

# پادکست استفان لیورا

قسمت ۲۹

کیف پول سامورایی  
و ابزارهای حفظ حریم خصوصی در بیت کوین



Samurai 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 سامورایی 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 اخیراً به ما پیوسته‌اند بگوییم که، خیلی از افراد در فضای بیت کوین 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. خوب عنوان یک مقدمه خیلی سریع بگوییم که، والت سامورایی پروژه خیلی جالبی است و من برای مدتی آن را دنبال می‌کردم. والت را امتحان کرده‌ام، به نظر من والت بیت کوینی آسان و ساده‌ای است. توسعه‌دهنده‌های والت سامورایی از بحث و گفتگو فرار نمی‌کنند و موضع سخت‌گیرانه‌ای در زمینه حفظ حریم خصوصی دارند، و چنین نگرشی بسیار عالی است. می‌توانیم با توسعه سامورایی والت مباحث را شروع کنیم، ویژگی‌ها، اهداف و حریم خصوصی در سامورایی والت. در وبسایت شما این شعار را دیدم که «ما فعالان در زمینه حریم خصوصی 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 بیت کوین 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 مهمان‌های قبلی من Adam Fiscor، مدیر فنی و توسعه‌دهنده ارشد والت واسابی است، که والت دیگری با تمرکز بر حریم خصوصی است که از فریم‌ورک 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 (فریم ورک یک ساختار مفهومی است که نرم افزارهای متفاوتی می‌توانند روی آن توسعه مخصوص خود را انجام دهند. - م). ادم فیسکور حدوداً 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 فریم ورک 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 بلاک چین بیت کوین طراحی شده‌اند. شرکت‌های تحلیل بلاکچین سعی به اکتشاف ارتباط آدرس‌ها و اطلاعات دیگر روی شبکه بیت کوین دارند. من معمولاً به این شرکت‌ها جاسوسان بلاک چین می‌گویم. اگر مفهوم کوین‌های لکه‌دار را قبول داشته باشید، (که من شخصاً 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 بلاک چین 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 شرکت‌های 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) بیت کوین بسیار مهم است. از نظر ایدئولوژیکی و از نظر کاربردی، اگر قابلیت تعویض پذیری نداشته باشیم ارزش بیت کوین به طور بنیادی پایین می‌آید.

## استفان:

درسته. این شرکت‌ها به روش‌های بسیاری می‌توانند حریم خصوصی شما رو از بین ببرند، روش‌هایی که مستقیماً در لایه تراکنش (شبکه بلاک چین) و بر اساس روش‌های کشف عمل می‌کنند. مثلاً اگر چند UTXO در یک تراکنش ادغام شوند، شرکت‌های آنالیز کننده بلاک چین 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 آنها 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، در مورد روش‌های شناسایی و درباره حملات متعدد به حریم خصوصی برایمان بگو.

## سامورای:

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

شبکه اینترنت هم استفاده می کنند، اگر از یک سرویس VPN شناخته شده یا شبکه Tor استفاده کنید، همه این اطلاعات را در کنار هم قرار می دهند و یک پروفایل از شما می سازند. تمام اینها از گذشته دغدغه های مختلف امنیتی و حریم خصوصی بوده اند ولی تمرکز ما روی حریم خصوصی در بلاک چین است. به همین دلیل چیزی که سامورایی می خواهد روی آن تمرکز کند، این است که کاربران بتوانند تراکنش هایی 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 بیت کوین از شخصی دریافت کرده اید. فرضاً اولین بیت کوین های شما هستند. این کوین ها ممکن است از دید شرکت های تحلیل بلاک چین لکه دار<sup>1</sup> به شمار بیایند، چون مثلاً در ارتباط با هک اکسچنج مت گاکس (Mt.GOX) باشند. ممکن است چنین چیزی را تجربه کنید که آن لحظه ای که بیت کوین خود را به اکسچنجی انتقال دهید آن گاه شرکت های تحلیل بلاک چین وارد عمل می شوند و اکسچنج با این اطلاعات فراهم شده از شرکت های تحلیل بلاک چین تصمیم بگیرد فعالیت شما را متوقف و دارایی شما را مسدود کند. اینجا اولین تجربه شما کاملاً منفی است در حالی که اشتباهی مرتکب نشده اید. هدف سامورایی جلوگیری از چنین اتفاق هایی 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 در این باره حرف بزنیم. به نظر شما تحت فشار زیادی از طرف جامعه بیت کوین قرار گرفتید درست است؟

## سامورای:

خیر در واقع. واکنش‌ها خیلی دلگرم کننده‌تر از چیزی بود که حدس می‌زدیم. 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<sup>۲</sup> یا همچین چیزی داشته باشیم یا اینکه شما فقط و فقط باید به بیت کوین فکر کنید، چون این امر حقیقت دنیای واقعی اطراف مان 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 این است که مشکل فهم بیت کوین در آموزش آن است و با این توجیه بی‌تفاوت از آن رد می‌شویم، انگار وقتی صحبت از کاربران جدید و نیاز آنها به یادگیری می‌رسد مشکل فقط در آموزش است. درست است مفاهیم شبکه بیت کوین 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 بیت کوین، برای کاربرانی که هرگز نمی‌خواهند یاد بگیرند مثل

2 Circular economy

عصا عمل می کند و آن‌ها را به آموزش ندیدن تشویق می کند. ما کاربرانی داشته‌ایم که پس از ۱۰ ماه استفاده و یا حتی پس از یک سال استفاده از والت سامورایی به پشتیبانی ایمیل می‌زنند و به معیار پول فیات درخواست پشتیبانی می‌کنند. مثلاً 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 کاملاً متفاوتی مواجه میشوند و فکر می‌کنند که از آنها 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 عملاً رایج است. دلیل بیشتر سر در گمی‌ها این بود چون دو تا قیمت بیت کوین 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، درخواست‌های 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؟



## سامورای:

بله بسیار زیاد! اما تعداد درخواست‌های پشتیبانی مهم و معقول هم زیاد بود که به دلیل بیان کردن مقدار دلاری (فیات) پیچیده می‌شدند. مثلاً پیش می‌آید که دیگر کاربران ایمیل می‌داند و می‌گفتند ما نمی‌توانیم مقدار خروجی باقی‌مانده<sup>۳</sup> را در والت بینیم و چنین چیزهایی. معمولاً مشکلاتی از قبیل مشکل ارتباط اینترنتی با Tor هستند که مشخصاً نیاز به بازبینی دارند، اما تشخیص اینکه در مورد کدام UTXO صحبت می‌کنند خیلی سخت است. چون مقدار بیت کوین به معادل دلاری در هر لحظه می‌تواند مبلغ بسیار متفاوتی باشد. به همین دلیل فهمیدن اینکه مشکل دقیقاً چیست و حل کردن آن نیاز به بررسی بیشتری دارد. حالا یک نفر مسئول پشتیبانی در والت سامورایی 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 بیاید، اما خب حذف مقدار فیات (دلاری) یکی از راه‌های کاهش مشکلات است و ارزشش را هم دارد، چون مسائل پیش پا افتاده‌ای مثل تغییر قیمت بیت کوین 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 تأثیری روی حذف و نصب نرم افزار داشته است؟ و خیر، تأثیری 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 زاویه‌ای 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، عالی. خب بهتره در باره PayNym، یا همان BIP47 صحبت کنیم. قبل تر عنوان کردی که افراد آدرس های خود را در شبکه های اجتماعی قرار می دهند و این مشکلی همیشگی و جدی برای حریم خصوصی است. کمی در این باره بگو که PayNym چطور می تواند در این موضوع به ما کمک کند.

## سامورای:

دقیقا یکی از بهترین موارد استفاده از PayNym برای رفع مشکل حریم خصوصی آدرس ها در دریافت حمایت های مالی (donation) است. وقتی شما می خواهید به صورت عمومی کمک های مالی دریافت کنید، ساده ترین روش همان روش پیش فرض بیت کوین است، به این شکل که، این کد QR آدرس بیت کوین من است، مقداری بیت کوین 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 شناسه های دیجیتالی دیگری از شما باشند. شما این شناسه را به یک آدرس خاص وصل میکنید و هر کسی که به این آدرس پول بفرستند ممکن است بتواند هویت شما را شناسایی کند که این یک مشکل حریم خصوصی است، به خصوص با در نظر گرفتن این واقعیت که بلاک چین قابل تغییر نیست<sup>۴</sup> و همه میتوانند همیشه به عقب برگردند و بلاک چین 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 می دهد یک کد ثابت را که تغییر نمی کند به اشتراک بگذارید، اما این امکان را برای کاربران فراهم می کند که به این کد، بیت کوین ارسال کنند بدون اینکه موجودی آدرس کمک های مالی را افشا کند یا تاریخچه تراکنش های آن را نشان دهد. در

---

4 immutable

نهایت 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) با آدرس‌های مخفی انجام میداد با این تفاوت که برای رسیدن به این هدف به جای استفاده از سرور از بلاک چین استفاده می‌کنیم.

### استفان:

خیلی جالبه، و اینکه آیا تنها نکته منفی این است که نمیتوانید مستقیماً 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 بیت کوین 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 نوتیفیکیشن‌ها 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 بلاک چین دارد. وقتی شما می‌خواهید چیز کوچکی را بازیابی کنید، برای اینکه والد 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 پرداخت های فوری دارند می‌توانند در یک حالت امن این کار را انجام دهند بدون اینکه حریم خصوصی آنها به خطر بیفتد. این کار با تبدیل های مختلفی صورت می‌گیرد، مثل بازیابی از بلاک چین به جای بازیابی از سرور رمزنگاری شده یا همچنین 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 صحبت های Adam Back و Matt Corallo (ادم بک مدیر شرکت بلاک استریم و مبدع هش کش در دهه ۹۰ میلادی که ساتوشی ایده ی 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 می گفتند که شرکت های آنالیز کننده بلاک چین در تاریخچه تراکنش ها معمولا ۴ یا ۵ گام به عقب برمی گردند و اگر در این گام ها مورد مشکوکی اتفاق افتاده باشد آنرا تحت رصد قرار می دهند. اگر به این موضوع فکر کنید، دیوانه کننده است. ۵ تراکنش قبل تر می تواند شامل افراد زیادی با فعالیت های متفاوتی باشد. از مرتبط کردن فردی که الان پول ارسال کرده به گذشته تراکنش های 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 گام های اضافه ای به تاریخچه تراکنش ها اضافه می شوند. از آنجایی که این کار چندان عجیب و غریب نیست. آنالیز کننده ها ۵ گام به عقب برمی گردند و می بینند که هیچ UTXO یا تراکنشی با آنچه در بلک لیست یا فعالیت های مشکوک آنها مطابقت داشته باشد پیدا نمی کنند، و اگر این طور نباشد عملیات موفقیت آمیز بوده است. مثل چک کردن در گمرک است یا در واقع نرم افزار آنالیز بلاکچین این شرکت ها را تبدیل به یک مامور گمرک بی انگیزه و بی حوصله می کنیم که به همه می گوید برو برو. این مامور طبق پروتکل درست وظیفه خود را انجام می دهد اما به نتیجه لازم نمی رسد. خب ما به راحتی می توانیم این کار را انجام دهیم و این کار را هم کردیم، Ricochet را ایجاد کردیم که ۴ قدم را به تراکنش اضافه می کند. Ricochet را کمی بیشتر از یک سال است که ارائه کرده ایم. و کاربران زیادی از آن استفاده می کنند و هرگز شکایتی نداشته ایم، هیچ وقت کسی نگفته که حسابش بسته شده یا موارد مشابه دیگر، پس به نظر می رسد 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 می کنند که صادقانه بگوییم، یکی از دلایل ادامه دادن ما است. با مقدار پولی که ما از آن دریافت میکنیم می توانیم هزینه های اجرایی، سرورها، نودها و کارمندها را پردازیم. Ricochet برای ما و همچنین کل اکوسیستم قابلیت مهمی است. دانستن این نکته هم مهم است که افراد آنالیز کننده بلاک چین برای مبارزه با

Ricochet باید هزینه بیشتری پرداخت کنند، چون به این مسئله فکر کنید: هر تراکنشی که وارد پلتفرم میشود، آنها 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 هزینه‌های 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 بی کیفیت تلقی خواهد کرد. این موضوع به سادگی در عوامل و انگیزه‌های اقتصادی خلاصه می‌شود. احتمالاً 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.

### سامورای:

در حال حاضر هم همین طور است، یعنی اگر فقط ۵ گام به عقب برگردند و بدون اینکه از شما 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.

## سامورای:

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 مثلاً ۲۵ بلاک بعد از زمانی باشد که Ricochet را شروع کرده‌اید. این کار ردپای Ricochet را برای پیدا کردن آن کاملاً پاک می‌کند. باید کمی خصومت آمیز 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 توییح 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 قوی برای آن باشد.

## استفان:

بله. همان طور که شما گفتید افراد از این عبارت به صورت غیر امنی استفاده می کنند. که شبیه به موش و گربه بازی است. یک سمت که تلاش بیشتری می کند سمت دیگر نیز تلاش خود را بیشتر می کند. خب یک نکته جالب هست که میخواهم سوال کنم. مثالی مانند واکسن و ایمنی جمعی که ایجاد می کند را در نظر بگیرید. آیا همچین مفهومی در بیت کوین داریم؟ که اگر تعداد کافی از افراد از این نوع تکنیک های حریم خصوصی و قابلیت هایی مثل کوین جوین، Stonewall و Ricochet استفاده کنند، باعث می شود حتی کاربرانی هم که از این قابلیت ها استفاده نمی کنند محافظت شوند؟

## سامورای:

قطعاً بله. فکر میکنم ادام فیسکور مقاله ای را در وبلاگ مدیوم<sup>۵</sup> خود نوشته بود با عنوان «حریم خصوصی یک کار تیمی است». مقاله درباره تشویق مردم برای استفاده از حریم خصوصی است. مسأله، محافظت از مجرمان و کمک به پول شویی یا چیزهایی از این قبیل نیست، بلکه حقوق اساسی اشخاص است، درباره حق داشتن حریم خصوصی در تراکنش ها است و اصلاً 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 می دهید به اندازه صحبت های شما مهم است به همین دلیل اصلاً جای بحث ندارد. برای همین من علاقه مند به ارتقای حریم خصوصی در سطح پروتکل بیت کوین هستم. این یک گام بزرگ برای رسیدن به این موقعیت مناسب برای حفظ حریم خصوصی کاربران بیت کوین 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

---

5 medium



نباشند. درست مثل whatsapp، که رمزنگاری آنها احتمالا خیلی هم عالی نیست اما رمز نگاری را برای همه قرار داده است. حتی آوردن کلمه رمزنگاری باعث می شود شما کمی آگاهی پیدا کنید که در آن چه اتفاقاتی در جریان است. من درباره نوعی تغییر صحبت می کنم که به آن نیاز داریم و چیزی نیست که والت سامورایی 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 پیاده سازی شده است. کمی در این باره برای ما بگو.

### سامورای:

بله، حتما. خب Stonewall تراکنش هایی را ایجاد می کند که به لحاظ ریاضی فرقی با یک تراکنش کوین جوین ندارند و در کل به صورت دیداری قابل تشخیص نیستند. در واقع شبیه به تراکنشی است که چند نفر به هم پیوسته اند تا یک تراکنش میکس معمولی را ایجاد کنند. شبیه به تراکنش های والت واسابی است به عنوان مثال، یا تراکنش های جوین مارکت و غیره. اما البته هیچ یک از این ها نیست، این قابلیت فقط والت شماس است، یک ترفند است، یک کوین جوین 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 شرکت های آنالیز کننده بلاکچین است. از نظر ریاضی آنالیز کننده ها نمی توانند به طور قطعی مشخص کنند که ورودی ها در

یک تراکنش Stonewall متعلق به یک والت است، همچنین نمی‌توانند تشخیص دهند که کدام خروجی مربوط به باقی پول<sup>۶</sup> 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<sup>۷</sup> در سامورایی به صورت دستی انجام شود یا اینکه به صورت خودکار انجام می‌شود.

## سامورای:

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 سامورایی 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، فعال تر میشود. اگر stonewall بتواند فعال شود، قوانین انتخاب کوین دیگری هم هستند که در والت سامورایی 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 UTXO ها در هیچ تراکنش دیگری

6 Change output

7 Coin selection

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

## استفان:

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

## سامورای:

خودم هم می خواستم به همین برسم چون با مسئله انتخاب کوین مرتبط است. امروزه بیشتر مقاله های آکادمیک و بیشتر تحقیقات درباره انتخاب UTXO اغلب درباره مبلغ و قدمت UTXO بوده اند. برای همین کاری که ما می کنیم این است که یک گام جلوتر برداریم و این گونه است که Boltzmann به این موضوع گره می خورد. چون Boltzmann به چیزی بیشتر از مبلغ و قدمت UTXO ها نگاه می کند. Boltzmann به چیزی به نام آنتروپی و همچنین راندمان حریم خصوصی والت برای یک تراکنش هم نگاه می کند. آنتروپی تراکنش، تعداد ترکیب هایی است که بین ورودی ها و خروجی ها، از نظر ریاضی ممکن است. یعنی به چند روش مختلف می توانید 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 می توانیم 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. مثلاً 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 هم اکنون 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 بیت کوین به والت شما ارسال میشود، معمولاً مقدار خیلی خیلی کمی است.

## استفان:

آها، مقدار خیلی کمی بیت کوین رایگان است؟

## سامورای:

بله اما بعدش شما آن بیت کوین را خرج می کنید، معمولا در یک تراکنش با ورودی های دیگر ادغام می شود، چون مقدار خیلی کمی است. خب حالا به شما دسترسی دارند، در واقع یک زنجیره از تراکنش های آتی شما برای حمله کننده ایجاد شده است که با دنبال کردن آن می تواند از همه چیز مرتبط به تراکنش های بیت کوین شما مطلع شود. با والت سامورایی می توانید 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 می گویند نصف والتمان را به عنوان غیر قابل خرج تیک زده ام و کلا فراموش کرده ام که آن ها را دارم، چون این مقادیر از مانده حساب کم می شود و شما نمی توانید آن را ببینید. باید به لیست UTXO ها برگردید و به عنوان قابل خرج آن ها را علامت گذاری کنید. مردم می گویند مثل این است که از جیب لباس مان یک اسکناس ۲۰ دلاری پیدا کردیم!

## استفان:

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

## سامورای:

درسته، بله.

## استفان:

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

## سامورای:

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 می گوئیم. به هر حال شما باید بیتکوین های میکس شده را زمانی خرج کنید، خود شما هم شاید فراموش نکنید اما خیلی از افراد فراموش می کنند و اگر مراقبت نشود نوع خرج کردن شما می تواند 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 سامورایی انجام میشود به این دلیل که نیازمند PayNym است و در حال حاضر فقط والت سامورایی 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 به کلی برطرف شده و این ابزار به سادگی و با استفاده از قابلیت سوروبان قابل استفاده است. -م)

### استفان:

منظور شما اینه که ممکن است کوین های شما به سرقت بروند یا اینکه فقط به شناسایی شدن شما کمک می کند؟

### سامورای:

کسی نمی تواند کوین های شما را بدزدد یا از مانده حساب شما مطلع شود یا چنین چیزهایی. تراکنش به این صورت عمل می کند که شما برای آنها بیت کوین ارسال میکنید. به عنوان مثال من می خواهم یک بیت کوین برای شما ارسال کنم و یک UTXO دو بیت کوینی دارم. اگر تراکنش من معمولی باشد، یک ورودی دو بیت کوینی داریم و در خروجی دو تا UTXO وجود دارد که هر کدام یک بیت کوین هستند. یکی برای شما ارسال می شود و دیگری به خودم برمی گردد. این یک تراکنش استاندارد است. خب حالا اگر از Stowaway استفاده کنیم، ورودی هنور هم برای من ۲ است.

### استفان:

چطوری؟

## سامورای:

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 بیت کوین داری. پس ما از UTXO دو بیت کوین که شما هم دارید استفاده می‌کنیم. خب تراکنش شما حالا یک ورودی ۲ بیت کوین از من دارد و یک ورودی دو بیت کوین از شما. یک خروجی سه تایی برای شما و یک خروجی یکی به من بر می‌گردد.

## استفان:

خیلی جالب است.

## سامورای:

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 بیت کوین ارسال کنیم. و آنها هم باید در مجموعه مشارکت کنند. پیچیده است. این روش را ما اختراع نکرده‌ایم و اعتبار کشف آن به گرگوری مکسول می‌رسد. سال پیش گرگ مکسول (یکی از توسعه‌دهندگان قدیمی و بسیار تاثیرگذار در روند توسعه بیت کوین در دهه اخیر. - م) ایده‌ای در این باره داشت که ما آن را در گفتگوهای درباره بیت کوین پیدا کردیم که به جایی هم نرسید. فکر می‌کنم او یکی از این تراکنش‌ها را دستی ایجاد کرده بود، و همانجا هم در انجمنی که بحث میشد هم این موضوع پایان یافت. افراد در آنجا مشارکت میکردند و UTXO های خود را در اختیار قرار می‌دادند تا مثلاً



مورد استفاده قرار بگیرند. ما آن تراکنش را پیدا کردیم و گفتیم چه تراکنش جالبی. در واقع یک کوین جوین کوچک است چون شما با یک نفر مشارکت دارید، یک کوین جوین بزرگ با چند نفر انجام نمی‌دهید، یک تراکنش یک یا دو نفره انجام می‌دهید. اما 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 طرفد هوشمندانه است، کاری که انجام می‌دهد این است که مجدداً مثل دیگر قابلیت‌هایی که صحبت کردیم به فرضیات حمله می‌کند. Stowaway خیلی شبیه به تراکنش معمولی بیت کوین است، کاملاً استاندارد، در حالی که اینطور نیست. هر دوی آن ورودی‌ها 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 شرکت‌های 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 هوشمندانه‌ای 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 خوبی‌های موبایلی بودن است. شما تعداد نسبتاً 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 فریم ورک 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 سریع تر خواهند بود.

## استفان:

انگیزه مالی آن بر چه پایه‌ای بنا شده است؟

## سامورای:

در حال حاضر ۱۰۰ درصد آماده نیستم که به آن پردازیم، 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 پرداخته 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

می آورید. 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 می کنم Luke JR و David Harding (دیوید هاردینگ یکی از توسعه دهندگان و نگه دارندگان پروژه های مختلف بیت کوین مانند وبسایت بیت کوین کور و مدیریت انجمن IRC بیت کوین است. - م) گفته بودند که اگر Trusted node ها به درستی اجرا نشوند، کاربران را در معرض خطرات بیشتری قرار می دهد، چون پورت RPC را در اینترنت قرار می دهد. توضیحی در این باره داری؟ یا اینکه راه پیشنهادی برای استفاده از آن داری؟ (این قابلیت در کیف پول سامورایی وجود داشت و باعث به راه افتادن بحث های زیادی شد. - م)

## سامورای:

ابتدا باید این نکته مهم را بگویم که به ندرت بحث ها و گفتگوهای نتیجه دار درباره موضوعات مهم در جاهایی مثل توئیتر پیدا می کنیم، 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 پی گیری موضوع را سخت تر میکند. همچنین مقابله با اطلاعات نادرست و یا اطلاعاتی که بازگو نشده اند را هم سخت تر میکند. اما خوشبختانه در آینده قادر خواهیم بود چنین موضوعاتی را به Github ببریم. من فکر می کنم که متد RPC که برای اتصال کاربران به فول نود است، باعث ایجاد یک حفره امنیتی نمی شود. احتمالاً منظور Luke این بوده که سیستم عددی Tonal برای افراد عادی

آسان تر خواهد شد. من بی احترامی نمی‌کنم چون Luke برای من بسیار قابل احترام است. اما به نظر من منظور او این بوده است. من شخصا وقتی بیت کوین کور<sup>۸</sup> 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 BTC D این کار را به صورت پیش فرض انجام داده. بیشتر روش‌های RPC از SSL و TLS استفاده می‌کنند، پس فکر نمی‌کنم 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 اندازی trusted nodeها برای UASF، گزینه Tor برای ما در دسترس نبود. من فکر می‌کنم 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 می‌کنید منتشر می‌کند نه از هر نودی. سربرگ Proof of work در بلاک را از گره شما میگیرد و آنها را با نودهای ما مقایسه میکند و اگر تفاوتی وجود داشته باشد به شما هشدار می‌دهد 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 جریان UASF 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 دارید که اطلاعات درست به شما می‌دهد. نرم‌افزار

کیف پول سامورایی 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 می گفتیم که خب اگر کاربری می خواهد سافت فورکی 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 می کند و بی تاثیر نیست. آخرین چیزی که در حال حاضر انجام می شود دریافت اطلاعات کارمزد از mempool واقع در فول نود شما است. ما همیشه موافق این بوده ایم که برنامه های بیشتری برای اطمینان از عملکرد فول نود ارائه کنیم. در نهایت برای اطمینان پیدا کردن از نودها میتوان زیرساخت سامورایی 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.

## سامورای:

نه در چند هفته آینده چون زمان بندی ۱۰۰ درصدی را نمی توانم بگویم اما در چند ماه آینده حتما آپدیت جدید خواهیم داشت.

## استفان:

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

## سامورای:

کار کردن با تیم GoTenna پروژه خوبی بود. چند وقت پیش Mule tool (ابزار هایی برای انتشار تراکنش های بیت کوین بدون نیاز از اینترنت) را راه اندازی کردیم، که یکی از اقدامات تحقیق و توسعه ما در برابر سانسور کردن تراکنش ها است.، تمام راه های مختلف انتشار تراکنش ها و دریافت داده های بلاک ها، بدون استفاده از اینترنت است. GoTenna هم تصادفاً با این موضوع روبرو شد. فکر می کنم 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 بیت کوین به کاربرانشان و ارائه GoTenna به کاربران ما علاقه مند 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 راه حل ها و رویکردهای مفهومی فعلی خود را، که آن زمان به آن Pony Direct می گفتیم را توسعه دهیم. کاری که Pony Direct انجام می داد این بود که تراکنش ها را از طریق SMS انتشار می داد، برای زمانی که شما اینترنت ندارید بسیار مفید است و حتما کار می کند. خب ما تصمیم گرفتیم آن را بر پایه

SMS و یا شبکه مش<sup>۹</sup> 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، تراکنش‌ها به قسمت‌هایی تقسیم شوند و هر قسمت با فرمت خودش باشد تا بعداً بتواند دوباره بازسازی شود. تمام اینها اوپن سورس هستند. این اپلیکیشن در کنفرانس HCPP 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 بیت کوین 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 کاملاً هم امن بوده است. با این تکنولوژی که در دسترس است، تصور اینکه بیت کوین نابود شود، سناریو احمقانه‌ای است.

## سامورای:

هر روز هم تکنولوژی های بیشتری عرضه می شوند. من یک چیزی دیدم که تراکنش ها را با کدهای موریس از طریق رادیو منتشر می کرد. 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 می گیرند. این نوع ابزارها اگر چه ممکن است در حال حاضر نو ظهور باشند اما می توانند خیلی مهم باشند.

## استفان:

درسته بسته به اینکه کجا زندگی می کنید می تواند 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 می توانند 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 بخوایم صادق باشم، این کار نمی تواند والت شما را در برابر بررسی دقیق تلفن تان ایمن نگه دارد. اگر گوشی خود را باز کنید و آن را به نیروهای امنیتی یا هر کسی که قرار است آن را بررسی کند بدهید و آنها 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 کرده ام و توصیه ام برای کسی که از والت سامورایی



استفاده می‌کند این است که اگر پسرینز 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 بررسی‌های عمیق‌تری در تنظیمات و دسترس‌های 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 بیت کوین یا اپلیکیشن‌های 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 بیت کوین صحبت کنیم، که در طول زمان تغییرات زیادی داشته. صحبت از تراکنش‌های 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 بیت کوین 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 کانال‌های پرداخت (کانال‌های لایتینگ) چطور فکر می‌کنی؟

## سامورای:

Schnorr خیلی خیلی هیجان‌انگیز 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 بیت کوین و والت‌های لایت‌نینگ را چطور می‌بینید؟ به نظر شما تمام والت‌های بیت کوین در نهایت لایت‌نینگ را در استفاده خواهند کرد؟ یا اینکه نقش‌های 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 والت‌های بیت کوین خوب را داشته باشند و از لایت‌نینگ برای پرداخت‌های 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 بیت کوین را در گوشی خود اجرا کنند. خیلی از کاربرها در حال حاضر این کار را می‌کنند. بجز بیت کوین می‌بینم که خیلی افراد ۳ یا ۴ تا اپلیکیشن چت را همزمان با هم اجرا می‌کنند. فکر می‌کنم چیزی که در نهایت اتفاق خواهد افتاد تخصصی شدن است. والت مخصوص لایت‌نینگ را خواهید داشت و والت بیت کوین روی شبکه اصلی را هم خواهید داشت. به نظر من به این شکل بهتر است و تخصصی سازی خوب است. احتمالاً 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 بینیم. 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 نیستیم. 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؟ اخیراً نمونه‌هایی بوده اند که افراد متوقف شده اند. مثلاً 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 برنامه‌ای دارید؟

## سامورای:

بله، قطعاً ما برای همچنین 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 این‌ها 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 می آید قبل از اینکه گوگل پلی اجازه دهد که اپلیکیشن‌های شرط‌بندی و قمار در پلی‌استور قرار بگیرند، با اینکه در خیلی از کشورها 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 راه‌هایی برای حل آن خواهیم داشت. به نظر من اگر مردم اپلیکیشن‌ها را بخواهند آن را به دست خواهند آورد. شاید هم حتی باعث تبلیغ سامورایی شود. مردم بگویند که این بچه‌های بدی که بیرون‌شان کرده‌اند را کجا می‌توانیم پیدا کنیم؟

(هم‌اکنون سامورای والت به جز گوگل پلی در وبسایت رسمی خودشان قابل دانلود است و در اپ‌استورهای آزاد دیگری مانند F-Droid و اپ‌استور کاپرهد و آورا 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 پلی‌استور 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 مثلاً به آنها می‌گوییم همچین کاری را می‌خواهیم انجام دهیم، مشکلی نیست؟ آنها 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 پردازیم و اخراج شدن از اپ استور هم یک احتمال همیشگی است به همین دلیل اصلاً آنرا نمی‌خواهیم.

**استفان:**

من خودم کاربر اندروید هستم اما نسخه آیفون کی می‌آید؟

**سامورای:**

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 سامورای 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؟

## سامورای:

ما درباره همه چیزهایی که به صورت عمومی می‌توانستیم به آنها پردازیم صحبت کردیم، تراکنش‌هایی از نوع Post Mix که کار بزرگی است، Stowaway Ricochet همه اینها بهبود یافته‌اند، Trusted node ها بهبود یافته‌اند و با چیزی که ما به آن Dojo می‌گوییم جایگزین شده‌اند. فکر کنم این یکی را قبلاً نگفتم. ما می‌خواهیم آنها را 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 اینها در حال آماده‌سازی هستند. ما یک تیم کوچک هستیم و خودمان بودجه مورد نیاز خودمان را تامین می‌کنیم. هدف ما همان‌طور که در ابتدا گفتید نه تنها VC ها نمی‌خواهند سرمایه‌گذاری کنند، واقعا هم ساختاری برای سرمایه‌گذاری 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، میتواند از طریق بیتکوین حمایت مالی ارسال کنند؟ آیا می‌توانند از Ricochet استفاده کنند؟

## سامورای:

بله، همه اینها هستند. ما در github و وبسایت خودمان در دسترس 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 می گفت من برای خرید این بطری آب از Ricochet استفاده کرده ام. نه خدای من، ما از کاربران همچنین چیزی را نمی خواهیم فقط وقتی قرار است به بایننس یا کوین بیس بیت کوین بفرستید از Ricochet استفاده کنید. همچنین می توانید در وبسایت ما حمایت مالی کنید. فکر می کنم اینجا یک کد پرداخت داشته باشیم که میتوانید استفاده کنیم، همچنین یک آدرس ثابت داریم که اگر بخواهید می توانید 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 بیت کوین؟

### سامورای:

توییت های لopp را در تویتر چک کنید به نظر من او درک خوبی از تکنولوژی های حریم خصوصی خارج از بیت کوین دارد.

### استفان:

عالی بود. صحبت هایی خیلی خوبی داشتیم. به نظر من خیلی آموزنده بودند و چیزهای زیادی درباره نحوه ساخت تراکنش ها 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.

## bitcoind.me

---

### منابع فارسی بیت‌کوین

معرفی کتاب‌ها، مقالات، خودآموزها، و بطور کلی منابع آموزشی و کاربردی معتبر حوزه بیت‌کوین، اقتصاد، و حریم خصوصی که توسط علاقمندان و فعالان جامعه فارسی‌زبان بیت‌کوین تالیف یا ترجمه شده‌اند