



安装、配置和管理。

用户手册

1.0测试版

2020年6月。

MiniQRNG是OpenQbit Inc.的注册商标，采用自由使用和商业许可。使用条款和条件见：
www.OpenQbit.com

内容

- 1. 介绍：3
- 2. 什么是Blockly编程？3
- 3. 什么是Termux？4
- 4. 什么是迷你QRNG？4
- 5. Termux内的存储配置。8
- 6. SSH（安全壳）服务器安装。9
- 7. 在手机（智能手机）上配置SSH服务器。10
- 8. Ambientes Blockly（App Inventor, AppyBuilder和Thunkable）。17
- 9. 迷你QRNG中块的定义和使用。18
- 10. 创建QRNG的"硬件"设备。30
- 11. 附件"OpenQbit量子计算"。36
- 12. 软件的许可和使用；40

1. 介绍：

今天的密码学是基于随机数序列的。目前使用的伪随机数发生器看似提供了随机的位序列，但实际上这些位序列有一定的规律，所以存在被黑客攻击或以其他方式操纵的风险，使信息在公共网络和盗版网络上传播。

在随机数发生器中整合物理熵源是克服这一安全威胁的最常用方法。但是，经典物理学是因果关系，所以用经典物理学生成的位序列的不可预测性无法得到证明。

另一方面，量子物理学本质上是随机的。量子随机数发生器（QRNG）产生的数字无法预测：QRNG显然是不可预测的。所以，如果在安全系统中使用量子随机数发生器，即使是算术运算速度快的超级计算机也无法预测这个安全系统使用的随机位序列。

量子物理学使用的方法是基于一个叫熵的基本概念。

介绍的類型

一般有两种类型的熵源，可以测量生成真随机数。第一类包括难以或无法测量的物理过程，或计算量太大，无法预测，或两者兼而有之。这就是caoticentropy的来源。大多数人都知道的一个常见的例子就是彩票机。将一组按顺序编号的球放在一个腔室中，通过旋转腔室或吹气通过腔室不断地混合在一起。让几个球从室内掉出来，球上标注的数字代表抽奖。由于球和摄像机之间的大量互动导致每个球可能的运动数量迅速增加，因此抽签是随机的。不仅这些相互作用的复杂性极高，而且没有明显的方法来准确观察或测量球、相机和气流的所有内部变量。第二种非常不同的熵源是量子力学。许多微观粒子或波，如光子、电子、质子等都具有量子力学特性，包括旋转、偏振、位置和动量。给定适当的构型来产生这些粒子，它们的旋转或偏振等具体数值不仅是未知的，而且在理论上无法预知，在没有进行测量之前，都是物理上确定的。

2. 什么是Blockly编程？

Blockly是一种**可视化的编程语言**，由一组简单的命令组成，我们可以将它们组合起来，就像拼图的碎片一样。对于那些想要以直观和简单的方式**学习如何编程的人来说**，或者对于那些已经知道如何编程并想要看到这种类型的编程潜力的人来说，这是一个非常有用的工具。

Blockly是一种不需要任何计算机语言背景的编程形式，这是因为它只是将图形块连接起来，就像我们玩乐高或拼图一样，你只需要具备一些逻辑性，就可以了！

任何人都可以为手机（智能手机）创建程序，不用再去搞那些难懂的编程语言，只需要图形化的方式把积木拼接起来，以简单、方便、快捷的方式进行创建。

3. 什么是Termux？

Termux是一款安卓终端模拟器，也是一款Linux环境下的应用，不需要路由和配置就可以直接工作。自动安装一个最小的基础系统。

我们将使用Termux，因为它的稳定性和易于安装和管理，但是，你可以使用Ubuntu Linux for Android的安装环境。

在这个Linux环境下，你将拥有MiniQRNG的通信过程的"核心"。

4. 什么是迷你QRNG？

Mini QRNG是软件和硬件，包括三种技术方案来创建QRNG（量子随机数发生器）。分类如下：

- a.- QRNG API。- 从外部服务器获得的量子随机数发生器。
- b.-MiniQRNG/软件。- 利用手机摄像头的物理特性（量子）得到的随机量子数发生器。
- c.-MiniQRNG/硬件。- 利用基于激光的量子物理特性的硬件获得的量子数发生器。后面我们会告诉你如何在家里低成本地建造它。

1. 安装和配置Termux终端。

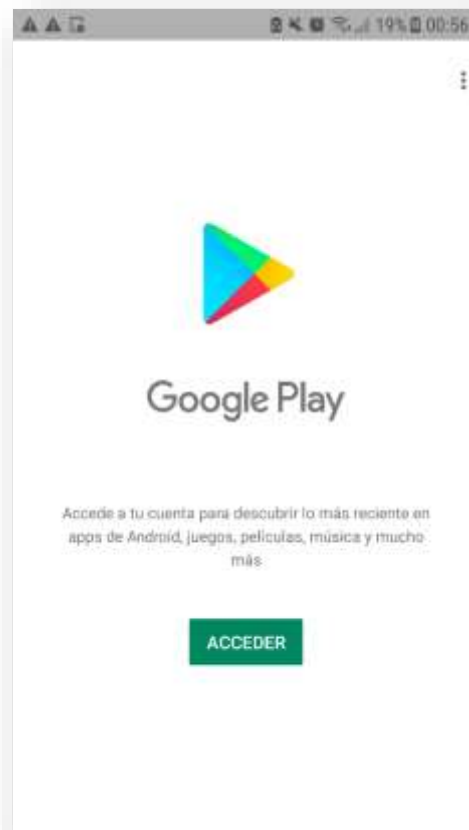
首先，我们需要一个Linux环境，因为每个Android系统都是基于Linux的，以保证工具的安全性和灵活性，我们将使用"Termux"终端，在该环境中安装帮助我们创建QRNGs的工具。

Termux是一个Linux模拟器，我们将安装必要的包来创建量子数。

使用Termux的主要优势之一是，您可以在不需要"旋转"手机（智能手机）的情况下安装程序。这确保了不会因为这种安装而失去制造商的保修。

Termux的安装。

在手机上，进入Google Play图标应用（play.google.com）。



通过应用程序"Termux"搜索，选择它并开始安装过程。



启动Termux应用程序。

启动后我们要执行以下两个命令来执行Linux操作系统模拟器的更新。

\$ apt update

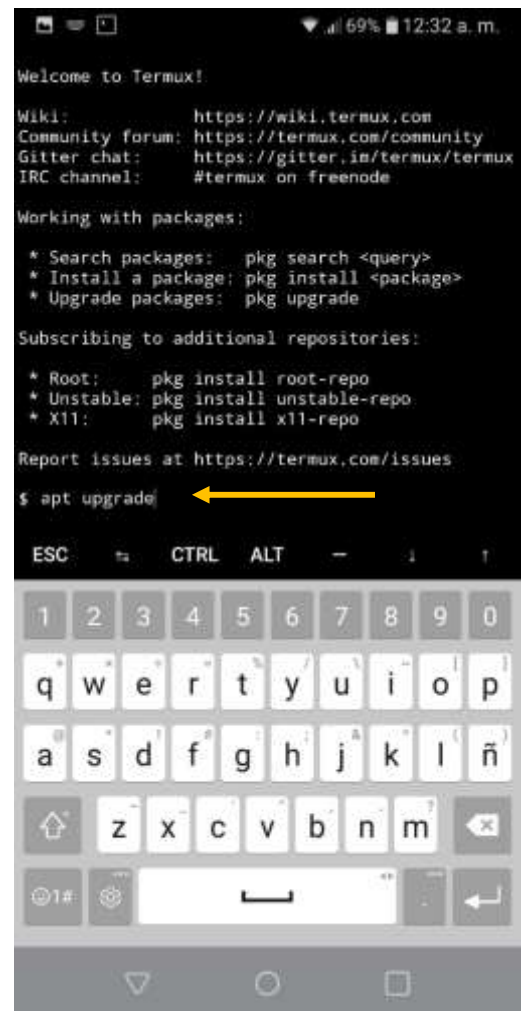
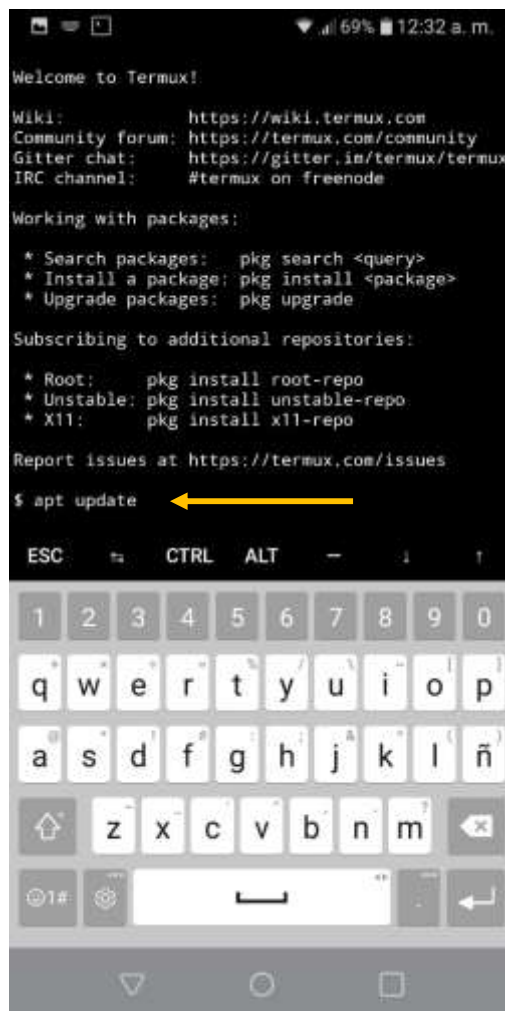
\$ apt升级

确认所有选项 Y(是)....。

Termux

Home \$ apt update

\$ apt upgrade



5. Termux内的存储配置。

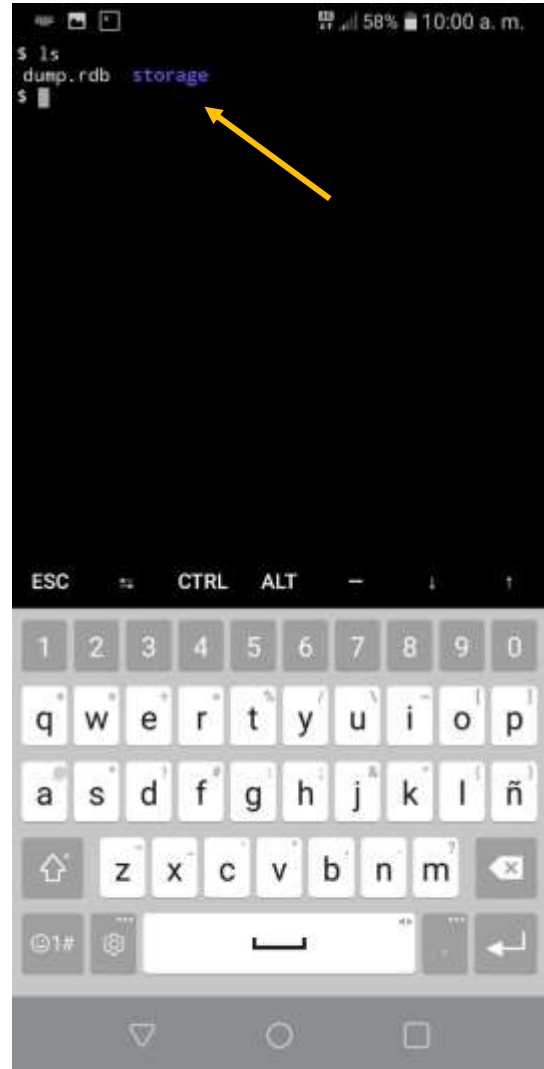
在您更新升级了Termux系统之后，我们将开始配置如何在Termux系统中查看手机的内部存储，这将帮助您能够在Termux和我们的手机信息之间进行信息交换。

可以通过在Termux终端上运行以下命令来简单快速地完成。

```
$ termux-setup-storage
```

当你执行上一条命令时，会出现一个窗口，要求你确认在Termux中创建一个虚拟存储（目录）。我们通过下达命令来验证。

```
$ ls
```

6. SSH（安全壳）服务器安装。

```
$ apt install openssh
```

```
$ apt install sshpass
```

```
$ apt install openssh
```

```
$
```

```
apt install sshpass
```

```
$ apt install openssh
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
krb5 ldns libdb libedit termux-auth
The following NEW packages will be installed:
krb5 ldns libdb libedit openssh termux-auth
0 upgraded, 6 newly installed, 0 to remove and 0
not upgraded.
Need to get 2255 kB of archives.
After this operation, 11.9 MB of additional disk
space will be used.
Do you want to continue? [Y/n] Y
Get:1 https://dl.bintray.com/termux/termux-packa
ges-24 stable/main arm libdb arm 18.1.32-4 [465
kB]
Get:2 https://dl.bintray.com/termux/termux-packa
ges-24 stable/main arm krb5 arm 1.18.1 [839 kB]
24% [2 krb5 131 kB/839 kB 16%]
```

```
$ apt install sshpass
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
sshpass
0 upgraded, 1 newly installed, 0 to remove and 0
not upgraded.
Need to get 7158 B of archives.
After this operation, 57.3 kB of additional disk
space will be used.
0% [Working]
```

我们已经完成了手机上本地主机SSH服务器的通信网络安装。

7. 在手机（智能手机）上配置SSH服务器。

我们将使手机中的SSH服务器能够从我们的PC连接到手机，并能够以更快、更舒适的方式工作，同时它还将帮助我们检查手机中的SSH服务器的服务是否正常工作，因为我们将使用它与Mini QRNG进行通信。

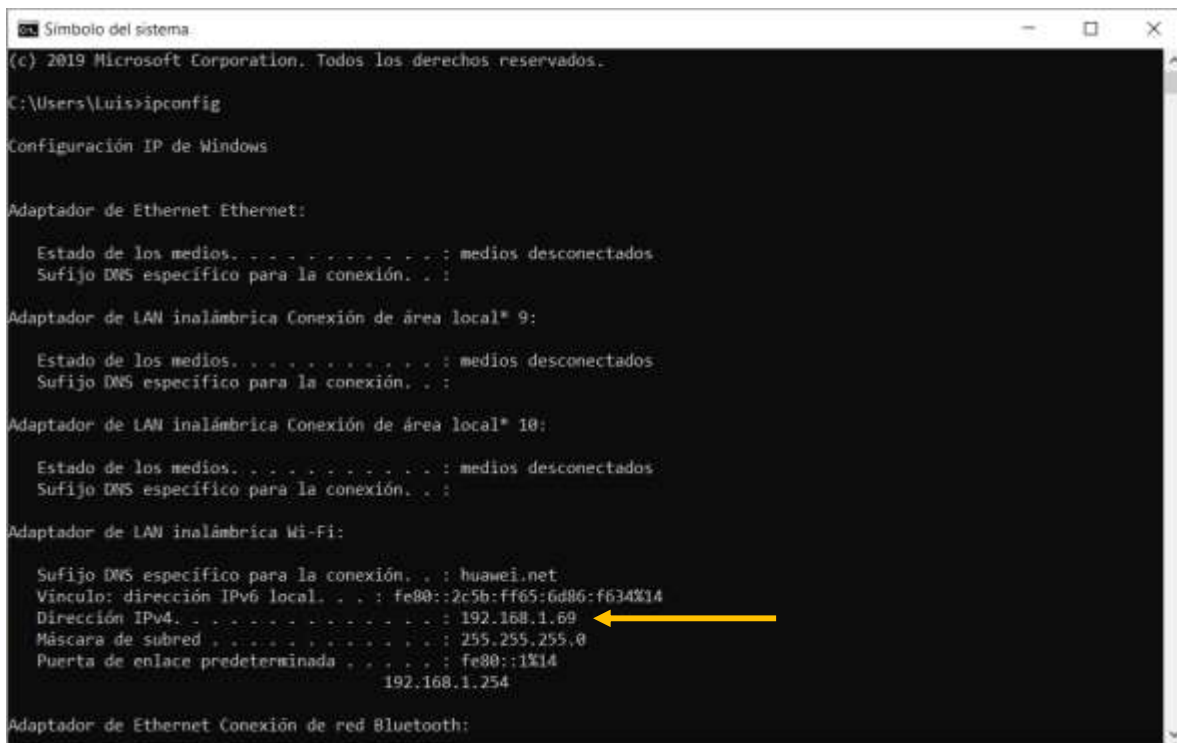
首先我们要做的是将手机和电脑连接到**同一个WiFi网络**，这样就可以看到对方了。IP或地址必须类似于192.168.XXX.XXX的XXX值是每个计算机中随机分配的可变数字。

这个例子是在LG Q6手机和装有Windows 10 Home的PC上测试的。

检查电脑连接到WiFi的IP或地址，我们必须在Windows中打开一个终端。

在底部面板搜索放大镜的地方写上cmd，按回车键。一个终端将打开，我们在其中写下命令。

C:\User_Name> ipconfig



```
Símbolo del sistema
(c) 2019 Microsoft Corporation. Todos los derechos reservados.
C:\Users\Luis>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 9:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 10:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Wi-Fi:

    Sufijo DNS específico para la conexión. . : huawei.net
    Vínculo: dirección IPv6 local. . . : fe80::2c5b:ff65:6d86:f634%14
    Dirección IPv4. . . . . : 192.168.1.69
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . : fe80::1%14
                                      192.168.1.254

Adaptador de Ethernet Conexión de red Bluetooth:
```

它将显示我们分配给PC的IP是192.168.1.69，但这很可能在每个情况下是不同的。

注意：应该取写有"IPv4地址"的地址，不要和网关混淆。

现在在Termux终端的手机的情况下，我们必须键入下面的命令来知道我们的用户的名字，我们将用来连接到拥有我们手机的SSH服务器，我们执行下面的命令。

\$ Whoami

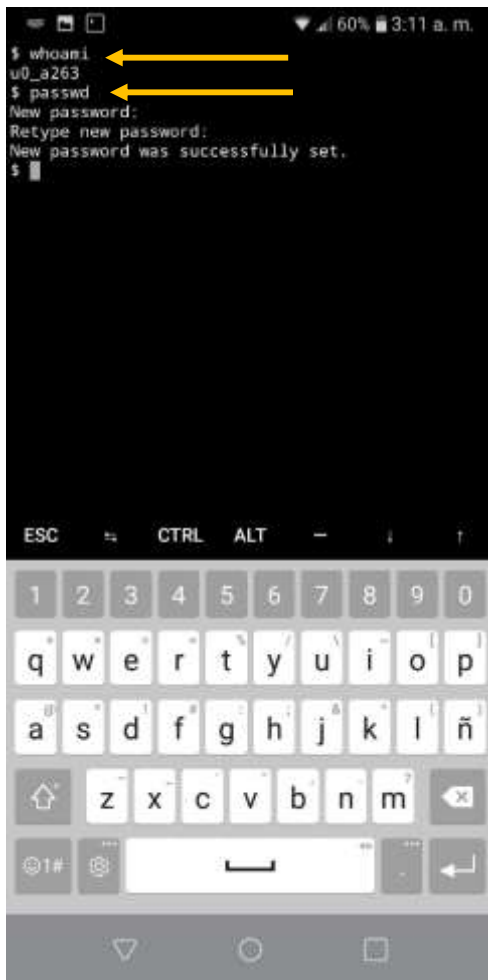
之后我们必须给这个用户一个密码，所以我们要执行下面的命令。

\$ passwd

它会要求我们输入密码并按回车键，再次要求我们输入密码我们确认后按回车键，如果已经**成功了**"新密码设置成功"在标记错误的情况下有可能是密码没有输入正确。再次执行该程序。

然后要知道我们在Termux中的IP是什么，我们输入以下命令，IP在"inet"后面。

\$ ifconfig -a



The screenshot shows a Termux terminal window with a black background and white text. The status bar at the top shows 60% battery and 3:11 a.m. The terminal output is as follows:

```
$ whoami
u0_a263
$ passwd
New password:
Retype new password:
New password was successfully set.
$
```

Two yellow arrows point to the '\$ passwd' and '\$' prompts. Below the terminal is a virtual keyboard with a QWERTY layout and function keys like ESC, CTRL, ALT, and a search icon.



The screenshot shows a Termux terminal window with a black background and white text. The status bar at the top shows 61% battery and 2:57 a.m. The terminal output is as follows:

```
e 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>
> mtu 1500
    inet 192.168.1.68 netmask 255.255.255.0
    broadcast 192.168.1.255
    inet6 fe80::257:c1ff:fee6:3051 prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 1000 (UNSPEC)
    RX packets 908745 bytes 947916536 (904.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 601034 bytes 93496881 (89.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

$
```

A yellow arrow points to the 'inet 192.168.1.68' line. Below the terminal is a virtual keyboard with a QWERTY layout and function keys like ESC, CTRL, ALT, and a search icon.

现在

是时候启动手机上的SSH服务器服务了，这样你就可以从电脑上接收会话了。我们在Termux终端执行以下命令，这个命令没有任何结果。

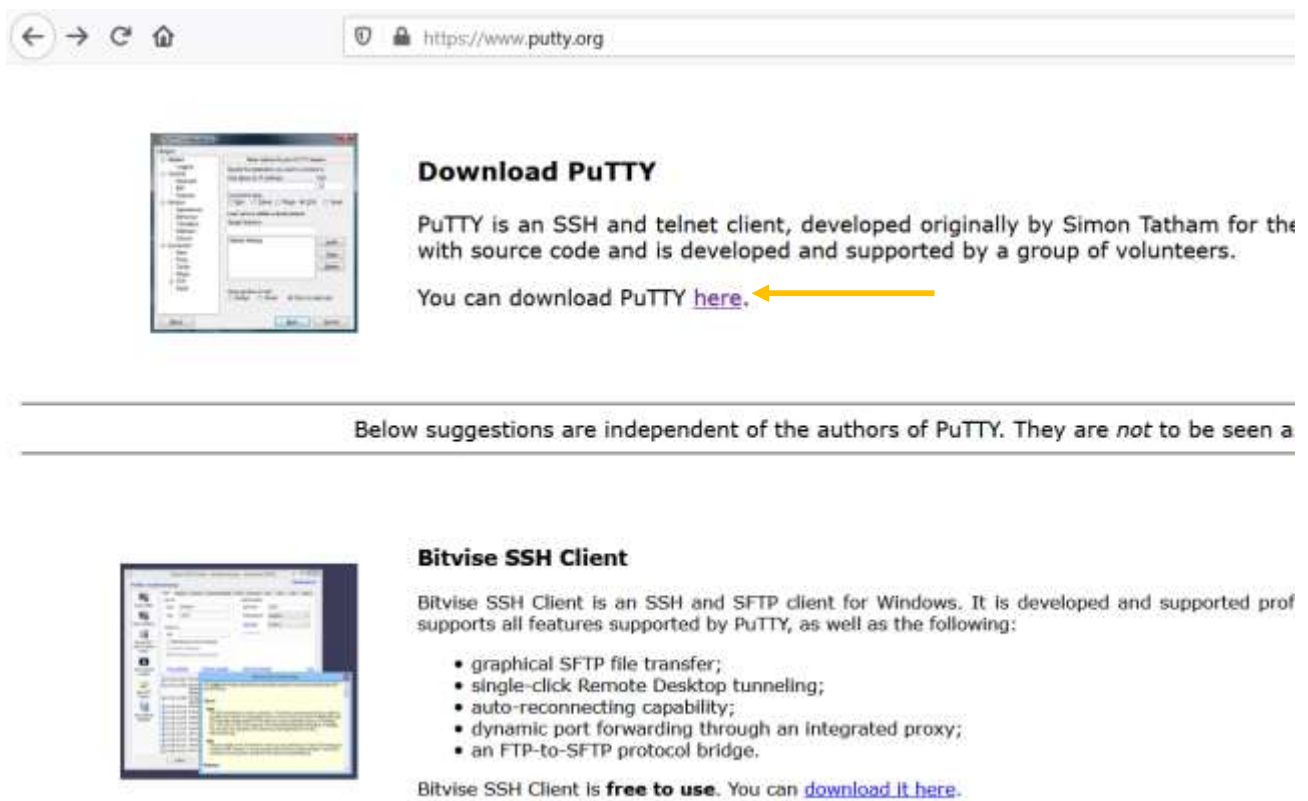
\$ sshd



现在我们要在电脑上安装一个程序，这个程序可以从电脑上与手机的SSH服务器进行通信。

我们要去<https://www.putty.org>

选择"您可以在这里下载PuTTY"的链接所在。



选择32位的版本，不管你的系统是不是64位的都可以。

Download PuTTY: latest release

[Home](#) | [FAQ](#) | [Feedback](#) | [Licence](#) | [Updates](#) | [Mirrors](#)
Download: [Stable](#) | [Snapshot](#) | [Docs](#) | [Contact](#)

This page contains download links for the latest released version of PuTTY. Currently this is 0.73, released on 2019-09-29.

When new releases come out, this page will update to contain the latest, so this is a good page to bookmark or link to. Alternative Release versions of PuTTY are versions we think are reasonably likely to work well. However, they are often not the most up-to-date, so you may want to check out the [development snapshots](#), to see if the problem has already been fixed in those versions.

Package files

You probably want one of these. They include versions of all the PuTTY utilities.

(Not sure whether you want the 32-bit or the 64-bit version? Read the [FAQ entry](#).)

MSI ('Windows Installer')

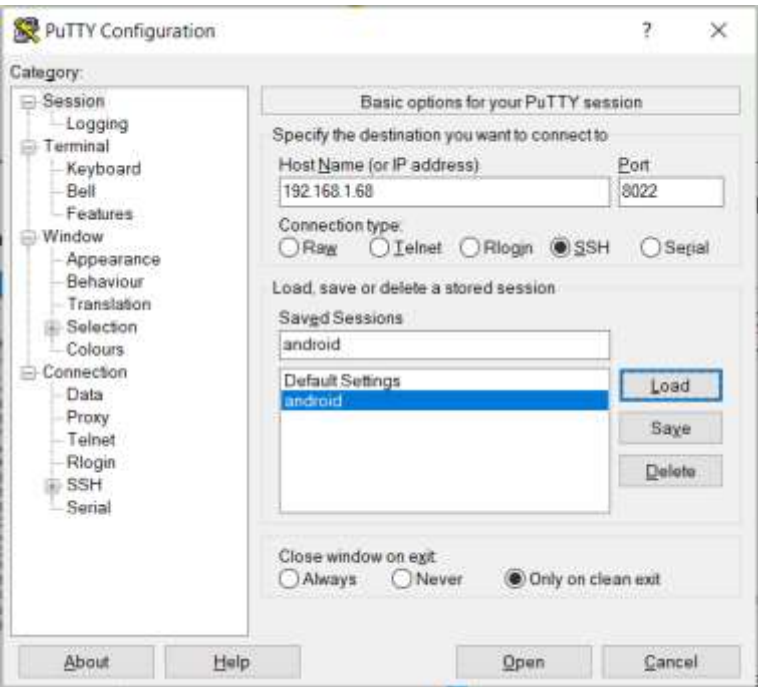
32-bit:	putty-0.73-installer.msi	(or by FTP)	(signature)
64-bit:	putty-64bit-0.73-installer.msi	(or by FTP)	(signature)

Unix source archive

.tar.gz:	putty-0.73.tar.gz	(or by FTP)	(signature)
----------	-----------------------------------	-------------	-------------

下载到电脑后，运行它并以默认选项进行安装。然后启动PuTTY应用程序。

在这个环节中，我们将从我们安装在手机中的Openssh服务器中输入数据。



输入手机的IP。

主机名或IP地址。

192.168.1.68 (IP例子)

港口：

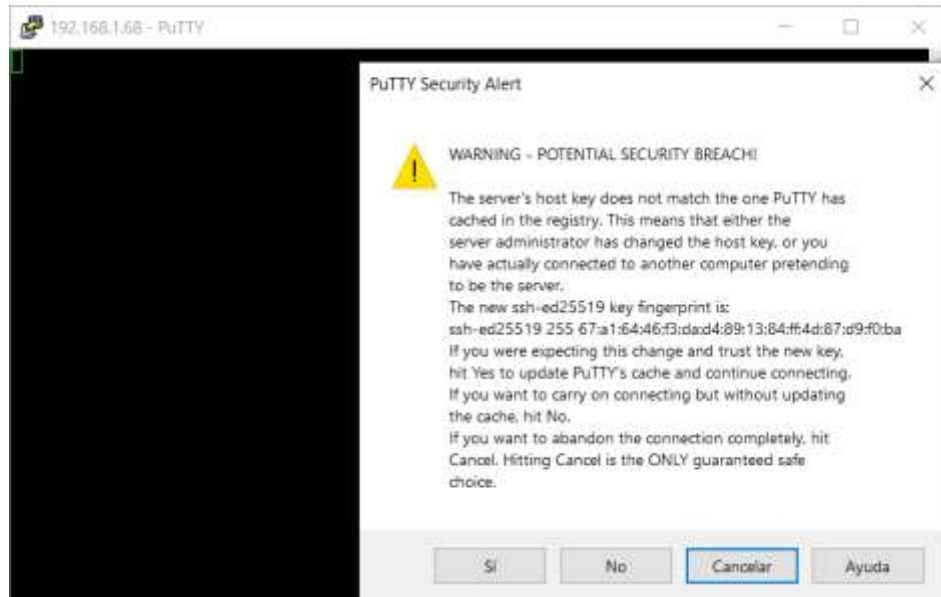
8022（移动SSH服务器的默认端口）。

我们可以在"保存的会话"中给会话起个名字，然后点击

保存按钮。

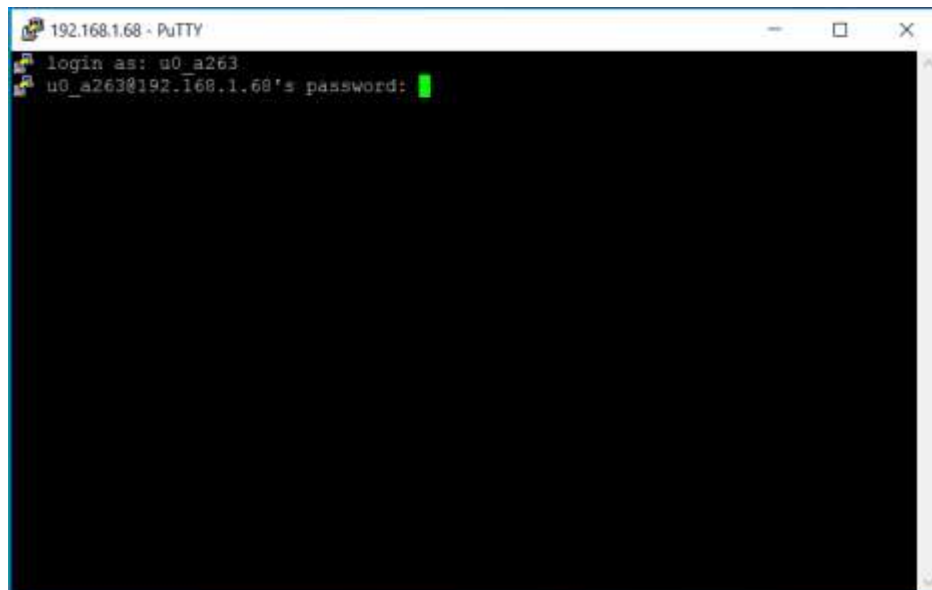
稍后在下半部分我们按下打开连接服务器的按钮，给出"Open"。

在PC上，当您第一次连接时，您会被要求确认信息加密密钥，点击"是"按钮。

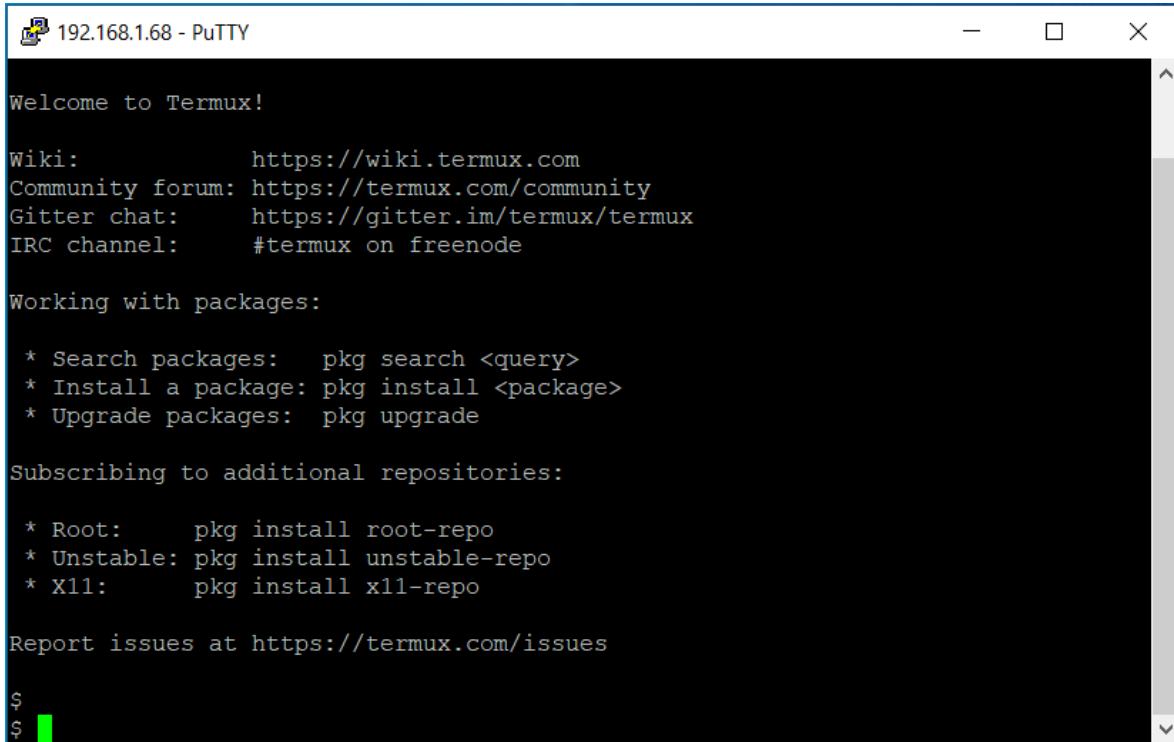


稍后会问我们要连接的用户。我们将使用之前获得的信息（用户和密码）。

在**登录为**：我们必须输入我们的用户，并给回车，然后我们会要求密码再次给回车按钮。



如果数据正确，我们将在从PC（客户端）在手机（SSH服务器）上执行的SSH（安全壳）会话中。



```
192.168.1.68 - PuTTY
Welcome to Termux!

Wiki:          https://wiki.termux.com
Community forum: https://termux.com/community
Gitter chat:   https://gitter.im/termux/termux
IRC channel:   #termux on freenode

Working with packages:

* Search packages:  pkg search <query>
* Install a package: pkg install <package>
* Upgrade packages: pkg upgrade

Subscribing to additional repositories:

* Root:    pkg install root-repo
* Unstable: pkg install unstable-repo
* X11:     pkg install x11-repo

Report issues at https://termux.com/issues

$
$
```

重要提示：请记住，PC的IP（地址）和连接在同一WiFi上的手机的IP（地址）可能会在每次断开和重新连接时发生变化，所以我们必须仔细检查每个设备的地址，这将确保设备之间通过手机的SSH服务器和PC（客户端）连接成功。

8. Ambientes Blockly (App Inventor, AppyBuilder和Thunkable)。

App Inventor是谷歌实验室创建的软件开发环境，用于构建Android操作系统的应用程序。用户可以，直观地，从一组基本工具，链接一系列的块来创建应用程序。该系统是免费的，可以方便地从网上下载。使用App Inventor创建的应用程序非常容易创建，因为不需要任何编程语言知识。

目前所有使用Blockly技术的环境，如AppyBuilder和Thunkable等都有他们的免费版本，他们的使用方式可以通过互联网在他们不同的站点，也可以在家里安装。

组成Mini BLoclyChain架构的块已经在App inventor和AppyBuilder中进行了测试，但由于它们的代码优化，应该可以在其他平台上使用。

在线版本。

应用发明家。

<https://appinventor.mit.edu/>

AppyBuilder。

<http://appybuilder.com/>

可通关。

<https://thunkable.com/>

要安装在您的计算机（PC）上的版本。

<https://sites.google.com/site/aprendeappinventor/instala-app-inventor>

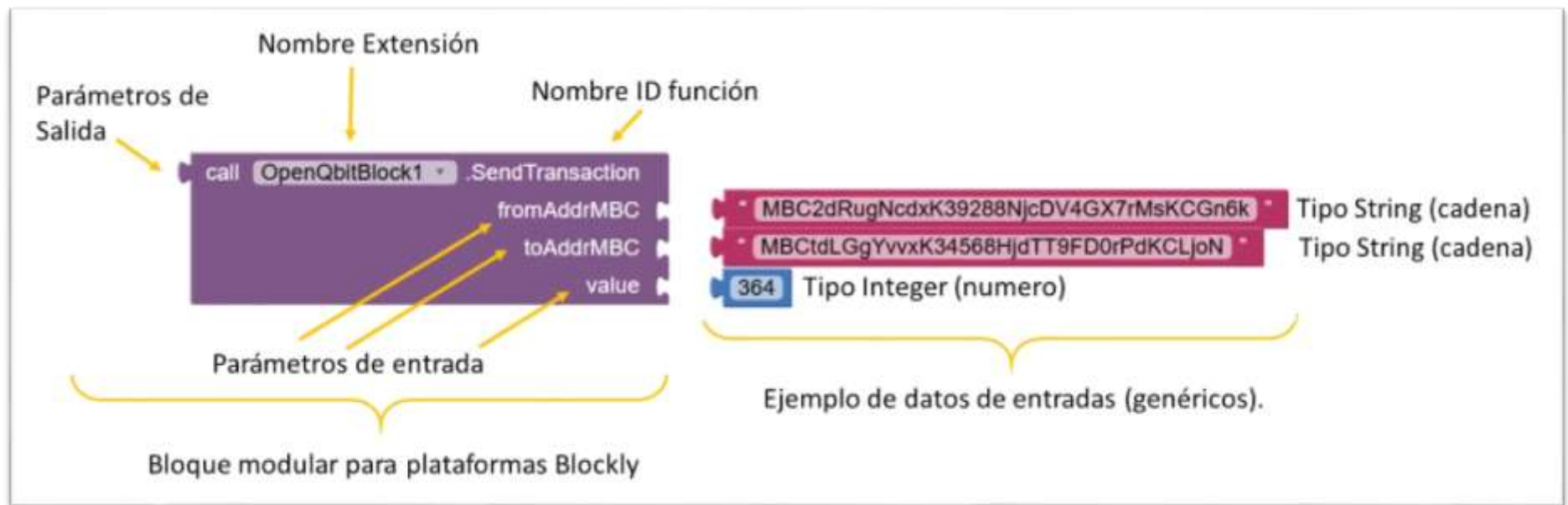
为Blockly区块的开发者提供环境。

<https://editor.appybuilder.com/login.php>

9. 迷你QRNG中块的定义和使用。

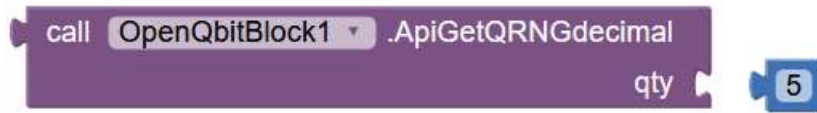
我们先来解释一下所有区块会有数据分布，它们的使用语法和配置。

在下面的例子中，我们可以看到一个模块块及其输入和输出参数，以及输入数据的类型，这些数据的类型可以是String（字符串）或Integer（整数或十进制）。我们将展示如何使用它，并配置它以使其正常运行。



每一个模块块都会有它的描述，并会被命名，如果它有任何强制性或可选性的依赖其他模块作为输入参数，集成过程将被公布。让我们从OpenQbitQRNGwithSSH扩展的块开始。

用于生成十进制随机量子数的块 - (ApiGetQRNGdecimal)



输入参数：**数量<整数>**

输出参数：给出输入的随机量子小数的数量"qty"，输入的数字在0和1的范围内，以JSON格式。

例如：

qty = 5; output: {"result": [0.5843012986202495, 0.7746497687824652, 0.05951126805960929, 0.1986079055812694, 0.03689783439899279]}。

描述：量子随机数生成器（QRNG）API

用于生成十进制随机量子数的块 - (ApiGetQRNGinteger)



输入参数：**数量<整数>**，**最小<整数>**，**最大<最大>**。

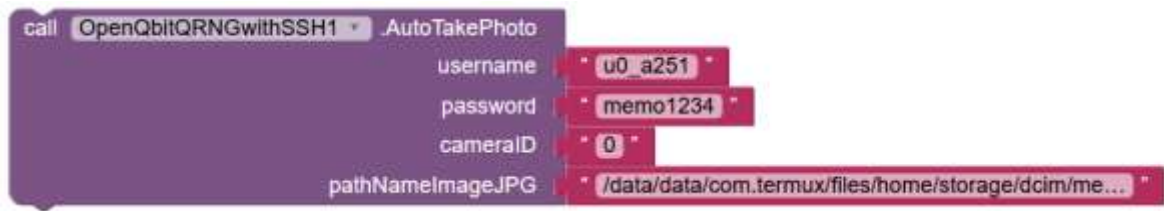
输出参数：给出输入的随机量子整数的数量"qty"，这些数字在最小和最大的范围内，采用JSON格式。

例如：

qty = 8, min = 1, max = 100; output: {"result": [3, 53, 11, 2, 66, 44, 9, 78]}

描述：量子随机数生成器（QRNG）API

阻止自动拍照--（自动拍照）。



输入参数：用户名 < String>, 密码 < String>, cameraID < String>, pathNameImageJPG < String>。

强制性依赖：要使用这个块，你必须满足两个软件依赖；在Termux终端中安装Termux-API模块。这个模块包含自动拍照和上传之前安装的SSH服务器的过程。

输出参数：以指定的路径输出JPG格式的照片（图像）。在你必须的道路上

描述：无需用户干预，自动创建JPG照片。

要安装Termux-API，必须在Termux终端中执行以下命令。

\$ pkg install termux-api

```
$ pkg install termux-api
Ign:2 https://dl.bintray.com/grimler/game-packag
es-24 games InRelease
Ign:3 https://dl.bintray.com/grimler/science-pac
kages-24 science InRelease
Ign:1 https://dl.bintray.com/termux/termux-packa
ges-24 stable InRelease
Get:5 https://dl.bintray.com/grimler/game-packag
es-24 games Release [5344 B]
Get:6 https://dl.bintray.com/grimler/science-pac
kages-24 science Release [6191 B]
Get:4 https://dl.bintray.com/termux/termux-packa
ges-24 stable Release [8255 B]
Get:7 https://dl.bintray.com/grimler/game-packag
es-24 games Release.gpg [475 B]
Get:8 https://dl.bintray.com/grimler/science-pac
kages-24 science Release.gpg [475 B]
Get:9 https://dl.bintray.com/termux/termux-packa
ges-24 stable Release.gpg [821 B]
0% [8 Release.gpg gpgv 6191 B]
```

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be upgraded:
  termux-api
1 upgraded, 0 newly installed, 0 to remove and 7
4 not upgraded.
Need to get 21.2 kB of archives.
After this operation, 4096 B of additional disk
space will be used.
Get:1 https://dl.bintray.com/termux/termux-packa
ges-24 stable/main arm termux-api arm 0.50-1 [21
.2 kB]
Fetched 21.2 kB in 1s (18.7 kB/s)
(Reading database ... 25317 files and directorie
s currently installed.)
Preparing to unpack .../termux-api_0.50-1_arm.de
b ...
Unpacking termux-api (0.50-1) over (0.50) ...
Setting up termux-api (0.50-1) ...
$
```

在Termux终端上执行以下命令，即可知道移动设备（智能手机）的ID（照片镜头识别器）的数量、数量和位置。

\$ termux-camera-info



```
$ termux-camera-info
[
  {
    "id": "0",
    "facing": "back",
    "jpeg_output_sizes": [
      {
        "width": 4160,
        "height": 3120
      },
      {
        "width": 4160,
        "height": 2340
      },
      {
        "width": 4160,
        "height": 2080
      },
      {
        "width": 3264,
        "height": 2448
      },
      {

```



```
    "manual_sensor",
    "manual_post_processing",
    5,
    6,
    4,
    7,
    "raw"
  ],
  {
    "id": "1",
    "facing": "front",
    "jpeg_output_sizes": [
      {
        "width": 2560,
        "height": 1920
      },
      {
        "width": 2560,
        "height": 1600
      },
      {
        "width": 2560,

```

在我们的例子中，我们使用的LG Q6 smarpone背面有两个ID"0"，正面有"1"。

现在，让我们测试API使用后置镜头的ID"0"拍摄一张照片，并在我们的案例中给它一个albitary名称test.jpg。

请记住，API只提供JPG格式的照片。

\$ termux-camera-photo -c 0 test.jpg。

前面的命令一定是自动创建了一个名字为test.jpg的文件，如果是这样的话，我们就可以使用块（AutoTakePhoto），别忘了用命令启动我们的本地SSH服务器：**\$ sshd**

注意：在变量pathNameImageJPG中，应该考虑使用Termux终端内部访问智能手机存储的路径。

/data/data/com.termux/files/home/storage/dcim/example.jpg。

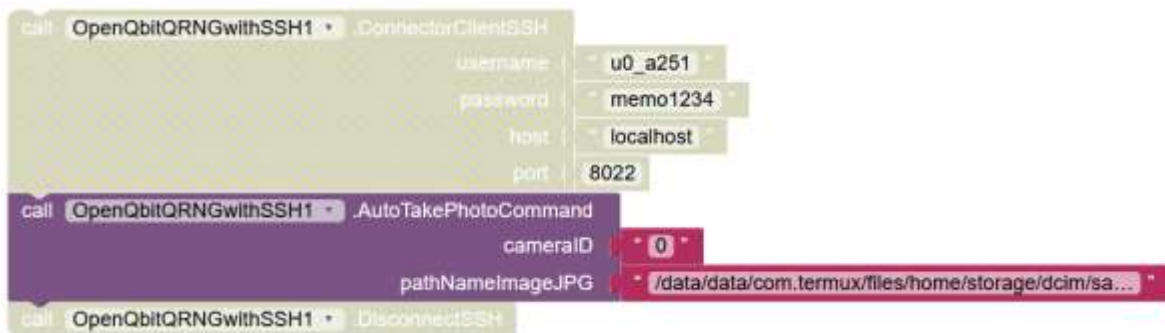
之前在安卓上的路线会和。

/mnt/sdcard/dcim/example.jpg

但是，我们一定要记住，在Termux终端中，查看手机开机的有效路径一定要始终认为是默认路径。

/data/data/com.termux/files/home/storage。

阻止自动拍照 ONLY COMMAND - (AutoTakePhoneCommand)。



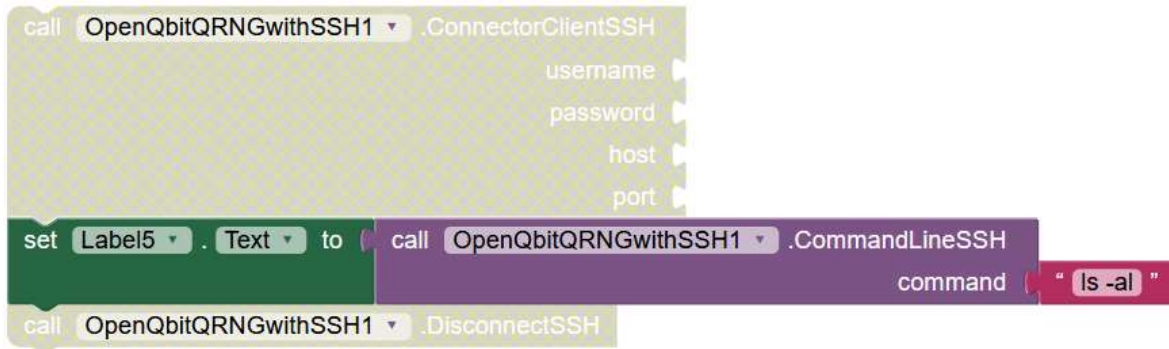
输入参数：CameraID <String>, pathNameImageJPG <String>。

强制性依赖：Block（ConnectorClientSSH）、Block（DisconnectSSH）。

输出参数：以指定的路径输出JPG格式的照片（图像）。

描述：无需用户干预，自动创建JPG照片。但与块（AutoTakePhoto）相比，不同的是，这个块只包含创建照片的命令，你需要先用块连接到SSH服务器（ConnectClientSSH），再使用块（DisconnectSSH）。

在Termux终端上执行命令的区块 - (CommandLineSSH)



输入参数：命令<字符串>。

强制性依赖：Block（ConnectorClientSSH）、Block（DisconnectSSH）。

输出参数：执行在Termux终端输入的命令。

描述：一个输入的命令被执行，首先需要块连接到SSH服务器（ConnectClientSSH），然后使用块（DisconnectSSH）。

块连接到远程或本地SSH服务器--（ConnectorClientSSH）。



输入参数：用户名<string>，密码<string>，主机<string>，端口<整数>。

输出参数：如果与Termux终端的ssh服务器连接成功，则给我们一个消息；"连接SSH"，如果不成功，则给我们一个NULL消息。

描述：通过SSH（安全壳）通信协议，将所选的SSH服务器连接到Termux终端的通信块。

用Base64算法（DecoderFileBase64）对文件进行解码的块。

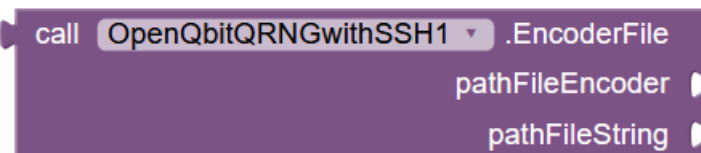


输入参数：pathFileBase64 <字符串>， pathFileOrigin <字符串>。

输出参数：输入块中的源文件（EncoderFileBase64）。

描述：Base64文件被转换为插入块中的原始文件（EncoderFileBase64）。

块将文件转换为Base64格式 - (EncoderFile)

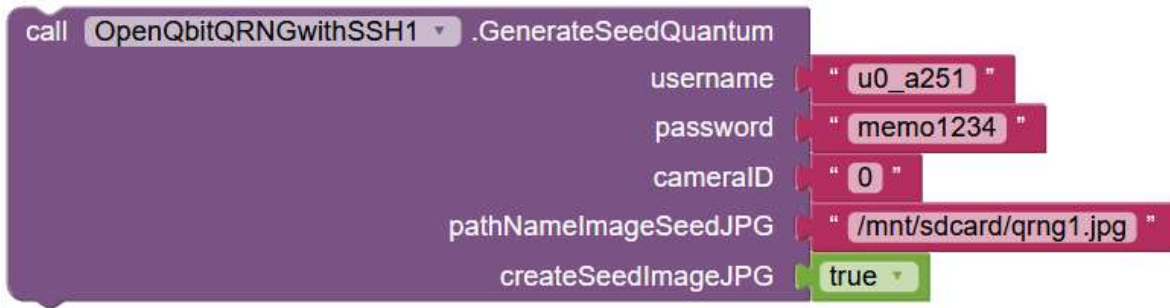


输入参数：pathFileOrigin <String> , pathFileBase64 <String>。

输出参数：Base64编码文件。

描述：将任何格式的源文件转换为Base64文件。文件名可以是任意的，由用户选择。

生成QRNG（量子随机数生成器）的区块 - (GenerateSeedQuantum)



输入参数：用户名<String>，密码<String>，摄像头ID<String>，路径名ImageJPG<String>。createSeedImageJPG<Boolean>。

如果布尔值为"True"，当每次执行该块时，将以输入的路径名称创建新的种子JPG图像。如果Boolean值为"False"，我们会停用JPG图像（照片）的选项，我们可以手动指出图像在我们选择中的位置，它可以是任何格式。

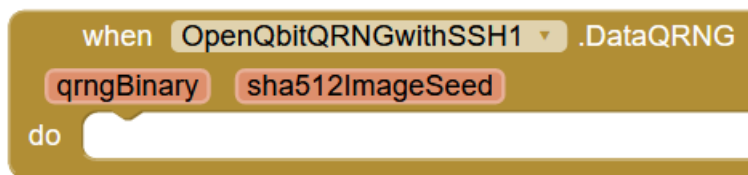
注意：生成QRNG的最佳结果是基于"RAW"格式的图像。DNG格式示例。

强制性依赖性：上述的Termux-API必须安装在区块中（AutoTakePhoto）。

输出参数：事件执行(DataQRNG)，并给我们两个值。

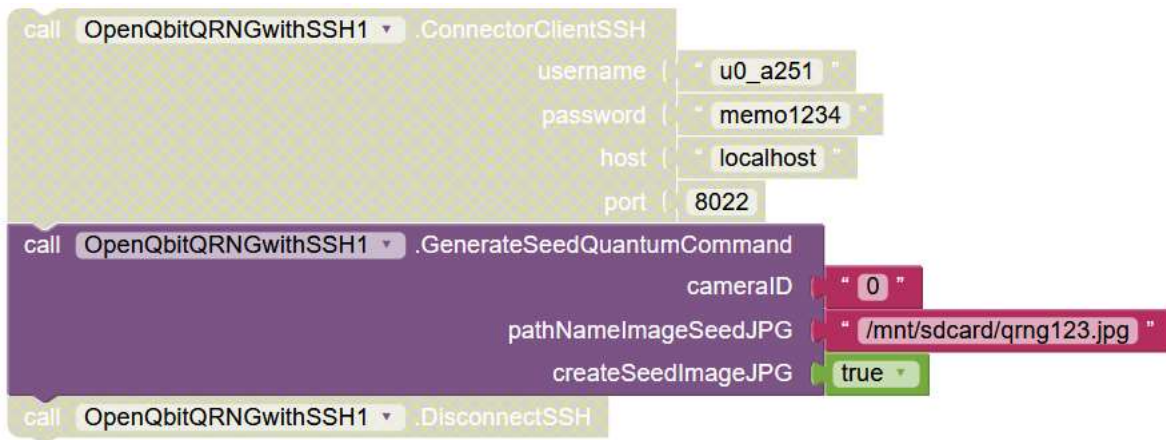
qrngBinary.-一串随机二进制数。

Sha512ImageSeed - 从JPG种子图像中提取随机数的Sha512。



描述：通过手机摄像头的光学传感器生成量子随机数(QRNG)，该算法是在采集随机照片的基础上，应用算法传递一串二进制数。

产生QRNG（量子随机数生成器）的块--（GenerateSeedQuantumCommand）。



输入参数：CameraID <String>, pathNameImageJPG <String>。 createSeedImageJPG <Boolean>。

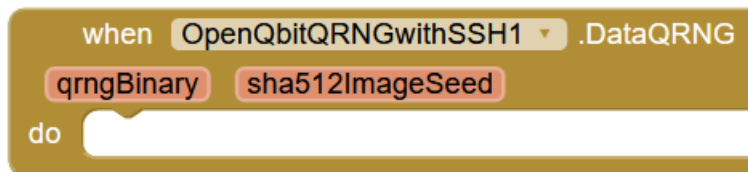
如果布尔值为"True", 当每次执行该块时, 将以输入的路径名称创建新的种子JPG图像。如果Boolean值为"False", 我们会停用JPG图像（照片）的选项, 我们可以手动指出图像在我们选择中的位置, 它可以是任何格式。

强制性依赖：Block（ConnectorClientSSH）、Block（DisconnectSSH）。

输出参数：事件执行(DataQRNG), 并给我们两个值。

qrngBinary.-一串随机二进制数。

Sha512ImageSeed - 从JPG种子图像中提取随机数的Sha512。



描述：通过手机摄像头的光学传感器生成量子随机数(QRNG), 该算法是在采集随机照片的基础上, 应用算法传递一串二进制数。

但与区块（GenerateSeedQuantum）相比，不同的是，这个区块只包含执行QRNG反应算法的命令，你需要先用区块连接SSH服务器（ConnectClientSSH），再使用区块（DisconnectSSH）。

块获取图像（照片）中的香农熵--（GetShannonEntropyFile）。



输入参数：用户名 <字符串> , 密码 <字符串> , pathFileImage <字符串>。

强制性依赖：Shannon_entropy模块需要安装在Termux终端。

输出参数：提供图像的熵。

例如：

产出：8.94596789873美元

描述：它给我们提供了一个图像的熵。熵是产生优质随机数的基本参数，熵越高，结果越好。

要安装Shannon熵模块，我们首先需要安装Python包，然后在Termux终端用以下命令安装Pillow和Shannon_entropy模块。

```
$ apt install Python
```

```
$ pip install Pillow
```

```
$ pip install Shannon_entropy。
```

```
$ apt install python
Reading package lists... Done
Building dependency tree
Reading state information... Done
python is already the newest version (3.8.3).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
$
```

```
$ pip install Pillow
Requirement already satisfied: Pillow in /data/d
ata/com.termux/files/usr/lib/python3.8/site-pack
ages (7.2.0)
$
```

```
$ pip install shannon_entropy
Requirement already satisfied: shannon_entropy i
n /data/data/com.termux/files/usr/lib/python3.8/
site-packages (0.2.1)
Requirement already satisfied: Pillow in /data/d
ata/com.termux/files/usr/lib/python3.8/site-pack
ages (from shannon_entropy) (7.2.0)
$
```

然后我们要在Termux的"Home"目录下创建一个名为"entropy.py"的Python文件，里面的代码如下。

从IL导入Image

导入数学

从shannon_entropy导入*。

导入系统

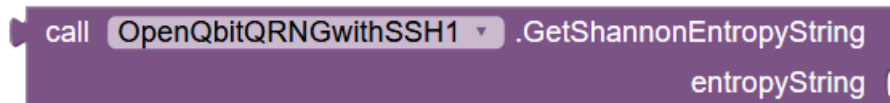
```
Img=Image.open(sys.argv[1])
```

打印Shannon_entropy(img))

我们保存文件，并有我们的环境与块使用（GetShannonEntropyFile）。

小贴士：事实上，通过这个Python安装，你可以用这种语言创建自己的程序，并通过区块（ConnectorClientSSH）运行。

从字符串中获取香农熵的块--（GetShannonEntropyString）。

A screenshot of a code editor with a purple background. It shows a function call: 'call OpenQbitQRNGwithSSH1 .GetShannonEntropyString entropyString'. The function name 'OpenQbitQRNGwithSSH1' is in a dropdown menu, and the output variable 'entropyString' is at the end of the line.

输入参数：entropyString>字符串>。

输出参数：提供一个字符串的熵。

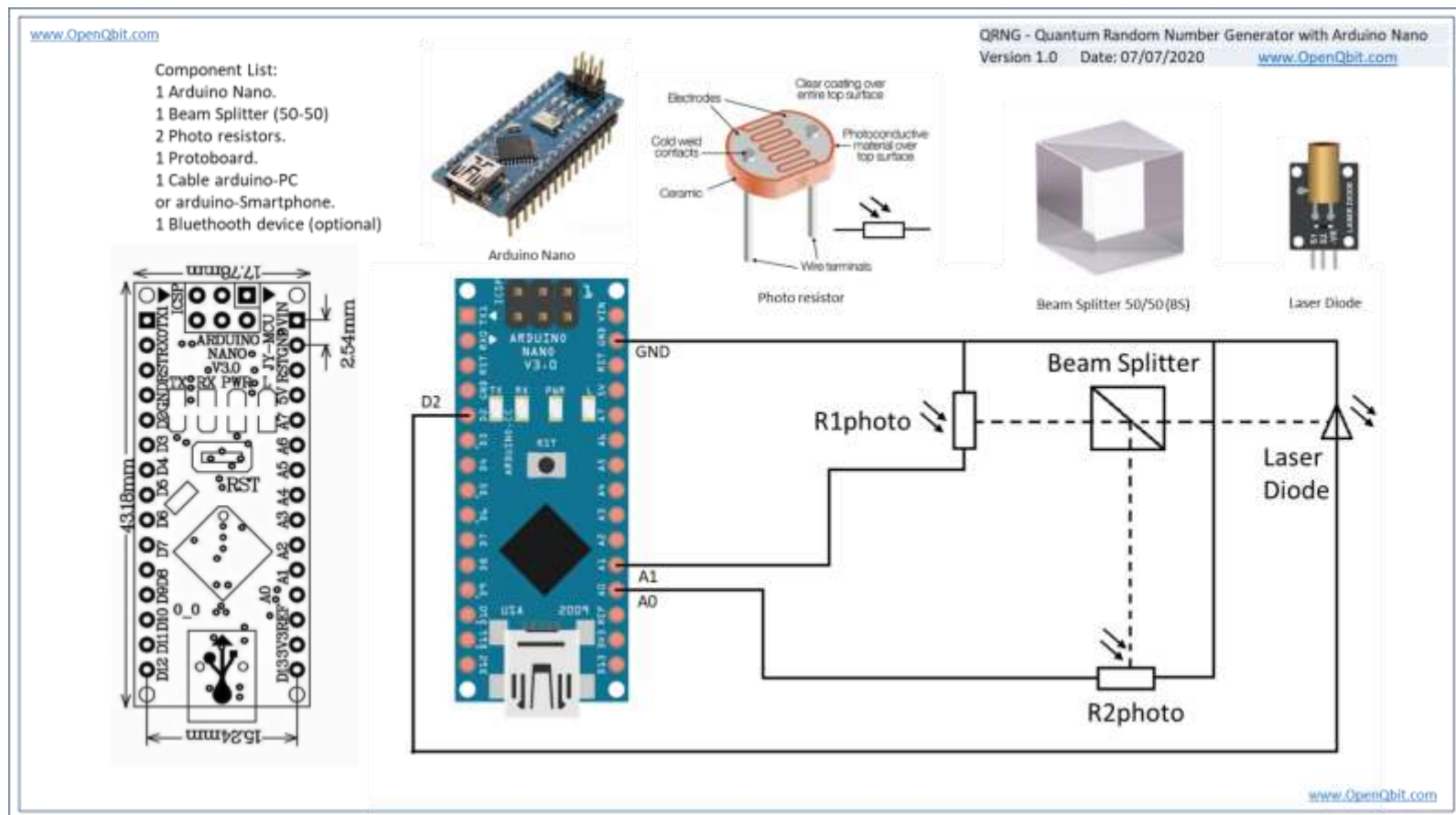
例如：

产出：5.76002345671人

描述：它给出了一串字符的熵。熵是产生优质随机数的基本参数，熵越高，结果越好。

10. 创建QRNG的"硬件"设备。

现在，我们将创建一个物理的"硬件"设备，以产生量子随机数（QRNG），用廉价的组件，可以很容易地在家里组装。



www.OpenQbit.com

QRNG - Quantum Random Number Generator with Arduino Nano
Version 1.0 Date: 07/07/2020 www.OpenQbit.com

QRNGv1.0.ino

Software
Program to arduino nano.

```
/* OpenQbitQRNG Firmware V1.0
*Author: Guillermo Vidal
*Copyright © 2020 OpenQbit, Inc.
*License: MIT
*/

int triggerQ = 2; // This pin will pulse our quantum circuit
int QuA0Pin = A0; // This pin measures the horizontal polarized photons
int QuA1Pin = A1; // This pin measures the vertically polarized photons
float Qu0 = 0;
float Qu1 = 0;

void setup() {
  // Just setting up triggerPin and serial connection
  pinMode(triggerQ, OUTPUT); // sets the digital pin 2 as output
  Serial.begin(9600);
}

int Random() {
  // Pulse the laser
  digitalWrite(triggerQ, HIGH);
  delay(300);
  digitalWrite(triggerQ, LOW);
  delay(300);
  // Read the photoresistors
  Qu0 = analogRead(QuA0Pin);
  Qu1 = analogRead(QuA1Pin);
  // Determine random bit
  if(Qu0>Qu1) { // More photons in the Qu0 mode, return 0
    return 0;
  } if(Qu0 < Qu1) { // More photons in the Qu1 mode, return 1
    return 1;
  } else {
    /* The same number of photons are in both modes!
    This is actually not an uncommon occurrence, for our
    purposes we will simply run the function recursively until
    a random bit can be generated.
    */
    Random();
  }
}

void loop() {
  Serial.print(Random());
}
```

Output console

0010110101011110101011010.....

www.OpenQbit.com

迷你QRNG - DIY - "自己动手"。

编译QRNGv10.inio程序并上传到arduous nano...



```
QRNGv10 Arduino 1.8.10
Archivo Editor Programa Herramientas Ayuda

QRNGv10

int triggerQ = 2; // This pin will pulse our quantum diposit
int QaAPin = A0; // This pin measures the horizontal polarized photons
int QvAPin = A1; // This pin measures the vertically polarized photons
float Qa0 = 0;
float Qv1 = 0;

void setup() {
  // Just setting up triggerPin and serial connection
  pinMode(triggerQ, OUTPUT); // sets the digital pin 2 as output
  Serial.begin(9600);
}

int Random() {
  // Pulse the laser
  digitalWrite(triggerQ, HIGH);
  delay(300);
  digitalWrite(triggerQ, LOW);
  delay(300);
  // Read the phototransistors
  Qa0 = analogRead(QaAPin);
  Qv1 = analogRead(QvAPin);
  // Determine random bit
  if(Qa0 > Qv1) { // More photons in the Qa0 mode, return 0
    return 0;
  } if(Qa0 < Qv1) { // More photons in the Qv1 mode, return 1
    return 1;
  } else {
    /* The case where both photons are in both modes!
     * This is actually not an uncommon occurrence. For the
     * purposes we will simply run the function repeatedly until
     * a random bit can be generated.
     */
    Random();
  }
}

void loop() {
  Serial.print(Random());
}
```

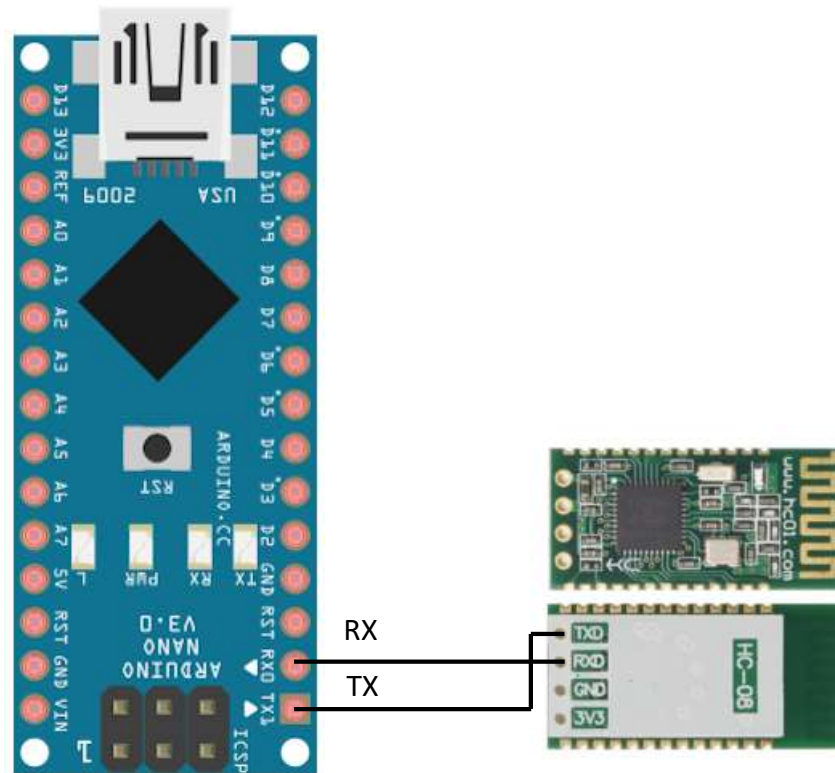
Compiled:

El sketch usa 2352 bytes (7%) del espacio de almacenamiento de programa. El máximo es 32768 bytes.
Las Variables Globales usan 140 bytes (7%) de la memoria dinámica, dejando 960 bytes para las Variables locales. El máximo es 2048 bytes.

10 Arduino Generated Libraries COM4

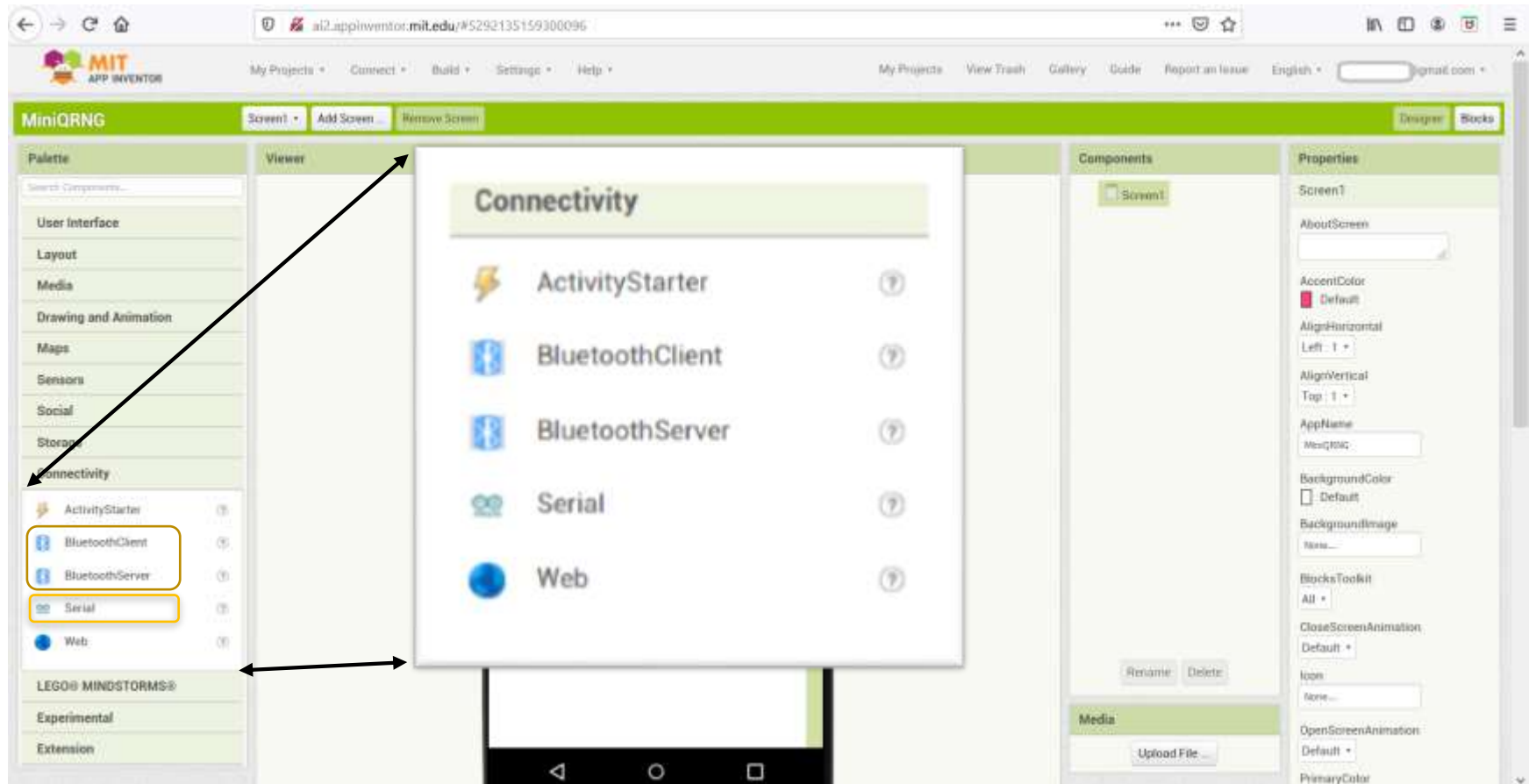
与arduous nano的通信方式有两种，一种是通过Serial端口，另一种是通过蓝牙连接。

对于蓝牙的连接非常简单，我们只需要购买HC-08模块或者类似的模块，然后按照以下方式连接即可。



迷你QRNG - DIY - "自己动手"。

以下串行或蓝牙组件可用于将App Inventor连接到Arduino。



现在编译并加载程序QRNGv10.inio只缺乏与arduous nano的通信，以保存数据（量子随机数），这些将是二进制格式，然而，获得的数据可以很容易地传递到另一种格式，如十六进制或十进制，这取决于最终的要求。

最后，要想看看串口或蓝牙连接如何工作的例子，这里有一些参考链接。

请记住，一切都通过Blockly编程，以测试与App Inventor这已经有块与arduino串行或其他blockly系统可能是类似的蓝牙焦油在线通信。

[http://kio4.com/appinventor/9A0_bluetooth RTX.htm。](http://kio4.com/appinventor/9A0_bluetooth_RTX.htm)

[http://kio4.com/appinventor/index.htm#bluetooth。](http://kio4.com/appinventor/index.htm#bluetooth)

<https://community.appinventor.mit.edu/>

11.附件"OpenQbit量子计算"。

量子计算是如何工作的？⁽²⁾

数字化转型给世界带来的变化比以往任何时候都要快，你会相信数字时代即将结束吗？**数字扫盲**已经被确定为一个领域，在这个领域，开放知识和学习技术的机会是迫切需要的，以解决社会和经济发展中的差距。随着另一个能够以惊人的速度和力量改变现有模式的新技术浪潮的即将到来，学习数字时代的关键概念将变得更加关键：**量子技术**。

在本文中，我们比较了传统计算和量子计算的基本概念；并开始探讨它们在其他相关领域的应用。

什么是量子技术？

纵观历史，人类通过科学了解自然界的运作方式，从而发展了科技。1900年至1930年间，对一些尚不十分清楚的物理现象的研究，产生了一种新的物理理论--**量子力学**。这一理论描述和解释了微观世界的功能，即分子、原子或电子的自然栖息地。由于这个理论，不仅可以解释这些现象，而且可以理解亚原子现实以一种完全反直觉的、近乎神奇的方式运作，在微观世界中发生了宏观世界中没有发生的事件。

这些量子**特性**包括量子叠加、量子纠缠和量子传送。

- **量子叠加**描述了一个粒子如何在同一时间处于不同的状态。
- **量子纠缠**描述了两个相距如意的粒子如何以这样的方式相关联，当与其中一个粒子相互作用时，另一个粒子会意识到它。
- **量子传送**利用量子纠缠将信息从一个地方传送到空间的另一个地方，而不需要穿越空间。

量子技术就是基于这些亚原子性质的量子特性。

在这种情况下，今天通过量子力学对微观世界的理解，使我们能够发明和设计能够改善人们生活的技术。使用量子现象的技术有很多，而且非常不同，其中一些技术，如激光或磁共振成像（MRI），已经陪伴我们半个多世纪了。然而，目前我们正在见证量子计算、量子信息、量子模拟、量子光学、量子计量、量子时钟或量子传感器等领域的技术革命。

什么是量子计算？首先，你要了解经典计算。




FIGURA 1.
Ejemplos de caracteres en lenguaje binario.

Character	Bits
7	111
A	01000001
\$	00100100
:)	0011101000101001

为了理解量子计算机的工作原理，我们可以方便地先解释一下我们日常使用的计算机（我们在本文中称之为数字计算机或经典计算机）的工作原理。这些和其余电子设备如平板电脑或手机一样，都是以比特为基本记忆单位。这意味着程序和应用程序是以比特为单位进行编码的，也就是以0和1的二进制语言进行编码。每当我们与这些设备进行交互时，例如按下键盘上的一个键，计算机内部就会产生、销毁和/或修改零和一的字符串。

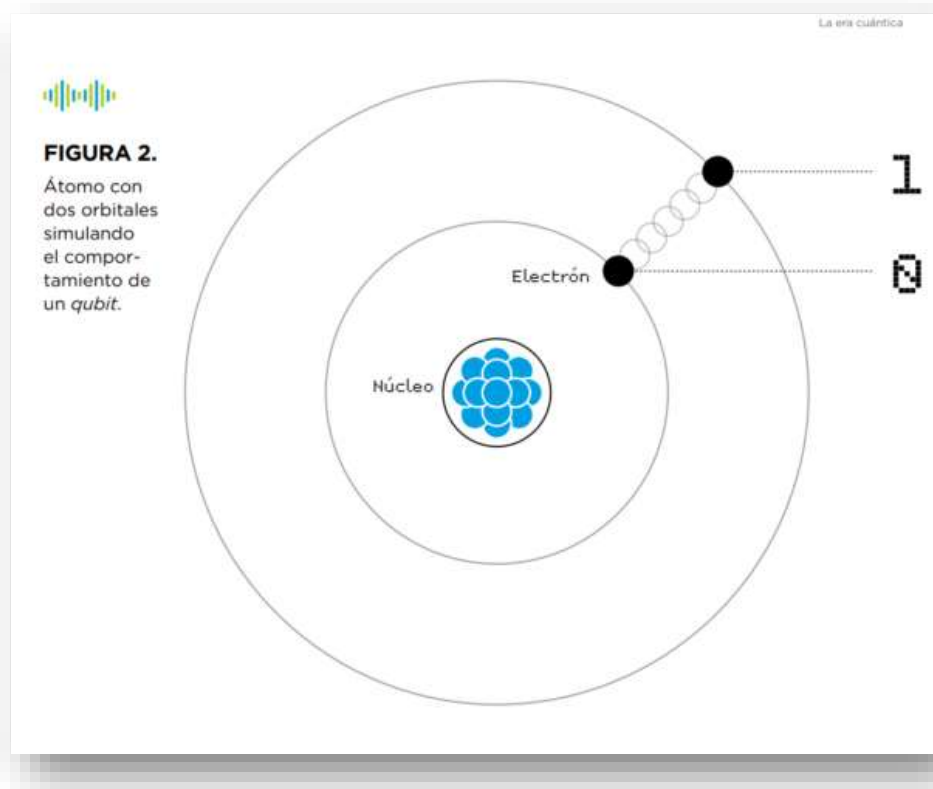
有趣的问题是，这些0和1在物理上是计算机内部的什么？零态和一态对应的是电流，这些电流通过称为晶体管的微观部件循环或不循环，晶体管作为开关。当没有电流流过时，晶体管为"关"，对应于位0；当有电流流过时，为"开"，对应于位1。

更简单地说，就好比0位和1位对应于空穴，所以空穴是0位，电子占据的空穴是1位。这就是为什么这些设备被称为电子器件的原因。举个例子，图1显示了一些字符的二进制书写。现在我们对今天的计算机是如何工作的有了一个概念，让我们试着了解量子是如何工作的。

从比特到夸比特

量子计算中的基本信息单位是量子比特或qubit。根据定义，Qubits是两级量子系统--我们将在这里看到一些例子--它和比特一样，可以处于低级，对应于低激发状态或能量定义为0，或者处于高级，对应于高激发状态或定义为1。然而，与经典计算的根本区别就在于此，夸比特也可以处于0和1之间的任何一种无限的中间状态，比如一半0一半1的状态，或者是0的四分之三和1的四分之一。

量子算法，指数级强和效算



的大高计。

量子

计算

机的目的是利用量子比特的这些量子特性，因为它们是量子系统，为了运行量子算法，使用重叠和交错的方式，提供比经典算法大得多的处理能力。重要的是要指出，范式的真正变化并不在于做与数字或经典计算机相同的事情--当前的计算机--但更快，正如在许多文章中可以读到的那样，而是量子算法允许以一种完全不同的方式执行某些操作，在许多情况下，这种方式被证明是更有效的--也就是说，在更短的时间内或使用更少的计算资源--。

我们来看一个具体的例子。让我们想象一下，我们在波哥大，我们想知道在一百万个去利马的选择中，哪一条是去利马的最佳路线（ $N=1,000,000$ ）。为了利用计算机找到最优路线，我们需要将100万个选项数字化，这意味着对经典计算机来说，要将它们翻译成比特语言，对量子计算机来说，要将它们翻译成 *qubits*。经典的计算机需要逐一分析所有的路径，直到找到所需的路径，而量子计算机则利用了被称为量子并行的过程，使其可以同时考虑所有的路径。这意味着，经典计算机需要 $N/2$ 步或迭代的顺序，即50万次尝试，而量子计算机只需要对注册表进行 \sqrt{N} 次操作，即1000次尝试，就能找到最优路径。

在前一种情况下，其优势是二次方的，但在其他情况下，其优势甚至是指数的，也就是说，在 n 个 *qubits* 的情况下，我们可以获得相当于 2^n 位的计算能力。为了说明这一点，人们通常会计算，在一台量子计算机中，我们可以拥有更多的基态--更多不同的和同时出现的字符串--比宇宙中的原子数量还要多，据估计，宇宙中的原子数量约为 280 个。另一个例子是，据估计，如果有一台 2000 到 2500 个基态的量子计算机，我们几乎可以破解今天使用的所有密码学（所谓的公钥密码学）。

为什么要了解量子技术？

我们正处在一个数字化转型的时刻，不同的新兴技术如区块链、人工智能、无人机、物联网、虚拟现实、5G、3D打印机、机器人或自动驾驶汽车等越来越多地出现在多个领域和行业。这些技术的目的是提高人类的生活质量，加速发展并产生社会影响，如今这些技术也在同步发展。只是我们很少看到公司开发利用其中两种或多种技术组合的产品，比如区块链和物联网或无人机和人工智能。虽然它们注定要融合，从而产生成倍的影响，但由于它们所处的发展初期阶段，以及具有技术专长的开发人员和人员的稀缺，意味着融合仍是一项有待完成的任务。

由于量子技术具有颠覆性的潜力，预计其不仅会与所有这些新技术相融合，而且会对几乎所有的新技术产生交叉影响。量子计算将威胁到数据的认证、交换和安全存储，对那些密码学有较多相关作用的技术有重大影响，如网络安全或区块链，负面影响不大，但也要考虑5G、物联网或无人机等技术。

你想练习量子计算吗？

网络上已经有几十个量子计算机模拟器，不同的编程语言已经在使用，如C、C++、Java、Matlab、Maxima、Python或Octave。另外，微软推出的Q#等新语言。你可以通过IBM和Rigetti等平台探索和玩转虚拟量子机。

Mini QRNG是由OpenQbit.com公司创建的，该公司专注于开发基于量子计算的技术，适用于私人和公共领域的不同类型。

为什么Mini QRNG与其他QRNG不同，简单来说就是因为该系统是以模块化的方式创建的，可以在家里轻松组装，成本相当低。

- (1) <https://blogs.iadb.org/conocimiento-abierto/es/como-funciona-la-computacion-cuantica/>

12. 软件的许可和使用；

安卓系统

<https://source.android.com/setup/start/licenses>

Termux

<https://github.com/termux/termux-app/blob/master/LICENSE.md>

节点

<https://raw.githubusercontent.com/nodejs/node/master/LICENSE>

蟒蛇

<https://www.python.org/download/releases/2.7/license/>

OpenSSH

<https://www.openssh.com/features.html>

Putty SSH

<https://www.chiark.greenend.org.uk/~sgtatham/putty/licence.html>

麻省理工学院App Inventor 2同伴和App Inventor Blockly。

<https://appinventor.mit.edu/about/termsofservice>

外部扩展：

JSOFTWARES

<https://thunkableblocks.blogspot.com/2017/07/jsontools-extension.html>

QRNG Mini系统的开源和商业版本的授权请见官方网站<http://www.openqbit.com>。

Mini QRNG, Mini BlocklyChain, MiniBlockly, BlocklyCode, MiniBlockMiniChain, QBlockly是OpenQbit注册的商标。

迷你QRNG是公共领域。

Mini QRNG中的所有代码和文档都被作者献给了公共领域。所有的代码作者和他们所工作的公司代表都签署了宣誓书，将他们的贡献献给了公共领域，这些宣誓书的原件都存放在OpenQbit墨西哥总部的保险箱中。任何人都可以自由地发布、使用或分发原始的Mini QRNG (OpenQbit)扩展，无论是源代码还是编译后的二进制文件，用于任何目的，商业或非商业，以及以任何方式。

前一段适用于Mini QRNG中可交付的代码和文档，这些Mini QRNG库的部分实际上是与一个更大的应用程序一起分组和运送的。编译过程中使用的一些脚本（例如，由autoconf生成的"配置"脚本）可能包含在其他开放源码许可证中。然而，这些编译脚

本都没有进入最终的 QRNG Mini 可交付库中，因此在评估您复制和使用 QRNG Mini 库的权利时，与这些脚本相关的许可证不应成为一个因素。

Mini QRNG中的所有可交付代码都是从头开始编写的。没有从其他项目或公开的互联网上获取任何代码。每一行代码都可以追溯到它的原作者，所有这些作者都有公共领域的奉献档案。因此，QRNG Mini的代码库是干净的，没有被其他开源项目授权的代码所污染，而不是开放的贡献

Mini QRNG是开源的，这意味着你可以随意复制，并且可以不受限制地使用这些副本做你想做的事情。但Mini QRNG并没有开源。为了使Mini QRNG处于公共领域，并确保代码不受专有或授权内容的污染，该项目不接受不明人士的补丁。Mini QRNG中的所有代码都是原创的，因为它是专门为Mini QRNG使用而编写的。没有从互联网上抄袭不明来源的代码。

迷你QRNG属于公共领域，不需要许可证。然而，一些机构希望得到法律证明，以证明他们有权使用迷你QRNG。发生这种情况的情况包括：

- 你的公司希望对侵犯版权的索赔进行赔偿。
- 你在一个不承认公有领域的司法管辖区使用迷你QRNG。
- 您所使用的Mini QRNG所在的司法管辖区不承认作者将其作品献给公共领域的权利。
- 您希望有一份有形的法律文件，作为您拥有使用和发布Mini QRNG合法权利的证据。
- 你的法律部门告诉你，你必须买一个许可证。

如果上述任何一种情况适用于您，OpenQbit公司（雇用所有Mini QRNG开发人员的公司）将向您出售一份Mini QRNG产权保证书。产权保证书是一份法律文件，声明Mini QRNG的宣称作者是真正的作者，作者拥有将Mini QRNG献给公有领域的合法权利，OpenQbit将针对授权索赔进行有力的辩护。迷你QRNG产权保证书的销售收入全部用于资助迷你QRNG的持续改进和支持。

贡献代码

为了保证Mini QRNG完全免费和免版税，该项目不接受补丁。如果你想做一个建议性的修改，并加入一个补丁作为概念验证，那就太好了。不过，如果我们从头开始重写你的补丁，也不要生气。非商业或开源许可证的类型谁使用它在这种模式和一些类似的不购买的支持，无论是个人或企业使用，无论公司的规模将受以下法律前提。

保修免责声明。除非适用法律要求或书面同意，许可方以"原样"提供本作品(每个贡献者提供其贡献)，**没有任何形式的**明示或暗示的保证或条件，包括但不限于所有权、非侵权、适销性或特定用途的适用性的任何保证或条件。您应自行负责确定本作品的正确使用或再分配，并承担与您行使本许可下的权限有关的任何风险。

因使用本软件而造成的任何经济或其他损失，均由受影响方承担。所有的法律纠纷将提交给墨西哥国家墨西哥城的法院审理。

对于商业支持、使用和许可，必须在OpenQbit或其公司与相关方之间建立协议或合同。

分销营销条款可能会在不通知的情况下发生变化，请到官方网站www.openqbit.com，查看任何非商业和商业的支持和授权条款的变化。

任何个人，用户，任何法律性质的私人或公共实体，或来自世界任何地方的人，只要使用本软件，就无条件地接受本文件中的条款，以及那些可以在任何时候在www.openqbit.com 的门户网站上修改的条款，而无需事先通知，并可由OpenQbit决定应用于非商业或商业用途。

任何关于Mini QRNG的问题和信息都应该被引导到App Inventor社区或各个Blockly系统社区，因为它们是。AppBuilder、Trunkable等和/或发到邮箱opensource@openqbit.com，对于需求的问题可能需要3到5个工作日才能得到答复。

支持与商业用途。

support@openqbit.com

商业用途的销售。

sales@openqbit.com

法律信息和许可问题或关切

legal@openqbit.com

