作为虚拟货币行业的人，我们经常会讨论加密资产放在钱包里是否安全。有很多细节需要注意。你知道安全加密资产吗？今天就让边肖告诉你吧！

安全NICO交易所带领业内顶尖团队参照银行标准建立的安全防护体系，通过平台、账户、钱包、内控管理等多层安全防护，最大限度降低系统风险，全方位、多层次保护用户资产。

AcToken钱包是一款数字资产钱包。

钱包只是AcToken将触角伸向虚拟货币的第一步，未来的愿景是打造打通金融圈和币圈的唯一通道。币圈有大量营销需求，希望接触到有投资意向的高净值人群。

如果你刚进入区块链世界，你会不知所措，看不懂陌生的数字和晦涩难懂的技术词汇。你如何迈出进入区块链大门的第一步？

首先，让&#039；不是研究什么是区块链，什么是智能合约，加密算法等等。你要做的第一步，就是先有自己的钱包。

在数字资产的世界里，钱包是一个密钥(包括私钥和公钥)的管理容器。。用户使用私钥对交易进行签名，从而证明他有权导出交易，他的交易信息不存储在钱包中，而是存储在区块链中。

AcToken是基于石墨烯底层技术的DPOS共识机制。可以达到百万TPS，毫秒级确认速度。AcToken是一个移动轻型钱包应用程序，可以与ABTC用户的底层数据进行通信。鑫数码一键交易平台。，旨在为普通用户提供一个安全、方便、简单、实用、功能强大的数字资产钱包应用。

钱包只是AcToken将触角伸向虚拟货币的第一步，未来的愿景是打造打通金融圈和币圈的唯一通道。币圈有大量的营销需求。希望接触到有投资意向的高净值人群。

通常情况下，它&#039；把它放在钱包里更安全。毕竟，这&#039；这是你自己的东西。如果你把它放在别处，它可能会丢失。

根据2021年1月12日AtlasVPN的研究，去年的区块链袭击给受害者造成了38亿美元的巨大损失。

这些数字是由Slowmist黑客安全团队提供的。，包括上述文章，是关于区块链项目、应用程序和令牌以及加密货币骗局的信息，这些信息占2020年所有区块链相关黑

客事件的13%。

运行在以太坊上的DApps和去中心化应用被攻击47次，当前价值4.463亿美元，其次是加密货币交易所被攻击28次(损失3.001亿美元)。

加密钱包是黑客最青睐的目标，损失近30.3亿美元。

加密货币钱包是一个用于存储私钥和公钥的软件程序，使用户能够发送和接收数字货币并监控其余额。

私钥，是掌握数字钱包的入口，只有私钥才能证明你是钱包里资产的主人，除了你没有人知道这串私钥。网络罪犯通常使用复杂的技术入侵数字钱包，在用户不知道的情况下窃取或转移加密资产&#039；的知识。。在保护数字货币免受网络攻击时，保护好钱包非常重要。

例：英国人乔恩(Jon)2010年开始比特币，把自己的私钥写在一张纸上，清洁工却把它扔了。从此，他钱包里的1万美元比特币就与他无关了。

以下是一些保护你的加密货币的方法：

01保持冷静

当你的加密资产被盗时，请保持冷静，不要&#039；不要惊慌。以免操作不当造成资产的二次损失。

如果您想更改您的密码、电子邮件或备份设备，请花一些时间来确保您能够清醒地完成所有步骤。

如果您的资金是离线存储的，那么你的资产处于安全状态，硬件钱包是最安全的资产存储方式。

02使用冷热钱包

热钱包是&quot在线钱包&quot，可用于在浏览器或移动设备上交易比特币。，可以随时访问。

与热钱包不同，冷钱包没有联网，因此不容易受到网络攻击。他们使用物理介质离线存储密钥，这也使他们能够抵御在线黑客攻击，所以冷钱包保存代币更安全。

热钱包适合日内交易，冷钱包更适合加密资产的长期存储。唐&#039；不共享私钥

每个加密货币钱包都有一个公钥和一个私钥。

私钥用于验证资产所有权和加密钱包，公钥用于识别钱包和接收资金的公共地址。

切勿与他人共享私钥或密码。共享私钥或密码实际上是给其他人获得自己的加密货币资产的机会。请记住信誉良好的加密货币公司绝不会要求用户提供密钥来帮助他们解决问题。

只有保护好私钥，才能控制自己的货币。这就是谚语&quot不是你的钥匙，不是你的硬币&quot。

04使用安全的网络

进行任何交易时，请使用安全的互联网连接，避免使用公共Wi-Fi网络。即使访问家庭网络，也可以使用VPN来提高安全性。使用VPN会改变IP地址和位置，它会对您的通信、数据、位置等隐私信息保密，从而提高您交易的安全性。

05使用多个钱包来分散资产

俗话说，把鸡蛋放在不同的篮子里，这样你就可以把资产分散在多个钱包里。日常交易用一个钱包，其余的放在单独的钱包里，增强资产安全性，减少意外情况下的账户损失

。

06定期更换密码尤为重要

。

美国一项研究显示，美国四分之三的千禧一代在十几个设备、应用和其他社交媒体账户上使用同一个密码。他还指出大多数人在50多个不同的地方使用同一个密码。

如果您的电子邮件地址遭到黑客攻击，我们建议您更改相关密码。考虑密码时，我们建议您选择包含多种类型的字符，如大小写字母和符号，以增强安全性。

定期更改密码有助于提高资产的安全性。如果您有多个钱包，您可以通过选择双因素身份验证(2FA)或多因素身份验证(MFA)来提高安全性。小心钓鱼活动

通过恶意广告和邮件进行网络诈骗在加密货币领域非常普遍，因此我们在进行加密货币交易时应该小心谨慎，避免点击任何可疑和未知的链接。

根据2021年1月12日发布的AtlasVPN报告，在过去的五年中，攻击数量总体呈下降趋势。虽然2019年有133起针对各种区块链平台、应用和令牌的协同攻击，但到2020年，这一数字下降了8%。。

随着加密货币行业的不断发展，我们学会采取必要的安全防范措施来保护自己的资产安全是非常重要的。

更多信息欢迎关注微信官方账号：1矿计算平台。

近年来，数字钱包安全事件频发。

2019年11月19日，ArsTechnica报道，两个加密货币钱包的数据泄露，220万账户信息被盗。安全研究员特洛伊亨特证实被盗数据来自加密货币钱包GateHub和RuneScape机器人提供商EpicBot的账户。

这已经不是Gatehub第一次遭遇数据泄露了。据报道，去年6月黑客入侵了大约100个XRP账本钱包，导致近1000万美元被盗。

2019年3月29日，比瑟姆布失窃案引起轩然大波。据推测这件事的起因是因为Bithumb拥有的g4ydomrxhege账号的私钥被黑客窃取。

随即，黑客将盗取的资金分散到各个交易所，包括火币、HitBTC、WB、EXmo等。根据非官方数据和用户估计比瑟姆遭受了高达300万EOS币(约1300万美元)和2000万XRP币(约600万美元)的损失。

由于数字货币的匿名性和去中心化，一定程度上难以追回被盗资产。因此钱包的安全性很重要。2020年8月9日CertiK&#039的安全工程师在DEFCON区块链安全大会上发表主题演讲：利用不安全的加密钱包。，分享对加密钱包安全性的见解。

Encryptedwallet是一款帮助用户管理账户和简化交易流程的应用程序。

一些区块链项目发布加密钱包应用程序以支持该链的开发——，如CertiK链的Deepwallet。

另外还有Shapeshift这样的公司。，它构建支持不同区块链协议的钱包。

从安全性的角度来看，加密钱包最重要的问题是防止攻击者窃取用户的助记符和私钥&#039；钱包。

过去一年，CertiK技术团队对几款加密钱包进行了测试和研究，分享了基于软件对不同类型加密钱包进行安全评估的方法和流程。

加密钱包的基本审计列表

应该评估一个应用程序。首先需要了解它的工作原理代码实现是否遵循最佳安全标准安全性不足的部分如何纠正和改进。

CertiK技术团队制定了一份加密钱包的基本审计清单。这个列表反映了所有形式的加密钱包应用(手机、web、扩展、桌面)，尤其是手机和web钱包，是如何产生和存储用户的&#039；私钥。

应用程序如何生成私钥？

应用程序如何以及在哪里存储原始信息和私钥？

钱包是否连接到受信任的区块链节点？

应用程序是否允许用户配置自定义区块链节点？如果允许的话，恶意区块链节点会对应用产生什么影响？

应用程序是否连接到中央服务器？如果是，客户端应用程序将向服务器发送什么信息？

应用程序是否要求用户设置高安全性密码？

当用户试图访问敏感信息或转账时，应用程序是否需要二次身份认证？

应用程序是否使用了易受攻击的第三方库？

有没有什么秘密(比如API密匙)，AWS凭据)在源代码库中泄露？

程序源代码中是否存在明显的不良代码实现(比如对密码学的误解)？

应用服务器是否强制TLS连接？

手机钱包

与笔记本电脑相比，手机等移动设备更容易丢失或被盗。

在分析针对移动设备的威胁时，需要考虑攻击者可以直接访问用户设备。

在评估期间，如果攻击者获得用户的访问权&#039；的设备，，或者用户设备感染了恶意软件，我们需要尝试识别对帐户和密码资产造成损害的潜在问题。

除了基本列表之外，在评估移动钱包时还应添加以下审核类别：

应用是否警告用户不要截图敏感数据？——安卓应用在显示敏感数据时是否会阻止用户截图？iOS应用是否警告用户不要截图敏感数据？

应用在后台截图中是否泄露敏感信息？

应用程序是否检测设备是否越狱/root？

应用是否锁定后台服务器的证书？

应用程序是否记录程序中的敏感信息&#039；s日志？

应用程序是否包含错误配置的deeplink和intent，它们是否会被利用？

应用包是否混淆了代码？

应用是否实现了反调试的功能？

应用程序是否检查应用程序重新打包？

(iOS)iOS钥匙串中存储的数据是否有足够的安全属性？

应用程序是否受到钥匙链数据持久性的影响？

当用户输入敏感信息时，应用程序是否禁用自定义键盘？

应用程序是否安全地使用&quotwebview&quot要加载外部网站？

网络钱包

对于完全去中心化的钱包，Web应用程序正成为一个不太受欢迎的选择。MyCrypto不允许用户在web应用中使用keystore/助记符/私钥访问钱包，MyEtherWallet也建议用户不要这样做。

相对于运行在其他三个平台上的钱包，以web应用的形式对钱包进行钓鱼攻击相对更容易；如果攻击者入侵web服务器，他可以将恶意的JavaScript注入到网页中。，轻松抢走用户&#039；的钱包信息。

然而，一个安全构建且经过全面测试的网络钱包仍然是用户管理其加密资产的最佳选择。

除了上述通用的基本审计类别，当我们评估客户端webwallet时，，并列出了以下要审核的类别：

应用程序中是否存在跨站点脚本XSS漏洞？

应用是否存在点击劫持漏洞？

应用程序是否具有有效的内容安全策略？

应用程序中是否存在开放重定向漏洞？

应用中是否存在HTML注入漏洞？

目前在web钱包中使用Cookie的很少，但是如果有，要检查：

Cookie属性

跨站请求伪造(CSRF)

跨域资源共享(CORS)配置错误

。

除了基本的钱包功能之外，应用程序是否还包括其他功能？这些函数有没有漏洞可以利用？

上面没有提到的OWASP前10大漏洞。

扩展钱包

metamask是最著名也是最常用的加密钱包之一，以浏览器扩展的形式出现。

扩展钱包的内部工作方式与web应用程序非常相似。

不同的是，它包含独特的组件，称为内容脚本和后台脚本。

网站通过内容脚本和后台脚本传递事件或消息，与扩展页面进行通信。

在扩展钱包评估期间最重要的事情之一是测试恶意网站是否可以在没有用户的情况下读取或写入属于扩展钱包的数据&#039；的同意。

除了基本列表之外，在评估扩展wallet时还应添加以下审计类别：

扩展需要什么权限？

扩展应用如何决定允许哪个网站与扩展钱包通信？

扩展钱包如何与网页交互？

恶意网站能否通过扩展中的漏洞攻击扩展本身或浏览器中的其他页面？

恶意网站可以在没有用户的情况下读取或修改属于该扩展的数据吗&#039；s的同意？

扩展钱包是否存在点击劫持漏洞？

扩展钱包(通常是后台脚本)在处理消息之前是否检查了消息的来源？

应用程序是否实施了有效的内容安全策略？电子桌面钱包

写完了web应用的代码，为什么不用这段代码在电子里构建一个桌面应用呢？

过去测试的桌面钱包，大约80%是基于电子框架的。。在测试基于电子的桌面应用程序时，我们不仅要寻找web应用程序中可能存在的漏洞，还要检查电子配置是否安全。

CertiK分析了Electron&#039的桌面应用程序。详情可以点击访问这篇文章。

以下是评估基于电子的桌面钱包时要添加的审计类别：

应用程序使用哪个版本的电子设备？

应用程序是否加载远程内容？

应用程序是否禁用&quot节点集成&quot和&quotenableRemoteModule&quot？

IstheapplicationenabledwithContextIsolation,SandboxandwebSecurityoptions?

应用程序是否允许用户从当前钱包页面跳转到同一窗口中的任何外部页面？

应用程序是否实施了有效的内容安全策略？

预加载脚本是否包含可能被滥用的代码？

应用程序是否将用户输入直接传递给危险的函数(例如&quot打开外部&quot)?

应用程序是否制定了不安全的自定义协议？

服务器端漏洞检查列表

我们测试过的加密钱包应用中，超过一半没有集中式服务器，它们直接与区块链节点相连。

CertiK技术团队认为这是一种减少攻击面和保护用户的方法&#039；隐私。

但是如果应用程序希望为客户提供比帐户管理和令牌传输更多的功能，它可能需要一个带有数据库和服务器端代码的集中式服务器。

服务器端组件要测试的项目高度依赖于应用程序特性。

根据调研和与客户接触中发现的服务器端漏洞，我们整理了以下漏洞清单。当然，它并不包含所有可能的服务器端漏洞。

认证和授权

KYC及其效力

竞赛条件

云服务器配置错误

Web服务器配置错误

不安全直接对象引用(IDOR)

服务器请求伪造(SSRF)

任何类型的注入(SQL，command，template)漏洞

任意文件读/写

业务逻辑错误

速率限制

总结

随着技术的发展，黑客实施的诈骗和攻击手段越来越多样化。

CertiK安全技术团队希望通过分享加密钱包的隐患，让用户更多了解数字货币钱包的安全问题，提高警惕。

现阶段很多开发团队对安全的重视程度远远低于对业务的重视程度，没有对自己的钱包产品做足够的安全防护。通过分享加密钱包的安全审计类别，CertiK希望加密钱包项目各方对产品安全标准有一个清晰的理解。从而推动产品安全升级，共同保护用户资产安全。

数字货币攻击是一种多技术维度的综合攻击，需要考虑数字货币中管理和流通过程中涉及的所有应用安全，包括计算机硬件和区块链软件。、钱包等区块链服务软件、智能合约等。

加密钱包需要注意对潜在攻击的检测和监控，避免多次被同样的方式攻击，加强数字货币账户的安全保护手段。，使用物理加密离线冷存储(coldstorage)保存重要数字货币。此外，还需要聘请专业的安全团队在网络层面进行测试，通过远程模拟攻击来发现漏洞。

TrustWallet是Bi&#039安。信任是一款界面干净整洁，安全性高的移动应用。它旨在促进不同区块链知识水平的用户采用加密货币。。信任提供了一个可以发送、接收和存储加密资产的可靠钱包。其内置的去中心化应用程序(dApp)浏览器可用于与dApp通信，并直接在智能手机或平板电脑上交易加密货币和收藏品。

TrustWallet是ios和Android设备的独立应用程序，允许用户管理自己的加密货币，并与去中心化应用程序(DApps)进行交互，包括DEX。。TrustWallet目前在国内主流应用商城、360手机助手、腾讯应用商店、OPPO软件商店、华为应用商店、小米应用商店都没有下载渠道。。只能通过官网、GooglePlay、苹果APPStore下载。

作为一款以太坊钱包，TrustWallet支持的虚拟数字货币资产主要是ERC20和ERC223代币。目前，，通过其trustwallet应用程序，您可以访问超过30，000个基于以太坊的令牌。

对比之前评测的钱包给出的用户需求知道和新手提示，TrustWallet设置的开门见山。创建钱夹之前没有风险警告。，单击创建Wallet直接跳转到备份助记符页面。虽然私钥助记页可以&#039；不要被抓住，钱包里有一个&quot复制&quot助记符的功能。点击后弹出一个系统分享页面，可以分享近20个应用，社交类app，资讯类app。

以下是常规的助记符验证，只要助记符排列顺序正确，备份就完成了。创建和备份的步骤非常简单，不需要用户注册应用登录账号和密码，流程极其精简。但全程没有专业术语解释和风险提示。，对小白用户非常不友好。

信任钱包&#039；的页面很简单，只有三个部分。相应的功能也很少，侧重于存储数字资产。页面会显示相关货币的实时价格，但没有趋势图。

除了用户设置和钱包，另一大功能是DApps。在这个盘子里，链接虚拟数字货币交易所、社交软件、应用市场等。如EASYTRADE、KyberNetwork、CanWork、Indorse和Multitokens。其中以EASYTRADE为代表。，链接11个交易所，是一个内置的交易所。

TrustWallet尚未开通国内社交渠道，但在国外活跃于Twitter和Telegram，每日资

讯和行业资讯更新及时。

总体来说，尽管缺乏新手提示和风险提醒，但TrustWallet简单的设置还是让新手很容易上手。但在功能上，由于对数字资产存储的简单限制，还是很难让老手们满意

将加密资产放在钱包中安全吗？对很多人来说都很头疼，尤其是在认识和现实的冲突中。安全加密资产也面临类似问题。关注我们，为您服务，是我们的荣幸！