پادکست استفان لیورا

قسمت ۲۹

کیف پول سامورایی
و ابزارهای حفظ حریم خصوصی در بیت‌کوین

Samourai Wallet

(این گفتگو در سال ۲۰۱۸ انجام شده است)

استفان:
سلام دوستان به برنامه ما خوش آمدید. این قسمت ۲۹ از پادکست استفان لیورا است. مهمان امروز من بسیار ویژه است. سایفرپانکی فوق‌العاده و توسعه‌دهنده ساموراییِ والت. به برنامه ما خوش آمدی.

سامورای:
ممنون، خوشحالم که اینجا هستم، من طرفدار پر و پا قرص پادکست شما هستم.

استفان:
خیلی ممنون. کاری که شما انجام داده‌اید را خیلی دوست دارم. برای شنوندگانی که اخیرا به ما پیوسته‌اند بگویم که، خیلی از افراد در فضای بیت‌کوین با نام مستعار فعالیت می‌کنند و از آنجایی که ما قصد نداریم اطلاعات کسی را فاش کنیم، اگر کسی با نام مستعار به برنامه ما بیاید، ما هم به خواسته‌اش احترام می‌گذاریم. خب عنوان یک مقدمه خیلی سریع بگویم که، والت ساموراییِ پروژه خیلی جالبی است و من برای مدتی آن را دنبال می‌کردم. والت را امتحان کرده‌ام، به نظر من والت بیت‌کوینی آسان و ساده‌ای است. توسعه‌دهنده‌های والت ساموراییِ از بحث و گفتگو فرار نمی‌کنند و موضع سخت‌گیرانه‌ای در زمینه حفظ حریم‌خصوصی دارند، و چنین نگرشی بسیار عالی است. می‌توانیم با توسعه ساموراییِ والت مباحث را شروع کنیم، ویژگی‌ها، اهداف و حریم خصوصی در ساموراییِ والت. در وبسایت شما این شعار را دیدم که «ما فعالان در زمینه حریم‌خصوصی هستیم که زندگی خود را وقف ساخت

نرم افزاری کرده‌ایم که سیلیکون‌ولی هرگز نخواهد ساخت، و قانون‌گذاران هرگز اجازه نخواهند داد و سرمایه‌گذاران هرگز روی آن سرمایه‌گذاری نخواهند کرد. ما نرم افزاری را ساخته‌ایم که شایسته بیت‌کوین است.» (دره سیلیکون در آمریکا، معروف به قطب کسب و کارهای اینترنتی. -م) کمی در باره این شعار برای ما صحبت کن.

سامورای:

بله، حتما. اما قبل از آن بگذارید روشن کنم که توسعه‌دهنده اصلی سامورایی آن کسی است که با نام کاربری @samuraiDev در توییتر است. من و توسعه‌دهنده سامورایی این پروژه را با هم شروع کردیم که به سال ۲۰۱۵ برمی‌گردد. ما با هم این شعار را نوشتیم که به نوعی ماموریت ما است. ما می‌خواهیم مطمئن شویم که هرچقدر پروژه بزرگتر می‌شود و هرچه افراد بیشتری از آن استفاده می‌کنند، به هدف اصلی خود وفادار بمانیم و این باعث می‌شود این پروژه ذاتاً برای هیچ سرمایه‌گذاری جذاب نباشد. البته هر دوی ما چه جدا جدا چه با هم، تجربه‌های منفی از سرمایه‌گذاران در گذشته داریم. به همین دلیل مطمئن شدیم که چنین چیزی را برای این نوع پروژه نمی‌خواهیم.

استفان:

درسته، من متوجه شده‌ام که شما عضو فریم‌ورک Zerolink هم هستید که ارائه‌دهنده نسخه‌ای از حریم خصوصی در بیتکوین است. یکی از مهمان های قبلی من Adam Fiscor ، مدیر فنی و توسعه‌دهنده ارشد والت واسابی است، که والت دیگری با تمرکز بر حریم خصوصی است که از فریم ورک ZeroLink استفاده

می‌کند. کمی در این باره بگو که به چه نحو باعث شکستن ارتباطات روی شبکه بلاکچین می‌شود و این موضوع چطور می‌تواند به حریم خصوصی کمک کند؟

سامورای:

خب ZeroLink یک فریم ورک عالی بود (فریم‌ورک یک ساختار مفهومی است که نرم افزارهای متفاوتی می‌توانند روی آن توسعه مخصوص خود را انجام دهند. – م). ادم فیسکور حدودا یک سال پیش یا کمی کمتر با ما تماس گرفت و از توسعه‌دهنده سامورایی خواست اگر بخواهد می‌تواند با فریم ورک همکاری کند. خب ما خیلی هیجان زده شدیم که کسی دستش را برای کمک دراز کرده و می‌خواهد با هم کار کنیم، خیلی خوشحال شدیم که میتوانیم در ZeroLink همکاری کنیم و سریع شروع به پیاده سازی کردیم. نرم‌افزاری که ما از فریم‌ورک ZeroLink ایجاد کردیم ویرلپول (Whirlpool) نام دارد که یکی از آخرین و جدیدترین ابزارها در مجموعه ابزارهای سامورای والت است. تمام این ابزارها برای شکستن ارتباطات در بلاک‌چین بیت‌کوین طراحی شده‌اند. شرکت‌های تحلیل بلاکچین سعی به اکتشاف ارتباط آدرس‌ها و اطلاعات دیگر روی شبکه بیت‌کوین دارند. من معمولا به این شرکت‌ها جاسوسان بلاک‌چین میگویم. اگر مفهوم کوین‌های لکه‌دار را قبول داشته باشید، (که من شخصا قبول ندارم) آن‌گاه این شرکت‌ها بعضی از تراکنش‌ها و خروجی‌های بیتکوین (utxo) در شبکه را لکه‌دار تشخیص می‌دهند. ما آمده‌ایم که وارد بازی شرکت‌های تحلیل بلاک‌چین شویم و مطمئن خواهیم شد که همه‌ی کوین‌ها لکه‌دار خواهند بود و هیچ کوین غیر لکه‌داری وجود نداشته باشد. این کار را با حمله به فرضیاتی که این شرکت های آنالیز کننده ایجاد کرده‌اند انجام میدهیم. والت‌های معمولی امکان تحلیل بر اساس فرضیات این شرکت‌ها را برایشان خیلی آسان کرده‌اند. سامورای والت با حمله به فرضیات این شرکت‌ها، شغل آن‌ها که تعیین لکه‌دار بودن و ایجاد لیست‌های سیاه است را سخت

می‌کند و به اصطلاح چوب لای چرخشان میگذاریم. این موضوع برای مفهوم fungibility (تعویض پذیری) بیت‌کوین بسیار مهم است. از نظر ایدئولوژیکی و از نظر کاربردی، اگر قابلیت تعویض پذیری نداشته باشیم ارزش بیت‌کوین به طور بنیادی پایین می‌آید.

استفان:

درسته. این شرکت‌ها به روش‌های بسیاری می‌توانند حریم خصوصی شما رو از بین ببرند، روش‌هایی که مستقیما در لایه تراکنش (شبکه بلاک‌چین) و بر اساس روش‌های کشف عمل می‌کنند. مثلا اگر چند UTXO در یک تراکنش ادغام شوند، شرکت‌های آنالیز کننده بلاکچین می‌توانند فرض کنند که بله این دوتا UTXO متعلق به یک نفر است. همچنین حملات در سطح شبکه هم وجود دارند. کمی در این باره بگو که چه ابزارهایی هستند که کاربر بتواند با انها از حریم خصوصی خود محافظت کند؟ در مورد زوایای مختلفی که کاربران باید در نظر داشته باشند، هر گونه ردی که می‌توانند روی شبکه از خود به جا بگذارند، درمورد روش‌های شناسایی و درباره حملات متعدد به حریم خصوصی برایمان بگو.

ساموررای:

همه این مسائل وجود دارند. اصلی ترین راهی که آنالیز کننده‌های بلاک‌چین اطلاعات موردنیاز جاسوسی خود را جمع‌آوری می‌کنند، در واقع با جمع‌آوری اطلاعات خارج از بلاک‌چین است. مثلا اطلاعاتی که در شبکه‌های اجتماعی منتشر می‌کنید، آدرس‌های از خودتان که در توئیتر یا انجمن‌های آنلاین قرار داده‌اید، همه اینها توسط این شرکت‌های جاسوسی بلاک‌چین در نظر گرفته و جمع‌آوری می‌شوند. پس فقط اطلاعات روی بلاک‌چین نیستند. همچنین از اطلاعات مرتبط به

شبکه اینترنت هم استفاده می‌کنند، اگر از یک سرویس VPN شناخته شده یا شبکه Tor استفاده کنید، همه این اطلاعات را در کنار هم قرار می‌دهند و یک پروفایل از شما می‌سازند. تمام اینها از گذشته دغدغه‌های مختلف امنیتی و حریم خصوصی بوده‌اند ولی تمرکز ما روی حریم خصوصی در بلاک‌چین است. به همین دلیل چیزی که سامورایی میخواهد روی آن تمرکز کند، این است که کاربران بتوانند تراکنش‌هایی را بسازند که مانع از شناسایی و مورد هدف واقع شدن آن‌ها بشود.

استفان:

منظورتون از مورد هدف واقع شدن چیست؟

سامورای:

فرض کنید که شما یک کاربر صاف و ساده بیتکوین هستید که تعدادی بیت‌کوین از شخصی دریافت کرده‌اید. فرضا اولین بیت‌کوین‌های شما هستند. این کوین‌ها ممکن است از دید شرکت‌های تحلیل بلاک‌چین لکه‌دار[1] به شمار بیایند، چون مثلا در ارتباط با هک اکسچنج مت‌گاکس(Mt.Gox) باشند. ممکن است چنین چیزی را تجربه کنید که آن لحظه ای که بیت‌کوین خود را به اکسچنجی انتقال دهید آن‌گاه شرکت‌های تحلیل بلاک‌چین وارد عمل می‌شوند و اکسچنج با این اطلاعات فراهم شده از شرکت‌های تحلیل بلاک‌چین تصمیم بگیرد فعالیت شما را متوقف و دارایی شما را مسدود کند. اینجا اولین تجربه شما کاملا منفی است در حالی که اشتباهی مرتکب نشده‌اید. هدف سامورایی جلو گیری از چنین اتفاق‌هایی است.

1 Tainted

استفان:

بله و مورد دیگری که تیم شما اخیرا انجام داده است، حذف معادل فیات (دلاری) در والت است که به نظرم اگرچه واقعا جنجال برانگیز است ولی در عین حال اگر بهش فکر کنیم واقعا چیز خوبی است. بیا کمی دراین باره حرف بزنیم. به نظر شما تحت فشار زیادی از طرف جامعه بیت‌کوین قرار گرفتید درست است؟

سامورای:

خیر در واقع. واکنش‌ها خیلی دلگرم کننده‌تر از چیزی بود که حدس می‌زدم. من فکر میکردم که خیلی آزار دهنده‌تر از این‌ها باشد. آنقدرها هم جدی نبود، ما تلاش نمی‌کردیم که یک کار بزرگ انجام دهیم، سعی نمیکردیم بگوییم که ما باید نوعی اقتصاد چرخه‌ای[۲] یا همچین چیزی داشته باشیم یا اینکه شما فقط و فقط باید به بیت کوین فکر کنید، چون این امر حقیقت دنیای واقعی اطراف ان نیست. همه افرادی که در سامورایی هستند، سالها است که برای بیت کوین کار می‌کنند و با بیت کوین زندگی می‌کنند. و ما مفهوم دنیای واقعی را میفهمیم و از آن در دنیای واقعی استفاده می‌کنیم. من با گذشت زمان متوجه شده‌ام که چیزی که دیگران همیشه می‌گویند این‌است که مشکل فهم بیت کوین در آموزش آن است و با این توجیه بی‌تفاوت از آن رد می شویم، انگار وقتی صحبت از کاربران جدید و نیاز آنها به یادگیری می رسد مشکل فقط در آموزش است. درست است مفاهیم شبکه بیت‌کوین بسیار پیچیده هستند اما مساله این است که کسی نیز آموزش نمی‌بیند. بسیاری کاربران هستند که پس از مدت‌ها فعالیت در این زمینه همچنان گاهی درک درستی از این موضوع ندارند. ما همیشه میگوییم مشکل آموزش است در حالی که مشکل این است که هیچ کسی آموزش نمی‌بیند و به این بهانه داشتن معادل فیات (دلاری) در والت بیتکوین، برای کاربرانی که هرگز نمی‌خواهند یاد

2 Circular economy

بگیرند مثل عصا عمل می‌کند و آن‌ها را به آموزش ندیدن تشویق می‌کند. ما کاربرانی داشته‌ایم که پس از ۱۰ ماه استفاده و یا حتی پس از یک سال استفاده از والت ساموراییی به پشتیبانی ایمیل می‌زنند و به معیار پول فیات درخواست پشتیبانی می‌کنند. مثلا می‌گویند من برای دوستم ۲۵۰ دلار فرستادم اما حالا ۳۷۵ دلار است. چه اتفاقی افتاده است؟ یا که مقدار اشتباهی را به موقع پرداخت در درگاه‌های خرید انتقال داده‌اند یا که مقدار اشتباهی را در والت دیگری فرستاده‌اند. یا خیلی اشخاص وقتی تراکنشی انجام می‌دهند و پس از مدت‌ها والت خود را باز می‌کنند، با مقدار دلاری کاملا متفاوتی مواجه میشوند و فکر می‌کنند که از انها کلاه‌برداری شده است. درست است که از یک کاربر جدید چنین انتظاری می‌رود ولی برای کاربری که ۱۲ ماه است فعالیت می‌کند چنین چیزی قابل قبول نیست. بنابر این منطق ما این است که ما یک والت دلاری نیستیم، ما یک والت فیات نیستیم، و از پشتیبانی از فیات در والت جلوگیری خواهیم کرد و برای تعیین قیمت به پذیرندگان تراکنش اتکا می‌کنیم. چیزی که به هر حال عملا رایج است. دلیل بیشتر سر در گمی‌ها این بود چون دو تا قیمت بیت‌کوین و دلار در دو والت یا درگاه خرید به ندرت یکسان خواهند بود. به همین دلیل تصمیم ما خیلی کاربردی بود. ما نیاز داشتیم تا کارها را ساده‌تر کنیم و درخواست‌های پشتیبانی را کاهش دهیم. و به شکل غیر قابل باوری هم نتیجه داده است، درخواست های پشتیبانی مرتبط با این مساله به شدت کاهش یافت.

استفان:

این مساله چه مشکلی برای شما داشت؟ آیا کاربرانی بودند که بگویند، اوه نه شما مقدار اشتباهی را ارسال کرده‌اید؟ یا چنین چیزهایی؟

ساموورای:

بله بسیار زیاد! اما تعداد درخواست‌های پشتیبانی مهم و معقول هم زیاد بود که به دلیل بیان کردن مقدار دلاری (فیات) پیچیده می‌شدند. مثلا پیش می‌آید که دیگر کاربران ایمیل می‌داند و میگفتند ما نمی‌توانیم مقدار خروجی باقی‌مانده[3] را در والت ببینیم و چنین چیزهایی. معمولا مشکلاتی از قبیل مشکل ارتباط اینترنتی یا Tor هستند که مشخصا نیاز به بازبینی دارند، اما تشخیص اینکه در مورد کدام UTXO صحبت می‌کنند خیلی سخت است. چون مقدار بیت‌کوین به معادل دلاری در هر لحظه می‌تواند مبلغ بسیار متفاوتی باشد. به همین دلیل فهمیدن اینکه مشکل دقیقا چیست و حل کردن آن نیاز به بررسی بیشتری دارد. حالا یک نفر مسئول پشتیبانی در والت ساموورایی است و تعداد زیادی درخواست پشتیبانی دریافت می‌شود. بنا براین باید کاری کنیم تا از زمان این شخص بیشترین بهره را ببریم و تنها راه آن کاهش تعداد ایمیل‌هایی است که به اشتباه ارسال می‌شود. شاید این استراتژی کمی خشن به نظر بیایید، اما خب حذف مقدار فیات (دلاری) یکی از راه های کاهش مشکلات است و ارزشش را هم دارد، چون مسائل پیش پا افتاده‌ای مثل تغییر قیمت بیت‌کوین نباید گریبان‌گیر پشتیبانی ما یا حتی دیگران هم باشد.در حال حاضر فقط کمی درگیری در نسخه‌های قدیمی داریم. درخواست‌های پشتیبانی معقول زمان کمتری برای رفع شدن نیاز دارند. بنا بر این فکر می‌کنم این ایده موفقیت‌آمیز بوده است. مورد دیگری که ما خیلی به آن دقت می‌کردیم این بود که آیا این تصمیم تاثیری روی حذف و نصب نرم افزار داشته است؟ و خیر، تاثیری نداشته. تعداد نصب نرم افزار واقعا بالا رفته و میانگین حذف شدن نرم افزار از آن زمان کمتر هم شده است. من فکر نمیکنم بالا رفتن تعداد نصب‌ها به این دلیل باشد. به نظر من از هر زاویه ای که نگاه کنیم، به نظر میرسد که تصمیم خوبی بوده، کاربران در کنار ما مانده‌اند و کاربران جدید هم هر روز به ما اضافه می‌شوند. بنا براین به نظر من این حرکت عالی بود.

3 Change output

استفان:

درسته، عالیه. خب بهتره در باره PayNym، یا همان BIP47 صحبت کنیم. قبل‌تر عنوان کردی که افراد آدرس‌های خود را در شبکه‌های اجتماعی قرار می‌دهند و این مشکلی همیشگی و جدی برای حریم خصوصی است. کمی در این باره بگو که PayNym چطور می‌تواند در این موضوع به ما کمک کند.

سامورای:

دقیقا یکی از بهترین موارد استفاده از PayNym برای رفع مشکل حریم خصوصی آدرس‌ها در دریافت حمایت‌های مالی (donation) است. وقتی شما می‌خواهید به صورت عمومی کمک‌های مالی دریافت کنید، ساده ترین روش همان روش پیش فرض بیت‌کوین است، به این شکل که، این کد QR آدرس بیت‌کوین من است، مقداری بیت‌کوین برای من ارسال کن، نباید در مورد چیزی از من سوال کنی و همه چیز رو به راه است. خب مشکل این است که یک شناسه را به صورت عمومی اعلام میکنید، که ممکن است هویت زندگی واقعی شما باشد یا شناسه‌های دیجیتالی دیگری از شما باشند. شما این شناسه را به یک آدرس خاص وصل میکنید و هر کسی که به این ادرس پول بفرستند ممکن است بتواند هویت شما را شناسایی کند که این یک مشکل حریم خصوصی است، به‌خصوص با در نظر گرفتن این واقعیت که بلاک‌چین قابل تغییر نیست[4] و همه میتوانند همیشه به عقب برگردند و بلاک‌چین را به دقت بررسی کنند. این یک مشکل برای حریم خصوصی است. BIP47 یا همان Paynym این مشکل را به این شکل حل میکند که اجازه می‌دهد یک کد ثابت را که تغییر نمی‌کند به اشتراک بگذارید، اما این امکان را برای کاربران فراهم می‌کند که به این کد، بیت‌کوین ارسال کنند بدون اینکه موجودی آدرس کمک‌های مالی را افشا کند یا تاریخچه تراکنش‌های آن را نشان دهد. در نهایت

4 immutable

یک ادرس منحصر بفرد تحت عنوان Stealth Address (آدرس پنهان) بین فرستنده و مالک کد پرداخت (paynym) ایجاد می‌شود و هر کسی که پول میفرستند بر اساس والتش آدرس متفاوتی را دریافت میکند. این راه حل خوبی برای مشکل آدرس‌های ثابت است. شبیه به کاری است که دارک والت (پروژه‌ای قدیمی که اکنون دیگر فعال نیست. -م) باآدرس های مخفی انجام میداد با این تفاوت که برای رسیدن به این هدف به جای استفاده از سرور از بلاک‌چین استفاده می‌کنیم.

استفان:

خیلی جالبه، و اینکه آیا تنها نکته منفی این است که نمیتوانید مستقیما پرداخت را انجام دهید و باید یک کانال PayNym با طرف مقابل ایجاد کنید و سپس ارسال را انجام دهید. درسته؟

سامورای:

بله این یک ایراد بزرگ است، به دو دلیل این مشکل را به عنوان نقطه ضعف اصلی می‌بینم. دلیل اول: برای تجربه کاربری یک فاجعه است. چون اول برای کانفرم شدن در بلاکچین باید منتظر بمانیم، صادقانه بگویم باید خیلی مصمم باشید که این همه منتظر بمانید و پس از آن پرداخت را انجام دهید. این مسئله باید حل شود. همچنین فکر میکنم که Luke Dashjr (یکی از توسعه‌دهندگان قدیمی و پرتلاش بیت‌کوین در دهه اخیر. -م) این را مطرح کرد که تراکنش‌های نوتیفیکیشن غیرضروری هستند. زمانی این نکته مطرح شد که Justus Ranvier (م. توسعه دهنده) پروپوزال این روش را برای کدهای پرداخت با قابلیت استفاده مجدد معرفی کرد. Luke نوتفیکیشن‌ها را به عنوان اسپم بلاکچین در نظر میگرفت. البته من با Luke موافق نیستم ولی به نظر من هم کمی غیرضروری است. من می‌دانم چرا تراکنش‌های

نوتیفای ایجاد شده‌اند. چون همان طور که گفتم نیازی به سرور ندارد، نیاز به یک بلاک‌چین دارد. وقتی شما می‌خواهید چیز کوچکی را بازیابی کنید، برای اینکه والت شما بتواند آدرس های مخفی را تشخیص دهد باید بداند که چه کسی به من متصل شده است و این کار را از طریق تراکنش های نوتیفای کننده انجام میدهد. با این حال ما داریم روی حل این مشکل کار می‌کنیم. فهرستی از کدهای پرداخت داریم به نام paynym.is و فکر میکنم که سال بعد قطعا بهبودهایی در وبسایت ما برای این کار یعنی paynym.is خواهیم داشت. نوعی پل ارتباطی برای کاربرانی که پرداخت‌های فوری دارند می‌توانند در یک حالت امن این کار را انجام دهند بدون اینکه حریم خصوصی انها به خطر بیفتد. این کار با تبدیل‌های مختلفی صورت می‌گیرد، مثل بازیابی از بلاک‌چین به جای بازیابی از سرور رمزنگاری شده یا همچین چیزی که مشخص می‌کند کدام کد پرداخت به کدام پرداخت شما مرتبط است یا برعکس. بنا بر این برای حل این مشکل باید تغییرات مختلفی ایجاد شود. کاری شبیه به مدل آدرس مخفی. اما باید دید انتخاب کاربرها چیست.

استفان:

خوبه، خب بهتره راجع به Ricochet صحبت کنیم. من درباره آن مطالعه کردم و به نظرم قابلیت بسیار جالبی است. برای مخاطبان ما کلیاتی در باره آن بگو. که چه چیزی هست و چگونه کار می‌کند.

سامورای:

بله حتما. ایده Ricochet از صحبت‌های Adam Back و Matt Corallo (ادم بک مدیر شرکت بلاک استریم و مبدع هش‌کش در دهه ۹۰ میلادی که ساتوشی ایده‌ی ماینینگ در بیتکوین را از او الهام گرفت – مت کورالو یکی از توسعه دهندگان

بسیار پرکار روی بیتکوین در دهه اخیر بوده. -م) در یک کنفرانس گرفته شد. آنها می‌گفتند که شرکت های آنالیز کننده بلاک‌چین در تاریخچه تراکنش‌ها معمولا ۴ یا ۵ گام به عقب برمی‌گردنند و اگر در این گام‌ها مورد مشکوکی اتفاق افتاده باشد آنرا تحت رصد قرار می‌دهند. اگر به این موضوع فکر کنید، دیوانه کننده است. ۵ تراکنش قبل‌تر می‌تواند شامل افراد زیادی با فعالیت‌های متفاوتی باشد. از مرتبط کردن فردی که الان پول ارسال کرده به گذشته تراکنش‌های قبل از او ایده Ricochet به ذهن ما رسید و خیلی هم ساده است. به این شکل که قبل از اینکه تراکنش به مقصد نهایی برسد گام‌های اضافه‌ای به تاریخچه تراکنش‌ها اضافه می‌شوند. از آنجایی که این کار چندان عجیب و غریب نیست. آنالیز کننده‌ها ۵ گام به عقب برمی‌گردند و میبینند که هیچ UTXO یا تراکنشی با آنچه در بلک‌لیست یا فعالیت‌های مشکوک آنها مطابقت داشته باشد پیدا نمی‌کنند، واگر این طور نباشد عملیات موفقیت آمیز بوده است. مثل چک کردن در گمرک است یا در واقع نرم افزار آنالیز بلاکچین این شرکت‌ها را تبدیل به یک مامور گمرک بی انگیزه و بی حوصله می‌کنیم که به همه می‌گوید برو برو. این مامور طبق پروتکل درست وظیفه خود را انجام می‌دهد اما به نتیجه لازم نمی‌رسد. خب ما به راحتی می‌توانیم این کار را انجام دهیم و این کار را هم کردیم، Ricochet را ایجاد کردیم که ۴ قدم را به تراکنش اضافه می‌کند. Ricochet را کمی بیشتر از یک سال است که ارائه کرده‌ایم. و کاربران زیادی از آن استفاده می‌کنند و هرگز شکایتی نداشته‌ایم، هیچ وقت کسی نگفته که حسابش بسته شده یا موارد مشابه دیگر، پس به نظر می‌رسد که خوب کار میکند و موثر است. برای همین فکر میکنم که قابلیت بسیار خوبی است. Ricochet یک قابلیت پولی است یعنی کاربران برای استفاده از این قابلیت پول پرداخت می‌کنند که صادقانه بگویم، یکی از دلایل ادامه دادن ما است. با مقدار پولی که ما از آن دریافت میکنیم می‌توانیم هزینه‌های اجرایی، سرورها، نودها و کارمندها را بپردازیم. Ricochet برای ما و همچنین کل اکوسیستم قابلیت مهمی است.

دانستن این نکته هم مهم است که افراد آنالیز کننده بلاک‌چین برای مبارزه با

Ricochet باید هزینه بیشتری پرداخت کنند، چون به این مسئله فکر کنید: هر تراکنشی که وارد پلتفرم میشود، انها ۵ قدم آخر آن را چک می‌کنند. خب ما از ۱۰۰ یا ۱۰۰۰ تا حرف نمی‌زنیم، از یک پلتفرم بزرگ با ۲۰ -۳۰ میلیون کاربر حرف می‌زنیم (م.سال ۲۰۱۸). برای ۴ یا ۵ قدم به خوبی کار می‌کند اما اگر بخواهیم ۷، ۸، ۹ و ۱۰ قدم را چک کنیم چه؟ این نه تنها هزینه های پردازشی را بالا میبرد و باعث کاهش یا از دست دادن درآمد شرکت‌های تحلیل بلاک‌چین می‌شود، بلکه همچنین صرافی یا بیزنسی که از شرکت‌های تحلیل بلاکچین خدمات می‌گیرد از این همه False Positive (مثبت کاذب – به اشتباه موردی صحیح اعلام شود که باعث پایین آمدن دقت تحلیل می‌شود) که به آن‌ها ارائه شده است خسته می‌شود و خدمات چنین شرکت‌هایی را بی‌کیفیت تلقی خواهد کرد. این موضوع به سادگی در عوامل و انگیزه‌های اقتصادی خلاصه می‌شود. احتمالا به همین دلیل است که از جانب صرافی‌ها واکنشی به Ricochet دریافت نکرده‌ایم. به نظر می‌رسد که به دلیل هزینه‌ها تعداد گام‌ها را برای تحلیل افزایش نداده‌اند. هم‌اکنون ۵ تراکنش به نظر استاندارد است و به اندازه کافی خوب هست.

استفان:

درسته همان طور که شما گفتید تعداد کاربران بسیار زیاد است و آنالیز کننده‌ها هم شروع به بررسی گام‌هایی می‌کنند که از نظر آنها مشکلی ندارد.

ساموررای:

در حال حاضر هم همین طور است، یعنی اگر فقط ۵ گام به عقب برگردند و بدون اینکه ازشما سوالی شود، مشکلی در تراکنش شما مشاهده نخواهند کرد. تاریخچه تراکنش‌ها خیلی زیاد است.

استفان:

نکته جالب در صحبت‌های شما نامتقارن بودن هزینه‌های دفاع از حریم خصوصی و هزینه‌های حمله به آن است. هزینه‌ای که یک حمله کننده به حریم خصوصی اطلاعات روی بلاک چین سعی به انجام آن دارد خیلی بیشتر از هزینه دفاع کاربران در مقابل این حمله است.

ساموری:

بله، برای ما به سادگی تغییر دادن یک متغیر (از ۵ به یک رقم بالاتر) است. چیزی را که عنوان نکردم این است که ما برنامه داریم تا Ricochet را ارتقا دهیم و در حال حاضر، در حال تست کردن آن هستیم. در نسخه جدید تراکنش‌ها بین بلاک‌های نامتوالی پخش می‌شوند. (هم اکنون این قابلیت اضافه شده و عنوان آن Staggered Delivery است. -م). بنابراین شما می‌توانید Ricochet را امروز در این بلاک شروع کنید و بلاک نهایی در گام بعدی، بلاک بعد یا دو بلاک بعد از الان باشد. یعنی زمانی که تراکنش شما به مقصد می‌رسد ممکن است مثلا ۲۵ بلاک بعد از زمانی باشد که Ricochet را شروع کرده اید. این کار ردپای Ricochet را برای پیدا کردن آن کاملا پاک می‌کند. باید کمی خصومت‌آمیز و از دید دشمن فکر کنیم، فکر کنیم که اگر به Ricochet حمله شود چه می‌شود؟ اگر بگویند که ما رد پای تمام Ricochet را شناسایی خواهیم کرد و این افراد را به شدت توبیخ خواهیم کرد چه؟ تیم سامورای والت به این شکل فکر می‌کند و آینده مساله را نیز از سمت شرکت‌های تحلیل بلاکچین در نظر می‌گیرد. به همین دلیل Ricochet با فاصله‌های چند بلاک متفاوت میتواند راه حل بسیار بسیار قویی برای آن باشد.

استفان:

بله. همان طور که شما گفتید افراد از این عبارت به صورت غیر امنی استفاده می‌کنند. که شبیه به موش و گربه بازی است. یک سمت که تلاش بیشتری می‌کند سمت دیگر نیز تلاش خود را بیشتر می‌کند. خب یک نکته جالب هست که میخواهم سوال کنم. مثالی مانند واکسن و ایمنی جمعی که ایجاد می‌کند را در نظر بگیرید. آیا همچین مفهومی در بیت‌کوین داریم؟ که اگر تعداد کافی از افراد از این نوع تکنیک‌های حریم خصوصی و قابلیت‌هایی مثل کوین‌جوین، `StoneWall` و `Ricochet` استفاده کنند، باعث می‌شود حتی کاربرانی هم که از این قابلیت‌ها استفاده نمی‌کنند محافظت شوند؟

سامورای:

قطعا بله. فکر میکنم ادام فیسکور مقاله‌ای را در وبلاگ مدیوم[5] خود نوشته بود با عنوان «حریم خصوصی یک کار تیمی است». مقاله درباره تشویق مردم برای استفاده از حریم خصوصی است‌مسأله، محافظت از مجرمان‌و کمک به پول‌شویی یا چیزهایی از این قبیل نیست‌بلکه حقوق اساسی اشخاص است، درباره داشتن حریم خصوصی در تراکنش‌ها است و اصلا جای بحث ندارد، چیزی است که برای همه است. به اندازه آزادی بیان، جزو حقوق اساسی است. در واقع بخشی از آزادی بیان است. اینکه چطور معاملات خود را انجام می‌دهید به اندازه صحبت‌های شما مهم است به همین دلیل اصلا جای بحث ندارد. برای همین من علاقه‌مند به ارتقای حریم‌خصوصی در سطح پروتکل بیت‌کوین هستم. این یک گام بزرگ برای رسیدن به این موقعیت مناسب برای حفظ حریم خصوصی کاربران بیت‌کوین است. اما تا زمان رسیدن به این موقعیت باید روی ساخت ابزارهایی تمرکز کنیم که قرار است از قسمت مهمی از استفاده کاربران باشند، حتی اگر بعضی افراد موافق این ابزارها نباشند. درست مثل

5 medium

Whatsaap، که رمزنگاری آنها احتمالا خیلی هم عالی نیست اما رمز نگاری را برای همه قرار داده است. حتی آوردن کلمه رمزنگاری باعث می‌شود شما کمی آگاهی پیدا کنید که در آن چه اتفاقاتی در جریان است. من درباره نوعی تغییر صحبت می‌کنم که به آن نیاز داریم و چیزی نیست که والت ساموراییی به تنهایی از عهده آن برآید، یک تلاش همگانی است.

استفان:

بله، یک چیزی که قبل تر به آن اشاره کردید درباره انگیزه است. اگر مسیری وجود دارد که نیاز به هزینه کردن دارد و مسیر دیگری هم هست که زیاد هزینه بر نیست، خب مردم احتمالا مسیر دوم را ترجیح میدهند. موضوع مرتبط با قابلیت StoneWall در سامورای والت است، برداشت من این است که این قابلیت به صورت پیش فرض در والت پیاده‌سازی شده است. کمی در این باره برای ما بگو.

سامورای:

بله، حتما. خب Stonewall تراکنش هایی را ایجاد می‌کند که به لحاظ ریاضی فرقی با یک تراکنش کوین‌جوین ندارند و در کل به صورت دیداری قابل تشخیص نیستند. درواقع شبیه به تراکنشی است که چند نفر به هم پیوسته‌اند تا یک تراکنش میکس معمولی را ایجاد کنند. شبیه به تراکنش های والت واسابی است به عنوان مثال، یا تراکنش‌های جوین‌مارکت و غیره. اما البته هیچ یک از این‌ها نیست، این قابلیت فقط والت شماست، یک ترفند است، یک کوین‌جوین تقلبی است.
Stonewall در رابطه با چیزهایی است که قبلا صحبت کردیم، در باره از بین بردن فرضیات و از بین بردن امکان کشف برای شرکت‌های آنالیز کننده بلاکچین است. از نظر ریاضی آنالیز کننده‌ها نمی‌توانند به طور قطعی مشخص کنند که ورودی‌ها در

یک تراکنش Stonewall متعلق به یک والت است، همچنین نمی‌توانند تشخیص دهند که کدام خروجی مربوط به باقی پول[۶] است.

استفان:

درسته. برداشت من این است که والت به صورت هوشمند کوین‌ها را برای ساخت تراکنش انتخاب می‌کند. ایا راهی هست که این انتخاب کوین[۷] در ساموراییی به صورت دستی انجام شود یا اینکه به صورت خودکار انجام می‌شود.

ساموررای:

انتخاب کوین موضوع مهمی است. همان طور که شما گفتید، انتخاب کوین در Stonewall یک الگوریتم است که استفاده می‌شود. می‌توانیم به شنوندگان شما لینک گیت‌هاب بخش‌هایی از الگوریتمی که توسعه‌دهندگان ساموراییی نوشته‌اند را بدهیم. اما به این شکل است که خروجی‌های موجود در والت شما (utxo) دسته بندی می‌شوند و براساس نوع آدرس، P2PKH یا P2WPK یا هر چیز دیگری، در مجموعه‌هایی قرار می‌گیرند و به صورت تصادفی پردازش می‌شوند. به دلیل این شرایطی که الگوریتم نیاز دارد هر تراکنشی نمی‌تواند یک تراکنش Stonewall باشد. والت این مورد را به شما هشدار خواهد داد. به نوعی هرچه بیشتر از والت استفاده شود، فعال‌تر میشود. اگر stonewall بتواند فعال شود، قوانین انتخاب کوین دیگری هم هستند که در والت ساموراییی وجود دارند. من فکر می‌کنم بیشتر والت های خوب Merge Avoidance دارند (م. یکی از تکنیک‌های حفظ حریم خصوصی)، بنا براین اگر UTXO ها در یکی از تراکنش‌های قبلی باهم دیده شده باشند، دوباره از آنها استفاده نمی‌کنند. یعنی از آن UTXOها در هیچ تراکنش دیگری

6 Change output

7 Coin selection

با هم استفاده نمی‌کنند. پس این یک نوع تکنیک انتخاب ساده برای جلوگیری از مشکل ادغام ورودی‌ها است. حالا اگر بخواهید تمام محتویات والت را انتقال دهید، نمیتوانید از ادغام ورودی ها جلوگیری کنید اما والت به شما اخطار میدهد که ورودی‌های شما ادغام خواهند شد. ایا مطمئنید؟

استفان:

هوشمندانه است، خوشم آمد. در همین رابطه من در بلاگ شما می‌خواندم که، یکی از راه‌هایی که شما این تراکنش ها را آنالیز می‌کنید با استفاده از چیزی به نام Boltzmann Scoring است. برای مخاطبان ما یک توضیح کلی بده که چی هست و چطور کار میکند؟

ساموررای:

خودم هم میخواستم به همین برسم چون با مسئله انتخاب کوین مرتبط است. امروزه بیشتر مقاله‌های آکادمیک و بیشتر تحقیقات درباره انتخاب UTXO اغلب درباره مبلغ و قدمت UTXO بوده‌اند. برای همین کاری که ما می‌کنیم این است که یک گام جلوتر برداریم و این گونه است که Boltzmann به این موضوع گره می‌خورد. چون Botlzmann به چیزی بیشتر از مبلغ و قدمت UTXO ها نگاه می‌کند. Boltzmann به چیزی به نام آنتروپی و همچنین راندمان حریم خصوصی والت برای یک تراکنش هم نگاه می‌کند. انتروپیِ تراکنش، تعداد ترکیبهایی است که بین ورودی ها و خروجی‌ها، از نظر ریاضی ممکن است. یعنی به چند روش مختلف می‌توانید تراکنش را تقسیم کنید و بگویید این ورودی برای این خروجی است یا این خروجی برای این ورودی و غیره. مورد دوم راندمان والت است، که تعداد ارتباط های قطعی است. که می‌توانیم با قطعیت بگوییم «خب این ورودی برای این خروجی است.» و

محاسبات پیچیده‌ای پشت آن است. خوشبختانه Lauren که پروژه OXT را اجرا می‌کند علاقه شدیدی به ریاضیات دارد و یکی از کسانی است که این ابزارها را توسعه داده و در کنار هم قرار می‌دهد. پس کاری که ما انجام می‌دهیم استفاده از این ابزارها است. مثل Boltzmann، تا UTXO هایی را انتخاب کند که حریم خصوصی کاربر را به حداکثر برساند. البته این هنوز عملی نشده هست و این مورد در حال تست است (هم اکنون در فوریه ۲۰۲۱ همه این قابلیت‌ها فعال و در حال استفاده هستند. -م). اما انتخاب UTXO یکی از مواردی است که در تحقیقات و توسعه تمرکز زیادی روی آن داریم. یک قابلیت عجیبی که داریم این است انتخاب کوین یا کنترل کوین در سمت کاربر را شروع کرده‌ایم. پس قادر خواهیم بود کنترل کوین با کیفیت بهتری، در آینده در والت داشته باشیم. مثلا اگر گفته شود من می‌خواهم از این UTXO خاص در والتم خرج کنم ما این اجازه را به کاربر می‌دهیم. اما در حال حاضر کاری که می‌توان در والت انجام داد این است که یک UTXO را به عنوان غیر قابل خرج تیک بزنیم (این قابلیت هم‌اکنون فعال و قابل استفاده است. -م). بنابراین شما به نوعی کوین کنترل برعکس انجام میدهید یعنی مشخص می‌کنید که من این UTXO را می‌خواهم خرج کنم و این UTXO را نمی‌خواهم خرج کنم. به نحوی والت را مجبور می‌کنید در شرایطی که شما می‌خواهید قرار بگیرد. و این موضوع به چند دلیل مفید است ولی ما این تابع را برای جلوگیری از نوع دیگری از حمله به حریم خصوصی ارائه داده‌ایم، که البته زیاد هم اتفاق نیفتاده است اما دو سه سال پیش خیلی شایع بود، به نام حمله Dusting. به این شکل که یک مقدار کمی بیت‌کوین به والت شما ارسال میشود، معمولا مقدار خیلی خیلی کمی است.

استفان:

آها، مقدار خیلی کمی بیت‌کوین رایگان است؟

سامورای:

بله اما بعدش شما آن بیت‌کوین را خرج می‌کنید، معمولا در یک تراکنش با ورودی‌های دیگر ادغام می‌شود، چون مقدار خیلی کمی است. خب حالا به شما دسترسی دارند، در واقع یک زنجیره از تراکنش‌های آتی شما برای حمله کننده ایجاد شده است که با دنبال کردن آن می‌تواند از همه چیز مرتبط به تراکنش‌های بیت‌کوین شما مطلع شود. با والت سامورایی می‌توانید این مقدار را به عنوان غیر قابل خرج تیک بزنید، و والت هرگز از آن استفاده نخواهد کرد.

موردی دیگر این است که افرادی هستند که به ما می‌گویند نصف والتمان را به عنوان غیر قابل خرج تیک زده‌ام و کلا فراموش کرده‌ام که آن‌ها را دارم، چون این مقادیر از مانده حساب کم می‌شود و شما نمی‌توانید آن را ببینید. باید به لیست UTXO ها برگردید و به عنوان قابل خرج آن‌ها را علامت‌گذاری کنید. مردم می‌گویند مثل این است که از جیب لباس‌مان یک اسکناس ۲۰ دلاری پیدا کردیم!

استفان:

شبیه به حمله اسب تروا است. و یک چیز دیگر، هر کسی که از یک آدرس عمومی برای دونیشن استفاده میکند در برابراین حمله آسیب پذیرتر است است. اگر کسی یک Dust به شما ارسال کند در حالی که شما از PayNym استفاده میکنید، این حمله احتمال موفقیت بسیار کمتری دارد.

ساموورای:

درسته، بله.

استفان:

خب موضوع بعدی که میخواهم درباره آن صحبت کنم و دیدم که یکی از اعضای تیم والت ساموورایی در باره آن نوشته بود، Stowaway است. قابلیت جدیدی که تیم شما روی آن کار می‌کنند. مدیر فنی تیم شما گفته بود که در هیچ کدام از خروجی ها مقدار واقعی مبلغی که خرج شده است را نشان نمی‌دهند. و تحت تاثیر همکاری قابل اعتماد بین دو والت است. میخواهی کمی در این باره صحبت کنی؟

ساموورای:

بله، Stowaway نوعی تراکنش منحصر به فرد است. بعد از اینکه کاربر کوین خود را در Whirlpool میکس کند این قابلیت در دسترس خواهد بود. این چیزی است که ما به آن تراکنش پس از میکسینگ یا postmix می‌گوییم. به هرحال شما باید بیتکوین‌های میکس شده را زمانی خرج کنید، خود شما هم شاید فراموش نکنید اما خیلی از افراد فراموش می‌کنند و اگر مراقبت نشود نوع خرج کردن شما می‌تواند تا حدودی حریم خصوصی بدست آمده شما از میکس کردن را به راحتی از بین ببرد. Stowaway یکی از سه نوع تراکنش بعد از میکس خواهد بود. Stowaway یک مشکل کوچک دارد، آن هم این است که بین کاربران والت ساموورایی انجام میشود به این دلیل که نیازمند PayNym است و در حال حاضر فقط والت ساموورایی و تعداد کمی از والت های دیگر هستند که از BIP47 پشتیبانی میکنند. پس برای اینکه بتوانیم به آن اعتماد کنیم نیاز به Paynym داریم. (این مشکل در زمان ترجمه این

گفتگو به‌کلی برطرف شده و این ابزار به‌سادگی و با استفاده از قابلیت سوروبان قابل استفاده است. –م)

استفان:

منظور شما اینه که ممکن است کوین‌های شما به سرقت بروند یا اینکه فقط به شناسایی شدن شما کمک می‌کند؟

سامورای:

کسی نمی‌تواند کوین‌های شما را بدزدد یا از مانده حساب شما مطلع شود یا چنین چیزهایی. تراکنش به این صورت عمل می‌کند که شما برای آنها بیت‌کوین ارسال میکنید. به عنوان مثال من می‌خواهم یک بیت‌کوین برای شما ارسال کنم و یک UTXO دو بیت‌کوینی دارم. اگر تراکنش من معمولی باشد، یک ورودی دو بیت‌کوینی داریم و در خروجی دوتا UTXO وجود دارد که هرکدام یک بیت‌کوین هستند. یکی برای شما ارسال می‌شود و دیگری به خودم برمی‌گردد. این یک تراکنش استاندارد است. خب حالا اگر از Stowaway استفاده کنیم، ورودی هنور هم برای من ۲ است.

استفان:

چطوری؟

ساموورای:

اینجا اعتماد وارد عمل می‌شود. من به شما که پول فرستاده‌ام می‌گویم که یک UTXO دیگر در والتت به من بده. نه این که برای من آن را ارسال کنی فقط اطلاعات آن را به من بده. بنا بر این اعتماد زمانی ایجاد میشود که من می‌گویم می‌توانم آن یک UTXO را ببینم. در این حالت شما یک UTXO دو بیت‌کوینی دارید. پس ما از UTXO دو بیت‌کوینی که شما هم دارید استفاده می‌کنیم. خب تراکنش شما حالا یک ورودی ۲ بیت‌کوین از من دارد و یک ورودی دو بیت‌کوینی از شما. یک خروجی سه تایی برای شما و یک خروجی یکی به من بر می‌گردد.

استفان:

خیلی جالب است.

ساموورای:

Stowaway خیلی منحصر به فرد است. مثل این است که بخواهم به یکی از مخاطبان مورد اعتمادم بفرستم. مورد اعتماد از این جهت که UTXO هایی که دارند را افشا می‌کنند. پس باید بدانیم که به چه کسی قرار است بیت‌کوین ارسال کنیم. و انها هم باید در مجموعه مشارکت کنند. پیچیده است. این روش را ما اختراع نکرده‌ایم و اعتبار کشف آن به گرگوری مکسول می‌رسد. سال پیش گرِگ مکسول (یکی از توسعه‌دهندگان قدیمی و بسیار تاثیرگذار در روند توسعه بیت‌کوین در دهه اخیر. - م) ایده‌ای در این باره داشت که ما آن را در گفتگوهایی درباره بیت‌کوین پیدا کردیم که به جایی هم نرسید. فکر می‌کنم او یکی از این تراکنش ها را دستی ایجاد کرده بود، و همانجا هم در انجمنی که بحث میشد هم این موضوع پایان یافت. افراد در آن‌جا مشارکت میکردند و utxoهای خود را در اختیار قرار می‌دادند تا مثلا

مورد استفاده قرار بگیرند. ما آن تراکنش را پیدا کردیم و گفتیم چه تراکنش جالبی. در واقع یک کوین‌جوین کوچک است چون شما با یک نفر مشارکت دارید، یک کوین‌جوین بزرگ با چند نفر انجام نمی‌دهید، یک تراکنش یک یا دو نفره انجام می‌دهید. اما این در اصل یک کوین جوین خیلی کوچک است. به همین دلیل ما خیلی برای آن هیجان زده شدیم و با خود فکر کردیم که می‌تواند یک روش برای خرج کردن کوین باشد. اگر درباره آن فکر کنید، این یک ترفند هوشمندانه است، کاری که انجام می‌دهد این است که مجددا مثل دیگر قابلیت‌هایی که صحبت کردیم به فرضیات حمله میکند. Stowaway خیلی شبیه به تراکنش معمولی بیت‌کوین است، کاملا استاندارد، در حالی که اینطور نیست. هر دوی آن ورودی ها متعلق به یک والت نیستند، نمی‌توان آنها را به هم مرتبط کرد، شبیه به همه تراکنش‌های استاندارد شما است و یک کوین جوین کوچک است. بنا بر این تمام فرضیاتی که شرکت های آنالیز بلاک‌چین انجام میدهند، نادرست خواهد بود. (این قابلیت در سامورای والت هم اکنون بسیار توسعه یافته و حتی به شکل آنلاین روی شبکه تور امکان انجام آن را خواهید داشت. -م)

استفان:

بله، ایده هوشمندانه ای است. و در ایده کوین جوین ما باید منتظر نوبت باشیم که ممکن است زمان‌بر باشد ولی در این روش فقط شما و یک نفر دیگر هستید.

سامورای:

بله در کوین جوین باید صبر کنید تا نوبتتان برسد و انتظار هم نداریم که مدت زمان زیادی را منتظر بمانیم. این یکی از خوبی های موبایلی بودن است. شما تعداد نسبتا زیادی کاربر خواهید داشت که واقعا نیاز نیست هیچ کاری انجام دهند، مجبور نیستند

چیزی را نصب کنند، کامپایل کنند، یا کار زیادی انجام دهند. در واقع موانع ورود استفاده از آن خیلی کم است. یکی از تفاوت های ZeroLink به عنوان یک فریم‌ورک و Whirlpool به عنوان یک محصول این است که whirlpool یک لایه انگیزه مالی اضافه کرده است. به همین دلیل انتظار داریم نقد شوندگی تسهیل شود و نوبت ها سریع‌تر خواهند بود.

استفان:

انگیزه مالی آن بر چه پایه‌ای بنا شده است؟

سامورای:

در حال حاضر ۱۰۰ درصد اماده نیستم که به آن بپردازیم، اما می‌خواهم بگویم که از نرم افزار Joinmarket الهام گرفته شده است، که من همیشه آن را تحسین می‌کنم. به خصوص انگیزه‌های اقتصادی که واقعا هوشمندانه است. فکر می‌کنم آنها هم همان مشکلاتی را داشته‌اند که من درباره‌اش گفتم، موانعی که برای استفاده از محصول وجود دارد. پس لایه انگیزه مالی از آن الهام گرفته است و دقیقا شبیه به مدل اصلی نیست ولی فکر می‌کنم چیز خیلی جالبی خواهد شد. من نمی‌توانم در باره جزئیات آن صحبت کنم. (در سال ۲۰۱۸ هنوز این قابلیت توسعه نیافته بود به همین دلیل سامورای به ایده‌ی آن نپرداخته است. توضیح آن به صورت کوتاه این است که لایه انگیزه مالی هم اکنون به عنوان freeriding در حال استفاده است. و این موضوع به این صورت عمل می‌کند که شما پس از میکس کردن کوین خود با نگه داشتن کوین خود در ویرلپول باعث افزایش نقدینگی برای میکس کردن دیگران در ویرلپول می‌شوید و همزمان هم تعداد میکس رایگان دریافت می‌کنید. هزینه‌ای متحمل نمی‌شوید اما تعداد میکس بیشتر و حریم خصوصی در سطح بالاتری بدست

می‌آورید. از این رو انگیزه مالی دارید که به ازای دریافت دفعات میکس بیشتر، امکان میکس برای دیگران با شما فراهم کنید. - م)

استفان:

موضع بعدی که خیلی مشتاقم در باره آن بدانم مفهوم گره های قابل اعتماد است (Trusted node). بحث های در توئیتر در این باره شده بود، افراد کمی هم نظراتی را ارائه داده بودند، فکر می‌کنم Luke JR و David Harding (دیوید هاردینگ یکی از توسعه دهندگان و نگه‌دارندگان پروژه‌های مختلف بیت‌کوینی مانند وبسایت بیت‌کوین کور و مدیریت انجمن IRC بیت‌کوین است. -م) گفته بودند که اگر Trusted node ها به درستی اجرا نشوند، کاربران را در معرض خطرات بیشتری قرار می‌دهد، چون پورت RPC را در اینترنت قرار می‌دهد. توضیحی در این باره داری؟ یا اینکه راه پیشنهادی برای استفاده از آن داری؟ (این قابلیت در کیف پول سامورایی وجود داشت و باعث به‌راه افتادن بحث‌های زیادی شد. -م)

سامورای:

ابتدا باید این نکته مهم را بگویم که به ندرت بحث‌ها و گفتگوهای نتیجه‌دار درباره موضوعات مهم در جاهایی مثل توئیتر پیدا می‌کنیم، به همین دلیل فکر میکنم که بهتر است از Github یا ایمیل یا چیزهایی شبیه به این استفاده شود. چون بحث کردن در توئیتر فقط پی‌گیری موضوع را سخت‌تر میکند. همچنین مقابله با اطلاعات نادرست و یا اطلاعاتی که بازگو نشده‌اند را هم سخت‌تر میکند. اما خوشبختانه در آینده قادر خواهیم بود چنین موضوعاتی را به Github ببریم. من فکر می‌کنم که متد RPC که برای اتصال کاربران به فول نود است، باعث ایجاد یک حفره امنیتی نمی‌شود. احتمالا منظور Luke این بوده که سیستم عددی Tonal برای افراد عادی

آسان‌تر خواهد شد. من بی احترامی نمی‌مکنم چون Luke برای من بسیار قابل احترام است. اما به نظر من منظور او این بوده است. من شخصا وقتی بیت‌کوین کور[8] SSL را حذف کرد، مخالف بودم. اما چون SSL چیز ترسناکی بود آن را حذف کردند. اگرچه به نظر من باید آن را با TLS جایگزین می‌کردند، با این کار می‌توانستند حالت رمزنگاری شده RPC را حفظ کنند. همان طور که BTCD این کار را به صورت پیش فرض انجام داده. بیشتر روش‌های RPC ازSSL و TLS استفاده می‌کنند، پس فکر نمی کنم منصفانه باشد که مقصر کارهای احمقانه کاربران برای دور زدن چیزهایی که در سطح گره ایجاد شده‌اند ما باشیم. پیشنهاد من ایجاد تونل SSH است که انجام آن روی دستگاه‌های موبایل چندان ساده نیست. در آن زمان، در جریان راه اندازیtrusted nodeها برای UASF، گزینه Tor برای ما در دسترس نبود. من فکر می کنم این خیلی مهم بود و هنوز هم برای کاربرانی که نود خود را اجرا می‌کنند مهم است. luke گفته بود که این چندان تاثیری ندارد، که درست نیست، تاثیر گذار است. دقیقا همان کاری را انجام می‌دهد که توضیح داده شده است. تراکنش شما را از نود شخصی خودتان که قوانین اجماع را کنترل می کنید منتشر می کند نه از از هر نودی. سربرگ Proof of work در بلاک را از گره شما میگیرد و انها را با نودهای ما مقایسه میکند و اگر تفاوتی وجود داشته باشد به شما هشدار می دهد و شما را آگاه می‌کند که یک چیزی درست نیست. این توصیه Peter Todd (یکی از توسعه‌دهندگان بیتکوین. –م) بود که در ردیت آن را پیشنهاد داده بود و پیاده سازی شد، و در جریانUASF هم خیلی مهم بود که نودهای ما به شما دروغ نگویند. ما حمایت بسیاری از UASF کردیم و می‌کنیم و اگر انشعابی وجود داشت، کاربر را آگاه می‌کردیم که گره ما از سافت فورکی که کاربر فعال کرده است پیروی می‌کند. گرچه می‌توانستیم دروغ بگوییم و کاربر هم به ما اعتماد کند. ما در معماری خود بسیار شفاف و صادقانه عمل کردیم که شما هنوز هم به والت سامورایی اعتماد

8 Bitcoin core

دارید که اطلاعات درست به شما می‌دهد. نرم‌افزار کیف پول ساموراییی به همین دلایل نسخه آلفا است و کاربران در این مرحله باید به ما اعتماد کنند. و ما برای این سخت تلاش میکنیم.

برای حل مشکل بحث بر انگیز زمان فعال سازی سافت فورک توسط کاربر، ما می‌گفتیم که خب اگر کاربری می‌خواهد سافت‌فورکی را دنبال کند و فول نود خودش را اجرا کند و تراکنش ها را از فول نود خودش منتشر کند، سپس سامورایی والت هشدار دهد که سربرگ `Proof of work` بلاک در فول نود شما و ما متفاوت است این یعنی چیزی این وسط درست نیست. ایده حل مشکل این بود، و کار هم می‌کند و بی تاثیر نیست. اخرین چیزی که در حال حاضر انجام می‌شود دریافت اطلاعات کارمزد از `mempool` واقع در فول‌نود شما است. ما همیشه موافق این بوده ایم که برنامه‌های بیشتری برای اطمینان از عملکرد فول‌نود ارائه کنیم.
درنهایت برای اطمینان پیدا کردن از نودها میتوان زیرساخت ساموراییی را کامل دور زد. این قدم بعدی که برای این موضوع باید برداریم. البته برای رسیدن به این موقعیت فقط چند هفته فاصله داریم کمی به مشکل زمانبندی برخوردیم اما به این قابلیت خیلی نزدیکیم. از یک طرف جای تاسف بود که باید با آن کنار بیاییم و از آن عصبانی بودیم. اما من زیاد نگران آن نیستم چون ما رویه و دستورالعمل را داریم و بیشتر مشکلاتی که قبلاً داشتیم حل شده اند ولی هنوز ارائه نشده اند.

استفان:

پس در چند هفته آینده باید منتظر آپدیت جدید باشیم.

ساموررای:

نه در چند هفته اینده چون زمان بندی ۱۰۰ درصدی را نمی‌توانم بگویم اما در چند ماه اینده حتما آپدیت جدید خواهیم داشت.

استفان:

بسیار خب. یک چیز دیگری که خیلی جالب است و خیلی ها از آن صحبت می‌کنند همکاری با شرکت GoTenna و ساخت نرم افزار Txtenna است. می‌خواهی کمی در این باره بگی؟

ساموررای:

کار کردن با تیم GoTenna پروژه خوبی بود. چند وقت پیش Mule tool (ابزار هایی برای انتشار تراکنش های بیت‌کوین بدون نیاز از اینترنت) را راه اندازی کردیم، که یکی از اقدامات تحقیق و توسعه ما در برابر سانسور کردن تراکنش‌ها است.، تمام راه های مختلف انتشار تراکنش ها و دریافت داده های بلاک‌ها، بدون استفاده از اینترنت است. GoTenna هم تصادفاً با این موضوع روبرو شد. فکر می‌کنم Richard Myers که مهندس اپلیکیشن های غیر متمرکز آنها است با این موضوع روبرو شد و همه ارتباطات ما با هم اتفاق افتاد و جلسه گذاشتیم. آنها به ارائه بیت‌کوین به کاربرانشان و ارائه GoTenna به کاربران ما علاقه‌مند شدند. ما هم فکر کردیم که پروژه خوبی خواهد شد که باعث ایجاد Mule Tool شد. بنا بر این ما به راهی فکر کردیم تا راه‌حل‌ها و رویکردهای مفهومی فعلی خود را، که آن زمان به آن Pony Direct می‌گفتیم را توسعه دهیم. کاری که Pony Direct انجام می‌داد این بود که تراکنش ها را از طریق SMS انتشار می‌داد، برای زمانی که شما اینترنت ندارید بسیار مفید است و حتما کار می‌کند. خب ما تصمیم گرفتیم آن را بر پایه

SMS و یا شبکه مش[9] GoTenna توسعه دهیم که اگر در محلی هستید که به راحتی به GoTenna متصل می‌شوید از آن استفاده کنید. این کار بود که در نهایت انجام دادیم. اگر از ایده راه حل مبتنی بر SMS استفاده شود باید از همان معماری استفاده شود، تراکنش ها به قسمت‌هایی تقسیم شوند و هر قسمت با فرمت خودش باشد تا بعدا بتواند دوباره بازسازی شود. تمام اینها اوپن سورس هستند. این اپلیکیشن در کنفرانسHCPP پراگ ارائه شد و خیلی هم جالب است.

استفان:

خیلی جالب بود. شخصی بود که من نمی‌توانم اسمش را به یاد بیاورم، فکر کنم اسمش Coinsurenz در توئیتر بود. او این کار را انجام داد. او یک دسته از GoTenna را در یک مسیر با هم ادغام کرد و مطمئن نیستم که از والت سامورایی استفاده کرده باشد، فکر کنم استفاده کرده باشد. این کار را برای انجام یک تراکنش بیت‌کوین به خوبی انجام داد که خیلی جالب بود.

سامورای:

بله فکر کنم برای مسیر خیلی طولانی هم این کار را کرده باشد.

استفان:

گفته می‌شود که کاملا هم امن بوده است. با این تکنولوژی که در دسترس است، تصور اینکه بیت‌کوین نابود شود، سناریو احمقانه ای است.

9 Mesh

سامورای:

هر روز هم تکنولوژی های بیشتری عرضه می‌شوند. من یک چیزی دیدم که تراکنش ها را با کدهای مورس از طریق رادیو منتشر می‌کرد. یک سری از کدهای آن خوب بودند که ما در صفحه Mule Tool آن را فورک کردیم و اضافه کردیم. فکر میکنم Motoshi در توئیتر بود که این کار را انجام داد. خب این خیلی خوب است چون خیلی افراد از آن الهام می‌گیرند. این نوع ابزار ها اگر چه ممکن است در حال حاضر نو ظهور باشند اما می‌توانند خیلی مهم باشند.

استفان:

درسته بسته به اینکه کجا زندگی می‌کنید می‌تواند مهم باشد.چیز دیگری که الان متوجه شدم، صحبت از کاربری در نیوزلند است (م. کاربر Coinsurenz) ، اخیرا قانونی تصویب کرده اند لغت دقیقش را یادم نیست اما همچین چیزی است که اگر شما وقتی که میخواهید وارد فرودگاه شوید گوشی خود را باز نکنید و همچنین پسورد را برای پلیس وارد نکنید، آنها می‌توانند شما را به زندان ببرند، خب با این ایده والت شما میتواند حالت مخفی داشته باشد و دستورات از راه دور اجرا شوند.

سامورای:

بله، قطعا این یک مورد استفاده است. اگر بخواهم صادق باشم، این کار نمی‌تواند والت شما را در برابر بررسی دقیق تلفن‌تان ایمن نگه دارد. اگر گوشی خود را باز کنید و آن را به نیرو های امنیتی یا هر کسی که قرار است آن را بررسی کند بدهید و انها هم به مدت زمان کافی گوشی را در دسترس داشته باشند ممکن است بتوانند والت شما را اگر در حالت مخفی باشد پیدا کنند و شما متهم به جرائم دیگر شوید. من در این بازه زیاد فکر کرده‌ام و توصیه‌ام برای کسی که از والت سامورایی

استفاده می‌کند این است که اگر پسفریز خود را یاد داشت کرده اند، به سادگی والت خود را حذف کنند و وقتی نیروهای امنیتی را رد کردند دوباره نصب کنند و والت را بازیابی کنند. فکر می‌کنم این قانونی ترین راه باشد. چون کسی را فریب نمی‌دهید و قانونی را زیر پا نگذاشته‌اید. ایده حالت مخفی در بازرسی‌های سطحی مفید است. وقتی که کسی به هر دلیلی گوشی شما را بازرسی می‌کند در صفحه اصلی گوشی چیزی وجود ندارد که آنرا اجرا کنید، بلکه باید شماره کد خاصی را شماره گیری کنید.گرچه اگر برسی های عمیق‌تری در تنظیمات و دسترسی‌های اپلیکیشن‌ها انجام دهند می‌توانند والت را پیدا کنند. پس اگر بدانند که دنبال چه چیزی هستند حتما والت را پیدا خواهند کرد. من نمی‌خواهم کسی در این مورد اشتباه برداشت کند. این ایده برای وقتی که کسی در کافه گوشی شما را بر می‌دارد و دنبال والت بیت‌کوین یا اپلیکیشن های بانکی میگردد می‌تواند مفید باشد چون چیزی پیدا نخواهند کرد.

استفان:

بله روش خوبی برای این است که کمی والت را مخفی نگه داریم. خب بیا کمی درباره تکنیک‌های حریم خصوصی در بیت‌کوین صحبت کنیم، که در طول زمان تغییرات زیادی داشته. صحبت از تراکنش های محرمانه است (طرح ادم بک با عنوان Confidential Transactions. –م) نظری در این باره داری؟ در باره ایده کلی Perfect binding در مقایسه با Perfect Hiding چه فکری می‌کنی؟

سامورای:

تنها چیزی که درباره تراکنش‌های محرمانه می‌توانم بگویم این است که ما می‌خواهیم آن را در شبکه اصلی و در پلتفرم ببینیم. این را قبلا در مصاحبه‌های دیگر گفته‌ام که شک دارم که بتوانیم تراکنش‌های محرمانه را به دلیل پیامدهایی که دارد در سطح پروتکل ببینیم. امیدوارم اشتباه کنم. باید نشست و تماشا کرد که چه خواهد شد. اما از نظر جزئیات نه در حال حاضر نظری ندارم.

استفان:

درباره سایر چیزهای بیت‌کوین چطور؟ مفاهیمی مثل Schnorr (شنور الگوریتم جدیدی برای تولید کلیدهای عمومی خصوصی و ادغام امضا است و هنوز روی شبکه بیتکوین فعال نشده است. -م) چند امضایی و کانال های پرداخت (کانال‌های لایتنینگ) چطور فکر می‌کنی؟

سامورای:

Schnorr خیلی خیلی هیجان انگیز است. من فکر می‌کنم که نوآوری خیلی بزرگی است و باعث ایجاد نوآوری‌های بزرگی هم خواهد شد. برای پروتکل Dandelion نیز واقعا هیجان زده هستیم و امیدواریم هر چه زودتر راه بیوفتد (دندلاین پروتکلی برای انتشار تراکنش بین فول‌نودها است که نظارت در سطح شبکه اینترنت را با چالش مواجه میکند – این قابلیت هنوز فعال نشده و احتمالا به دلایل متفاوتی که باعث ایجاد محدودیت می‌شوند کنار گذاشته شود. -م). من با کانال‌های پرداخت آشنا نیستم. اطلاعاتی ندارم باید در باره آن مطالعه کنم.

استفان:

بله. رابطه بین والت‌های بیت‌کوین و والت‌های لایتنینگ را چطور میبینید؟ به نظر شما تمام والت‌های بیت‌کوین در نهایت لایتنینگ را در استفاده خواهند کرد؟ یا اینکه نقش های متفاوتی را ایفا خواهد کرد؟ به عنوان مثال من می‌دانم که شما محصول دیگری به نام Sentinel دارید که به کاربران این امکان را می‌دهد که Xpub ها را در آن قرار دهند و والت خود را زیر نظر بگیرند. به نظر شما مردم ممکن است sentinel یا والت های بیت‌کوین خوب را داشته باشند و از لایتنینگ برای پرداخت های هر روزه خود استفاده کنند. به نظر شما عملی هست که مردم دوتا والت روی تلفن همراه خود استفاده کنند؟

سامورای:

سوال خوبی است من در این باره زیاد فکر کرده‌ام. صادقانه بگویم، یک چیزی را که مطمئنم این است که افراد می‌توانند بدون هیچ مشکلی، بیشتر از یک والت بیت‌کوین را در گوشی خود اجرا کنند. خیلی از کاربرها در حال حاضر این کار را می‌کنند. بجز بیت‌کوین میبینم که خیلی افراد ۳ یا ۴ تا اپلیکیشن چت را همزمان با همم اجرا می‌کنند. فکر می‌کنم چیزی که در نهایت اتفاق خواهد افتاد تخصصی شدن است. والت مخصوص لایتنینگ را خواهید داشت و والت بیت‌کوین روی شبکه اصلی را هم خواهید داشت. به نظر من یه این شکل بهتر است و تخصصی سازی خوب است. احتمالا شما با این رویکرد موافق نباشید و رویکرد متفاوتی داشته باشید، بلاخره می‌بینیم که چه اتفاقی خواهد افتاد. اما خب بله چیزهای زیادی را درباره لایتنینگ ببینیم. ما در مورد لایتنینگ به عنوان یک تکنولوژی خیلی هیجان زده هستیم و من فکر می‌کنم که مهم است که زیر ساخت‌های آن اکنون ایجاد شوند. به نظر من لایتنینگ از این قبیل پروژه‌ها نیست که شما نرم‌افزار را بسازید و کاربران به سمت آن روی بیاورند بلکه به این شکل است که لایتنینگ را باید بسازید و

آماده کنید و هنگامی که آماده شد کاربرانی که به آن نیاز داشته باشند از آن استفاده خواهند کرد. اما مطمئن هم نیستم. به نظر من این یک توسعه مثبت در این فضا است. زیرساخت‌ها به گونه‌ای ایجاد شده اند که اگر نیاز باشد آماده خواهند بود.

استفان:

بله درسته، راه خوبی برای فکر کردن در این باره است. درباره مقابله با سانسور چطور؟ اخیرا نمونه هایی بوده اند که افراد متوقف شده اند. مثلا Alex Jones (م. مجری و صاحب برنامه تلویزیونی) از رسانه‌های اجتماعی زیادی اخراج شد. فکر می‌کنید والت سامورایی ممکن است از Google Play یا App Store اخراج شود؟ و آیا برای چنین شرایطی برنامه ای دارید؟

سامورای:

بله، قطعا ما برای همچین موقعیتی فکر کرده‌ایم، باید دیوانه باشیم که به چنین چیزی فکر نکنیم. در حال حاضر برای عرضه از گوگل پلی استفاده می‌کنیم، تنها روشی است که در حال حاضر داریم. چون نرم‌افزار در حال حاضر نسخه آلفا (اولیه) است، و می‌خواهیم نصب از روش APK را محدود کنیم، چون می‌خواهیم مطمئن شویم که کاربران نرم‌افزار والت را به سرعت اپدیت میکنند و باگ‌هایی که لازم است برطرف می‌شوند. پس اگر الان گوگل پلی ما را بیرون بیندازد با مشکل روبرو می‌شویم. احتمال چنین مشکلاتی را می‌دهیم. ولی دلیلی وجود ندارد که نتوانیم سریعاً به F-Droid (یک اپ استور برای نرم افزارهای آزاد. –م) برویم یا لینک دانلود مستقیم بگذاریم یا از اپ استورهای دیگر استفاده کنیم، همه این ها برای ما باز هستند. ما قصد داریم که برای نسخه ۱.۰ صد درصد از دانلود مستقیم و F-Droid استفاده کنیم. بنا بر این وقتی نسخه ۱.۰ را منتشر کنیم چندین روش برای دریافت

محصول خواهیم داشت و به نظرم مشکل بزرگی برا ما نخواهد بود. یادم می‌آید قبل از اینکه گوگل پلی اجازه دهد که اپلیکیشن‌های شرط‌بندی و قمار در پلی‌استور قرار بگیرند، با اینکه در خیلی از کشور ها قانونی بودند، این شرکت‌ها اپلیکیشن‌های موبایلی داشتند و اپلیکیشن‌ها را به مشتریان‌شان عرضه می‌کردند و میلیون‌ها مشتری هم از اپلیکیشن آن‌ها استفاده می‌کردند. پس اگر آنها مشکلی برای عرضه اپلیکیشن ایجاد کنند ما هم حتما راه هایی برای حل آن خواهم داشت. به نظر من اگر مردم اپلیکیشنی را بخواهند آن را به‌دست خواهند آورد. شاید هم حتی باعث تبلیغ ساموراییی شود. مردم بگویند که این بچه‌های بدی که بیرون‌شان کرده‌اند را کجا می‌توانیم پیدا کنیم؟

(هم‌اکنون ساموری والت به جز گوگل‌پلی در وبسایت رسمی خودشان قابل دانلود است و در اپ استورهای آزاد دیگری مانند F-Droid و اپ استور کاپرهد و آورارا قابل دانلود است. -م)

استفان:

مثل Barbara Streisand (م. اثر باربرا استرایسند که به نام بازیگر آمریکایی است و اشاره به این دارد که در برخی رخدادها سعی به پنهان کردن یا بازدارندگی امری باعث جلب توجه بیشتر به آن شود)

سامورای:

امیدوارم که همچین اتفاقی نیفتد. ما قوانین پلی استور گوگل را هر بار که تغییری در آن ایجاد می‌شود مرور می‌کنیم تا مطمئن شویم که هیچ قانونی را زیر پا نمی‌گذاریم. ما با گوگل به خوبی کار میکنیم. با گوگل به گونه‌ای همکاری داریم که مثلا به آنها می‌گوییم همچین کاری را می‌خواهیم انجام دهیم، مشکلی نیست؟ انها هم

می‌گویند که این کار باعث نقض قوانین است نباید انجام دهید.کار با گوگل به نسبت اپل یا دیگر اکوسیستم‌ها خیلی خیلی راحت‌تر است. اما برای اپل باید با احتیاط شدید تری عمل کنیم چون برای وارد شدن به اپ استور اپل نه تنها باید زمان زیادی صرف کنیم بلکه هزینه زیادی را هم باید بپردازیم و اخراج شدن از اپ استور هم یک احتمال همیشگی است به همین دلیل اصلا آنرا نمی‌خواهیم.

استفان:

من خودم کاربر اندروید هستم اما نسخه آیفون کی میاد؟

ساموررای:

در حال کار روی آن هستیم. به زودی در اپ استور آیفون خواهد آمد. خود والت سامورایی هم توسعه‌هایی داشته که امیدواریم اوایل سال جدید آن را ارائه دهیم. (برنامه‌ی ساموررای والت برای عرضه نرم افزار روی آیفون اکنون تغییر کرده و عرضه در آیفون برای آن‌ها در اولویت نیست. -م)

استفان:

خوبه، چیز دیگری هم هست؟ فکر می‌کنم درباره بعضی از قابلیت‌ها صحبت کردیم اما به نظرت قابلیت یا بروزرسانی جدیدی هست که مخاطبان ما باید منتظر آن باشند؟

ساموورای:

ما درباره همه چیزهایی که به صورت عمومی می‌توانستیم به آنها بپردازیم صحبت کردیم، تراکنش هایی از نوع Post Mix که کار بزرگی است،Stowaway Ricochet همه اینها بهبود یافته اند، Trusted node ها بهبود یافته‌اند و با چیزی که ما به آن Dojo میگوییم جایگزین شده‌اند. فکر کنم این یکی را قبلا نگفتم. ما می‌خواهیم آنرا با یک سرویس‌دهنده فول نود ادغام کنیم تا کاربران بتوانند در موبایل خود از طریق سرویس‌های Tor ، تجربه‌ای ساده برای اتصال به فول نود داشته باشند. همه اینا در حال آماده سازی هستند. ما یک تیم کوچک هستیم و خودمان بودجه مورد نیاز خودمان را تامین می کنیم. هدف ما همان‌طور که در ابتدا گفتید نه تنها VC ها نمی‌خواهند سرمایه‌گذاری کنند، واقعا هم ساختاری برای سرمایه گذاری روی سامورای والت وجود ندارد.VC ها در کل آن را دوست ندارند.

استفان:

در باره این موضوع، اگر کسی بخواهد از شما حمایت کند چطور میتواند؟ خب این یک ابزار اوپن سورس است، میتوانند از طریق بیتکوین حمایت مالی ارسال کنند؟ آیا می‌توانند از Ricochet استفاده کنند؟

ساموورای:

بله، همه اینها هستند. ما در github و وبسایت خودمان دردسترس هستیم. شما می‌توانید به قست issue در انجا مراجعه کنید، می‌توانید درخواست ارسال کنید، در تلگرام با ما درباره قابلیت‌ها صحبت کنید. از Ricochet استفاده کنید. صادقانه بگویم این بزرگترین راهی است که می‌توانید از ما حمایت مالی کنید. از آن وقتی می‌خواهید به یک اکسچنج واریز کنید از آن استفاده کنید. در یک کنفرانس فردی

را ملاقات کردم که می‌گفت من برای خرید این بطری آب از Ricochet استفاده کرده ام. نه خدای من، ما از کاربران همچین چیزی را نمی‌خواهیم فقط وقتی قرار است به باینس یا کوین‌بیس بیت‌کوین بفرستید از Ricochet استفاده کنید. همچنین می‌توانید در وبسایت ما حمایت مالی کنید. فکر می‌کنم اینجا یک کد پرداخت داشته باشیم که میتوانید استفاده کنیم، همچنین یک آدرس ثابت داریم که اگر بخواهید می‌توانید از آن استفاده کنید.

استفان:

به عنوان کلام آخر. توصیه ای برای کاربران داری در مورد حفظ حریم خصوصی به صورت کلی نه فقط در بیت‌کوین؟

سامورای:

توییت های lopp را در توییتر چک کنید به نظر من او درک خوبی از تکنولوژی های حریم خصوصی خارج از بیت‌کوین دارد.

استفان:

عالی بود. صحبت هایی خیلی خوبی داشتیم. به نظر من خیلی آموزنده بودند و چیزهای زیادی درباره نحوه ساخت تراکنش‌ها و ابتکارات مختلفی که در پروژه داشتید، یاد گرفتم. به نظر من پروژه خیلی خوبی است. ممنون که آمدی.

سامورای:

ممنونم که منو دعوت کردید. عالی بود.

ترجمه متن اپیزود شماره ۲۹ پادکست استفان لیورا توسط nodrunner و بازبینی و صفحه‌بندی آن توسط سایت منابع فارسی انجام شده است.

هرگونه استفاده از این ترجمه برای همگان آزاد است.