SCAM — MONDAY

January 31 / 2022

If you can't explain the scam to a seven-year-old, you're probably the one getting scammed.

فهرست

مقاله هفته:
اسکمرها از آن‌چه در آیینه می‌بینید به شما نزدیک‌تر هستند

مقاله هفته:
اسکمرها از آن‌چه در آیینه می‌بینید به شما نزدیک‌تر هستند

عمو سم/ @cryptosamz

کلمه‌ی اسکم یا کلاهبرداری یکی از رایج‌ترین کلماتی است که این روزها توسط اکثر فعالین بازار کریپتوکارنسی خیلی تکرار می‌شود، چیزی که همه فعالین بازار حداقل چند بار در طول فعالیتشان با آن مواجه شده‌اند، ولی نکته اینجاست که این مسأله نه‌تنها جدید نبوده بلکه یکی از پدیده‌های بسیار قدیمی و رایج در جوامع انسانی در طول تاریخ بوده است.

این پدیده ریشه در طمع، حرص و رویای یک‌شبه پول‌دار شدن افراد دارد و هرکجا که تجمیع ثروت و سرمایه وجود داشته باشد سروکله‌ی این قشر زحمتکش هم پیدا می‌شود. پس وجود این افراد در این فضا اجتناب‌ناپذیر و غیرقابل‌انکار هست.

یکی از بهترین معیارهای شناخت موقعیت‌های خطرناکِ مشکوک به اسکم که نیازی به هیچ دانش تخصصی و ابزار خاصی ندارد این است که بدانید "هر زمان و هرکجا که پیشنهاد و شرایط بنظرتون با عقل و منطق متداول همخوانی نداره و خیلی جذّابه، به آن به دید اسکم نگاه کنید" این همان مثل قدیمی "پنیر مجانی فقط توی تله موش هست" را تداعی می‌کند.

مادام که افراد، بدون داشتن تخصص و تلاشی خاص، سودای یک‌شبه پول‌دار شدن را در ذهن داشته باشند، این قانون ادامه‌دار خواهد بود و به طرز معناداری می‌توان همه‌ی قواعدش را تکراری دانست.

مشکل در بازارهای مالی و بخصوص بازار نوظهور کریپتوکارنسی از جایی شروع و تشدید می‌شود که افراد پس از ورود به بازار و آشنایی با مفاهیم اوّلیه دچار توهم و شاید فراموشی نسبت به تمامی مفاهیمی می‌شوند که طی سالیان متمادی در دنیای واقعی تجربه کرده‌اند. در صورتی که این فضا به یکباره توسط عوامل فرازمینی ساخته نشده است بلکه همان افرادِ رشد یافته در جوامع سنتی‌تر این فضا را به وجود آورده‌اند، پس قواعد بازی و شرایط مستثنی نیست و چه‌بسا به دلیل دانش کم اکثر فعّالین و ذات مالی آن، افراد با نظریات و تفکرات ناسالم بیشتری جذبِ آن شده باشند.

برای عینیّت بخشیدن به این موضوع که شرایط حاکم بر بازار رمزارز با فعّالیت‌های رایج اقتصادی دنیای عادی ما هیچ تفاوتی ندارد و فقط کافی است که با دید منطقی و نه رؤیاپردازانه به آن نگاه کنیم، از چند مثال تاریخی در زمینه‌یِ اسکم و وجه اشتراکشان با دنیایَ رمزارزها استفاده می‌کنیم:

برای اوّلین‌بار، ۲۳۰۰ سال پیش در یونان باستان شخصی بعد از بیمه کردن یک کشتی و بار آن، خودش اقدام به غرق کردن کشتی خالی کرده و بعد از گرفتن پول بیمه اقدام به فروختن بار کشتی نمود و عملاً به اولین اسکمر شناخته شده‌ی تاریخ تبدیل شد. این مثال تطابق دارد با همان فاندرهای پروژه‌هایی که با قراردادن بَک دُر (در پشتی) در کد کانترکت اقدام به دزدی از پروژه‌ی خودشان می‌کنند و یا استخر نقدینگی توکن خودشان رو خشک کرده و خیل عظیمی از سرمایه‌گذاران را به مال‌باخته تبدیل می‌کنند.

مقاله هفته: اسکمرها از آن‌چه در آیینه می‌بینید به شما نزدیک‌تر هستند

مطرح‌ترین و به‌نوعی پدر اسکمرها جناب آقای چارلز پانزی بزرگوار است که با دادن وعده‌ی سود بالا در مدت‌زمانی کوتاه اقدام به جذب سرمایه‌ی زیادی کرد.
او با دریافت پول از تازه‌واردها سودهای افراد قبلی را پرداخت می‌کرد تا زمانی که ورودی طرح جوابگوی میزان سودی که باید پرداخت می‌کرد نبود و با این روش توانست ۲۰ میلیون دلار در سال ۱۹۲۰ کلاهبرداری کند.
دقیقا مشابه همین رویکرد را شرکت‌های به اصطلاح سرمایه‌گذاری و سبدگردانی حوزه‌ی کریپتوکارنسی و همین‌طور پروتکل‌های دیفای که وعده‌ی سودهای بالا را می‌دهند، بکار می‌برند. حتی پلتفرم‌هایی که ادعای استخراج ابری به شما می‌دهند نیز عملاً جزء همین دسته‌ی پانزی‌ها قرار می‌گیرند.
ساده‌ترین راه و سوال حیاتی برای گرفتار نشدن در دام این قبیل اسکم‌ها این است که از خودتان بپرسید: چرا باید این درصد بالای سود را به ما بدهند در صورتی که می‌توانند با درصد خیلی پایین‌تری مبالغ خیلی بیشتری را جذب کرده و سود بیشتری عایدشان شود؟

آقای ویکتور لوستیگ هم تقریباً ۱۰۰ سال پیش در یک اقدام هوشمندانه توانست برج ایفل را به یک تاجر بفروشد. یعنی زمانی که هنوز حرفی از مفاهیم امروزی متداول در دنیای تکنولوژی نبود.
امروزه وارثان ژن آقای لوستیگ با بهره‌گیری از مفاهیم داغ و ترند شده در این فضا دقیقا مشابه همان کار را انجام داده و شروع به فروش برج‌ها و آسمان‌خراش‌هایی در متاورس می‌کنند و آن جماعتی که همگی پدر بزرگی داشته‌اند که سالها پیش چند هکتار زمینش را مفت فروخته وگرنه امروز میلیونر بودند، هم به‌خاطر جبران جفایی که پدربزرگ در حقّشان کرده، چشم‌بسته شروع به خرید طبقات مختلف برج و زمین‌های دنیای متاورسی می‌کنند که هنوز نخبه‌ترین افراد فقط در حدّ همان عینک‌های vr از آن می‌دانند.
اسطوره‌ی بعدی، آقای میگه رن هلندی هم مورد جالبی داشته که باز هم حوالی ۱۲۰ سال پیش با مهارت بسیار اقدام به جعل آثار هنری و نقّاشی‌های معروف می‌کرده و این آثار رو می‌فروخته است. این بار توسعه دهندگان و برنامه‌نویسان، حتی نه چندان حرفه‌ای، با سوار شدن بر روی امواج و هایپ بازار توکن‌های NFT، همان مسیرِ جد بزرگوار خویش آقای میگه رن را در پیش گرفته و با ساختن توکن‌های NFT از هر چیز بی‌ارزشی که نه ذات هنر در آن دخیل است و نه ارزش‌آفرینی برای مالک اثر به وجود می‌آورد، یاد آن بزرگوار را جاودانه نگه می‌دارند.

در صورتی که کاربرد این توکن‌ها چیزی به مراتب فراتر از تصور غلط شکل گرفته در موردشان است و همان‌طور که "میگه رن" به آثار هنری و کالکتورها لطمه می‌زد، متاسفانه اسکمرهای این حوزه هم آسیبی به‌مراتب بزرگ‌تر به سرمایه‌گذاران این حوزه و حتی کل بازار رمزارزها می‌زنند.

جذاب‌ترین افراد اسکمر از دید من، وارثان آقای اباگ نیل هستند که خیلی شبیه کاراکتر وطنی خودمان یعنی همان مرد هزار چهره می‌باشند. این شخص یک جاعل حرفه‌ای در زمینه مدارک و عناوین بوده که توانسته بود با جعل مدارک چندین سال به‌عنوان دکتر، خلبان و وکیل فعّالیت رسمی داشته باشد.

فکر می‌کنم وی بزرگ‌ترین نسل را از خودش به جای گذاشته است چون متداول‌ترین نوع اسکمی که تقریبا هرروزه با آن سروکار داریم از همین نوع است. یعنی افرادی که به محض آشنایی با یکی از مبانی بازار رمزارز و در کوتاه‌ترین زمان ممکن تبدیل به استادی بی‌بدیل در این حوزه شده و اقدام به ارائه‌ی آموزش می‌کنند.

اینان به دلیل عمق کم از درک مطالب، در بهترین حالت افراد بسیار خطرناکی برای تمام فعالین بازار هستند چون حتی اگر قصد کلاهبرداری سازمان‌یافته‌ای هم نداشته باشند به دلیل جهل حاکم بر افکارشان باعث ضرر کردن سایرین شده و بنابراین اسکمر شناخته می‌شوند. این بخش عمده‌ی اسکمرهای اطراف ما هستند. بخش کوچک‌تری از این طبقه‌ی اسکمرها با کسب اعتبار از طریق جعل اخبار و اطلاعات دیگران و شبکه‌سازی از طرق مختلفی مانند ساخت توکن‌های بدون پشتوانه و کاربرد و فروش آن توکن‌ها به مخاطبینی که اعتمادشان را جلب کرده‌اند در جهت اهداف خودشان گام برمی‌دارند.

اسکمرها در لحظه به لحظه‌ی تاریخ و قدم به‌قدم در کنار ما بوده و با پیدایش هر پدیده و تکنولوژی جدیدی خودشان را با آن سازگار کرده‌اند. لذا از این بابت باید به آن‌ها به دلیل ممارست و مداومت در امر خطیر اسکمری جایزه‌ی یک عمر تلاش بی‌وقفه اعطا کرد. چون دقیقا با پیدایش پول به معنای شناخته شده‌ی امروزی آن، بانکدارها با چاپ پول بدون پشتوانه شروع به اسکم کردن مردمی که صاحب پول بانک‌ها بودند، کردند و پس از آن با ظهور تکنولوژی‌های گوناگون، از طریق ارسال فکس‌های فیک درمورد مبالغ هنگفت پول، تبلیغات کالاهای بی‌مصرف و بی‌کیفیت در تلویزیون، ایمیل‌های تروجان و تهدیدآمیز و یا فیشینگ‌های اینترنتی تا به امروز در دنیای جدید و سرشار از فرصت اسکم هنوز همراه ما هستند و قطعا تا روزی که بشر در قید حیات باشد و مادام که رویای یک‌شبه پول‌دار شدن و طمع در افراد وجود داشته باشد این قصّه همچنان ادامه خواهد داشت. در مقابل افرادی هم خواهند بود که برای رفع این نیاز پاسخی داشته باشند، افرادی که واقعا هدفشان مشترک است، ولی نتیجه‌ی نهایی همان رسیدن به رویای خود افراد اسکمر است که هیچ پیامدی جز از دست رفتن سرمایه‌ی باقی افراد نخواهد داشت.

عیب می جمله چو گفتی هنرش نیز بگو، البته قصدم تعریف از هنر اسکمرها نیست ولی واقعا باید از این جهت هم موضوع را نگاه کنیم که در بسیاری از مواقع وجود این افراد شاید عامل فزاینده‌ی سرعت رشد و پیشرفت باشد. شاید اگر بانکدارها و دولت‌ها در نقش بزرگ‌ترین اسکمرهای تاریخ تا این حد به مردم فشار نمی‌آوردند، هیچ گاه ساتوشی ایده‌ی خلق بیتکوین به سرش نمی‌زد، ایده‌ای که احتمالا نقطه‌ی شروع انقلابی باشد که به‌خاطر ابعاد فنی، خاصیت تمرکززدایی و شفافیتش در نهایت باعث شود که بشر بتواند از شرّ اسکمرها برای همیشه خلاصی یابد. همین‌طور که امکان جعل بیتکوین نزدیک به صفر است شاید همین فضای کریپتوکارنسی‌ها روزی با چیزی مانند NFT بتواند جلوی جعل نه‌تنها آثار هنری، بلکه هویت و مالکیت را هم به صورت مطلق بگیرند. شاید همین DAOها یک روز بتوانند جای حکومت‌ها را بگیرند و حقوق برابر شهروندی را برای همه افراد جامعه به صورت یکسان فراهم کنند. شاید همین DEFIها بتوانند فرصت‌های مالی برابری را برای همه آدم‌ها در هرکجای دنیا به وجود آورند و اگر همه‌ی این شایدها به حقیقت بپیوندد احتمالا ما به آن آرمان شهری که ادیان وعده‌اش را داده‌اند برسیم، جایی که دیگر اسکمری وجود نداشته باشد تا من بخواهم ۴ ساعت با موبایل برای شما در موردش تایپ کنم.

درست است که آموزش و توسعه‌ی مهارت‌های فنی به ما کمک می‌کند که کمتر گرفتار اسکم شویم، ولی قبل از رسیدن به آن مرحله از تخصص، می‌توانیم با داشتن نگاهی شکاکانه نسبت به تمام موقعیت‌های سرمایه‌گذاری در حوزه‌ی کریپتوکارنسی‌ها خودمان را تا حد امکان از این خطر حفظ کنیم.

"هرجا پیشنهاد وسوسه کننده بود، شک کنید"

Janbal

کیف پول سیف پال موجود شد

قیمت: ۲/۸۳۰/۰۰۰

www.janbal.io

janbal.io

SafePal S1
Hardware
Wallet

اخبار

اسکمرها حدود ۱۴ میلیارد دلار در سال ۲۰۲۱ از سرمایه‌گذاران سرقت کردند

علی‌رغم بحث‌های زیاد بر سر بازی Crypto Cars، سرتیک اعلام کرده است که عنوان Rug Pull برای این پروژه درست نیست

سال گذشته بیش از ۹۵,۰۰۰ نفر گزارش دادند که حدود ۷۷۰ میلیون دلار به دلیل طرح‌های کلاهبرداری کریپتویی در رسانه‌های اجتماعی از دست داده‌اند

کلاهبرداران در سال ۲۰۲۱ چهارده میلیارد دلار کریپتو سرقت کردند

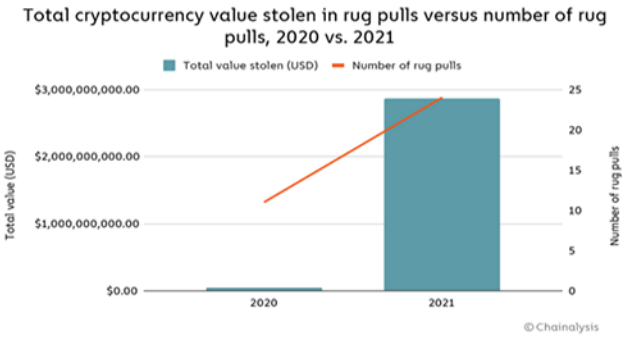
با گزارش جدیدی که نشان می‌دهد کلاهبرداران در سال گذشته ۱۴ میلیارد دلار رمزارز را تصاحب کردند، جرایم رمزارزها در سال ۲۰۲۱ رکوردشکنی کرد.
بر اساس «گزارش Crypto Crime ۲۰۲۲ Report» شرکت داده‌های بلاک‌چین Chainalysis که روز پنجشنبه ۶ ژانویه منتشر شد، این تقریباً دوبرابر ۷/۸ میلیارد دلاری است که کلاهبرداران در سال ۲۰۲۰ سرقت کردند.

ویلیام ای. کویگلی، سرمایه‌گذار برجسته و یکی از بنیان‌گذاران زنجیره بلوکی WAX می‌گوید با رونق علاقه به رمزارزها در سال گذشته، جای تعجب نیست که «کلاهبرداران در سطح المپیک» به فرصت‌های جدیدی برای فعالیت‌های غیرقانونی توجه کرده باشند.
کوئیگلی در طی یک میزگردی که ماه گذشته توسط شرکت بلاک‌چین Light Node Media برگزار شد، گفت که ماهیت تکنولوژی بالای کریپتو به جذب کلاهبرداران پیچیده ادامه خواهد داد.
یک کلاهبرداری اخیر «بازی ماهی مرکب» را در نظر بگیرید که در آن سرمایه‌گذاران ادعا می‌کنند رمزارز جدید SQUID و یک بازی آنلاین همه‌جانبه مرتبط در واقع فقط یک کلاهبرداری بوده است.
سرمایه‌گذاران ادعا می‌کنند که توسعه دهندگان پس از افزایش سرسام‌آور قیمت رمزارز ناپدید شدند و ظاهرا با بیش از ۳ میلیون دلار پول فرار کردند.

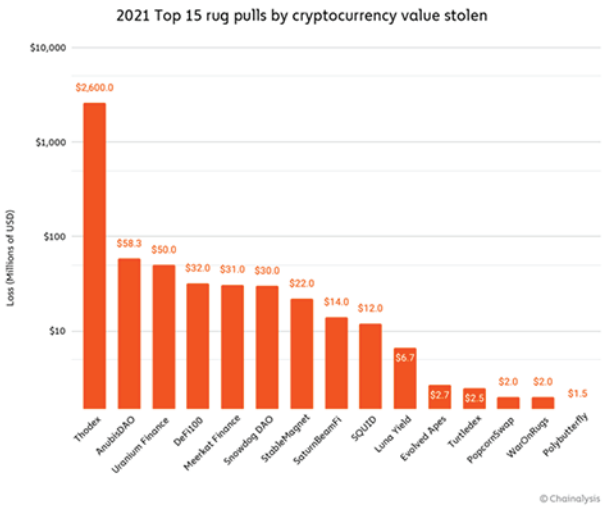
اخبار

کلاهبرداری 'Rug Pull' در دیفای امسال ۲/۸ میلیارد دلار به دست آورد

«راگ پول» ۳۷ درصد از کل درآمد کلاهبرداری را در سال جاری به خود اختصاص داده است در حالی که این میزان در سال ۲۰۲۰ تنها ۱ درصد بوده است.



Thodex صرافی کریپتو ترکیه‌ای پس از ناپدید شدن بنیانگذاران با بیش از ۲ میلیارد دلار وجوه مشتری در آوریل ۲۰۲۱، ، در رتبه اول قرار گرفت.
پس از آن AnubisDAO با الهام از dogecoin با ۵۸ میلیون دلار و صرافی مبتنی بر زنجیره هوشمند بایننس اورانیوم فاینانس ۵۰ میلیون دلار قرار دارند نام های دیگر این لیست مانند Meerkat Finance و Evolved Apes، تا Polybutterfly را شامل می شود



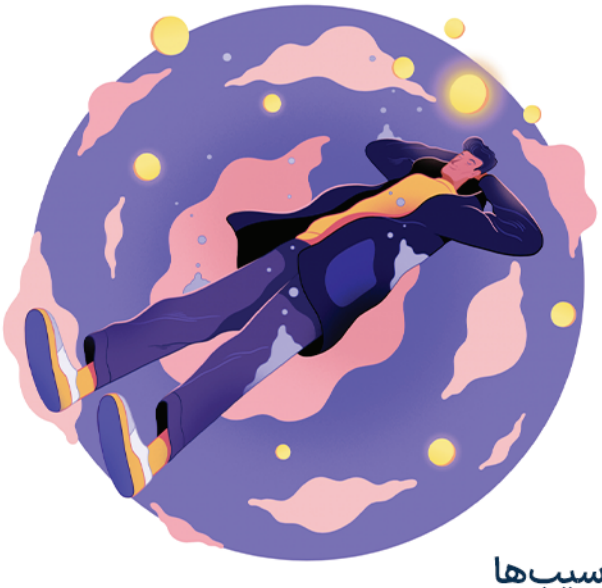
کت و شلوارهای توخالی

مهدی / @MahdiSD007

« تا حالا خوابی دیدی که یقین داشته باشی کاملا واقعیه؟
چی میشد اگه نمی‌تونستی از اون خواب بیدار شی؟
در اون‌صورت، چطور می‌تونستی فرق بین «دنیای واقعی» و عالم رویا رو تشخیص بدی؟» (ماتریکس)
واژگان در گذر زمان دستخوش تحولات معنایی بسیاری شده و دایره‌ی مصادیق‌شان گسترده‌تر شود.
یکی از واژگانی که از روزهای آغازین پیدایش رمزارزها سکونت دائم در این دنیای جدید نو را اختیار کرده واژه‌ی « اسکم » است. اسکم در فارسی به «کلاهبرداری» برگردانده شده است. کالبدشکافی معنای کلاهبرداری، درنهایت ما را به ۳ عنصر در بطن معنای واژه‌ی اسکم می‌رساند: «تلاشی برنامه‌ریزی شده» برای «فریب دادن دیگری» به‌منظور «آسیب زدن به او».
برای تغییر دایره‌ی مصادیق یک واژه، کافیست که عناصر معنایی آن از منظری جدید مورد توجه قرار گرفته و تفسیری دیگر شوند. میان ساکنین دنیای رمزارزها، از میان این ۳عنصر، آنچه که بیشتر در کانون توجه قرار داشته «آسیب زدن» بوده است. اما چه آسیبی؟
آسیب مالی. به عبارت دیگر، در نگاه متداول، اسکم هر پروژه‌ای است که در تلاش برای فریفتن شما به منظور خالی کردن جیبتان باشد.

کت و شلوارهای توخالی

اما آیا «آسیب زدن» فقط به «آسیب مالی» ختم می‌شود؟ آیا نمی‌توان «آسیب روانی» را در ذیل مصادیق «آسیب» قرار داد؟
دلیل آنکه این روزها در میان توضیحات پدیدارشناسانه پیرامون اسکم با مفهوم «اسکم عشقی/عاطفی» هم روبرو می‌شویم چیست؟ درحقیقت، اگر موشکافانه‌تر نگاه کنیم، آنچه که درنهایت اسکم را دردناک می‌کند آثار روانی آن بر روی قربانی است، آثاری نظیر خشم، شرمساری، احساس گناه، بی‌اعتمادی و....
در این مقاله سعی دارم دو پدیده‌ی «پکیج‌فروشی» و «سیگنال‌فروشی» را از همین منظر آسیب‌های روانی مورد توجه قرار دهم تا ببینیم آیا می‌توان درنهایت این دو را بعنوان مصادیقی از اسکم برشمرد یا نه.
پیش از شروع، لازم است با تعریف «پکیج‌فروشی» منظور دقیق خود از این پدیده را روشن کنم. بی‌تردید، آموزش آنلاین و پکیج‌های آموزشی یکی از ذاتیات دنیای پساکرونایی شده است.
لذا روی صحبتم با عزیزانی که (اولا) ثمره‌ی تلاش علمی خود را در قالب پکیج عرضه کرده، (ثانیا) در قبال نواقص و ایرادات پکیج‌های خود رفتاری مسئولانه داشته و (ثالثا) پکیج‌های خود را با توسل به رانت تبلیغاتی و دادن وعده‌های دروغین به مخاطب عرضه نمی‌کنند، نبوده و نیست.
منظورم از «پکیج فروشی» پدیده‌ای است که در آن «رایگان‌ترین آموزش‌ها» با «گران‌ترین قیمت‌ها» به کمک «وعده‌های دروغین تبلیغاتی» توسط فرد یا افراد «غیرمسئول» به مخاطب عرضه یا به تعبیر بهتر «انداخته» می‌شوند.



آسیب‌ها
ترسیم تصویرنادرست از بازار

«تصویر ما را اسیر می‌کند و نمی‌توانیم از آن بیرون شویم، زیرا در زبان ما نهفته است و زبان سرسختانه آن را برای ما تکرار می‌کند» (ویتگنشتاین)

نداشتن تصویر مطابق با واقعیت از هر پدیده‌ای باعث می‌شود که در تعامل با آن دچار اشتباهات بسیار شویم.
نداشتن درکی درست از جهان و روابط علّی-معلولی حاکم بر آن، نیاکان ما را قرن‌ها به‌سمت تفاسیر اسطوره‌محور و خیالی از پدیده‌های جهان کشانده بود.
لذا، پیش‌شرط ضروری برای عملکرد صحیح، داشتن «تصویری واقعی» از شرایطی‌ست که در آن هستیم که اگر قفس برای پرنده قفس ترسیم شود (نه دشت و صحرا)، پرنده با زدن خود به درب و دیوار قفس زخمی و ملول نمی‌شود.
«پکیج‌فروشان» با دادن وعده‌هایی نظیر «تریدر حرفه‌ای، راز کسب موفقیت در بازار، درآمد بالا از دنیای رمزارزها و...»، این ذهنیت را در تازه‌واردان ایجاد می‌کنند که با دانش تکنیکال به کسب درآمدی مستمر دست خواهند یافت.
اما با ورود به دنیای ترید متوجه می‌شوند که بین «برهوت واقعیت بازار» و آنچه که اینان (مستقیم یا غیرمستقیم) به وی تلقین کرده‌اند تفاوت بسیاری وجود دارد.

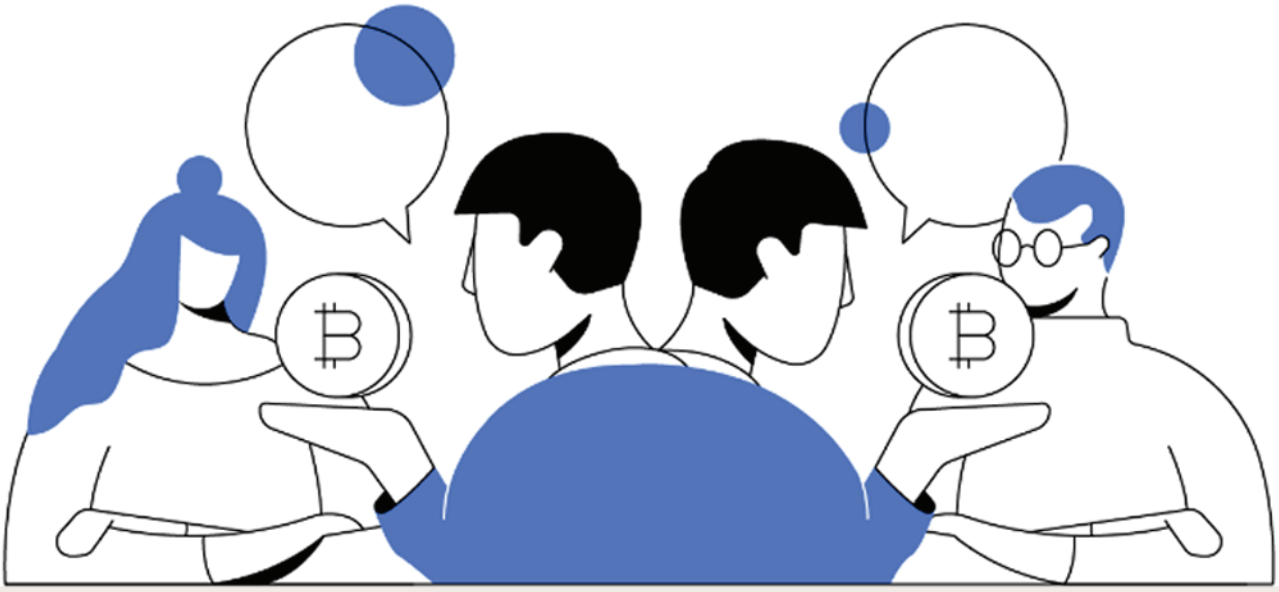
کت و شلوارهای توخالی

در پکیج‌ها صحبتی از استرس‌ها، اضطراب‌ها، عدم قطعیت‌ها و ریزش‌های یکباره‌ی بازار نیست. در آنجا صحبت به گونه‌ای است که گویا با شکسته‌شدن یک خط روند، یک کانال، یک مقاومت یا حمایت و... می‌توان وارد ترید شد.
تازه‌وارد ساعت‌های متوالی از عمر خویش را در حباب آرزوهایش فارغ از این که آیا اصلا این مباحث به روز هستند یا نه و آیا جای دیگر به‌صورت رایگان عرضه شده‌اند یا نه - صرف مرور پکیج‌ها می‌کند و به قول تامس هریس: «چه حماقتی! از اینکه تمام زندگیمان هدر رود در هراسیم، اما از اینکه هر روز تکه‌تکه‌ی آن را دور بریزیم ابایی نداریم»
کانال‌های سیگنال نیز از یک‌طرف با دادن سیگنال‌های پی‌درپی (در تمام تایم‌فریم‌ها/ اسپات یا فیوچرز)، به مخاطبی که هیچ درکی از مفاهیمی مثل «ریسک به ریوارد» ندارد و از طرف دیگر با پررنگ جلوه دادن سیگنال‌های موفق خود - البته اگر اساسا حتی سیگنال‌های تارگت خورده‌ی آنها را با توجه به ریسک به ریواردشان موفق بدانیم - وی را در یک سراب ذهنی نسبت به مارکت فرو می‌برند. سرابی که بشارت کسب درآمدی خوب و مستمر (به کمک چند ابزار تکنیکال و آشنایی با چند سایت آماری) را به او می‌دهد. این درحالیست که باتجربه‌ها به خوبی می‌دانند که بهترین تحلیلگرها می‌توانند بدترین تریدرها باشند.

فشـــارهای روحی

«فردی در اتاقی گرفتار است، در قفل نیست، اما او هرگز به ذهنش نمی‌رسد که به جای فشار دادن، باید در را به‌سمت داخل بکشد» (ویتگنشتاین)

حالا تازه‌واردی که با ذهنی پر از مفاهیم و توهمات وارد فضای بی‌رحم بازار شده، در هرتلاش با شکست مواجه می‌شود. استاپ‌لاس‌های خورده شده، ریزش‌ها یا صعودهای ناگهانی بازار، لیکوئیدشدن‌ها و... هر روز بر اضطراب و فشارهای روانی او می‌افزایند و او هربار از خود می‌پرسد: چرا هرچه دقیق‌تر خطوط روند، مقاومت‌ها و حمایت‌ها را رسم می‌کنم باز هم موفق نمی‌شوم؟
دیگر نه پکیج‌فروش و نه حاتم سیگنال بخش، هیچ‌کدام پاسخگوی سؤالاتش نیستند.
اکنون او مانده و تلاش‌های مذبوحانه‌ای برای یافتن تایم‌فریم مطلوب، استراتژی موفق و... حال آن‌که نمی‌داند «بازار بیش از آنکه بازی خطوط باشد بازی روانیست» و هر سیستم معاملاتی (از اسکَلپ تا هولد) وضعیت روانی خاص خودش را طلب می‌کند.
و «تغییردادن این ذهنیت» مانند هر ذهنیت راسخ دیگری، اگر ناممکن نباشد درنهایت سخت است.



دابل اسپـندینگ

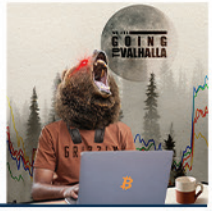
«یک بار به من آسیب بزن: شرم بر تو؛ دوبار به من آسیب بزن: شرم بر من» (ریچل سیمونز)

من این اصطلاح فنی را برای اشاره به این واقعیت تلخ استخدام می‌کنم که تازه‌وارد گرفتار شده در چنگ این دو گروه، دوبار ضرر مالی می‌دهد، یک بار با پرداخت پول گزاف برای خرید پکیج و سیگنال، و بار دیگر با تقدیم سرمایه‌ی خود به بازارسازان بازار.

خـــاتمه

«به من از حقایق مگو، به‌جایش برایم داستان بگو، داستانت را به مردمی بگو که دوست دارند باورش کنند، بازاریابی ابزار قدرتمندی است، خردمندانه از آن بهره‌گیر، دروغ را زندگی کن» (ست گادین)

سخن بیش از این‌هاست اما همین توضیح مختصر کافیست تا این دو پدیده را هم به مصادیق کلمه‌ی اسکم اضافه کنیم. همانطور که کسب توانایی علمی برای تحلیل فنی پروژه‌ها و تشخیص موارد اسکم لازم و ضروریست، «تحلیل روانی و رفتارشناسی» این کاسبان و بازاریابان نیز برای حفاظت از خود در برابر دام‌های از جنس «لبخندها، ماشین‌ها و دفاتر لاکچری؛ نیکوکاری‌های مزورانه؛ سیگنال‌بخشی‌های حاتمانه و وعده‌های دروغین همراهی با دانشجویان‌شان اهمیت بسزایی دارد، که اولاً «خالی کردن ذهن» از توانایی شفاف اندیشیدن هیچ‌گاه گناهی کمتر از «خالی کردن جیب» نبوده و نیست و ثانیا برای شناختن «علی حسنی»ها آشنایی با «تاریکی» لازم است.



انواع اسکم و کلاهبرداری در دنیای کریپتوکارنسی

گریزلی /@GrizzlyBTClover

بازار رمزارزها یک فرصت سرمایه‌گذاری مشروع اما پرخطر است، در واقع یک سرمایه‌گذاری بسیار سوداگرانه است، بنابراین همانطور که می‌توانید در آن بسرعت پول زیادی کسب کنید می‌توانید با سرعت بالاتری پول بیشتری را از دست بدهید.
یکی از مخاطرات بزرگ این دنیا، خطر کلاهبرداری یا اسکم است. اسکمرها از انواع ترفندها برای دست‌یابی به پول شما بهره می‌گیرند، از هک کردن حساب‌هایتان گرفته تا ایجاد کوین‌های کاملا جعلی، و با افزایش محبوبیت رمزارزها، هم شیوه‌های کلاهبرداری متنوع شده و هم تعداد آنها افزایش می‌یابد.

انواع کلاهبرداری با رمزارزها

اکثر مردم واقعا نمی‌دانند که رمزارز چیست یا چگونه کار می‌کند و این جهل فرصتی عالی برای کلاهبرداران ایجاد می‌کند.
این روزها علاقه‌ی زیادی به سرمایه‌گذاری در بازار رمزارزها دیده می‌شود، اما درک کمی از نحوه‌ی کارکرد آنها در میان این علاقه‌مندان وجود دارد.
ادعاهای کلاهبرداران باورپذیرند زیرا که سرمایه‌گذاران نمی‌دانند چه چیز واقع‌بینانه و چه چیزی غیرواقعی است.
اشکال مختلفی از کلاهبرداری در دنیای رمزارزها وجود دارد که می‌تواند سرمایه‌گذاران را به دام بیاندازد.
مجله‌ی FTC و Entrepreneur از این ۷ مورد به عنوان رایج‌ترین شیوه‌های کلاهبرداری که باید مراقب آنها بود نام برده است.

۱- هک کردن

هکرها همواره راهی برای نفوذ به بخش‌های مختلف بازار رمزارزها مانند صرافی‌ها، کمپانی‌های استخراج و کیف پول‌ها و ... پیدا کرده‌اند.
از آنجا که حساب‌های رمزارزی تحت پوشش بیمه‌ی FDIC قرار نمی‌گیرند، وقتی که دارایی‌ها از دست بروند، معمولا دیگر راهی برای بازگرداندن آنها وجود ندارد.
موارد زیر برجسته‌ترین هک‌های رمزارزی تا به امروزند:

- هک Mt. Gox در سال ۲۰۱۴ که در آن از یک صرافی رمزارز مستقر در توکیو ۴۶۰ میلیون دلار پول نقد و بیتکوین به سرقت رفت.

- هک DAO در سال ۲۰۱۶ که در آن یک شرکت سرمایه‌گذاری خطرپذیر فعال بر روی بلاک‌چین اتریوم، ۳/۶ میلیون اتر به ارزش تقریبی ۷۰ میلیون دلار را از دست داد.

- هک Bitfinex در سال ۲۰۱۶ که در آن یک صرافی مستقر در هنگ‌کنگ بیش از ۶۰ میلیون دلار بیتکوین خود را از دست داد.

- هک NiceHash در سال ۲۰۱۷ که در آن هکرها به سیستم پرداخت یک شرکت استخراج بیتکوین اسلوونیایی نفوذ کرده و ۶۴ میلیون دلار را سرقت کردند.

- هک Coincheck در سال ۲۰۱۸ که در آن هکرها نزدیک به ۵۰۰ میلیون دلار توکن را از یک صرافی مستقر در توکیو به سرقت بردند.

مهم‌ترین اقدامی که برای محافظت خود می‌توانید انجام دهید این است که تمام تخم‌مرغ‌های خود را در یک سبد قرار نداده و پس‌انداز زندگی خود را در هیچ صرافی نگهداری نکنید.

۲- سرمایه‌گذاری‌های جعلی

در این مورد، کلاهبرداران سایت‌های جعلی‌ای را برای سرمایه‌گذاری یا استخراج رمزارزها راه‌اندازی می‌کنند. آنها روش‌های مختلفی برای جذب قربانیان به این سایت‌ها دارند که در ادامه به برخی از آنها اشاره می‌کنیم.

برخی اوقات آنها به عنوان سرمایه‌گذارانی ظاهر می‌شوند که نکاتی را به‌صورت آنلاین به اشتراک می‌گذارند.

در موارد دیگر، ایمیل‌هایی از طرف «مدیران سرمایه‌گذاری» ارسال می‌کنند تا قربانیان را به سرمایه‌گذاری در این زمینه مجاب کنند.

تبلیغ فرصت‌های سرمایه‌گذاری در رمزارزهای جعلی می‌تواند قربانیان بالقوه‌ای را از طریق رسانه‌های اجتماعی جذب کند.

یکی دیگر از شگردهای این کلاهبرداران برقراری روابط ساخته‌گی در سایت‌های دوست‌یابی است که در بستر یک رابطه‌ی عاشقانه‌ی آنلاین، قربانیان خود را فریب داده و آنها را جذب می‌کنند.

از دیگر شگردهای سایت‌های سرمایه‌گذاری دادن وعده‌های بازدهی کلان است.

در اینجا برای قانونی جلوه دادن خویش از گواهینامه‌های جعلی استفاده می‌کنند.

گاهی اوقات این سایت‌ها چندین لایه سرمایه‌گذاری را با ادعای بازدهی بیشتر برای سرمایه‌گذاری‌های بزرگ‌تر پیشنهاد می‌دهند. در این حالت قربانیان متقاعد می‌شوند که به فرصت خوبی برای کسب سود دست یافته‌اند.

در برخی موارد، این سایت‌ها سرمایه‌گذاران را برای سال‌ها تحت فشار قرار می‌دهند. آنها به صورت دوره‌ای گزارش‌هایی جعلی برای قربانیان ارسال می‌کنند تا به آنها نشان دهند که چگونه «سرمایه‌گذاری‌شان» در حال رشد است.

اما اولین باری که قربانی سعی به برداشت آن وجوه کند، متوجه می‌شود که سرمایه‌اش از دست رفته است. بدتر از آن، زمانی است که صاحبان سایت آنها را متقاعد کرده که باید برای دسترسی به پول خود «هزینه‌ی برداشت» (کارمزد تراکنش) بپردازند و در ازای آن چیزی به آنها ندهند.

۳- کلاهبرداری با ادعای ارسال هدیه

در اینجا کلاهبرداران در لباس افراد مشهور یا سرمایه‌گذاران معروفی ظاهر می‌شوند که قصد دارند به سرمایه‌گذاران کوچک کمک نمایند.

آنها مدعی می‌شوند که اگر رمزارز خود را برایشان بفرستید، مقداری از دارایی رمزارزی خود را به سرمایه‌ی شما اضافه کرده تا به چند برابر شدن سرمایه‌گذاری‌تان کمک کنند.

در واقع، هر پولی که برای آنها ارسال می‌کنید مستقیما به جیب کلاهبرداران می‌رود. طبق گزارش FTC، در یک دوره‌ی شش‌ماهه، کلاهبردارانی که خودشان را ایلان ماسک معرفی کرده بودند، توانستند بیش از ۲ میلیون دلار رمزارز از قربانیان خود به سرقت برند.

۴- پیشنهاد شغل‌های ساختگی

برخی از کلاهبرداران سعی نمی‌کنند که شما را متقاعد کرده تا پول خود را وارد بازار رمزارزها کنید. در عوض، آنها به شما شغلی را پیشنهاد می‌کنند. آنها پیشنهاد مشاغل جعلی خود را در وب‌سایت‌های استخدامی پست می‌کنند تا افرادی را برای استخراج رمزارزها، فروش آنلاین آنها، جذب سرمایه‌گذاران و یا کمک به خرید بیتکوین، پیدا کنند. اما آنچه بعدا اتفاق می‌افتد متفاوت است. در برخی موارد، کلاهبرداران برای ثبت و بررسی درخواست‌تان از شما هزینه‌ای دریافت می‌کنند، سپس پول و در پاره‌ای اوقات حتی اطلاعات شخصی‌تان را نیز به سرقت می‌برند.

۵- کلاهبرداری ICO

عرضه اولیه کوین یا ICO، راه‌اندازی یک رمزارز جدید است. یک فرصت هیجان‌انگیز برای سرمایه‌گذاری در پروژه‌ای است که ممکن است بیتکوین بعدی شود.
سرمایه‌گذاری در ICOها همیشه خطرناک است زیرا هیچ راهی برای پیش‌بینی عملکرد کوین جدید وجود ندارد. اما برخی از ICOها فقط خطرناک نیستند. آنها کاملا کلاهبرداری‌اند.
دو نوع کلاهبرداری ICO وجود دارد. برخی مواقع این کلاهبرداری به کمک یک توکن کاملا جعلی محقق می‌شود.
مجرمان چیزی شبیه به یک آلت‌کوین جدید ایجاد می‌کنند و آن را با هیاهوی زیادی عرضه می‌کنند. سپس به سادگی هر پولی که سرمایه‌گذاران در آن می‌گذارند را به جیب می‌زنند.
نمونه‌ی بارز این مدل کلاهبرداری پروژه‌ی OneCoin بود که طبق گزارش بی‌بی‌سی بیش از ۴ میلیارد یورو از سرمایه‌گذاران سراسر جهان به دست آورد.
در موردی دیگر کمیسیون بورس و اوراق بهادار ایالات متحده عرضه‌ی اولیه‌ی ۱۵ میلیون دلاری PlexCoin را تعطیل کرد و آن را یک «کلاهبرداری سایبری تمام‌عیار» خواند.

نوع دیگر کلاهبرداری در ICO به این شکل است که کلاهبرداران یک رمزارز قانونی را که دارای یک ICO واقعیست، جعل می‌کنند. آنها یک وب‌سایت جعلی یا حساب رسانه‌ای اجتماعی ایجاد کرده و با کمک ایمیل‌های فیشینگ حاوی پیشنهاد «پیش‌فروش» سعی در جذب قربانیان خود می‌کنند. سرمایه‌گذاران با خیال اینکه باید هرچه زودتر از این فرصت بهره بگیرند اقدام به سرمایه‌گذاری می‌کنند، غافل از اینکه با این کار سرمایه‌ی خود را دودستی تقدیم کلاهبرداران کرده‌اند.
در چنین مواقعی از سایت‌هایی مانند CoinDesk کمک بگیرید تا مطمئن شوید که آیا ICO پیشنهاد شده قانونی است یاخیر. درضمن مراقب ایمیل‌ها و پست‌های رسانه‌های اجتماعی که فرصت خرید اولیه را به شما می‌دهند، باشید.
- SEC با راه‌اندازی سایتی به نام HoweyCoins نکاتی را در مورد سوالاتی که هنگام بررسی یک ICO باید پرسیده شود مطرح کرده و از این طریق به سرمایه‌گذاران در مورد علائم هشداردهنده‌ی کلاهبرداری در ICO آموزش داده است.

۶-کیف پول‌های جعلی

در این شیوه کلاهبرداران کیف پول جعلی خود را به صورت آنلاین و یا در فروشگاه‌های اپلیکیشن موبایل عرضه می‌کنند.
آنها کلید اصلی این کیف پول‌ها را پیش خود نگه داشته تا بتوانند به تمام رمزارزهای ذخیره شده در آن دسترسی داشته باشند. داستان کیف پول بیتکوین گلد ۲۰۱۷ مثال خوبی از این مدل کلاهبرداریست.
یک هکر باهوش، سازندگان بیتکوین گلد را متقاعد کرد تا سایت mybtgwallet.com را برای ذخیره‌ی رمزارز خود تبلیغ کنند. سپس سازنده‌ی این سایت بیش از ۳ میلیون دلار بیتکوین و بیش از ۲۰۰هزار دلار از رمزارزهای دیگر را به سرقت برد. امن‌ترین روش این است که بیشتر سرمایه‌ی خود را در کیف پول "سردی" که به اینترنت متصل نیست نگهداری کنید و دارایی خود را تنها زمانی از آنجا به کیف پول «گرم» متصل به اینترنت خود انتقال دهید که قصد معامله‌ی آن را داشته باشید.

۷- بدافزار سرقت بیتکوین

بدافزارها انواع مختلفی دارند، از میان آنها می‌توان به ویروس‌هایی که باعث آسیب جدی به سیستم شما می‌شوند، نرم‌افزارهای جاسوسی که اطلاعات شخصی شما را می‌دزدند و باج‌افزارهایی که دستگاه شما را به‌نوعی گروگان نگه می‌دارند، اشاره کرد. بسیاری از بدافزارها به طور خاص و با هدف سرقت رمزارزها طراحی شده‌اند.
این برنامه‌ها می‌توانند اعتبار ورود به حساب‌های رمزنگاری شما را ضبط کنند، کل دارایی کیف پول شما را بدزدند و یا زمانی که وسط انجام تراکنش هستید وارد حساب شما شوند.
یکی از جدیدترین برنامه‌های بدافزار سرقت رمزنگاری، WeSteal است.

به گفته‌ی Palo Alto Networks، این بدافزار با جستجوی کلیپ بورد شما برای یافتن الگوهایی که با شناسه‌های کیف پول بیتکوین یا اتریوم شما مطابقت دارند، تلاش کرده و سپس آن شناسه‌ها را با یک کد جدید جایگزین می‌کند. حالا هر زمان که شما معامله‌ای انجام دهید، پول به جای کیف پول واقعی‌تان به این کیف پول جعلی جدید منتقل می‌شود.

برای محافظت از رایانه‌ی خود در برابر این نوع بدافزارها، همان اقدامات پیشگیرانه‌ای که در برابر هر تهدید دیجیتال دیگری می‌کنید در پیش بگیرید.
از یک برنامه‌ی آنتی‌ویروس خوب به‌همراه فایروال برای محافظت از داده‌های ورودی و خروجی خود استفاده کنید. از سیستم خود با رمزهای عبور قوی یا یک مدیر رمز عبور مانند Keeper محافظت کنید. همچنین می‌توانید از VPNهایی مانند NordVPN استفاده کنید تا اتصال اینترنتی واقعی خود را مخفی نگه دارید. اگر می‌خواهید کاملا ایمن باشید، حتی می‌توانید یک رایانه‌ی جداگانه و اختصاصی داشته باشید که کاری جز ورود به حساب‌های رمزنگاری شما انجام نمی‌دهد.

گاهی وقت‌ها دستگاه‌های ماینر دچار مشکلاتی می‌شن که منشا نرم‌افزاری داره و نیاز به تعمیر دستگاه یا متخصص تعمیرات نداره ولی شما باید با مراحل عیب‌یابی یا شناخت عیب‌های نرم‌افزاری ماینر آشنایی کامل داشته باشین تا بتونید خودتون مشکل رو شناسایی و برطرف کنین.

در پیج هش‌بان پست‌های آموزشی و کاربردی برای عیب‌یابی و رفع مشکلات نرم‌افزاری دستگاه ماینر وجود داره که می‌تونین با اون آموزش‌ها مشکلات نرم‌افزاری یا ابتدایی ماینر خود رو بدون هزینه برطرف کنین.

برای دیدن این آموزش‌ها حتما پیج هش‌بان رو دنبال کنید.

hashabancom

هش‌بان

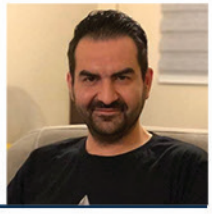
تعمیرات تخصصی ماینر

WWW.HASHBAN.COM

بدون هزینه درستش کن

hashabancom

۰۲۱-۴۴۰۰۰۶۶۴



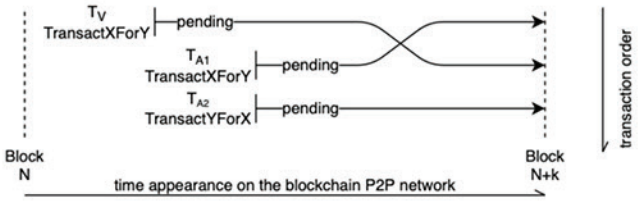
حمله ساندویچ در Defi چیست و چگونه باید از آن جلوگیری کرد؟

یاشار راشدی /@yashar_rashedi

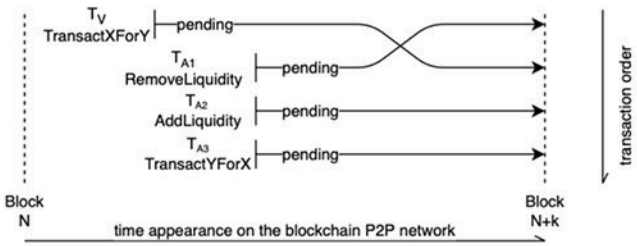
«حمله ساندویچ» نوعی از حمله در مارکت DeFi است که در آن حمله‌کننده، از خاصیت ساخته شدن بر پایه قرارداد هوشمند اپلیکیشن‌های غیرمتمرکز DeFi استفاده می‌کند که بر خلاف نام جذابش برای قربانی اصلا خوشایند نیست.

حمله ساندویچ دقیقا چیست؟

به طور ساده حمله ساندویچ به‌صورت احاطه کردن تراکنش کاربر میان دو تراکنش دیگر انجام می‌شود. یکی از این تراکنش‌ها قبل و یکی دیگر بعد از تراکنش کاربر انجام می‌شود و به همین علت به حمله ساندویچ معروف شده است. دلیل این نوع حمله، کسب سود برای حمله‌کننده با وارد کردن زیان به کاربر است که معمولا بر روی اکسچنج‌های غیرمتمرکز انجام شده و باعث دست‌کاری قیمت می‌شود.



Sandwich attack strategy 1, when liquidity taker attacks taker



Sandwich attack strategy 2, when liquidity provider attacks taker

حمله‌های ساندویچ به علت شفافیت تراکنش‌هایی که در mempool هستند و هنوز تأیید نشده‌اند و امکان slippage در DEXها وجود دارد قابل اجرا است.

حمله ساندویچ در Defi چیست و چگونه باید از آن جلوگیری کرد؟

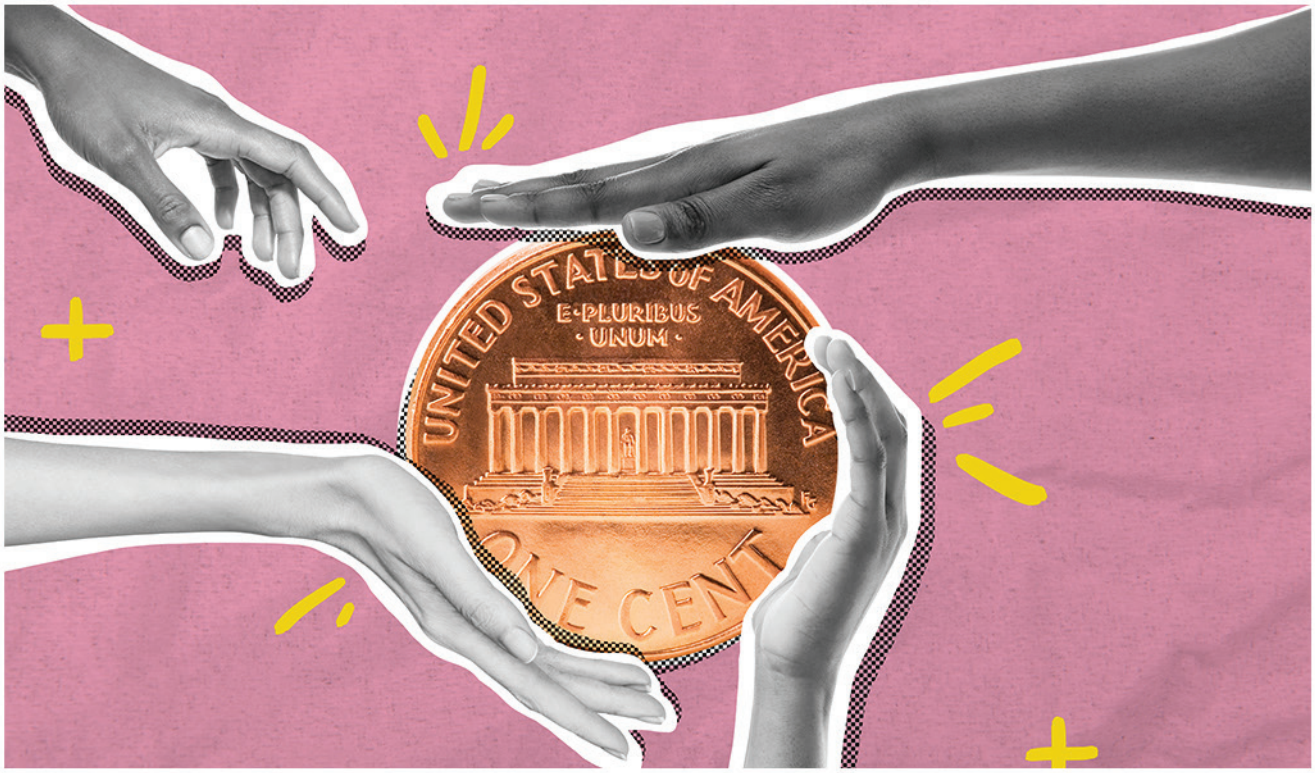
به طور خلاصه slippage پارامتری است که توسط کاربر قابل تنظیم است که در آن بین ۱ تا ۳ درصد نوسان در قیمت سفارش اجرا شده را نادیده می‌گیرد.
اکثر این حملات توسط ربات‌هایی که برای همین منظور برنامه‌نویسی شده‌اند انجام می‌شود و معمولا بر روی تراکنش‌هایی راحت‌تر انجام می‌شود که فی تراکنش پایین‌تر دارند.

آیا این نوع حمله برای حمله‌کننده سودآور است؟
با توجه به اینکه از لحاظ فنی انجام این نوع حمله خیلی کار پیچیده‌ای نیست، این نوع از حمله ممکن است سودآور باشد ولی نه خیلی زیاد، مخصوصاً در حال حاضر که DEXها تلاش می‌کنند راهکارهایی برای مقابله با این نوع حمله ایجاد کنند.

چگونه از شر این حملات در امان باشیم؟
ساده‌ترین راهکار قابل انجام از طرف کاربران، تعیین فی تراکنش به‌اندازه مناسب و بالا است که برای حمله‌کننده توجیه اقتصادی برای حمله وجود نداشته باشد.
راهکارهای دیگری توسط DEXها در حال پیاده‌سازی است که جزئیات سفارش‌ها را mempool مخفی می‌کند مثل استفاده از پروتکل‌هایی مانند ZK-Snarks است.
اکسچنج‌های غیرمتمرکزی مانند 1INCH هم در حال حاضر راهکاری به نام تراکنش‌های flashbot را پیاده‌سازی کرده است که باعث مخفی شدن جزئیات سفارش در mempool می‌شود.

در نظر داشته باشیم که پلتفرم‌های DeFi در مراحل اولیه خود هستند و همیشه حملات و راه‌های جلوگیری از آن‌ها ارائه خواهد شد و روزبه‌روز پیشرفت خواهند کرد.

دیدگاه دسته‌جمعی پول‌دار شدن



اولین و ساده‌ترین راه برای تشخیص یک کلاه برداری پیشنهاد عام‌المنفعه است. وقتی کسی از پروژه‌ای به شما خبر می‌دهد که در رابطه با آینده آن اطمینان صددرصد دارد، تنها یک برداشت از پیشنهاد ایشان باید داشته باشید: اینکه خود او یا افرادی که با آنها در ارتباط است این پروژه را کنترل می‌کنند.

نشانه بعدی پیشنهاد برای هولد بلندمدت است. ذات فروش چیزی که پشت آن هیچ ارزشی ذخیره نشده، کنترل عرضه و تقاضا با پیشنهاد هولد بلندمدت آن کوین یا توکن است.

نتیجه این است که شما و دسته‌ای که خرید کردید و هولدر کوین هستید تبدیل می‌شوید به گواهی رشد و افزایش قیمت پروژه و لایه بعدی از خریداران جذب می‌شود. این جذب لایه‌لایه‌ای تا جایی می‌تواند ادامه پیدا کند که طمع مالک پروژه اسکم و توانایی بازاریابی اجازه می‌دهد. به همین دلیل شما به‌صورت ضمنی در حال پول‌دار شدن هستید اما این طمع که از این هم بیشتر بخرید یا بیشتر نگه دارید باعث می‌شود که در آخر شما پول و سرمایه خود را از دست بدهید.

سیگنال

یکی دیگر از راه‌های جذب سرمایه برای پروژه‌های اسکم، سیگنال‌هایی است که در هزاران گروه و به‌صورت رایگان یا پولی در اختیار شما قرار داده می‌شود.

به شما پیشنهاد می‌دهم که این سؤال را از خود بپرسید: در بازاری که هفت روز هفته و ۲۴ ساعت شبانه‌روز در حال کار کردن است و همچنین از هر حرکت بازار، چه بالا چه پایین، امکان سود گرفتن هست، همین‌طور با ابزاری مثل وام‌ها و مارجین‌هایی که در اختیار شما قرار داده می‌شود، آیا من

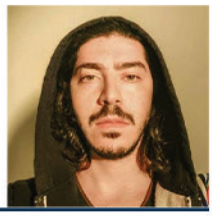
به‌عنوان کسی که تلاش برای سیگنال دادن دارم با تمرکز بر روی نهایتاً ۵ تا ۱۰ ارز، ماهانه صدها سیگنال برای شما نمی توانم صادر بکنم؟ اما وقتی یک پروژه در کانال‌ها سیگنال می‌شود رفتار دومینووار به این شکل است که ابتدا در گروه اصلی که نه من و نه شما هرگز عضو آن نخواهیم شد سیگنال خرید صادر می شود و بعد در گروهای زیرشاخه برای صدها هزار نفر سیگنال خرید صادر می شود، در نتیجه این رفتار، افرادی که خریدهای بسیار حجیمی در گروه اصلی کرده‌اند، به خریداران خردی که در کانال‌های سیگنال اوردر خرید می‌گذارند می‌فروشند و سود صددرصد عاید افراد اول می‌شود.

فاندامنتال

اگر فکر می‌کنید که چیزی که در کف تایم لاین آن را اخبار یا فاندامنتال می‌نامند ارزش سرمایه‌گذاری دارد سخت در اشتباهید. فاندامنتال و اخبار بنیادی یک ویژگی بدیهی دارند آن هم اینکه شما این اطلاعات را به‌صورت شخصی به‌مانند یک کارآگاه واکاوی می‌کنید و مهم‌ترین نشانه آن این است که شما نهایتا جزو ۵ درصد اول افرادی باشید که به این اطلاعات ارزشمند دستیابی پیدا کرده‌اید.
به‌عنوان‌مثال در موضوع سیگنال افرادی که در گروه اصلی هستند و در جریان تمام پروژه کلاهبرداری قرار دارند می‌توانند بگویند که رانت اطلاعاتی دارند و این اخبار برای آنها ارزنده است، حالا سوال اصلی اینجاست، آیا شما اگر عضو گروه اصلی باشید بلافاصله در تمام شبکه‌های اجتماعی شروع به جار زدن در رابطه با اتفاقی که قرار است رخ بدهد می‌کنید؟ پس این نتیجه را می‌توان گرفت که چیزی که به خورد شما در شبکه‌ها به عنوان اخبار فاندامنتال می‌دهند، چیزی جز اخبار پیش‌خور شده نیست و هدف فقط اضافه کردن شما به زنجیره تبلیغاتی پروژه است. البته که برای تمام مثال‌ها استثنا هم وجود دارد به‌عنوان مثال دیتای آنچین قابل دست‌کاری نیست و شما به‌صورت شخصی امکان استخراج آن را دارید پس اگر جای درست را هدف بگیرید زودتر از عموم به حقیقت پی می‌برید.
اما چیزی که به‌عنوان وایت پیپر یا رودمپ یا توکنمیک در دسترس عموم قرار گرفته در ابتدا امکان صحت‌سنجی آن وجود ندارد و در انتها بدانید که منتظر شما بوده پس برای تمام سوال‌های شما جواب مناسب آماده کرده است.

ذات تمام پروژه‌ها جذب سرمایه است

بعد از اینکه درگیر پیشنهادهای ساده‌لوحانه‌ای که در بالا توضیح داده شد نشدید، در جریان باشید که خطر هنوز رفع نشده و حربه‌های دیگری که برای افرادی که سرمایه‌شان را سخت‌تر خرج می‌کنند آماده شده است. در مجموع تمامی افرادی که در بازارهای مالی فعالیت می‌کنند دسته‌های متفاوتی را تشکیل می‌دهند که به این دسته‌ها "پرسونا" گفته می‌شود. پس اگر وارد این بازار شدید بدانید که پشت در بعدی همیشه یک پیشنهاد وسوسه‌انگیز برای شما در نظر گرفته شده که با تمامی پیشنهادهایی که تا حالا شنیده‌اید متفاوت است، اما همیشه در نظر داشته باشید که الگوی رفتاری و شخصیت هر فردی که در این بازار است به‌راحتی قابل تشخیص و برای هر کدام راهکاری وجود دارد. پس در نظر داشته باشید که این خطر هیچ‌وقت رفع نخواهد شد.



بررسی یک پروژه برای تشخیص کلاهبرداری

سینا / @sinazhr

بررسی پروژه ccar بر اساس مقاله شت‌کوین شناسی

قبلا مقاله‌ای تحت عنوان "شت‌کوین شناسی" و موارد هشدارآمیز هنگام بررسی یک پروژه کریپتو را در هفته‌نامه منتشر کرده بودیم. امروز قصد داریم یک پروژه کریپتو که در حال حاضر هم بحث کلاهبرداری آن مطرح شده را با هم بررسی کنیم.

به گفته صاحبین پروژه: CryptoCars از فیلم Cars الهام گرفته شده است - یک فیلم کمدی ورزشی پویانمایی کامپیوتری محصول ۲۰۰۶ آمریکا که توسط استودیوی انیمیشن پیسکار تولید شده و توسط والت دیزنی منتشر شده است. احتمالا اسم این پروژه را شنیدید و در جامعه فارسی هم تبلیغش توسط افراد مختلف انجام شده بود. پروژه‌ای که شما با بازی پول درمیارید. چه چیزی از این بهتر؟!

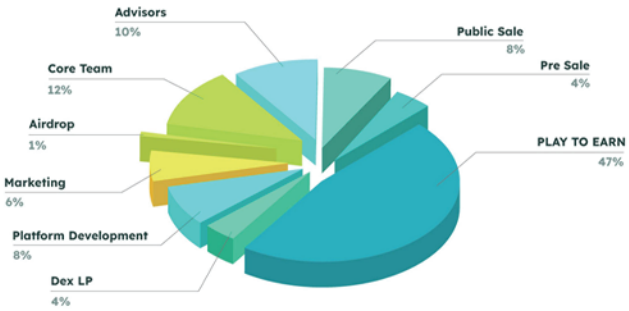
بررسی یک پروژه برای تشخیص کلاهبرداری

در حال حاضر توکن اصلی این بازی CCAR$ که بر بستر اسمارت چین باینینس ایجاد شده از اوج قیمتی ۱/۷ دلار به تنها حدود یک سنت رسیده است! گفته شده مدیر اصلی و برنامه‌نویسان، پروژه را رها کردند و حجم بالایی توکن در صرافی‌های غیرمتمرکز فروخته شده است (در اطلاعیه رسمی، تعطیلات عید در ویتنام دلیل این غیبت ذکر و گفته شده از ده روز دیگر برمی‌گردیم)
در اطلاعیه دیگری گفته شده قرار است توکن‌ها را تعویض کنیم و CCAR۲ را با یک میلیارد توکن ساخته‌ایم! مجدد ۸۰ درصد موجودی توکن در یک آدرس قرار گرفته است.
با whois دامنه اطلاعاتی به دست نمی‌آید لطفا مشخصات مخفی شده را اشتباهی راستی آزمایی نکنید. بر روی سروری که این وب سایت قرار دارد، حدود ۷۰ سایت دیگر مستقر هستند که نشان میدهد سایت حتی روی هاست اشتراکی بالا آمده و در حد یک سرور مجازی یا اختصاصی هم هزینه نشده است!

بررسی وایت پیپر (White paper)

وایت پیپر این پروژه (اگه بشه گفت) در قسمت مدل درآمدزایی به این صورت مطرح شده که شما ماشین می‌خرید و بعد با بردن بازی در سبک‌های مختلف درآمدزایی می‌کنید. مشکل اصلی چنین پروژه‌هایی زمانی رخ خواهد داد که بازیکن جدیدی وارد نشود (این بحران در اکثر بازی‌های مشابه قابل پیش‌بینی است) اما آیا طراحان برای کنترل چنین بحرانی رویکردی دارند؟ در وایت پیپر این پروژه هیچ اطلاعات دیگری نیست.

بررسی هولدرها و توکنومیک



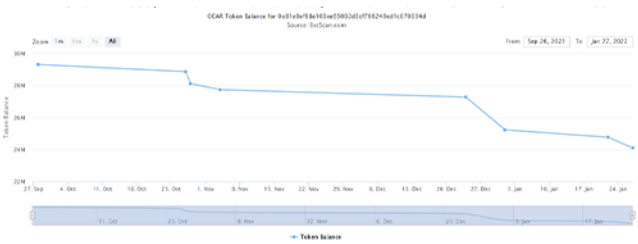
	Total Supply	Percent	Vesting Period
Advisor	10M	10%	No vesting plan
Core Team	12M	12%	25 months
Marketing	6M	6%	20 months
Platform Development	8M	8%	12 months
Airdrop	1M	1%	10 months
DEX Liquidity	4M	4%	
Public Sale	8M	8%	
Pre Sale	4M	4%	
Play to earn	47M	47%	
Total Amount	100M	100%	

طبق اطلاعاتی که در سایت این پروژه مطرح شده تنها ۸ درصد از توکن‌های این پروژه به صورت عمومی فروش می‌رود و بقیه تقریبا در مالکیت پروژه است!

به بررسی هولدرهای این توکن می‌پردازیم:

Rank	Address	Quantity	Percentage	Value
1	0x1063b64d4d8308be1662685d43f94f34b96d7108	32,608,566.587421721980403912	32.6086%	$497,623.03
2	KIPS: Locked Wallet	24,107,999.999999999957	24.1076%	$367,894.03
3	0x2304541016102a95efcee67759ad92518fa3fce677	10,000,000	10.0000%	$152,605.00
4	PancakeSwap V2: CCAR 3	9,399,255.997590896171625191	9.3995%	$143,437.35
5	Gate.io	6,451,730.370610059311554504	6.4517%	$98,456.63
6	0x55b24f8f6971ff6169941e76ef193dcdcbc7a4590b	531,584.601430260668546775	0.5316%	$8,112.25
7	0x9e31aef04094fe6735951f8648ca07c5ff22215e5	524,501.324312340628165571	0.5245%	$8,004.15
8	CryptoCars: CCAR Token	471,408.079685342747868906	0.4714%	$7,193.92

همانطوری که مشاهده می‌کنید حدود ۸۰ درصد توکن‌های پروژه در آدرس‌های مرتبط با پروژه یا صرافی هاست.



با بررسی یکی از آدرس‌های منتصب به تیم پروژه به نظر می‌رسد که حجم بالایی توکن در روزهای اخیر به صرافی پنکیک برده شده (حدود ۴ میلیون توکن) و به صورت کوین باینس در تراکنش های کوچک‌تر نقد شده‌اند!
این بلایی است که اکثر پروژه‌های با توکنومیک بد پتانسیلش را دارند. دامپ توکن‌های انبار شده بر سر خریدران ساده.

بررسی تیم پروژه

در بررسی وب سایت، شبکه‌های اجتماعی و ... هیچ اثری از اسامی اصلی تیم پروژه به چشم نمی‌خورد. مدیران در شبکه‌های اجتماعی همگی با اسامی ملقب هستند. چطوری امکان دارد بر روی پروژه‌ای که هیچ فردی ازش مشخص نیست سرمایه‌گذاری کرد؟ (بماند که خود این افراد و سوابقشان باید راستی‌آزمایی شوند) این برای پروژه حساسیت برانگیز هست که تیم مخفی شده یا افراد جهت کلاهبرداری مخفی شده‌اند؟

شرکای استراتژیک و مشاورین چه کسانی هستند؟
شریک؟ استراتژیک؟ مشاورین؟ فراموشش کن هیچکسی این پروژه را گردن نمی‌گیرد

نقشه راه

نقشه راه پروژه مواردی کلی و تا سه ماه دوم سال ۲۰۲۲ است، نکته جالب در نقشه راه، در سه ماه دوم سال ۲۰۲۱ کار برنامه‌نویسی پروژه شروع شده و سه ماه بعد فروش آغاز شده است!

حجم بازار و بررسی liquidity pool

با توجه به اینکه حجم بالایی از فروش پروژه بر روی صرافی‌های غیرمتمرکز است می‌توانیم با هم استخر نقدینگی پنکیک سواپ پروژه را بررسی کنیم. دو استخر نقدینگی برای توکن CCAR روی این دکس پیدا کردیم که در سایت dextools.io استخر اصلی را بررسی می‌کنیم:
استخر WBNB/CCAR که ۲۹۱,۰۵۴ دلار موجودی دارد که البته با اطلاعات پنکیک سواپ کمی مغایرت دارد (ولی موجودی کامل خالی نشده است)
نکته تاسف برانگیز دیگر ارزش این استخر در تاریخ ۲۵ نوامبر به بالای ۴ میلیون دلار رسیده بوده است! اقبال این حجم مالی به چنین پروژه‌ای نشان می‌دهد چه مقدار زیادی افراد ناآگاه در کریپتو در حال فعالیت هستند.

جمع بندی

هیچ اطلاعات مفید دیگری از طریق جستجو در گوگل، گیت‌هاب و... مشاهده نشد. متاسفانه وقتی در طول سال گذشته هشدار به کلاهبرداری‌های متعدد داده میشد، عده‌ای افراد هشدار دهنده را نادان و... خطاب می‌کردند که جلوی پول دار شدن کاربران را می‌گیرند!
هنوز هم پروژه‌های متعددی وجود دارد که پتانسیل انواع کلاهبرداری را دارند، برخی فکر می‌کنند روش کلاهبرداری در کریپتو فقط از طریق ساختن یه توکن و دامپش در همون ابتدا است. خیر، خیلی از پروژه‌های به ظاهر خوب هم خطر ناپدید شدن صاحبین یا خروج ناگهانی، دامپ کردن توکن ها بر سر هولدرها و یا حتی فریب و ادامه دادن وعده‌ها برای جذب بیشتر نقدینگی خواهند داشت.
مجدد تکرار می‌کنم حتی اگر رمزارزی در صرافی‌های متمرکز هم لیست شده باشند اما موارد متعددی نشانه‌های هشدارآمیز لیست را داشته باشند، خطر کلاهبرداری بسیار بالا خواهد بود.

If You Want To Donate Us

LNURL1DP68GURN8GHJ7MR9VA
JKUEPWD3HXY6T5WVHXXMMD9
AKXUATJD3CZ7CTSDYHHVVF0D3
H82UNV9UUNGWG7TSHAU

BTC
(Lightning)

BNB
(bep20)

USDT
(Trc20)

TOMO

XRP

Dogecoin

TRX

#18

SCAM — MONDAY

January 31 / 2022