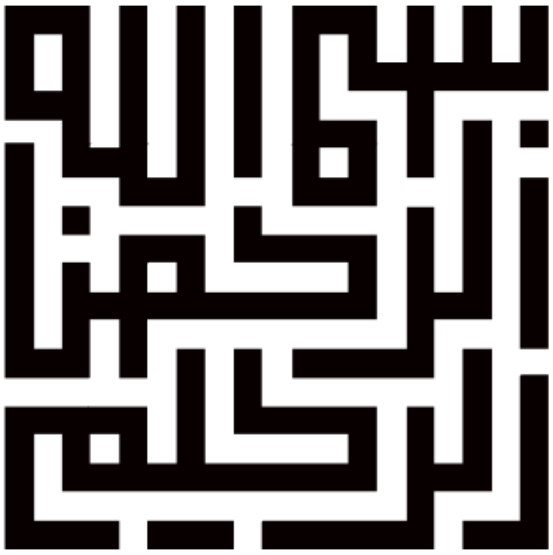
بنام خدا

بررسی معماری پیام‌رسان‌های اجتماعی مبتنی فناوری زنجیره بلوکی با تمرکز بر روی خصیصه‌های کیفی امنیت و حریم خصوصی

مرکز ماهر

تابستان ۹۷



«وَإِذْ قَالَ إِبْرَاهِيمُ رَبِّ اجْعَلْ هَـٰذَا الْبَـلَدَ آمِنًا»

و هنگامی که ابراهیم گفت: «پروردگارا این شهر را شهری امن قرار ده»

(سوره ابراهیم، آیه ۳۵)

فهرست مطالب

فصل ۱ مقدمه

بانک‌های اطلاعاتی به طور معمول توسط یک سازمان نگهداری و کنترل می‌شوند. در نتیجه امکان مداخله و یا سانسور اطلاعات توسط این سازمان وجود دارد و بانک اطلاعاتی در برابر دستکاری و تغییرات خرابکارانه داده‌ها آسیب پذیر است. یک راه برای اینکه مطمئن شویم که یک موجودیت بانک اطلاعاتی را دستکاری نکرده است این است که بانک اطلاعاتی، عمومی باشد و هر کس بتواند یک نسخه از ان را برای خود نگهداری کند. در نتیجه هر کس برای اینکه بفهمد نسخه کپی او دست نخورده و سالم است، می‌تواند آنرا با نسخه دیگران مقایسه کند. این شیوه تا زمانی که داده‌ها استاتیک باشد مناسب است اما اگر امکان تغییر و افزوده شدن اطلاعات جدید وجود داشته باشد، مشکل سازگاری نسخه‌های توزیع شده پیش می‌آید. در نتیجه موجودیت‌هایی که یک نسخه کپی از بانک اطلاعاتی را در اختیار دارند باید تصمیم بگیرند که چه تغییراتی مجاز است و این تغییرات به چه ترتیبی باید اعمال شوند. فناوری زنجیره بلوکی[1] این مشکل را با ایجاد شبکه از کامپیوترها (گره‌ها) که هر یک یک کپی از بانک اطلاعاتی را در اختیار دارد و همچنین مجموعه قوانینی که مشخص‌کننده ترتیب اعمال تغییرات جدید است بر طرف می‌کند.

این فناوری، ابتدا برای ایجاد ارز دیجیتالی بیت‌کوین[2] مورد استفاده قرار گرفت اما به تدریج سایر کاربردهای بالقوه این فناوری آشکار گردید. دون و الکس تپسکات در کتاب انقلاب زنجیره بلوکی می‌نویسند: «زنجیره بلوکی یک دفتر کل دیجیتالی غیر قابل فسخ و غیر قابل دستکاری که می‌توان آنرا به گونه‌ای برنامه‌ریزی کرد که نه تنها تراکنش‌های مالی، بلکه هر موجودیت مجازی واجد ارزشی را ثبت کند[3]». این دفتر کل توزیع شده[4] امکان کد کردن یک قرارداد ساده تحت عنوان قرارداد هوشمند[5] را فراهم می‌کند که با برقرار شدن یک سری شرایط، می‌تواند اجرا شود. در همین راستا، اتریوم[6]، که یک پروژه متن باز مبتنی بر زنجیره بلوکی است، تلاش می‌کند تا این قابلیت را فراهم کند. با کمک این فناوری، امکان پرداخت نظیر به نظیر و تعامل مستقیم بین طرفین درگیر و به اشتراک‌گذاری غیر متمرکز منافع اقتصادی آن فراهم می‌گردد. توانایی اعتبارسنجی هویت، یکی از دغدغه‌های مهم در تراکنش‌های مالی آنلاین است و دفاتر کل توزیع شده، شیوه‌ای ارتقاء یافته برای اثبات هویت فرد و همچنین دیجیتالی کردن اسناد شخصی است. برچسب زمانی و مکانی مبتنی بر زنجیره بلوکی امکان تصدیق اطلاعات مرتبط با کالاهای تولید شده توسط شرکت‌ها را برای مصرف کنندگان فراهم می‌کند.

از آنجایی که همه چیز شفاف و در معرض و در دسترس عموم قرار دارد امکان برگزاری انتخابات و یا رای‌گیری به صورت شفاف وجود دارد و قراردادهای هوشمند مبتنی بر اتریوم می‌تواند به خودکار کردن این فرایند کمک کند. ارزیابی و تخمین احتمال وقوع یک رویداد بر اساس نظرات و ایده گروه وسیعی از مردم معمولا از درجه بالایی از صحت برخوارد است و برایند نظرات، باعث خنثی شدن اثرات پیشداوری بر روی نتیجه نهایی می‌شود. بر همین اساس کاربردهای متکی بر خرد جمعی می‌تواند از قابلیت‌های زنجیره بلوکی بهره گیرد.

اطلاعات دیجیتالی می‌تواند به شکل نامحدودی بازتولید و در شکل گسترده‌ای از طریق اینترنت پخش شود. در نتیجه کاربران از محتوای رایگان استفاده می‌کنند بدون اینکه صاحبان آن اثر بتوانند از منافع آن بهره‌مند شوند. با کمک زنجیره بلوکی و

---

[1] Blockchain
[2] Bitcoin
[3] Don & Alex Tapscott
[4] Distributed Ledger
[5] Smart Contract
[6] Ethereum

قراردادهای هوشمند، از حقوق مالکیت معنوی به شکل اتوماتیک محافظت می‌شود و در نتیجه ریسک کپی و توزیع اثر از بین می‌رود. امکان ذخیره‌سازی غیر متمرکز فایل در این بستر مزایای آشکاری با خود به دنبال دارد. توزیع داده‌ها در سراسر شبکه از فایل‌ها در برابرگم شدن یا هک شدن محافظت می‌کند. با کمک IPFS[7]، امکان تجسم نحوه عملکرد وب توزیع شده به راحتی میسر است. IPFS، مشابه شیوه جابجایی فایل در BitTorrent، نیازی به ارتباط متمرکز مشتری-خدمتگزار ندارد و اینترنت می‌تواند از وب سایت‌های کاملا غیر متمرکز تشکیل شود که به طور بالقوه جابجایی فایل را سرعت می‌بخشد.

یکی دیگر از کارکردهایی که می‌توان بر بستر زنجیره بلوکی ارائه شود نرم‌افزارهای ارتباطی توزیع شده و غیر متمرکز است. در این مقاله تلاش می‌کنیم برخی از نرم‌افزارها و پروتکل‌های ارتباطی که مبتنی بر فناوری زنجیره بلوکی هستند را معرفی کنیم. به همین منظور ابتدا مفهوم زنجیره بلوکی و ویژگی‌های آنرا شرح می‌دهیم. سپس به معرفی دو نرم افزار پیام‌رسان به نام‌های KeyBase و Status که بستر ارتباطی انها مرتبط با زنجیره بلوکی است می‌پردازیم و در پایان یک پروتکل ارتباطی موسوم به پروتکل مرکوری[8] می‌پردازیم که مبتنی بر زنجیره بلوکی اتریوم است و امکان پیاده سازی فرم‌های مختلف ارتباطی را فراهم می‌کند.

---

[7] Inter Planetary File System

[8] Mercury Protocol

فصل ۲ فناوری زنجیره بلوکی

زنجیره بلوکی یک دفترکل توزیع شده است که امکان ثبت تراکنش‌ها بین طرفین را به شیوه‌ای موثر، قابل تصدیق و دائمی فراهم می‌کند. این دفتر کل می‌تواند به شیوه‌ای برنامه ریزی شود که تراکنش‌ها به شکل اتوماتیک، فعال گردند. با کمک زنجیره بلوکی می‌توان دنیا را در قالب قراردادهای تصور کرد که در آن هر فرایند دارای یک رکورد دیجیتالی و یک امضاء است که با کمک آن شناسایی، اعتبارسنجی، ذخیره و به اشتراک گذاشته می‌شود در حالیکه در برابر حذف، تغییر، دستکاری و یا بازبینی مجدد محافظت می‌شوند و درنتیجه نیازی به عوامل واسطه و کارگزاری نیست. پنج اصل زیر بنایی این فناوری عبارت است از :

۱. هر یک از طرف‌ها در زنجیره بلوکی به کل بانک اطلاعاتی و تاریخچه کامل آن دسترسی دارد و هیچ فردی نمی‌تواند داده‌ها یا اطلاعات را تحت کنترل خود داشته باشد. هر یک از طرف‌ها می‌تواند رکوردهای مربوط به شرکای خود را به شکل مستقیم و بدون نیاز به یک واسطه، اعتبار سنجی و تصدیق کند.
۲. تعاملات و ارتباطات به شکل مستقیم بین گره‌های نظیر به نظیر صورت می‌گیرد و هر یک از گره‌ها اطلاعات را ذخیره و آنرا برای سایر گره‌ها ارسال می‌کند.
۳. هر تراکنش و ارزش و مقدار منتسب به آن، برای همه کسانی که به سیستم دسترسی دارند، آشکار است. هر کاربر زنجیره بلوکی آدرس یکتایی دارد که متشکل از کاراکترها و اعداد است که با کمک آن شناسایی می‌شود. در مواجه با دیگران، کاربر می‌تواند ناشناس باقی بماند و یا هویت خود را به دیگران اثبات کند. تراکنش‌ها بین آدرس‌های زنجیره بلوکی صورت می‌گیرد.
۴. هنگامی که تراکنش وارد بانک اطلاعاتی شد و حساب‌ها به روز شد، رکوردها دیگر تغییر نمی‌کنند زیرا آنها به همه تراکنش‌های قبل از خود لینک شده‌اند. الگوریتم‌های محاسباتی و رویکردهای مختلفی به کار گرفته می‌شوند تا نسبت به دائمی بودن اطلاعات و مرتب بودن آنها بر اساس زمان وقوع و دسترسی همگانی به آنها، اطمینان حاصل شود.
۵. طبیعت دیجیتالی دفترکل این امکان را فراهم می‌کند تا تراکنش‌های زنجیره بلوکی با منطق محاسباتی پیوند خورده و قابل برنامه ریزی باشد. در نتیجه کاربران می‌توانند الگوریتم‌ها و قواعدی را تعریف کنند که به شکل اتوماتیک منجر به فعال شدن تراکنش‌ها بین گره‌ها شود.

برای درک اولیه زنجیره بلوکی، می‌توان یک صفحه گسترده[9] را تصور کرد که هزاران نسخه از آن در شبکه‌ای از کامپیوترها کپی و پخش شده است و امکان به‌روز رسانی مدوام آن نیز وجود دارد. در واقع با یک بانک اطلاعاتی اشتراکی توزیع شده مواجه هستیم که در یک مکان ذخیره نشده است بلکه رکوردهای اطلاعاتی آن به شکل عمومی در دسترس و قابل ارزیابی و اعتبارسنجی است و هیچ نسخه متمرکزی از این اطلاعات وجود ندارد تا در معرض آسیب‌پذیری توسط هکرها قرار گیرد بلکه این اطلاعات به طور همزمان بر روی میلیون‌ها کامپیوتر میزبانی شده است و اطلاعات آن در اختیار هر کسی که به اینترنت دسترسی دارد می‌باشد. بنابراین زنجیره بلوکی فاقد یک نقطه شکست[10] است به نحوی که در آن با مساله گم شدن تراکنش‌ها مواجه نیستیم و امکان انجام تبادل بدون رضایت یکی از طرفین وجود ندارد و اعتبار تراکنش‌ها را در بالاترین سطح تضمین می‌کند.

شبکه‌ای از گره‌های محاسباتی به همراه مجموعه قوانینی که مشخص کننده ترتیب اعمال تغییرات جدید است، زنجیره بلوکی را تشکیل می‌دهند. این شبکه مبتنی بر اجماع و توافق است در نتیجه همه گره‌ها در هر لحظه روی حالت بانک اطلاعاتی توافق

---

[9] Spreadsheet
[10] Single point of failure

دارند و هیچ یک از آنها قدرت دست بردن و یا سانسور اطلاعات را ندارد. با حفظ دنباله حسابرسی همه تغییرات رخ داده، این امکان برای همگان فراهم می‌شود تا بررسی کنند آیا بانک اطلاعاتی درست و صحیح است یا نه. این دنباله حسابرسی، تشکیل شده است از تک تک تغییرات اعمال شده که اصطلاحا به آن تراکنش می‌گویند. مجموعه‌ای از تراکنش‌هایی که توسط یک گره اضافه شده است تشکیل یک بلوک را می‌دهند.

زنجیره بلوکی ترتیب اعمال تراکنش‌ها را مشخص می‌کند و ترتیب بلوک‌ها نیز در آن مشخص است و در آن هر بلوک یک ارجاع به بلوک پیش از خود دارد. در نتیجه، زنجیره‌ای از بلوک‌ها شکل می‌گیرد که هر یک از آنها، به بلوک قبل از خود اشاره می‌کنند.

۲ ۱ ویژگی‌های امنیتی زنجیره بلوکی

این شبکه به شکل غیر متمرکز و بر مبنای نظیر به نظیر عمل می‌کند. ذخیره شدن داده‌ها در کل شبکه ریسک نگهداری متمرکز داده‌ها را از بین می‌برد و در نتیجه نقطه آسیب‌پذیری متمرکزی که بتواند مورد سوء استفاده هکرها قرار گیرد وجود ندارد. رویکرد امنیتی آن مبتنی بر رمزنگاری است و مفهوم کلید عمومی و کلید خصوصی است. کلید عمومی در حکم آدرس فرد در زنجیره بلوکی است و کلید خصوصی نقش رمز عبور را ایفا می‌کند که اجازه دسترسی فرد به دارایی‌های دیجیتالی خود را فراهم می‌کند. وقتی یک گره جدید به این شبکه می‌پیوندد، کار خود را با یک بانک اطلاعاتی خالی آغاز می‌کند و سپس با دانلود کردن همه بلوک‌ها و اعمال تراکنش‌های موجود در آن، بانک اطلاعاتی را در همان حالتی خواهد یافت که سایر گره‌ها آنر می‌بینند. هر گره، یک مدیر برای زنجیره بلوکی است که داوطلبانه به شبکه می‌پیوندد با این وجود عوامل انگیزشی برای مشارکت گره‌ها در این شبکه وجود دارد.

به زنجیره بلوکی تشکیل شده می‌توان در قالب یک کل[11]، نگاه کرد که اجزاء آن قابل دستکاری و تغییر نیستند و در صورت تغییر، نیازمند حجم عظیمی از توان محاسباتی برای بازنشانی اطلاعات کل این شبکه هستیم. این مساله اگرچه از منظر تئوری امکان‌پذیر است، اما در عمل امکان وقوع آن وجود ندارد زیرا همانطور که پیشتر گفته شد، این شبکه مبتنی بر اجماع است و یکی از مهمترین جنبه‌های پروتکل اجماع، قواعدی است که مشخص می‌کند، بلوک‌ها چگونه و چه زمانی به زنجیره اضافه می‌شوند. درنتیجه همگان روی حالت بانک اطلاعاتی توافق دارند و سیر زمانی و ترتیب وقوع رویدادها غیر قابل تغییر است. در حال حاضر دو پروتکل اصلی برای اجماع موسوم به اثبات کاری (PoW[12]) و اثبات سهامی (PoS[13]) وجود دارد.

PoW پروتکلی است که در بیت‌کوین و اتریوم به کار گرفته شده است و مانند پازلی است که حل آن دشوار است اما اگر حل شود، اعتبار سنجی درست بودن راه حل، به سادگی امکان پذیر است. در این پروتکل، به تلاش‌های لازم جهت حل این پازل، کار[14] می‌گویند و به راه حل آن، اثبات کاری می‌گویند. خط سیر زمانی رویدادها در آن را می‌توان امن در نظر گرفت زیرا اگر تاریخچه وقایع بازنویسی شود، راه حل به دست آمده برای همه بلوک‌های بعدی نادرست و نامعتبر می‌شود. در نتیجه برای اینکه سایر گره‌ها را متقاعد کنیم که زنجیره تغییریافته یک زنجیره صحیح است، باید همه کارهای بعد از این تغییر را مجدد انجام شود. به عبارت دیگر یک گره باید بتواند این کارها را سریعتر از همه گره‌های دیگر انجام دهد که به آن اصطلاحا حمله اکثریت[15]

---

[11] As a Whole
[12] Proof of Work (PoW)
[13] Proof of Stake (PoS)
[14] Work
[15] Majority Attack

یا حمله ۵۱ درصد[16] می‌گویند و معنای آن این است که یک گره باید حداقل ۵۱ درصد از توان محاسباتی همه گره‌ها برای انجام کار و یافتن اثبات کاری را داشته باشد. اگر چنین مساله‌ای بتواند رخ دهد در آن صورت یک گره خواهد توانست ترتیب وقوع تراکنش‌ها را عوض کند و یا تراکنشی که انجام داده است را تغییر دهد.

این پروتکل، ممکن است راه‌حل‌های متمرکز را ترویج کند زیرا هزینه توان محاسباتی کاهش خواهد یافت اما PoS پروتکل اجماع جدیدتری نسبت به PoW است که نیاز به انرژی کمتری دارد و ایجاد شبکه‌ای غیر متمرکز از گره‌ها را ترغیب می‌کند. در واقع تولید بلوک‌ها در زنجیره بلوکی از طریق سهام[17] کنترل می‌شود نه از طریق توان محاسباتی و دارندگان سهام تلاش می‌کنند از شبکه محافظت کنند. اگرحمله اکثریت بخواهد رخ دهد، فرد باید ۵۱ درصد از سهام شبکه را بخرد که بسیار گران تمام خواهد شد و باوقوع حمله، ارزش سهام ویران خواهد شد.

[16] 51% Attack
[17] Stak

فصل ۳ پیام‌رسان KeyBase

KeyBase یک دایرکتوری کلید[18] است که میان هویت افراد در شبکه‌های اجتماعی و کلیدهای رمزنگاری، نگاشت و ارتباط برقرار می‌کند و این امکان را به کاربران خود می‌دهد تا هویت خود را از طریق لینک بین هویت‌های آنلاین نظیر توئیتر و کلیدهای رمزنگاری تعریف شده در KeyBase اثبات کنند. علاوه بر واسط وب، KeyBase نسخه‌های مشتری مخصوص ویندوز، اندروید، مک و iOS و اکثر نسخه‌های توزیع شده لینوکس ارائه کرده است که قابلیت‌های مختلفی را به کاربران ارائه می‌دهد. به عنوان نمونه امکان گفتگو با استفاده از رمزنگاری سراسری[19] موسوم به چت KeyBase و یک فضای ذخیره سازی ابری موسوم به فایل‌سیستم KeyBase را فراهم می‌کند که امکان ذخیره سازی و دسترسی خصوصی به فایل‌ها را فراهم می‌کند.

شکل ۱واسط کاربری KeyBase

۳ ۱ ساختار KeyBase

هر حساب در KeyBase دارای یک زنجیره امضا[20] موسوم به sigchain است که لیست مرتبی از اعلامیه‌ها[21] است که بیان کننده چگونگی تغییر این حساب در گذر زمان می‌باشد. به عنوان مثال وقتی شما فردی را دنبال می‌کنید، یک اعلامیه جدید

---

[18] Key directory
[19] End-to-end encryption
[20] Signature chain
[21] Statement

موسوم به لینک[22] ایجاد شده و در sigchain شما منتشر می‌شود. هر لینک توسط یکی از کلیدهای کاربر امضا می‌شود و شامل شماره ترتیب و مقدار هش‌شده لینک قبلی است. بنابراین سرور نمی‌تواند لینک جدیدی را ایجاد کرده و یا لینکی را نادیده بگیرد بدون اینکه کل زنجیره را نامعتبر سازد. برای این منظور از یک درخت عمومی مرکل[23] استفاده می‌شود تا برگشت[24] زنجیره به یک حالت قبلی را دشوار سازد. یک حساب در KeyBase می‌تواند دارای چندین کلید باشد که اصطلاحا به آن کلید برادر[25] می‌گویند. افزودن و یا حذف آنها می‌تواند از طریق اضافه کردن یک لینک به sigchain صورت گیرد. با لغو کردن یک کلید، لینک‌های قبلی همچنان معتبر می‌مانند زیرا بررسی هر لینک برمبنای حالت حساب کاربری در آن لحظه از sigchain است.

KeyBase امکان ذخیره عمومی امضاهای کاربران را در یک فرمت استاندارد فراهم می‌کند و از این طریق کاربران می‌توانند هویت خود را اثبات کنند، نشان دهند که مالک یک کلید عمومی هستند، دنبال کردن یک فرد را اعلام کرده و یا اعتبار یک چیز را لغو کنند. به عنوان مثال وقتی یک کاربر می‌خواهد ارتباطی بین هویت خود در KeyBase و یک حساب توئیتری را اثبات کند، اعلامیه‌ای را امضا کرده و آنرا در توئیتر و KeyBase منتشر می‌کند. این حساب‌ها می‌تواند در معرض آسیب پذیری هکرها باشد بنابراین در کنار اطلاعات مرتبط با اعلامیه جدید، مقدار هش شده امضای قبلی نیز، امضا می‌شود.

۲-۳ پشتیبانی از Following در KeyBase

KeyBase تلاش می‌کند تا کلید عمومی کاربری که به دنبال آن هستیم را به شکل قابل اعتمادی در اختیار ما قرار دهد و برای این منظور یک پروتکل اعتبار سنجی سه مرحله‌ای استفاده می‌کند که به شرح زیر است.

شکل ۲- فردی که قصد اراسال پیام به او را دارید

مرحله ۱ : درخواست

فرض کنید می‌خواهید یک پیام رمزنگاری شده برای یکی از دوستان خود با حساب کاربری Maria ارسال کنید. برای این منظور نسخه مشتری شما از سرور KeyBase در مورد هویت Maria سوال می‌کند و سرور اطلاعاتی از قبیل کلید عمومی[26]

---

[22] Link
[23] Merkle Tree
[24] Roll Back
[25] Sibling Key
[26] Public key

این فرد، حساب توئیتری او و لینکی در توئیتر که گواهی اثبات هویت به شمار می‌رود را برمی‌گرداند. این گواهی درواقع یک اعلامیه رمزنگاری شده است که ادعا می‌کند از طرف شخصی با حساب کاربری Maria در KeyBase است. سرور می‌تواند در معرض آسیب پذیری باشد. بنابراین به اطلاعات برگشت داده شده از سمت سرور با دیده شک نگاه می‌کنیم و مرحله دوم از فرایند اعتبارسنجی انجام می‌شود.

شکل ۳- به اطلاعات برگشتی در مرحله اول باید با شک رفتار کرد

مرحله ۲ : ارزیابی اطلاعات توسط مشتری

نسخه مشتری،مرحله دوم اعتبارسنجی را با رمزگشایی گواهی اثبات هویت که در مرحله قبلی دریافت کرده بود آغاز می‌کند. در صورتیکه این مرحله با موفقیت انجام شود، نسخه مشتری می‌تواند این نتیجه‌گیری را انجام دهد که فردی که اطلاعاتش در مرحله اول توسط سرور برگشت داده شده است به سه چیز دسترسی دارد :

- حساب کاربری KeyBase تحت عنوان Maria
- حساب توئیتری
- کلید خصوصی مرتبط با کلید عمومی ارسال شده در مرحله اول

شکل ۴- ارزیابی صحت اطلاعات در مرحله دوم از منظر رمزنگاری

مرحله ۳ : ارزیابی انسانی

مرحله ۱ و ۲ بدون دخالت کاربر انجام می‌شود. در خلال مرحله ۱ و ۲ هویت کاربر از منظر پروتکل‌های رمزنگاری مورد تائید قرار گرفته است. در مرحله سوم این حساب کاربری از منظر شما مورد ارزیابی قرار می‌گیرد تا مشخص شود که آیا فرد پیدا شده همان شخصی است که قصد ارسال پیغام به او را دارید؟

شکل ۵- ایجاد نگاشت حساب کاربر در KeyBase به هویت آنلاین او در یک شبکه اجتماعی

انجام مراحل ۲ و ۳ برای یک کاربر به شکل مکرر، خیلی مناسب نیست. برای اجتناب از این کار می‌توانیم یک تصویر لحظه‌ای از هویت آن کاربر بسازیم و اطلاعات دریافتی از مرحله ۱ را به همراه اطلاعات اضافی در مورد ارزیابی خود را با کمک کلید خصوصی خود امضا کنیم. در نتیجه با راه اندازی مجدد فرایند اعتبارسنجی برای همان کاربر، سرور KeyBase تعریف ما از آن کاربر را که از طریق کلید خصوصی ما رمزنگاری و امضا شده است و غیر قابل دستکاری است را در اختیار ما قرار می‌دهد. البته نسخه مشتری می‌تواند ارزیابی خود را در مرحله ۲ انجام دهد تا بتواند متوجه تغیرات شود. مزیت این شیوه این است که اگر به عنوان مثال ۱۰۰ نفر Maria را دنبال کرده باشند، همه آن تصویر یکسانی مشابه با ما از Maria دارند. در نتیجه اگر قدمت تصویر آنها از Maria به ماه‌ها قبل باز می‌گردد و تصویر ما از هویت او، اخیرا ساخته شده است می‌توان اطمینان پیدا کرد که در زمانی که تصمیم به دنبال کردن Maria گرفته ایم، هویت او مغشوش نشده است.

شکل ۶- هر چه افراد بیشتری در گذشته فرد را تایید کرده باشند، قابلیت اطمینان بیشتر خواهد شد.

۳ ۳ به کارگیری زنجیره بلوکی بیت کوین[27]

در سمت سرور KeyBase چند دغدغه امنیتی وجود دارد :

- حمله DDOS از سوی هکرها
- رخنه و نفوذ در سرور و آلوده کردن کد سرور و کلیدها و ارسال داده‌های نادرست به مشتری
- رخنه و نفوذ در سرور و توزیع کد آلوده سمت مشتری

رویکرد ابتدایی KeyBase برای پاسخگویی به این دغدغه‌ها اینگونه بود که هر کاربر زنجیره امضای مخصوص به خود را داشت که به صورت یکنواخت با هر اعلان[28] جدید، رشد می‌کرد. همچنین سرور یک درخت سراسری مرکل[29]را نگهداری می‌کرد که شامل همه زنجیره‌های امضا بود و علاوه بر این، ریشه این درخت پس از امضای جدید یک کاربر، توسط سرور امضا شده و منتشر می‌گردید. با این وجود این امکان وجود دارد که نفوذگر به سرور با fork کردن حالت آن، به دو نفر، نسخه‌های متفاوتی را نشان دهد. با به کارگیری زنجیره بلوکی بیت کوین این مشکل نیز بر طرف شد و همه اعلان‌های عمومی به شکل قابل راستی آزمایی امضا شده و در زنجیره بلوکی بیت‌کوین درهم‌سازی[30] می‌شود. بنابراین با استفاده از این زنجیره بلوکی می‌توان جدیدترین ریشه درخت مرکل در KeyBase را به دست آورد. وقتی یک نفر، یک اعلان امضا شده را به سرور KeyBase آپلود می‌کند درخت مرکل KeyBase تحت تاثیر قرار می‌گیرد که در نتیجه آن، زنجیره بلوکی بیت‌کوین تغییر کرده و سایر کاربران می‌توانند متوجه این تغییر شوند. حال آنها می‌توانند با عقب رفتن در این زنجیره، متوجه شوند که این تغییر چه بوده است.

---

[27] Bitcoin Blockchain
[28] Announcement
[29] Merkle Tree
[30] Hash

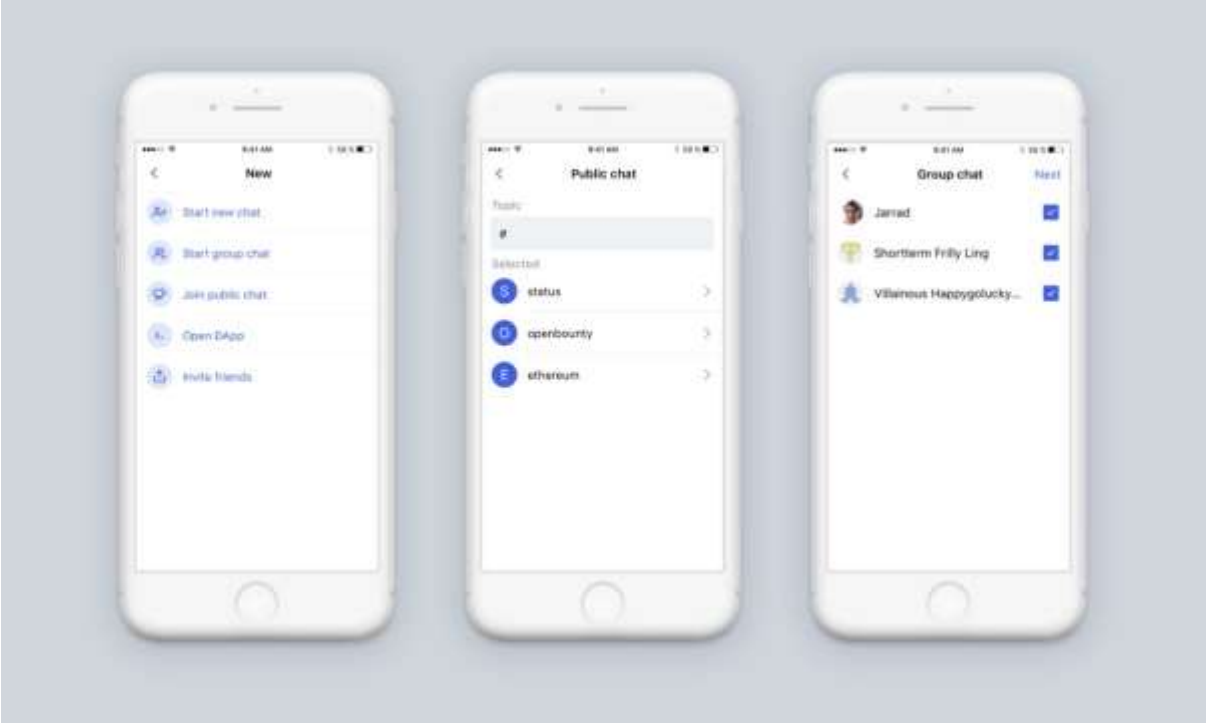
فصل ۴ پیام‌رسان Status

در حال حاضر شبکه‌های اجتماعی از سه دسته تشکیل شده است : صاحبان شبکه اجتماعی، تبلیغ‌کنندگان و کاربران. هر دسته نقش خود را در تداوم و گسترش این پلتفرم بازی می‌کند با این وجود هر کدام اهداف و انگیزه متفاوتی دارند که همزیستی و همراستا کردن آنها با چالش همراه است. نقش صاحبان شبکه اجتماعی جذب و حفظ کاربران روی پلتفرم شبکه اجتماعی تا بتوانند از فعالیت‌های کاربر نفع ببرند و برای این منظور بر الگوریتم‌هایی تکیه می‌کنند که بیشترین تبلیغات مرتبط با کاربر را به او نشان می‌دهد. یا می‌توانند با جمع‌آوری داده‌ها، رفتار و عقیده کاربر را استخراج کنند و به نوعی شیوه فکر کردن، باورها و احساسات کاربر را دستکاری کنند. تبلیغ‌کنندگان یا کارگزارن و دلال‌های داده و اطلاعات[31]، امکان استخراج ارزش افزوده از شبکه و در نتیجه تدوام آنرا به‌وجود می‌آورند. این کار از طریق خرید اطلاعات کاربر و یا تبلیغات هدفمند بر اساس اطلاعات موجود در پروفایل کاربر می‌تواند صورت بگیرد. کاربران کاملا با هدف دیگری به این شبکه‌ها نزدیک می‌شوند و به شکل غیر مستقیم تحت تاثیر اطلاعاتی هستند که در نتیجه تعامل با دوستان و یا افرادی که علایق خود را به اشتراک می‌گذارند قرار می‌گیرند و معمولا ضعیفتر از آن هستند که اطلاعاتی که مصرف می‌کنند و یا سمت و سوی توسعه شبکه را بتوانند کنترل کنند.

Status یک پلتفرم پیام‌رسانی متن باز و یک واسط موبایلی است که برای تعامل با نرم‌افزارهای غیرمتمرکز در بستر شبکه اتریوم ارائه شده است و ایده‌ای که در آن دنبال می‌شود ارائه نسل جدیدی از شبکه‌های اجتماعی موسوم به شبکه‌های اجتماعی-اقتصادی[32] است که در آن کاربران، مالک واقعی سهام شبکه‌ای که در آن مشارکت دارند باشند[33] و انگیزه همه طرف‌های درگیر بتواند با یکدیگر همراستا شود و در آن بتوان شبکه‌ای را ایجاد کرد که به طور طبیعی، رفتارهایی را ترویج کند که نفع همه شرکت‌کنندگان در آن باشد. با انتشار توکن شبکه Status موسوم به Status Net کار(Token (SNT شبکه‌ای ایجاد شد که کاربران آن، ذینفعان آن نیز هستند و این امکان فراهم شده است که رفتار شبکه و نرم‌افزار آن در راستای علایق کاربران باشد به گونه‌ای که آنها این امکان را دارند که بر روی سمت و سوی توسعه و نحوه تکامل شبکه تاثیر بگذارند.

---

[31] Data Broker
[32] Socio-economic network
[33] Everyone-as-a-stakeholder



شکل ۷ نسخه موبایلی Status

قبل از اینکه ذینفعان بتوانند ارتباط و تراکنشی با یکدیگر برقرار کنند نیازمند یک بستر هستیم که در شکل فعلی و رایج آن توسط یک واسط قابل اعتماد (صاحب شبکه) تامین می‌گردد. در عصر فراگیر شدن زنجیره بلوکی اتریوم و پروتکل‌های مرتبط با آن که شالوده و ستون فقرات Web 3.0 را تشکیل می‌دهند، می‌توان از واسط و بستری استفاده کرد که غیر متمرکز، بدون نیاز به مجوز، مبتنی بر وجود عدم اعتماد، دارای دسترسی عادلانه، بر مبنای توافق و قابل راستی آزمایی و اعتبار سنجی است. بستر و واسطی که به شکل غیر قابل تغییری رکوردهای تراکنش‌ها را حفظ می‌کند تا زمانیکه اکثریت شبکه اتریوم موافق باشند.

در این پلتفرم پیام‌رسانی غیرمتمرکز، Status در قالب یک گره عمل می‌کند که مستقیما به شبکه اتریوم وصل است و به‌گونه‌ای طراحی شده است تا بتواند با برنامه‌های غیرمتمرکزی که بر بستر اتریوم اجرا می‌شوند تعامل کند. در نتیجه در اکوسیستمی از اپلیکیشن‌های غیر متمرکز، Status می‌تواند در حکم یک دروازه[34] برای تجارت آزاد، پرداخت‌های همتا به همتا و ارتباطات همتا به همتا برای هرکسی که به گوشی‌های هوشمند و اینترنت دسترسی دارند عمل کند. در حال حاضر سرویس‌هایی که Status در اختیار کاربران خود قرار می‌دهد عبارتند از :

- ارسال و دریافت پیام‌های رمزنگاری شده، قراردادهای هوشمند و پرداخت‌ها
- مرورکردن، گفتگو و تعامل با اپلیکیش‌های غیر متمرکز و ربات‌های گفتگو[35]
- ذخیره و کنترل، دارایی‌های رمزنگاری شده در کیف پول Status

[34] Gateway
[35] Chat bot

به دلیل طبیعت همتا به همتا بودن پروتکل‌های ارتباطی اتریوم برخی از تجربه‌های مورد انتظار کاربر مانند اطلاع پیدا کردن از اینکه یک دوست، به پیام ما پاسخ داده است با چالش‌هایی همراه است و نیازمند طراحی این مساله در قالب غیر متمرکز هستیم. در پروتکل Whisper v5 هنگامی که مشتری ها آفلاین هستند برخی از گره‌ها وظیفه ذخیره پیام‌ها را برعهده دارند. بر همین اساس می‌توان توانایی آنها را توسعه داد تا از ارسال اعلان[36] پشتیبانی کنند. در نتیجه امکان پایه‌گذاری یک بازار برای تامین کننده‌گان سرویس ارسال اعلان به وجود می‌آید که در آن ذینفعان برای بهره‌مندی از این سرویس باید هزینه‌ای در قالب SNT پرداخت کنند. در همین راستا Status نیز پروتکل تحویل دوباره پیام در صورت آنلاین شدن دو طرف را پیاده سازی کرده است.

[36] Push Notification

فصل ۵ آشنایی با Dust و پروتکل مرکوری

پلتفرم‌های ارتباطی متمرکز که بر بستر سرورهای خصوصی ساخته می‌شوند تنها به میزان ضعیف‌ترین مکانیسم‌های دفاعی مورد استفاده در آنها، امن هستند. به طور معمول حریم خصوصی کاربران از طریق فروش داده‌ها و عادات رفتاری کاربران نقض می‌شود و محتوا محدود به یک پلتفرم خاص می‌باشد. پروتکل مرکوری، پروژه‌ای متن باز برای پلتفرم‌های ارتباطی است که تلاش می‌کند از مزیت غیر متمرکز بودن فناوری زنجیره بلوکی استفاده کند. Dust و Broadcast اولین برنامه‌های کاربردی بودند که تلاش کردند این پروتکل را پیاده سازی کنند.

هدف از برنامه Dust این بود که مالکیت محتوای تولید شده در نتیجه گفتگو را به کاربران برگردانند. برخلاف سایر پلتفرم‌ها که داده‌ها را بر روی دیسک ذخیره می‌کند، Dust همه پیام‌ها را در حافظه ذخیره می‌کند. در نتیجه دست یافتن به محتوای پیام توسط خرابکاران بسیار سخت‌تر خواهد شد و هنگام حذف پیام، اطلاعات غیر قابل بازیابی است. بنابراین Dust پلتفرم خصوصی امنی در مواجهه با چشم‌های کنجکاو، به کاربران ارائه می‌کند. از طرفی در ساخت پروتکل مرکوری تلاش شده است تا با استفاده از ویژگی‌ها و مزایای فناوری زنجیره بلوکی صنعت ارتباطات ارتقاء یافته و قدرت بیشتری به کاربر نهایی از منظر شفافیت اطلاعات، محرمانگی و امنیت ارائه شود. داده‌های ذخیره شده در زنجیره بلوکی، به شیوه غیر متمرکز ذخیره می‌شوند و همگان به آن دسترسی داشته و به شکل شفاف قابل راستی آزمایی است. غیرمتمرکز بودن آن وجود یک نقطه شکست را از بین می‌برد و در نتیجه اعتبار رویدادهای رخ داده در آن را تضمین می‌کند.

در این پروتکل، ویژگی‌های ارتباطی مختلفی پیاده سازی شده است و برای این منظور از یک توکن پیام‌رسانی سراسری[37] موسوم به GMT استفاده شده است که مبتنی بر توکن استاندارد اتریوم موسوم به ERC20 است. این توکن مشارکت کاربران در پلتفرم‌هایی که با پروتکل مرکوری یکپارچه سازی شده‌اند را ترویج می‌کند به این نحو که، کاربرانی که دارای GMT هستند امکان تعامل و انجام تراکنش با سرویس‌های پروتکل مرکوری روی زنجیره بلوکی را دارند. همچنین پروتکل مرکوری این امکان را فراهم می‌کند تا یک کاربر روی یک پلتفرم پیام‌رسانی بتواند به شکل امن، پیام خود را از طریق زنجیره بلوکی به یک پلتفرم پیام‌رسانی دیگر ارسال کند، به شرط اینکه پروتکل مرکوری در این پلتفرم‌های پیام رسانی، یکپارچه سازی شده باشند. این مساله باعث گسترش اکوسیستم به همه کاربران پلتفرم‌هایی که با پروتکل مرکوری یکپارچه سازی شده‌اند می‌شود.

شکل ۸-پشته فناوری

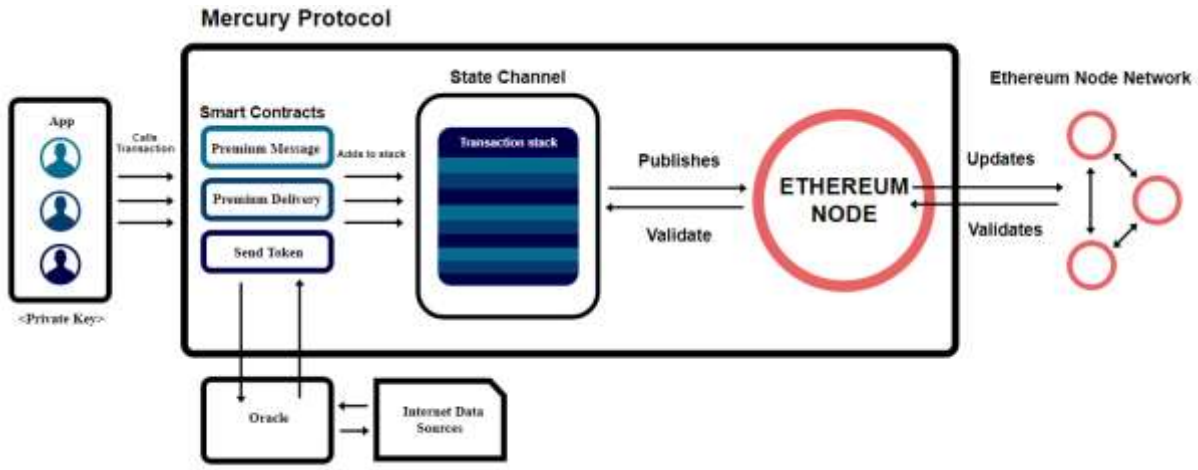
توکن‌های ساخته شده در زنجیره بلوکی، می‌توانند در حکم دارایی‌های مجازی به حساب آیند و می‌تواند به عنوان یک شاخص سودمند برای مشارکت در پلتفرم ارتباطی مورد استفاده قرار گیرند. این توکن‌ها در بستر زنجیره بلوکی اجرا می‌شوند و سیستمی

---

[37] Global Messaging Token (GMT)

را ایجاد می‌کنند که امکان ایجاد یک پلتفرم ارتباطی غیرمتمرکز را فراهم می‌کند. وقتی کاربر محتوای واجد ارزشی را که توسط یک پلتفرم مشخص شده است را تولید می‌کند این توکن به عنوان جایزه به او اهدا می‌شود که او می‌تواند با کمک این توکن، از سرویس‌های پولی آن پلتفرم بهره‌مند شود. این مساله‌ای انگیزه‌ای برای مشارکت بیشتر کاربران ایجاد می‌کند و ایده زیربنایی پشت سر GMT است.

دلیل استفاده از اتریوم این است که هدف اصلی اتریوم چیزی ورای ایجاد، ثبت و انتقال توکن‌های شبکه زنجیره بلوکی است و می‌توان آنرا یک فناوری زنجیره بلوکی تعمیم یافته در نظر گرفت که دارای یک زبان برنامه‌نویسی مخصوص به خود است که با کمک آن می‌توان فرمت‌های تراکنش اختصاصی و توابع تغییر حالت را برنامه نویسی کرد و قواعد مورد نظر را مشخص و آپلود نمود به گونه‌ای که امکان تفسیر اتوماتیک آن وجود داشته باشد. به عبارت دیگر این فرم تعیمم یافته از فناوری زنجیره بلوکی، قابلیتی را فراهم می‌کند که به قرارداد هوشمند[38] موسوم است که در واقع یک برنامه کامپیوتری است که مستقیما دارایی‌های مجازی (توکن‌ها، نام دامنه‌ها، شناسه‌ها) را کنترل می‌کند و در نتیجه امکان کد کردن پروتکل‌ها روی بستر زنجیره بلوکی را فراهم می‌کند. قراردادها دارای آدرس‌ها و دارایی‌های مجازی[39] مخصوص به خود هستند و تنها از طریق قواعد تعریف شده در کد قرارداد می‌تواند این دارایی را به فرد دیگری منتقل کند و این انتقال دارایی برای همه طرف‌های این شبکه، آشکار است. این قراردادهای هوشمند می‌توانند برای کارکردهای متفاوتی مورد استفاده قرار گیرد زیرا با کمک آن می‌توان قواعد پیچیده صدور و ساختار انگیزشی اتوماتیک آنرا کد کرد.



۱-۵ سرویس‌های ارتباطی مبتنی بر GMT

با استفاده از GMT می‌توان به سرویس‌های ارتباطی مختلفی دسترسی داشت و به عنوان نمونه Dust سرویس‌های مختلفی در این زمینه به کاربران خود ارائه می‌کند. به طور معمول مدل‌های ارتباطاتی را می‌توان به سه دسته تقسیم کرد:

۱. یک به یک: دیالوگ رفت و برگشتی بین دو طرف است مانند نوشتن نامه، تماس تلفنی، پیام متنی رد و بدل شده بین دو طرف
۲. یک به چند: اعلان و یا یک انتشار یک طرفه مانند رادیو است.

[38] Smart Contract
[39] Digital asset

۳. چند به چند: گفتگو بین مجموعه ای از افراد و موجودیت‌ها است مانند آنچه در اتاق‌های گفتگوی دیجیتالی رخ می‌دهد.

در دسته پیام‌های خصوصی یک به یک، امکان ارسال پیام‌های حجیم در قالب فایل‌های PDF یا MOV وجود دارد. همچنین می‌توان نوع خاصی از پیام اضطراری را برای یک کاربر ارسال کرد که تا زمانی که به آن پاسخ داده نشود، به طور مرتب کاربر را از دریافت آن پیام مطلع می‌کند. همچنین امکان ارسال پیام به خارج از Dust، به سایر پلتفرم‌هایی که با پروتکل مرکوری یکپارچه سازی شده‌اند، نیز وجود دارد. در دسته یک به چند، امکان ارسال پیام به دسته‌ای از کاربران که ایجاد کننده محتوا را دنبال[40] نکرده‌اند وجود دارد. همچنین امکان ارسال پیام به دنبال کننده‌گان یک حساب مشخص نیز وجود دارد و با کمک آن می‌توان یک گروه اجتماعی را هدف گرفت.

هدف از طراحی GMT این است که کاربران بتوانند با انجام اعمالی مشخص آنرا از ارائه کننده‌گان سرویس به دست بیاورند. در واقع وقتی به یک پلتفرم جهت ارائه سرویس، GMT تخصیص می‌یابد، بخشی از آن به عنوان عامل انگیزشی به کاربرانی که رفتار مشخصی را از خود نشان می‌دهند تخصیص خواهد یافت و در نتیجه، اکوسیستمی به‌وجود می‌آید که مشارکت کاربران را از طریق اهدای GMT تشویق می‌کند. به عنوان مثال ایجاد کننده محتوا می‌تواند از طریق ایجاد مستمر محتوا و یا ایجاد محتوا بر اساس فیدبک مصرف کننده محتوا، GMT دریافت کند. مصرف کننده محتوا نیز می‌تواند از طریق فیدبک دادن در مورد کیفیت محتوا، پاسخ دادن به پیام‌ها و اعلان‌ها در یک بازه زمانی مشخصی، به اشتراک گذاشتن و باز پخش مجدد آن، GMT دریافت کند. همچنین راه‌های انگیزشی دیگری از قبیل وارد شدن به سیستم، دعوت دوستان به پلتفرم، پخش محتوای تجاری نظیر آگهی‌های تبلیغاتی و رسیدن به نقاط عطف پلتفرم (مثلا تعداد مشخصی پیام ارسال کند) برای دریافت GMT وجود دارد. این عوامل انگیزشی باعث می‌شود که موجودی حساب شما از طریق GMT های اهدایی مثبت شود و بتوانید آنها را برای بهره‌مندی از سرویس‌های پولی مصرف کنید بدون اینکه نیازمند منابعی خارج از این اکوسیستم باشید.

[40] Follow

منابع

- https://blockgeeks.com/guides/what-is-زنجیره بلوکی-technology/
- https://en.wikipedia.org/wiki/زنجیره بلوکی
- https://www.mercuryprotocol.com/files/Mercury_Protocol_whitepaper.pdf
- https://keybase.io/docs/server_security
- https://keybase.io/docs/sigchain
- https://keybase.io/docs/server_security/following
- https://keybase.io/docs/server_security/merkle_root_in_زنجیره بلوکی_بیت‌کوین
- https://wiki.status.im/The_Status_Netکار_Whitepaper