区块链安全研究中心
Blockchain Security Research Center

加密数字钱包APP信息安全现状白皮书（2018年）

上海交通大学 网络空间安全学院
CAICT泰尔终端实验室 中国信息通信研究院 China Telecommunication Technology Labs-Terminals
掌御科技

检测单位：

上海交通大学网络空间安全学院

中国信息通信研究院泰尔终端实验室

上海掌御信息科技有限公司

联合发布单位：

中国区块链应用研究中心

杭州加密谷区块链科技有限公司

上海淳粹文化传媒有限公司

版权申明

免责声明

该《加密数字钱包 APP 信息安全现状白皮书》（简称《白皮书》）由区块链安全研究中心（由上海交通大学网络空间安全学院、中国信息通信研究院泰尔终端实验室、上海掌御信息科技有限公司联合成立）采用公开、合法的信息，运用相应的科学研究方法，对当前加密数字钱包行业相关 Android 移动应用（APP）做出的信息安全分析评判。工信部组织本次检测工作并由上述三家单位联合发布该《白皮书》，其目的在于促进加密数字钱包安全生态发展，提高加密数字钱包企业移动安全水平，实现用户和企业共赢。本次检测不对企业数据、用户隐私造成任何破坏，旨在发现应用本身的安全问题，对于存在的安全问题不做深入利用。所有安全信息按照企业内部流程处理完成之前不会对外公开。

该《白皮书》的检测对象的信息安全测试完全针对相应加密数字钱包企业自身对外公开发布的 APP 程序进行，并对所有抽样平台进行同等测试、科学统计、客观评定，过程无任何主观因素及人为干预。

该《白皮书》代表测试单位区块链安全研究中心观点，旨在表明某一家加密数字钱包信息安全综合情况，代表相关各平台在信息安全方面的综合实力，不体现平台的盈利能力等其它特性，仅供读者参考。相关机构或者用户须根据情况自行判断。测试单位力求在《白皮书》中提供信息的完整和准确性，但是并不对此作任何形式的保证。《白皮书》中提供的数据、观点、文字等信息不构成任何法律证据，不代表官方机构意见。《白皮书》中所涉及的相关排名，均仅限于本次测试的对象范围。如果《白皮书》中的研究对象发生变化，测试单位将不另行通知。对《白皮书》数据有异议，可以联系联合发布单位（中国区块链应用研究中心、杭州加密谷区块链科技有限公司、上海淳粹文化传媒有限公司）。

未获得测试单位的书面授权，任何人不得对本白皮书进行任何形式

的有悖原意的删节和修改。如引用、刊发，需注明出处为本次白皮书测试及联合发布单位（上海交通大学网络空间安全学院、中国信息通信研究院泰尔终端实验室、上海掌御信息科技有限公司、中国区块链应用研究中心、杭州加密谷区块链科技有限公司、上海淳粹文化传媒有限公司）。

该《白皮书》是测试单位根据公开可查的数据，依据专业模型和算法，通过公平、严谨的测试、计算和分析得出的研究成果，不收取任何费用，不涉及任何商业行为。

测试单位在该《白皮书》发布后，将继续跟进其内容中所涉及的各个加密数字钱包 APP，并持续关注加密数字钱包行业的信息安全问题，定期出具相关分析报告。如需获取更加专业、详细的报告内容，请联系联合发布单位（中国区块链应用研究中心、杭州加密谷区块链科技有限公司、上海淳粹文化传媒有限公司）。

请任何人员不要咨询相关收费问题！如果有人冒充测试或联合发布单位工作人员借检测、评级或排名等事项向各加密数字钱包平台骗取钱财，请及时向此《白皮书》的联合发布单位（中国区块链应用研究中心、杭州加密谷区块链科技有限公司、上海淳粹文化传媒有限公司）进行举报。

目录

关键字

APP：这里是指 Android 系统中运行的手机软件。

加密数字钱包：加密数字钱包是专门用来管理基于区块链技术的数字资产的应用,提供钱包地址的创建、加密数字货币转账、每个钱包地址交易历史的查询等基础金融功能。

静态检测：在不运行软件的情况下，利用 JEB，APKTOOL 等工具对手机软件的源代码或二进制代码进行语法语义的理解，从而进行安全性分析。

动态检测：通过实际运行软件，记录运行相关信息，收集运行结果，来测试手机软件的安全性。

漏洞：手机软件的代码或协议等方面的具体实现存在安全性的缺陷，而这些缺陷可能导致攻击者在未授权的情况下访问软件或系统的敏感数据，或破坏软件及系统。

风险：手机软件的代码或协议等方面的具体实现存在安全性的不足，这些不足会大大增加软件本身或系统被攻击的可能。

ADB：Android Debug Bridge，一种 Android 的调试工具，可以连接 Android 设备和 PC 端。

Webview：Android sdk 自带的功能性组件，用来加载一个网页。

Webview 漏洞：由于 Webview 对其加载的 JS 代码校验不足，导致某些加载的恶意 JS 代码可以利用软件本身的权限来执行恶意行为。

组件：Android 应用程序由一些零散的有联系的组件组成，通过一个工程 manifest 绑定在一起。组件包括 activity，service，receiver，provider 等。

组件暴露：在非开发人员有意的前提下，APP 的组件接口可以被其他 APP 非法调用，可能会导致 APP 敏感数据泄漏，功能泄漏，数据污染等安全问题。

密码学误用：由于开发人员对密码学相关知识的匮乏，错误的使用了安全性不足的加密算法或将密码，IV 等信息硬编码在了代码中，使得加密失去了保护数据的效果。

加壳：APP 对代码自我保护的方法。将原有的代码加密保存，当 APP 首先运行“壳”程序，再释放并解密保护的代码。加壳可以有效防止攻击者对代码的静态分析。

混淆：APP 对代码中出现的类名，变量名，方法名进行替换，将原来有实际意义的名称替换为无意义的名称，来隐藏原代码中各类名称透露的信息，大大增加了攻击者对代码的静态分析的难度。

风险范围：在本次检测过程中，所提及的安全风险影响的全体 APP 的比例。

哈希值：APP 可执行文件的数字指纹，可用于唯一确定一个 APP 身份。

一、 背景

为促进区块链产业的发展、响应国家区块链行业政策，区块链安全研究中心（由上海交通大学网络空间安全学院、中国信息通信研究院泰尔终端实验室、上海掌御信息科技有限公司联合成立）对2018年主流的14个加密数字钱包Android移动应用进行信息安全评估。本次评估遵循客观、全面、专业原则，每一个测试样本皆经过严格的安全评估流程。本次评估历时30天（2018年10月15日至11月14日），共计投入11名资深移动应用与安全专家（其中上海交通大学网络空间安全学院4人、中国信息通信研究院泰尔终端实验室3人、上海掌御信息科技有限公司4人）。

1. 目的

2017年是加密数字货币的爆发之年——比特币涨幅近13倍,很多人认为，加密数字货币是金融行业中最大的革命力量之一。但与此同时，作为金融领域中最具争议的话题，也有不少人抨击比特币背后毫无支撑，是彻头彻尾的泡沫。

毋庸置疑的是，比特币的崛起和上涨，引发了全球对加密数字货币未来前景的关注和期待。2018年，加密数字货币将有希望迎来重大转折。在当下加密货币的发展探索中，安全存储是最为关键的一环，是决定其健康可持续发展的基石。因此，打造安全可靠的数字货币钱包作为数字资产的存储地是至关重要的。

实际上加密数字钱包APP的井喷式发展并没有充分考虑对于相关信息安全的保护。在满足了便捷性和功能性的需求后，加密数字钱包APP的安全性又如何？ 目前行业内大部分为客户提供加密数字钱包的APP都缺少规范的安全监管标准和流程，许多APP缺乏对其代码和业务逻辑的充分安全性测试，导致其包含的安全漏洞会将重要的数据信息暴露给黑客，将使用该应用的客户置于风险之中。基于对区块链技术的深度探索与挖掘、在安全领域多年积

攒的经验和认知，区块链安全研究中心（由上海交通大学网络空间安全学院、中国信息通信研究院泰尔终端实验室、上海掌御信息科技有限公司联合成立）采用公开、合法的信息，运用相应的科学研究方法，对当前加密数字钱包行业相关 Android 移动应用（APP）做出的信息安全分析评判，推出《加密数字钱包 APP 信息安全现状白皮书》，主要目的是分析评估当前加密数字钱包 APP 中存在的典型信息安全问题和风险，并对其中存在的高风险进行预警。

2. 检测机构介绍

区块链安全研究中心 BSRC 由上海掌御信息科技有限公司与上海交通大学网络网络空间安全学院、中国信息通信研究院泰尔终端实验室共同组建。BSRC 致力于区块链安全领域的基础研究，开展包括但不限于区块链安全技术研发、安全行业标准制定、区块链应用场景安全研究、区块链金融应用合规性研究等工作。

2.1 上海交通大学网络空间安全学院

上海交通大学网络空间安全学院（原信息安全工程学院），是由国家教育部、科技部、上海市政府和上海交通大学共同建设的国内首家学院建制的国家信息安全专业人才培养基地，拥有一支包括教授、副教授、兼职教授等 60 余名青年骨干教师和 200 多名博士、硕士研究生构成的高水平科研学术团队，先后承担了 300 余项国家重要科研项目及横向项目，取得了包括国家科技进步二等奖等一系列重要科研成果，并参与国家一系列重要的信息安全标准制定和法规建设等。

2.2 中国信息通信研究院泰尔终端实验室

中国泰尔实验室(CTTL)始建于 1981 年，行政隶属于工业和信息化部中国信息通信研究院(CAICT)，由工业和信息化部和国家质量监督检验检疫总局

授权设立。实验室经历了不断的发展和融合，现在的实验室是由工业和信息化部中国信息通信研究院所属的电信传输研究所、通信计量中心、邮电工业标准化研究所和保定泰尔通信设备抗震研究所通过业务重组和资源整合而组成的。中国泰尔实验室是集信息通信技术发展研究，信息通信产品标准、测试方法、通信计量标准、计量方法研究，国内外产品的测试、验证、技术评估、测试仪表计量、通信软件的评估、验证为一体的高科技组织。

2.3 上海掌御信息科技有限公司

上海掌御信息科技有限公司是专业的区块链安全服务提供商，由国际顶尖的白帽子技术团队和密码学博士组成，曾是银联云闪付底层白盒密码引擎的技术供应商，也参与了多个国家标准和行业标准的制定，并与工信部中国泰尔终端实验室、上海交通大学网络空间安全学院共同成立了区块链安全研究中心，致力于区块链基础链、智能合约、应用客户端的黑盒安全测试和白盒代码审计，同时也提供加密数字热钱包和冷钱包的底层安全解决方案和身份验证方案。

3. 联合发布单位介绍

3.1 中国区块链应用研究中心

中国区块链应用研究中心是公益机构，由互联网金融博物馆联合部分区块链业界的领袖机构成立，其宗旨是与监管机构密切合作，共同推动区块链行业的培训认证和规范发展，鼓励区块链在实体经济中的场景应用，防范金融风险，促进中国区块链业界与全球同行的交流，建立行业规则。

3.2 杭州加密谷区块链科技有限公司

杭州加密谷区块链科技有限公司加密谷 Live（CryptoValley Live）是具有全球视野的区块链新媒体品牌，关注全球加密经济产业趋势，以图文、视

频、直播、会议等形式报道全球区块链前沿资讯与深度思考。加密谷在瑞士楚格、旧金山、上海、香港、东京均设有记者站，运营中心设立在上海。

3.3 上海淳粹文化传媒有限公司

上海淳粹文化传媒有限公司（简称：淳粹传媒）以数据为基础，以知识为核心，以媒介为渠道，借助数知媒外部数据集成服务平台和资源管理系统，通过数据应用和资源整合为客户提供核心人物 IP 打造、风险与危机管理等整体解决方案。

二、 加密数字钱包 APP 信息安全现状

1. 评分综述

为了检验加密数字钱包 APP 的安全现状，本次报告针对当前 Android 平台上 14 款主流的加密数字钱包 APP 客户端软件进行了一次全面的安全性测评。从测试结果可以看出，目前加密数字钱包 APP 的整体信息安全性并不高，每个 APP 都存在不同程度的信息安全问题。其中普遍存在的问题集中在加密算法的误用、网络传输保护不足、应用程序缺乏保护措施、本地文件及系统日志敏感信息泄漏等几个方面。除此之外，个别 APP 还存在组件暴露漏洞、可数据备份漏洞、Webview 远程执行漏洞、拒绝服务攻击漏洞、网络接口攻击漏洞等等其他安全问题。由此可见，加密数字钱包 APP 的安全性严重不足，急需增强安全保护措施。根据 APP 私钥存储机制的不同，我们将测试的 APP 分成 2 类：去中心化数字加密钱包 APP 和中心化数字加密钱包 APP，其私钥分别存储在 APP 本地和中心服务器。

1. 去中心化数字加密钱包 APP 评分维度（根据如下结果维度来评分）：

a) 私钥使用安全；

b) 私钥传输安全；

c) 私钥存储安全；

d) 运行环境安全；

e) 用户账户安全。

2. 中心化数字加密钱包 APP 评分维度（根据如下结果维度来评分）：

a) 私钥使用安全；

b) 数据传输安全；

c) 数据存储安全；

d) 密码算法协议安全；

e) APP 代码保护强度

f) 泄漏信息敏感程度。

具体分值：根据评分维度综合得出。

说明：各项评分越低，代表安全性越不足。最高 100 分，最低 10 分。单个 APP 最后总分根据 5 个维度得分相加后除以 5 得到。

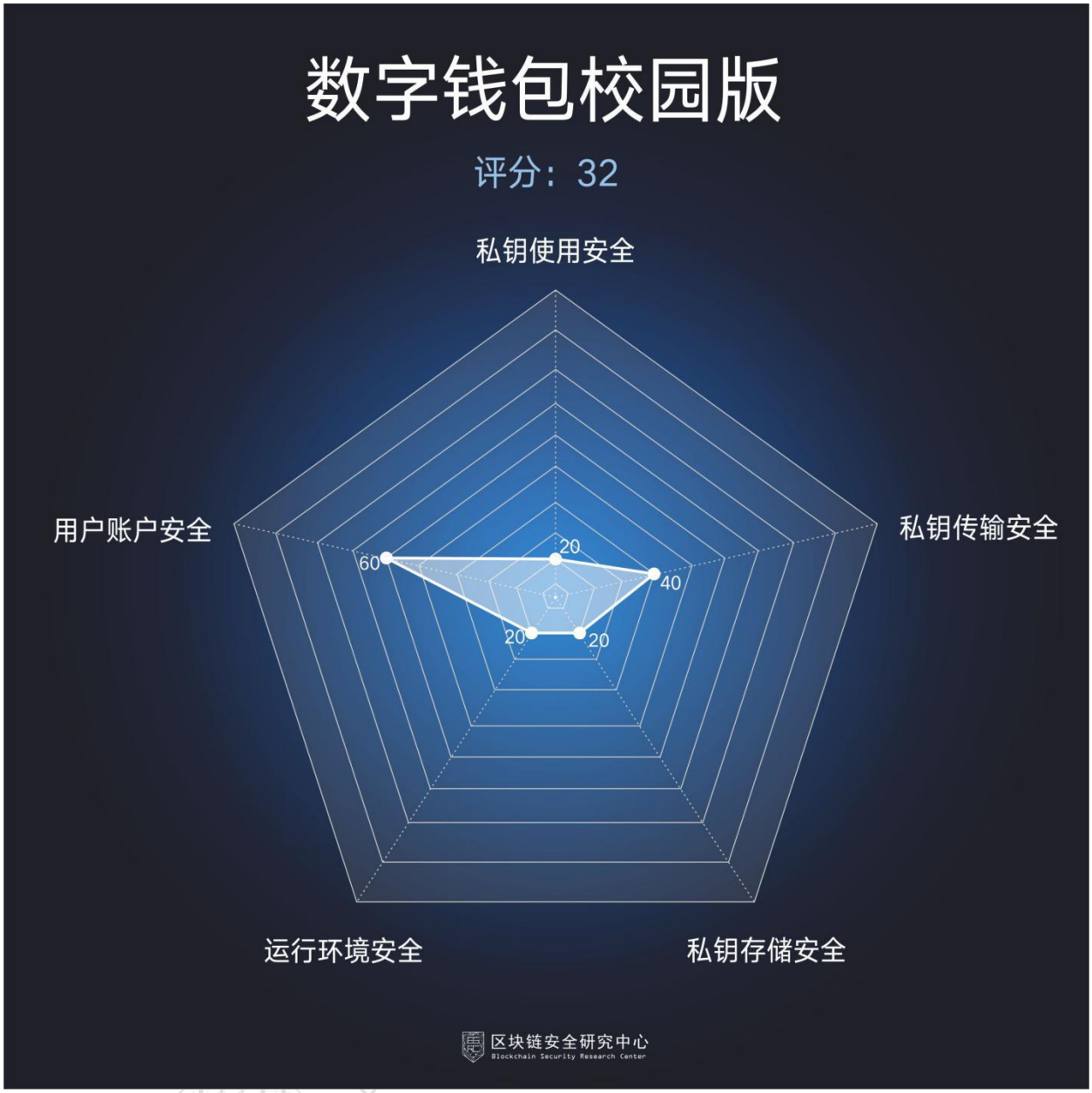
2. 去中心化加密数字钱包 APP 测试结果

2.1. 数字钱包校园版

包名：cn.jointcenter.wallet

版本：v1.0.4

评分：32



点评：

该 APP 安全性严重不足，体现在如下方面：作为加密数字钱包 APP，对于钱包私钥的保护力度不足。在私钥使用方面，APP 没有利用助记词来生成私钥并辅助记忆，而是直接生成私钥，这样导致私钥不得不在本地进行存储，增加了泄漏风险。在私钥传输方面，私钥会以明文的形式在网络上传输，很容易被攻击者窃取。在私钥存储方面，APP 直接将其明文存储在本地，同样存在极大泄漏风险。在用户帐户安全方面，虽然 APP 采用了 HTTPS 协议进行数据传输，但由于缺乏证书绑定，使得攻击者在替换手机证书的情况下，依然可

以中间人攻击。APP 并没有对业务数据进行加密保护，用户账户密码都以明文形式传输，这使得账户安全大大降低。在运行环境安全方面，APP 没有采用加壳保护，同时缺少模拟器及 ROOT 环境检测，这使得运行环境也存在安全威胁。

网络数据包举例（敏感信息明文传输）：

本地文件举例（钱包私钥明文存储）：

```
dreamlte:/data/data/cn.jointcenter.wallet/shared_prefs # cat secret_Info.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="address">11118pLYZoafLM8u6ikn3gnx9v4jjVATnQbf6VT2k1qg7ZXU</string>
    <int name="min_amount" value="5000" />
    <boolean name="has_pws" value="false" />
    <string name="pub">-----BEGIN PUBLIC KEY-----&#10;MFkwEwYHKoZIzj0CAQYIKoEcz1UBgi0DQgAE/zH1fGLmPw5cNDSx3+i0k6dM6Ole&#10;JskdUxQkcK03HAn9KqGYQsOWDhgZAEFWmEPIeblPvtcpqH2Zjz2ELL5zmA==&#10;-----END PUBLIC KEY-----</string>
    <string name="pri">-----BEGIN PRIVATE KEY-----&#10;MIGHAgEAMBMGByqGSM49AgEGCCqBHM9VAYItBG0wawIBAQQgHSuBUKJFN4QZo3DP&#10;EirZpTF9Q650AOY8883cPaRLlt6hRANCAAT/MfV8YuY/Dlw0NLHf6LSTp0zo6V4m&#10;yR1TFCRwrTccCf0qoZhCw5YOGBkAQVaYQ8h5uU++1ymofZmPPYQsvnOY&#10;-----END PRIVATE KEY-----</string>
    <boolean name="has_pay_pws" value="false" />
    <string name="mobile">13162525243</string>
</map>
```

2.2. JAXX

包名：com.kryptokit.jaxx

版本：v1.3.18

评分：40

点评：

该 APP 安全性严重不足，体现在如下方面：作为加密数字钱包 APP，对于钱包私钥的保护力度不足。在私钥使用方面，App 在每次启动的时候都会从位于 App 私有目录下的数据库文件中读取用户钱包账户的助记词，将其转化为用户钱包账户的 Seed，该信息在整个 App 生命周期中会一直残留在内存中，即时使用结束后仍无法得到回收，攻击者可以通过内存搜索的方式获取该 Seed。而在用户导入、生成助记词的界面，App 也未做相应的防截屏防护。在私钥存储方面，该 App 未遵从数字货币钱包的标准实现，而是简单地使用密

钥固定的 AES 算法对助记词进行加密后保存在本地，存在极大泄漏风险。在用户帐户安全方面，虽然该 App 采用了 HTTPS 协议进行数据传输且对 HTTPS 证书进行了校验，但它没有对证书进行绑定，仍存在中间人攻击的可能，这使得账户安全大大降低。在运行环境安全方面，该 App 未做加壳、混淆处理，主要逻辑均用 javascript 实现并保存在 assets 目录下，同时缺乏执行环境检测和重打包检测，攻击者可以相对轻松地查看 App 代码逻辑。

助记词加密代码截图：

源码目录：assets\jsdist\com\Utils2.js

```
Utils2.getSeedHex = function () {
    if (!Utils2.seedHex)
        Utils2.seedHex = thirdparty.bip39.mnemonicToSeedHex(getStoredData('mnemonic',
true));
    return Utils2.seedHex;
};
```

源码目录：assets\js\utils\cacheUtils.js

```
function getStoredData(key,decrypt){
    if(typeof key !== 'undefined'){
        var value ;
        value = window.localStorage.getItem(key);
        value = (decrypt == true) ? decryptSimple(value) : value;
        return value;
    }
}
```

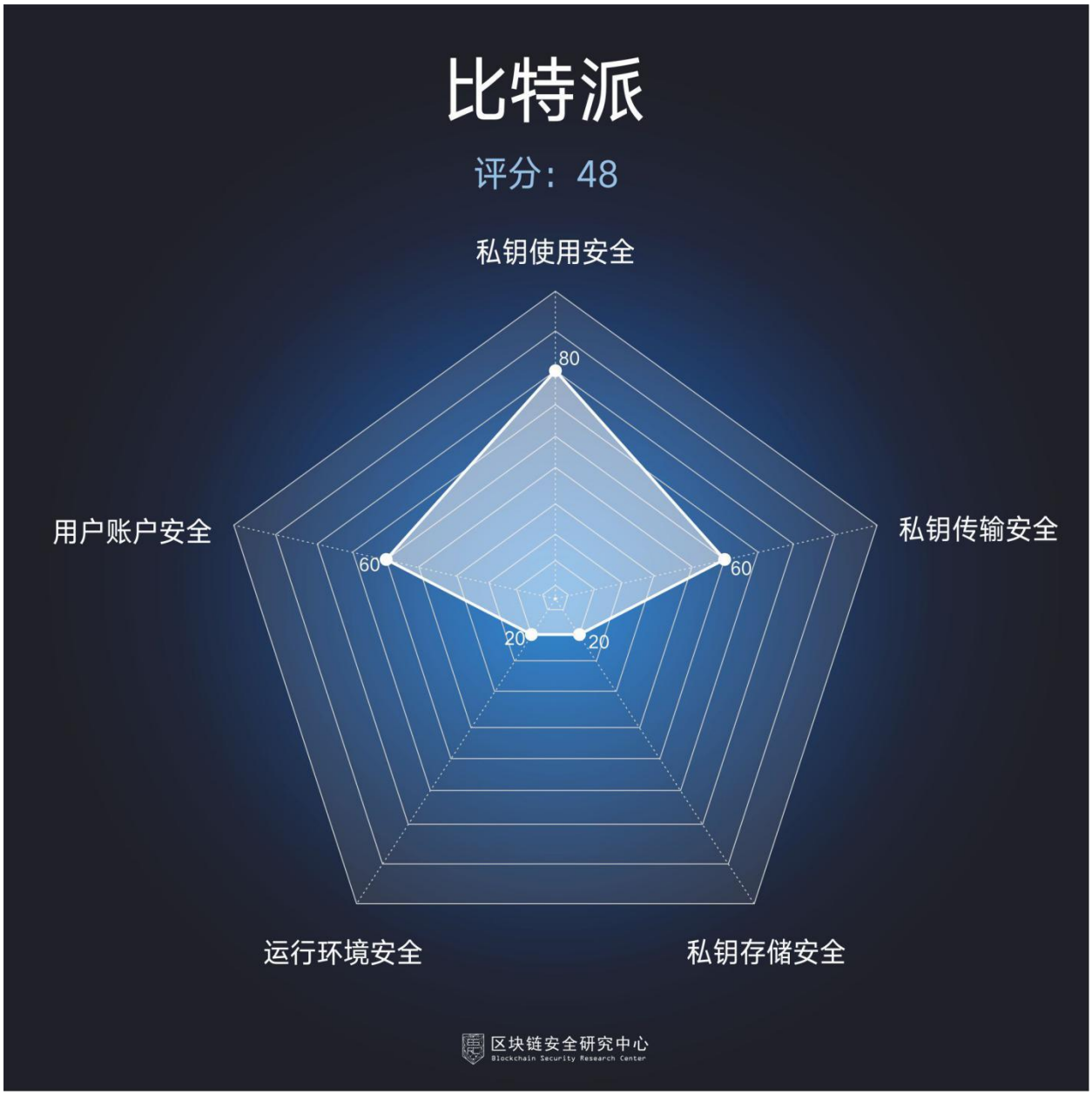
```
var key = "6Le0DgMTAAAAANokdfEial"; //length=22
var iv  = "mHGFxENnZLbienLyALoi.e"; //length=22
var keyB;
var ivB;
function decryptSimple(encryptedTxt) {
    keyB = thirdparty.CryptoJS.enc.Base64.parse(key);
    ivB = thirdparty.CryptoJS.enc.Base64.parse(iv);
    var decrypted = thirdparty.CryptoJS.AES.decrypt(encryptedTxt, keyB, { iv: ivB });
    var decryptedText = decrypted.toString(thirdparty.CryptoJS.enc.Utf8);
    return decryptedText;
}
```

2.3. 比特派

包名：com.bitpie

版本：v3.6.6

评分：48



点评：

该 APP 安全性严重不足，体现在如下方面：作为加密数字钱包 APP，对于钱包私钥的保护力度不足。在私钥存储方面，App 将用于生成助记词的种子不经加密直接存储在本地 SharedPreference 文件中，攻击者获取后可以恢复出助记词，进而取得钱包私钥。在用户帐户安全方面，虽然 APP 采用了 HTTPS 协议进行数据传输且对 HTTPS 证书进行了校验，但没有对证书进行绑定。攻

击者在替换手机证书的情况下，依然可以进行中间人攻击。同时，对于 PIN 密码的存储，App 选择了 Java 提供的 HashCode 接口，安全性也存在很大不足，这使得账户安全大大降低。在运行环境安全方面，APP 缺乏混淆，加壳等保护措施，也缺乏重打包检测，在 ROOT 设备、模拟器环境下均可正常运行，因而攻击者可以轻易对 APP 代码进行逆向分析。

网络数据包举例（敏感信息如用户名、密码等明文传输）：


```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Tue, 30 Oct 2018 02:47:13 GMT
Content-Type: application/json; charset=UTF-8
Content-Length: 728
Connection: close

{"btf_split": 1, "lch_split": 1, "addresses": [{"address_type": 0, "receiving_index": 0, "address": "15thZyF56WPJERzfT1CyWkDTYJjYw8nAsj"},
{"address_type": 2, "receiving_index": 0, "address": "3ACDdAmRwJwMpQz7HjnedTbQFdYZu2RVnn"}], "address":
"15thZyF56WPJERzfT1CyWkDTYJjYw8nAsj", "btg_split": 1, "btvnew_split": 1, "lbtc_split": 1, "user_id": 1578466, "cdy_split": 1, "btp_split": 1,
"default_bank_card_id": null, "receiving_index": 0, "god_split": 1, "bifi_split": 1, "user_name": "noname-819411414427", "safe_split": 1, "bcc_split":
1, "sbtc_split": 1, "bcx_split": 1, "bpa_split": 1, "btv_split": 1, "token": "1b4acb017c8b2194c6174a5fe82645e1dc039aacf1ec264af36df083adc07b29",
"bbc_split": 1, "bcd_split": 1, "btw_split": 1}
```


本地文件举例（敏感信息如助记词种子，登录 token、手势密码等明文存储）：


```
<boolean name="languageExSupport" value="true" />
<int name="orderPledgeEnough" value="0" />
<string name="exOtcCoinCode">BTC,ETH,ETH-EOS,BCC,OMNI-BTC-USDT,LTC,ETC,BTG,SBTC,BTN-NEW</string>
<int name="precision" value="0" />
<string name="pinCodeType">sixDigit</string>
<int name="userId" value="1578518" />
<string name="token">9cc28cbe14b32f7f25cadc35117a86c87f3ed06d3eb4bb7be2d4ee326435cf6a</string>
<string name="pinCode">-1031087265;695786889</string>
<boolean name="agreeTermsOfService" value="true" />
<string name="bip39Language">en</string>
<int name="defaultBankCardId" value="0" />
<int name="vipPledgeEnough" value="0" />
<string name="addresses">12t8L1CnxsP4WEBx5YQimJAiRp1MWovZF6,0,0&amp;3MtxztZyYuc5hHagizchASMEG9aA7dCQWV,2,0</string>
<string name="userAddress">12t8L1CnxsP4WEBx5YQimJAiRp1MWovZF6</string>
<int name="receivingAddressIndex" value="0" />
<int name="defaultAddressType" value="0" />
<long name="userBalance" value="0" />
<string name="fullnodeUrl">47.88.174.175:50051</string>
<int name="txAcceleratorCnt" value="0" />
<string name="userName">noname-539768059081</string>
<int name="kycLevel" value="0" />
<boolean name="updateAddressDataBase" value="true" />
<int name="notificationIdHandled" value="6808960" />
<string name="instantCoinCodes">{&quot;instantCoins&quot;:[{&quot;coinCode&quot;:&quot;BTC&quot;,&quot;supportPieBank
ETH&quot;,&quot;supportPieBank&quot;:0},{&quot;coinCode&quot;:&quot;EOS-EOS&quot;,&quot;supportPieBank&quot;:0},{&quot;c
ot;supportPieBank&quot;:1},{&quot;coinCode&quot;:&quot;OMNI-BTC-USDT&quot;,&quot;supportPieBank&quot;:1}]}</string>
<string name="solidityNodeUrl">39.105.66.80:50051</string>
<boolean name="openPieStore" value="true" />
<string name="seed">119cbb362094b5ad83a3f74c1c361287db14b908f87b1d8852f437cfb6fd31a7d131a850d14cf5ad8e0565b8e3bb750a0
g>
<boolean name="otcOnlineStatus" value="false" />
<boolean name="seedPhraseEntropyWritten" value="false" />
<int name="price" value="4431284" />
<int name="userGender" value="0" />
<string name="seedPhraseEntropy">2ffe6090c0dc9a684ad865f75eaceccf</string>
<boolean name="otcVipNotice" value="false" />
<boolean name="seedPhraseWrittenAgain" value="false" />
<int name="canPledegeVip" value="0" />
```

2.4. Kcash

包名：com.kcashpro.wallet

版本：v2.5.0

评分：64

点评：

该 APP 安全性存在不足，体现在如下方面：作为加密数字钱包 APP，对于钱包私钥的保护力度不足。在私钥使用方面，在用户导入、生成助记词的界面，App 也未做相应的防截屏防护。在私钥存储方面，虽然使用用户输入的口

令作为加密私钥的种子，但实现中并未遵循数字货币钱包标准，仅仅将用户口令做两次 SHA512 变换（未加盐）后便存储在本地。而用户口令由六位数字构成，因而攻击者获取到哈希后的口令后可以通过暴力破解的方式得到用户输入的口令,从而取得钱包的控制权。在用户帐户安全方面,该 App 未做 HTTPS 证书校验，攻击者可以相对轻松地对通信消息进行监听和篡改，这使得账户安全大大降低。在运行环境安全方面，虽然 App 在 ROOT、模拟器环境下均可正常运行，但同时 App 对代码进行了加壳、混淆操作，也做了重打包检测，因此攻击者逆向代码的难度相对较大。

本地存储的口令哈希等信息：


```
- <map>
    <string name="sha_password_6299b4a67eb7bbf76ad4d47ee2c46a9caee69107a0818b2f">
        3c2a6eb64cc629de76c419308830c53bbe63b874f6a526f7cd784182b33a2f5f3daaab47b5bde5868b82e4dd3b521d147a7542292b689acdf60122b97e99523f</string>
    <string name="sha_password_526c41c120321e057ea6471b5557c0f558493c7d65686fcf">
        3c2a6eb64cc629de76c419308830c53bbe63b874f6a526f7cd784182b33a2f5f3daaab47b5bde5868b82e4dd3b521d147a7542292b689acdf60122b97e99523f</string>
    <string name="sha_password_44a210156ed988ac7980098828e6e8a82e723a5ec64164bb">
        3c2a6eb64cc629de76c419308830c53bbe63b874f6a526f7cd784182b33a2f5f3daaab47b5bde5868b82e4dd3b521d147a7542292b689acdf60122b97e99523f</string>
    <string name="key_wallet_id_list">
        ["44a210156ed988ac7980098828e6e8a82e723a5ec64164bb","6299b4a67eb7bbf76ad4d47ee2c46a9caee69107a0818b2f","526c41c120321e057ea6471b5557c0f558493c7d65686fcf"]</string>
    <string name="key_curr_wallet_id">526c41c120321e057ea6471b5557c0f558493c7d65686fcf</string>
    <string name="526c41c120321e057ea6471b5557c0f558493c7d65686fcf">{"actAddress":"ACTFfKFaw2SigZ7cCyKpEhbiQRaMUX4QChQr","bchAddress":"1KMjvrxg2tRp3pCXZk2fT7eN34eEFxi2Mo",
        "btcAddress":"1NTrJsrUh5sRHqHipwHUfw6jK9uETSG5fb","createTime":0,"eosAddress":"EOS77hWydkSawRfF2PXQmCr44cyd3i4qUyc4AcRNCeSbL2RVtoYBu",
        "etcAddress":"0xe37EC7dE9f504e4D83775a09eB0015eCd94D9946","ethAddress":"0x3f9FB9D715218a740Ddfaab2Ad4CfbdFC281dC37",
        "gxsAddress":"GXC76j3fzAhwKHmh1LjCyBnAmcBVWDwmznsunfSMhU5mBBgBRSZ3","id":"526c41c120321e057ea6471b5557c0f558493c7d65686fcf","isMnemonicNew":true,
        "ltcAddress":"LbqtE9Ety5sUjCFhK1Jbrpxcy12Ni7imvg","name":"Kcash-wall","needBackup":true,"tokenDBVersion":0,"type":"wallet_type_mult"}</string>
    <string name="44a210156ed988ac7980098828e6e8a82e723a5ec64164bb">{"actAddress":"ACTCeE5ormfBEmJDxgqYdsyJrRJygwvtYTbK","bchAddress":"1Cmn4seRKxGbJajnwYZCY5hFMDddN3d4rM",
        "btcAddress":"1NcJyKXnhsRVRk2NL9zAaCMVg9NXouycrx","createTime":0,"eosAddress":"EOS6DZ7N32RNA25dBnwsH1f4rjDy197KPHKg4r7FSZ7GrTTrmFpiP",
        "etcAddress":"0xB7661EeAD04339E463621bB73A043E44c30BE9c9","ethAddress":"0xD346c117880A296e5CfE1BDaB1efeC2b4299E7E8",
        "gxsAddress":"GXCBJ56pGdqB6cxMXsbB4hVBdrDhnMbVZrXEBiKnTYUBjovGPCxV3","id":"44a210156ed988ac7980098828e6e8a82e723a5ec64164bb","isMnemonicNew":true,
        "ltcAddress":"LPfs8eKtPtJT9anzVM8BcNxdbLdpQCyo84","name":"Kcash-wallet","needBackup":false,"tokenDBVersion":232,"type":"wallet_type_mult"}</string>
    <string name="6299b4a67eb7bbf76ad4d47ee2c46a9caee69107a0818b2f">{"actAddress":"ACT56yhfYS5g4Qqx9PvY3sgR7FBqqwHb5NZ3","bchAddress":"151TyHJweNY7Q2y7H9yY5qc4CKcVjcAihW",
        "btcAddress":"1424QZmPpE4p4rWiBG58YkaicHpLJf2juh","createTime":0,"eosAddress":"EOS6aUxg8mKkGGMxkLUmBfYJi2GnuLqdfT7sTyDmfyURkQf8ZcJLw",
        "etcAddress":"0x7c649c1bBfC20ad43ba7c80ba6cB508811304AC7","ethAddress":"0x62B81f5cD8e8d52eD6c4781239FBB16a46BC0F94",
        "gxsAddress":"GXC7SkShDuEsNAVsujsVbCHEVD6Pv58SXf9hK7NzYzfpryr7ESvLF","id":"6299b4a67eb7bbf76ad4d47ee2c46a9caee69107a0818b2f","isMnemonicNew":true,
        "ltcAddress":"LdbAquYJhBoFD9wRbWVpEidiWXw2rxDBvk","name":"Kcash2","needBackup":false,"tokenDBVersion":0,"type":"wallet_type_mult"}</string>
    <string name="encrypt_mnemonic_526c41c120321e057ea6471b5557c0f558493c7d65686fcf">
        {"ciphertext":"96dcaab9465c726585e563744bd8ce8a27df4b14897ec717ad6c8ff6cc86418a9ea93e6a4705b02eb20740da9f8fbf56511ef3c3351d6dfec24a9078afb714b30a7bf82487024ae57225dadf",
        "iv":"4eecd65a107bf03796d3759235d584a1","mac":"086676196741748O3a05459189413fa7204616d08cb78f0535b5ad31c3e7492c",
        "salt":"bf6885a8d2771d723b89a5b7376c435af29ea21468576f96458c5d0bcdd28b31"}</string>
    <string name="encrypt_mnemonic_6299b4a67eb7bbf76ad4d47ee2c46a9caee69107a0818b2f">
        {"ciphertext":"050ab81206Ib3a51f39a5674ef21abf01c146607c815bcf4903cf3216529ae96e0fc4c60322df1bfd0608e4cf01408800cd99450dbed1b15c7a161e19123350aea772a0dbabc39b0825a37fa3a3a84155f",
        "iv":"88410fc4665ddd00a5a1ac55d44ef0d9","mac":"30decd2c609ad5a3ac89bb7536d00b7ec5d6bd0481a7ddcc227f00054b51e0dd4",
        "salt":"6319a621b4764f42b40a8fa55bdc39e5189623b9cb9e93f2a11d900758f30395"}</string>
    <string name="encrypt_mnemonic_44a210156ed988ac7980098828e6e8a82e723a5ec64164bb">
        {"ciphertext":"3ea8b06c0fb7b5c2986a80fed6d9f766f76ffc531aedc3fa662364ecd94b2818b32f018f73ff757d0603f6df6935fd9e1e4c960397fb8a192833ba65c43a57e0bf5ec19576d0bcdcc4dd28846b23e0724bdcba",
        "iv":"ebdf6d465d698c521cefef0db116581Z","mac":"684f6ef823167ab76538a760a220dc24a1494f6a0e210e2d72cabd34e2d7008",
        "salt":"75af23e306a90cd71e7077ae7617387e9220a18068a8ada5fb421cf2842d12b6"}</string>
</map>
```


网络通信截图（敏感信息如手机号等遭到泄露）：

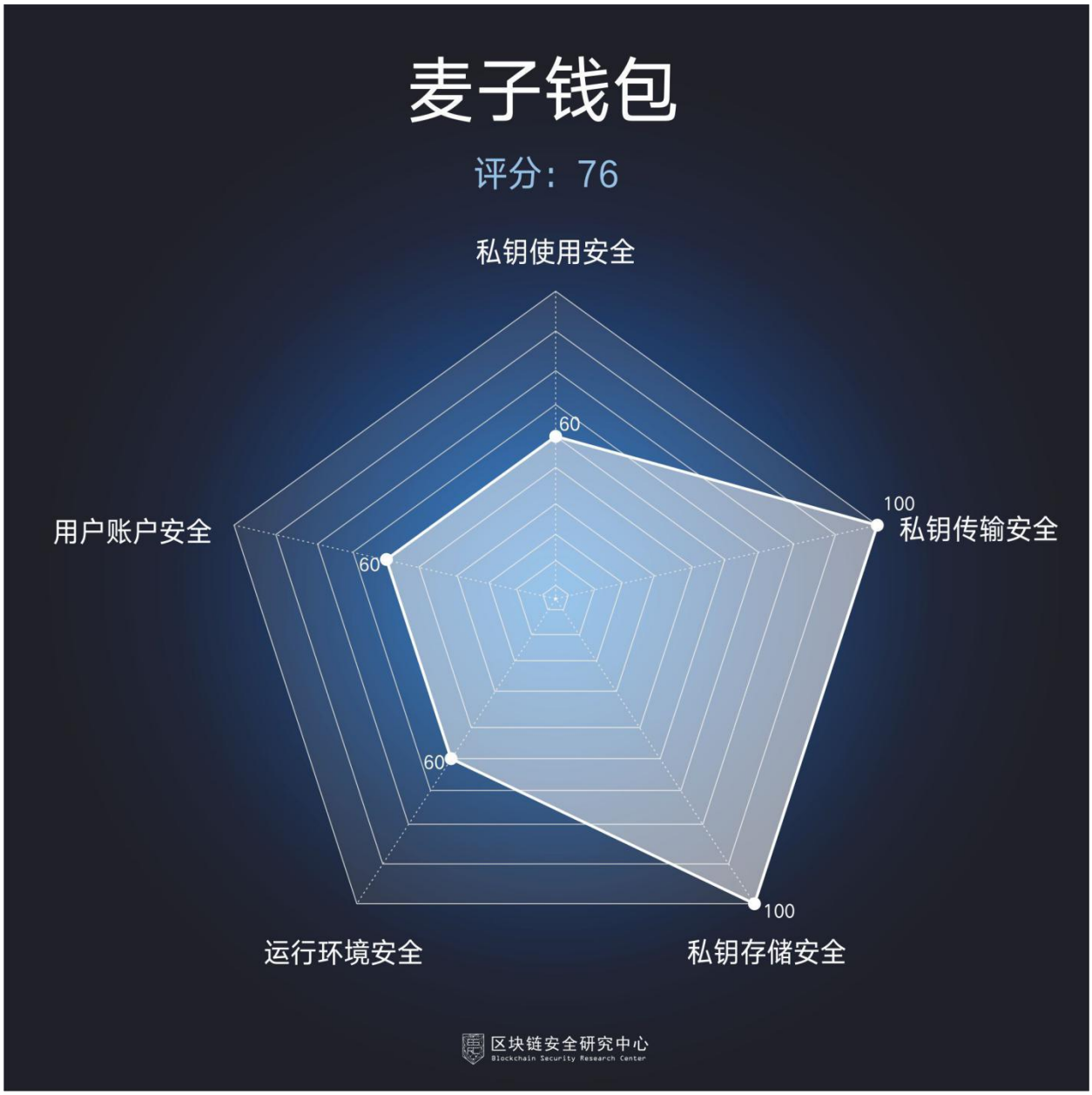
```
POST /user/loginOrRegister HTTP/1.1
kcash-versioncode: 50
kcash-versionname: 2.5.0
kcash-client: android
kcash-channel: UPDATE
kcash-language: zh
Content-Type: application/json; charset=utf-8
Content-Length: 120
Host: api2.kcash.com
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.9.0

{"phone":"18780013533","uid":"2711203991ea9b1297911c746221eb7c26f126c344c80c8c","verifyCode":"91813","countryCode":"86"}
```

2.5. 麦子钱包

包名：com.medishares.android

版本：v1.8.1

评分：76



点评：

该 APP 安全性存在不足，体现在如下方面：作为加密数字钱包 APP，对于钱包私钥的保护较好。在私钥使用方面，APP 私钥通过用户设置的钱包密码产生的助记词来生成。钱包的导入，使用都需要通过助记词。但在用户导入、生成助记词的界面，App 未做相应的防截屏防护。在私钥存储方面，App 依照数字货币钱包标准进行实现，相对安全。在用户帐户安全方面，虽然 APP 采

用了 HTTPS 协议进行数据传输且对 HTTPS 证书进行了校验，但没有对证书进行绑定，仍存在中间人攻击的可能，这使得账户安全大大降低。在运行环境安全方面，虽然 App 对代码进行了加壳、混淆操作，但 App 在 ROOT、模拟器环境下均可正常运行，同时没有进行重打包检测，攻击者获取、逆向代码的难度相对较小。

网络数据包举例（敏感信息如邮箱、Token 等泄露）

HTTP/1.1 200 OK
Date: Wed, 07 Nov 2018 09:50:45 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 351
Connection: close
X-Powered-By: PHP/7.1.8
Set-Cookie: PHPSESSID=iadusa20mtkeresq9ajh4i584k; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding

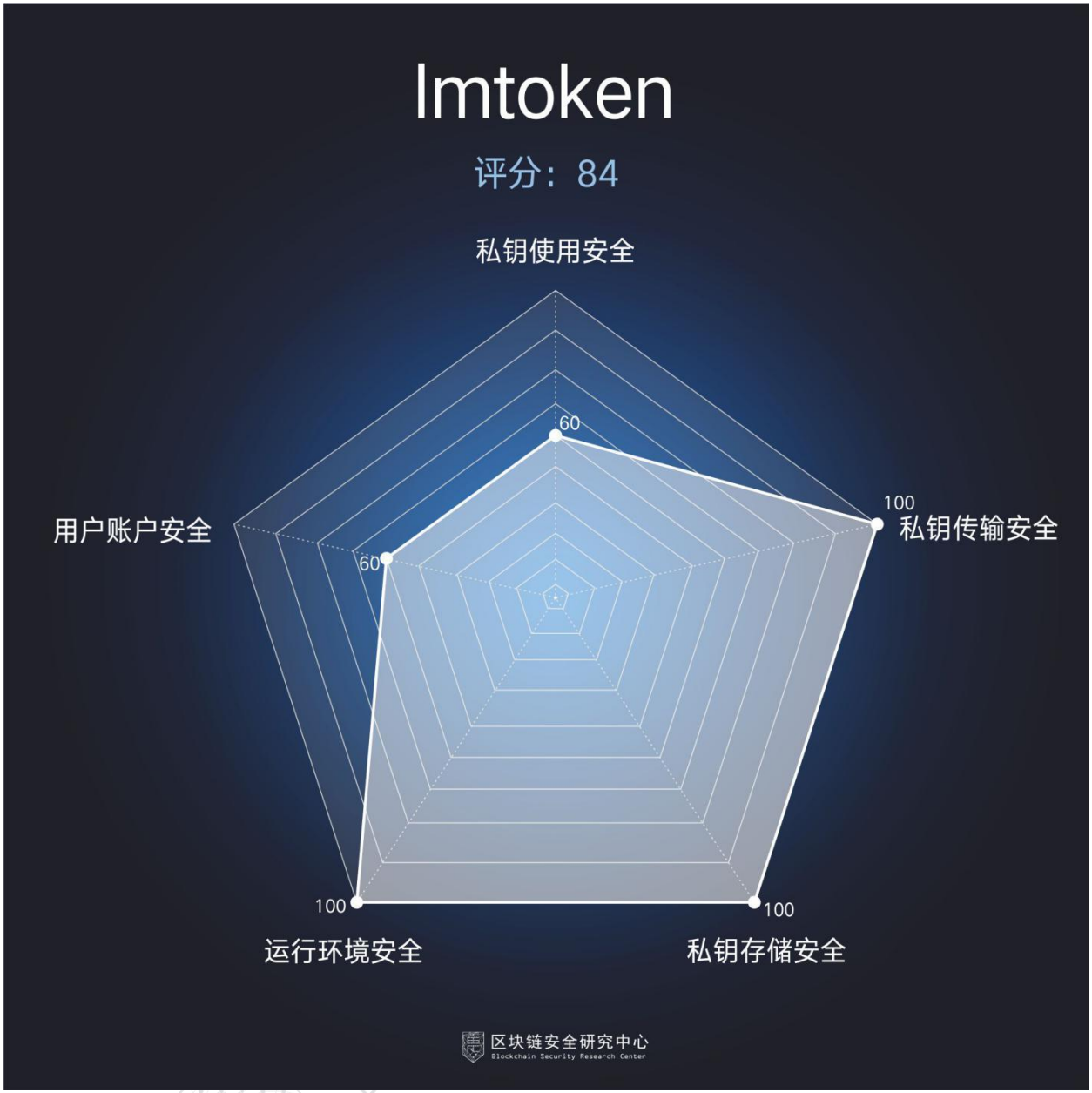
{"success":true,"data":{"accessToken":"NLUCMUNRY3XSFRNP74W3PE3AV42UNAA6VYUPGJTW7KTQLL798A6YHE554E2C6APU","u
serData":{"ID":"98827","uID":"UA1541584245","mobile":"","email":"837575715@qq.com","level":0,"name":"","nickname":"","country
":"","idCard":"","passport":"","driverLicense":"","workCard":"","isKyc":0,"headimg":"","bindAddress":[]}},"message":""}

2.6. Imtoken

包名：im.token.app

版本：v2.1.2

评分：84



点评：

该 APP 安全性较好，体现在如下方面：作为加密数字钱包 APP，对于钱包私钥的保护较好。在私钥使用方面，APP 私钥通过用户设置的钱包密码产生的助记词来生成。钱包的导入，使用都需要通过助记词。但在用户导入、生成助记词的界面，App 未做相应的防截屏防护。在私钥存储方面，App 依照数字货币钱包标准进行实现，相对安全。在用户帐户安全方面，虽然 APP 采用了 HTTPS 协议进行数据传输且对 HTTPS 证书进行了校验，但没有对证书进行绑定，仍存在中间人攻击的可能，这使得账户安全大大降低。在运行环境安全方面，

虽然 App 在 ROOT、模拟器环境下均可正常运行，但同时 App 对代码进行了加壳、混淆操作，也做了重打包检测，因此攻击者逆向代码的难度相对较大。

网络数据包举例：

```
POST /rpc HTTP/1.1
accept: application/json, text/plain, */*
authorization: Token null
x-identifier: im14x5UGM28AQYrDqm6WM9zE3ixo2DG3GPdgZP4
x-client-version: android:2.1.2.337:9
x-device-token: 229d6b5e4f9138a7
x-locale: zh-CN
x-currency: CNY
x-device-locale: zh-CN
x-api-key: 3bdc0a49ba634a8e8f3333f8e66e0b84
Content-Type: application/json; charset=utf-8
Content-Length: 270
Host: mainnet-auth.tokenlon.im
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.6.0

{"jsonrpc":"2.0","id":1,"method":"authService.auth","params":[1541586112,"im14x5UGM28AQYrDqm6WM9zE3ixo2DG3GPdgZP4","229d6b5e4f9
138a7","0xe1e235251a53387faf2eb783924c52c2048a083f3fc1978b8f45b0fbdbd198d15f1c90d32b28b08b667e88ccae94cff2358437d8bac6ae8
9611d6a0decf64ef11b"]}
```

3. 中心化加密数字钱包 APP 测试结果

3.1. LBank

包名：com.superchain.lbank

版本：v2.1.8

评分：24

点评：

该 APP 安全性严重不足，体现在如下方面：虽然 APP 采用了 HTTPS 协议进行数据传输，但由于缺乏证书校验，使得攻击者依然可以中间人攻击。同时，APP 并没有对业务数据进行加密保护，很多敏感数据（包括用户名，密码等）都以明文形式传输，用户面临较大隐私泄露甚至财产损失的风险。在代码保护方面，APP 缺乏混淆，加壳等保护措施，攻击者可以轻易对 APP 代码进行逆向分析。

网络数据包举例（用户名密码明文传输）：

```
POST /login HTTP/1.1
Host: mobile.lbkex.com
Connection: close
Content-Length: 69
Accept: application/json, text/javascript, */*; q=0.01
_uuid:
accept-language: zh-CN
User-Agent: Mozilla/5.0 (Linux; Android 6.0; Nexus 6P Build/MDB08K; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/68.0.3440
Origin: file://
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Encoding: gzip, deflate
Cookie: acw_tc=AQAAAOeXywvyIQYAYyd4yhMbdY+D+e6A
X-Requested-With: com.superchain.lbank

username=18780013533&password=hjskskskk&deviceNumber=1233132&source=2
```

3.2. OKEx

包名：com.okinc.okex

版本：v2.1.2

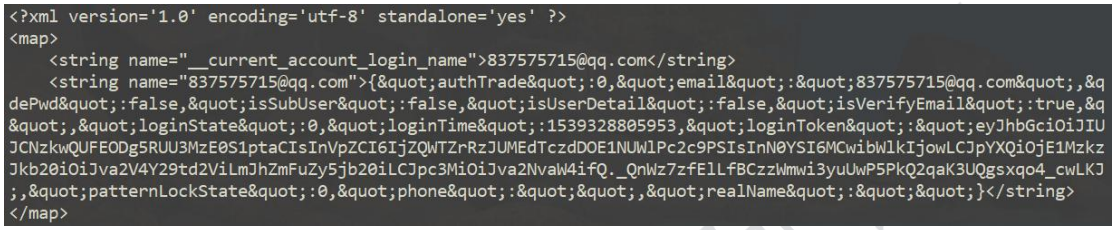
评分：26

点评：

该 APP 安全性严重不足，体现在如下方面：虽然 APP 采用了 HTTPS 协议进行数据传输且对 HTTPS 证书进行了校验，但没有对证书进行绑定。攻击者在替换手机证书的情况下，依然可以中间人攻击。而对于登录用户名、密码等敏感信息，APP 未进行加密操作直接进行传输，对于手势密码、登录 token、IMEI、UUID 等信息，APP 未进行加密操作便直接存储，因此用户面临较大隐私泄露甚至财产损失的风险。在代码保护方面，APP 虽然对代码进行了混淆，但并未进行加壳操作，也未做 ROOT 检测、反调试检测，攻击者可以轻易对 APP 代码进行逆向分析。

网络数据包举例（敏感信息如用户名、密码等明文传输）：

本地文件举例（敏感信息如登录 token、手势密码等明文存储）：



3.3. IDAX

包名：ex.com.exchange

版本：v1.2.8

评分：28

点评：

该 APP 安全性严重不足，体现在如下方面：虽然 APP 采用了 HTTPS 协议进行数据传输，但由于缺乏证书校验，攻击者依然可以进行中间人攻击。同时，APP 将登录密码、登录 token 等敏感信息明文存储在本地，并且在传输过程中未对敏感数据（用户名、密码等）进行任何加密措施，因此用户账号信息存在泄露的风险。在代码保护方面，APP 虽然做了加壳操作，并进行了重打包检测、模拟器环境检测，但并未对代码进行混淆操作，也没有进行 ROOT 检测和反调试检测，攻击者仍可以相对容易地对 APP 代码进行逆向分析。

网络数据包举例（敏感信息如登录密码等明文传输）：

```
POST /api/Login HTTP/1.1
token:
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJJZCI6MjgyMTAyLCJFbWFpbCI6IjgzNzU3NTcxNUBxcS5jb20iLCJJcCI6IjIwMi4xMjAuMzkuOTkiLCJJc01
mYVBhc3NlZCI6ZmFsc2UsIkNyZWF0ZVRpbWUiOiIyMDE4LTEwLTEyVDA4OjE3OjI3LjQ2MDAwN1oifQ.euczRrRAedcQ1jo18GFQCaOWPdgzaD
Vf7veCSwWxnCE
lang: zh_cn
UserSource: android
Content-Type: application/x-www-form-urlencoded
Content-Length: 208
Host: www.idax.mn
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.5.0

UserName=837575715%40qq.com&Password=FRHfrh1329&geetest_challenge=47cfb2589f34ec781bc0b1b1d6fa37c0eq&geetest_validate=6
497cc1be61c8564aa0e369af4916c5f&geetest_seccode=6497cc1be61c8564aa0e369af4916c5f%7Cjordan
```

本地文件举例（敏感信息如登录 token、登录密码等明文存储）：

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="token">eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJJZCI6MjgyMTAyLCJFbWFpbCI6IjgzNzU3NTcxNUBxcS5j
b20iLCJJcCI6IjIwMi4xMjAuMzkuOTkiLCJJc01mYVBhc3NlZCI6ZmFsc2UsIkNyZWF0ZVRpbWUiOiIyMDE4LTEwLTIzVDAzOjU5OjI5Ljc2NT
k3MjFaIn0.SGvdqbE07zBJryUiQztuYqqskpYA_6YI8e44GUfV-q0</string>
    <string name="password">FRHfrh1329</string>
    <string name="userName">83***qq.com</string>
</map>
```

3.4. Bibox

包名：com.bibox.www.bibox

版本：v1.4.1

评分：32

点评：

该 APP 安全性存在不足，体现在如下方面：虽然 APP 采用了 HTTPS 协议进行数据传输且对 HTTPS 证书进行了校验，但没有对证书进行绑定。攻击者在替换手机证书的情况下，依然可以进行中间人攻击。在数据传输过程中，APP 并未对敏感信息进行加密，用户名、密码等信息均以明文形式进行传送。同时，对于本地保存的数据 APP 也未做加密处理。在代码保护方面，APP 虽然进行了加壳和反调试检测，但代码并未做混淆，同时缺乏模拟器检测、ROOT 检测、重打包检测等，攻击者仍可以相对容易地对 APP 代码进行逆向分析。

网络数据包举例（敏感信息如登录密码、邮箱地址等明文传输）：

```
POST /v1/user HTTP/1.1
Origin: https://moapi.bibox360.com
Referer: https://moapi.bibox360.com
Content-Type: application/json; charset=utf-8
Content-Length: 323
Host: moapi.bibox360.com
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.9.1

{"cmds":"[{\"body\":{\"pwd\":\"FRHfrh1329\",\"fallback\":\"false\",\"challenge\":\"3df18a073a2963b6bd0fa68423b395338b\",\"email\":\"837575
715@qq.com\",\"active_with_number\":1,\"seccode\":\"b633649fd35ab850b515db2f8187701b|jordan\",\"validate\":\"b633649fd35ab850b515d
b2f8187701b\"},\"cmd\":\"user/add1\"}]","isClient":"4"}
```

本地文件举例（敏感信息明文存储）：

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="session_id">U2FsdGVkX1809/XvVRQls22DNsn5jID840MhiUpjB2h832WpgVuvVmqDeiSy9EqUCMu80tt/q7nwEnsBQv6UoA=
=</string>
    <string name="session_https_id">8c231f33272bd2bc3f98ccb4dcc8d93602a0fd19</string>
</map>
```

3.5. EXX

包名：com.exx.exx

版本：v4.0.5

评分：48

点评：

该 APP 安全性存在不足，体现在如下方面：虽然 APP 采用了 HTTPS 协议进行数据传输，但由于缺乏证书校验，攻击者依然可以进行中间人攻击。同时，APP 虽然对登录密码等敏感信息进行加密后传输，但仍存在一些用户隐私数据（包括姓名、身份证号、手机号等）在某些环节直接通过明文传送，用户的隐私存在被泄露的风险。在代码保护方面，APP 缺乏混淆，加壳等保护措施，也未做 ROOT 环境检测、模拟器检测、反调试检测等，攻击者可以轻易对 APP 代码进行逆向分析。

网络数据包举例（敏感信息明文传输）：

HTTP/1.1 200
Server: Tengine
Content-Type: application/json;charset=UTF-8
Connection: close
Date: Mon, 22 Oct 2018 08:59:48 GMT
CNDServer: cache_server_1
Via: cache2.l2st4-2[970,0], cache9.cn60[1004,0]
Timing-Allow-Origin: *
EagleId: 3acdddd115401987873582111e
Content-Length: 816

{"datas":{"userInfo":{"loginMobileAuth":0,"googleStatus":0,"realAuthType":0,"isAlipay":0,"loginPwd":1,"thirdAssetMove":0,"isWechat":0,"safePwd":0,"realAuth":0,"countryCode":"+86","googleAuthFailReason":"","loginGoogleAuth":0,"isBusinesUser":0,"realAuthFailReason":"","email":"837575715@qq.com","nickName":"主账户","isBank":"","mobileAuth":1,"mobileAuthFailReason":"","mobile":"+86 18780013533","photo":"https://www.exx.com/src/images/userhead/u012.jpg","safePwdLevel":0,"userName":"837575715@qq.com","userId":"689780","recommendCode":"769c5f2ef0e56bd5e5f72e8e424ed492","loginPwdLevel":60,"realName":"","mobileStatus":0,"safePwdAuth":false,"googleAuth":0,"loginEmailAuth":0,"userType":1,"assistCoin":"usd","emailAuth":1,"apiStatus":0}},"resMsg":{"code":1000,"method":"doAuthMobile","message":"手机认证成功"}}

Cookie: zJSESSIONID=8EDBF0A
User-Agent: okhttp/3.10.0

本地文件举例（敏感信息明文存储）：

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="uuid">d22d0a34-22b2-4c80-b0a4-27b0fdd38cf0</string>
</map>
```

3.6. ZB

包名：com.vip.zb

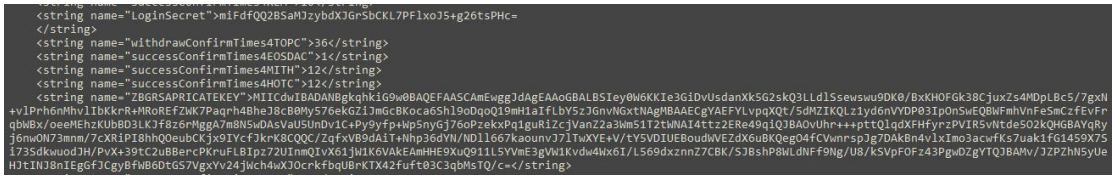
版本：v1.4.7

评分：54

点评：

该 APP 安全性存在不足，体现在如下方面：虽然 APP 采用了 HTTPS 协议进行数据传输，但缺乏证书校验，攻击者仍然可以进行中间人攻击。此外，虽然 APP 对于网络传输过程中的敏感数据都进行了加密，但其将手势密码、RSA 私钥等敏感信息明文存储在本地，所以用户有隐私泄露的风险。在代码保护方面，APP 虽然进行了加壳、反调试检测和重打包检测，但代码并未做混淆，同时缺乏模拟器检测、ROOT 检测，攻击者仍可以相对容易地对 APP 代码进行逆向分析。

本地文件举例（敏感信息如手势密码、RSA 私钥等明文存储）：



3.7. Coinbase

包名：com.coinbase.android

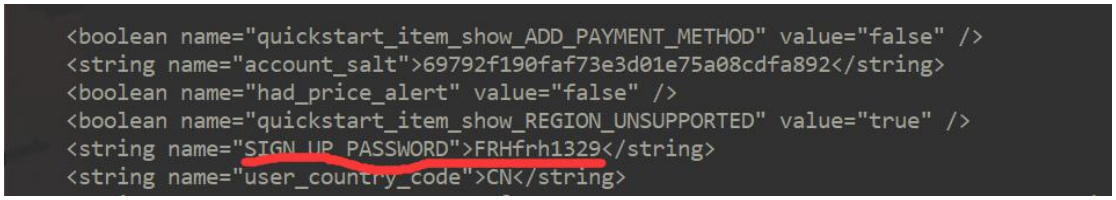
版本：v5.10.1

评分：64

点评：

该 APP 安全性较好，但依旧存在安全隐患，体现在如下方面：APP 使用了 HTTPS 协议进行数据传输，并对 HTTPS 证书进行了绑定，有效地抵御了中间人攻击。不过对于一些敏感数据如注册用户邮箱、注册用户密码、token 等敏感信息直接以明文形式存储在本地，使得 App 安全性下降。而在代码保护方面，APP 缺乏混淆，加壳等保护措施，也缺乏重打包检测，在 ROOT 设备、模拟器环境下均可正常运行，因而攻击者可以轻易对 APP 代码进行逆向分析，了解代码内部逻辑。

本地文件举例（敏感信息如登录 token、注册用户密码等）：

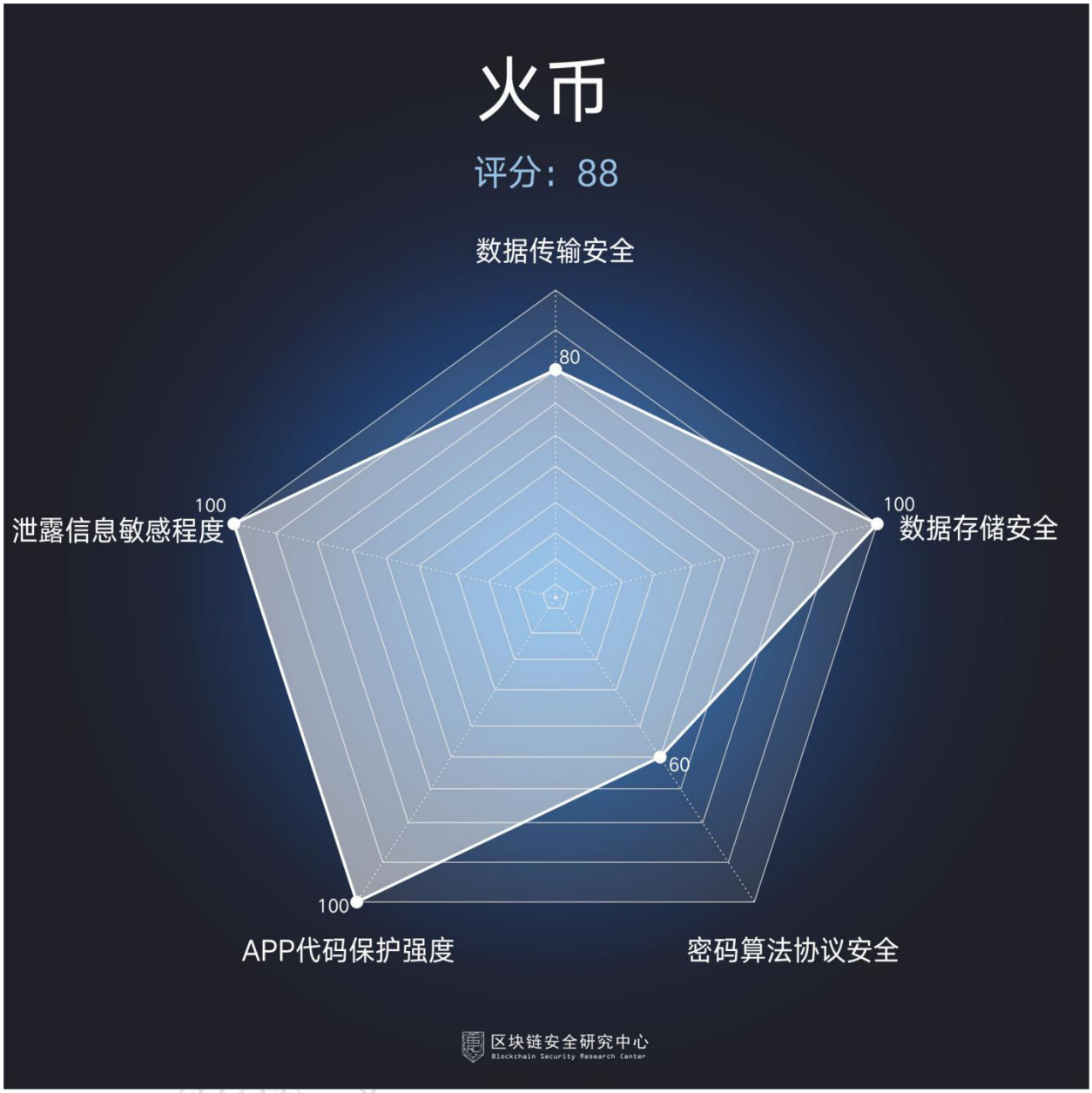


3.8. 火币

包名：pro.huobi

版本：v3.5.2

评分：88



点评：

该 APP 安全性较好，但依旧存在安全隐患，体现在如下方面：虽然 APP 采用了 HTTPS 协议进行数据传输且对 HTTPS 证书进行了校验，但没有对证书进行绑定。攻击者在替换手机证书的情况下，依然可以中间人攻击。此外，APP 中存在 RSA 私钥硬编码的问题，虽然造成的危害不大，但属于密码学误用的情况。APP 在代码保护方面做得相对完善，进行了加壳和混淆操作，同时也做了 ROOT 检测、反调试检测、重打包检测等，可以在很大程度上抵御攻击者对 APP 代码的逆向分析。

网络数据包举例（未做 HTTPS 证书绑定）：

```
POST /-/x/uc/uc/open/login HTTP/1.1
Accept-Language: zh-CN
Connection: close
appType: 1
appVersion: 352
Huobi-Website: huobi.pro
Content-Type: application/json; charset=UTF-8
Content-Length: 979
Host: l10n-pro.dangpu.com
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.8.0
ADRUM: isAjax:true
ADRUM_1: isMobile:true

{"fingerprint":"00000000-28f5-0b6a-0000-0000146fdf8c","way":"APP_HUOBI_PRO","password":"58e49420821aabae9c23b22b79189f1b","afs":{"
session":"nc1-01W8fUo7tiNBKrkhR8ACXXKUJgY6a24fUXJoZdv_ox8SUg6WYEkj7JCQkhXjKO5kG5m-sTtpWZiubQ2qcBTOIznQ-nc2-0561M3bob
-R8gv1KNXk15v5f3YpiSGBZojZa_3ylBGXzEKYd4zVnecz1jZg8UlKYNDqcek5QLehxz0OwZN3gM9rUNI4c9gYWjf2xWpSMaO-hYCnJYeVj-jtdofRR
DG993mse8HH7Rt6xf8uI2S7O9yw3bau4a0Zxm6bGQk-zLc0VZfydZ5Ah9b_N2zNNkughgPN0Xze6A1F9nHSHiPlCZQtvifhIuI2ppBFbHdtM_IpTt
njTEZ6afunTO0EmU_I7TmlNyUPEA2nfUPTkY-72leC8r4OKCuDCjqJKEwxUOrazylTwOsaVoqrHbkFl7h8YzN-fO4NXCp584sgtLZXhRCtOWe73a-
P3HoiQBVgvqgcZPZMnrqxNTSywuNLLzK1dx7IUbQ87nWDmOxyGxehZkQaEgH8adxrfu93YidDYB2GVt4YFuv9fa46ypaJJIGmbCDireKbXpZ5GL
T8xlw1-_Ibw-nc3-01YGjVYP56xB8j7o4jZfyVf6lepaaiisdv0BXs_8mPtw9woxxtX2C19CzsTDQlzUnMPklDMgy9ZrLFdpwRVXMOaY4jK03TcugT62x
Wl9f5Yo4D8qhWsbCHq_DvsvYULoCnOpp4wp0UcE5FV43mKkRA2znd-b4z4fcvjk3Z69qAtzU-nc4-FFFFA000000001796C1B","platform":"1"},"ga
_switch":true,"login_name":"837575715@qq.com"}
```

4. 加密数字钱包 APP 信息安全十大风险

4.1. 签名私钥泄露

- 风险描述：钱包将所使用的用户私钥对外进行传输，导致核心秘密信息泄露。
- 危害指数：★★★★★

该风险可导致用户最核心的密钥信息被第三方获得。数字钱包私钥属于用户进行交易时电子签名的制作数据。2005 年 4 月 1 日起施行的《中华人民共和国电子签名法》（2015 年修订，下称《电子签名法》）在第十三条中，进一步规定了可靠的电子签名应当满足的条件：（一）电子签名制作数据用于电子签名时，属于电子签名人专有；（二）签署时电子签名制作数据仅由电子签名人控制。私钥泄露（例如上传至服务器的行为）明显违背了《电子签名法》的要求，不符合安全实践，且不符合法律规定。

- 风险范围：15%

4.2. 通信数据明文发送

- 风险描述：客户端 APP 与服务器端交互的数据通过明文的通信信道传输。
- 危害指数：★★★★★

该风险可导致用户在使用 APP 过程中发生的交易信息等秘密数据会被网络上恶意中间人窃听甚至篡改，导致相关敏感信息被窃取，或者导致相关交易过程遭到攻击。

- 风险范围：15%

4.3. 通信数据可解密

- 风险描述：客户端 APP 与服务器端交互的数据加密传输，但数据依然可以被解密。
- 危害指数：★★★★½

该风险可导致用户在使用 APP 过程中发生的交易信息等秘密数据会被网络上恶意中间人窃听甚至篡改，导致相关敏感信息被窃取，或者导致相关交易过程遭到攻击。

- 风险范围：30%

4.4. 私钥/助记词不安全存储

- 风险描述：客户端 APP 将私钥和助记词等敏感数据以明文或者固定密钥加密（通过逆向分析程序可以破解该数据）的方式存储在本地，攻击者可以通过访问相关本地数据解密私钥或助记词。
- 危害指数：★★★★

该风险可导致用户存储在手机上的金融交易信息和密码口令等秘密数据完全暴露在攻击者面前。若用户手机遗失，则黑客可以了解用户进行的过的相关交易信息，甚至可以冒充用户登录进行交易。

- 风险范围：20%

4.5. 内存中明文形式存放私钥/助记词

- 风险描述：客户端 APP 在非交易过程中，在内存中以明文形式存放私钥或助记词，对敏感数据缺乏加密保护和相关必要的擦除。
- 危害指数：★★★⯪

该风险可导致在存在安全漏洞的手机上使用 APP 过程中，恶意代码可以通过访问相关进程的内存获取用户的私钥或助记词等敏感信息。

- 风险范围：30%

4.6. 密码学误用

- 风险描述：客户端 APP 代码中使用了不安全的密码学实现，例如固定硬编码的对称加密，ECB 模式的对称加密，CBC 模式中 IV 固定，不安全的公钥进行非对称加密等。
- 危害指数：★★★

该风险可导致用户进行的交易信息、密码口令等秘密数据可能会被解密。黑客可以监听用户进行的所有交易信息。

- 风险范围：40%

4.7. 功能泄露

- 风险描述：客户端 APP 中高权限的行为和功能没有被安全的保护，被其他无授权的应用程序调用或访问。
- 危害指数：★★★⯪

该风险可导致用户相关交易可能会被同一台设备上其它 APP 获取，若其它 APP 中存在恶意软件，就可以监听用户进行的所有交易信息。

- 风险范围：35%

4.8. 可二次打包

- 风险描述：客户端 APP 可被修改代码后，重新打包发布在市场上供用户下载。
- 危害指数：★★⯪

该风险可导致用户容易下载到破解版的 APP，用户一旦下载安装这类破解版 APP，会导致所有秘密数据完全暴露在攻击者面前。黑客不仅可以监听用户进行的所有交易信息，还可以篡改交易内容甚至冒充用户登录进行交易。

- 风险范围：50%

4.9. 可调试

- 风险描述：客户端 APP 能够被调试，动态的提取、修改运行时的程序数据和逻辑。
- 危害指数：★★⯪

该风险可导致用户手机在被恶意软件 root 之后，进行的交易信息、密码口令等秘密数据完全暴露在攻击者面前。黑客不仅可以监听用户进行的所有交易信息，还可以篡改交易内容甚至冒充用户登录进行交易。

- 风险范围：70%

4.10. 代码可逆向

- 风险描述：客户端 APP 的逻辑能够被轻易获取和逆向，得到代码和程序中的敏感数据。
- 危害指数：★★

该风险可导致攻击者更为方便的理解程序逻辑，降低攻击门槛，制作仿冒 APP。

- 风险范围：70%

5. 加密数字钱包 APP 测试安全排行

根据对测试的 14 款加密数字钱包 APP 的评分进行排列，得到以下列表：

- 去中心化加密数字钱包 APP 排行：

排行	APP名称	私钥使用安全	私钥传输安全	私钥存储安全	运行环境安全	用户帐户安全	得分
1	Imtoken	60	100	100	100	60	84
2	麦子钱包	60	100	100	60	60	76
3	Kcash	60	100	60	80	20	64
4	比特派	80	60	20	20	60	48
5	JAXX	20	80	20	20	60	40
6	数字钱包校园版	20	40	20	20	60	32

区块链安全研究中心 Blockchain Security Research Center

- 中心化加密数字钱包 APP 排行：

排行	APP名称	数据传输安全	数据存储安全	密码算法协议安全	APP代码保护强度	泄漏信息敏感程度	得分
1	火币	80	100	60	100	100	88
2	Coinbase	100	40	60	40	80	64
3	ZB	60	50	60	60	40	54
4	EXX	60	20	100	20	40	48
5	Bibox	50	20	20	50	20	32
6	IDAX	20	20	20	60	20	28
7	OKEx	50	20	20	20	20	26
8	LBank	20	20	20	20	40	24

区块链安全研究中心 Blockchain Security Research Center

说明：评分越高代表越安全

三、 检测说明

1. 检测对象的选择

此次检测对象的选择是基于市面上主流的加密数字钱包 APP，选择 14 款 APP 作为此次加密数字钱包信息安全现状检测的最终样本库。

2. 检测标准

2.1. 加密数字钱包的私钥使用安全

加密数字钱包应用会按照密码学原理创建 1 个或多个钱包地址，每个钱包地址都对应 1 个公私钥对。每次交易都必须使用私钥对交易记录进行签名以证明对相关钱包地址里面的资产有控制权。私钥是唯一能够证明对于数字资产有控制权的凭证，而且私钥一旦创建就不能修改，没法重置，只要私钥不丢失，资产就不会丢失。尤其对于去中心化加密数字钱包来说，用户终端私钥存储的安全性是非常核心和关键的问题，如果设计不当则有可能会导致私钥的流失、资产的被盗。对于私钥的使用，我们认为需要遵循以下安全标准：

a) **钱包私钥不能存放在服务器上，无论是否加密。**数字钱包的口令和私钥，都属于用户进行交易时电子签名的制作数据。2005 年 4 月 1 日起施行的《中华人民共和国电子签名法》（2015 年修订，下称《电子签名法》）在第十三条中，进一步规定了可靠的电子签名应当满足的条件：（一）电子签名制作数据用于电子签名时，属于电子签名人专有；（二）签署时电子签名制作数据仅由电子签名人控制。因而将私钥上传至服务器的行为，明显违背了《电子签名法》的要求，既不符合安全实践，又不符合法律要求。

b) **钱包私钥不能存放在外部存储卡上，无论是否加密。**因为外部存储器是任何应用程序都能够读写访问的，并不受系统的隔离机制，因此对于敏感的钱包私钥，应该存放在系统为每个应用程序分配的私有目录下。相比于外部存储器，该私有目录对每个应用程序隔离，只有敏感数据所属的应用程序自己可以访问，这样可以利用系统自带的沙盒隔离机制保护本地数据安全。

c) **钱包私钥不能以明文存储在私有目录。**即便是在正确设置了权限的前

提下，钱包私钥也不允许明文存储在私有目录下。存储在在私有目录的数据依然可能被高权限的程序读取（如：root 权限），此时只有加强对数据本身的加密保护才能提高攻击者破解的难度和门槛。正确做法应该是利用助记词对钱包私钥进行高强度的安全加密，在本地只能存储私钥密文。

d) **使用过钱包私钥后需要及时清理内存。**即使私钥进行安全的加密存储，在使用过程中仍旧需要解密。由于钱包私钥的安全敏感程度非常高，因此私钥不能长期残留在内存之中。如果没有及时的回收内存，会存在私钥明文被窃取的风险。因此在钱包私钥使用过后，必须及时清理内存，避免使用全局变量存储私钥。

e) **钱包私钥需要配合助记词使用，生成助记词过程禁止截屏。**用户依赖助记词来记忆私钥并进行解密和使用私钥，因此助记词的安全性同样十分重要。APP 本地同样不能明文存储助记词，且在生成助记词的过程中需要防止用户主动截屏，或恶意程序后台截屏的操作，防止助记词通过图片的形式泄漏。

2.2. 交易数据传输方法和实现

加密数字钱包应用程序的通信数据通常包含了诸多重要数据，例如账户密码，隐私数据，交易信息等等，数据传输方法和实现如果不安全，则会造成严重的后果，使攻击者具有在中间信道对数据进行窃取，篡改的能力。对于交易通信数据的安全，我们认为应有以下标准：

a) **钱包私钥不能通过网络传输。**钱包私钥属于极其敏感的隐私数据，即使通信信道安全也不允许同服务器之间进行网络传输。无论在传输过程中，还是存储在服务器端，都存在泄漏的风险，威胁用户财产安全。钱包私钥必须保存在客户端，并利用用户密码进行安全加密存储。

b) **不能使用 HTTP 明文进行数据通信。**HTTP 是明文的消息传输协议，面临一系列的安全隐患，容易被攻击者窃听，篡改，劫持等。如果应用程序使用 HTTP 进行明文数据通信，则与服务器通信的敏感数据将失去安全保证。

c) **使用 HTTPS 则需要验证证书以及绑定证书。**如果应用程序使用加密协议 HTTPS 与服务器通信，也并不意味着通信一定安全。HTTPS 协议需要客户端应用程序通过验证证书或者在客户端绑定证书的方式，来验证服务器的身份。否则，攻击者可以进行中间人攻击，通过替换证书的方式来解密流量，达到窃听、篡改通信数据的效果。

d) **若使用自定义协议，则需要有完善的密钥交换协议。**如果应用程序使用自定义的通讯协议与服务器通信，则为了保护通信数据的安全，该协议需要有完善的密钥交换和高强度的加密算法来保证协议的安全。否则，攻击者依然可以通过协议的逆向分析找到破解协议的方式，从而达到窃听和篡改数据的目的。

2.3. 服务器安全

加密数字钱包应用程序对应的服务器安全也是移动互联网 APP 信息安全中的重要一环。客户端通过对服务器的请求可以得到服务器的反馈信息，如果服务器出现安全隐患，则可能导致服务器的关键数据被窃取，甚至出现服务器被控制的严重危害。

我们认为，服务器通过与客户端的通信接口，应当能够抵御常见的安全威胁，如 SQL 注入，XSS，任意文件读取、下载，任意代码执行等。

2.4. 代码保护

客户端代码中通常包含有与业务密切相关程序的重要逻辑、敏感数据以及与服务器交互的接口等，保护好这些代码，不让攻击者轻易获取和分析，

可以大大提高攻击者的攻击门槛和难度，从各个方面减少攻击的可能性，从而提高系统的安全性。我们认为对客户端代码的保护，有如下安全标准：

a) **完整性检查。**移动应用程序容易被二次打包，从而面临盗版、欺诈用户、程序执行流程被篡改等方面的风险。应用程序应具备对自身代码完整性校验的能力，防止攻击者轻易地对程序进行篡改。

b) **防逆向分析。**应用程序的代码可以通过逆向工具获取，攻击者通过阅读逆向代码可以获取程序的执行逻辑。为了加大攻击者分析的难度，提高攻击者破解程序的门槛，应用程序应当使用混淆、加壳等保护手段，来防止程序代码被攻击者轻易地分析。

c) **防进程注入。**进程注入能够动态地了解程序运行信息，从而动态修改程序逻辑，获取程序的机密信息。应用程序需要具备防止其他程序轻易进行进程注入的能力，提高攻击者注入的成本，从而保护自身的数据和逻辑不被窃取。

3. 检测方法

3.1. APP 的下载和锁定

本报告所检测的样本，取自 2018 年 11 月 16 日前官方发布的 Android 应用。在测试期间，个别应用存在强制更新的情况，我们则同步更新相应的 Android 应用并以官方所推送的版本作为检测样本。对于每个测试的样本，我们均以 SHA-1 哈希值作为区分样本、锁定样本的依据，同时标注对应的版本号。至检测工作完成，报告发布之日起，由于应用可能存在新的版本，故可能与检测期间中锁定的应用所报告的问题有所出入。

3.2. 静态检测

本报告所使用的 Android 应用程序静态分析技术基于开源 Android 应用

程序反汇编引擎实现，在常规的反汇编结果基础上，引出一系列接口，可有效提取静态反汇编结果，以便于在反汇编结果之上进行高层的语义分析，达到静态检测应用程序安全性的目的。静态检测技术的特点在于快速、兼容性强、自动化程度高、便于扩展，只需实现针对一类安全问题，制定静态安全检测的规则和策略，静态检测系统就能够自动地输出检测结果。

静态检测系统分为两部分，底层为反汇编引擎，上层为分析工具。底层的反汇编引擎支持对 Android 应用程序的解包、资源解码、反汇编 dex 可执行文件、打包、签名等功能。同时将资源文件以及可执行代码的解码和反汇编结果存储在分析结构体中，并引出一系列接口，便于上层的分析工具进行二次开发和调用。反汇编引擎支持对资源文件解码的接口包括直接获得应用程序的基本信息以及应用程序组件及其属性、权限使用、证书信息、附件文件类型等。对可执行文件的反汇编支持获得应用程序自定义的类及类的基本属性，方法及方法的基本属性，方法内部的反汇编指令。基于底层返回引擎的接口，编写不同的分析工具满足不同的应用程序安全性分析需求。

3.3. 动态检测

本报告所使用的 Android 应用程序动态分析技术主要基于自主开发动态检测系统 InDroid 实现，该系统的最大特点在于，它作为一个具有安全分析功能虚拟机核心引擎 InDroid VM，能够取代 Android 移动智能终端系统中原有的 Dalvik VM 及 ART VM 引擎，无缝链接到现有的 Android 系统中去，形成一个拥有动态应用程序分析能力的 Android 系统。同时我们的 InDroid 能够部署在真实的 Android 设备上，可以有效地规避应用程序对常规动态分析系统的检测。

InDroid 包含了两部分，前端是程序执行和插桩监视引擎，能够在正常执行应用程序的同时，以很小的代价记录执行过程和中间数据，并将其变换为数据流、指令流和控制流等易于程序分析的形式，对其进行在线或离线分析。

后端是恶意行为分析引擎，引擎本身具备信息提取、算法识别等功能，能够对前端输出的数据进行分析判断，给出恶意行为分析结果，另外还提供了可扩展的接口进行规则定义，能够不断提高分析的精确性。

本次报告中，我们主要使用 InDroid 系统来进行文件存储安全分析、流量分析（辅以 Burpsuite）等较为复杂的安全分析操作。

3.4. 深度检测

本次报告中，对于部分较为有影响力、用户数较多的 APP，在自动化安全检测的基础上，我们投入了行业内顶尖的 Android 应用程序分析人员对其进行更为详细的深度人工检测。并对自动化检测中发现的每一个问题进行了模拟攻击实验，了解漏洞在不同环境下可能带来的危害，同时我们也对漏洞的成因进行了人工分析，我们期待能够和厂商一起对相应的漏洞进行必要的修补。

3.5. 危害性重现

在进行本次报告的 APP 安全测试过程中，我们充分考虑了 APP 的使用场景，考虑到不同的环境会给 APP 带来不同程度的安全要求。在常规的安全检测外，我们深入的分析了 APP 在以下环境下的安全性：

a) APP 所处的 Android 系统版本较为陈旧；

b) APP 运行于可被 root 的 Android 设备上；

c) APP 运行于不安全的（公共）WiFi 环境下。

3.6. 评分

在完成对 APP 的各项安全检测后，我们汇总通过不同方法所发现的 APP 安全漏洞。通过人为的评估和反复论证，我们为每一个安全漏洞赋予一个安

全危害分数。通过计算一个 APP 内所包含的安全漏洞的安全危害分数，我们对每一个被检测的 APP 进行了评分，该评分能够较为客观地反映该 APP 的信息安全水平。

四、 潜在风险及解决方法

1. 潜在风险

本次加密数字钱包 APP 安全评测由国内权威的测试机构、研究机构和安全服务企业（上海交通大学网络空间安全学院、中国信息通信研究院泰尔终端实验室、上海掌御信息科技有限公司）联合完成，整个检测过程耗时 29 天，对样本中的 14 个加密数字钱包 APP 进行了深入测试，发现了大量安全问题。我们测试发现，参与测试的大部分 APP 均存在加密算法误用、加密协议实现不正确、不完整的情况，并且在保护用户的交易信息、防止交易被篡改、防止用户身份被盗用方面表现不佳。

作为与数字资产安全息息相关的关键对象，加密数字钱包 APP 存在诸多的安全隐患，考虑到我们的测试对象均关系到高度敏感的用户数字资产交易，我们指出，数字加密钱包 APP 的安全性与国计民生紧密关联。随着移动互联网和数字资产的普及，更多的用户开始使用加密数字钱包 APP 进行在线数字资产交易。根据 Statista 统计，截止到 2018 年 Q2 季度，全球加密数字资产钱包用户数为 2576.4 万人，同比增长 72.1%，环比增长 7.6%，可见数字资产钱包用户增长态势十分迅猛,截至 2017 年 Q2 用户数为 1496.8 万人;截至 2018 年 Q1 用户数为 2395.3 万人。

从用户行为上看，加密数字钱包应用的安装数量和打开数量逐渐呈上升趋势，且涉及的数字资产数量巨大。一旦不法分子利用此类 APP 中存在的安全漏洞进行攻击，轻则盗窃无辜民众数字资产，重则扰乱金融市场秩序，甚至对国家和社会的安全稳定发展造成极大负面影响。

2. 解决方法

2.1. 构建权威性的安全标准

尽管移动互联网和智能移动终端设备的发展已经在过去的十年间取得了长足进步，但是在安全防护方面一直缺乏相应的跟进措施。目前国际上已有的互联网安全评测体系或工具都是针对传统网络结构，或者只就某一项（入侵检测、数据泄漏等）指标进行评测，例如美国国家标准技术研究所（NIST）虽然给出了各种层次和系统的安全标准（建议），但并没有为移动智能终端相关的安全性制定统一标准。移动智能终端相关的安全评测体系尚且十分缺乏，加密数字钱包 APP 的安全则更加缺乏实际的测试评估工作。

国内目前已发布的移动应用软件安全相关标准中，与加密数字钱包 APP 相关的包括中国银联编写的《移动终端支付应用软件安全规范》，该规范主要针对的是银行类应用的安全实现，规范了基于智能卡客户端、无智能卡客户端、基于移动终端浏览器支付软件架构以及支付应用软件的安全要求、后台系统的安全要求、用户安全要求、数据安全要求、客户端支付软件和智能卡的交互安全等。而对于加密数字钱包 APP 软件，在开发过程中往往对上述安全问题没有特别严格的要求，因而存在的问题远远多于支付类应用软件。这也充分说明，如果能够为加密数字钱包 APP 开发制定一套详细的安全规范和测试安全标准，必将有效地降低加密数字钱包 APP 安全问题发生的概率。本《白皮书》中对于加密数字钱包 APP 的测试实属首次。我们希望通过全面深入的实际测试，总结出一套加密数字钱包 APP 应该遵循的安全规范和测试安全标准，并为后续开发人员提供指导。

2.2. 政策推动

APP 安全特别是加密数字钱包 APP 的安全，是国家、开发商、广大用户三方面共同的需求。国家对 APP 安全的规范工作正在不断建设与完善。2012 年

12 月 11 日，工业和信息化部发布了对 App 应用进行备案管理通知，目的在于建立一个长效的评估体系，对智能手机应用程序、内置软件进行评估和抽查，而且相关的国家实验室和研究院都参与到其中。2014 年 4 月至 9 月工业和信息化部联合公安部、工商总局在全国范围开展“打击治理移动互联网恶意程序专项行动”，将互联网恶意程序设为重点打击治理项目之一。在加密数字钱包 APP 领域，也亟需从国家、政府层面上推行相关的政策，强制要求 APP 开发商和运营企业接受安全检测，遵守安全规范，从而进一步推动加密数字资产安全工作，提高系统安全水平。

2.3. 构建企业广泛参与的安全生态

移动生态环境长期以来一直是由诸多软硬件厂商、开发人员和各大运营商共同推动发展。随着加密数字钱包 APP 市场发展周期的推进，错综复杂的安全情况，越来越高频的安全威胁，都预示着加密数字钱包 APP 安全攻防战场将更加焦灼，仅仅通过某一单一组织来保证加密数字钱包 APP 生态环境的信息安全是不现实的。参考互联网移动端安全发展的轨迹，加密数字钱包 APP 开发者与独立的第三方加密数字钱包 APP 安全测试机构、安全服务提供企业合作，将成为加密数字钱包 APP 安防的主流趋势。

在实际安全攻防过程中，政策的制定必须和现实密切契合，也就是说必须通过真实的安全威胁、安全攻击来总结出相应的策略，执行相关安全检测。在这一点上，我们主张由那些在第一线上从事安全分析和安全服务的企业来提出相关策略，由第三方权威测试机构来引导和制定相关检测规范，引导 APP 开发商和服务提供商实现更为安全的产品。

2.4. 普及安全知识，提高用户信息安全意识

在本次测试过程中，我们也发现在现实生活中，许多用户认为对于加密数字钱包 APP，只要是通过正规的渠道下载并在安全的网络环境下使用，再担

心安全问题是多余的。但是我们的测试表明，大部分加密数字钱包 APP 的密码学应用存在问题，其数据保护机制不完整，缺少检验。如果 APP 自身就存在安全方面的隐患甚至是安全漏洞，那么就很有可能轻易被黑客攻击，从而造成用户的信息泄露和财产损失。

下面是本次测试的主要承担方——上海掌御科技有限公司的信息安全专家指出一些较为常见的，存在于加密数字钱包 APP 中的安全问题以及相应的对策：

1) 及时升级加密数字钱包 APP，保持最新版本，防止旧版本安全漏洞遭到利用；

2) 使用专用的移动设备和移动网络进行操作，并及时升级移动操作系统；

3) 关注权威测评机构最新发布的加密数字钱包 APP 安全测试报告。

同时，上海掌御科技有限公司的信息安全专家也对加密数字钱包 APP 的开发商提出了相关建议。从我们的测试情况来看，当前存在的大部分问题是因为开发人员缺乏安全意识和专业的安全开发知识所导致，开发人员在设计数据保护方案，特别是针对深层核心的敏感数据的保护方案时，务必对方案进行严格的安全论证。在对加密算法、协议等的应用方面，没有把握的情况下应当咨询专业研究团队并进行相关安全审计。

五、 结束语

客观地讲，加密数字钱包只是整个数字资产金融体系的一部分，而金融的核心则是风控，风控之中的重要一环就是用户信息安全。加密数字钱包的主要目标客户就是普通大众，其参与门槛低、受众面广、受众基数大，每一款产品的信息安全都将影响到数量众多的普通用户的切身利益。

无论从数字金融本身还是社会民生的角度，我们都将不得不以十分严肃的态度来面对加密数字钱包 APP 的信息安全问题。而我们希望行业内尽早建

立关于加密数字钱包的安全评判标准，我们也希望通过本白皮书让用户更清楚的认识和了解数字货币钱包的安全性问题、提高警惕；并通过提出数字货币钱包安全标准的方式促进行业内同类产品的安全升级，共同保护用户资产的安全性。

未来，我们也将不断地对这一问题进行持续跟进，争取利用我们的专业特长，通过我们的不懈努力，最终能够对加密数字钱包 APP 信息安全总体水平的提高做出应有的贡献和促进作用。我们将继续跟进该《白皮书》中所涉及的各个加密数字钱包 APP，并持续关注加密数字钱包行业的信息安全问题，定期出具相关检测和分析报告。