گزارش جامع(مقاله رسمی) شبکه سنتیویت

عنوان: سنتیویت – وب جهانی

چکیده

سنتیویت یک وب سایت ترکیبی است(به طور متمرکز انجام شده و با اجزای غیرمتمرکز توسعه یافته) که به عنوان جایگزینی مناسب و واقعی برای وب مدرن ساخته شده است. این شبکه به هدف برتری توانایی هایی که هر شبکه صرفا متمرکز یا غیر متمرکز می تواند ارائه دهد طراحی شده است. سنتیویت به طور مستقیم به موارد زیر می پردازد: بحران پهنای باند، پروتکل های منسوخ شده و قدیمی، عدم پاسخگویی،DNS فرسوده و خراب، عدم هویت، امنیت واکنشی،قوانین حوزه و طبقه بندی وب

تمرکز

این گزارش جامع و دقیق بر روی طراحی شبکه اصلی که به عنوان شبکه مبنا، پایه وسازنده برای

Viat, hApps و وب جهانی عمل میکند متمرکز شده است. گزارش جامع تکمیلی دیگری بر

روی VIAT منتشر خواهد شد.تکنولوژی تماما بر حصول اطمینان از این که سنتیویت یک انقلاب تحول زا و لزوما یک جایگزین تکاملی در ساختار مدرن اینترنت محسوب نمیشود، متمرکز شده است.

مقدمه

وضعیت وب جهان گستر

هم اکنون ما در حال استفاده از یک رسانه ویرانگردر اتصال ارتباطات در مقیاس جهانی هستیم. خواسته های بشریت به طور چشمگیری در حال افزایش است که باعث میشود شبکه وب جهانی به سادگی نتواند پاسخگوی آن باشد. همانطور که ما در حال رشد، تکامل، سفرو کشف فراتر از منظومه شمسی هستیم، وظایف ضروری ما تبدیل به انقلابی در تکنولوژی ای که ما به آن وابسته هستیم میشود.

وضعیت کنونی شبکه جهانی وب قوی و رضایت بخش نیست. اگر بشریت همچنان به مشکلات مخرب موجود در اینترنت ادامه دهد، اینترنت "غرب وحشی خود رو"(Wild Wild Web) باقی خواهد ماند. تقاضای روزافزون بشر هرگز توسط وضعیت کنونی وب پاسخکو نخواهد بود. ما باید به لحاظ تحولی یا انقلابی و نه تکاملی فکر کنیم. راهکار مناسب، جایگزینی کامل سیستم های معاصر، مرورگرها، زبان ها، پروتکل ها و سیستم عامل ها با افزایش امنیت، سرعت، کارایی، پاسخگویی، اعتماد، هویت، قابلیت و اطمینان است. برای انتقال به یک عصر جدید اطلاعات باید چیزی که ما با آن راحت هستیم جایگزین کنیم.

بحران پهنای باند

پهنای باند محدود است و نیازهای ما فراتر از شبکه ها است. برای حل این مسئله ما نیازمند تکنولوژی انقلابی مدرن برای جایگزینی اجزای موجود هستیم. در غیر اینصورت خطوط سریع و اولویت بندی داده ها تنها انتخاب ماست. همه ی ترسی که گروه ها از لغو شبکه نامشخص و بی اثر دارند تنها انتظار ما در حفظ وب گردی خواهد بود. افزایش اجتناب ناپذیر IoT ، دستگاه های بیشتر برای هر شخص و در هر خانه، اتومبیل های اتوماتیک،تجزیه و تحلیل بیمه اتومبیل،واستفاده کشورهای در حال توسعه بصورت آنلاین از پهنای باندی که ما در دسترس نداریم.

شبکه قدیمی و منسوخی که به آن استناد میکنیم در حال تخرب خودش است.

HTTP و DN مدت ها قبل بدون توجه به نیازهای مدرن ساخته شده اند. پهنای باند روز به روز در

حال استفاده شدن است، HTTP همچنان در حال ارائه مقیاس پذیری بالای خود هستند درحالیکه DNS مقیاس پذیر و قابل اعتماد نیستند.

اگر بتوانیم نیمی از وب ها را از سرورهای DNS مخصوص DOS ببندیم، یک مشکل ساختاری آشکار به وجود خواهد آمد.HTTP حمل کننده فعلی پول است.

کل اقتصاد دیجیتال از طریق HTTP انتقال داده میشود. هر گونه کاهش سرعت HTTP و DNS به منزله ی کاهش شدید اقتصاد جهانی است. DNS و HTTP به طور ذاتی فرسوده شده اند،مقیاس پذیری ضعیفی دارند، خیلی آهسته هستند، دارای ویژگی های مدرن نیستند،پهنای باند مصرف می کنند،و هزینه مصرف کنندگان و کسب و کار درآن میلیاردها دلار است. اگر ما این مسئله را حل نکنیم، ضربه بزرگی به اقتصاد وارد خواهیم کرد.اگر همه ی تاثیرات دلار را در نظر بگیرید به زودی متوجه میشوید که یک وب سایت کند میتواند یک بحران انسانی جهانی باشد.

1. یک ثانیه تاخیر میتواند به ارزش 1.6 میلیون دلار فروش در آمازون باشد.
2. ده سال پیش، آمازون متوجه شد که هر100میلی ثانیه تاخیر به ارزش یک درصد از فروش است.
3. ده سال بعد، مطالعه Akamai 2017 نشان داد که هر100 میلی ثانیه تاخیر در زمان بارگذاری وبسایت میتواند نرخ تبدیل را 7 درصد کاهش دهد- که کاهش قابل توجهی در فروش است- 6 درصد- از زمانی که آمازون برای اولین بار در مورد تاخیر در ثانیه و میلی ثانیه صحبت کرد. این نشان می دهد هیچ چیز برای خرده فروشان آنلاین آسان تر نمی شوند، زیرا تجربه کاربر برای موفقیت تجارت الکترونیک حیاتی است.

شکست شبکه غیرمتمرکز WEB AKA WEB 3.0

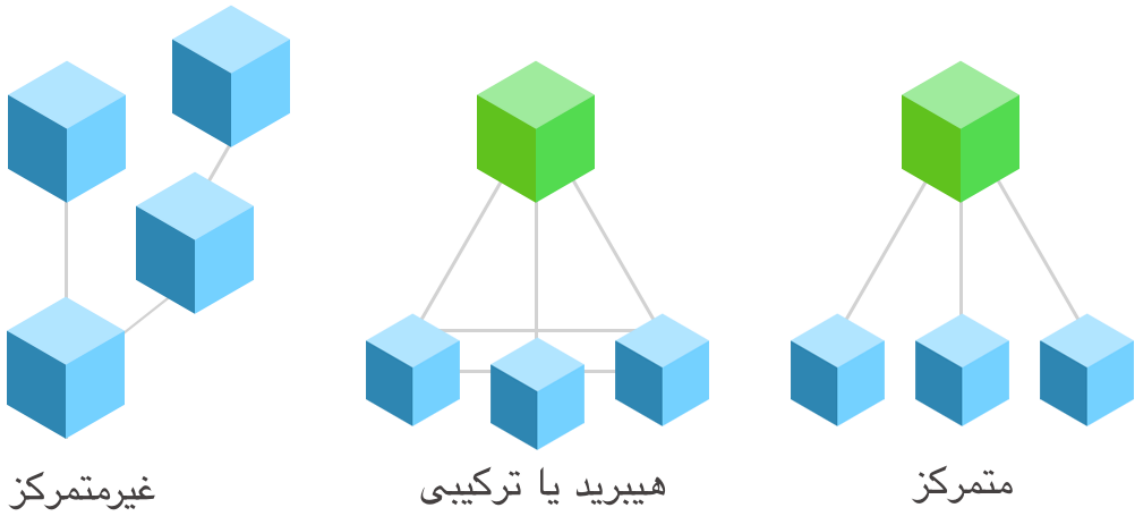
ما می دانیم که اقتصاد جهانی نیازمند یک وبسایت پرطرفدار و ارزان است. اگر یک وبسایت صرفا غیرمتمرکز جایگزین یک وبسایت مدرن گردد،پس از آن بحران پهنای باند را تسریع خواهد کرد و سبب تخریب وبسایت خواهد شد. عبارت وب 3.0 یک جهان سح آمیز، یک ایده تحول انگیز یا یک راه حل

نیست؛ بلکه برداشت پول نقد است. معاملات در نانوثانیه ها اتفاق می افتند؛ اقتصاد جهانی فرصتی برای دقیقه یا ثانیه ای انتظار برای انسداد زمان به منزله ی تأیید و سپس انتشار از طریق شبکه را ندارد. جایگزینی که برای وب انتخاب میشود نباید برای مشتریان کندتر و گرانتر باشد. وب 3.0 قیمت بیشتری دارد ولی این هزینه در پشت چیزهای متفاوتی مانند هزینه های بسیار کم برای راه اندازی این برنامه پنهان شده است. واقعیت این است که شما چیزی را دریافت میکنید که قیمتش را پرداخت کرده اید. وب سایت 3.0 به جای خدمات به کاربران، هزینه می بخشد که همین باعث کاهش عملکرد آن می شود.

یکی دیگر از بحث های رایج این است که کاربران را از طریق رمزگذاری همگن قادر به کنترل داده های خود کنیم. به جای حل این مسئله ازطریق توپولوژی، نیازمند نوآوری در هر جنبه ای از وب و درخواست های بیشتر از خدمات وب هستیم. مشکل توپولوژی وب درمقایسه با مشکل تکنولوژی منسوخ شده آن بسیار کم است. اگر پروژه های Web 3.0 واقعا در مورد تغییرات وب مشغول بودند، در واقع آنها بر مسائل واقعی تمرکز می کردند. هر دو توپولوژی، موارد مورد استفاده خود را دارند اما بصورت کلی هر دوی آنها یک راه حل برای یک مشکل در حال رشد و بدون کنترل است.

رمز نویسی وب جهانی(سدیم بومی)

- امضاهای کلیدی
  - امضای تک بخشی: Ed25519
  - امضای چند بخشی: Ed25519ph
- رمزگذاری بسته
  - رمزگذاری معتبر با داده های اضافی
  - رمزگذاری یک پیام با یک کلید ونگهداری محرمانه آن
  - محاسبه تست تأیید اعتبار. این برچسب برای اطمینان از این که پیام، و همچنین اطلاعات اختیاری، غیر محرمانه (غیر رمزگذاری شده)، تبادل نشده است استفاده می شود.
  - رمزگذاری: رمز عبور جریانXChaCha20
  - تأیید اعتبار:Poly1305 MAC
- تبادل کلید - دوره مشترک کلید های مخفی
  - BLAKE2B-512
    - BLAKE2 یک تابع رمزنگاری سریعتر ازMD5, SHA-1, SHA-2, و SHA-3 است ،هنوز هم حداقل به عنوان آخرین استاندارد SHA-3 امن است
    - بهینه شده برای سیستم عامل های 64 بیتی ، از جمله ARM های فعال NEON و تولید خلاصه هایی با اندازه های متفاوت، بین 1 تا 64 بایت
  - X25519 –جفت کلید زودگذر و کوتاه مدت
    - محاسبه و تخمین رازی که بین فرستنده و گیرنده به اشتراک گذاشته شده است،با استفاده از کلید مخفی فرستنده و کلید عمومی گیرنده (یا برعکس)
- شبکه های ترکیبی



پروتکل ها

پروتکل های جریان داده جهانی

پروتکل انتقال داده

پروتکل های جریان داده جهانی یک UDP بر مبنای تاخیر کم ، زمان واقعی، دو سمتی، رمزگذاری شده و پروتکل انتقال اطلاعات قابل اعتماد است.

مشکلات

همانطور که در مقدمه آمده است: خواسته های کاربران در طول زمان تغییر کرده و نیازهای ما از وب افزایش یافته است. تغییرات HTTP یک تنگنای عمده را ایجاد می کند. استاندارد HTTP و TCP هر دو مسائل بزرگی هستند. مراکز داده های بزرگ، در حال انتقال اطلاعات فراوان از یک نقطه به نقطه دیگر دارای تأخیر و هزینه هایی میشوند که مربوط به ساختار قدیمی اینترنت می باشند. HTTP به خصوص زمانی مشکل است که کاربران در حال تجربه، عملکرد کمی دارند، پهنای باند محدود است، اتصال به شبکه تضعیف شده یا نیاز به پاسخ نزدیک به زمان واقعی است.

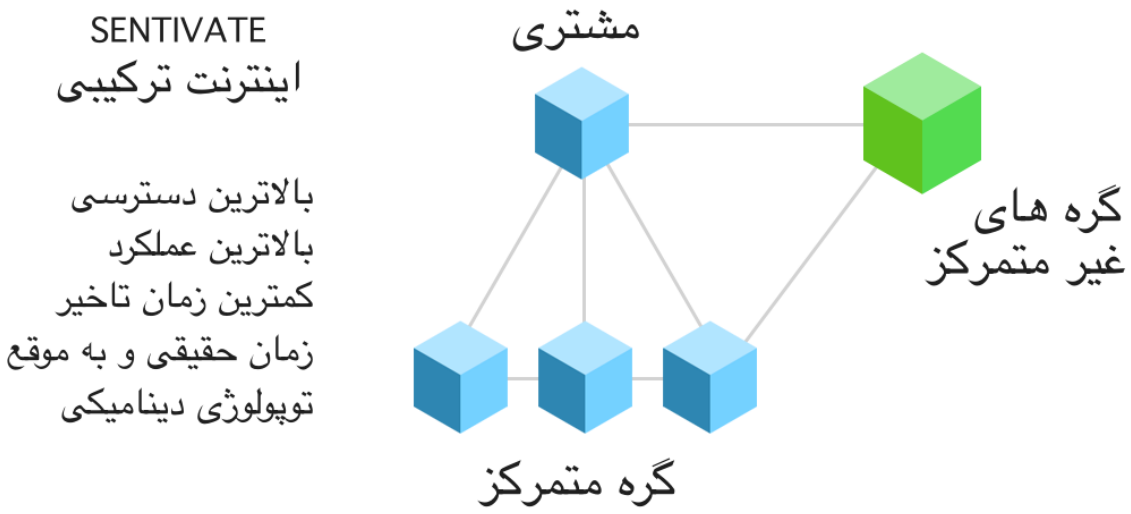
راه حل ها

اولین قدم در ساخت وب جهانی، جایگزینی HTTP به طور کامل با UDSP است. پروتکل های جریان داده جهانی UDP مبنی بر تاخیر کم ، زمان واقعی، دو سمتی، رمزگذاری شده و پروتکل انتقال اطلاعات قابل اعتماد است. در وب جهانی همه ارتباطات، جریان ها، و یا انتقال هر نوع داده با استفاده از UDSP انجام میشود. هنگام بازدید از یک سایت در UDSP جهانی، پروتکل به جای HTTP استفاده می شود. ماژول های سرور و پردازشگر خاص UDSP برای بازدید یا میزبانی یک وب سایت در شبکه Sentivate مورد نیاز است.UDSP پایه و بنیاد شبکه Sentivate است.

UDSP قابلیت اطمینان دینامیکی را در سطح اتصال دارد ، یا براساس تقاضای درخواست شده بین طرفین به کار گرفته می شود.UDSP رمزگذاری را اجرا می کند که این به این معنی است که تمام اتصالات UDSP به صورت پیش فرض و بدون هیچ استثنایی رمزگذاری می شوند.UDSP از IPv6، Multiplexingو Multihoming پشتیبانی می کند.UDSP بر کلید های رمزنگاری و XChaCha20 برای برقراری ارتباط متکی است.

UDSP زمان واقعی وب سایت و محاسبات پراکنده را اولویت بندی می کند. دو سمتی بودن ارتباطات باعث می شود شبکه کمتر مسدود شود که سبب کمبود تاخیر برای اتصال میشود.UDSP به مراتب کمتر از HTTP صحبت می کند و می تواند به صورت برنامه ای برای تنظیم استانداردهای قابلیت اطمینان خودش تنظیم شود. این باعث می شود UDSP یک پروتکل بسیار مفید باشد که در آن نیاز به خروجی و اطمینان بالا و همچنین تاخیر کم وجود دارد.

در وضعیت ارتباطات شبکه ای بسیار متغیر و ضعیف هم به دلیل طبیعت پویای برنامه ای، UDSP میتواند موثر وکارآمد باشد.UDSP دارای معماهای اختیاری در بسته ها است است که به ارائه دهندگان و حل کننده ها اجازه می دهد تا VIAT کسب کنند. پازل ها می توانند متفاوت باشند و بنابراین آنها یک گواه پویا از کارهستند. پازل ها ممکن است بسته بندی شده باشند یا به داده های مورد نیاز برای حل آنها نیاز داشته باشند. این قابلیت در گزارش جامع بعدی برای VIAT توصیف خواهد شد. پازل ها همچنین به عنوان کنترل احتمالی و راهی برای محدود کردن آسیب بالقوه از حملات DDOS عمل می کنند.
Sentivate یک حمله معمولی DDOS را از طریق معرفی پازل های مختلف در پاکت ها به سود تبدیل میکند. هنگامی که مشتری یک پازل را حل می کند،client (مشتری) و domain(یک شبکه فرعی که از گروهی از مشتری و سرورها ساخته شده) از طریق شبکه با Viat اعتبار داده می شوند. اگر سرور تحت حمله DDOS باشد، سرور می تواند به صورت پویا پاداش و اعتبار را 100٪ برای domain در نظر بگیرد. این موضوع این اطمینان را میدهد که مهاجم ها بیشتر در معرض ضرر مالی هستند و فقط میتوانند مقدار کمی کسب کنند. پازل ها تضمین میکنند که هر دو طرف پاداشی برای عمل صادقانه خود خواهند داشت.



سیستمdomain(دامنه) جهانی

گواهی Domain (دامنه)

مسیریابی و پارامترهای رمزی

گواهی domain مسیریابی، رمزنگاری و اطلاعات اضافی مرتبط با نام میزبان را ارائه می دهد. که توسط 3 یا چند جفت کلیدی و مهم امضا می شود: اپراتور، Master(کارفرما و اصلی) و یک ثبت کننده مجازdomain. برای ایجاد یک دستاورد موفق، گواهی domain و امضای معتبر مورد نیاز است.

گواهی کوتاه مدت domain به عنوان کیف پولی عمل میکند که منابع مالی را برای هر پازل ای که آن را به مشتریان توزیع می کند، ذخیره می کند. بخشی از داده کاوی Viat به آدرس کیف گواهی زودگذرفرستاده میشود.

ثبت کننده DOMAIN(دامنه)

گواهی های امضا و آپلود

ثبت کننده domain (DR)، برای ثبت domain و مدیریت گواهی عمومی domain استفاده می شود. DR گواهی های عمومی مرتبط با نام میزبان را معتبرسازی و امضا میکند. DR سپس گواهی را به سیستم اطلاعات domain که گواهی را برای توزیع ذخیره می کند انتقال میدهد.

سیستم اطلاعاتی DOMAIN

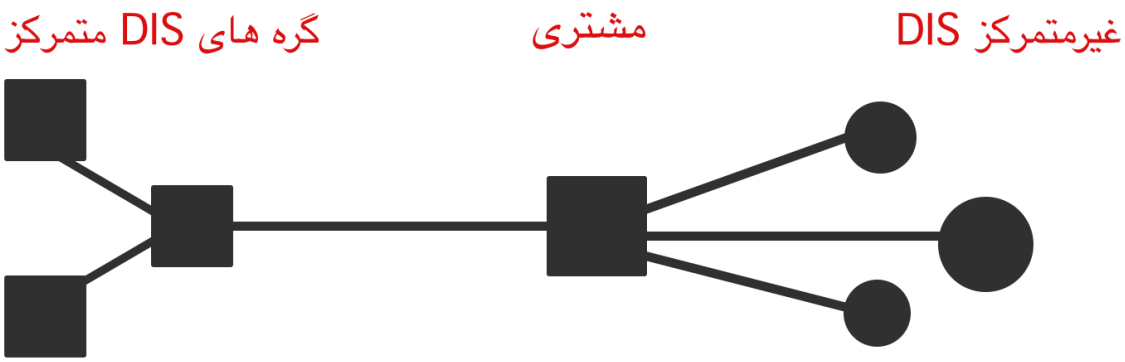
مسیریابی و رمزنگاری domain(دامنه) پرس و جو

سیستم اطلاعاتی DOMAIN (DIS) ، اطلاعات خاص را به شکل گواهیDOMAIN از نام میزبان خوانا توسط انسان بازمی گرداند . DIS گواهی DOMAIN را که شامل جزئیات رمزنگاری و اطلاعات مسیریابی است بازمیگرداند. با رمزنگاری نام های میزبان همراه با اطلاعات مسیریابی، 0-RTT بدون نیاز به اینکه مشتری از قبل domain را بازدید کند ممکن است. این یک مزیت منحصر به فرد TLS 1.3 است که در آن 0-RTT به طور پیش فرض در دسترس است در حالیکه در TLS 1.3 یک نفر باید از قبل سایت را بازدید کند. قبل از اینکه مشتریان به یک وب سایت متصل شوند، ابتدا بایستی با نام میزبان خوانا توسط انسان DIS را پرس و جو کنند.DIS دارای سرورهای متمرکز و یک شبکه غیر متمرکز است تا برای مشتریان سریع ترین راه ممکن برای دسترسی به گواهی های domain را فراهم کند.

DIS به عنوان یک لایه دیگری برای دفاع از حملات مرتبط با گواهی های نامعتبر عمل می کند. هنگامی که گواهی های نامعتبر برای درخواست اطلاعات از DIS برای رفتن به یک سرویس مورد استفاده قرار می گیرند، DIS به راحتی پاسخ را رد می کند. گره ها و اشکال غیرمتمرکز که گواهی هایdomain را دارند، می توانند از طریق خدمات آنها به Viat دسترسی داشته باشند. این قابلیت به صورت کامل توسط گزارش جامع Viat شرح داده خواهد شد.

شبکه sentivate

سیستم اطلاعات domain(دامنه) ترکیبی



DOMAINS (دامنه ها)

اسم میزبان خوانا توسط انسان

Domain هایی که در Sentivate نامگذاری می شوند، دارای نام الحاقی کامل هستند و می توانند نام های مجاز را برای اشخاص با علامت تجاری داشته باشند. قوانین و مقررات domain برای سازماندهی وب، نام های آزاد domain برای شرکت های جدید، حفاظت از علائم تجاری، محدود کردن فعالیت های مخرب، و ایجاد برنامه های توصیفی بیشتر طراحی شده اند.

به عنوان مثال، می توانید به سادگی با تایپ کردن آمازون در مرورگر Sentivate به سایت آمازون بروید. قوانین domain در شبکه Sentivate مشکل تر است.فروش نام های کمپانی ها به منظور کسب سود به کمپانی های دیگر به طور کامل غیرقانونی است، و قانون "استفاده از آن یا از دست دادن آن" حکم فرما است. محتوا یا سرویسdomain باید با پسوند آن مرتبط باشد. به عنوان مثال، فروشگاه آمازون باید از پسوندdomain فروشگاه، "Amazon.store" استفاده کند. پسوند های domain کوتاه برای domain های خاص وجود دارد. به عنوان مثال، وب سایت شرکت آمازون باید از پسوند شرکت، Amazon.company یا اصطلاح کوتاه Amazon.com استفاده کند.Bitcoin ، Ethereum، و Litecoin رمزنگاری ارزها هستند و سایت هایی که به آنها اختصاص داده شده، باید از پسوندرمزنگاری ارز استفاده کنند. با این حال، یک سایت خبری مربوط به بیت کوین باید از پسوند .news و یا .blog

استفاده کند. هر domain ای که ممکن است دارای محتوای تصادفی یا دلخواه باشد، باید از پسوند .abstract استفاده کند.

سیستم شناسایی جهانی

گواهی هویت

جفت های کلیدی و مهم master(کارفرما و اصلی) وephemeral(زودگذر)

گواهی هویت، (IC)، اسنادی است که میتوانند اطلاعات رمزنگاری که شما را در شبکه نشان می دهند، ارائه دهند و توسط یک ثبت کنده هویت امضا شده اند. یک گواهی هویت دو جفت کلیدی رمزنگاری دارد: master(اصلی و کارفرما) و ephemeral(زودگذر). جفت کلید اصلی به طور خاص برای امضای گواهی های زودگذر استفاده می شود و هسته ی شناسایی جفت کلیدی است. جفت کلید کوتاه مدت می تواند با اختیاری مالک جایگزین شود. گواهی های هویت، اعتبار مشتریان را در شبکه به صورت رمزنگاری تأیید و تصویب می کنند.

گواهی های کوتاه مدت (EC)، نوعی گواهی فرعی برای گواهی اصلی هستند. گواهی های زودگذربه عنوان پروفایل هایی است که برای دسترسی به خدمات تعریف شده توسط کاربر استفاده می شود. به عنوان مثال، گواهی کیف پول، گواهی بانکی، گواهی مرور وب عمومی و یا برای هر سرویس. با این حال، می توانید از یک گواهی کوتاه مدت برای تمام خدمات استفاده کنید.EC ها برای فرایند تبادل کلید استفاده می شوند که اتصال UDP دو طرفه بین مبدا و میزبان برقرار می شود.

کاربران می توانند بمحض ثبت نام ، وارد سایت شوند و و یک خرید با گواهی هویت خود انجام دهند. سرورها برای برقراری ساختار موفقیت آمیز UDSP نیاز به گواهی مشتری دارند. گواهی هویت،مبنا ای برای یک سیستم اعتباری غیرمتمرکز است که می تواند رفتار خوب و بد مربوط به گواهی های خاص را ثبت کند. هانی پات میتواند برای جلوگیری از دسترسی استفاده کننده های بد شناخته شده به سرویس امنیت شبکه، استفاده شود.

گواهی هویت می تواند به هویت و دارایی های واقعی جهان مرتبط باشدو باعث میشود که SENTIVATE به پایگاهی ایدا آل برای رای گیری امن، خصوصی و قابل رسیدگی در انتخابات تبدیل شود. فروشگاه ها و شرکت ها می توانند IC ها یی که کاربران را قادر می سازد از طریق Viat به طور مستقیم پرداخت یا اهدا کنند، تایید کنند.

ثبت کننده هویت

اعتبار سنجی و امضا

ثبت کننده هویت (IR) ، خدماتی است که گواهی ها را امضا می کند وهمچنین اولین لایه حفاظت از شبکه است. IR با فیلتر کردن گواهی های معیوب،جلوگیری از حملات Sybil و استفاده کننده های بد، از شبکه محافظت می کند. ثبت کننده هویت تضمین می کند که گواهی های مخرب امضا نشده است و ین باعث میشود که سرویس ها به طور موثر تلاش های اتصال آنها را رد کنند. همچنین امضاهای دروغ را می توان از طریق DIS رد کرد بنابراین به طور بالقوه یک سرویس را محافظت می کند و برخی از منابع خود را قبل از دسترسی نجات می دهد.

یک شبکه غیر متمرکز و زنجیره بلوکی غیر قابل چرخش برای تقویت اعتبار گواهی های ارسال شده برای امضا به کار گرفته می شود. اگر گواهی با موفقیت توسط شبکه آزمایش شود، IR این گواهی را امضا می کند. سپس این گواهی می تواند با موفقیت توسط سرویس ها و DIS استفاده شود. در طی تبادل اولیه، بسته اول حاوی گواهی هایی است که برای ایجاد جریان UDSP لازم است. اگر امضاها با موفقیت تایید شوند، بقیه فرایند تبادل همچنان ادامه دارد و به همین دلیل رد میشوند.

گواهی های فعال مستقیما به روز و امضا می شوند. هنگامی که یک گواهی مجددا امضا می شود، یک فیلد دیگر به گواهی اضافه می شود که زمان سپری شده از امضای قبلی گواهی را نشان می دهد. این خدمات را با یک لایه اضافی اعتماد برای گواهی های خاص ارائه می دهند.

توسعه

hApps

برنامه های ترکیبی شبکه های جهانی

برنامه های ترکیبی، خود ساخته و جریان یکپارچه ای از برنامه ها هستند. برنامه های ترکیبی با استفاده از روش های واکنشی، پویا و مدولار ایجاد شده اند.hApps دارای مزایای استفاده از شبکه های متمرکز و غیر متمرکز و حصول اطمینان از بالاترین پتانسیل مقیاس پذیری هستند.

داراییهای hApps در پرونده های خود قرار دارند و در صورت نیاز به مشتری ارائه می شود.hApps در طول زمان جریان یافته و ساخته شده اند. فقط یک بار صفحه اول شروع می شود و پس از آن صفحات به صورت پویا ساخته می شوند، همانطور که مشابه برنامه های تک صفحه ای مورد نیاز است. فقط زمانی که مشتری به منابع نیاز دارد، آن ها واکشی و تحویل داده می شوند.

اجازه جریان دارایی بالای مدولار توسط اجزاء Sentivate داده میشود. به عنوان مثال، اجزاء می توانند دارایی های مشابه در CSS یا HTML را به اشتراک بگذارند و ضمانت کنند که دارایی های مشترک تنها یک بار دانلود شده و کد تکراری هرگز بر روی سیم ارسال نمی شود. ظرفیت سرور و پهنای باند با استفاده از این روش به طور چشمگیری کاهش می یابد،زیرا مشتری دقیقا از همان چیزی است که مورد نیاز است استفاده میکند.

برنامه های ترکیبی می توانند از CDN غیر متمرکز P2P انتخاب شده برای دارایی ها علاوه بر سرویس مقصد نیز استفاده کنند. استفاده از یک شبکه تحویل محتوا ترکیبی، به این معنی است که برنامه های ترکیبی دارای قابلیت دسترسی، مقیاس پذیری و پهنای باند بیشتری هستند.

hApps معتبرسازی، سندیت ، اجازه و اختیار به مشتریان را به طور خودکار در طول تبادل و ارتباط اولیه برقرار میکند. Backend های hApps می توانند با کلید های عمومی یا گواهی های آنها، مشتریان را ذخیره و مرجع نمایند. همچنین میتوانید از آن به عنوان oAuth برای کل اینترنت یادآوری کنید.
خدمات، دیگر نیازی به نگرانی در مورد در هم سازی، ذخیره سازی و یا رمزگذاری کلمه عبور ندارند. مشتریان می توانند به سرعت با کلیک بر روی یک دکمه یا به صورت خودکار به سرویس وارد شوند. کاربران، دیگر نیازی به یادآوری یا ایجاد کلمه عبور پیچیده ای ندارند زیرا استفاده از کلید میانبر برای آنها امن تر و راحت تر است. اگر سرویس ها از شما درخواست نام کاربری نکردند، آنها می توانند از طریق کلید عمومی شما را شناسایی کنند. این بدان معنی است که برای برخی از خدمات کاربران نیازی به ایجاد نام کاربری و رمز عبور در طول فرآیند ثبت نام ندارند.

VIAT

رمزگزاری ارز بومی

Viat نوعی رمزگزاری ارز بومی روی شبکه ی sentivate است. Viat یک زنجیره بلاک ترکیبی نیز دارد. سیستم های اصلی Viat به صورت غیر متمرکز میزان شده اما با اجزای متمرکز افزایش یافته است (مخالف وب سایت Sentivate). Viat به منظور سرعت، امنیت، و برخی از پایین ترین هزینه های در دسترس معامله طراحی شده است. بخش مرکزی Viat می تواند معاملات فوری را پردازش و امنیت کیف پول را فراهم کند و همچنین زمانی که شبکه غیر متمرکز در حال بارگیری سنگینی است باعث کاهش تراکم شبکه شود. با این حال، این ویژگی های متمرکز تنها در اختیار کاربران قرار می گیرد تا مسیر خود را ایجاد کنند.

داده کاوی

Viat دلیلی برای پویایی کار است، که می تواند به دو روش داده کاوی (mining) شود. داده کاوی مستقیم، روش اصلی ای است که در گزارش جامع توضیح داده خواهد شد و روش دوم از طریق استفاده از بسته های پازل در UDSP است. پک های پازل زمانی که در حال بررسی وب جهانی است، داده کاوی غیر فعال viat را میسر میکند. با این حال، آنها به طور پیش فرض فعال نیستند.موقعیت هایی هایی که باعث میسر شدن پک های پازل می شوند عبارتند از: بمحض اتصال ارتباط، بررسی ارتباط زنده، حفاظت DDoS، کنترل تراکم، و یا سرویس هایی را انتخاب می کند که آن را به دلایل خاص فعال کند. فعال شدن پک های پازل بستگی به سرویس دارد. این امر سبب میشود که نیازی به داده کاوی ثابت در پس زمینه وجود نداشته باشد و همچنین باعث اهمیت فرایند داده کاوی واقعی میشود. در غیر این صورت، در طول زمان، میتواند منجر به استفاده منابع و عمر باتری شود.

قابلیت همکاری

گواهی هویت و domain نیز به عنوان کلید های کیف پول Viatمضاعف میشوند. این ویژگی باعث میشود تا کاربران نه تنها بلافاصله در یک اتصال ارتباطی به سرویس وارد شوند، بلکه راهی برای خرید کالا از سرویس ها، سایت ها انعامی و یا بازپرداخت مشتریان را فراهم می کنند.Viat بخش جدایی ناپذیر از قابلیت های کامل وب جهانی است که بدون آن تنها بخشی از تصویر وجود دارد.