Decentralization in Bitcoin Networks and a comparison to Ethereum Networks

توسط فرزین میرزائی بادیزی
99442299

خلاصه. ارزهای رمزپایه مبتنی بر بلاک چین نشان داده‌اند که چگونه می‌توان سیستم‌های متمرکز سنتی مانند ارزها را به شکلی غیرمتمرکز به‌طور ایمن پیاده‌سازی کرد. با این حال، مطالعات اندازه گیری کمی در مورد سطح عدم تمرکز آنها در عمل انجام شده است. ما یک مطالعه اندازه گیری در مورد معیارهای مختلف عدم تمرکز دو ارز دیجیتال پیشرو با بزرگترین سرمایه بازار و پایگاه کاربر، بیت کوین و اتریوم ارائه می کنیم. ما میزان تمرکززدایی را با اندازه‌گیری منابع شبکه گره‌ها و اتصال بین آنها، الزامات پروتکل مؤثر بر عملکرد گره‌ها و استحکام دو سیستم در برابر حملات بررسی می‌کنیم. به طور خاص، ما تکنیک‌های اندازه‌گیری اینترنتی موجود را تطبیق دادیم و از شبکه رله فالکون به عنوان ابزار اندازه‌گیری جدید برای به دست آوردن داده‌هایمان استفاده کردیم. ما متوجه شدیم که نه بیت کوین و نه اتریوم خواص بهتری نسبت به دیگری ندارند. ما همچنین پیشنهادهای ملموسی برای بهبود هر دو سیستم ارائه می دهیم.

1 مقدمه

تمرکززدایی یک ویژگی مربوط به تقسیم کنترل بر پروتکل است. در پروتکل‌های بیت‌کوین و اتریوم، کاربران تراکنش‌ها را برای ماینرها ارسال می‌کنند تا آن‌ها را در بلاک‌ها قرار دهند. تمرکززدایی بهتر ماینرها به معنای مقاومت بالاتر در برابر سانسور تراکنش های فردی است. برای ارتباط، بیت کوین و اتریوم همچنین دارای یک شبکه همتا به همتا برای انتشار بلاک ها و اطلاعات تراکنش هستند. هم بیت‌کوین و هم اتریوم دارای گره‌های کامل هستند که دو نقش مهم را ایفا می‌کنند: (1) انتقال بلوک‌ها و تراکنش‌ها به ماینرها (2) و پاسخگویی به سؤالات کاربران نهایی در مورد وضعیت بلاک چین. درک ویژگی های شبکه گره های کامل برای طراحی پروتکل و تجزیه و تحلیل انعطاف پذیری هر شبکه در برابر حملات بسیار مهم است. تحقیقات در حال انجام راه‌هایی را برای غیرمتمرکز کردن شبکه‌های بیت‌کوین و اتریوم بدون اندازه‌گیری در شبکه زیربنایی بررسی می‌کند. از این رو، بحث‌ها و تصمیم‌گیری‌ها در مورد شبکه‌های زیربنایی اغلب بر اساس فرضیات است تا اندازه‌گیری.

در این مقاله، ما یک مطالعه اندازه گیری جامع در مورد معیارهای عدم تمرکز در این سیستم های عملیاتی ارائه می کنیم و روشن می کنیم که آیا مفروضات موجود در عمل برآورده می شوند یا خیر. ما تکنیک‌های اندازه‌گیری اینترنتی قبلی را برای بیت‌کوین و اتریوم تطبیق می‌دهیم و از رویکردهای جدید برای به دست آوردن داده‌های لایه برنامه استفاده می‌کنیم. منابع اصلی داده ما عبارتند از (1) اندازه گیری مستقیم این شبکه ها از چندین نقطه نظر، (2) یک شبکه رله

بیت کوین به نام Falcon که ما آن را به مدت یک سال استقرار و اجرا کردیم، و (3) تاریخچه بلاک چین بیت کوین و اتریوم. مطالعه ما یافته‌هایی را در مورد ویژگی‌های شبکه، تأثیر الزامات پروتکل، امنیت و تعاملات مشتری ارائه می‌کند. این مقاله سه موضوع را در بر گرفته. اول، ابزارها و تکنیک های جدیدی برای اندازه گیری شبکه های ارز دیجیتال مبتنی بر بلاک چین ارائه می کند. ابزار کلیدی معرفی شده در اینجا شبکه رله فالکون است که ما ساختیم تا به عنوان ستون فقرات برای حمل بلوک ها عمل کند. این شبکه برای بیت کوین در پنج قاره مستقر شد و یک نقطه برتری منحصر به فرد را در بلوک های هرس شده ایجاد کرد. دوم، ما یک مطالعه مقایسه ای از معیارهای عدم تمرکز در بیت کوین و اتریوم انجام می دهیم. یافته‌های کلیدی ما عبارتند از: (1) شبکه بیت‌کوین می‌تواند پهنای باند مورد نیاز برای گره‌ها را تا ضریب 1.7 افزایش دهد و همان سطح عدم تمرکز را در سال 2016 حفظ کند، (2) شبکه بیت‌کوین از نظر جغرافیایی خوشه‌تر از اتریوم است و گره‌های بسیاری دارد. احتمالاً در دیتاسنترها ساکن هستند. (3) اتریوم نسبت به بیت کوین از قدرت استخراج کمتری برخوردار است و از شبکه رله سود می برد، و (4) ماینرهای کوچک نوسانات بیشتری را در پاداش های بلاک در بیت کوین نسبت به اتریوم تجربه می کنند.

2.1 پروتکل بیت کوین

بیت‌کوین پروتکلی است که تراکنش‌ها را به گروه‌هایی به نام بلوک‌ها ترتیب می‌دهد. این پروتکل فاصله تولید بلوک 10 دقیقه با حداکثر اندازه 1 مگابایت را هدف قرار می دهد. در زمان اندازه‌گیری‌های ما، 100 بلوک آخر دارای اندازه بلوک متوسط 0.99 مگابایت و میانگین فاصله زمانی 9.8 دقیقه بودند. پروتکل وایر (Wire) یک شبکه همتا به همتا را بر اساس بلوک سیلابی و اعلامیه های تراکنش پیاده سازی می کند.

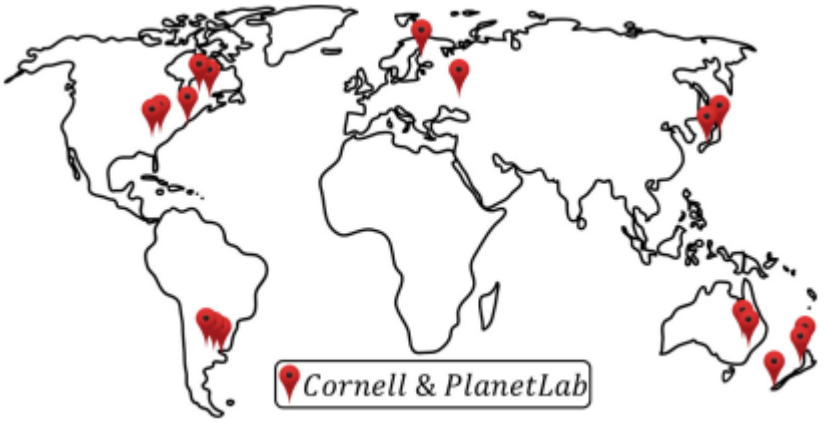
شبکه همتا به همتا از طریق پیوندهای نقطه به نقطه شکل می گیرد. برای ایجاد یک پیوند، کلاینت ها یک اتصال TCP ایجاد می کنند و یک دست دادن سه طرفه در سطح پروتکل انجام می دهند. دست دادن در سطح پروتکل وضعیت هر مشتری، مانند ارتفاع بلاک چین و یک رشته نسخه مرتبط با نرم افزار در حال اجرا را مبادله می کند. هنگامی که یک کلاینت یک بلوک جدید را کشف یا دریافت می کند، شبکه را با هش بلوک پر می کند. اگر یک کلاینت همسایه به بلوک نیاز داشته باشد، بلاک را بر اساس مقدار هش درخواست می کند. فرمت‌های بلوک مختلفی مانند بلوک‌های فشرده [17] و مرکل [44] وجود دارد، اما ما روی بازیابی بلوک‌های کامل تمرکز می‌کنیم.

2.2 پروتکل اتریوم

پروتکل اتریوم [28] بر ارائه پلتفرمی برای تسهیل ساخت برنامه های غیرمتمرکز روی بلاک چین تمرکز دارد. برای توالی تراکنش ها، اتریوم طرحی الهام گرفته از اجماع ناکاموتو و پروتکل GHOST را اتخاذ می کند [64].

اتریوم از یک قانون انتخاب زنجیره ای استفاده می کند تا از قدرت استخراج باقی مانده در بلوک های هرس شده برای بهبود امنیت استفاده کند. این پروتکل شامل بلوک هایی به نام uncles در

بلاکچین خود می شود و به ماینرهای مربوطه پاداش می دهد [70]. اتریوم فاصله بلوکی بین 10 تا 20 ثانیه را هدف قرار می دهد [41]. اندازه بلوک به طور غیرمستقیم توسط هزینه اجرا به نام گاز تعیین می شود که در طول زمان در نوسان است. درزمان اندازه‌گیری‌های ما، 100 بلوک آخر با اندازه بلوک میانه 2.9 کیلوبایت و فاصله متوسط 16.3 ثانیه تولید شد.
در اتریوم، مشتریان با هش بلاک مربوطه درخواست بلاک می‌کنند. مشتریان قدیمی بلوک هایی را درخواست می کنند که از یک بدنه و هدر تشکیل شده است، در حالی که مشتریان جدیدتر هر قطعه را جداگانه درخواست می کنند. سیستم اندازه گیری در این مقاله بر بازیابی بلوک های کامل و بدنه های بلوک تمرکز دارد.



نمودار1. زیرساخت اندازه گیری بر روی 18 گره توزیع شده در سطح جهانی ساخته شده است.

3 زیرساخت سیستم اندازه گیری

ارزهای رمزپایه مبتنی بر بلاک چین در شبکه‌های همتا به همتای جهانی که دامنه‌های مدیریتی متعددی را در بر می‌گیرند، کار می‌کنند. اندازه‌گیری چنین شبکه‌هایی به کاوش در رابطه بین همتایان، قابلیت‌های همتاهای فردی و ویژگی‌های سیستم به عنوان یک کل مربوط می‌شود. امنیت و انصاف آن برای توصیف بیت‌کوین و اتریوم، سیستم اندازه‌گیری بلاک چین (BMS) را به کار بردیم، یک سیستم اندازه‌گیری نسبت به آزمایش‌هایی با مدت زمان متفاوت – از چند روز تا 12 ماه.

جدول 1. جدول زمانی اندازه گیری. (همه تاریخ ها در سال 2017 هستند مگر اینکه غیر از این ذکر شده باشد.)

Measurement	Network		Num. Nodes	Dates
Bandwidth (All) Latency (BTC IPv4) *(Single beacon)*	BTC	IPv4	3441	Jan 11–16;Jan 30–Mar 16
		IPv6	515	Jan 13–14; Apr 20–25
		Tor	127	Jan 13; Apr 23–25
	ETH	IPv4	285	Mar 27–Apr 25
Peer-to-Peer Latency *(Mult. Vantage Pts.)*	BTC	IPv4	3390 (5.7M edges)	Jan 10–15; Jan 30–Mar 01
	ETH	IPv4	4302 (9.3M edges)	Mar 01–Apr 11
Latency *(Single Beacon)*	BTC	IPv6	845	Jan 13–14; Feb 03–Apr 25
Pruned Blocks	BTC	IPv4	5977	May 5 2016–Apr 29

ویژگی‌های شبکه. BMS از چندین نقطه برتر برای به دست آوردن دید جامعی از شبکه های ارزهای دیجیتال استفاده می کند. برای ثبت تکامل این شبکه‌ها، BMS به طور مداوم داده‌هایی را در مورد پهنای باند ارائه‌شده همتاها و تأخیر همتا به همتا جمع‌آوری می‌کند. BMS ابتدا به یک همتا متصل می شود، اندازه گیری ها را جمع آوری می کند و سپس قبل از ادامه به همتای بعدی، اتصال را قطع می کند. این اندازه‌گیری‌ها (1) گره‌های بیت‌کوین متصل به IPv4، IPv6، و Tor [23]، و (2) گره‌های اتریوم متصل به IPv4 را هدف قرار می‌دهند. از ماه می 2017، اتریوم هیچ گره توری ندارد، عمدتاً زیرا Tor منحصراً TCP است، در حالی که کشف گره اتریوم مبتنی بر UDP است. علاوه بر این، این مطالعه شبکه IPv6 اتریوم را حذف می‌کند زیرا BMS قادر به کشف گره‌های کافی برای رسیدن به نتایج کلی نبود. جدول 1 جدول زمانی جمع آوری داده ها برای هر شبکه و تعداد گره های اندازه گیری شده در هر اندازه گیری را نشان می دهد. برای تخمین تأخیر همتا به همتا، BMS از چندین نقطه برتر که به صورت جغرافیایی در سراسر جهان توزیع شده اند استفاده می کند. شکل 1 توزیع جغرافیایی زیرساخت اندازه گیری را نشان می دهد. پانزده گره از هجده گره در شبکه تحقیقاتی جهانی PlanetLab [14]] قرار دارند و سه گره باقی مانده بخشی از شبکه دانشگاهی کورنل هستند که در Ithaca، نیویورک واقع شده است. برای اندازه گیری پهنای باند ارائه شده گره ها در بیت کوین و اتریوم، BMS از گره هایی با منابع گسترده استفاده کرد. به طور خاص، اندازه‌گیری حداکثر پهنای باندی که گره‌های بیت‌کوین و اتریوم به آن دسترسی دارند، به گره‌هایی با (۱) ظرفیت دانلود بالا نیاز دارد تا اطمینان حاصل شود که گلوگاه‌ها در دستگاه اندازه‌گیری نیستند، و (۲) ظرفیت دیسک کافی برای ذخیره نتایج دقیق. از آنجایی که این ماشین‌ها به ظرفیت پهنای باند بالاتری نسبت به آنچه در زیرساخت‌های مشترک، مانند گره‌های PlanetLab قابل دستیابی

است، نیاز دارند، برخی از داده‌های BMS با استفاده از گره‌های نشانگر اختصاصی و خوب‌تجهیز شده در دانشگاه کورنل جمع‌آوری شدند.
در نهایت، BMS باید نمونه ای از گره ها را از شبکه های بیت کوین و اتریوم انتخاب کند. برای این منظور، BMS از فهرستی شامل گره‌های سایت‌های خزنده گره بیت‌کوین و اتریوم [1،31] و یک ابرگره اتریوم مستقر شده به صورت محلی که با محدودیت همتای بالایی پیکربندی شده است، استفاده می‌کند. تفاسیر در این مقاله فرض می‌کند که استنباط‌های حاصل از گره‌های عمومی قابل دسترسی نماینده کل شبکه‌های آن‌ها هستند. در واقع، این شبکه ها حاوی گره هایی هستند که برای عموم قابل مشاهده نیستند، به عنوان مثال، آنها در پشت NAT یا فایروال قرار دارند. یکی از این دسته از گره ها بخشی از استخراج است. در حالی که بسیاری از زیرساخت‌های استخراج خصوصی هستند، کار اندازه‌گیری قبلی نشان می‌دهد که عملیات استخراج اغلب دارای گره‌های دروازه برای ارتباط با شبکه همتا به همتا هستند [56].
ویژگی‌های گره‌های استخر استخراج داخلی با تمرکز این مقاله متعامد هستند.
اطلاعات بلاک چین یک رویکرد ساده لوحانه برای به دست آوردن اطلاعات در مورد بلاک چین، اجرای ساده یک گره بیت کوین و اتریوم است. با این حال، این مانع از اطلاعاتی می شود که نمی توان از طریق پروتکل های سیم مربوطه به دست آورد. بسیاری از معیارهای مهم تمرکززدایی حول تجزیه و تحلیل بلوک هایی متمرکز می شوند که بخشی از بلاک چین اصلی نیستند. در اتریوم، بسیاری از این بلاک‌ها تبدیل به عمو می‌شوند که به سادگی می‌توان آن‌ها را از طریق پروتکل وایر درخواست کرد. اما در بیت کوین، بلوکی که بخشی از بلاک چین اصلی نیست، به سادگی هرس می شود. بلوک های هرس شده در بیت کوین هیچ تاثیری بر وضعیت سیستم ندارند. آنها بدون تأثیر بر صحت توسط مشتریان حذف می شوند. بنابراین، اتصال مستقیم به ماینرها برای گرفتن بلوک های هرس شده بسیار مهم است.
یکی از اجزای حیاتی BMS برای مشاهده بلوک های هرس شده، شبکه رله فالکون است که بلاک ها را بین ماینرهای بیت کوین رله می کند. شبکه رله فالکون از مسیریابی برش برای انتشار سریع بلوک ها در سراسر جهان استفاده می کند و ماینرها را تشویق می کند تا به فالکون متصل شوند. در واقع، فالکون به طور مستقیم به حداقل 36.4 درصد از کل قدرت هش بیت کوین متصل است. از آنجایی که فقط یک شبکه رله عملیاتی دیگر برای بیت کوین وجود دارد [16،18]، فالکون بلوک هایی را مشاهده کرده است که در سایر گره های به خوبی متصل دیده نشده اند [8].

4 اندازه گیری

در این بخش، اندازه گیری های انجام شده توسط BMS را ارائه می دهیم. برای هر اندازه گیری، روش شناسی را توصیف می کنیم و به دنبال آن نتایج تجزیه و تحلیل خود را بیان می کنیم. مانند هر مطالعه اندازه گیری یک مصنوع در مقیاس بزرگ و غیرقابل ابزار، اندازه گیری ها بی نقص نیستند. ما هر بخش را با پرداختن به برخی از منابع احتمالی خطا و کاهش آنها به پایان می رسانیم.

4.1 پهنای باند ارائه شده

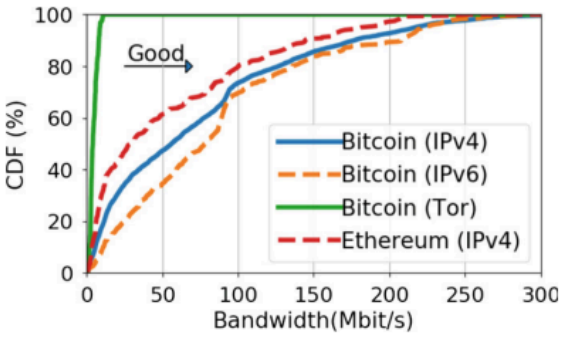
پهنای باند تدارک دیده تخمینی از ظرفیت انتقال یک گره است که مشخص می کند گره چقدر پهنای باند برای برقراری ارتباط با بقیه شبکه ارز های دیجیتال دارد. پهنای باند تدارک دیده بیشتر به ماینر ها کمک می‌کند تا بلاک‌ها را سریع‌تر به/از شبکه منتشر و جمع‌آوری کنند. بنابراین، برای یک ماینر مخرب قرار گرفتن در شبکه برای دستیابی به ویژگی عجله [35] و حمله به بلاک چین دشوارتر می شود. آگاهی از پهنای باند ارائه شده همچنین به تنظیم پارامترهای پروتکل، مانند اندازه بلوک و فرکانس کمک می کند.

روش‌شناسی. BMS پهنای باند ارائه‌شده هر همتا را با درخواست مقدار زیادی داده از هر همتا و مشاهده سرعتی که همتاها می‌توانند داده‌ها را به گره‌های اندازه‌گیری BMS ارسال کنند، اندازه‌گیری می‌کند. BMS این کار را با درخواست بلوک‌هایی انجام می‌دهد که برای اولین بار بیش از یک سال پیش دیده شده‌اند - مشابه اینکه یک گره بیات از بلوک‌ها برای همگام‌سازی حالت می‌خواهد. هر درخواست مجموعه ای از بلاک ها در بیت کوین و بلاک ها یا بدنه های مربوطه در اتریوم را درخواست می کند. سپس، BMS زمان را به دوره‌ها تقسیم می‌کند و تعداد بایت‌های دریافتی در طول هر دوره را ثبت می‌کند. این فرآیند تا زمانی ادامه می‌یابد که یا BMS همه داده‌ها را دریافت کند یا به یک بازه زمانی از پیش تعریف‌شده 30 ثانیه برسد. مهلت زمانی طولانی به BMS کمک می کند تا اثرات ناشی از شروع آهسته TCP و سایر نویز های اولیه را حذف کند، همچنین جهش های کاذب در توان عملیاتی ناشی از بافر در هسته توسط BMS را شناسایی و حذف می کند. در نهایت، BMS داده های جمع آوری شده را برای تعیین پهنای باند ارائه شده پردازش می کند. برای انجام این کار، ابتدا جریان های داده مستقل را با ترکیب دوره های متوالی حاوی انتقال داده های فعال شناسایی می کند. سپس، جریان‌های کوتاه‌تر از 500 میلی‌ثانیه را حذف می‌کند تا مصنوعات اولیه‌سازی مانند شروع آهسته TCP را کاهش دهد. سپس BMS حداکثر توان عملیاتی مشاهده شده را در بین جریانهای پیوسته مجزای باقیمانده به عنوان پهنای باند تدارک دیده شده از همتای راه دور خروجی می دهد.

نکته:آزمایش‌ها در این مقاله بر روی سرورهایی با لینک‌های 1 گیگابیت در دانشگاه کورنل اجرا می‌شوند. این موضوع از سال 2016 تا 2017 تغییر نکرده است که به ما امکان مقایسه با یک مطالعه پیشین در سال 2016 را می‌دهد [20].

	Bitcoin			Eth.
	IPv4 [Mbps]	IPv6 [Mbps]	Tor [Mbps]	IPv4 [Mbps]
10%	5.7	11.0	2.1	3.4
33%	23.3	45.2	3.1	11.2
50%	56.1	78.2	4.1	29.4
67%	91.1	94.3	5.6	68.3
90%	177.0	207.9	8.1	144.4
Avg.	73.1	86.5	4.7	55.0
Std. Dev.	68.4	66.9	2.4	58.8

(a) Provisioned bandwidth statistics.



(b) CDF

نمودار2. آمار در مورد توزیع پهنای باند ارائه شده و CDF.

نتایج. ما مشاهده می کنیم که گره های بیت کوین در هر دو شبکه IPv4 و IPv6 به طور مداوم پهنای باند بالاتری نسبت به گره های اتریوم IPv4 دارند. به طور خاص، گره های بیت کوین IPv4 و IPv6 میانه حدود 1.9× و 2.7× پهنای باند گره معمولی IPv4 اتریوم دارند. در مقابل، گره‌های بیت کوین Tor در مقایسه با گره‌های متصل مستقیم، پهنای باند کمتری دارند، اگرچه غیرقابل استفاده نیستند – برای مثال، 90 درصد آنها بیش از 2 مگابیت بر ثانیه دارند. تحقیقات در حال انجام جایگزین هایی برای شبکه Tor را بررسی می کند که ارتباطات کارآمدی را نیز فراهم می کند [50]. شکل 2b توزیع تجمعی اندازه گیری های پهنای باند را نشان می دهد.
افزایش شدید در منحنی های بیت کوین IPv4/IPv6 در حدود 10 مگابیت در ثانیه و مناطق 100 مگابیت در ثانیه نشان دهنده ظرفیت های پهنای باند معمولی یک کاربر خانگی و نمونه معمولی بیت کوین EC2 آمازون است. برای اتریوم، ما تجمع مشابهی را در اطراف منطقه 10 مگابیت بر ثانیه مشاهده می‌کنیم، اما پهنای باند به طور مساوی روی گره‌های باقی‌مانده توزیع می‌شود. همانطور که توزیع طولانی و انحراف استاندارد بالاتر نشان می دهد، پهنای باند گره های بیت کوین IPv4/IPv6 در مقایسه با گره های اتریوم در محدوده وسیع تری از مقادیر پخش شده است. در حالی که بهترین نودهای بیت کوین دارای حدود 300 مگابیت در ثانیه پهنای باند اضافی هستند، بالاترین ظرفیت گره های اتریوم که BMS مشاهده کرده است به 250 مگابیت در ثانیه محدود شده است.
یکی از جالب ترین اکتشافات این مطالعه این است که شبکه بیت کوین از نظر پهنای باند ارائه شده به طور فوق العاده ای بهبود یافته است. نتایج نشان می‌دهد که گره‌های بیت‌کوین IPv4 که قبلاً در سال 2016 با پهنای باند متوسط 33 مگابیت بر ثانیه به شبکه متصل می‌شدند، اکنون از فوریه 2017 دارای پهنای باند متوسط 56 مگابیت بر ثانیه هستند. به عبارت دیگر ، پهنای باند ارائه شده برای یک گره کامل معمولی اکنون 1.7× آنچه در سال 2016 بود است.

پارامترهای حیاتی سیستم، مانند حداکثر اندازه بلوک و فرکانس بلوک را می توان با افزایش پهنای باند ارائه شده افزایش داد. افزایش پهنای باند ارائه شده نشان می دهد که اندازه بلوک را می توان با ضریب 1.7 افزایش داد بدون اینکه تمرکز بیش از سطح واقعی آن در سال 2016 افزایش یابد.

هشدارها. مانند هر تکنیک اندازه گیری در دنیای واقعی، نتایج ما در بالا مشمول محدودیت های تجربی و خطاهای مورد انتظار هستند. دقت اندازه‌گیری‌ها ممکن است تحت شرایط خاصی کاهش یابد، از جمله مواردی که: (1) گلوگاه شبکه در کنار چراغ اندازه‌گیری قرار دارد تا همتای راه دور، (2) ترافیک شبکه در سمت BMS با جمع‌آوری‌شده تداخل می‌کند. در نتیجه، (3) همتای راه دور عمداً ترافیک را شکل می دهد تا پهنای باند موجود برای BMS را به طور انتخابی محدود کند، به عنوان مثال از طریق محدود کردن پهنای باند، و (4) پهنای باند حالت پایدار متفاوت بین بیت کوین و اتریوم، که اعداد یک سیستم را نسبت به سیستم دیگر تغییر می دهد. راه اندازی زیرساخت پهنای باند ما به حداقل رساندن عدم دقت احتمالی به دلیل دو مشکل اول کمک می کند. علاوه بر این، تجزیه و تحلیل پیاده‌سازی‌های محبوب بیت‌کوین [5] و کلاینت اتریوم [19،42،60،61] نشان می‌دهد که مورد سوم توسط این نرم‌افزار پشتیبانی نمی‌شود و برای راه‌اندازی به کار اضافی، بالقوه غیر ضروری نیاز دارد. برای تأیید تأثیر آخرین مشکل، یک کلاینت اتریوم و بیت‌کوین را اجرا کردیم و دیدیم که مصرف پهنای باند آنها 0.2 مگابیت بر ثانیه متفاوت است، که حدود 1 درصد خطا در اندازه‌گیری‌های ما در بالا نشان می‌دهد.

علاوه بر تجزیه و تحلیل ما در بالا، ما همچنین انتظار داریم که مصنوعات خاصی را در داده های خود ببینیم. همانطور که در بالا ذکر شد، ما شاهد خوشه‌هایی از گره‌ها با سرعتی در حدود 10 مگابیت بر ثانیه و 100 مگابیت در ثانیه هستیم که به ترتیب ظرفیت‌های پهنای باند معمولی کاربران خانگی و EC2 هستند.

4.2 ساختار شبکه

ساختار شبکه همتا به همتا عمیقاً بر امنیت و عملکرد ارزهای دیجیتال تأثیر می گذارد. یک شبکه خوشه‌بندی شده جغرافیایی می‌تواند به سرعت یک بلوک جدید را در بسیاری از گره‌های دیگر منتشر کند، و انتشار بلوک‌ها/تراکنش‌های متضاد را سریع‌تر از گره‌های صادق برای استخراج‌کننده‌های مخرب چالش‌برانگیزتر می‌کند. با این حال، یک شبکه کمتر خوشه‌ای ممکن است نشان دهد که گره‌های کامل توسط طیف متنوع‌تری از کاربران اداره می‌شوند، که برای تمرکززدایی نیز مفید است.

روش‌شناسی. از آنجایی که اندازه‌گیری مستقیم بین همتاهایی که کنترل نمی‌کنیم امکان‌پذیر نیست، از تکنیک‌های برآورد پیشرفته برای ایجاد مرزها و به دست آوردن بینش در ساختار شبکه استفاده می‌کنیم.

Single Beacon Latency: ابتدا اندازه گیری های پینگ ICMP مستقیم را از گره های BMS برای همه همتایان در شبکه جمع آوری می کنیم. ما حداقل تأخیر پینگ مشاهده شده را گزارش می‌کنیم، زیرا یک محدودیت فیزیکی در فاصله تا چراغ BMS ایجاد می‌کند.
تأخیر Peer-to-Peer: اندازه گیری تأخیر peer-to-peer مستلزم دسترسی به نقاط پایانی است. هم در بیت کوین و هم در اتریوم، همتایان همسایگان خود را آشکار نمی کنند. پنهان کردن ساختار شبکه حریم خصوصی و امنیت را افزایش می دهد [45،56]، اما همچنین استنباط ویژگی های شبکه را دشوارتر می کند. BMS تخمین های تأخیر را برای ابرمجموعه ای از پیوندهای واقعی بین همتایان شناخته شده ارائه می دهد. ما برای اندازه های کمی متفاوت شبکه، 3390 برای بیت کوین و 4302 برای اتریوم، نرمال نمی کنیم، زیرا نمونه های ما از هر دو شبکه بسیار شبیه بودند. از آنجایی که اندازه‌گیری تأخیرهای همتا به همتا به طور مستقیم امکان‌پذیر نیست، ما با استفاده از تکنیک‌های ادبیات قبلی، محدودیت‌هایی را از تأخیرهای مشاهده‌شده از چراغ‌های چندگانه تعیین می‌کنیم [37]. BMS با اندازه گیری های گرفته شده از یک چراغ شروع می شود. سپس، از نابرابری مثلث برای تخمین مرزهای بالا و پایین برای تأخیر بین همتایان استفاده می کند. تکرار این فرآیند از سایر نقاط برتر، مجموعه ای از مرزها را برای هر جفت همتا به دست می دهد. در نهایت، BMS با انتخاب حداکثر کران پایین و حداقل کران بالا، محدوده ای را برای تخمین تاخیر بین هر همتا تعیین می کند. این مقاله همچنین میانگین تأخیر کران پایین و کران بالایی را بین همتایان ارائه می‌کند. در این مطالعه، BMS شامل گره هایی است که از فورک DAO [10] در اندازه گیری های خود برای اتریوم پشتیبانی نمی کنند.
فاصله جغرافیایی: BMS حداقل اندازه گیری تأخیر مکرر را برای حذف اثرات شبکه گذرا و گرفتن فاصله جغرافیایی بین دو گره می گیرد [13،43،69]. BMS همچنین از داده های موقعیت جغرافیایی IP برای محاسبه فاصله بین گره های همتا به عنوان اعتبار سنجی اضافی در نتایج ما استفاده می کند. برای محاسبه فواصل، BMS فرمول هاورسین [63] را با استفاده از مقادیر مختصات جمع‌آوری‌شده از یک سرویس مکان‌یابی مبتنی بر IP اعمال می‌کند [46].

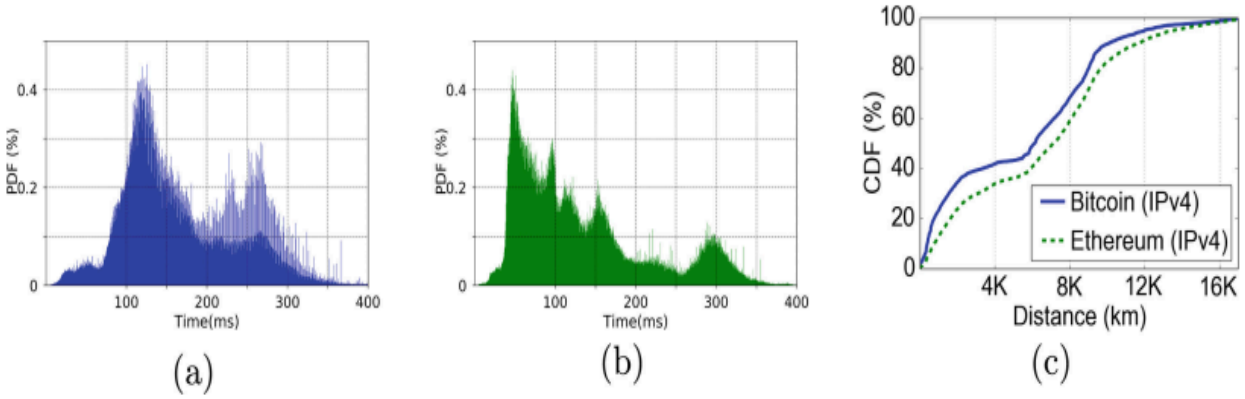
جدول2. حداقل تأخیرهای تک چراغ مشاهده شده و تخمین تأخیر P2P.

	Single beacon		Peer-to-Peer	
	Bitcoin		Bitcoin	Eth.
	IPv4 [ms]	IPv6 [ms]	IPv4 [ms]	IPv4 [ms]
10%	29	40	48	92
33%	78	80	79	125
50%	89	95	109	152
67%	98	95	152	200
90%	201	165	286	276
Avg.	97	103	135	171
Std. Dev.	59	62	88	76

نتایج. اندازه‌گیری‌های ما نشان‌دهنده تفاوت‌های قابل‌توجهی بین تاخیرهای P2P شبکه‌های IPv4 بیت‌کوین و اتریوم است که در جدول 2 و PDF نشان داده شده است.

مشاهده می کنیم که بیت کوین دارای تعداد بیشتری گره است که از نظر جغرافیایی در مقایسه با اتریوم نزدیکتر هستند. شکل 3 نشان می‌دهد که محتمل‌ترین تأخیرهای اتریوم در حدود 120 میلی‌ثانیه متمرکز شده‌اند، در حالی که گره‌های بیت‌کوین تمایل دارند حدود 50 میلی‌ثانیه جمع شوند. تنها 13 درصد از تأخیرهای اتریوم زیر 100 میلی‌ثانیه است، در حالی که بیت‌کوین به طرز شگفت‌آوری 46 درصد را نشان می‌دهد. علاوه بر این، تخمین تاخیر همتا به همتا بین گره‌های اتریوم به طور متوسط ۲۶.۷ درصد بیشتر از بیت‌کوین است. این نزدیکی جغرافیایی بین گره‌ها، همراه با مشاهده اینکه بیت‌کوین دارای گره‌های زیادی با پهنای باند 100 مگابیت بر ثانیه است (به بخش 4.1 مراجعه کنید)، نشان می‌دهد که تعداد زیادی گره بیت‌کوین در مراکز داده کار می‌کنند. به طور خاص، 56 درصد از گره های بیت کوین و 28 درصد از گره های اتریوم متعلق به یک سیستم خودمختار است که خدمات میزبانی اختصاصی را ارائه می دهد که از نظر آماری تفاوت معنی داری در سطح معناداری 1 درصد دارد.

در واقع، گره های اتریوم در یک منطقه جغرافیایی متمرکز نیستند، بلکه به طور مساوی در سراسر جهان توزیع شده اند. شکل 3c تابع توزیع تجمعی (CDF) فواصل بین گره های همتا به همتا را بر اساس اطلاعات موقعیت جغرافیایی IP نشان می دهد. نتایج از یافته‌های ما به‌دست‌آمده از اندازه‌گیری‌های تاخیر شبکه پشتیبانی می‌کنند، که نشان می‌دهد گره‌های اتریوم از نظر جغرافیایی پراکنده‌تر از گره‌های بیت‌کوین هستند. به عنوان شواهد اضافی، استفاده از موقعیت جغرافیایی در فواصل P2P و رسم CDF در شکل 3c نشان می‌دهد که گره‌های اتریوم به طور گسترده‌تری از بیت‌کوین جدا شده‌اند.



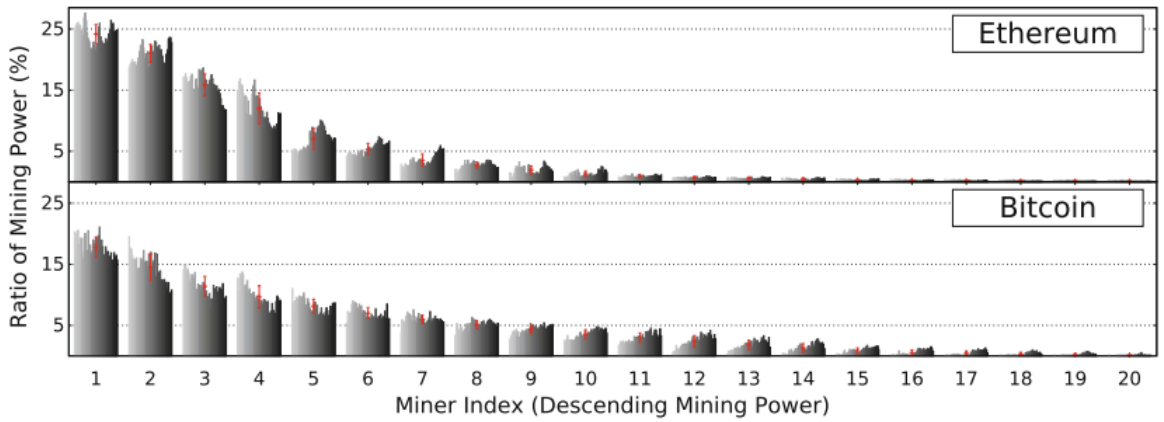
نمودار3. هیستوگرام تاخیرهای P2P در اتریوم (a) و بیت کوین (b)، و همچنین CDF فواصل جغرافیایی (c).

بررسی سلامت. دو ستون اول جدول 2 تاخیر تک چراغی را در شبکه های بیت کوین IPv4/IPv6 نشان می دهد. نتایج نشان می دهد که هم میانگین و هم متوسط تاخیر گره های IPv4

کوچکتر از گره های IPv6 هستند. زیرا گره های IPv6 کمتر از گره های IPv4، ما انتظار این نتیجه را داریم زیرا گره های IPv4 به احتمال زیاد به چراغ های ما نزدیک تر هستند.
در حالی که تعداد زیادی کار وجود دارد که شیوع نقض نابرابری مثلث در اینترنت را نشان می دهد [12،52،67]، دلایل متعددی وجود دارد که اندازه گیری های BMS به طور قابل توجهی تحت تأثیر قرار نمی گیرند. اول، نشان داده شد که چنین تخلفاتی کمتر از 5 درصد از عکس های فوری شبکه رخ می دهد [52]. از آنجایی که ما حداقل تأخیر مشاهده شده را از یک فانوس دریایی می گیریم، نقض نابرابری مثلث فقط در کمتر از 1٪ مواقع در مجموعه داده ما رخ می دهد [52]. TIVها همچنین هنگام برخورد با تاخیرهای کمتر از 300 میلی ثانیه که تقریباً کل مجموعه داده ما را شامل می شود، به طور قابل توجهی کمتر رایج هستند [67]. برای اطمینان از اینکه نتایج فوق برای مجموعه داده ما نیز صادق است، از یک سرویس موقعیت جغرافیایی به عنوان حقیقت زمین برای تأیید نتایج خود استفاده کردیم.
یکی دیگر از محدودیت‌های مطالعه ما این است که جمع‌آوری اندازه‌گیری‌ها با استفاده از پینگ‌های ICMP از گره‌هایی که ترافیک ICMP را مسدود می‌کنند و از گره‌های Tor که فقط از طریق TCP ارتباط برقرار می‌کنند، غیرممکن است.

4.3 توزیع قدرت استخراج

استخراج در شبکه‌های ارزهای دیجیتال یک فرآیند پیچیده است که عموماً به قدرت محاسباتی قابل توجهی نیاز دارد. با توجه به سطوح دشواری استخراج فعلی بیت‌کوین و اتریوم، استفاده از سخت‌افزار کالا برای تولید بلوک عملی نیست [21] و به درجاتی از تمرکز در فرآیند استخراج کمک می‌کند. با این وجود، تا زمانی که چندین نهاد مختلف در استخراج درگیر هستند، سیستم درجه‌ای از تمرکززدایی را حفظ می‌کند. در این زمینه، ما تمرکززدایی فرآیند استخراج بین بیت‌کوین و اتریوم را ارزیابی و مقایسه می‌کنیم.



نمودار4. توزیع قدرت استخراج در شبکه های بیت کوین و اتریوم. میله ها، انحراف استاندارد مشاهده شده از میانگین را نشان می دهند.

روش‌شناسی. برای ارزیابی قدرت استخراج‌کنندگان در بیت‌کوین و اتریوم، توزیع هفتگی آن‌ها را در 10 ماه گذشته، از 15 جولای 2016، تجزیه و تحلیل کردیم. تخمین‌های قدرت ماینینگ ما بر نسبت بلوک‌های زنجیره اصلی تولید شده توسط موجودیت‌های مجزا تکیه می‌کنند. در نتیجه،

بلوک های هرس شده در بیت کوین و عموها در اتریوم بر این تخمین ها تأثیری ندارند. در هر دو شبکه، ماینرها داوطلبانه هویت خود را به عنوان بخشی از هر بلوکی که استخراج می کنند، افشا می کنند. ما این داده ها را از یک API عمومی برای بیت کوین [9] و یک کاوشگر بلاک چین برای اتریوم [32] به دست آوردیم. در بیت‌کوین، 1.8 درصد از بلاک‌ها ناشناس بودند، که گویی توسط استخراج‌کنندگان مجزا تولید شده‌اند. در نهایت، هویت‌ها را برای شناسایی و ادغام موارد تکراری به صورت دستی پردازش کردیم. این شامل استخرهایی می‌شود که توسط یک مدیر اداره می‌شوند [47] و هویت‌های متعددی که یک استخر را نشان می‌دهند، که با جستجوی نام استخر مشابه با برچسب مربوطه، به‌عنوان مثال، «DwarfPool1» و «DwarfPool2» شناسایی می‌شوند. در حالی که توجه به این نکته مهم است که ماینرها می توانند استخراج کننده انفرادی یا ماینینگ استخر باشند، این تمایز برای اهداف این تحلیل بی اهمیت است. این استدلال که استخرهای استخراج درجه ای از تمرکززدایی را ارائه می دهند به دلیل اینکه شرکت کنندگان در استخر ماینینگ رفتار اپراتور استخر را بررسی می کنند، هیچ پشتیبانی تجربی ندارد. به عنوان مثال، شناسایی حملات سانسور توسط اپراتورهای استخر توسط شرکت کنندگان استخر اگر غیرممکن نباشد، دشوار است. علاوه بر این، زمانی که ماینرها در سه نوبت مختلف در تاریخ بیت کوین از آستانه 51 درصد فراتر رفتند، شرکت کنندگان استخر علیرغم شواهد واضحی از رفتاری که به طور گسترده غیرقابل قبول بود، استخر را منحل نکردند. مهم‌تر از همه، اینکه آیا استخرهای استخراج درجه‌ای از تمرکززدایی را ارائه می‌دهند یا خیر، برای اهداف این مقاله، که یک گزارش تاریخی دقیق ارائه می‌کند، بی‌اهمیت است. ما آنچه را که در زمان استخراج بلوک‌ها اتفاق افتاد، همانطور که در بلاک چین ثبت شده است، گزارش می‌کنیم. به این ترتیب، مهم نیست که ماینرها بخشی از یک استخر بوده اند یا اینکه آنها معدنچیان انفرادی بوده اند. در زمانی که یک بلوک به زنجیره متعهد شد، شرکت‌کنندگان استخر به‌عنوان بخشی از همان نهاد معدنی به‌طور ناخواسته همکاری می‌کردند.

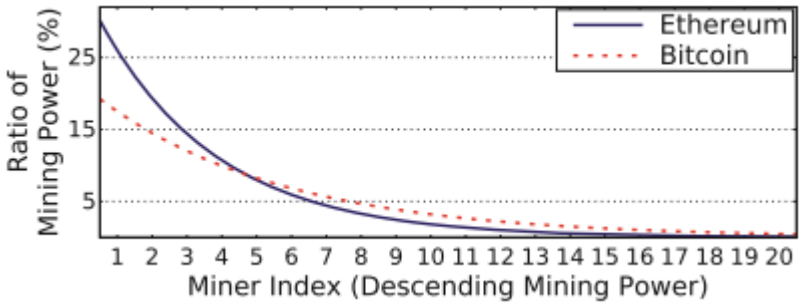
نتایج. برای هر هفته از دوره تجزیه و تحلیل، ما قدرت استخراج متناظر موجودیت ها را محاسبه کردیم و بر اساس آن هر ماینر را رتبه بندی کردیم. شکل 4 20 توزیع قدرت هفتگی برتر در شبکه های اتریوم و بیت کوین را نشان می دهد. هر گروه از میله‌ها مجموعه‌ای از نسبت‌های قدرت ماینینگ هفتگی را به ترتیب زمانی نشان می‌دهد که به عنوان کسری از بلوک‌های ارائه‌شده توسط یک ماینر تعریف می‌شود. شکل 4 نشان می دهد که در بیت کوین، قدرت ماینینگ هفتگی یک نهاد واحد هرگز از 21 درصد قدرت کلی تجاوز نکرده است. در مقابل، ماینر برتر اتریوم هرگز کمتر از ۲۱ درصد از قدرت استخراج را نداشته است. علاوه بر این، چهار ماینر برتر بیت کوین بیش از 53 درصد از میانگین قدرت استخراج را دارند. به طور متوسط، 61 درصد از قدرت هفتگی تنها توسط سه ماینر اتریوم تقسیم می شد. این مشاهدات حاکی از فرآیند استخراج کمی متمرکزتر در اتریوم است.

اگرچه ماینرها در طول دوره مشاهده رتبه‌های خود را تغییر می‌دهند، هر نقطه فقط توسط چند ماینر رقابت می‌شود. به طور خاص، تنها دو استخراج کننده بیت کوین و سه ماینر اتریوم تا کنون رتبه برتر را داشته اند. همین استخر ماینینگ 29 درصد مواقع در بیت کوین و 14 درصد مواقع در اتریوم در رتبه اول بوده است. بیش از 50 درصد از قدرت استخراج منحصراً توسط هشت ماینر در بیت کوین و پنج ماینر در اتریوم در طول دوره مشاهده شده به اشتراک گذاشته

شده است. به نظر می رسد حتی 90 درصد از قدرت ماینینگ تنها توسط 16 ماینر در بیت کوین و تنها 11 ماینر در اتریوم کنترل می شود. از این رو، هر دو پلتفرم برای حفظ بلاک چین به شدت به تعداد کمی از نهادهای استخراج متمایز متکی هستند. در واقع، در شکل 5 می بینیم که روندهای قدرت ماینینگ می توانند به صورت توزیع های نمایی با منحنی های $0.21e^{(-0.19x)}$ و $0.35e^{(-0.30x)}$ در بیت کوین و اتریوم مناسب باشند. این منحنی ها ضریب مقدار تعیین 0.99 را به دست می دهند.

این نتایج نشان می‌دهد که یک سیستم حد نصاب بیزانسی [53] با اندازه 20 می‌تواند به تمرکززدایی بهتری نسبت به استخراج اثبات کار با هزینه منابع بسیار کمتر دست یابد. این نشان می دهد که تحقیقات بیشتر برای ایجاد یک پروتکل اجماع بدون مجوز بدون چنین درجه بالایی از تمرکز ضروری است.

نمودار 5. خطوط روند نمایی برای توزیع متوسط توان استخراج.



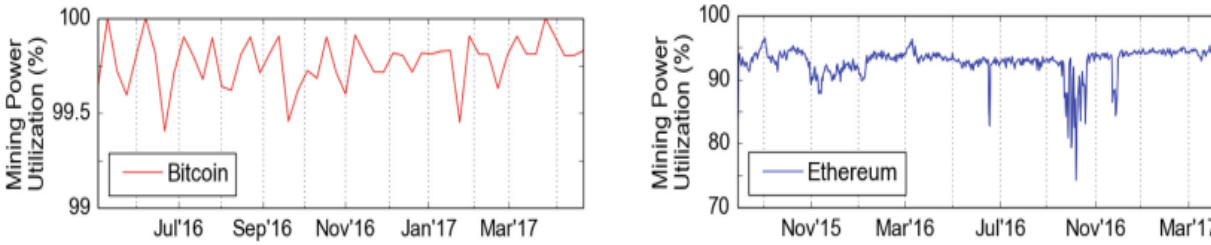
بررسی سلامت: مشابه سایر آثار موجود در ادبیات [58،68]، ما این فرض را داریم که معدنچیان به طور دقیق خود را شناسایی می کنند. ماینری که بخش قابل توجهی از قدرت هش را به ارز دیجیتال کمک می‌کند، می‌تواند مقداری تأثیر بر تغییرات پروتکل داشته باشد. بنابراین، این احتمال وجود دارد که ماینرها بخواهند بلاک هایی را که تولید کرده اند، ادعا کنند. در حالی که ماینرهای قوی نفوذ سیاسی پیدا می‌کنند و اعضای بیشتری را جذب می‌کنند، بزرگ شدن بیش از حد باعث ایجاد هشدار در جامعه در مورد تمرکز می‌شود. در نتیجه، چنین ماینرهایی ممکن است تصمیم بگیرند که این اطلاعات را پنهان یا مبهم کنند تا کمتر قدرتمند به نظر برسند - به عنوان مثال، با تولید چندین هویت. به عنوان مثال، دو استخر بزرگ ماینینگ، Ethpool و Ethermine، به طور عمومی نشان می‌دهند که مدیر یکسانی دارند [47]. بنابراین، هر تجزیه و تحلیل مبتنی بر داده های داوطلبانه ماینرها به سمت یک شبکه غیرمتمرکزتر از واقعیت منحرف می شود.

4.4 استفاده از توان استخراج

استفاده از توان استخراج [34]، که کسری از بلوک های استخراج شده را که در زنجیره اصلی باقی می مانند، اندازه گیری می کند، به عنوان معیاری برای ارزیابی کارایی یک پروتکل، و همچنین یک متریک درجه دوم برای استحکام در برابر عقبگردها عمل می کند. با افزایش

استفاده از توان ماینینگ، پروتکل می تواند انرژی بیشتری را به کار مفید تبدیل کند و در نتیجه هزینه حمله را افزایش دهد.

روش‌شناسی. برای بررسی استفاده از توان استخراج، توزیع هفتگی و روزانه بلوک‌های هرس شده در بیت‌کوین و عمو ها در اتریوم را در مقایسه با بلاک‌های زنجیره اصلی تحلیل کردیم. ما این داده ها را از (1) شبکه فالکون، (2) یک مشتری محلی بیت کوین، و (3) کاوشگرهای بلاک چین عمومی برای بیت کوین [9] و اتریوم [32] بازیابی کردیم. به طور خاص، کاوشگر بلاک چین بیت کوین و فالکون به ترتیب 12 درصد و 20 درصد از کل 124 بلوک هرس شده را به طور انحصاری ارائه کردند. هر دو منبع مجموعاً عامل کشف 68 درصد باقی مانده بودند.



(a) Bitcoin- weekly MPU from 99% (b) Ethereum- daily MPU from 70%

نمودار 6. استفاده از قدرت استخراج برای هردو رمزارز بیتکوین و اتریوم

نتایج. شکل 6a و b به ترتیب توزیع هفتگی و روزانه استفاده از توان استخراج در شبکه های بیت کوین و اتریوم را نشان می دهد. یافته ها نشان می دهد که استفاده از بیت کوین به طور مداوم از 99 درصد فراتر می رود که نشان می دهد یک بلوک بریده شده در بیت کوین یک رویداد نسبتاً نادر است. در مقابل، استفاده روزانه در اتریوم معمولاً در محدوده 90٪ تا 94٪ قرار می گیرد و هرگز از آستانه 97٪ فراتر نمی رود. در طول سال 2016، اتریوم گاه به گاه افت استفاده را تجربه می کند، از 74% تا 88%، به ویژه در طی (1) روزهای پس از بهره برداری از آسیب پذیری DAO [10] از 17 تا 18 ژوئن، (2) حملات به شبکه اتریوم [11,66] بین 22 سپتامبر تا 19 اکتبر و (3) روزهای پس از هارد فورک Spurious Dragon [48] بین 23 تا 29 نوامبر. این نتایج نشان دهنده یک رابطه قوی بین استفاده از توان استخراج و رویدادهای واقعی در اتریوم است. این ممکن است به اقدامات پیشگیرانه ای نسبت داده شود که شبکه را برای کاهش سرعت مهاجم DAO ارسال می کند، بازیگران بدی که بلوک هایی با تقاضای منابع بیش از حد تولید می کنند، و ماینرهایی با کلاینت های قدیمی. این نتایج نشان می دهد که یک شبکه رله مانند فالکون برای شبکه اتریوم بسیار مفید است.

بررسی سلامت. طراحی پروتکل اتریوم، همتایان را موظف می‌کند تا بلوک‌های عمویی را که در زنجیره اصلی نیستند، ذخیره و منتشر کنند. در مقابل، بلاک چین بیت کوین تنها زنجیره اصلی را ذخیره می کند، بنابراین همتایان بلوک های هرس شده را منتشر نمی کنند. بنابراین، گرفتن چنین بلوک هایی در بیت کوین مستلزم نظارت فعالانه بر شبکه است. در حالی که شبکه رله فالکون انگیزه قوی برای ماینرها فراهم می کند تا بلوک ها را از طریق آن رله کنند، برخی

از ماینرها ممکن است این کار را انجام ندهند. در نتیجه، ممکن است برخی از بلوک‌های هرس‌شده‌ای را که توسط شبکه بیت‌کوین ایجاد شده‌اند از دست بدهیم.

4.5 انصاف

بخش 4.3 توزیع قدرت ماینینگ را با تمرکز بر حضور ماینرها در زنجیره اصلی مورد بحث قرار داد. تأثیر این توزیع بر نرخ بلوک هرس شده استخراج‌کننده نامشخص است. برای کشف این رابطه، انصاف را بررسی می کنیم، که به عنوان نسبت سهم ماینر از بلوک های هرس شده به قدرت استخراج او تعریف می شود. در یک پروتکل منصفانه، ماینرها باید بلوک‌های هرس شده را متناسب با قدرت ماینینگ خود تولید کنند که در نتیجه انصاف نزدیک به 1 است. انصاف بیشتر از 1 نشان می‌دهد که یک ماینر ضعیف است، در حالی که انصاف کمتر از 1 حاکی از یک مزیت است.

روش شناسی. ما از شبکه فالکون و یک کاوشگر بلاک چین بیت کوین [8] برای بازیابی بلوک های هرس شده بیت کوین استفاده کردیم، به ترتیب 109 و 99 بلوک از هر منبع به دست آوردیم که منجر به 124 بلوک هرس شده مجزا شد. عموها از یک کاوشگر بلاک چین اتریوم جمع آوری شدند [32]. مشابه بخش 4.3، نتایج ما فرض می‌کند که ماینرها داوطلبانه خود را در بلوک‌های عمو/هرس شده شناسایی می‌کنند. یک اخطار در جمع آوری بلوک های هرس شده وجود دارد، زیرا تشویق ماینرها برای رله کردن بلوک ها از طریق فالکون، مطابقت آنها را تضمین نمی کند. ذخیره سازی صریح عموها در اتریوم احتمالاً نسبت بیشتری از بلوک های هرس شده را جذب می کند.
نتایج. شکل 7 توزیع عادلانه 20 ماینر برتر با بالاترین قدرت استخراج را نشان می دهد. نتایج نشان می‌دهد که در هر دو شبکه، چهار ماینر برتر عموماً موفقیت بیشتری در الحاق بلوک‌ها به زنجیره اصلی نشان می‌دهند. برای مقایسه توزیع‌های عادلانه بیت‌کوین و اتریوم، آزمون خوبی برازش Kolmogorov-Smirnov با مقدار p 0.01 انجام شد. به طور شگفت انگیزی، اتریوم و بیت کوین تفاوت های قابل توجهی را در انصاف نشان می دهند و یک دوره زمانی ثابت را حفظ می کنند. واریانس در انصاف ماینر بیت کوین بسیار بزرگتر از اتریوم است (1.72 در مقابل 0.25). با این حال، میانگین هر دو توزیع عادلانه بسیار مشابه است، اتریوم در 1.08 و بیت کوین در 1.22 است.
واریانس بالا فشار تمرکز را ایجاد می کند، زیرا ماینرهای کوچکتر ممکن است با از دست دادن درآمد به دلیل نمرات عادلانه گذرا بالا دست و پنجه نرم کنند. اختلاف واریانس نتیجه مستقیم تعداد بسیار کمتر بلوک های تولید شده در بیت کوین است. فرکانس بلاک بالاتر اتریوم به ماینرهای کوچکتر سود قابل پیش بینی تری نسبت به ماینرهای بزرگتر می دهد. پروتکل های بلاک چین باید هم واریانس و هم میانگین پاداش های بلاک را در نظر بگیرند. صرفاً افزایش فرکانس بلوک ممکن است مشکل واریانس را برطرف نکند، زیرا می تواند بر توزیع توان استخراج تأثیر بگذارد. افزایش فرکانس بلوک اتریوم ممکن است به توزیع متمرکزتر قدرت ماینینگ آن کمک کند (به بخش 4.3 مراجعه کنید).
بررسی سلامت. مشابه بخش 4.4، نتایج ما فرض می‌کند که ماینرها داوطلبانه خود را در بلوک‌های عمو/هرس شده شناسایی می‌کنند. اگر ماینرها اطلاعات نادرست ارائه دهند، سیستم

ممکن است منصفانه تر از آنچه که هست به نظر برسد. به‌علاوه، اخطار جمع‌آوری بلوک‌های هرس‌شده همچنان ادامه دارد، زیرا تشویق استخراج‌کنندگان برای انتقال بلوک‌ها از طریق فالکون، تضمینی برای انطباق نیست. ما گمان می کنیم که ذخیره سازی صریح عموها در اتریوم امکان تجزیه و تحلیل دقیق تری را فراهم می کند.
در نهایت، فرکانس پایین‌تر تولید بلاک بیت‌کوین و نرخ بلاک کاهش‌یافته در مقایسه با اتریوم، نویز را به معیار انصاف وارد می‌کند و تفسیر آن را در بیت‌کوین در مقایسه با اتریوم چالش‌برانگیزتر می‌کند.

5 نتیجه گیری

خلاصه ای از مطالبی که در این مبحث به انها پرداخته و سعی در تحلیل آن داشتیم.

مقایسه تمرکززدایی: نتیجه‌گیری جنبه غیرمتمرکز دو ارز دیجیتال محبوب، بیت‌کوین و اتریوم را مورد بحث قرار می‌دهد. این اهمیت تمرکززدایی در ارزش پیشنهادی پلتفرم های مبتنی بر بلاک چین را برجسته می کند.
تکنیک‌های اندازه‌گیری: این کار بر تکنیک‌های اندازه‌گیری جدید، از جمله شبکه فالکون و روش‌های اندازه‌گیری اینترنتی تثبیت‌شده، برای به دست آوردن اطلاعات در مورد لایه کاربردی متکی است.
ظرفیت شبکه: مشاهدات نشان می دهد که بیت کوین در مقایسه با اتریوم دارای ظرفیت شبکه بالاتری است. با این حال، اشاره می‌کند که گره‌های بیت‌کوین خوشه‌تر هستند، که نشان‌دهنده تمرکز بالاتر در مراکز داده است.
فرآیندهای استخراج: هر دو بیت کوین و اتریوم فرآیندهای استخراج نسبتاً متمرکز را نشان می دهند. نتیجه گیری نشان می دهد که تحقیقات بیشتری برای تمرکززدایی بیشتر پروتکل های اجماع بدون مجوز لازم است.
جوایز بلاک و واریانس: اتریوم در مقایسه با بیت کوین واریانس کمتری در جوایز بلاک دارد. نوسانات پاداش استخراج به عنوان یک معیار مهم اما اغلب نادیده گرفته می شود.
رشد بیت کوین: بیت کوین رشد قابل توجهی را تجربه کرده است که امکان افزایش بالقوه اندازه بلوک را بدون به خطر انداختن تمرکززدایی در مقایسه با ایالت در سال 2016 فراهم می کند.
استفاده از توان استخراج: اتریوم در مقایسه با بیت کوین از قدرت استخراج پایین تری برخوردار است که به فرکانس بلاک بالاتر آن نسبت داده می شود.
توصیه‌ها: نتیجه‌گیری نشان می‌دهد که اتریوم می‌تواند از یک شبکه رله برای افزایش استفاده از توان ماینینگ بهره‌مند شود.

در ادامه و قبل از منابع و مراجع نویسندگان از افراد خاص تشکر می کنند و از منابع مالی که از تحقیق حمایت کرده اند، قدردانی می کنند.

قدردانی: نویسندگان از ویتالیک بوترین و داوران ناشناس به خاطر بازخوردشان در مورد پیش نویس های قبلی تشکر می کنند. Ittay Eyal پشتیبانی از کمک هزینه تحصیلی Viterbi در مرکز مهندسی کامپیوتر در Technion را تایید می کند. منابع مالی و پشتیبانی برای این کار توسط منابع مختلفی از جمله AFOSR، NSF، ONR، NIST، Facebook، Infosys و IC3 ارائه شد. برنامه کمک هزینه پژوهشی فارغ التحصیلان بنیاد ملی علوم نیز از این کار تحت گرنت شماره DGE-1650441 حمایت کرد. نظرات، یافته‌ها و نتیجه‌گیری‌هایی که در اینجا بیان شده است، متعلق به نویسندگان است و لزوماً منعکس‌کننده دیدگاه‌های بنیاد ملی علوم نیست.

مراجع

0. (Lecture Notes in Computer Science 10957) - Financial Cryptography and Data Security_22nd International Conference, FC 2018, Nieuwpoort, Curaçao, February 26 – March 2

1. 21.CO. Bitnodes. https://bitnodes.21.co/. Accessed June 2017
2. Apostolaki, M., Zohar, A., Vanbever, L.: Hijacking bitcoin: routing attacks on cryptocurrencies. arXiv preprint arXiv:1605.07524 (2016)
3. Benben Team. Benben. http://benben.com.gh/. Accessed Oct 2016
4. Biryukov, A., Khovratovich, D., Pustogarov, I.: Deanonymisation of clients in Bitcoin P2P network. In: Proceedings of the ACM Conference on Computer and Communications Security (CCS), pp. 15–29 (2014)
5. Bitcoin Community. Bitcoin source. https://github.com/bitcoin/bitcoin. Accessed June 2017
6. Bitcoin Community. Protocol rules. https://en.bitcoin.it/wiki/Protocol rules. Accessed June 2017
7. Bitcoin Community. Protocol specification. https://en.bitcoin.it/wiki/Protocol specification. Accessed June 2017
8. Blockchain Info Team. Blockchain Info. https://blockchain.info/. Accessed May 2017
9. BlockTrail Team. Blocktrail API. https://www.blocktrail.com/api/docs#api data. Accessed Apr 2017
10. Buterin, V.: Critical update re: DAO vulnerability. https://blog.ethereum.org/ 2016/06/17/critical-update-re-dao-vulnerability/. Accessed Apr 2017
11. Buterin, V.: Transaction spam attack: next steps. https://blog.ethereum.org/2016/ 09/22/transaction-spam-attack-next-steps/. Accessed Apr 2017
12. Cangialosi, F., Levin, D., Spring, N.: Ting: measuring and exploiting latencies between all tor nodes. In Proceedings of the ACM SIGCOMM Conference on Internet Measurement (IMC), pp. 289–302 (2015)
13. Chandrasekaran, B., et al.: Alidade: IP geolocation without active probing. Technical report, Duke University (2015)
14. Chun, B., et al.: PlanetLab: an overlay testbed for broad-coverage services. ACM SIGCOMM CCR 33(3), 3–12 (2003)
15. CoinMarketCap. Cryptocurrency market capitalizations. https://coinmarketcap. com/. Accessed May 2017
16. Corallo, M.: The Bitcoin relay network. BIP 152. http://bitcoinrelaynetwork.org/. Accessed May 2017
17. Corallo, M.: Compact block relay. BIP 152. https://github.com/bitcoin/bips/blob/ master/bip-0152.mediawiki.

Accessed June 2017 Decentralization in Bitcoin and Ethereum Networks 455
18. Corallo, M.: FIBRE: Fast internet Bitcoin relay engine. https://github.com/ bitcoinfibre/bitcoinfibre. Accessed Apr 2017
19. Cpp-ethereum Authors: Ethereum C++ client. https://github.com/ethereum/ cpp-ethereum. Accessed Apr 2017
20. Croman, K., et al.: On scaling decentralized blockchains (a position paper). In: Proceedings of the Workshop on Bitcoin and Blockchain Research (BITCOIN), Barbados (2016)
21. Cryptocompare Team. Cryptocurrency mining calculator. https://www. cryptocompare.com/mining/calculator. Accessed June 2017
22. Decker, C., Wattenhofer, R.: Information propagation in the Bitcoin network. In: Proceedings of the IEEE International Conference on Peer-to-Peer Computing, pp. 1–10, Trento, Italy (2013)
23. Dingledine, R., Mathewson, N., Syverson, P.:Tor: the second-generation onion router. In: Proceedings of the USENIX Security Symposium (2004)
24. Donet Donet, J.A., P´erez-Sol`a, C., Herrera-Joancomart´ı, J.: The Bitcoin P2P network. In: B¨ohme, R., Brenner, M., Moore, T., Smith, M. (eds.) FC 2014. LNCS, vol. 8438, pp. 87–102. Springer, Heidelberg (2014). https://doi.org/10.1007/978- 3-662-44774-1 7
25. Ethereum Community. devp2p forward compatibility requirements for homestead. https://github.com/ethereum/EIPs/blob/master/EIPS/eip-8.md. Accessed Apr 2017
26. Ethereum Community. DΞVp2p wire protocol. https://github.com/ethereum/ wiki/wiki/%C3%90%CE%9EVp2p-Wire-Protocol. Accessed Apr 2017
27. Ethereum Community. Ethereum wire protocol. https://github.com/ethereum/ wiki/wiki/Ethereum-Wire-Protocol. Accessed Apr 2017
28. Ethereum Community. A next generation smart contract and decentralized application platform. https://github.com/ethereum/wiki/wiki/White-Paper. Accessed Apr 2017

29. Ethereum Community. RLPx: Cryptographic network & transport protocol. https://github.com/ethereum/devp2p/blob/master/rlpx.md. Accessed Apr 2017
30. Ethereum Community. RLPx encryption. https://github.com/ethereum/goethereum/wiki/RLPx-Encryption. Accessed Apr 2017
31. EthereumJ. The Ethereum nodes explorer. https://www.ethernodes.org/. Accessed June 2017
32. Etherscan Team. Etherscan: The Ethereum block explorer. https://etherscan.io/. Accessed June 2017
33. Ethstats Team. Ethstats. https://ethstats.net/. Accessed June 2017
34. Eyal, I., Gencer, A.E., Sirer, E.G., van Renesse, R.: Bitcoin-NG: a scalable blockchain protocol. In: Proceedings of the USENIX Symposium on Networked Systems Design and Implementation (NSDI), pp. 45–59, Santa Clara, CA, USA (2016)
35. Eyal, I., Sirer, E.G.: Majority is not enough: Bitcoin mining is vulnerable. In Proceedings of the International Financial Cryptography and Data Security Conference, Barbados (2014)
36. Feld, S., Sch¨onfeld, M., Werner, M.: Analyzing the deployment of Bitcoin's P2P network under an AS-level perspective. In: Proceedings of the International Workshop on Secure Peer-to-Peer Intelligent Networks and Systems, vol. 32, pp. 1121– 1126 (2014)
37. Francis, P., et al.: IDmaps: a global internet host distance estimation service. IEEE/ACM Trans. Netw. (TON) 9, 525–540 (2001) 456 A. E. Gencer et al.
38. Garay, J., Kiayias, A., Leonardos, N.: The Bitcoin backbone protocol: analysis and applications. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9057, pp. 281–310. Springer, Heidelberg (2015). https://doi.org/10.1007/978- 3-662-46803-6 10
39. Gencer, A.E., van Renesse, R., Sirer, E.G.: Short paper: service-oriented sharding for blockchains. In: Kiayias, A. (ed.) FC 2017. LNCS, vol. 10322, pp. 393–401. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70972-7 22
40. Gervais, A., Karame, G.O., Capkun, V., Capkun, S.: Is Bitcoin a decentralized currency? In: Proceedings of the IEEE Symposium on Security and Privacy, vol. 3, no. 12, pp. 54–60 (2014)
41. Gervais, A., Karame, G.O., W¨ust, K., Glykantzis, V., Ritzdorf, H., Capkun, S.: On the security and performance of proof of work

blockchains. In: Proceedings of the ACM Conference on Computer and Communications Security (CCS), pp. 3–16, Vienna, Austria (2016)
42. Go-ethereum Authors: Official Go implementation of the Ethereum protocol. https://github.com/ethereum/go-ethereum. Accessed Apr 2017
43. Guha, S., Murty, R., Sirer, E.G.: Sextant: a unified framework for node and event localization in sensor networks. In: Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp. 205–216. ACM (2005)
44. Hearn, M., Corallo, M.: Connection bloom filtering. BIP 37. https://github.com/ bitcoin/bips/blob/master/bip-0037.mediawiki. Accessed Sept 2017
45. Heilman, E., Kendler, A., Zohar, A., Goldberg, S.: Eclipse attacks on Bitcoin's peer-to-peer network. In: Proceedings of the USENIX Security Symposium, pp. 129–144, Washington, D.C., USA (2015)
46. IP Info Team. IP Info. http://ipinfo.io/. Accessed Apr 2017
47. jackwinters. Ethpool & Ethermine voting on the soft fork. https://forum.daohub.org/t/ethpool-ethermine-voting-on-the-soft-fork /5364. Accessed Apr 2017
48. Jameson, H.: Hard fork no. 4: Spurious Dragon. https://blog.ethereum.org/2016/ 11/18/hard-fork-no-4-spurious-dragon/. Accessed Apr 2017 49. Koshy, P., Koshy, D., McDaniel, P.: An analysis of anonymity in Bitcoin using P2P network traffic. In: Christin, N., Safavi-Naini, R. (eds.) FC 2014. LNCS, vol. 8437, pp. 469–485. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3- 662-45472-5 30 50. Kwon, A., Lazar, D., Devadas, S., Ford, B.: Riffle: an efficient communication system with strong anonymity. In: Proceedings of the Privacy Enhancing Technologies Symposium (PETS) (2016) 51. Loibl, A.: Namecoin. namecoin.info (2014) 52. Lumezanu, C., Baden, R., Spring, N., Bhattacharjee, B.: Triangle inequality variations in the internet. In: Proceedings of the ACM SIGCOMM Conference on Internet Measurement (IMC), pp. 177–183 (2009) 53. Malkhi, D., Reiter, M.: Byzantine quorum systems. J. Distrib. Comput. 11(4), 203–213 (1998) 54. Maymounkov, P., Mazi`eres, D.: Kademlia: a peer-to-peer information system based on the XOR metric. In: Druschel, P., Kaashoek, F., Rowstron, A. (eds.) IPTPS 2002. LNCS, vol. 2429, pp. 53–65. Springer, Heidelberg (2002). https://doi.org/10. 1007/3-540-45748-8 5 55. McCorry, P., Shahandashti, S.F., Hao, F.: A

smart contract for boardroom voting with maximum voter privacy. In: Kiayias, A. (ed.) FC 2017. LNCS, vol. 10322, pp. 357–375. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70972-7 20 56. Miller, A., et al.: Discovering Bitcoin's public topology and influential nodes (2015) Decentralization in Bitcoin and Ethereum Networks 457 57. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008) 58. Nayak, K., Kumar, S., Miller, A., Shi, E.: Stubborn mining: generalizing selfish mining and combining with an eclipse attack. IACR Cryptology ePrint Archive 2015, 796 (2015) 59. Pappalardo, G., Di Matteo, T., Caldarelli, G., Aste, T.: Blockchain inefficiency in the Bitcoin peers network. arXiv preprint arXiv:1704.01414 (2017) 60. Parity Authors: Ethereum Rust client. https://github.com/paritytech/parity. Accessed Apr 2017 61. Pyethapp Authors: Python based client implementing the Ethereum protocol. https://github.com/ethereum/pyethapp/. Accessed Apr 2017 62. Reyzin, L., Meshkov, D., Chepurnoy, A., Ivanov, S.: Improving authenticated dynamic dictionaries, with applications to cryptocurrencies. In: Kiayias, A. (ed.) FC 2017. LNCS, vol. 10322, pp. 376–392. Springer, Cham (2017). https://doi.org/ 10.1007/978-3-319-70972-7 21 63. Sinnott, R.W.: Virtues of the haversine. Sky and Telescope (1984) 64. Sompolinsky, Y., Zohar, A.: Secure high-rate transaction processing in Bitcoin. In: B¨ohme, R., Okamoto, T. (eds.) FC 2015. LNCS, vol. 8975, pp. 507–527. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-47854-7 32 65. Statoshi Team: Statoshi info. http://statoshi.info/. Accessed May 2017 66. Swende, M.: Announcement of imminent hard fork for EIP150 gas cost changes.
https://blog.ethereum.org/2016/10/13/announcement-imminent-hard-forkeip150-gas-cost-changes/. Accessed Apr 2017 67. Wang, G., Zhang, B., Ng, T.: Towards network triangle inequality violation aware distributed systems. In: Proceedings of the ACM SIGCOMM Conference on Internet Measurement (IMC), pp. 175–188. ACM (2007) 68. Wang, L., Liu, Y.: Exploring miner evolution in Bitcoin network. In: Mirkovic, J., Liu, Y. (eds.) PAM 2015. LNCS, vol. 8995, pp. 290–302. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-15509-8 22 69. Wang, Y., Burgener, D., Flores, M., Kuzmanovic, A., Huang, C.: Towards streetlevel client-independent IP geolocation. In: Proceedings of the USENIX Symposium on Networked Systems Design and Implementation (NSDI), pp. 365–379. USENIX Association (2011) 70. Wood, G.: Ethereum: a

secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper (2014)