**基于区块链技术的实验室文档管理系统**

**操作说明书**

**目录**

[1.引言](#_Toc11999_WPSOffice_Level1) [1](#_Toc11999_WPSOffice_Level1)

[1.1 目的](#_Toc978_WPSOffice_Level2) [1](#_Toc978_WPSOffice_Level2)

[1.2 背景](#_Toc30428_WPSOffice_Level2) [1](#_Toc30428_WPSOffice_Level2)

[2.用途](#_Toc978_WPSOffice_Level1) [1](#_Toc978_WPSOffice_Level1)

[2.1 功能](#_Toc26830_WPSOffice_Level2) [1](#_Toc26830_WPSOffice_Level2)

[2.2 性能](#_Toc1719_WPSOffice_Level2) [1](#_Toc1719_WPSOffice_Level2)

[2.3 安全保密](#_Toc4849_WPSOffice_Level2) [2](#_Toc4849_WPSOffice_Level2)

[3.运行环境](#_Toc30428_WPSOffice_Level1) [5](#_Toc30428_WPSOffice_Level1)

[3.1 硬件和软件](#_Toc17498_WPSOffice_Level2) [5](#_Toc17498_WPSOffice_Level2)

[4.使用说明](#_Toc26830_WPSOffice_Level1) [5](#_Toc26830_WPSOffice_Level1)

[4.1 连接到别的电脑](#_Toc27618_WPSOffice_Level2) [5](#_Toc27618_WPSOffice_Level2)

[4.2 上传文件到区块链](#_Toc25282_WPSOffice_Level2) [7](#_Toc25282_WPSOffice_Level2)

[4.3 下载文件到电脑](#_Toc2337_WPSOffice_Level2) [9](#_Toc2337_WPSOffice_Level2)

[4.4 更新数据](#_Toc6952_WPSOffice_Level2) [11](#_Toc6952_WPSOffice_Level2)

[4.5 帮助](#_Toc20991_WPSOffice_Level2) [11](#_Toc20991_WPSOffice_Level2)

[4.5.1错误消息](#_Toc978_WPSOffice_Level3) [12](#_Toc978_WPSOffice_Level3)

[4.5.2自动连接](#_Toc939_WPSOffice_Level2) [14](#_Toc939_WPSOffice_Level2)

[4.5.3更新区块链问题](#_Toc30428_WPSOffice_Level3) [15](#_Toc30428_WPSOffice_Level3)

[4.5.4程序卡住](#_Toc26830_WPSOffice_Level3) [16](#_Toc26830_WPSOffice_Level3)

[4.6退出](#_Toc22570_WPSOffice_Level2) [16](#_Toc22570_WPSOffice_Level2)

# **1.引言**

## 1.1 目的

本手册的目的是指导用户，了解如何使用“基于区块链技术的实验室文档管理系统”。本手册介绍了如何通过本地网络分发文件且描述了如何实现此类文件分发，其中包括对区块链技术的讨论。

## 1.2 背景

“基于区块链技术的实验室文档管理系统”由郑州源创吉因实业有限公司开发，由软件工程师王义凯编写。这款软件被设计为分发和保护用户上传文件的替代方法。

# **2.用途**

## 2.1 功能

软件程序可以使用区块链技术存储和分发任何文件（PDF，DOC，XLSX，JPG等）。它不像比特币的区块链有1MB的大小限制，也不像以太坊收费2.11美元只用于存储1KB和0.10美元用于读取1KB数据。它的区域块是全部免费使用并且没有文件大小的限制。

## 2.2 性能

对于接收、存储和发送小文件，这款软件稳定的同时可以达到预期的效果。由于区块链的“工作证明”（在下一节中讨论），处理大于几MB的文件时，所以运行速度可能会变缓。

## 2.3 安全保密

区块链技术通常非常安全，可防止篡改，每个区块用哈希加密的方式连接。哈希是一串数字和字母用来标识数据。哈希的概念如图1所示：



图1

由于其安全性和速度，哈希函数是被用于SHA-512而且通常是不可逆的。因为没有一个函数可以使用SHA-512哈希并将其转换回其原始输入。如图2所示：

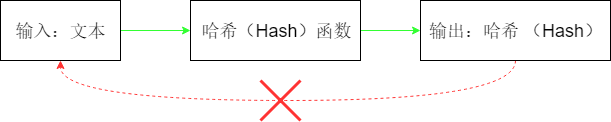


图2

区域块的内容被看作初始输入内容去完成哈希。“基于区块链技术的实验室文档管理系统”用于区域块的数据、区域块指数和先前的哈希数值,还有哈希的创建时间和别的属性去确定区域块。根据之前的哈希，一个区域块链可以被用于去连接先前的区域块。如图3所示：

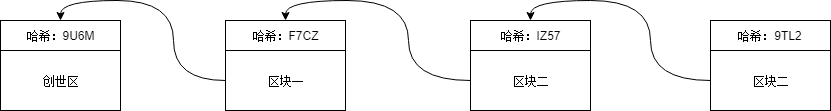


图3

如果一个黑客想要篡改块一，那么更改块的输出值将更改哈希。因此，块二将无法链接到块一，如下面的图4所示。

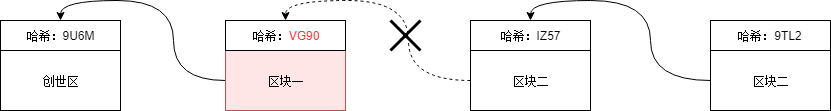


图4

通过一些方式可以检测到损坏块的位置。然而，现代计算机在计算哈希中很快，黑客可以轻松地改变其余块的哈希值。这就是为什么区块链技术结合了区块链的“工作证明”概念，使得创建有效哈希变得更加困难。

这里讨论的“基于区块链技术的实验室文档管理系统”有一个“工作证明”，规定除了创世块（第一个不包含实际数据的块）之外的所有块的哈希开头都有一定数量的零。如图5所示：

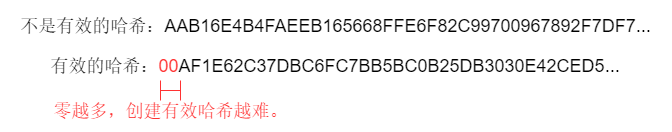


图5

每个哈希必须有2个前导零。虽然这个要求似乎毫无意义，但它使得有效哈希的创建变得更加困难。因此，与几百KB的文件相比，大于几MB的文件需要更长的时间才能添加到区块链中。

然而，防止篡改的最大保护是许多区块链应用的P2P（对等）网络组件。网络中的每个节点或计算机都有一个区块链的副本，如图6所示。当一个节点向区块链添加一个块时，网络中的每个节点都会接收到新的块且验证该块，然后将其添加到他们的区块链副本。因此，为了破坏整个区块链，黑客需要篡改区块链网络中超过一半的节点。所以，这个程序非常安全。

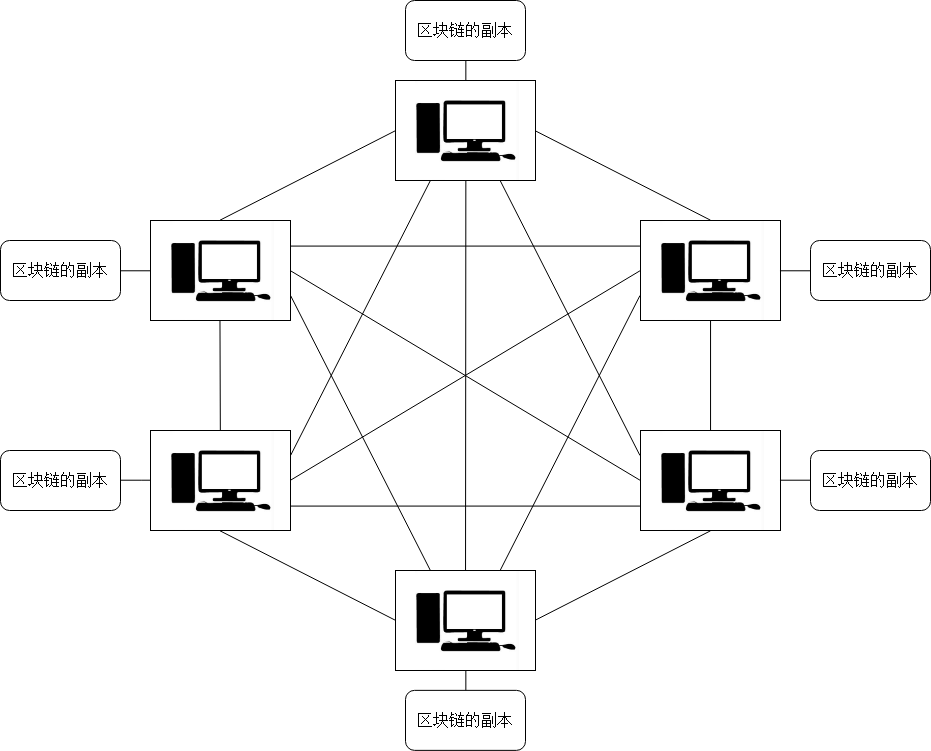


图6

# **3.运行环境**

## 3.1 硬件和软件

普通Windows PC可以运行这个软件。源代码用C++编写，使用Qt Creator 4.6.2 Community Edition进行编译。这软件可以通过使用Winebottler在Mac和Linux计算机上运行，虽然速度可能很慢。

# **4.使用说明**

主界面如下图7所示。



图7

## 4.1 连接到别的电脑

要连接到一个计算机，请点击“连接电脑”。将出现一个对话框，如图8所示。

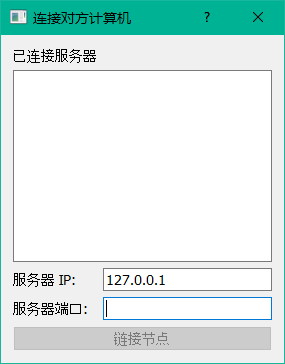


图8

IP地址将自动填入计算机的当前IP地址，这比较方便。因为这个区块链应用程序旨在用于本地网络。本地网络中的IP地址共享相同的网络组件。在其他计算机的IP地址和端口号已填满后，按“链接节点”，“基于区块链技术的实验室文档管理系统”将尝试与另一台计算机通信。如果通信成功，将显示通知，如图9所示。



图9

## 4.2 上传文件到区块链

如图10所示，点击“上传文件”将提示用户从其计算机中选择要添加到区块链的文件，将区块链的长度增加1。

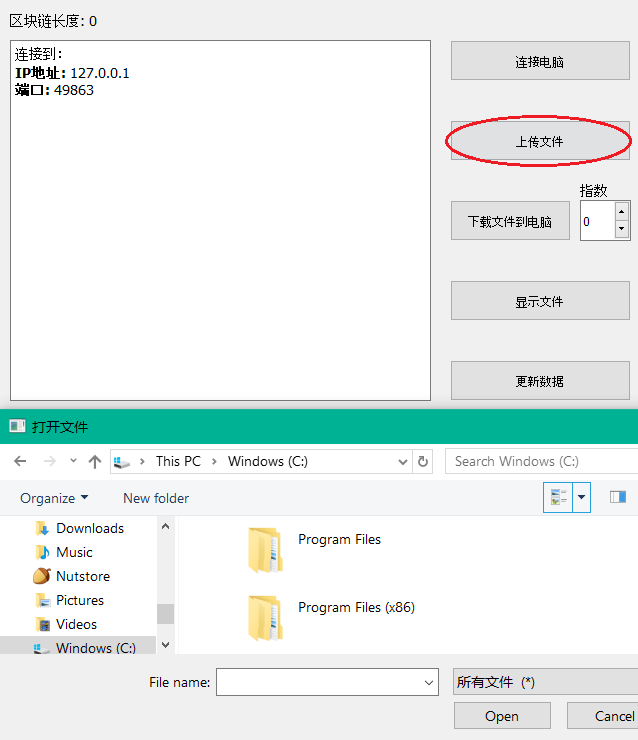


图10

在将文件添加到块之后将显示块的SHA-512哈希，并且块已被附加（挖掘）到区块链。如图11所示。



图11

添加块后，新块将自动发送到网络上的任何连接节点。

## 4.3 下载文件到电脑

如图12所示，点击“显示文件”可获取当前在区块链上的文件列表及其各自的索引。

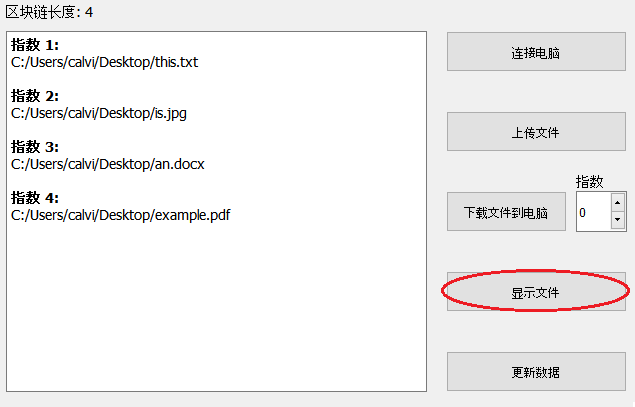


图12

将“指数”更改为与要保存在计算机上的所需文件对应的数字后，点击“下载文件到电脑”将提示用户找到将文件保存在其计算机上的路径，如下图13所示。

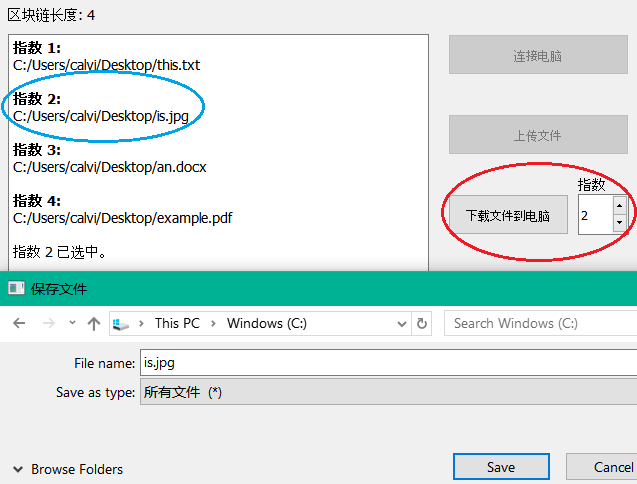


图13

## 4.4 更新数据

单击“更新数据”会将区块链保存到这个应用程序目录中的“blockchain”文件中。然后，它将检查连接的节点，以查看其结束时区块链的任何更改。如果大多数节点具有不同版本的区块链，则此计算机上的区块链将被更新，然后保存在“blockchain”文件中。

## 4.5 帮助

### 4.5.1错误消息

使用此应用程序时，用户可能会遇到错误消息和通知。图14是网络通知的示例。

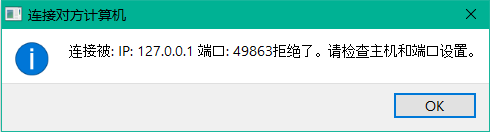


图14

网络通知和错误通常是由错误的端口和IP地址引起的，或者计算机已停止运行这个程序。此外，计算机的防火墙可能阻止了区块链应用程序与其他计算机进行通信。

严重错误与区块链本身有关。图15显示了当块的散列与“blockchain”文件中保存的哈希不匹配时发生的错误消息。

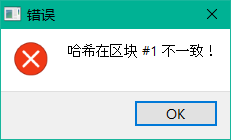


图15

图16显示了一个错误消息，它是块1引用除块0之外的散列的结果。请记住，区块链中的哈希值通过引用其先前的哈希值进行链接。因此，改变一个块的散列将导致后续块与所有先前块分离。

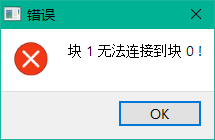


图16

区块链中出现的错误（如图15和16所示）将导致“上传文件”和“更新数据”选项被锁定，如下图17所示。这是为了防止用户的区块链被上传到其他节点，以防用户的区块链被篡改。连接到网络上的节点将导致修复被篡改的区块链，从而解决问题。

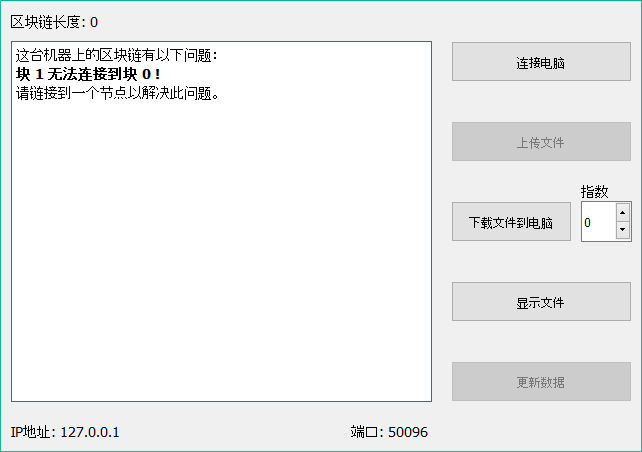


图17

最严重的错误是“基于区块链技术的实验室文档管理系统”无法打开“blockchain”文件。“基于区块链技术的实验室文档管理系统”将在显示错误消息后立即关闭，如图18所示。创建文件“blockchain” （无文件扩展名）将解决问题，但要使文件与节点的最新版本保持同步。在特定网络中，“blockchain”文件必须与该网络的节点具有相同的创世块（有关详细信息，请参阅4.5.3）。

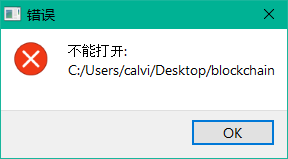


图18

### 4.5.2自动连接

“基于区块链技术的实验室文档管理系统”可以在启动时自动连接到其他节点，因为其他节点已经启动并运行。如果先前连接的节点已停止运行“基于区块链技术的实验室文档管理系统”，则这个程序将给出网络连接错误。在与这个软件和“blockchain”文件相同的目录中，有一个名为“connections.txt”的文本文件（如果没有，则在这个软件时将自动创建“blockchain”文件 关闭现有连接）。

要配置启动时“基于区块链技术的实验室文档管理系统”连接的内容，可以修改“connections.txt”。文本文件包含以下格式的IP地址和端口号：

<IP 地址> <端口号>

下面的图19显示了这种情况的一个示例。请注意，IP地址共享相同的网络部分（83.95.250）。这是因为本地网络中的IP地址共享相同的网络组件。

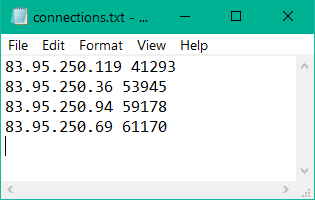


图19

### 4.5.3更新区块链问题

如果更新区块链有任何问题，请打开“blockchain”文件，而不是区块链软件，删除所有内容，然后粘贴以下内容：

0 1531877114 TkFNRTogIERBVEE6IEdlbmVzaXMgQmxvY2s= 0 91629c3d6c07c2d358688ef3daedf9a420dbeb7d518b08de4bcfa4af2488f400bc3a9ecfd70697780213210ce172e0720adf7c160fb4b6b4cc54489fb36945b9

在记事本上粘贴文本应该给出下面的结果，如图20所示。

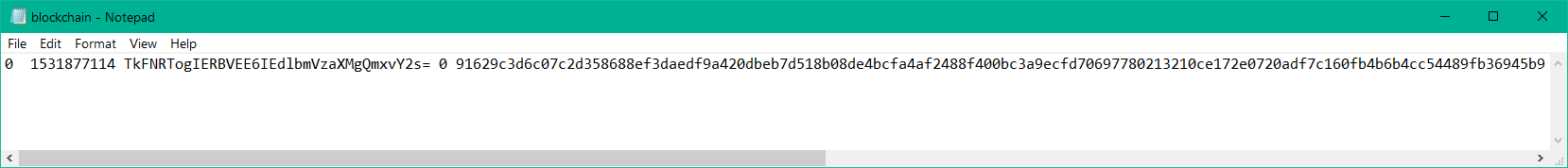


图20

这个文本构成了区块链的起源块。在这种情况下，文本是“基于区块链技术的实验室文档管理系统”用于郑州源创吉因实业有限公司的标准起源块。通过简单地使区块链仅保持创世块，用户计算机上的区块链被重置。因此，连接到网络上的节点将提供区块链的其余块。如图21所示，以红色突出显示的文本是创世块的哈希值。

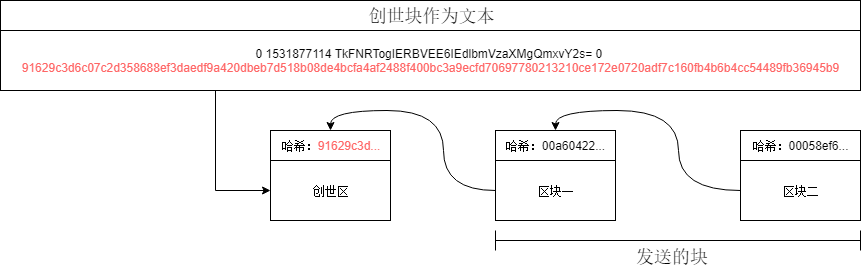


图21

起源区块是区块链中最重要的区块，因为不同的发生区块将产生不同的区块链。

### 4.5.4程序卡住

如果“基于区块链技术的实验室文档管理系统”被冻结，那么它可能只是计算大文件的散列。由于区块链技术中的“工作证明”概念，计算大文件的散列（即使它超过几MB）比计算几个KB文件的散列要花费更长的时间。另一个可能的原因是这个程序正在发送一个大文件或另一台计算机，恰好同时将文件上传到区块链。

## 4.6退出

关闭这个程序将导致区块链自动检查更新并将区块链保存到PC。如果“基于区块链技术的实验室文档管理系统”已连接到网络中的其他节点，则当先前连接的节点已停止运行这个程序时，可能会出现网络错误通知。但是，如果区块链已被篡改，则这个程序将简单地关闭。