、物品损坏、与实物不符等情况的惩罚，但涉及到租赁方和出租方的信任问题，有待进一步讨论和解决。

## 结论

随着区块链技术的成熟，未来各行各业都可以使用区块链，以实现安全可信的、自动化的社会构建。智能合约与人工智能技术结合是未来的研究趋势。

目前该项目链上代码基本上使用的是固定的合约模板，如何运用在不同的真实业务领域，如何实现智能合约的真正自动生成，未来智能合约由谁来编写、检验、测试、认证、修改，以及如何确定区块链技术一套完备的标准并且建立相关完善的监督监管机制，都是当前需要探索的问题。

智能合约与区块链的应用与改进，我们一直在路上。

## 附录

附自然语言物品租赁合同简单测试用例一份：

甲方向乙方租用物品，有关事项经甲乙双方协商后达成如下协议：

甲方（租赁方）

姓名：\_李四\_

电话号码：\_16922833103\_

地址：\_北京市海淀区学院路 37 号对面\_

身份证号码：\_131181199901013523\_

乙方（承租方）

姓名：\_老王\_

电话：\_377481223\_

地址：\_北京市海淀区五道口男子技术学院\_

身份证号码：\_1000000000003213123\_

甲乙双方同意按照下列条款签订本租赁合同(以下简称“合同”)以资共同遵守：

#### 第一条合同依据和租赁物件

1. 甲方根据乙方上级主管部门的批准并根据乙方租赁委托书的要求，租赁物件的名称、规格、型号、数量和使用地点详见本合同附表第 1、5 项，该附表为本合同不可分割的组成部分。

#### 2. 租赁物品信息：

名称：\_笔记本电脑\_

单价：\_9000\_元

件数：\_1\_ 件

备注：\_本物品为惠普笔记本电脑\_

#### 第二条租赁物件的所有权

1. 在租赁期间，附表所列租赁物件的所有权属于甲方。乙方对租赁物件只有使用权，没有所有权。乙方不得在租赁期内对租赁物件进行销售、转让、转租、抵押或采取其他任何侵犯租赁物件所有权的行为。

2. 在租赁期满后，甲方可同意乙方续租或按附表第 11 项所列名义货价将租赁物件售与乙方。名义货价同最后一期租金一并支付。名义货价交清后，该租赁物件的所有权随即转归乙方。

#### 第三条租金的计算和支付

##### 付款方式：

1、双方就\_月付\_（月付/日付/合同起始日期一次性付清）达成共识，月付即为每租赁期满一个月即支付一次。

2、现金方式\_300\_元/次

3、合同签订后，甲方向乙方缴纳\_原物品价值的\_  
百分之\_5\_（视为 100）作为押金。

4、滞后支付双方合约终止。

5、如因余额不足滞后支付，第一天将弹出提示信息，第二天仍未交付则处罚金

500 元

备注：1. 租金以租赁物件的总成本为基础计算。租赁物件的总成本包括租赁物件的价款、海运费、保险费和融资利息(融资利息从甲方支付或甲方实际负担之日起计算)及银行费用等。总成本是甲方用外汇和人民币分别支付上述全部金额、费用的合计额。

2. 租金用美元额度支付时：乙方应在签订本合同后的 30 天内将本合同预计所需要的美元额度采用银行划拨的方式划入甲方中国银行总行营业部的美元额度户头。租金用甲方同国外支付租赁物件价款的同一货币计价。在每期对国外支付租金的当日按中国银行的外汇牌价兑换成美元,并以贸易内部结算价格(1 美元兑换×元人民币)同乙方结算。乙方用人民币支付租金,由甲方通过中国人民银行向乙方托收。

3. 租金直接用外币支付时：租金用租进或购进租赁物件的同一货币计价和支付。每期租金,由乙方在规定的支付日期内直接汇入甲方在中国银行总行营业部的帐户。

4. 租金用调剂美元支付时：租金用甲方向国外支付租赁物件价款的同一货币计价。在每期对国外支付租金的当日按中国银行的外汇牌价兑换成美元,并以中国银行调剂美元价格(1 美元兑换×元人民币)同乙方结算。乙方用人民币支付租金,由甲方通过中国人民银行向乙方托收。

#### 第四条交货和归还日期

交货日期:

经双方协商,乙方在收到甲方押金后,必须在\_2018\_年\_3\_月\_1\_日前交货,同时乙方应对所提供的办公设备保质保量,确保甲方办公的正常使用。滞后交货,双方合约终止。

归还日期:

双方约定,乙方在使用完甲方出租的物品后,如无特殊不可抗因素,必须在\_2018\_年\_8\_月\_4\_日前返还。否则将按违规处理,合同终止。

#### 第五条租金的变更和罚款利息

1. 在租赁期内,由于我国政府或租赁物件出口国政府增减有关税项、税率等因素必须变更租金时,甲方用书面通知乙方这种变更并提出新的实际租金,乙方承认这种变更。



2. 租赁物件的总成本与其概算租金不符时，甲方在租赁物件全部交货后，用书面通知乙方实际租金的金额，并以此金额为准对概算租金作出相应的变更，乙方承认这种变更。

3. 乙方延迟支付租金时，甲方将按照延付时间计算，每日加收延付金额的万分之三的利息。

#### 第五条质量保证及事故处理

1. 租赁物件的质量保证条件同甲方与卖方签订的购货协议中的质量保证条件相符。如果在质量保证期内发生质量问题属于卖方责任时，甲方同意将购货协议规定的索赔权转让给乙方，并协助乙方办理索赔事宜。当需要卖方派人来华时，甲方负责办理邀请外商来华的手续。

2. 在租赁期内，因乙方责任事故致使租赁物件遭受损失时，乙方应对此承担全部赔偿责任。

3. 如发生以上任何情况，都不影响本合同的继续执行和效力。

#### 第六条租赁物件的使用、维修、保养和费用

1. 租赁物件在租赁期内由乙方使用。乙方应负责日常维修、保养，使设备保持良好状态，并承担由此产生的全部费用。

2. 租赁物件在安装、保管、使用等过程中致使第三者遭受损失时，由乙方对此承担全部责任。

3. 租赁物件在安装、保管、使用等过程中发生的一切费用、税款，均由乙方负担。

#### 第七条租赁物件的损坏和毁灭

1. 乙方承担在租赁期内发生的租赁物件的毁损(正常损耗不在此限)和灭失的风险。

2. 在租赁物件发生毁损或灭失时，乙方应立即通知甲方，甲方可选择下列方式之一由乙方负责处理并承担其一切费用：(1)将租赁物件复原或修理至完全能正常使用的状态；(2)更换与租赁物件同等型号、性能的部件或配件、使其能正常使用；(3)当租赁物件灭失或毁损至无法修理的程度时，乙方应按附表第9项规定的预定损失金额，赔偿甲方。

#### 第八条租赁物件的保险

1. 按 FOB 或 C&F 条件交货时，由甲方办理租赁物件的进口运输保险手续。

2. 租赁物件自运抵乙方安装或使用地点之日起由甲方向中国人民保险总公司投保

财产险(保险期至本合同终结时为止),为应付自然灾害所引起的租赁物件的毁损风险。

3. 在租赁期间,如发生保险事故,乙方应立即通知甲方和中国人民保险总公司在当地的分公司,并向甲方提供检验报告和有关资料,会同甲方向中国人民保险总公司索赔。本条各项保险费均计入总租金内用外币支付,由乙方负担。根据第八条应由乙方支付给甲方的款项,可在保险赔偿金内减免抵偿。

#### 第九条 租赁保证金

1. 本合同一经签订乙方即向甲方支付附表第8项规定的租赁保证金,作为履行本合同的保证。

2. 租赁保证金不计利息,在租赁期满时归还乙方或抵最后一期租金的全部或一部分。

3. 乙方违反本合同任何条款时,甲方将从租赁保证金中抵扣乙方应支付给甲方的款项。

#### 第十条 违反合同时的处理

1. 除本合同第四条所规定的条款外,未经对方书面同意,任何一方不得中途变更或解除合同。任何一方违反本合同将按我国《经济合同法》的有关条款处理。

2. 乙方如不支付租金或违反本合同的任何条款时,甲方有权采取下列措施: (1) 要求乙方及时付清租金和其他费用的全部或一部分。 (2) 终止本合同,收回或要求归还租赁物件,并要求乙方赔偿甲方的损失。

3. 租赁物件交货前,由于乙方违反本合同而给甲方造成的一切损失,乙方应负责赔偿。

#### 第十一条 经济担保

担保单位: \_北京航空航天大学学生会\_

不论发生何种情况乙方未按照本合同附表的要求支付租金时,乙方经济担保人将按《经济合同法》第十五条的规定承付乙方所欠租金。

#### 第十二条 争议的解决

1. 有关本合同的一切争议,甲乙双方及乙方的经济担保人应首先根据我国《经济合同法》等法规的有关条款来解决。如不能解决时,提请有关经济法庭判决。

2. 甲方与外商签订的购货协议或租赁合同需要仲裁时乙方有责任提供必要的资料并协助甲方对外进行交涉。

#### 第十三条 本合同的附件

1. 本合同附件是本合同不可分割的组成部分，与本合同正文具有同等法律效力。

本合同附件： (1) 租赁合同附表； (2) 租赁委托书及附表； (3) 租赁设备确认书； (4) 甲方购货协议副本； (5) 乙方租金偿还担保与还款计划书。

#### 第十四条续租规定

1、本合约\_允许\_续租

2、若续租，租金为原来的百分之\_80\_

其他造成合约终止的因素：

1、实物与租赁约定不符

2、租物损坏

#### 第十五条其他

1. 本合同正本一式二份，自甲乙双方签章后生效，双方各执一份正本为凭。合同副本除乙方经济担保人必持一份外，其他需要份数由双方商定。

2. 对本合同内容的任何修改、补充或变更(除第四条外)须采用书面形式，经双方加盖公章后正式生效。本合同修改、变更部分应视为本合同不可分割的组成部分。

合同开始日期：\_2018\_年\_2\_月\_1\_日

合同结束日期：\_2018\_年\_8\_月\_1\_日

本协议一式两份，甲乙双方各执一份。自合同签订之日起生效，未尽事宜，经甲乙双方协商后签订补充协议，具同等法律效力。

甲方（签章）：\_\_李四\_\_

乙方（签章）：\_\_老王\_\_

签订日期：\_\_2018\_\_年\_\_1\_\_月\_\_22\_\_日

## 参考文献

- [1]胡凯,白晓敏,于卓等. 智能合约工程[J]. 中国计算机学会通讯, 2017, (5)
- [2]蔡维德. 区块链技术与应用[J]. 中国计算机学会通讯, 2017, (5)
- [3]郁莲,邓恩艳. 区块链技术[J]. 中国计算机学会通讯, 2017, (5)
- [4]子平. 连接未来的“区块链”[N]. 中国纪检监察报, 2018-03-06(006).
- [5]袁勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(04):481-494.
- [6]沈鑫,裴庆祺,刘雪峰. 区块链技术综述[J]. 网络与信息安全学报, 2016, 2(11):11-20.
- [7]黄洁华,高灵超,许玉壮,白晓敏,胡凯. 众筹区块链上的智能合约设计[J]. 信息安全研究, 2017, 3(03):211-219.
- [8]刘德林. 区块链智能合约技术在金融领域的研发应用现状、问题及建议[J]. 海南金融, 2016(10):27-31.
- [9]王春宇,张守坤. 智能合约与金融合约[J]. 商, 2016(06):198.
- [10]姚忠将,葛敬国. 关于区块链原理及应用的综述[J]. 科研信息化技术与应用, 2017, 8(02):3-17.
- [11]鲁静,宋斌,向万红,周志明. 基于区块链的电力市场交易结算智能合约[J]. 计算机系统应用, 2017, 26(12):43-50.
- [12]李赫,孙继飞,杨泳,汪松. 智能合约如何可信地与外部世界交互[J]. 中国金融电脑, 2017(08):55-59.
- [13]李保利,陈玉忠,俞士汶. 信息抽取研究综述[J]. 计算机工程与应用, 2003(10):1-5+66.
- [14]鲁松,白硕. 自然语言处理中词语上下文有效范围的定量描述[J]. 计算机学报, 2001(07):742-747.