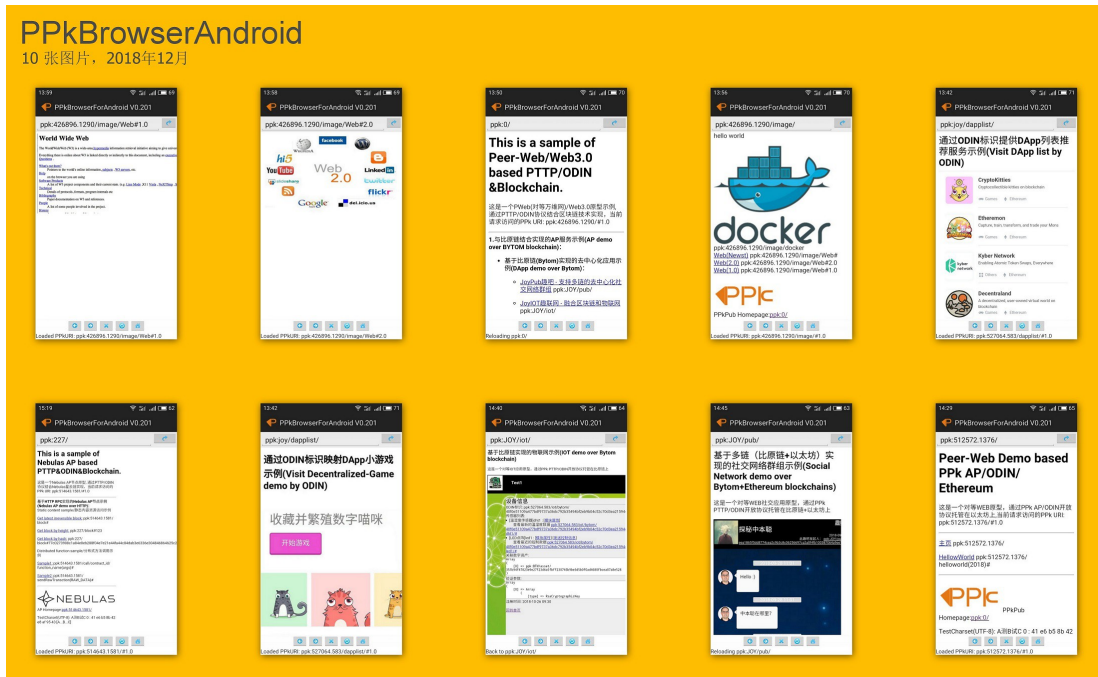


PPk 浏览器快速指南

2019-06-21 PkPub.org

通过 PPK 浏览器可以很方便地浏览支持 PTTT 协议的内容服务，同时其内置了一个简单的比特币钱包功能，可以快速上手注册管理奥丁号（ODIN），以及体验接收和发送比特币。



奥丁号（ODIN）是 Open Data Index Name（开放数据索引命名）的缩写，是基于区块链的自主、唯一、安全、持久的命名标识协议，是“对等、可信的新型 DNS”。

PTTP 是 Peer Trusted Transfer Protocol（对等可信传输协议）的缩写。每一个奥丁号 URI 会被解析映射到一个或若干个 AP（Access Point，即数据访问点）上，由 AP 节点按照 PTTT 协议负责中转或提供具体信息服务。AP 可以理解为对等、可信的 PPK 网络里的“中继器”(Relay)和"WEB 服务器"(Web Server)。PTTP 协议就是 AP 向外提供数据内容的访问接口标准协议，是融合奥丁号、区块链和 ICN/NDN 未来网络体系架构设计等多个领域新兴技术而定义的一种对等可信的信息交换协议，是“融合区块链技术的新型 HTTP 协议”。

关于奥丁号（ODIN）和 PTTT 协议的详细定义请访问 <http://ppkpub.org> 获取。

一、在安卓手机上安装 PPk 浏览器

安卓手机用户可以下载安装最新版本的 PPk 浏览器安卓 APP。

下载地址：

<https://github.com/ppkpub/PPkBrowserAndroid/raw/master/bin/PPkBrowser.zip>

将上述地址复制到安卓手机浏览器里访问，下载后解压，点击其中的“ppkbrowser.apk”，即可开始安装，安装完成后打开运行。

注：

(1) 如果安装时提示“确认安装尚未验证的应用”，点击确认即可。

(2) 目前 APP 只支持 Android 安卓系统，苹果手机 iOS 因为相关应用商店政策限制不支持。

(3) 电脑和苹果手机上可以通过浏览器访问网页版工具，来注册奥丁号，具体说明请参考：
https://ppkpub.github.io/docs/DOC_PPk_BrainTool_Tutorial.pdf

PPk 浏览器的主界面显示效果如下图所示：



窗口底部的多个操作功能按钮说明如下：



二、如何浏览 PPK 网络上的内容资源？

在传统万维网（WWW）网络里，我们使用 IE、Chrome 等网页浏览器，通过超文本传输协议（HTTP）访问全球不同的 Web 网站。而使用 PPK 浏览器，就可以通过对等、可信的 PTTP 协议来访问 PPK 网络上的内容节点。

在 PPK 浏览器的地址栏里，可以很方便地访问直接输入“ppk:”起始的新型区块链域名来测试支持 PTTP 协议的新型内容网站服务，如下图所示：



在浏览器上方有一个网址输入框，输入的是以“ppk:”起始的奥丁号对应网址。当输入网址，点击 按钮后，PPk 浏览器将执行以下流程来处理：

第 1 步：因为图中示例输入的“ppk:0/”是一个短地址，与从 0 开始累加的注册奥丁号的顺序号对应，首先会在客户端本地被相应转换成标准地址“ppk:426896.1290/”。如果在这里的网址输入框直接输入标准格式的奥丁号如“ppk:426896.1290/”，则直接进入第 2 步。

第 2 步：按照标准格式的奥丁号，客户端根据该标识对应存放在比特币区块链上的访问点 AP 参数，进一步解析指向实际的 AP 节点 URL（类似传统 DNS 域名解析到 IP 地址的过程）。

第 3 步：由客户端按 AP URL 中对应的实际承载协议类型（如图中示例的 HTTP 协议）来组织发送符合 PTTP 协议的兴趣包（Interest）给 AP 节点，并获得其所应答的内容数据包（Data）。

第 4 步：客户端按该奥丁号存放在比特币区块链上的可信验证参数自主对内容数据包进行可信验证，验证通过后将内容正文显示到浏览器窗口。

上图中示例显示的内容正文是一个简单的 HTML 网页内容，用户可以点击其中的链接来跳转访问到其他内容资源。

PPk 网络里的 AP 所提供的内容资源可以是纯文字的，也可以是图文混合的，如下图所示是一个

带有图片的简单页面：



可以是静态资源，也可以是动态方法，如下图所示是一个访问动态方法的简单示例，将传入参数 1，2，3 相加后得到应答结果 6：

可以托管运行在传统的 Web 服务器上，也可以灵活承载在以太坊 ETH，比原链 BTM，超级账本 Fabric 等等支持运行智能合约或链上代码的这些不同类型的区块链平台上，如下图所示是一个访问以太坊上的智能合约获得应答内容的简单示例：

在这些示例的基础上，可以在浏览器端实现类似 AJAX 等更复杂的网页交互功能，配合多种区块链平台的浏览器钱包插件类似 Metamask，可以更好地开发采用 PPK 奥丁号和 PTPP 协议的应用服务。更为有用的是，通过奥丁号配合 PTPP 协议可以帮助应用不需要再绑定于具体区块链平台，也不再受制于传统 DNS 域名和 IP 网络通信机制的局限，提供内容服务的 AP 可以是传统机房里拥有全网静态 IP 地址的服务器，也可以是物联网场景下灵活组网的终端设备，任意设备间都可以自由达成对等、可信的信息交换。

三、注册奥丁号

打开 PPK 浏览器后，点击“设置”按钮，就可以查看你的比特币钱包地址和余额等信息，如下图所示。



比特币，一种数字加密货币，缘起一个神秘大神的程序，超高算力支持的工作量证明（PoW）算法，保证了比特币网络中每一个参与节点上区块链数据的一致性和难以篡改，可以支持全球点对点无需中介的交易支付。

上图中“比特币地址”下方的类似“1HiNok...”这样的一串字符就是你的比特币钱包地址，复制后发送给别人，就能接收别人给你发送的比特币了。

在这里点击“导入新地址”按钮，可以导入自己已有 BTC 地址的私钥使用，效果是一样的。客户端支持导入多个地址进行注册和管理，点击“切换其它地址”后从具体地址列表选择即可。

注意：第一次运行时，请复制备份好自动新建钱包地址时提示备份的私钥，一旦丢失，将无法恢复。

因为奥丁号是基于比特币协议来运行的，所以你需要先拥有一些比特币才能注册自己的奥丁号，刚开始一般有 0.001BTC 就足够体验了。

获得比特币有两种方式，程序“挖矿”或在线买卖。现在“挖矿”已经是专用挖矿设备和专业矿工的天下，普通人很难通过电脑挖矿来获得比特币，目前可以通过像 coincola.com, localbitcoins.com 这样的交易网站来小额买入（这些网站上都有比较详细的中文操作说明），也可以直接从手里持有比特币的朋友那里获赠或购买。

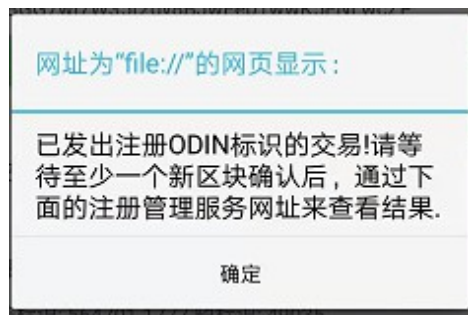
有了一定数量的比特币（余额显示有 0.00003BTC 以上）后，就可以开始注册奥丁号了。点击设置界面里的“快速注册一个奥丁号”按钮，弹出对话框如下图所示：



按提示输入一段文字（作为备忘信息，也可以不填），点击“确定”按钮后，将看到如下图这样的提示：



确认上述注册交易信息无误后，点击“确定”按钮即可发送该交易，稍后会收到发送成功的提示信息，如下图所示：



除了通过上述“设置”界面快速注册奥丁号外，还可以打开注册管理服务来操作更复杂的注册和管理功能，具体操作方法说明如下：

点击“设置”界面里的“注册管理扩展服务网址”区域的“打开”按钮，如下图所示：

当前地址相关奥丁号信息

已注册数: 2

最近注册: 完整标识: 573572.2340 短标识: 74378

待确认交易数: 0

(注: 待确认交易数包括ODIN注册、普通转账等多类交易在内, 仅供参考)

快速新注册一个奥丁号

注册管理奥丁号服务网址

http://tool.ppkpub.org:9876/odin

打开

浏览器将显示对应的注册管理服务页面, 如下图所示:



标准奥丁号	序号	时间	附注
573572.2340	74378	2019-04-28 14:38:00	JEF
573572.2164	74377	2019-04-28 14:38:00	torr

点击其中的“注册新奥丁号”按钮, 就可以进入注册新奥丁号的操作界面了, 如下图所示:



首先，可以直接点击“与注册者相同”按钮将自己的比特币地址指定作为标识的管理者。如果为了方便管理或更高的安全性，作为注册者你也可以输入一个自己其它的比特币地址作为管理者。

然后，输入一段文字作为所注册奥丁号的备忘名称；再根据需要可以选择输入自己的电子邮件地址，不输入也可以；再从“配置权限”下拉列表选择一种对标识配置信息做修改的权限验证方案，一般选择缺省的“注册者或管理者任一方都可以修改配置”即可，如需要调整可以按照奥丁号协议的定义来具体选择。

最后，点击“提交注册”按钮，再次确认所提示注册交易信息无误后，点击“确定”按钮即可发送该交易，客户端会将你填写的信息按奥丁号协议规范组织打包成比特币交易并广播到比特币网络，如下图所示。



现在可以先关闭 PPK 客户端，然后到网页浏览器里访问 <http://btc.com>，在其网页右上角的查询框里输入你的比特币钱包地址，比如上述示例中的 1HiNok9GdcTjabsqsd3A66sb1MyXiGTygQ，就可以查询你所发出的奥丁号注册交易的被确认情况，显示如下：



当类似上图中红圈处的显示文字从“未确认”变成确认数值大于等于 1 时，就说明刚才你所发出的奥丁号注册交易已被比特币区块链所确认收录，现在就可以重新打开 PPK 浏览器查看注册结果了，点击“设置”按钮，就可以查看最新注册到的奥丁号信息，如下图所示：



上图中红圈处显示的“573572.2340”就是新注册得到的 ODIN 完整标识，其中 573572 是对应交易被收录的区块号，2340 是交易在该区块内部所收录全部交易列表中的索引号，这两个数字就组成了唯一存在的奥丁号完整标识。而按照奥丁号在 BTC 区块链上注册的顺序，从 0 开始，依此加 1，得到对应的短标识，如上图中的 74378。

如果注册了多个奥丁号，可以点击上图中“注册管理扩展服务网址”区域的“打开”按钮，就可以查看到自己注册的奥丁号列表了。

注意：

1. 因为奥丁号体系是基于比特币的区块链来运行的，所以在你进行注册和修改配置操作时，点击提交后看到绿色文字提示（例如“你的操作请求已被提交到比特币网络，请等待至少 1 个比特币新区块的确认结果（约 10 分钟）”）后请耐心等待比特币网络的新出块确认。

2. 需要确保你的钱包里有少量但足够的比特币以支持发送注册和修改请求（所支付的交易费用将被支付给比特币矿工）。

相比传统的 DNS 域名注册机制，基于比特币系统的奥丁号的注册和管理效率不够快，操作方法也有所差异，但作为一种全新的技术应用，奥丁号的自主、唯一、可信、持久等特性却是超越传统 DNS 域名机制的，很好地适配了区块链技术的价值精髓，值得各位真正关注区块链技术发展的朋友来体

验和使用，提出优化改进意见。我们后续也会继续补充完善技术实现来提升使用体验。

四、如何管理自己的奥丁号？

点击 PPK 浏览器底部的“设置”按钮，再点击“注册管理扩展服务网址”区域的“打开”按钮，就可以查看到自己注册的奥丁号列表了，然后点选“我管理的奥丁号”，就可以查看到自己有权限管理的奥丁号列表。

点击所要查看的奥丁号对应显示文字如“513468.490”，就可以查看该标识的详细情况，如下图所示：

查看详细属性 ODIN[40687]:559997.2523

更新...

- 管理者比特币地址：
1HVSDUmW3abkitZUoZsYMKZ2PbiKhr8Rdo
- 附注名称：1502
- 电子邮件：
- 配置权限：注册者或管理者任一方都可以修改配置
- 注册者比特币地址：
1HVSDUmW3abkitZUoZsYMKZ2PbiKhr8Rdo
- 时间：2019-01-25 11:07:35 区块:559997
- 数据访问点
创建你的第一个对等网页AP示例 (托管在像
区块链等分布式平台上) ...
- 内容可信设置：
- 转义英文名称列表 (可以代替数字标识使用, 如 ppkabc/
) :

[GOMTP, GOMTQ, GOMTR, GOMUP,
GOMUQ, GOMUR, GOMVP, GOMVQ,

如果需要修改上述配置信息，可以点击“更新”按钮，显示如下图所示：

修改配置信息 ODIN[40687]:559997.2523

设置访问点...

内容可信设置...

转移注册者...

管理者比特币地址

1HVSDUmW3abkitZUoZsYMKZ2PbiKhr8Rdo

附注名称

1502

电子邮件(可选)

管理者的公开邮箱

配置权限

注册者或管理者任一方都可以修改配置

提交更新

在这里可以修改奥丁号的一些基本信息，包括管理者地址、标识名称、联系邮箱和权限验证策略。修改完成后点击“更新基本信息”按钮就可以发出更新标识的交易了，同样需等待比特币网络确认后就会生效。

五、使用奥丁号作为自己的自主身份（体现去中心化身份标识新体验）

在注册获得自己的奥丁号后，就可以选用一个奥丁号，设为自己的自主身份，在访问应用服务时自主验证登录，不需要再记用户名密码，在不同应用服务都能用同一个自主身份轻松登录；更新验证权限时也只需要自主在比特币区块链上修改一次，不需要到不同应用服务处多次修改。

因为奥丁号是支持多级扩展的，类似传统域名的多级域名机制，分为根奥丁号和扩展奥丁号。根奥丁号是注册在 BTC 链上的，如“ppk:123”；扩展奥丁号则是由根奥丁号拥有者自行扩展、灵活定义的，比如某个应用的根奥丁号是“ppk:joy”，通过该应用来注册的下属用户标识，就是扩展奥丁号，类似“ppk:joy/btmid/YourName#”或者兼容 DID 的“did:ppk:joy/btmid/YourName#”。两类奥丁号的注册方式和标识存储位置上有差别，但都可以用作用户自主身份，使用效果是一样的。可以参考奥丁号和 PPK 开放协议的资料进一步了解（<https://ppkpub.github.io/docs/>）。

一般按照以下 3 步就能快速开启将奥丁号作为自主身份的新体验：

- (1) 选择一个自己注册的奥丁号，设为自己的自主身份标识；
- (2) 给该奥丁号关联一对公私钥，其中私钥安全存放于用户手机，而将公钥发布到网络上；
- (3) 访问支持奥丁号的应用服务，自主验证登录成功后，即可正常使用。

具体操作过程说明详见下文。

5.1 使用根奥丁号作为自主身份

打开 PPK 浏览器，点击“设置”界面里的“开放自主的用户身份”区域的“从我注册的奥丁号中选取”按钮，如下图所示：



开放自主的用户身份

当前使用的身份标识

查看开放信息 从我注册的奥丁号中选取

已发布到网络上的公钥（供第三方验证身份签名时使用）

测试密钥签名

从“我注册的奥丁号”列表里点击选择一个自己的奥丁号，进入查看其属性，如下图所示：

查看详细属性 奥丁号
[74689]:573724.2470

将该奥丁号设为我的自主身份

更新...

• 管理者比特币地址：
1HiNok9GdcTjabsqsd3A66sb1MyXiGTygQ

• 附注名称：

• 电子邮件：

• 配置权限：

• 注册者比特币地址：
1HiNok9GdcTjabsqsd3A66sb1MyXiGTygQ

• 时间: 2019-04-29 13:33:32 区块:573724

点击“将该奥丁号设为我的自主身份”按钮后，将弹出提示窗口，如下图所示：

查看详细属性 奥丁号
[74689]:573724.2470

请确定切换使用新的奥丁号

请确定使用下面的奥丁号作为用户身份
ppk:74689#

取消

确定

1HiNok9GdcTjabsqsd3A66sb1MyXiGTygQ

• 时间: 2019-04-29 13:33:32 区块:573724

点击“确定”按钮，确认将对应显示的奥丁号设为你的自主身份即可。

然后点击“设置”按钮，返回设置界面，查看里面的“开放自主的用户身份”区域，将显示你“当前使用的身份标识”已经变为刚设定的奥丁号，如下图所示：

开放自主的用户身份

当前使用的身份标识

ppk:74689#

查看开放信息

从我注册的奥丁号中选取

已发布到网络上的公钥（供第三方验证身份签名时使用）

测试密钥签名

本机保存的身份密钥

查看/配置密钥

更新公钥到网络上

下一步，为了能够自主验证身份，需要生成一对密钥（公钥和私钥），私钥受保护地存放在浏览器内部，用于生成验证所需签名信息；公钥作为奥丁号的关联配置信息被发布到网络上。这样应用服务就可以通过奥丁号关联获取开放的公钥，用来验证你的私钥签名，确认你是对应相应身份标识的合法访问者。

点击上图底部的“查看/配置密钥”按钮，系统将自动为你生成所需密钥，如下图所示：



默认采用 RSA 算法生成密钥（1024 位长度），可以点击上图里的“复制”按钮自行备份。用户也可以使用第三方 RSA 密钥生成工具，来生成更长更安全的密钥（比如 2048 位），然后“粘贴”到上图对应界面来使用。

注：粘贴导入的 RSA 密钥需要符合下述 JSON 格式的字符串定义：
`{"RSAPublicKey": "Base64 编码的公钥字符串", "RSAPrivateKey": "Base64 编码的私钥字符串"}`

确认密钥生成无误后，点击“确定”按钮保存，这是系统将提示“需要将新设置的公钥发布到网络上”，如下图所示：



点击“确定”按钮，系统将调用奥丁号注册管理工具来发布公钥，如下图所示：

验证算法

SHA256withRSA

公钥

CZcTqRDbE4m3LdKv7VMzsKhEYDvZzgk5Aw7lc1
X0jFOMbB0pjcrsrwWUAP4bbf9qyQTWKhRbXXSkTnt
80eeuf6HeZIDee+IMQBE8eV7DXT6e/UOnzO
iSR8n0EXfnTkaWuUjA6Y0srriX8fE/MIT+3+1+AYE70

私钥

本机私钥受保护

请注意备份好私钥！

选择公钥的存储方式

IPFS(星际文件系统)

提交更新

用户可以在这里选择公钥在网络上的存储方式，默认采用 IPFS 分布式存储服务，也可以选择其它分布式存储服务，然后点击“提交更新”按钮，系统会将对应公钥，上传到所选择的分布式存储服务上，获得一个类似"ipfs:xxxxx"或"btmfs:xxxxx"等这样的存储位置网址，并被自动关联更新到对应奥丁号在 BTC 区块链的配置信息里。等到这条配置更新交易被 BTC 网络确认，就可以通过 PPK 浏览器的“设置”界面查看，如下图所示：

开放自主的用户身份

当前使用的身份标识

ppk:74689#

查看开放信息

从我注册的奥丁号中选取

已发布到网络上的公钥（供第三方验证身份签名时使用）

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQ
D0dKG+neErEBzX1YJgiaV4EU9cETEB4xWBvgeQ
Ok+cglwao0RqZUIa9l4ue7lC+ubfDc9srs+Th1Mkm9o

测试密钥签名

本机保存的身份密钥

本机密钥有效，对应公钥已发布到网络上；对应的私
钥只在本机安全保存，可在验证身份时自主签名。

查看/配置密钥

更新公钥到网络上

密钥配置更新确认完成后，可以点击“测试密钥签名”按钮，弹出对话框，如下图所示：



点击“确定”按钮提交签名，通过验证后看到如下图所示，就说明上述奥丁号的自主验证设置已经成功了。



完成奥丁号的自主验证设置后，现在就可以登录具体的应用服务了。这里以 PPK 奥丁号自主拍卖交易工具为例，来说明如何使用奥丁号来自主验证身份并登陆应用服务。

在 PPK 浏览器里地址栏里输入 `ppk:joy/swap/` 或者 <http://tool.ppkpub.org/swap/>，即可访问 PPK 奥丁号自主拍卖交易工具示例，主页显示如下图所示：



点击网页右上角的弹出菜单按钮，如下图所示：



然后点击“以奥丁号登录”功能，进入登录页面，显示如下图所示：



登录界面将自动列出你在 PPK 浏览器里已设定的自主身份标识，如上图示例里的“ppk:74689#”。

现在点击“使用支持奥丁号的 APP 自主验证身份”绿色按钮，将弹出确认签名的对话框，如下图所示：



点击“确定”按钮提交签名，通过验证后看到如下图所示，就说明指定奥丁号的登录已经成功了。



点击“确定”按钮关闭该提示对话框，应用网页将自动切换到对应用户登录成功后的主页，并可以点击网页右上角的弹出菜单按钮，查看到用户的已登录状态信息，如下图所示：



说明在这里示例应用里，你已经用自主注册的根奥丁号（如 ppk:74689#）作为用户身份，通过自主验证登录成功了。

5.2 使用扩展奥丁号作为用户身份

这里以 PPK-JoyAsset 比原数字资产自主拍卖交易工具原型为例，来说明如何通过比原链注册获得扩展奥丁号，然后配合 PPK 浏览器来自主验证身份并登陆应用服务。

扩展奥丁号是由根奥丁号拥有者自行扩展、灵活定义的，比如 PPK-JoyAsset 应用的根奥丁号是“ppk:joy”，通过该应用来注册的下属用户标识，就是扩展奥丁号，其定义类似“ppk:joy/btmid/YourName#”，对应兼容 DID（去中心化身份标识）规范的定义为“did:ppk:joy/btmid/YourName#”。

在 PPK 浏览器里地址栏里输入 `ppk:joy/asset/` 或者 <http://btmdemo.ppkpub.org/asset/>，即可访问 PPK-JoyAsset 数字资产自主拍卖交易工具原型示例，主页显示如下图所示：



点击网页右上角的弹出菜单按钮，如下图所示：



然后点击“注册新用户”功能，进入注册页面，显示如下图所示：

在比原链上注册兼容DID的扩展奥丁号

用户名

YourName

(注：建议用英文字母和数字作为用户名。通过本应用在比原链上注册，得到的是兼容DID的扩展奥丁号，类似"did:ppk:joy/tbmid/YourName#"，注意有别于注册在BTC链上的扩展奥丁号如"ppk:123/"，两者的注册方式和标识存储位置上有差别，但使用效果是一样的，扩展奥丁号和根奥丁号都可以登录本应用，可以参考奥丁号和PPK开放协议的资料进一步了解。)

电子邮箱（可选）

头像URL

http://ppkpub.org/images/user.png

头像预览

比原钱包地址

验证公钥

MIGfMA0GCsGqSslb3DQEBAQUAA4GNADCBiQKgBQCFQC2D9HbsnmYBO7JfMP8skypDsHsZmbvHrJEOvcb4+3BYfY8PNv9vXDIUXmbUNsJ5xaDyX0V15RIG

公钥将与用户注册信息一起保存并被公开访问。

签名密钥（JSON）

{"RSAPublicKey":"\r\nOvcb4+3BYfY8PNv9vXT/BgCMcpy7JEO8JnfZf+Yr\n4Y7kpGHgkwQ51ewDAQAB\r\n","RSAPrivateKey":"MIICdgIBADANBgkqhkiG9w0BAQEF"}
此密钥仅供测试用，请自行复制保存，用于后续测试体验过程。

注意将这里生成的签名密钥字符串（包含公钥和私钥）复制备份，后续需要设置到PPK浏览器里保存。

在比原链上注册新用户标识

参考上图里的红色说明，填写必要的新用户信息，复制备份好签名密钥字符串后，点击“在比原链上注册新用户标识”绿色按钮提交，应用服务将在比原链上注册对应的新用户，成功后将自动以该新用户身份登录使用，回到主页可以查看，如下图所示：



点击上图中的用户帐户链接，可以查看该用户的详细属性，如下图所示：

 **Yao88**

身份标识： did:ppk:joy/btmid/Yao88#

使用该奥丁号作为自主身份

对应PPk协议URI:
ppk:527064.583/btmid/Yao88/#

电子邮件： yao88@test.com

创建时间： -----

拥有者钱包地址：
bytom:tm1qhcewj8xff9y9nyvntu4h6plmdqg9d0w6c

发布拍卖总次数： 0 （好评率 ..%） ,

参与报价总次数： 0 （好评率 ..%） ,

退出登录状态

在上图点击“使用该奥丁号作为自主身份”绿色按钮，将弹出提示信息如下图所示，点击“确定”按钮确认将对应显示的奥丁号设为你的自主身份即可：



在应用服务处注册用户获得扩展奥丁号，并设为自己的自主身份后，可以点击 **PPk** 浏览器底部的“设置”按钮，返回设置界面，查看里面的“开放自主的用户身份”区域，将显示你“当前使用的身份标识”已经变为刚设定的奥丁号，如下图所示：

开放自主的用户身份

当前使用的身份标识

did:ppk:joy/btmid/Yao88#

查看开放信息 从我注册的奥丁号中选取

已发布到网络上的公钥（供第三方验证身份签名时使用）

MIGfMA0GCSqGSib3DQEBAQUAA4GNADCBiQKBgQCFQC2D9HbsnmYBO7JfMP8skypDsHoZmbvHrjJE
Ovcb4+3BYfY8PNv9vXDiuXmbUNsJ5xaDyX0V15RiG

测试密钥签名

本机保存的身份密钥

查看/配置密钥 更新公钥到网络上

注意上图里显示的公钥，是在注册新用户时由应用服务已经发布到网络上了，现在我们需要将注册新用户时所复制备份的对应私钥，保存到 PPK 浏览器里，以后就可以自主验证登录了。点击上图里的“查看/配置密钥”按钮，显示如下图所示：

查看/设置标识验证密钥

标识：did:ppk:joy/btmid/Yao88#

算法：RSA

公钥：
MIGfMA0GCSqGSib3DQEBAQUAA4GNADCBiQKBgQCFQC2D9HbsnmYBO7JfMP8skypDsHoZmbvHrjJE

私钥：
MIICdglBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBAIVALYP0duyeZgE7sl8w/yyTKkOwehmZu8euMkQ69xvj7cFh9jw8

复制 粘贴

取消 确定

点击“粘贴”按钮，将注册新用户时所复制备份的对应私钥导入上图对话框，替换掉默认自动生成的密钥，确认无误后，点击“确定”按钮保存即可。回到设置界面，可以看到“本地保存的身份密钥”一栏已经有相应提示，如下图所示，就说明已经将密钥保存到浏览器里了：

当前使用的身份标识

did:ppk:joy/btmid/Yao88#

查看开放信息 从我注册的奥丁号中选取

已发布到网络上的公钥（供第三方验证身份签名时使用）

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCFQC2D9HbsnmYBO7JfMP8skypDsHoZmbvHrjJE
Ovcb4+3BYfY8PNv9vXDiUXmbUNsJ5xaDyX0V15RiG
_ks+E2BdknazlIXaT/RoCMcnvZ.IE08.Inf7f+

测试密钥签名

本机保存的身份密钥

本机密钥有效，对应公钥已发布到网络上；对应的私钥只在本机安全保存，可在验证身份时自主签名。

查看/配置密钥 更新公钥到网络上

密钥配置完成后，可以点击“测试密钥签名”按钮，弹出对话框，如下图所示：

按资源标识生成签名

资源地址：
did:ppk:joy/btmid/Yao88#

签名算法：SHA256withRSA
原文内容：
about:setting,did:ppk:joy/btmid/Yao88#

生成的签名：

OKiB+9DQt+NvM5Qotf0AqC6
X4khYqx2IGcDxgPMtSXpQtWz
hYRGcoj4sZAJwdHnYmPKcmo
uswl4m
PWAJDhs1Aj56LQEQdFpfKSS

复制 粘贴

取消 确定

点击“确定”按钮提交签名，通过验证后看到如下图所示，就说明上述新注册的扩展奥丁号的自主验证设置已经成功了。

网址为“file:///”的网页显示：

签名验证通过

确定

完成扩展奥丁号的自主验证设置后，现在就可以登录具体的应用服务了，具体操作过程与使用根奥丁号的操作方法是一样的，可以参考前文“使用根奥丁号作为自主身份”一节里，自主验证身份并登陆应用服务示例的详细说明。


5.3 扫码快捷登录

这里以 PPk 奥丁号自主拍卖交易工具原型为例，来说明使用 PPk 浏览器来扫码快捷登陆应用服务。

首先请确认已按前文的说明，安装好 PPk 浏览器安卓版最新版的应用（0.3.4 版以上），并设定了一个根奥丁号或扩展奥丁号作为自主身份标识。

在电脑浏览器里打开支持扫码登录的应用服务，比如 PPk 奥丁号自主拍卖交易工具示例（<http://tool.ppkpub.org/swap/login.php>），显示如下图所示



点击“使用支持奥丁号的 APP 扫码登录”按钮，就会出现相应的二维码，然后在安卓手机上打开 PPk 浏览器应用，并点击右上角的扫码图标 ，就会出现相应的“扫一扫”操作界面，如下图所示：



将手机的摄像头对准电脑浏览器上显示的登录二维码，清晰扫码并识别成功后，手机上将显示对应的登录确认界面，如下图所示：

PPK 数字资产拍卖

☰

确认扫码登录

用户奥丁号

ppk:74689#

确认登录

对应的用户信息设置

用户昵称

ppk:74689#

头像URL

http://ppkpub.org/images/user.png

确认要登录使用的奥丁号显示无误后，点击“确认登录”按钮，将弹出签名验证对话框，如下图所示：

按资源标识生成签名

资源地址：
ppk:74689#

签名算法：SHA256withRSA

原文内容：
http://tool.ppkpub.org/swap/,ppk:74689#,5d9c7eca-ceb5-4783-9ff1-0688fb57f8a9

生成的签名：
HDJGAMfjHjmmiWSxtlZu3Ja
mK7Ba/
OxxUI8zpnOwJ+ixImU452+hX
J/Sq6Yz9fXpG30Pa/X5cL9H
UdMrS3i4iupEI0IZsdgGi4cjvYD

复制
粘贴

取消 确定

点击“确定”按钮提交签名，通过验证后看到如下图的提示，就说明指定奥丁号的扫码验证已经通过了。

扫码验证通过，请回到所登录设备上继续访问。
Verified ok as ppk:74689#

然后回到电脑浏览器上，应用服务网页会自动切换到登录成功后的页面，就可以正常操作了。

六、使用奥丁号快速发布自己的第一个对等网页（体现对等 WEB 新概念）

在注册自己的奥丁号后，下一步就可以搭建一个支持 PTTT 协议的对等内容服务节点即 AP，将新注册的奥丁号设置映射到这个 AP，就可以被 PPK 客户端浏览访问了。

PPk 浏览器的配置管理工具支持通过 Dat、IPFS、BtmFS 等多种分布式存储服务来快速建立一个简单的 AP 网站示例，并很方便地关联到自己所注册的奥丁号。

打开 PPK 浏览器，点击“设置”界面里的“注册管理扩展服务网址”区域的“打开”按钮，从“我管理的奥丁号”选择一个自己的奥丁号，点击“更新”按钮，再点击下方的“创建你的第一个对等网页 AP 示例.（托管在区块链等分布式平台上）..”链接，如下图所示：

- 创建你的第一个对等网页AP示例(托管在像区块链等分布式平台上)...

创建对等网页AP示例（托管在像区块链等分布式平台上）

转移注册者...

欢迎来到属于 ppk40762 的对等网站示例页面。

该页面去中心化托管在Dat、IPFS、BtmFS等不同特色的分布式存储服务上。

简单的开始，体验PPK新业态（PWEB/DWEB/WEB3.0）的第一步...

This is the first PeerWeb page of ppk40762

The page is stored on BtmFS which is a distributed file system based byatom blockchain.

Dat分布式数据同步协议
IPFS(星际文件系统)
BTMFS(基于比原区块链构建的分布式文件系统)

SHA256withRSA

MIICDgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBAIYMQBfrLuerIdBGFU9jLEeGhSz
csGiDbt1uln0D/qjtJyMEklhgRzLQIA78A8ddgCXf11BJAM6eJUR5azhjUjdSNinCjZluqa21QAx
T2r+N9ulDS8HLpXXBXRbRfKfUWQVkpXaj1mXe31XemEM4bzan9XkoBJRZw3DsLzKuxHAQMBAEEC

该私钥用于对所发布的页面内容进行签名，对应通过“内容可信设置”声明的公钥，访问者可验证内容合法性。

简单编辑下你所要展示的示例网页内容，选择托管内容的分布式存储服务类型（Dat、IPFS 或 BtmFS），点击“提交更新”就可以发布了。系统会将你所编辑的示例内容，上传到所选择的分布式存储服务上，并获得一个类似“dat:xxxxx”、“ipfs:xxxxx”或“btmfs:xxxxx”等这样的网址，被自动关联更新到对应奥丁号在 BTC 区块链的配置信息里，等到这条配置更新交易被 BTC 网络确认，就可以通过 PPK 浏览器访问了，比如你使用的奥丁号是 40762，在 PPK 浏览器里输入 ppk:40762 就可以看到效果了，这就是你的第一个“去中心化”托管在分布式存储服务上的对等网页示例，而不是承载在单一的传统 WEB 服务器上了。

更进一步，对于有一定 WEB 开发能力的朋友，可以参考 PPk 的示例源码来开发更为复杂的 AP 服务，具体可以参看下述说明文档里的第六节“如何搭建一个支持 PTTP 协议的内容节点 AP 接入 PPk 网络？”详细了解：

https://ppkpub.github.io/docs/DOC_PPk_JavaTool_Tutorial.pdf

类似传统 DNS 域名的安全升级方案 DNSSEC，奥丁号原生支持内容可信配置功能，数据请求者可以对从 AP 获得的数据内容自主进行可信验证。具体请参考上述参考文档里的第七节“如何让自己的 AP 节点发布的内容自证可信？”详细了解。