注册管理 ODIN 标识和搭建 PTTP 测试节点指南

2018-11-29　PPkPub.org

通过 PPk 的 Java 版本电脑客户端可以很方便地注册管理 ODIN 标识，浏览支持 PTTP 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，可以用于体验接收和发送比特币。

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 ODIN 标识 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 PTTP 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 ODIN 标识、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 ODIN 标识和 PTTP 协议的详细定义请访问 http://ppkpub.org 获取。

这里以在常用的 Windows7 操作系统下安装和使用 PPk 的 Java 客户端为例，其他的电脑操作系统如 Ubuntu Desktop 等可以参考并自行安装。

一、Windows7 下安装

1. 下载最新版本的 PPk 客户端软件。

在电脑的网页浏览器里访问“ http://ppkpub.org ”并点击页面里“开放资源”一栏里的“百度网盘”进入下载页面，或者直接输入网址“ http://pan.baidu.com/s/1o7A8Gn4 ”进入下载页面，如下图所示：

在下载网页上点击进入 PPk 目录，然后点选文件名为“PPkTool-0.X.X.zip”的压缩文件后点击

“下载”按钮即可开始下载，如下图所示：

2. 解压刚下载的“PPkTool-0.X.X.zip”文件。

注意：

如果此前已经安装过 PPk 客户端的旧版本，只需要将解压后的新版本文件复制到旧版本安装目录下覆盖原有程序文件即可。

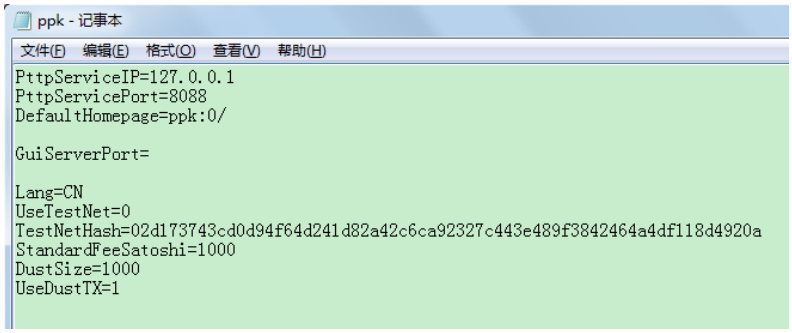
3. 到刚解压的目录下，双击运行“需先安装 Java(Windows).exe”，按照提示点击“安装”按钮启动在线安装 Java 运行环境支持软件，稍等片刻后即可安装完成。

注意：

如果确认你的电脑上此前已经安装过 Java1.8 以上版本，可以跳过这里的第 3 步，直接到第 4 步操作。

如果上述在线安装 Java 运行环境未成功，可以尝试从第 1 步的下载网页中直接下载对应操作系统版本的离线安装包（32 位操作系统：jre-8u11-windows-i586.exe 或 64 位操作系统：jre-8u11-windows-x64.exe）进行安装。

4. 用记事本或其它文本编辑器打开 resources 目录下的配置文件 ppk.conf，显示如下图所示：



上述客户端的运行配置参数中，缺省的交易成本费用为 StandardFeeSatoshi=1000，即 1000 聪或 0.00001 BTC,可以根据实际比特币网络中交易拥堵情况动态加大或减少这个费用值。可以访问 https://btc.com/ 查看网页下方的“当前最佳手续费”来相应设置，比如显示是“0.00003 BTC/kVB”, 这里的 0.00003BTC 换算成 3000 聪，则相应在配置文件里修改成 StandardFeeSatoshi=3000 就是比较合适当前比特币网络情况的交易费用，在此基础上适当将交易费用设高一点可以加快交易的被确认速度。

客户端缺省的界面显示语言为中文，如果需要切换为英文，可以将 Lang=CN 修改为 Lang=EN 即可。

客户端缺省是连接到 ODIN 标识的正式网络，对于开发人员如果需要切换到测试网络，可以修改 UseTestNet=0 改为 UseTestNet=1 。

5. 双击运行“ppk.bat”启动客户端。

6.客户端启动后会先进行数据下载，同步比特币的区块链数据，等数据同步完成后，进入主界面，显示如下图所示：

可以看到窗口顶部显示有以下功能菜单：

开放数据索引命名 ODIN: 可以查看比特币区块链上已注册的 ODIN 标识列表，注册新的 ODIN 标识，配置管理自己拥有的 ODIN 标识。

我的钱包: 钱包管理，可以查看 PPk 客户端内置比特币钱包的余额，进行转账操作，以及将其他比特币钱包地址的私钥导入使用。

开放社区: PPk 开源项目相关的网络社区资源，包括简介、网络文章、开放资料等。

点击“我的钱包”后，可以查看你的比特币钱包地址和余额等信息，如下图所示。

将上图中“我的钱包地址”下方的类似“1JMBNL4wEmfzBda...”这样的一串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。

在客户端“我的钱包”这里也可以导入自己已有 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，具体从右上角地址列表选择就行。

注：

1.请复制备份好 resources /db 目录下的钱包数据文件 wallet.dat。

2.如果要查看 wallet.dat 里面的私钥，可以编辑 resource 目录下的 ppk.conf 文件，加入一行

DEBUG_KEY=1

然后重新打开客户端，从右上角地址列表选择地址进入钱包查看，下方就会显示该地址对应的私钥（有多种格式，一般采用 WIF 格式，即以 5,K 或 L 起始的字符串）。

二、如何获得比特币？

比特币，一种数字加密货币，缘起一个大神的程序，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并难以篡改，可以支持全球点对点无需中介的交易支付。

因为 ODIN 标识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 ODIN 标识，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购买。

三、注册 ODIN 标识

当你的 PPk 客户端内置比特币钱包地址里有一定数量的比特币（余额显示有 0.001BTC 以上就足够了）后，就可以开始注册 ODIN 标识了，具体操作方法说明如下：

启动 PPk 客户端，等数据同步完成后显示主窗口，点击其中的“注册一个新 ODIN 号”按钮，如下图所示：

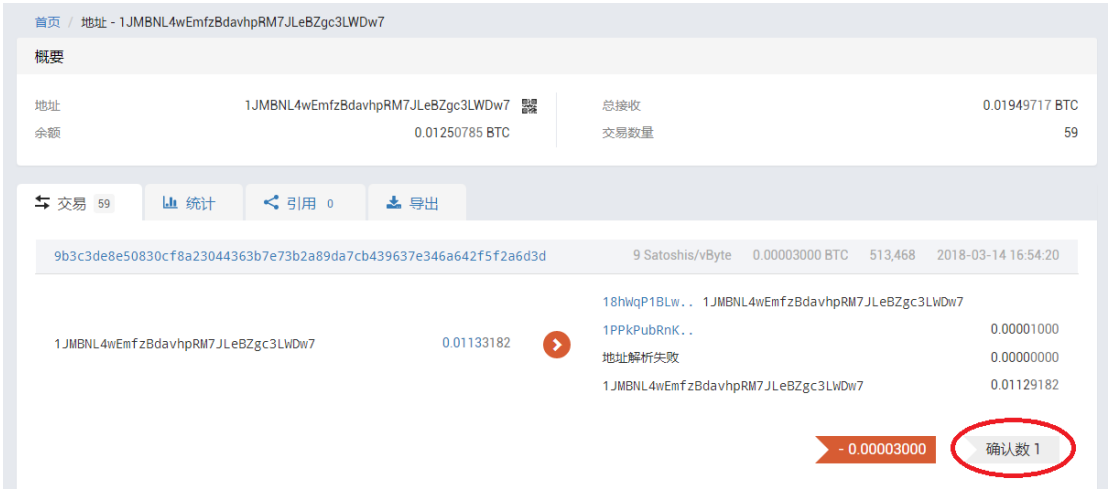
就可以进入注册新 ODIN 标识的操作界面了，如下图所示：

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 ODIN 标识的备忘名称；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 ODIN 标识协议的定义来具体选择。

最后，点击“提交注册”按钮，客户端会将你填写的信息按 ODIN 标识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 1JMBNL4wEmfzBdavhpRM7JLeBZgc3LWDw7，就可以查询你所发出的 ODIN 标识注册交易的被确认情况，显示如下：



当上图中红圈处的确认数值大于等于 1 时，就说明刚才你所发出的 ODIN 标识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 客户端程序查看注册结果了，点击主窗口上方的“开放数据索引命名 ODIN”，然后点选“我注册的 ODIN 号”就可以查看到自己注册的 ODIN 标识列表了，如下图所示：

上图中红圈处显示的“513468.490”就是新注册得到的 ODIN 标识，其中 513468 是对应交易被收录的区块号，490 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 ODIN 标识。

注意：

1.因为 ODIN 标识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，不要着急进行重复点击操作。

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 ODIN 标识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，ODIN 标识的自主、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 ODIN 标识？

点击 PPk 客户端主窗口上方的“开放数据索引命名 ODIN”，然后点选“我管理的 ODIN 号”，就可以查看到自己有权限管理的 ODIN 标识列表了，如下图所示：

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

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：

在这里可以修改 ODIN 标识的一些基本信息，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。

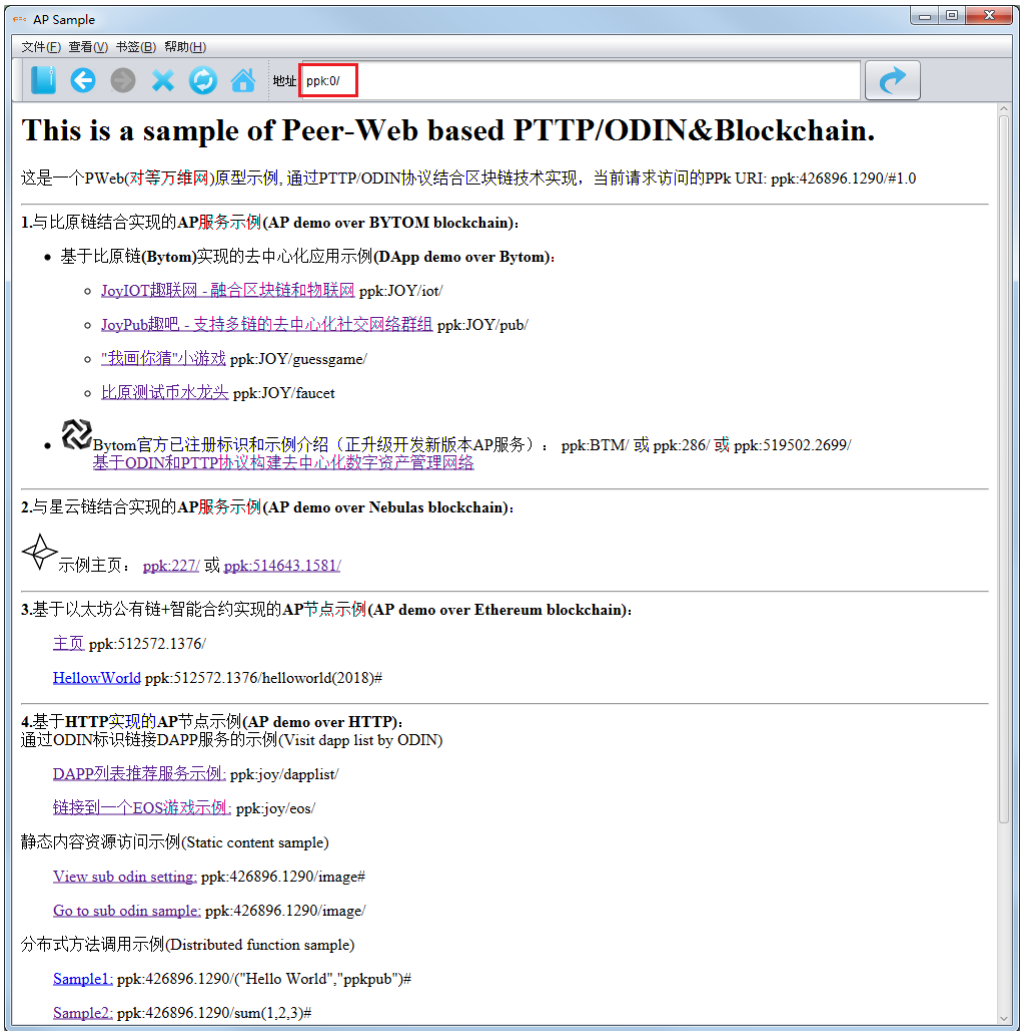
就像传统 DNS 域名需要设定所映射的 IP 地址一样，ODIN 标识也需要映射到支持 PTTP 协议的内容节点 AP（Access Point）来提供实际的内容服务。在上图中，点击“设置访问点”即可进入设置，具体将在后面第六节“如何搭建一个支持 PTTP 协议的内容节点 AP 接入 PPk 网络？”详细说明。

类似传统 DNS 域名的安全升级方案 DNSSEC，ODIN 标识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。在上图中，点击“内容可信设置”即可进入设置，具体将在后面第七节“如何让自己的 AP 节点发布的内容自证可信？”详细说明。

五、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。在 PPk 客户端支持相应的内容浏览代理服务，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 客户端安装目录下，双击运行“ppk_browser.bat”即可启动 PPk 浏览器进程 ，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 协议的本地 AP 内容服务，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 ODIN 标识对应网址。当输入网址，点击“Go”按钮后，PPk 内容代理服务进程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 ODIN 标识的顺序号对应，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 ODIN 标识如“ppk:426896.1290/”，则直接进入第 2 步。

第 2 步：按照标准格式的 ODIN 标识，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）。

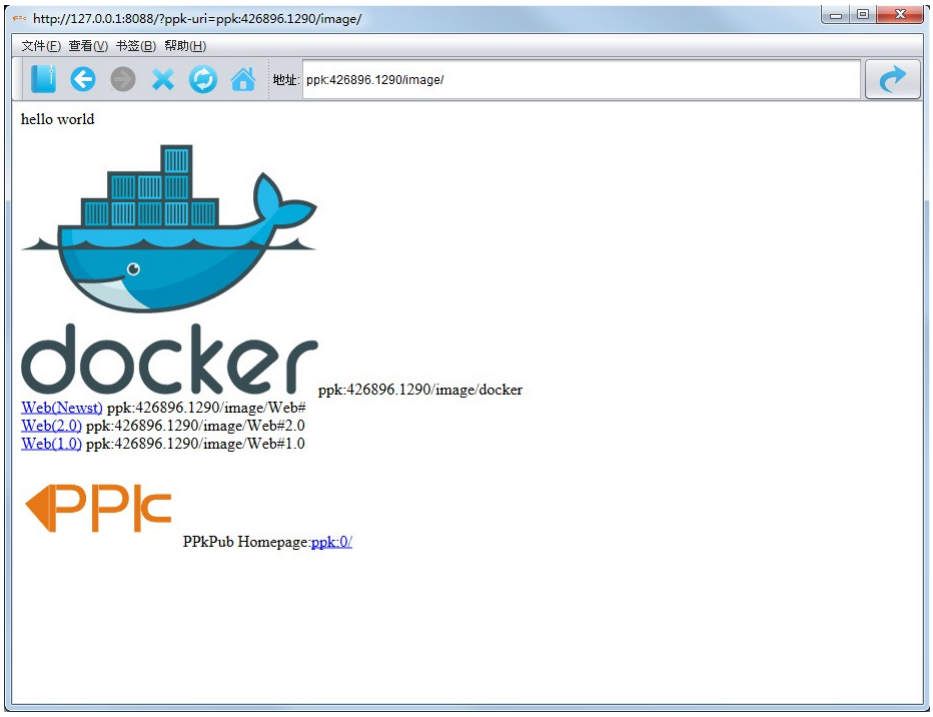
第 3 步：由客户端按 AP URL 中对应的实际承载协议类型（如图中示例的 HTTP 协议）来组织发送符合 PTTP 协议的兴趣包（Interest）给 AP 节点，并获得其所应答的内容数据包（Data）。

第 4 步：客户端按该 ODIN 标识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。

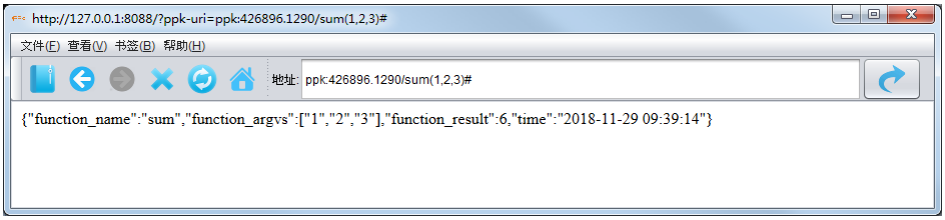
上图中示例显示的内容正文是一个简单的 HTML 网页内容，用户可以点击其中的链接来跳转访问到其他内容资源。

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：

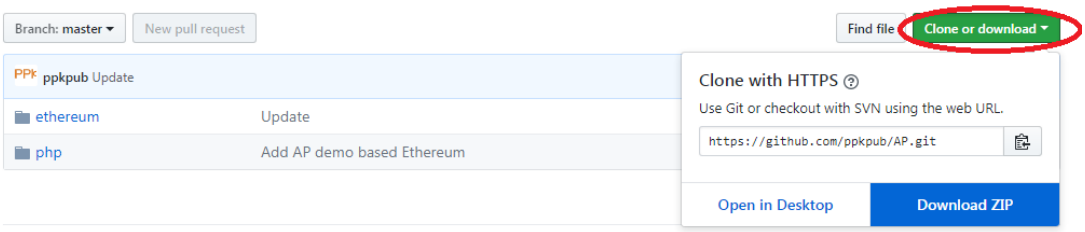
在这些示例的基础上，可以在浏览器端实现类似 AJAX 等更复杂的网页交互功能， 配合多种区块链平台的浏览器钱包插件比如 Metamask，可以更好地开发采用 PPk ODIN 标识和 PTTP 协议的应用服务。更为有用的是，通过 ODIN 标识配合 PTTP 协议可以帮助应用不需要再绑定于具体区块链平台，也不再受制于传统 DNS 域名和 IP 网络通信机制的局限，提供内容服务的 AP 可以是传统机房里拥有全网静态 IP 地址的服务器，也可以是物联网场景下灵活组网的终端设备，任意设备间都可以自由达成对等、可信的信息交换。

六、如何搭建一个支持 PTTP 协议的内容节点 AP？

在注册自己的 ODIN 标识后，下一步就可以搭建一个支持 PTTP 协议的内容节点即 AP，将新注册的 ODIN 标识设置映射到这个 AP，就可以被 PPk 客户端浏览访问了。

这里以网站开发常用的 PHP 语言为例，在新浪云服务（SAE）的虚拟主机上搭建一个基于 HTTP 协议实现的 AP 简单示例，其他程序语言和虚拟主机服务商可以参考实现。实现过程如下：

1. 从 PPkPub 的 GitHub 开源代码库下载实现 AP 的示例源码，在电脑浏览器里访问下述网址：
   https://github.com/ppkpub/AP
   显示如下图的网页：



点击其中的“Clone or download ”绿色按钮，再点击“Download ZIP”按钮，就可以下载源码压缩文件了。

2. 将下载的源码压缩文件（文件名为 “AP-master.zip ” ）解压后，进入解压文件夹下的 php 子文件夹。

3. 进入 resource 子文件夹，将其中的“426135.698”文件夹改名为“513468.490”，然后进入改名后的“513468.490”文件夹，用记事本等文本编辑器分别打开“#1.0#” 和“image_demo#1.0#”，将这两个文件原文中的“426135.698”都替换为自己新注册的 ODIN 标识，例如前述第三节示例中的“513468.490”，然后保存退出。

5. 回到 php 文件夹，再进入 key 子文件夹，将其中的“426135.698.json”文件改名为“513468.490.json”。

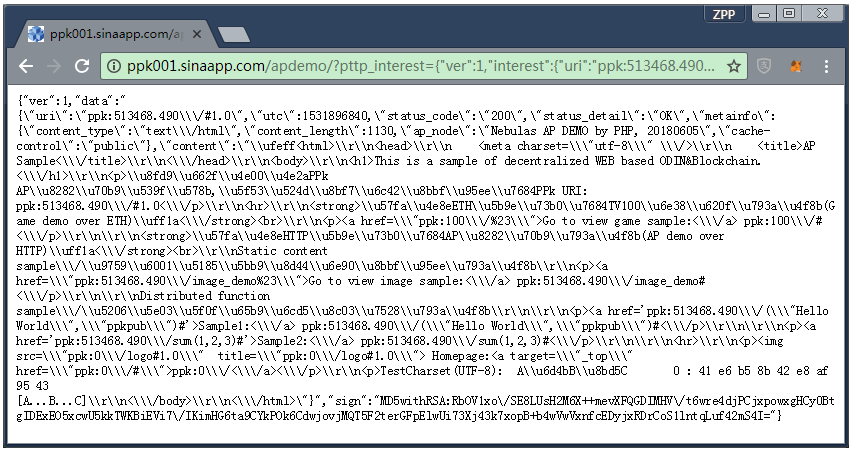
6. 以新浪云服务（SAE）的虚拟主机为例，假设你的网站主地址是 http://ppk001.sinaapp.com/ 。到自己虚拟主机的主目录下新建一个名为“apdemo”的文件夹，然后将上述修改后的 php 文件夹下的所有文件都上传到该新建文件夹下，那么你所搭建的 AP 的访问入口地址 URL 就为：

http://ppk001.sinaapp.com/apdemo/

在获得上述的访问入口地址 URL 后，可以在电脑浏览器里输入类似下方的网址进行测试：

http://ppk001.sinaapp.com/apdemo/?pttp_interest={"ver":1,"interest":{"uri":"ppk:513468.490/"}}

将这里的 ppk001.sinaapp.com 替换成你的网站地址，513468.490 替换成你自己的 ODIN 标识即可。如果浏览器显示结果如下图，说明 AP 已经部署成功了。



7. 现在要做的是将 ODIN 标识映射到刚部署成功的 AP 节点。点击 PPk 客户端主窗口上方的“开放数据索引命名 ODIN”，然后点选“我管理的 ODIN 号”查看到自己有权限管理的 ODIN 标识列表了，如下图所示：

点击所要操作的 ODIN 标识如“513468.490”所在行右侧的“更新”按钮，再点击“设置访问点”按钮进入设置，显示如下图所示：

将前面部署 AP 时获得的访问入口地址 URL（例如“http://ppk001.sinaapp.com/apdemo/”）填入第一行，然后点击“设置访问点”按钮确认提交，就可以发出更新 AP 访问点配置的交易了，同样需等待比特币网络确认后就会生效。

8. 等上一步提交更新的交易被确认后，进入浏览器，在显示区域最上方的网址输入框输入你所注册的 ODIN 标识对应网址例如“ppk:513468.490/”后，点击“Go”按钮，将显示如下图所示的网页内容：

这就说明已成功将你注册的 ODIN 标识映射到了你所部署的 AP，其他用户都可以通过 PPk 客户端来

浏览访问了。

更进一步，我们还可以设置所注册 ODIN 标识的“可信验证参数”，使得 PPk 浏览器可以从 AP 获取的内容验证其是否可信。具体设置请参考后面第七节“如何让自己的 AP 发布的内容自证可信？”详细说明。

七、如何让自己的 AP 节点发布的内容自证可信？

类似传统 DNS 域名的安全升级方案 DNSSEC，ODIN 标识原生支持内容可信配置功能，依靠公开的比特币区块链，数据请求者可以对从支持 PTTP 协议的内容节点即 AP（Access Point）获得的数据内容自主进行可信验证。

这里作为一个简单示例，我们采用结合 SHA256 哈希算法的 RSA 非对称签名验证算法，对于实际应用，还可以灵活选择更高强度的哈希算法。我们要做的是按 RSA 非对称算法生成一对公私钥，将私钥配置在 AP 受保护目录下对所发布内容进行签名使用，而将公钥信息作为对应 ODIN 标识的配置参数关联保存到比特币区块链上公开，这样内容访问者从 AP 拿到包含对应 ODIN 标识地址和签名的内容数据包后，就可以自主从比特币区块链上获取对应 ODIN 标识的配置参数，并用其中包含的公钥来验证所获得内容数据包签名的合法可信性。

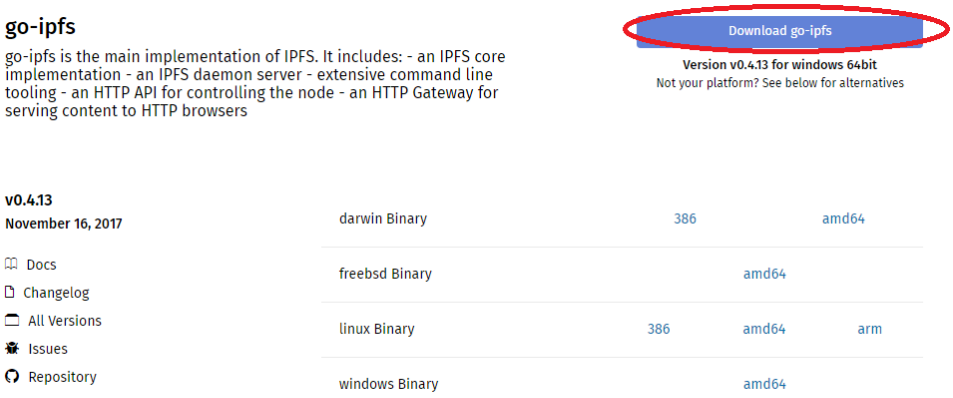
因为公钥数据比较长，不适合打包到交易里直接存放到比特币区块链上，我们采用 IPFS 分布式存储网络来实际存储公钥，而将所获得的类似“ipfs:xxxxx”这样的资源网址 URI 打包到比特币交易信息里保存到比特币区块链上。

为了能上传公钥到 IPFS 分布式存储网络里，我们需要先安装 IPFS 的客户端，这里以在 Windows7 操作系统下安装和运行 IPFS 服务为例，其他操作系统可参考安装。具体过程如下：

1. 用电脑浏览器访问 IPFS 网站下载安装包，网址如下：

https://dist.ipfs.io/#go-ipfs

其网页显示如下图所示：



2. 点击上图中的“Download go-ipfs”按钮开始下载。下载完成之后解压，得到文件夹 go-ipfs 。

3. 进入命令行模式，输入命令 ipfs init 在本机初始化建立一个 IPFS 节点。

4. 输入命令 ipfs daemon 就可以启动 IPFS 节点服务器了。

关于 IPFS 更详细的说明可以访问 https://ipfs.io 或这篇网上教程（https://steemit.com/ipfs/@zlj280316532/ipfs-windows）来深入了解。

安装和启动运行 IPFS 服务后，我们就可以运行 PPk 客户端来生成和上传公钥了，具体操作过程如下：

1.点击 PPk 客户端主窗口上方的“开放数据索引命名 ODIN”，然后点选“我管理的 ODIN 号”查看到自己有权限管理的 ODIN 标识列表了，如下图所示：

点击所要操作的 ODIN 标识如“513468.490”所在行右侧的“更新”按钮，再点击“内容可信设置”按钮进入设置，显示如下图所示：

2. 用鼠标将显示区域往下滚动，使用第二种更新可信设置的方式，由客户端来自动生成公私钥，并在提交更新时自动将公钥保存到 IPFS 分布式存储网络用于公开验证使用，操作界面显示如下图所示：

上图示例中已经生成好一对公私钥，请注意先将私钥内容复制备份到自己的私人文件中保存好。再查看下显示区域底部所提示的当前 IPFS 服务状态，如果显示为“[IPFS:OK]”说明 IPFS 服务正常可用，否则说明 IPFS 服务不可用，则需要先参考前述的 IPFS 安装运行的说明来确保已安装和启动运行 IPFS 服务。

3. 确认已备份保存好私钥和 IPFS 服务正常后，就可以点击“提交更新”按钮确认提交了，PPk 客户端会自动将公钥上传到 IPFS 上，再将得到的 IPFS 资源地址放入 ODIN 标识的内容可信配置更新交易里发送到比特币网络，等待比特币网络确认后就会生效。

4.用 Windows 系统的文件管理器打开 PPk 客户端的安装文件夹，进入 resources\db\keys 子文件夹，找到其中文件名与你的 ODIN 标识相同的文件（例如“513468.490.json”），将其复制上传到你的虚拟主机上 AP 部署文件夹的“key” 子文件下。

5.进入 PPk 浏览器，在显示区域最上方的网址输入框输入你所注册的 ODIN 标识对应网址例如“ppk:513468.490/”后，点击“Go”按钮，如能正确显示对应的网页内容，说明内容可信配置已经生效。