

سامانه کاستادی کیف پول دژکی

شرکت پیشرو فناوری اطلاعات رادین



مقدمه

ظهور فناوری نوین بلاکچین اگر چه بستری امن برای تبادل دارایی‌های دیجیتال به ارمغان آورده است، اما همچنان مسئله امنیت و حفظ کلید خصوصی کیف پول‌های حضانتی در صرافی‌های متمرکز به عنوان یک چالش جدی مطرح است.

محصول دژکی یک راه‌حل امنیتی برای پاسخ به چالش مذکور است که با بهره‌گیری از مکانیزم‌های امنیتی سخت افزاری و نرم افزاری امنیت کیف پول‌های صرافی‌های متمرکز را تضمین نموده و دارایی‌های دیجیتال را در برابر خطراتی چون هک، سرقت، تغییر موجودی کیف پول‌ها و غیره حفاظت می‌کند.

این محصول ضمن به کارگیری پیشرفته‌ترین الگوریتم‌های امنیتی، قابل رقابت با بهترین نمونه‌های خارجی بوده و به دلیل قابلیت پشتیبانی از شبکه‌های بلاکچین متعدد به عنوان گزینه‌ای کارآمد برای استفاده در صرافی‌های رمزارز به شمار می‌رود.

صورت مسئله

- امنیت یک صرافی ارز دیجیتال به عنوان اولین و مهم‌ترین معیار در انتخاب صحیح یک صرافی به شمار می‌رود.
- صرافی‌های متمرکز رمزارز به عنوان محلی از انباشت سرمایه، همواره در معرض خطرات امنیتی جدی همچون هک و سرقت قرار دارند.
- در صورت هک شدن و از دست رفتن سرمایه، ذینفعان مختلف این صنعت متحمل خسارات جبران‌ناپذیری می‌شوند.
- صرافی‌های رمزارز نیازمند استفاده از روش‌های امن برای ساخت کیف پول و ذخیره‌سازی کلیدهای خصوصی هستند به نحوی که امکان نفوذ به آن‌ها و زیرساخت رمزنگاری مورد استفاده به کمترین حد ممکن برسد.

صورت مسئله

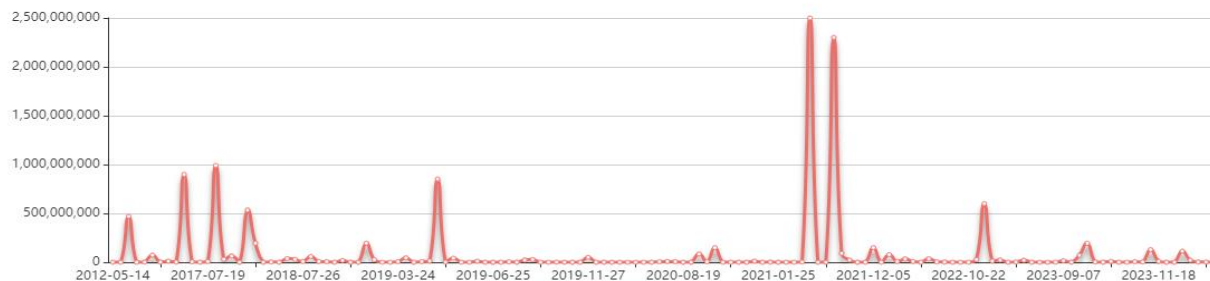
● بر اساس گزارش شرکت امنیتی بلاکچین SlowMist، صنعت کریپتو از سال ۲۰۱۲ تاکنون هدف حملات هکری مختلف قرار گرفته و بالغ بر ۳۱ میلیارد دلار متضرر شده است.

● به طور ویژه بیش از ۳۰ درصد از مقدار فوق از صرافی‌های رمزارز به سرقت رفته است.

[SlowMist Hacked Statistical]:

Exchange hack event(s) 140 ;

The total amount of money lost by blockchain hackers is about \$ 11,532,509,981.39 ;



Source: <https://hacked.slowmist.io/statistics>

محصول دژکی راه حلی برای امنیت صرافی‌های رمزارز

استفاده از ترکیب راه‌حل‌های سخت افزاری و نرم‌افزاری به منظور افزایش امنیت صرافی‌های متمرکز



راه‌حل سخت‌افزاری دژکی:

- ایجاد کلیدهای خصوصی درون سخت‌افزار HSM-Blocksafe و عدم امکان دسترسی به آن‌ها
- ساخت کیف پول
- انجام عملیات‌های رمزنگاری و الگوریتم‌های مختلف امضای دیجیتال درون سخت‌افزار
- انجام تراکنش

راه‌حل نرم‌افزاری دژکی:

- پشتیبانی از عملیات پیچیده رمزنگاری جهت ساخت کیف پول‌های HD Wallet
- پشتیبانی از عملیات رمزنگاری جهت انجام تراکنش‌های چند امضایی Multi Signature Transaction
- پشتیبانی از عملیات پیشرفته رمزنگاری جهت انجام تراکنش‌های مبتنی بر امضای چند نفره Multi Party Computation

قابلیت‌های محصول دژکی

● محصول کاستادی دژکی اولین محصول کاستادی در بازار کریپتوی ایران است که با به کارگیری روش‌های امنیتی سخت‌افزاری و نرم‌افزاری با هدف حفاظت از کلید خصوصی کیف پول‌های حضانتی و افزایش امنیت صرافی‌های متمرکز توسعه داده شده و با مشخصات بهترین کاستادی‌های موجود در جهان مطابقت دارد.

● این محصول قابلیت‌های مختلفی از جمله ساخت کیف پول HD Wallet، انجام تراکنش‌های چند امضایی، انجام تراکنش‌های مبتنی بر محاسبات چند نفره و تنظیم سطوح امنیتی مختلف برای انجام عملیات‌های متفاوت را دارد.

● دژکی در حال حاضر قابلیت پشتیبانی از شبکه‌های بلاکچینی متعددی نظیر بیت‌کوین، اتریوم، بایننس، ترون، کاردانو، لایت‌کوین، دوج‌کوین، پالیگان، ریپل و رمزارزهای بومی و توکن‌های موجود بر روی این شبکه‌ها را دارد.

معرفی ویژگی‌های محصول دژکی

● امکان ساخت و مدیریت کیف پول‌های HD Wallet

- در سامانه دژکی دو سطح دسترسی ادمین و کاربر برای سامانه تعریف شده است که کاربر با دسترسی ادمین می‌تواند اقدام به ساخت تعداد زیادی کیف پول‌های HD Wallet کند. کلیه مراحل ساخت کیف پول اعم از تولید seed، محاسبات رمزنگاری مبتنی بر curve انتخابی و تولید کلید عمومی و خصوصی به صورت سخت‌افزاری با استفاده از دستگاه HSM-Blocksafe انجام می‌شود و به دلیل عدم خروج کلیدهای خصوصی از دستگاه، عملاً امکان دسترسی به آن‌ها وجود ندارد.

ساخت کیف پول اچ‌دی

نام کیف پول اچ‌دی:

HexSeed:

Curve Type:

ایجاد

معرفی ویژگی‌های محصول دژکی

امکان ساخت و مدیریت انواع کیف پول

- در حال حاضر کاربر سامانه می‌تواند به یکی از چهار روش شامل: ساخت کیف پول عادی ذیل HD Wallet، ساخت کیف پول با استفاده از کلید عمومی، ساخت کیف پول چند عاملی و ساخت کیف پول دو عاملی، اقدام به ساخت کیف پول لازم برای استفاده در سامانه کرده و برای انجام تراکنش از آن‌ها استفاده کند.
- کلیه مراحل تولید کلید عمومی و خصوصی کیف پول‌ها به صورت سخت‌افزاری با استفاده از دستگاه HSM-Blocksafe انجام شده و عملاً دسترسی به کلید خصوصی کیف پول‌ها امکان‌پذیر نخواهد بود.

ساخت کیف پول

عادی ساخت با استفاده از کلید عمومی چند عاملی دو عاملی

نام

انتخاب رمز ارز

HD Wallet

ساخت کیف پول

معرفی ویژگی‌های محصول دژکی

● امکان ساخت کیف پول‌های چند امضایی و انجام تراکنش‌های چند امضایی

- در حال حاضر محصول دژکی قابلیت پشتیبانی از ساخت کیف پول چند امضایی و انجام تراکنش‌های چند امضایی برای شبکه‌های بیت‌کوین و ترون را دارد.
- در اینگونه کیف پول‌ها انجام موفق یک تراکنش وابسته به امضای چند کاربر است.

+ ساخت کیف پول چند امضایی بیت‌کوین

کیف پول‌های تحت کنترل کاربر

#	نام	آدرس	تعداد امضاکنندگان	حداقل امضای مورد نیاز	ایجاد تراکنش	تاریخچه
1	MultiSigBitcoinWalletByLeilaShafiee	tb1qaprvhd8f86l6xe7xjxz49sgj008jp687xl7g8t3mpkthvpyurts5vrhfl	3	2	+	🕒

تراکنش‌های در انتظار تایید

#	مقدار	آدرس گیرنده	تعداد امضاکنندگان	وضعیت	امضای تراکنش
---	-------	-------------	-------------------	-------	--------------

تنظیمات دسترسی کیف پول

🔑

LeilaShafieeTeronwallet1.18.09.1402

آدرس کیف پول

TSUI8iBx7iN2hCPh1H7dPL56bcLV8Jp6Ny

🔑

نام کیف پول

آدرس کیف پول

اجازه دسترسی

نام	وزن	آدرس	حداقل آستانه	دسترسی

+ افزودن کلید دسترسی

+ افزودن گروه دسترسی

🗑 حذف گروه دسترسی

معرفی ویژگی‌های محصول دژکی

امکان ساخت کلید خصوصی مبتنی بر محاسبات چند نفره Multi party computation

- ساخت کلید خصوصی چند نفره جهت انجام فرآیند امضا و انجام تراکنش‌های MPC قابلیت‌هایی است که در حال حاضر تعداد محدودی از شرکت‌ها و صرافی‌های بزرگ دنیا از آن بهره می‌برند. محصول دژکی با پیاده‌سازی الگوریتم‌های پیچیده رمزنگاری قابلیت پشتیبانی از تراکنش‌های مبتنی بر محاسبات چند نفره را فراهم می‌کند. در این مکانیزم امنیتی گروهی از کاربران با مشارکت با یکدیگر اقدام به ساخت یک جفت کلید عمومی-خصوصی می‌کنند به گونه‌ای که هر ترکیب t نفر از n نفر آن‌ها بتوانند امضای معتبر تولید کرده و تراکنش را امضا کنند. در واقع کلید خصوصی و عمومی با مشارکت همزمان کاربران ساخته می‌شود و هیچ کاربری به تنهایی کلید را در اختیار ندارد و امضای معتبر با مشارکت ترکیبی از عوامل مشارکت کننده در ساخت کلید انجام می‌شود. در طول فرآیند ساخت کلید یا امضا لازم نیست افراد به یکدیگر اعتماد داشته باشند زیرا پروتکل مورد استفاده صداقت افراد را تضمین می‌کند.

ایجاد دسترسی ساخت کلید چند نفره:

نام کلید:

تعداد امضای معتبر:

کاربران دارای دسترسی:

saadat

samiei

rahmati

izadi

shafiei

+ افزودن

ایجاد دسترسی ساخت

معرفی ویژگی‌های محصول دژکی

انجام تراکنش

- در سامانه دژکی کاربر می‌تواند با انتخاب کیف پول، رمز ارز و در اختیار داشتن آدرس کیف پول مقصد تراکنش را انجام دهد. پس از انجام تراکنش، لینک تراکنش برای کاربر ارسال می‌شود. کلیه عملیات رمزنگاری مربوط به امضاهای دیجیتال به صورت سخت‌افزاری با استفاده از دستگاه HSM-Blocksafe انجام می‌شود.

پرداخت رمز ارز

رمز ارز مورد نظر را انتخاب کنید

کیف پول مورد نظر را انتخاب کنید

کل موجودی
قابل برداشت
در سفارش
شبکه انتقال

BTC 0
BTC 0
BTC 0
Segwit

توجه: لطفا در وارد کردن اطلاعات زبردقت کنید.

آدرس کیف پول مقصد

وارد کردن آدرس نامرست ممکن است منجر به از دست رفتن منابع مالی شما شود.

مقدار برداشتی

مقدار برداشتی را به واحد کوین مربوطه وارد کنید.

انجام تراکنش

معرفی ویژگی‌های محصول دژکی

امنیت

- سامانه دژکی در حال حاضر دارای چهار سطح امنیتی است که کاربر با انتخاب آن‌ها می‌تواند عملیات مورد نظر خود اعم از ورود به سامانه، انجام تراکنش، تغییر دسترسی تراکنش‌های چند امضایی و انجام تراکنش‌های چند امضایی را با هر ترکیبی از سطوح امنیتی انجام دهد.
- سطوح امنیتی که در سامانه دژکی استفاده می‌شوند عبارتند از:

- رمز عبور
- SMS OTP
- Email OTP
- Google Authenticator

تنظیمات امنیتی				
عملیات	رمز عبور	تایید دومرحله‌ای گوگل	تایید دومرحله‌ای ایمیل	تایید دومرحله‌ای پیامکی
	تغییر	فعال سازی	✓	✓
ورود به حساب کاربری	☒	☐	☐	☐
انجام تراکنش	☒	☐	☐	☒
تغییر دسترسی چندامضایی	☒	☐	☐	☒
تراکنش چندامضایی	☐	☐	☐	☐
امضای تراکنش چندامضایی	☐	☐	☐	☐

مزیت رقابتی

● استفاده از ماژول سخت افزاری مطمئن در کنار راه حل نرم افزاری

- در حال حاضر کیف پول های حضانتی در صرافی های متمرکز از طریق راه حل های نرم افزاری ساخته و نگهداری می شوند. استفاده از ماژول سخت افزاری و انجام کلیه عملیات رمزنگاری و امضای دیجیتال به صورت سخت افزاری و عدم امکان دسترسی به کلیدهای خصوصی کیف پول ها که موجب افزایش امنیت این کیف پول ها می شود، یکی از مهم ترین وجه تمایز این محصول نسبت به سایر محصولات مشابه است.

● در دسترس بودن ماژول امنیتی سخت افزاری برای شرکت رادین

● قابلیت انجام تراکنش های مبتنی بر محاسبات چند نفره (MPC):

- پیاده سازی الگوریتم های پیچیده رمزنگاری جهت انجام یک امضای چند نفره یک قابلیت مهم امنیتی است که در حال حاضر شرکت های معدودی در جهان از آن بهره می برند. وجود این قابلیت در محصول دژکی به عنوان یک مزیت رقابتی مهم نسبت به دیگر محصولات موجود به شمار می رود.

● قابلیت پشتیبانی از شبکه های مختلف بلاکچین

- محصول دژکی از شبکه های بلاکچین مختلفی شامل: Bitcoin, Ethereum, Tron, Dogecoin, Litecoin, Binance, Ripple, Polygon, cardano و الگوریتم های امضای دیجیتال ECDSA و EdDSA پشتیبانی می کند.

● عدم وجود نمونه داخلی مشابه

رقبای محصول

در حال حاضر نمونه مشابه داخلی برای محصول کاستادی که ترکیبی از دستگاه HSM و نرم افزار باشد، وجود ندارد.



نمونه های مشابه خارجی:

- کاستادی کوین بیس (CoinBase Custody)
 - نگهداری امن، پوشش بیمه

- کاستادی بیت گو (BitGo)
 - والت چند امضایی، پوشش بیمه

- کاستادی جمینی (Gemini Custody)
 - والت سرد، HSM، پوشش بیمه

- کاستادی انکوراژ (Anchorage)
 - احراز هویت بیومتریک، پوشش بیمه

- کاستادی اوربیتوس (Orbitos)
 - والت سرد، ولت چند امضایی، پوشش بیمه

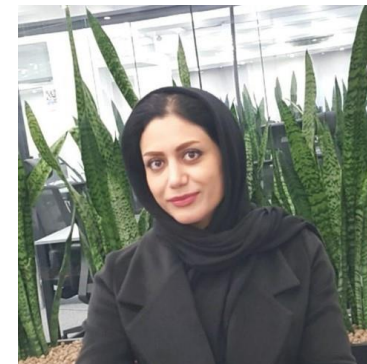
معرفی تیم



محسن سمیعی
مدیر محصول



میثاق سعادت
مدیر پروژه



لیلا شفیعی
مدیر دپارتمان بلاکچین
توسعه دهنده بلاکچین



فاطمه ایزدی

توسعه دهنده Frontend



رحمت انجیرابی
توسعه دهنده Backend

با تشکر از توجه شما

شرکت پیشرو فناوری اطلاعات رادین

دپارتمان بلاکچین

دی ماه ۱۴۰۲

