



منتشر شده توسط

تهیه کننده

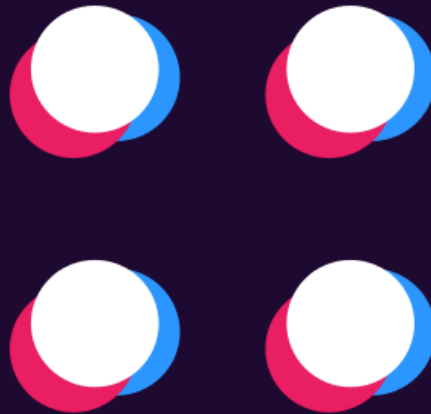
آرمان جنگ میری

کوین ایران



کوین ایران بزرگترین پایگاه خبری فارسی زبان در حوزه فناوری بلاکچین، ارزهای رمزنگاری شده و پلتفرم های مرتبط با بلاکچین است. این وب سایت در سال ۱۳۹۲ توسط بابک جلیلود و آرش محبوب، با هدف اطلاع رسانی، آموزش و مشاوره به جامعه فارسی زبان علاقه مند به رمز ارزها راه اندازی شد و اولین مقاله آن در ۱۴ دی ماه همان سال، با عنوان «بیت کوین چیست؟» منتشر گردید. هدف کوین ایران از معرفی این فناوری ایجاد محیطی پژوهشی و آموزشی در راستای استفاده صحیح از این فناوری جهت ارائه تسهیلات و رفاه به جوامع فارسی زبان است.

www.coiniran.com

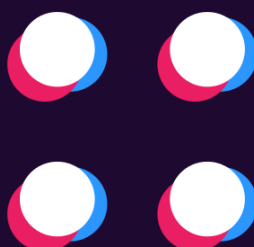


B L O C K S T A C K

اینترنت غیر متمرکز و امن بر بستر بلاکچین

مقایسه اینترنت فعلی و اینترنت غیر متمرکز

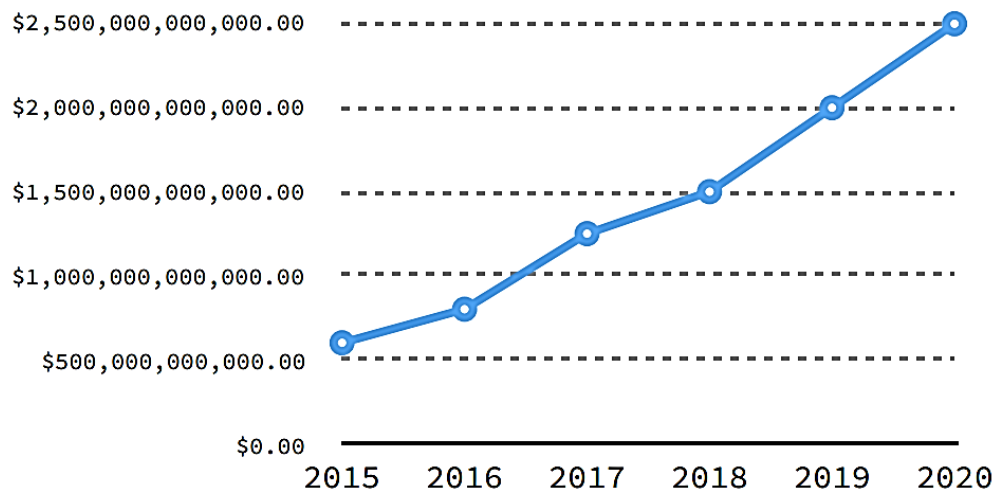
 BLOCKSTACK	Application Layer (HTTP, DNS, PKI)
	Transport Layer (TCP, UDP)
	Network Layer (IP)
	Link Layer (Ethernet, WLAN)
Already Decentralized	



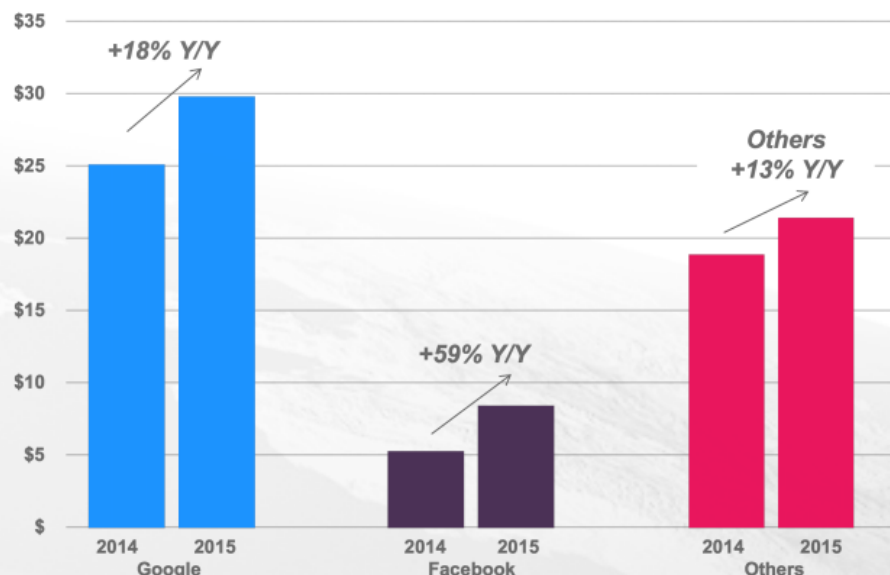
اینترنت فعلی	اینترنت BLOCKSTACK
ریسک حملات DDoS به سرورهای DNS و Phishing	عملیات DNS توسط بلاکچین مدیریت می‌شود. (کاهش حملات DDoS)
مشخص بودن آدرس منابع مورد استفاده وبسایت‌ها (طعمه هکرها)	مشخص نبودن آدرس منابع مورد استفاده وبسایت‌ها (قابل استنتاج توسط بلاکچین)
ذخیره اطلاعات کاربران به صورت خام	ذخیره اطلاعات کاربران به صورت رمزگذاری شده (دسترسی تنها در اختیار کاربر)
مالکیت و نظارت سرورهای مرکزی سایت‌ها بر روی اطلاعات کاربران به خطر افتادن حریم خصوصی	مالکیت و نظارت کاربران بر روی اطلاعات خود و حفظ حریم خصوصی



هزینه خسارت مالی ناشی از حملات سایبری در سال های مختلف

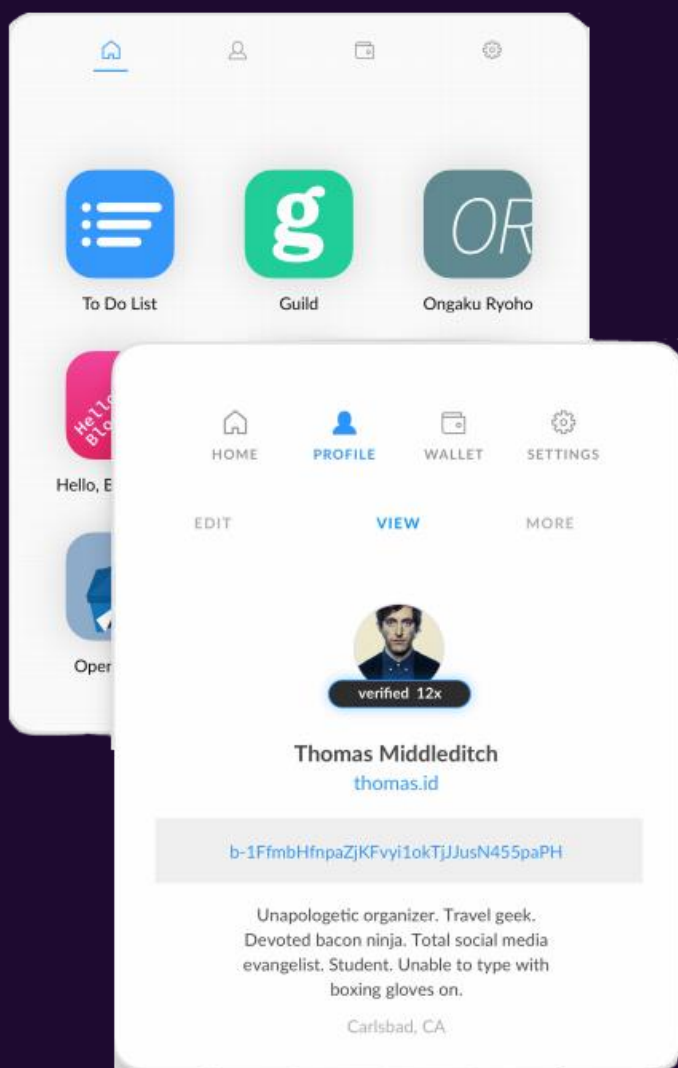


درآمدی که شرکت های بزرگ اینترنتی از تبلیغات هدفمند بر اساس داده های شخصی کاربران به دست می آورند
بر حسب میلیارد دلار





معرفی اجمالی پروژه از دید کاربری



برای استفاده از تمامی برنامه های غیرمتمرکز توسعه داده شده توسط بستر Blockstack ابتدا می بایست مرورگر آن را دانلود و نصب نمایید.

سپس باید یک اکانت جدید برای آن بسازید. با ساخت اکانت، به شما یک Blockstack ID تعلق می گیرد که مانند کلید خصوصی در رمز ارزها، هویت اصلی شما در اکوسیستم برنامه های غیرمتمرکز بر بستر Blockstack می باشد و دسترسی شما به فایل های شخصی تان در این اینترنت و فضای ابری با این ID تعیین می شود.

همچنین با نصب این مرورگر، بسته های نرم افزاری Keychain نیز بر روی سیستم شما نصب می گردد. وظیفه اصلی سیستم Keychain رمزگذاری کردن فایل های شخصی شما قبل از آپلود و فرستادن آن در اینترنت است. فایل هایی که به صورت رمزگذاری شده در فضای ابری ذخیره شده و شما می توانید با Blockstack ID و کلید خصوصی خود و از طریق Virchualchain بر بستر بلاکچین Blockstack به آنها دسترسی داشته باشید.



مروری بر مشکلات فعلی اینترنت

اینترنت در آغاز پیدایش خود در دهه ۱۹۹۰ با هدف متصل کردن کامپیوترها در سراسر دنیا ماهیتی غیرمتمرکز را در پیش گرفت. با گذر زمان و رشد فزاینده تعدادی از شرکت‌های خدمات دهنده نظیر مایکروسافت، گوگل، آمازون، فیسبوک و ... و ایجاد بسترهای ذخیره سازی ارزان و با حجم زیاد سهم بالایی را از این بازار تصاحب کردند و به این ترتیب ذخیره سازی بخش زیادی از اطلاعات در حال گردش روی اینترنت شکل متمرکز به خود گرفت.

هر چندی که این تمرکز لزوماً به معنای مالکیت و دست درازی به اطلاعات افراد نیست و این شرکت‌ها هریک سیاست گذاری هایی برای صیانت از اطلاعات افراد به کار می‌گیرند. به عنوان مثال شرکت گوگل در این [لینک](#) توضیح داده که امنیت داده های کاربران را چگونه مدیریت می‌کند.

اما با شروع بحث Big Data و آنالیز داده ها و استخراج آمار و اطلاعات ارزشمند از این داده ها توسط شرکت های مذکور و فروش این تحلیل های آماری به دیگر شرکت ها، مخالفت و بحث های زیادی را در جامعه کاربران ایجاد نمود که کماکان نیز ادامه دارد.

بحث امنیت و سرقت اطلاعات کاربران از جمله اطلاعات مالی آنها از طریق نفوذ و هک سایت ها و حملات سایبری نیز نگرانی عمیقی در جامعه کاربران ایجاد نموده است.

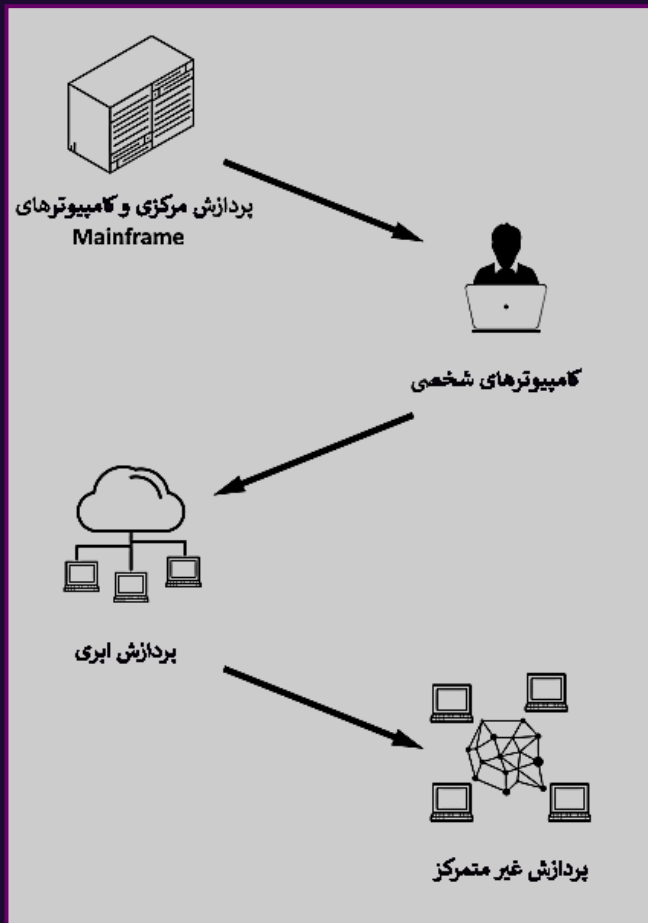
موضوع مورد اهمیت دیگر ردیابی فعالیت های کاربران در هنگام گشت و گذار وب و فروش این اطلاعات به بنگاه های تبلیغاتی بوده که باعث هجوم سیل عظیمی از تبلیغات مربوط و نامربوط به کاربران می شود.

همچنین یکی از بزرگ ترین کلاه برداری های شایع اینترنتی، هک سرورهای DNS (سرورهای که تبدیل دامنه سایت ها به IP و آدرس واقعی آنها در شبکه را انجام می‌دهند) است که بجای برگرداندن آدرسی واقعی، کاربران به آدرس های اشتباهی هدایت کرده اطلاعات وارد شده توسط کاربر را به سرقت می‌برند که موسوم به حملات Phishing هستند.



Blockstack و تغییراتی بنیادی در نحوه عملکرد شبکه اینترنت

سیر تکاملی پردازش در کامپیوترها



در اینجا هم اگر کلیدهای خود را گم کنید با اینکه اطلاعات شما به صورت رمزگذاری شده در فضای ابری ذخیره شده اند و اطلاعات مالکیت آنها در فضای بلاکچین ثبت شده است ولی شما مالکیت آنها را از دست می دهید.

دسترسی به اطلاعات تنها با این کلیدها امکان پذیر بوده و به همین دلیل اطلاعات کاربران تنها توسط خودشان قابل استفاده است.

پروژه Blockstack با تغییر در نحوه ارتباط بین لایه های مختلف شبکه اینترنت و معرفی زیرساخت های ارتباطی جدید بر بستر بلاکچین، قصد دارد مشکلات شبکه فعلی اینترنت از حیث امنیت و حریم خصوصی را حل کرده و علاوه بر آن تجربه ای کاملاً غیر متمرکز از اینترنت را در اختیار کاربران خود قرار دهد.

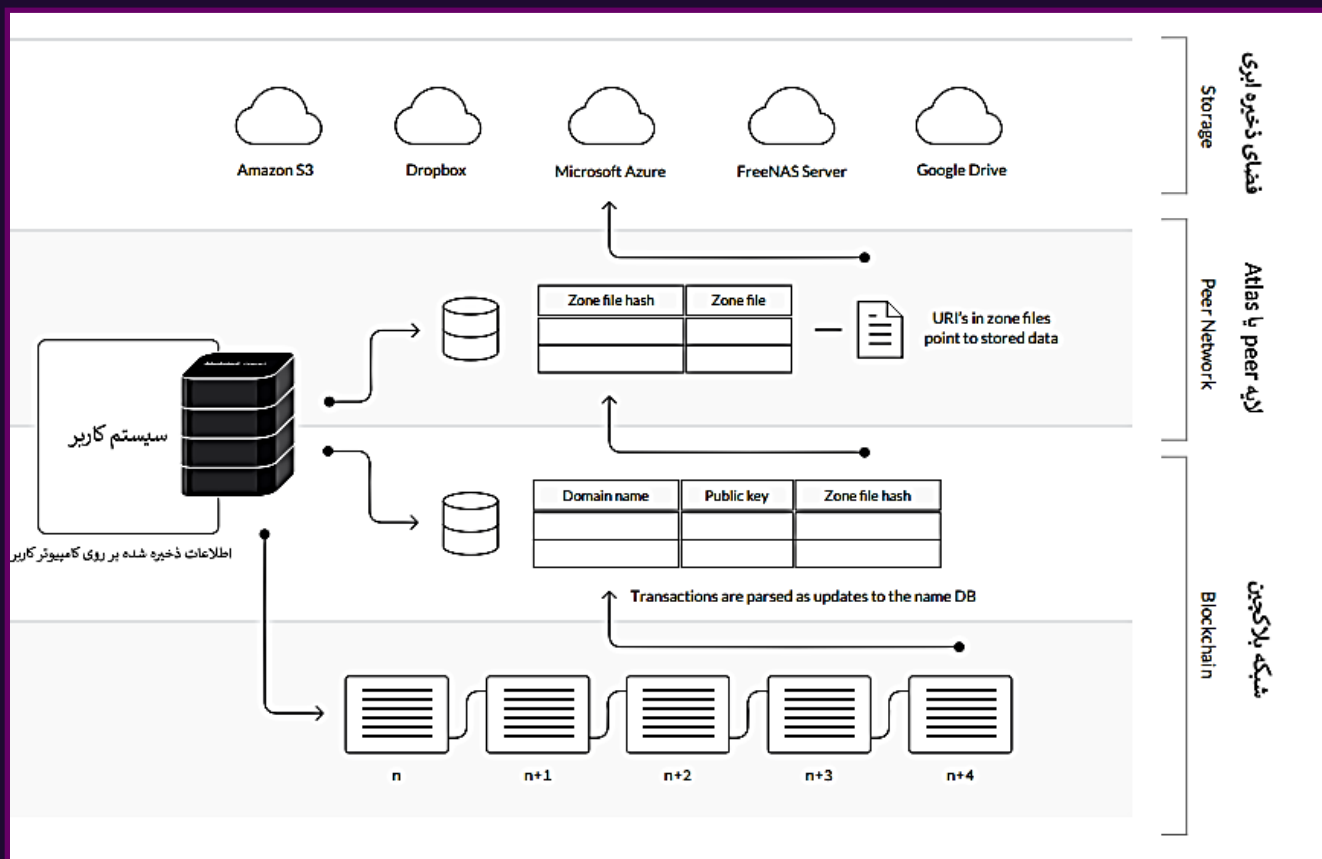
در اینترنت Blockstack تمام اطلاعات مربوط به کاربر، اعم از هویت و داده های خام (فایل ها) ابتدا در سیستم خود کاربر ذخیره و رمزگذاری می شود و سپس در سرورهای ابری موجود در اینترنت به صورت غیر متمرکز و رمزگذاری شده ذخیره می شود.

سپس گره های شبکه بلاکچین Blockstack به نام Virtualchain با استفاده از کلیدهایی که در ازای اطلاعات در اختیار کاربران قرار می گیرد، اطلاعات ذخیره شده و رمزگذاری شده در اینترنت را تعیین مالکیت کرده و پس از رمزگشایی محتوای آنها را مشاهده می کنند. عملیات لینک کردن دیتای ذخیره شده در فضای ابری و نسبت دادن آن به کاربران بدون نیاز به هیچ سرور خاص و کاملاً توسط بلاکچین و به طور غیر متمرکز انجام می شود.

همچنین تمام کلیدهای تولید شده مانند تمام رمزارزها تنها در اختیار شما قرار دارند و در جای دیگری ذخیره نمی شوند و همانطور که برای مثال اگر در آنجا کلید خصوصی (Private key) کیف پول بیتکوین خود را گم کنید، بیتکوین های خود را از دست می دهید.



ساختار شبکه Blockstack



شبکه Blockstack سیستمی متن باز و متشکل از سه لایه است که در شکل بالا نشان داده شده است. این سه لایه عبارتند از:

- ✓ لایه بلاکچین که با تکنولوژی منحصر به فرد Virtualchain، پایین ترین لایه است و دو وظیفه مهم بر عهده دارد: یکی مهیا کردن بستر ذخیره سازی اطلاعات برای عملیات مختلف و دیگری ایجاد اجماع بر روی اینکه ترتیب زمانی عملیات نوشتن چگونه انجام شود.
- ✓ لایه میانی به نام (Peer یا شبکه Atlas) که در آن عملیات اکتشاف (discovery) انجام میشود. به عبارت دیگر از طریق zone file ها عملیات مسیر یابی انجام میشود. دقیقاً شبیه کاری که در DNS Zone ها انجام میشود.
- ✓ لایه بالایی به نام Gaia که در اصل یک سیستم ذخیره فایل ها و داده ها به صورت ابری و غیر متمرکز بوده و قابلیت ذخیره بازیابی اطلاعات رمزگذاری شده و پخش شده بین چند سرویس ذخیره فایل ابری را در خود دارد



عملکرد Blockstack و چگونگی ارتباط لایه ها با هم

دلیل این تصمیم ماهیت رفتاری شبکه های بلاکچین و لزوم همگام بودن اطلاعات تمام گره های شبکه در تمام لحظات است. شبکه های بلاکچین در گذر زمان و به خودی خود شدیداً حجیم می شوند و هر گره در هر لحظه باید با اطلاعات شبکه تا به آن لحظه همگام شده باشد.

حال اگر فایل های حجیم در خود شبکه آپلود شوند، هر گره باید تریلیون ها بایت را ذخیره و همگام سازی کند که عملاً غیر ممکن به نظر می رسد. مسیریابی فایل ها در این لایه نیز تماماً با عملیات رمزگذاری و Hash ها انجام می شود و آدرس و اطلاعات بسیاری از فایل های شخصی تنها با داشتن کلید خصوصی کاربر قابل مشاهده است.

لایه سوم یا Gaia (بالاترین لایه در شکل بالا) لایه Storage نامگذاری می شود و همانطور که گفته شد این لایه در واقع همان سرویس های ذخیره فایل ابری متداول مانند آمازون، گوگل و ... بوده و فایل ها و محتوای آپلود شده در فضای هاست وبسایت های مختلف در این لایه قرار دارد.

نکته جالب اینجاست که با وجود ذخیره این فایل ها در فضاهای ابری متداول، در این سیستم امکان ذخیره سازی این اطلاعات به صورت غیرمتمرکز (پخش کردن محتوای یک فایل در چندین مسیر مختلف) وجود دارد.

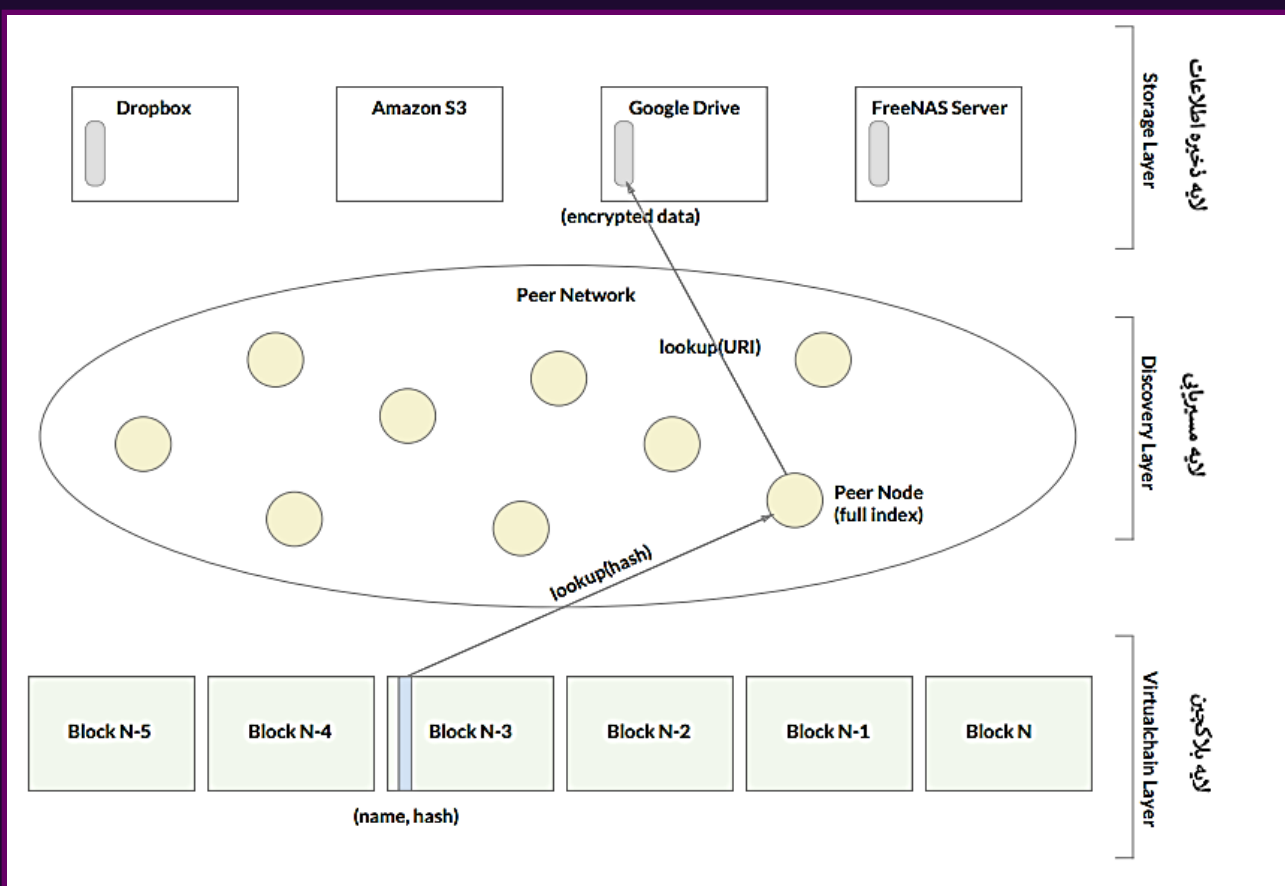
لایه پایینی بلاکچین، همانطور که از نام آن مشخص است، وظیفه اصلی انجام عملیات بلاکچینی از جمله بررسی صحت و سقم رمزگذاری ها و عملیات مسیریابی DNS را با استفاده از فناوری Virtualchain برعهده دارد. مسیریابی اطلاعات عمومی سایت ها با استفاده از Public Key ها در این لایه انجام می شود.

به طور مثال تبدیل نام دامنه سایت ها به آدرس متناظر دریافت محتوای آنها (عملیات DNS) در این لایه انجام می شود. همچنین عملیات فهرست سازی فایل های مورد نیاز یک دامنه با استفاده از نام دامنه و کلیدهای عمومی نیز در این لایه انجام شده و برای هر کدام از فایل ها یک Zone file hash نیز تولید می شود.

لایه بالاتر لایه Peer یا شبکه Atlas نام گذاری شده است. وظیفه اصلی این لایه، مسیریابی فایل های رمزگذاری شده و ذخیره شده در فضای ابری (Google Drive, Amazon, Dropbox , ...) و برقراری ارتباط بین دامنه، محتوای فایل و کاربر درخواست کننده آن می باشد. به بیان دیگر، این سیستم ذخیره سازی فایل ها و محتوای وبسایت را کاملاً خارج از شبکه بلاکچین خود در نظر گرفته و تنها آدرس دسترسی به آنها را در لایه peer محاسبه کرده و کاربران را به آنها لینک می کند.

علاوه بر آن محتوای فایل‌ها ابتدا در کامپیوتر خود فرد آپلود کننده رمزگذاری می‌شود و کلیدهای عمومی و خصوصی دسترسی به آن نیز تنها در اختیار خود فرد قرار می‌گیرد و بدین ترتیب تنها کاربر آپلود کننده می‌تواند محتوای فایل‌های شخصی خود را مشاهده کند. همچنین آدرس دسترسی به این فایل‌ها (URI) نیز توسط Zone file hash ها در لایه peer که خود پیش‌تر در لایه بلاکچین مشخص شده‌اند، محاسبه می‌شود. این موضوع باعث می‌شود که نه سرویس‌های ذخیره فایل مانند Google, Amazon بدون اجازه کاربران به محتوای فایل‌های رمزگذاری شده دسترسی داشته باشند و نه هکرها بتوانند مستقیماً مسیر فایل‌ها و منابع استفاده شده در یک وبسایت را ردگیری کنند.

مراحل دسترسی و مسیریابی یک فایل رمزگذاری شده در یک فضای ابری





مزایای ذخیره فایل ها به روش Gaia در حفظ حریم خصوصی و مالکیت اطلاعات

دسترسی و مشاهده اطلاعات این فایل ها تنها توسط کلیدهایی که در اختیار خود کاربر قرار دارد امکان پذیر بوده و صحت دسترسی به فایل ها و مسیریابی به آنها نیز توسط شبکه بلاکچین و لایه peer انجام می شود، به همین دلیل سرویس های ذخیره فایل، هیچ دسترسی به محتوای فایل های ذخیره شده در خود ندارند.

مثال: دسترسی به بک سابت و فایل های شخصی مرتبط با حساب کاربر

در آن سابت در Blockstack

کاربری دامنه Coiniran.io را در مرورگر خود وارد می کند

۱. ابتدا نام این دامنه در شبکه بلاکچین *Virtualchain* بررسی شده و *hash* های مربوط به آن یافت شده و فهرست فایل های مورد نیاز آن لیست می شود.

۲. با استفاده از *hash* های یافت شده در بلاکچین برای آن دامنه، *zonefile* ها و مسیرهای رسیدن به فایل ها (*URI*) در لایه *peer* یا شبکه *Atlas* محاسبه می شود.

۳. با استفاده از *URI* های تولید شده توسط *zonefile* ها در لایه *peer*، فایل ها از فضای ذخیره سازی ابری *Gaia* دانلود می شوند.

۴. محتوای فایل ها با توجه به دسترسی کاربران و کلیدهای خصوصی و عمومی آنها (که توسط بلاکچین تایید شده است) رمزگشایی شده و مشاهده می شود.

سیستم *Blockstack* در حال حاضر عرضه نهایی شده و بیش از ۷۴۰۰۰ دامنه نیز در آن ثبت شده است و به دلیل متن باز بودن توسط بسیاری از شرکت ها و توسعه دهندگان در حال بروزرسانی مداوم می باشد.

در اینترنتی که امروزه به طور روزمره استفاده می کنیم، اطلاعات کاربران بعد از ورود به یک سایت بزرگ مانند Facebook به صورت متمرکز در سرورهای آنها ذخیره می شود و در هنگام گشت و گذار در آنها، کامپیوتر کاربر تنها نقش یک صفحه نمایش و دریافت کننده اطلاعات را به خود می گیرد. این موضوع کاملاً با ماهیت غیرمتمرکز اینترنت در تضاد است.

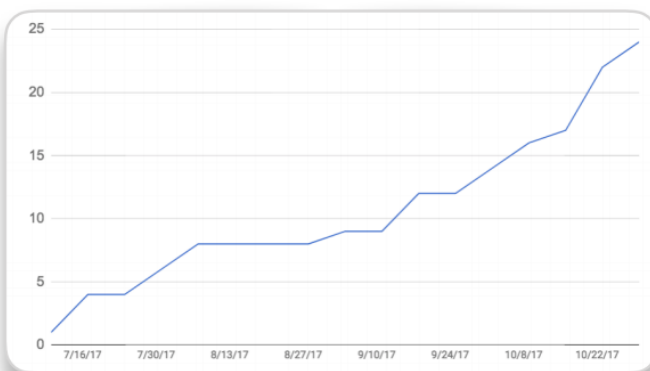
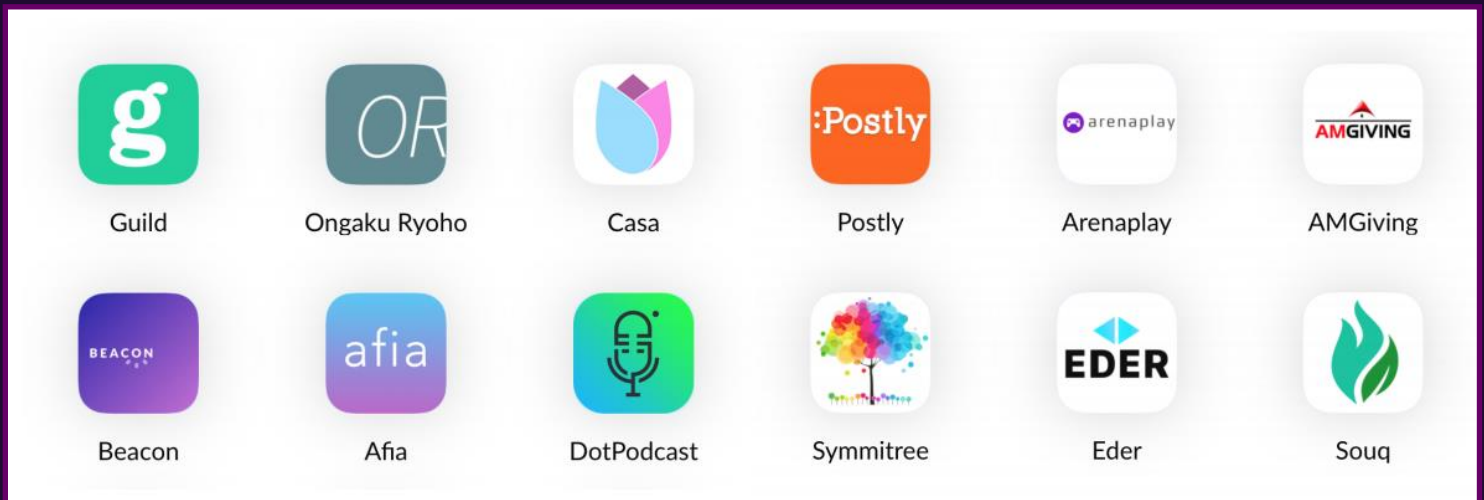
بزرگ ترین تفاوت و مزیت استفاده از سیستم ذخیره سازی *Gaia* در *Blockstack*، ذخیره اطلاعات و وبسایت های بزرگ (مانند Facebook، Instagram و) نه در سرورهای خود این سایت ها، بلکه در فضای ابری انتخاب شده توسط خود کاربر (*Dropbox*، *Google Drive* و) است. آن هم به صورت رمزگذاری شده است.

به بیان ساده تر، بعد از ورود به یک سایت تمام اطلاعات کاربری، اعم از اطلاعات هویتی، موضوعات مورد علاقه، گزارش صفحات مشاهده شده و جستجوهای انجام شده توسط کاربر و ریز فعالیت های وی، به جای ذخیره شدن در سرورهای مرکزی سایت، در قالب فایل هایی به کامپیوتر خود کاربر فرستاده شده، در همانجا رمزگذاری شده و کلیدهای خصوصی و عمومی آنها نیز در اختیار خود کاربر قرار می گیرد. سپس این سایت ها در فضای ابری مشخص شده توسط خود کاربر (*Google Drive*، *Dropbox* و) آپلود می شوند.

همین موضوع باعث می شود اطلاعات کاربر عملاً در اختیار خود وی باشد تا آن سایت. سرویس های ذخیره فایل به صورت ابری (مانند *Dropbox*، *Google Drive* و ...) نیز به دلیل رمزگذاری شدن فایل ها به محتوای آنها دسترسی ندارند و تنها وظیفه نگهداری آنها را بر عهده دارند.

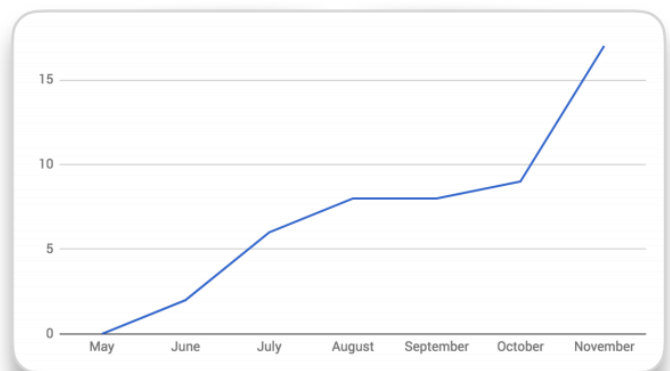


نمونه ای از برنامه های تولید شده بر بستر Blockstack



تعداد تیم های برنامه نویسی در حال توسعه برنامه های تحت

Blockstack



تعداد برنامه های ثبت شده در مرورگر Blockstack

12,977
عضو

27
همایش



BLOCKSTACK