链塔智库

Block Data

市场主流数字货币硬件钱包研究报告

2018年7月20日

目录

CONTENTS

前言

PREFACE

随着区块链行业的日渐成熟，数字货币市场的安全问题成了刻不容缓、亟待解决的问题。

无数的数字资产丢失的事件证明了再安全的技术也不能百分之百无漏洞，只要接触网络，就会给黑客制造可乘之机。目前最安全的办法就是一个与网隔绝的硬件来储存私钥。市面上的硬件钱包越来越多，说明硬件钱包的使用率和价值也原来越高。

链塔智库BlockData对硬件钱包产品的种类及具体产品进行了研究，从安全性、使用性能等各角度对比分析了国内外主流硬件钱包产品。

1.硬件钱包综述

1.1 硬件钱包定义

数字货币硬件钱包是一种实体设备，私钥储存在设备内的受保护区域中。硬件钱包与纸质钱包类似，但在收付款方面的功能更强。到目前为止，还没有发生过大规模的硬件钱包漏洞或黑客窃取资金事件。硬件钱包也能抵抗病毒，因私人密钥不能以明文的形式从这些设备中移除。目前，越来越多的数字货币交易者选择硬件钱包。

1.2 硬件钱包分类

市面上的硬件钱包的实现方式主要有两大类别。一种是以Legder Nano S、碧盾、Trezor、KeepKey为代表的基于芯片的硬件钱包，另一种是以库神、Bepal为代表的基于安卓系统的钱包，也称为类手机钱包。

前者的保护重点是私钥本身的芯片级安全保护，强调的是即使用户遗失或设备被黑客窃取情况下，私钥也不会流失，也能保护用户的资产安全。后者保护重点是冷热端在交易时隔离，当设备未遗失的情况下，也未被针对性破解攻击的情况下，交易是安全的。总之，相对基于硬件的芯片的硬件钱包，类手机钱包在黑客拿到物理设备后更容易发起针对性攻击。

项目	芯片类	安卓系统类
代表产品	Legder Nano S	库神
保护机制	私钥本身的芯片级安全保护	冷热端在交易时隔离
一般情况	保护程度一样	保护程度一样
丢失情况	保护程度高	保护程度低
安全性	高	较高

2.硬件钱包安全性对比

2.1 硬件钱包安全性指标

1.私钥保存安全性

硬件钱包保存的是一个密钥对（一个公钥＋一个私钥）。 谁拥有了这个密钥，谁就拥有了钱包里的资产，那么就可以支配这些资产了。而一旦密钥丢失，那么这些资产也就永久性地丢失了。所以作为硬件钱包，在安全性问题上，首要解决的就是如何采用极为安全的方式来保存用户的秘钥。

硬件钱包的私钥被保存在硬件设备内，私钥的签名过程都在硬件钱包中进行。市面上的硬件钱包基本都能保证私钥不会流出到PC端，从这一角度来看，安全性是可以得到有效保障的。

此外，硬件钱包使用的芯片种类至关重要。使用安全芯片的硬件钱包能够有效地实现对私钥保护。相较而言，使用普通ARM芯片的硬件钱包对于私钥的保护相对偏弱，因为没有使用专门的安全芯片对私钥进行存储。如果黑客获取到物理设备，比较容易发起针对性攻击。

2.防电子攻击

黑客如果获取到硬件钱包，会采用多种方式侵入到硬件中，包括侵入式攻击（物理攻击，使用探针进行监听）和非侵入式攻击。一种典型的非侵入式攻击是电子探测攻击，攻击方式包括SPA和DPA攻击。

采用安全芯片的硬件钱包比普通ARM芯片更能有效抵御攻击。对于各种形式的电子探测攻击，都能做出有针对性的防护，可以有效地抵御各种形式的电子探测攻击 。

3.防交易伪造

在一个交易过程中，硬件钱包是没有能力判断计算机或手机运行环境的安全性的，也不能把安全体系建立在要求用户的计算机或手机运行环境安全的基础上。而在针对操作流程和安全体系的攻击中，黑客会通过攻破计算机或手机的客户端软件诱骗用户同意签署一个伪造的交易。

为防止这一类攻击，一个好的硬件钱包应该做以下两个核心的验证，来保障签署的交易和实际发生的交易一致。

一是要有用于可视化验证交易信息的可信的显示屏，而不依赖于电脑或手机端的信息显示。二是可信任的确认按钮，用来确认或拒绝签署交易。

因此很多硬件钱包会设计一个独立的显示屏，来让用户确认发送的目的地址和交易金额与客户端显示结果的一致性。

2.2 安卓系统类钱包安全性对比

一级指标	二级指标	库神	Bepal
安全性	私钥保护	私钥会留到内存中，内存中无安全防护	私钥会留到内存中，内存中无安全防护
	设备破拆后私钥安全性	私钥易流出芯片，安全度低	私钥易流出芯片，安全度低
	抗电子探测攻击	不抗电子攻击	不抗电子攻击
	防交易伪造	双屏对比交易信息，防交易伪造	双屏对比交易信息，防交易伪造

2.3 芯片类钱包安全性对比

一级指标	二级指标	Ledger Nano S	Trezor	KeepKey	碧盾
安全性	私钥保护	安全芯片	普通ARM芯片	普通ARM芯片	安全芯片
	设备破拆后私钥安全性	私钥不流出芯片，安全度高	私钥会流出芯片，但不流出设备，安全度较高	私钥会流出芯片，但不流出设备，安全度较高	私钥不流出芯片，安全度高
	抗电子探测攻击	抗电子攻击	不抗电子攻击	不抗电子攻击	抗电子攻击
	防交易伪造	双屏对比交易信息，防交易伪造	双屏对比交易信息，防交易伪造	双屏对比交易信息，防交易伪造	双屏对比交易信息，防交易伪造

3.硬件钱包使用性能对比

3.1 硬件钱包使用性能指标

1.交易方便性

指钱包在交易时是否方便。对于国内的用户来说，大部分数字资产相关的软件都要翻墙才能使用。

2.密码输入方便性

PIN码是硬件钱包安全的重要保障，因为外部PC环境可能存在安全隐患，如键盘输入可能被黑客监视，因此PIN码的输入不能从PC端直接输入。Ledger Nano S，Trezor，KeepKey和碧盾在PIN码的输入上采用了不同的输入方式。

举例来说，Ledger Nano S的方案是通过纯硬件按钮进行操作，这样保证了PIN码输入的安全性，且不容易被截获。但Ledger Nano S使用起来很不方便，频繁的操作也会降低使用寿命。

Trezor和KeepKey使用硬件上的打乱的密码键盘配合PC上点击虚拟键盘的方式进行PIN码的输入。相对来说，不需要频繁地进行按钮操作，使用方便性上强了很多。

碧盾的PIN码在技术上有创新。即使键盘操作被黑客截获，黑客也无法窃取到设备的PIN码。

3. 交易流畅性

指钱包在网页端或App界面操作时的速度，比如页面打开是否流畅，指令提交反应速度等等。

3.2 安卓系统类钱包使用性能对比

一级指标	二级指标	库神	Bepal
便捷性	交易方便性	设备上有App，需要手机和设备间反复扫二维码，比较繁琐	设备上有App，需要手机和设备间反复扫二维码，比较繁琐
	密码输入方便性	安卓系统，操作较简单	安卓系统，操作较简单
	交易流畅性	设备上有App，发送和接收较流畅	设备上有App，发送和接收较流畅

3.3 芯片类钱包使用性能对比

一级指标	二级指标	Ledger Nano S	Trezor	KeepKey	碧盾
便捷性	交易方便性	需要使用Chrome浏览器安装浏览器插件；需要翻墙才能使用	通过客户端结合网页使用；需要翻墙才能使用	需要使用Chrome浏览器安装浏览器插件；需要翻墙才能使用	客户端；无需翻墙即可使用
	密码输入方便性	使用设备上的按钮操作，操作较繁琐	设备上的数字键盘配合PC上鼠标输入，较便捷	设备上的数字键盘配合PC上鼠标输入，较便捷	直接使用键盘进行输入，操作便捷
	交易流畅性	网页端操作，发送和接收较流畅	网页端操作，发送和接收较流畅	网页端操作，发送和接收较流畅	用户的引导式操作

4. 硬件钱包其他指标对比

4.1 硬件钱包其他指标

1.支持币种种类

指钱包支持的币种种类，支持种类越多的钱包则受众越为广泛。

2.可恢复性

一般硬件钱包都会有助记词，目的是为了帮助用户记忆复杂的私钥（ 64 位的哈希值)。

4.2 安卓系统类钱包其他指标对比

指标	库神	Bepal
币种支持	支持BTC、ETH等数十个币种及ERC20	支持BTC、ETH等数十个币种及ERC20
可恢复性	支持12个助记词恢复	支持12个助记词恢复

4.3 芯片类钱包其他指标对比

指标	Ledger Nano S	Trezor	KeepKey	碧盾
支持币种	支持BTC、ETH等数十个币种及ERC20	支持BTC、ETH等数十个币种及ERC20	支持BTC、ETH等数十个币种及ERC20	支持BTC、ETH和部分ERC20代币
可恢复性	支持24个助记词恢复	支持24个助记词恢复	支持12个助记词恢复	支持24个助记词恢复

4. 4硬件钱包日常防护设计

考虑硬件钱包使用较为频繁，日常使用需要考虑防尘防水防摔设计，尤其以防水功能需求最为普遍。

4.4.1安卓系统类钱包其他指标对比

指标	库神	Bepal
防水设计	未明确标识	未明确标识

4.4.2芯片类钱包其他指标对比

指标	Ledger Nano S	Trezor	KeepKey	碧盾
防水设计	未明确标识，外观有明显缝隙	声称防水，但外观有明显缝隙	未明确标识，正面整块塑胶覆盖防水	IPX67级防水防尘，整体取消实体按钮设计

4. 5硬件钱包零售价格对比

作为一个硬件，在市场推广阶段除上述各种因素外，价格是用户购买决策的重要考量。安卓系统类硬件钱包零售价格较高，均超过3000元，而主流芯片类钱包零售价格均未超过2000元，碧盾零售价甚至下探至599元，堪称硬件钱包的价格杀手。

4.5.1安卓系统类钱包零售价格对比

指标	库神	Bepal
价格	4288元	3280元

4.5.2芯片类钱包零售价格对比

指标	Ledger Nano S	Trezor	KeepKey	碧盾
价格	1188元	1199元	1699元	599元

结语

CONCLUSIONS

- 目前，硬件钱包是所有钱包中安全系数最高的。
- 市面上的硬件钱包的实现方式主要有两大类别。一种是以Legder Nano S、碧盾、Trezor、KeepKey为代表的基于芯片的硬件钱包，另一种是以库神、Bepal为代表的基于安卓系统的钱包，也称为类手机钱包。
- 和基于芯片的硬件钱包相比，黑客拿到物理设备后更容易对类手机钱包发起针对性攻击。
- 从安全性对比来看，芯片类比安卓系统类的安全系数高。Ledger Nano S和碧盾由于使用安全芯片因此安全性最高。
- 从使用性能对比来看，安卓系统类更加智能，用户体验更好，但需要手机和设备间反复扫二维码，比较繁琐。芯片类的由于设备比较简易，操作起来也容易一些。
- 和来自国外Ledger nano S、Trezor和Keepkey相比，国产的库神、Bepal和碧盾均不用翻墙，大大降低了用户的使用门槛。
- 硬件钱包的零售价从599-4288元不等，显然不同的价格策略是因为选择不同的用户群体。相对来讲库神和Bepal更专注于数字资产的高端人群，而售价不足599元的碧盾更适合关注钱包性价比的用户。

法律声明

STATEMENT

知识产权声明

本报告为链塔智库BlockData制作，报告中所有数据、表格、图片均受有关商标和著作权法律保护，部分数据采集自公开信息，知识产权为原作者所有。我们相信数据的价值，我们同样相信分享也能创造价值，我们欢迎各组织和个人采用我们的报告和数据，在此之前告知我们即可。

免责条款

本报告中所载所有内容为链塔智库分析师通过访谈、市场调查、信息调研整理及其他方式方法获得，并结合链塔智库独有的数据和分析资源，建立相关预测模型估算而得，为区块链行业从业者提供基本参考，受研究方法和数据获取渠道所限，本报告只提供受众作为各类市场活动参考资料，不构成任何投资或交易买卖建议。如果访问者依据本报告信息进行投资或进行交易买卖而遭受损失，本公司对此不承担责任。

链塔智库

链 我们深刻认识到区块链数据的价值，专注用深度数据赋能区块链产业。

塔 我们关注每一个细分领域的头部项目，Top X只是我们展现的手段。

智 我们只与业内顶尖的合作伙伴、区块链专家、行业分析师为伴，提供专业的数据服务。

库 我们拥有全球最全的区块链项目库，时刻扫描和追踪全球区块链动态。

我们是链塔智库 推崇专注专心专业，坚持公开公正公平，“天赐时代 睿见未来”，预见更多可能。

全球首家区块链数据服务提供商

扫码关注公众号

扫码进入小程序

网址：www.blockdata.club

微信订阅号ID：liantazhiku

链塔智库合作伙伴

独家大数据支持平台：TalkingData

联合发布媒体（排名不分前后）：

BiaNews Beta　三言财经 Sanyan Blockchain　3区　耳朵财经　金色财经

火星财经　猎云财经　星球日报 DDAILY

媒体深度合作伙伴（排名不分前后）：

猛犸财经 www.mema24.com　链路财经 linksfin.com　互链脉搏 INTERCHAIN PULSE　链道学社　财链社

挖链网 walian.cn　区块链蓝海 BLUE SEA OF BLOCK CHAIN　千氪财经 WWW.KG.COM　核财经 HE CAI JING　TuoniaoX.com 鸵鸟区块链

未来财经 weilaicaijing.com　JINNIU.CN 金牛财经

链塔智库

Block Data

全球区块链数据服务提供商

1600+项目入库/800+机构入驻/100+专家学者观点

扫码关注公众号

ID：liantazhiku

扫码进入

小程序

『链塔智库BlockData』，全景式扫描和追踪全球区块链公司/项目，提供深度数据服务，专注于区块链行业研究、分析、项目评级。全球最全的区块链项目库1600+（数据每周都在更新）。