تحلیل امنیت یک شبکهٔ همتابه‌همتا مبتنی بر زنجیرهٔ قالبی

ارائه پایان‌نامه برای دریافت درجهٔ کارشناسی ارشد در رشتهٔ مهندسی برق

محمدتقی بدخشان

استاد راهنما: دکتر محمدعلی اخایی

دانشگاه تهران

۲۱ مهر ۱۳۹۹

فهرست عناوین

۱ مقدمه

۲ تعاریف، اصول و مبانی نظری

۳ مروری بر کارهای انجام شده

۴ ارائهٔ روش

۵ کارهای آینده

عملکرد و مزایای بیت‌کوین

مقدمه

اجزای بیت‌کوین

۱. ابزارهای رمزنگاری
۲. شبکهٔ همتابه‌همتا
۳. الگوریتم اجماع

مزایای بیت‌کوی

۱. مقاوم در برابر سانسور
۲. مقاوم در برابر تغییر
۳. دارای گم‌نامی نسبی
۴. شفافیت در ساز و کار، تورم و نقدینگی

حریم خصوصی در بیت‌کوین

مقدمه

اهمیت:

- محافظت از دارایی افراد
- حفظ گم‌نامی فعالین اجتماعی/سیاسی
- افشای اطلاعات یک فرد می‌تواند منجر به افشای اطلاعات افراد مرتبط گردد

حملات:

- گراف تراکنش
- تحلیل ترافیک
- کشف آدرس‌های اصلی یک کیف‌پول و آدرس IP آن
- و غیره ...

گره کامل

گره‌ها در بیت‌کوین

تعریف (گره کامل)

گره کامل گرهی است که تمام زنجیره بلوکی را ذخیره کرده و توانایی تصدیق آن را داشته و قادر به مسیریابی و تبادل اطلاعات در شبکه همتا به همتای بیت کوین باشد.

- گره کامل از بالاترین سطح امنیت و حریم خصوصی در شبکهٔ بیت‌کوین برخوردار است.
- پیاده‌سازی هستهٔ بیت‌کوین (Bitcoin-core)

گره سبک

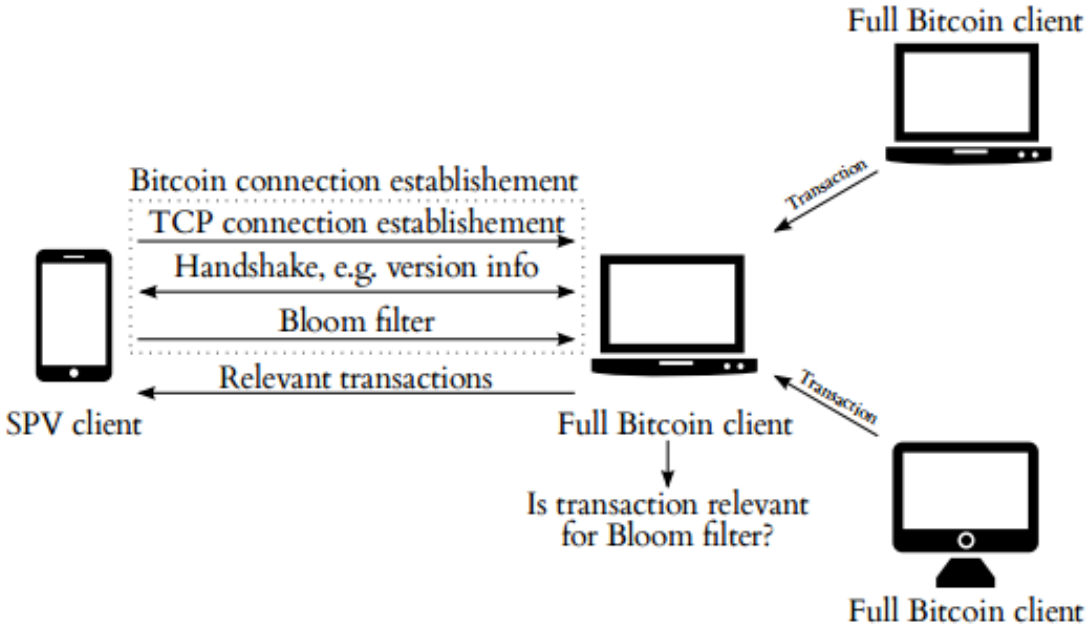
گره‌ها در بیت‌کوین

تعریف (گره سبک)

گره سبک زنیجرهٔ بلوکی را دانلود و ذخیره نمی‌کند. از روش درستی سنجی پرداخت ساده‌شده (SPV) وجود یک تراکنش در زنجیرهٔ بلوکی را می‌تواند تصدیق نماید.

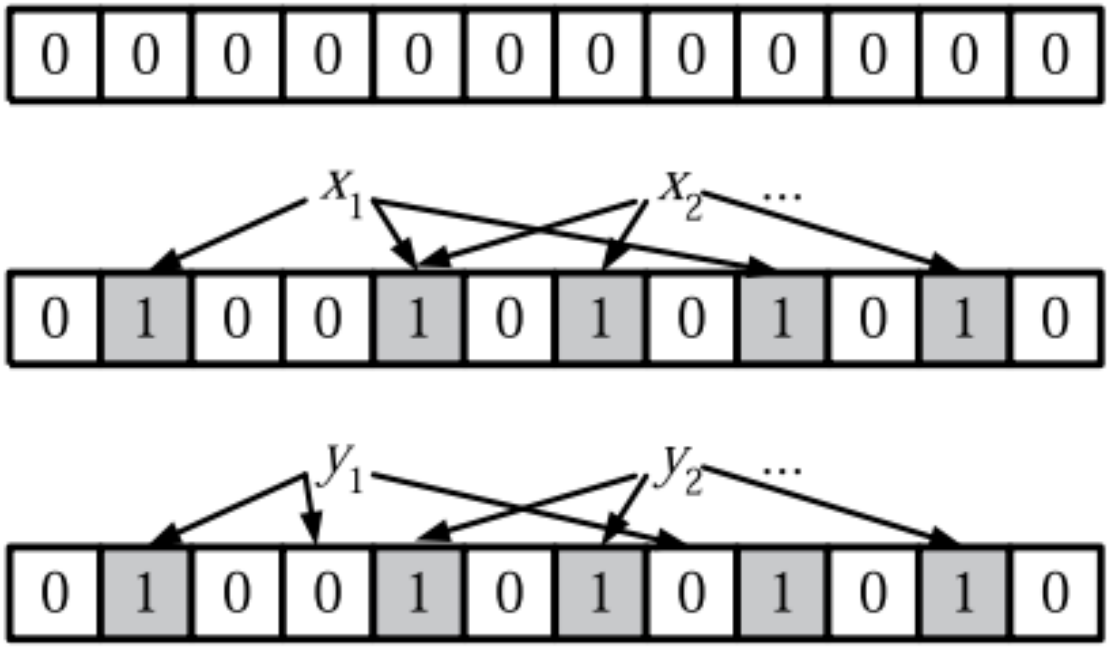
- گره سبک نیاز دارد که به گره(های) کامل اعتماد نماید.
- وابستگی گره سبک به گره‌های کامل در تصدیق تراکنش‌ها، حریم خصوصی گره سبک را نقض می‌کند.
- پیاده‌سازی‌های متعددی برای گره سبک وجود دارد، مانند: بیت‌کوین‌جی (BitcoinJ)، الکترام(Electrum) و پیکوکوین (PicoCoin)

گره سبک در شبکهٔ همتابه‌همتای بیت‌کوین



شکل: ارتباط گره سبک با یک یا چند گره کامل در شبکهٔ همتابه‌همتای بیت‌کوین [GCKG14]

فیلتر بلوم



شکل: نمایش فیلتر بلوم [BM04]

فیلتر بلوم در گره سبک (بیت‌کوین‌جی)

- BIP 37
- عناصر قرارداده شده:
- چکیدهٔ تراکنش (TXID)، نبشته‌ها(Script) در خروجی، COutPoint در وردی، نبشته‌ها در ورودی

- $P_t = \%۰.۱$ (نرخ خطای نوع دو)
- $M = m + ۱۰۰ = ۲N + ۱۰۰$ (ظرفیت)
- افزایش تدریجی اعضا

- قراردادن PubKey و PubKeyHash
- باعث ایجاد آسیب‌پذیری ([Nic15])

احتمال حدس آدرس‌های اصلی فیلتر بلوم

آسیب‌پذیری‌های فیلتر بلوم

$P_{h_{(j)}}$ برابر است با احتمال حدس صحیح j عنصر اصلی فیلتر بلوم [GCKG۱۴]:

جدول: مقادیر $P_{h_{(.)}}$ با توجه به N ($P_t = \%۰.۱$). [GCKG۱۴].

N	۱	۱۹	۴۹	۵۴	۸,۹۹۹
$P_{h_{(۱)}}$	۱	۰.۴۲	۰.۰۰۰۲۱	۰.۱۴	۰.۲۱
$P_{h_{([N/۲])}}$	—	۰.۰۰۰۰۲۶	۰	۰	۰
$P_{h_{([N])}}$	۱	۰	۰	۰	۰

افزایش این احتمال با در دست داشتن فیلترهای بلوم متعدد با عناصر مشترک

عدم توجه به حاشاپذیری

آسیب‌پذیری‌های فیلتر بلوم

	b[0]	b[1]	b[2]	b[3]	b[4]	b[5]	b[6]	b[7]	b[8]
x_1	1	0	1	0	0	0	0	1	0
x_2	0	0	1	1	0	0	0	1	0
x_3	0	0	0	1	0	1	0	0	1
B(S)	1	0	1	1	0	1	0	1	1
v_1	1	0	1	1	0	0	0	0	0
v_2	0	0	1	0	0	1	0	1	0
v_3	1	0	0	0	0	1	0	1	0

شکل: یک فیلتر بلوم با عناصر اصلی $\{x_1, x_2, x_3\}$ و عناصر پوششی $\{v_1, v_2, v_3\}$.[BBL۱۲]

باقی آسیب‌پذیری‌ها

آسیب‌پذیری‌های فیلتر بلوم

۱. بار پردازشی بالا سمت گره کامل ⇐ حملهٔ منع خدمت (DoS)

۲. عدم اتصال مداوم گره‌های سبک به شبکهٔ همتابه‌همتای بیت‌کوین

- بررسی ترکانش‌های منطبق شده با فیلتر بلوم که در همسایگی زمان درخواست گره سبک در زنجیرهٔ بلوکی ثبت شده‌اند.
- مقایسهٔ بسامد درخواست کاربر سبک با بسامد تراکنش‌های منطبق شده.

۳. تحلیل گراف تراکنش‌ها و حذف تراکنش‌های غیر مرتبط

۴. حذف تراکنش‌هایی که شامل آدرسی ساخته شده قبل از BIP37

اصلاح رفتار کاربر سبک

- قرار ندادن جفت مقدار PubKey و PubKeyHash در یک فیلتر بلوم.
- استفاده از تمام ظرفیت فیلتر بلوم
- ساخت فیلتر بلوم با آدرس‌هایی که تحت مالکیت گره سبک نیست.
- ساخت آدرس با توجه به فیلتر بلوم تولید شده
- بار پردازشی بالا سمت گره سبک

- پرهیز از ایجاد فیلترهای بلوم متعدد با عناصر مشترک

[GCKG14]: Gervais et al., *Proceedings of the 30th Annual Computer Security Applications Conference*

معیار حاشاپذیری-γ

محاسبهٔ γ با توجه به فرمول زیر:

$$\gamma(B) \approx \left(1 - \exp\left(-\frac{N_v k}{n\left(1 - e^{-km/n}\right)}\right)\right)^k \quad (1)$$

- $N_v = (N_u - m) \times P_f$
- استفاده از رگرسیون خطی برای تخمین N_u

[KTO17]: Kanemura et al., *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*

فیلتر کردن بلوک

- BIP 157, 158
- گره کامل به ازای هر بلوک یک «فیلتر بلوک» تولید می‌کند.
- استفاده از روش کدگذاری گلومب-رایس برای فشرده سازی فیلتر
- احتمال خطای نوع ۲ برابر $\frac{۱}{M}$ است.
- حجم تخمینی برای یک فیلتر بلوک به ازای $M = ۷۸۴۹۳۱$ و $P = ۱۹$ کمتر از ۱۸ کیلوبایت است.

[OAP17]: Osuntokun et al., *bips/bip-0157.mediawiki at master · bitcoin/bips - Client Side Block Filtering*

بازیابی اطلاعات خصوصی

- استفاده از روش ترکیبی IT-PIR و C-PIR
- کاربر لازم است که سرایند زنجیرهٔ بلوکی و فایل‌های مانیفست را داشته باشد.
- تقسیم‌بندی پایگاه داده به سه دستهٔ هفتگی، ماهانه و تمام مدت و ایجاد مانیفست برای هر کدام.
- حجم فایل مانیفست برای دستهٔ هفتگی، ماهانه و تمام-مدت به ترتیب ۷۲، ۲۱۸ مگابایت و ۳ گیگابایت است.

- پیشنهاد خرد کردن دستهٔ تمام-مدت به چند زیر دستهٔ کوچک‌تر.

[QHGR19]: Qin et al., *2019 Crypto Valley Conference on Blockchain Technology, CVCBT 2019*

محیط اجرای قابل اعتماد

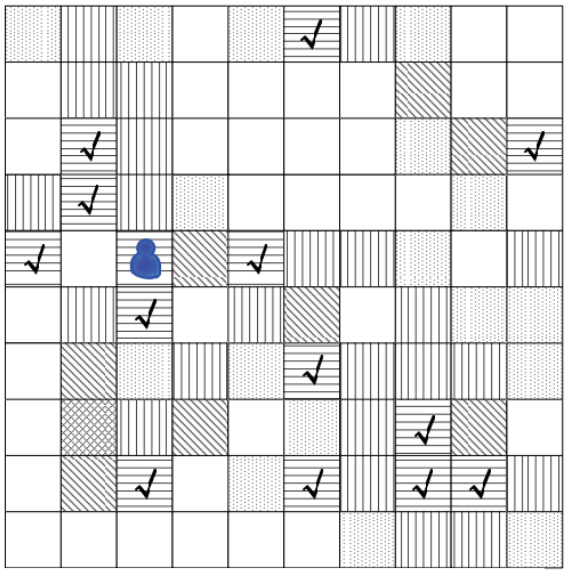
- استفاده از SGX
- ارائه دو روش

۱. پنجرهٔ پویش (Scanning Window)
   - نرمالایز کردن اندازهٔ پاسخ و اطلاعات جست‌وجو شده
   - جلوگیری از حملهٔ زمانی ← سربار پردازشی زیاد (۷۳ ثانیه برای پردازش ۱۰۰ بلوک)

۲. و پایگاه دادهٔ ناآگاهانه (Oblivious Database)
   - بهره‌گیری از ORAM
   - بدون نیاز به اثبات مرکل

[MKW+19]: Matetic et al., *Proceedings of the 28th USENIX Security Symposium*

ایدهٔ پروتکل



- ایده از مقالهٔ [NLZ+15]
- آدرس‌های پوششی دارای احتمال پرسمان یکسانی با آدرس اصلی باشند. ← افزایش آنتروپی درخواست.

[NLZ+15]: Niu et al., *Proceedings - IEEE INFOCOM 2015*

فرض و تعاریف

فرض

احتمال درخواست اطلاعات مربوط به هر آدرس a_n، به شرطی که مربوط به یک گره کامل نباشد، متناسب است با احتمال استفاده از آن آدرس در شبکهٔ بیت‌کوین.

$$\Pr\{a_n\} = \begin{cases} 0, & \text{if } a_n \in A_{f_j}, \quad \forall_j : 1 < j < W \\ \Pr\{a_{l_{ic}}\}, & \text{if } a_n = a_{l_{ic}} \in A_{l_i}, \quad \forall_{i,c} : 1 < i < M,\ 1 < c < C_{l_i} \end{cases} \tag{۲}$$

$$\Pr\{a_n\} \propto p(a_n) \triangleq \frac{|T_{a_n}|}{\sum_{m=1}^{N} |T_{a_m}|}; \forall i\ a_n \in A_{l_i} \tag{۳}$$

ملاحظات مستقل از سازوکار پروتکل

ملزومات پروتکل

کلیات:

- حفظ حریم خصوصی کاربر سبک
- بار محاسباتی و پهنای باند مصرفی پایین
- عدم الزام به اضافه کردن تجهیزات سخت‌افزاری یا نرم‌افزاری غیر معمول به گره کامل
- امکان سادهٔ ارائهٔ خدمات مبتنی بر روش ارائه شده ← جلوگیری از متمرکز شدن شبکه.
- نیاز به اعتماد به دیگر گره‌های شبکه تا حد امکان پایین باشد.

ملزومات پروتکل

ملاحظات در انتخاب آدرس‌های هم احتمال

- کاربر سبک امکان محاسبهٔ بسامد دخ‌داد همهٔ آدرس‌ها در زنجیرهٔ بلوکی را ندارد
- درخواست مستقیم آدرس‌های هم احتمال با یک آدرس مشخص از یک گره کامل ← نیازمند اعتماد و نقض حریم خصوصی
- باید اطلاعات اضافهٔ در خواست داده شده حداقل شود.
- تغییر مداوم آدرس‌های پوششی باعث به خطر افتادن حریم خصوصی کاربر سبک می‌شود.

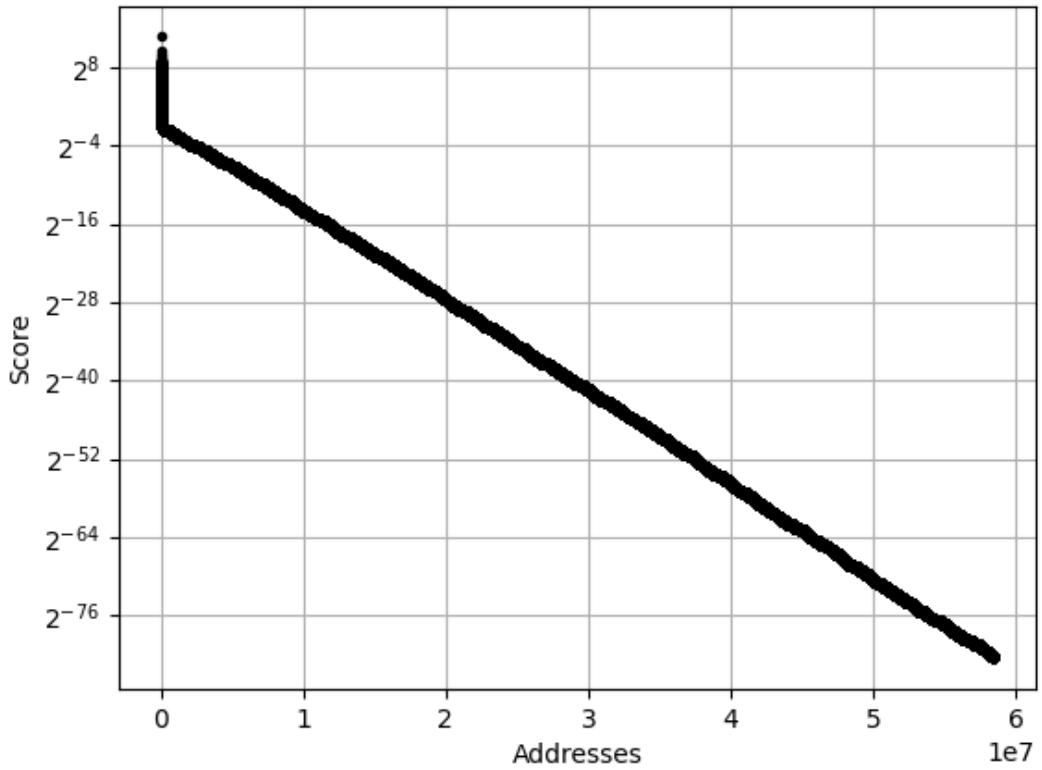
محاسبهٔ مستقل از دیگر آدرس‌ها

- هر گره سبک باید تعداد تراکنش‌های مرتبط با خود را ذخیره نماید.
- برای هر آدرس a_n یک امتیاز به صورت زیر محاسبه می‌شود

$$s_{a_n}^{t_\circ} = \beta NT_{a_n}^{t_\circ} + (1-\beta)s_{a_n}^{t_\circ - 1} \qquad (۴)$$

- هر دوره زمانی قابل تنظیم است. در این پیاده‌سازی مقدار آن برابر یک روز یا ۱۴۴ بلوک در نظر گرفته شده است.

امتیاز آدرس‌های بیت‌کوین



شکل: امتیاز آدرس‌های بیت‌کوین در مقیاس لگاریتمی از ۲۶ ژوئن ۲۰۱۹ الی ۰۲ دسامبر ۲۰۱۹

محاسبهٔ آفلاین در سمت کاربر سبک

- در طراحی انجام شده، گره‌های سبک لازم است اطلاعات زیر را ذخیره داشته باشد:
- سرایند زنجیرهٔ بلوکی
- تمام تراکنش‌های مرتبط با خودش و این که در کدام بلوک‌ها قرار گرفته‌اند

- امتیاز به صورت آفلاین و بدون نیاز به ارسال اطلاعات اضافی قابل محاسبه است.
- اگر کاربر سبک سابقه تراکنش‌هایش را نداشت، می‌تواند با آزمون و خطا تکه‌های مختلف را امتحان نماید.
- قراردادن آدرس‌ها با ترتیب الفبایی درون تکه‌ها

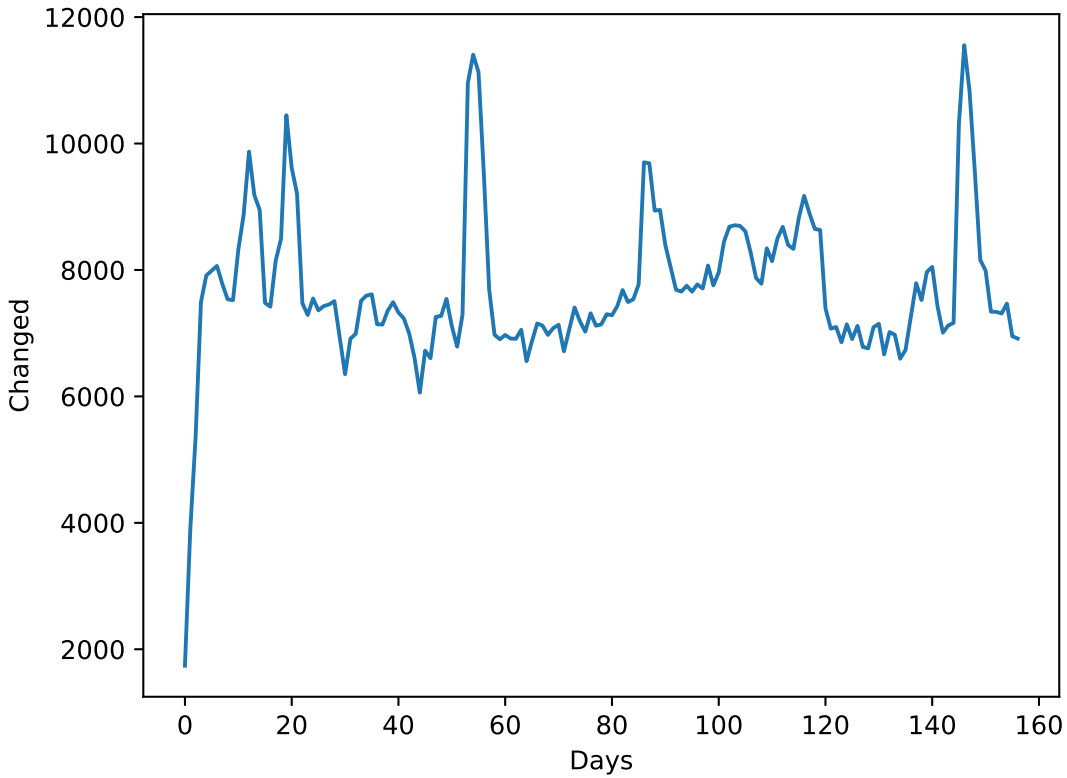
ابزارهای پیاده‌سازی شده

پیاده‌سازی و شبیه‌سازی

- راه‌اندازی در کنار نرم‌افزار هستهٔ بیت‌کوین
- عدم استفاده از واسط‌های برنامه‌نویسی
- تجزیهٔ مستقیم فایل‌های blk.dat
- امکان تجزیهٔ انواع نبشته‌ها

- استفاده از پایگاه دادهٔ ردیس
- نیاز به ۳۶ گیگ حافظهٔ دائمی

تغییر آدرس‌ها در میان تکه‌ها

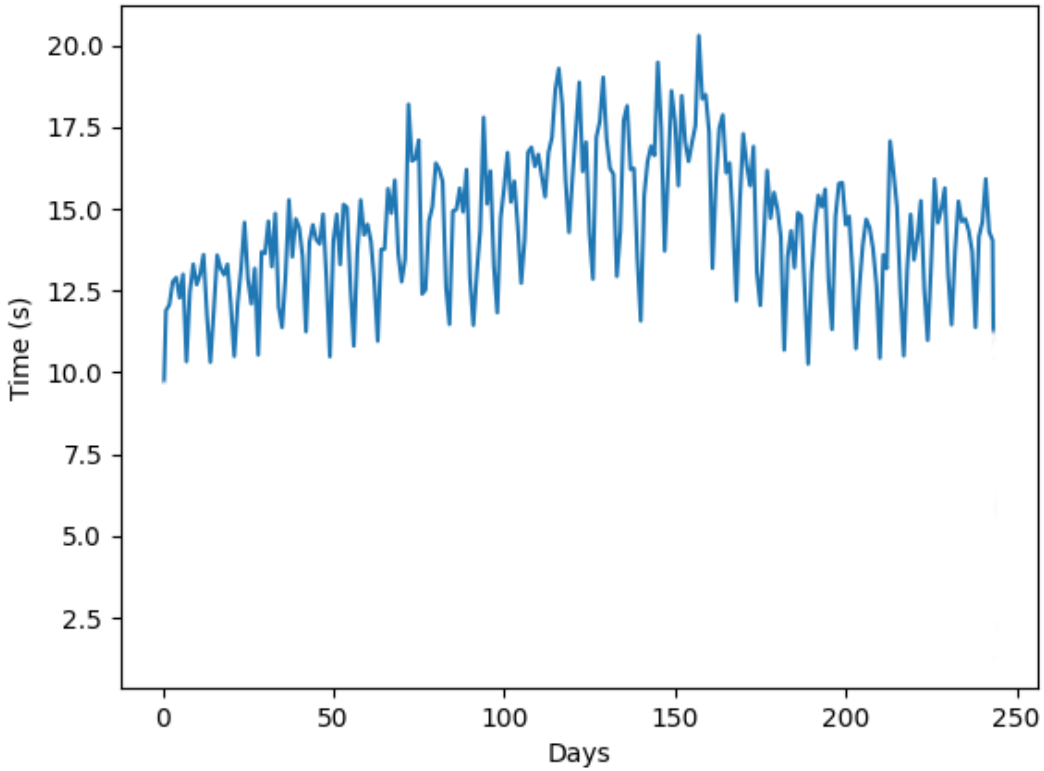


شکل: جابه‌جایی آدرس‌ها در میان تکه‌های مختلف از ۲۶ ژوئن ۲۰۱۹ الی ۰۲ دسامبر ۲۰۱۹.
$(\beta = ۰.۳)$

به روزرسانی و هم‌گام‌سازی

- با حذف آدرس‌های با موجودی صفر، زمان محاسبهٔ امتیاز آدرس‌ها از ۲۵ دقیقه به ۲ دقیقا کاهش پیدا می‌کند.
- در همگام‌سازی اولیهٔ یک گره کامل تازه اضافه شده، می‌توان تنها امتیاز آدرس‌هایی که در روزهای مورد بررسی استفاده شده‌اند را بررسی نمود.

زمان به روزرسانی وضعیت‌ها در حالت هم‌گام‌سازی



شکل: زمان به روز رسانی امتیازها برای هر روز از ۱۹ ژانویه ۲۰۱۹ الی ۲۱ سپتامبر ۲۰۱۹.

امنیت
بحث و مقایسه

- امکان تعیین آدرس‌های پوششی به صورت هوشمندانه و به مقدار دلخواه
- استقلال بین درخواست‌های متفاوت کاربر سبک
- مقاوم در برابر تحلیل بسامد
- عدم نیاز به تجهیزات سخت‌افزاری و نرم‌افزاری پیچیده
- امکان سادهٔ راه‌اندازی گره‌های کامل ارائه دهندهٔ این خدمت ← تمرکز کمتر شبکه

پهنای باند مصرفی و پردازش سمت کاربر

بحث و مقایسه

پهنای باند مصرفی:

- قابل تنظیم، شامل تراکنش‌های اصلی به علاوهٔ تراکنش‌های پوششی و اثبات مرکل آن

پردازش سمت گره کامل:

- پردازش سنگینی در سمت گره کامل وجود ندارد

کارهای آینده

- صحت‌سنجی فرض انجام شده با استفاده از آزمایش
- تعیین پارامتر بهینهٔ β

Giuseppe Bianchi, Lorenzo Bracciale, and Pierpaolo Loreti.

Better than nothing privacy with bloom filters: To what extent?

Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7556 LNCS:348–363, 2012.

Andrei Broder and Michael Mitzenmacher.

Network applications of bloom filters: A survey.

Internet Mathematics, 1(4):485–509, 2004.

Arthur Gervais, Srdjan Capkun, Ghassan O. Karame, and Damian Gruber.

On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients.

Proceedings of the 30th Annual Computer Security Applications Conference, page 326–335, 2014.

Kota Kanemura, Kentaroh Toyoda, and Tomoaki Ohtsuki.

Design of privacy-preserving mobile bitcoin client based on γ-deniability enabled bloom filter.

2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2017-October:1–6, 2017.

Sinisa Matetic, Kari Kostiainen, Karl Wüst, Ghassan Karame, Moritz Schneider, and Srdjan Capkun.

BITE: Bitcoin lightweight client privacy using trusted execution.

Proceedings of the 28th USENIX Security Symposium, pages 783–800, 2019.

Jonas David Nick.

Data-Driven De-Anonymization in Bitcoin.

ETH Zurich, pages 1–32, 2015.


Ben Niu, Qinghua Li, Xiaoyan Zhu, Guohong Cao, and Hui Li.
Enhancing privacy through caching in location-based services.
Proceedings - IEEE INFOCOM, 26:1017–1025, 2015.


Olaoluwa Osuntokun, Alex Akselrod, and Jim Posen.
bips/bip-0157.mediawiki at master · bitcoin/bips - Client Side Block Filtering, 2017.
https://github.com/bitcoin/bips/blob/master/bip-0157.mediawiki.


Kaihua Qin, Henryk Hadass, Arthur Gervais, and Joel Reardon.
Applying private information retrieval to lightweight bitcoin clients.
In *Proceedings - 2019 Crypto Valley Conference on Blockchain Technology, CVCBT 2019*, pages 60–72. Institute of Electrical and Electronics Engineers Inc., jun 2019.