مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

عصر فضای مجازی
چهل و سوم

CRYPTO ANARCHY

درآمدی بر رمزآنارشی

An introduction
to Cryptoanarchism

عصر فضای مجازی

گزارش شماره ۴۳
خرداد ۱۳۹۹

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

درآمدی بر رمز آنارشی

**محتوای انتشار یافته در این اثر
الزاماً بیانگر دیدگاه مرکز ملی فضای مجازی نیست**

تهیه شده در مرکز ملی فضای مجازی
(گروه مطالعات بنیادین)

تهیه کننده: محمداسماعیل حسنی جبل کندی؛
دانشجوی دکتری ریاضی دانشگاه تربیت مدرس
ناظر علمی: دکتر حسین مطلبی کربکندی

نشانی: تهران، میدان آرژانتین، خیابان بیهقی، نبش
خیابان ۱۶غربی، پلاک ۲۰
تلفن: ۰۲۱-۸۶۱۵۱۰۶۱
کد پستی: ۱۵۱۵۶۷۴۳۱۱

فهرست

سخن نخست

سخن نخست

فضای مجازی با شتاب شگرف و رو به تزایدی که در حال بسط و گسترش است تمام ساحات اجتماعی، اقتصادی، سیاسی و فرهنگی زندگی بشر را درنوردیده و هر روز بخش بزرگی از زندگی واقعی را در خود فرو برده و حیات متفاوت و جدیدی به آن می‌دهد. لذا به نظر می‌رسد دو نگاه کلان به فضای مجازی وجود دارد: نگاه اول که بالاخص در ابتدای رشد و تکوین فضای مجازی مسلط شده بود، آن را همچون ابزاری کنار سایر ابزارهای بشری تصویر می‌کرد که تنها طریقیت داشت. اما نگاه دوم، در نتیجه رشد تحولات خیره‌کننده فضای مجازی و سایه گستری آن در حوزه‌ها و شئون بشر در یک دهه اخیر آن را چون سکویی می‌داند که بسیار فراتر از شأن ابزاری حیات انسان‌ها را سامان جدیدی داده و ادعای تمدن نوینی را دارد. رویکردی که از قضا از چشمان بصیر رهبر انقلاب نیز دور نمانده و انتظاری تمدنی از فضای مجازی در ایران را مطالبه داشته‌اند.

در همین راستا گزارش‌های عصرفضای مجازی تلاش می‌کند تا فهم سازمان‌ها و دستگاه‌های مرتبط با حوزه فضای مجازی را ارتقاء بخشیده و آن‌ها را برای مواجهه فعال و خردمندانه با تحولات این عرصه مهیا سازد.

سید ابوالحسن فیروزآبادی
دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

چکیده

چکیده

آنارشیسم به عنوان یکی از مکاتب اصلی بشری، طرفدارانی برای خود دارد. آن‌ها با شعار آزادی بشر از شر قدرت های فاسد جهانی، در پی جامعه ایده‌آلی هستند که هیچ نهاد متمرکزی دارای قدرت نیست و مردم از قید و بند قدرت‌ها رها هستند. واضح است که آنارشیست‌ها حکومت‌ها و قدرت‌های متمرکز فعلی را مانع تبلور این تفکر می‌دانند. لذا آنارشیست‌ها راهکارهای مختلفی برای نیل به آرمان خود انتخاب کردند. این راه‌کارها طیف وسیعی از پدیده‌ها، از تبلیغات اجتماعی گرفته تا از میان برداشتن یا ناتوان‌سازی نظارت دولتی را دربر می‌گیرد. آنارشیست‌های ریاضیدان نیز به سهم خود سعی کردند تا با ابزارهای رمزنگاری میان مردم و دولت‌ها حائل ایجاد کنند و امکان نظارت‌های دولتی را از بین ببرند و در نهایت نیز امنیت حریم خصوصی مردم را تأمین نمایند.

بدین ترتیب رمزنگاری به عنوان فضایی که می‌توانست ابزارهای لازم برای ساخت این حصارها را تأمین کند مورد توجه آنارشیست‌ها

قرار گرفت.

به این ترتیب رمزآنارشی وارد ادبیات سیاسی شد و به نقش‌آفرینی پرداخت. در این نوشتار سعی داریم گزارشی از وضعیت رمزآنارشیسم در جهان ارایه دهیم، آرمان‌های رمزآنارشی را بشناسیم، ساختارهایی که طراحی کرده‌اند، ابزارهای‌شان را معرفی کنیم، عوارض ضدامنیتی آن را بشناسیم و همچنین تاثیر رمزآنارشیستی بر یکی از جوامع آنارشیستی عصر حاضر و نیز حالات محتمل درباره آینده رمزآنارشی را تا حدودی بررسی کنیم.

واژگان کلیدی: آنارشیسم، رمزنگاری، رمزآنارشی، گمنامی، رمزارز

مقدمه

مقدمه

در صد سال اخیر ارتباطات و استفاده از تجهیزات ارتباطی گسترش فزاینده‌ای داشته است، به حدی که برای انسان امروزی حذف ابزارهای ارتباطی ناممکن به نظر می‌رسد. با گسترش رایانه‌ها و پدیده اینترنت، فضای زندگی بشر دستخوش تحولات عمیقی شد. از جمله این تحولات می توان به تقویت توان نظارتی دولت‌ها، گسترش ارتباطات، تحولات عمیق اقتصادی و ... اشاره نمود. در چنین فضایی آنارشیست‌ها به دلیل مخالفت بنیادی که با مسئله دولت دارند، به فکر افتادند که حریم خصوصی افراد در برابر دولت‌ها محافظت کنند. برنامه‌نویسان آنارشیستی که راه چاره را در ترور و اعتراضات خیابانی نمی‌دیدند، سعی کردند ابزارهایی تولید کنند که جامعه با استفاده از آن‌ها خواه ناخواه به سمت آنارشیسم حرکت کند.

لذا ساختارهایی را طراحی کردند که امروزه با استفاده از ارزهای دیجیتال دولت‌ها قادر به رصد تراکنش‌های مالی که با این ابزار

انجـام می‌پذیـرد، نیسـتند و نمی‌تواننـد از آن‌هـا مالیـات بگیرنـد، دارایی‌هـای مخالفـان سیاسی‌شـان را مسـدود کننـد محدودیت‌هـای خریـد و فـروش اعمـال نماینـد (یـا حتـی پول‌هـای کثیـف را رصـد کننـد). رمزآنارشیسـت‌ها سـعی می‌کننـد توانایـی حکومت‌هـا را در شـنود اتبـاع خـود بـه حداقـل برسـانند و بـه ایـن ترتیـب آزادی بیـان را تامیـن کننـد حتـی اگـر ایـن فضـای آزاد منجـر بـه سوءاسـتفاده‌های گسـترده از سـوی مجرمیـن شـود. از طـرف دیگـر حکومت‌هـا سـعی می‌کننـد ابزارهایـی طراحـی کننـد کـه بتوانـد دامنـه نفـوذ قـدرت حاکمیـت را عمیق‌تـر کنـد. در ایـن درگیـری طبیعـی اسـت کـه رمزنـگاری[1] بـه عنـوان ابـزار حفـظ محرمانگـی، یـار اصلـی آنارشیسـت‌ها در ایـن میـدان رقابـت خواهـد بـود.

رمزنـگاری عبـارت اسـت از علـم احـراز امنیـت یـک بُعـد از یـک پیـام در برابـر حمـلات مهاجـم[2]، بـه طـوری کـه طرفیـن قانونـی ارتبـاط، از تأمین بـودن آنچـه نمی‌خواسـتند دیگـران مطلـع شـوند، خاطرجمـع باشـند. ایـن امنیـت می‌توانـد ناتوانـی مهاجـم از خوانـدن پیـام، جعـل هویـت، تخریـب پیـام و مـواردی از ایـن دسـت باشـد. لازم بـه تذکـر اسـت کـه در ایدئولـوژی آنارشیسـم، مهمتریـن دشـمن، مهاجـم و عامل اختـلال در امنیـت، نهادهای قـدرت و به‌خصـوص حکومت‌هـا هسـتند.

در واقـع نـکات فـوق، اسـاس ایـن ایـده بـود کـه رمزنـگاری بـه عنـوان ابـزاری پایـه ای می‌توانـد امنیـت یـک آنارشیسـت را در برابـر تهدیدهـای حکومتـی تأمیـن کنـد. لـذا آنارشیسـت‌ها در پـی ابزارسـازی‌هایی هسـتند تـا بتواننـد قـدرت نظارتـی و حاکمیتـی مهاجـم (حکومـت) را خنثـی کنند.

1. Cryptography
2. Adversary

بخش اول

رمز آنارشی چیست؟

بخش اول

رمزآنارشی چیست؟

نخستین گام در تأمین هدف آنارشی، ناتوان کردن حکومت در شنود اطلاعات است. اگر حکومت بتواند پیام‌های کاربران را مشاهده کند، می‌تواند به دلیل محتوای نامطلوب پیام‌ها از ابزار قانون (به تعبیر آنارشیستی ابزار خشونت آمیز قانون) در جهت منافع خودش استفاده کند[1]. لذا در نخستین گام، یک آنارشیست باید محرمانگی پیام مخابره شده را تأمین کند. گام دوم، ناتوان کردن حکومت در رهگیری ارتباطات است. اگر مهاجم (دولت) بتواند یک پیام را رهگیری کند، قادر خواهد بود بر اطلاعات نظارت داشته باشد و حتی می‌تواند کاربران را در استفاده از پیام‌های رمزنگاری شده محدود کند. با تأمین دو گام فوق، امنیت در تبادل پیام تأمین می‌شود.

اما برای رمزآنارشیست‌ها تأمین امنیت به تنهایی کافی نیست. دولت ها می‌توانند با وضع قوانین تحت فشار قرار دادن مالکین سرویس‌های مختلف که ارسال اطلاعات از طریق آنان انجام می‌پذیرد، به اطلاعات کاربران دسترسی پیدا کنند.

۱. در نگاه آنارشیستی، قانون همان تهدید به خشونت و اعمال قانون، اعمال خشونت تعبیر می‌شود.

لذا باید سرویس‌دهندگانی به صورت گمنام ایجاد شوند. به این ترتیب لازم است تا پست الکترونیکی[1]، سرور[2]، VPS[3] و ... نیز به صورت گمنام ساخته شوند. اما دولت‌ها هنوز هم می‌توانند تراکنش‌های مالی را در فضای سایبری پیگیری کرده و مشتریان سرویس‌های ارزی را شناسایی کنند. علاوه براین کارفرما، کارگزاران خود را می‌شناسد و می‌تواند تحت تأثیر قدرت دیگران، کارگزاران را در اختیار نهادهای اعمال قدرت حاکمیت (دادگاه) قرار دهد. راهکار آنارشیست‌ها برای مبارزه با این فرایند، ابداع مفهوم رمزارزها[4] بود.

رمزارزها، ارزهای دیجیتالی هستند که معمولا بر پایه توان پردازشی مورد استخراج قرار می‌گیرند. این امر هر کسی را قادر می‌سازد در فرایند تولید رمزارزها فعالانه وارد عمل شود. عموم رمزارزها مرکزیت ندارند و هر کسی می‌تواند از آن‌ها بدون محدودیت استفاده کند. در این صورت هیچ نهادی قادر به اعمال محدودیت بر این قسم رمزارزها نخواهد بود. بنابراین با در نظر گرفتن مفهوم رمزارز، یک سرویس دهنده می‌تواند بدون داشتن اطلاعات هویتی مشتری، سرویس‌رسانی غیر رایگان داشته باشد.

پس از عملیاتی شدن پروتکل‌های گمنامی[5] و ظهور رمزارزها، نوبت به بازارهای گمنام بود. طبق باورهای آنارشیسم، سایت های خدمات رسانی خود می‌توانستند به مراکز قدرت تبدیل شوند و منجر به ایجاد فساد در جامعه گردند. همچنین خاطره شناسایی سایت های دارک وب[6] مانند سیلک رود[7] نشان می‌داد که تمرکز بر

1. Email
2. Server
3. Virtual private server
4. Cryptocurrency
5. Anonymity protocols
6. Dark-web
7. Silk Road

روی یک وب‌سایت، نقطه ضعفی برای آنارشیست هاست. بنابراین ظهور بازارهای گمنام باعث شد تا دردسرهای ناشی از چنین مشکلاتی تا حد زیادی رفع گردد.

امروزه علاوه بر گمنامی، محرمانگی، رمزارزها و موارد مشابه، شاهد تحولات دیگری در تاریخ نرم‌افزار هستیم که در عملیاتی شدن اهداف آنارشیسم تأثیرگذار بوده اند. اریک ریمون[1] از چهره‌های برجسته نهضت متن‌باز[2]، صراحتاً خود را یک آنارشیست می‌داند و نهضت متن‌باز را بستری برای اهداف آنارشیستی معرفی می کند.

برخی از شرایط طبیعی، دستیابی به آرمان‌های رمزآنارشی را تسهیل می‌کند و برخی دیگر، موانعی بر سر راه دستیابی به آنها ایجاد می‌نماید. شرایطی مانند لزوم تأمین امنیت در برابر مهاجمان از طریق رمزنگاری، با توجه به اینکه تفاوتی در ماحصل عمل مهاجم داخلی و خارجی وجود ندارد، موجب شده است دولت‌ها به ناچار حدودی از رمزآنارشی را تسهیل کنند. هرچند تلاش می‌کنند در فضای داخلی با استفاده از ابزارهای قانونی (مانند لزوم تحویل کلیدهای رمزنگاری در برخی کشورها)تا حدودی مانع آسیب‌های رمزآنارشی شوند. از جمله موانع طبیعی بر سر راه گسترش رمز آنارشی اشکالاتی است که در الگوریتم‌ها و نرم‌افزارها وجود دارند و می‌توانند تهدیدی برای حریم خصوصی قلمداد شوند. همچنین انگیزه‌هایی همچون دستیابی به پول بیشتر افراد را وسوسه می‌کند که حریم خصوصی مردم را نقض کرده و به دنبال شکستن رمزها

1. Eric S. Raymond
2. Open source movement

باشند. در فصل آخر به شرح موانع رمزآنارشی خواهیم پرداخت.

البته دستیابی به آرمان‌های رمزآنارشی، نیازمند همکاری طیف عظیمی از دانشمندان در حوزه‌های مختلف اعم از علم ریاضی، علوم رایانه، فیزیک و ... است. عصاره سیاستی که این محققین، که لزوماً هم آنارشیست نیستند، را با سواستفاده از حس علم‌دوستی در راستای اهداف رمزآنارشی گرد آورده و به خدمت گرفته است را می‌توان درجمله زیر خلاصه کرد [۱]:

«چالش‌های علمی و تکنیکی عظیمی در توسعه و حفظ این سیستم‌های رمزنگاری وجود دارد، که باعث می‌شود برخی از برنامه‌نویسان به پیوستن به چنین پروژه‌هایی علاقه‌مند باشند.»

۱-۱. بیانیه رمزآنارشی

در سال ۱۹۸۸ میلادی، تیموتی می[1] بیانیه رمزآنارشی را منتشر کرد. متن این بیانیه چندباری ویرایش شد و شما در ادامه ترجمه ویرایش ۱۹۹۲ آن را مطالعه می‌کنید [۲]:

« شبحی در حال تسخیر دنیای مدرن است، شبح رمزآنارشی.

تکنولوژی رایانه در آستانه فراهم آوردن این امکان است که افراد و گروه‌ها به شیوه‌ای کاملاً ناشناس با یکدیگر ارتباط برقرار کنند. ممکن است دو نفر به مبادله پیام بپردازند، تجارت کنند و قراردادهای الکترونیکی را بدون دانستن نام حقیقی یا هویت قانونی طرف مقابل، مورد مذاکره قرار دهند. فعالیت‌های انجام گرفته بر روی شبکه‌ها،

1. Timothy C. May

به وسیله مسیریابی‌های وسیعی که برای بسته‌های رمز شده انجام می‌شود و همچنین محفظه‌های ضد دستکاری که پروتکل‌های رمزنگاری را پیاده‌سازی می‌کنند، غیرقابل ردگیری خواهند بود. بنابراین اعتبار افراد در چنین سیستم‌هایی اهمیت محوری خواهد داشت، که بسیار مهم‌تر از رتبه اعتباری در جهان امروز است. این تحولات به صورت کامل ماهیت مقررات دولتی، پرداخت مالیات و کنترل روابط اقتصادی و همچنین توانایی حفاظت از اطلاعات را تغییر خواهند داد و حتی موجب ایجاد تغییر در ماهیت اعتماد و اعتبار خواهند شد.

تکنولوژی این انقلاب، که قطعاً یک انقلاب اجتماعی و اقتصادی نیز هست، به صورت تئوریک در قالب روش‌هایی در دهه گذشته وجود داشته‌است. این روش ها بر مبنای رمزنگاری کلید عمومی، سیستم‌های ضد تعاملیِ دانش صفر و پروتکل‌های نرم‌افزاری مختلف به منظور انجام تعاملات، احراز هویت و تأیید محتوا شکل گرفته‌اند. تا کنون، با هدف بررسی این اهداف در اروپا و آمریکا کنفرانس‌های علمی مختلفی برگزار شده‌است که بیشتر آن ها تحت نظارت اداره امنیت ملی قرار گرفته‌اند. اما تنها در سال‌های اخیر بوده است که شبکه‌های رایانه‌ای و رایانه های شخصی، سرعت کافی برای تحقق این ایده‌ها را به دست آورده‌اند و قطعاً در ده سال آینده در تحقق این ایده‌ها به اندازه‌ای سریع خواهند شد که غیرقابل توقف قلمداد گردند. در آینده شبکه‌های با سرعت بالا، ISDN[1]، محفظه‌های

1. Integrated services digital network

ضد دستکاری، کارت‌های هوشمند، ماهواره‌ها، فرستنده‌های کوبانـد، رایانه‌های مالتی‌میپز و تراشه‌های رمزنگاری که امروزه در حال توسعه هستند بخشی از تکنولوژی روز خواهد بود.

البته دولت سعی خواهد کرد که گسترش این فن‌آوری را با استناد به نگرانی‌های امنیتی ملی، مانند استفاده توسط فروشندگان مواد مخدر، فرار مالیاتی یا ترس از فروپاشی اجتماعی متوقف کند. البته مشخص است که بسیاری از این مسائل نیز جای نگرانی دارد. رمزآنارشی اجازه می‌دهد اسرار ملی آزادانه تجارت شود و امکان تجارت مواد غیرقانونی و سرقت شده را نیز فراهم می‌آورد. یک بازار رایانه‌ای ناشناس حتی باعث می‌شود که بازارهای نامناسب برای ترور و اخاذی به وجود آید و بستر مناسبی برای سود بردن مجرمین مختلف و عناصر خارجی از شبکه رمزی فراهم خواهد شد. اما این مسائل نمی‌توانند مانع گسترش رمزآنارشی شوند.

همانطور که فناوری چاپ، قدرت صنفی قرون وسطایی را کاهش و ساختار قدرت اجتماعی را تغییر داد، روش‌های رمزنگاری نیز ماهیت شرکت‌ها و دخالت دولت در معاملات اقتصادی را تغییر خواهند داد. به همراه بازارهای اطلاعاتی نوظهور، رمزآنارشی یک بازار سیال برای هر آنچه که می‌تواند در قالب کلمات و تصاویر بیان شود، ایجاد می‌کند. این امر دقیقاً شبیه به اختراع به ظاهر جزئی سیم خاردار است که محافظت از مزارع وسیع را ممکن ساخت و به دنبال آن مفاهیم مربوط به زمین و حقوق مالکیت بر مزارع و زمین‌ها در غرب

تغییر پیدا کرد. یافته‌های به ظاهر معمولی در شاخه رمز در علم ریاضیات، مانند گیره‌های سیمی هستند که سیم‌های خاردار کشیده شده به دور نوعی از مالکیت معنوی را از بین می‌برند. برخیزید، شما چیزی برای از دست دادن ندارید جز این سیم‌های خارداری که به دورتان کشیده شده است.»

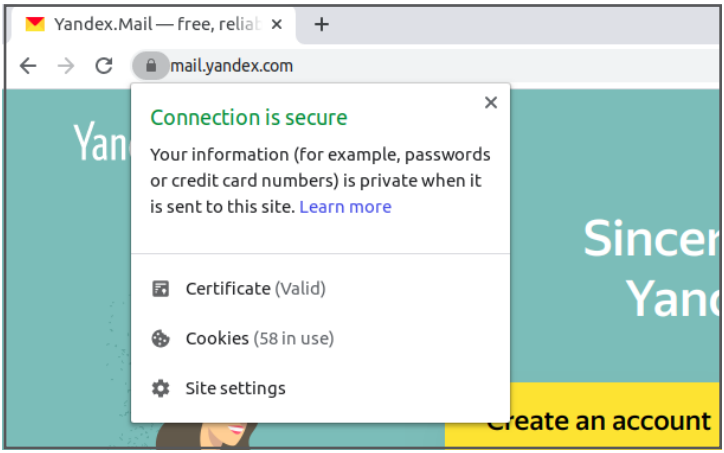
۲-۱. محرمانگی محتوای پیام

سرویس‌های مخابرات و پست به عنوان دو بازوی اصلی حکومت در کنترل ارتباطات مردمی به شمار می‌روند. معمولاً قوانین کشورها اجازه‌ی شنود کلی و همگانی پیام‌ها را به دولت آن کشور نمی‌دهد، با این حال همواره در قوانین کشورها شرایطی تعیین می‌شود که حکومت می‌تواند حریم خصوصی افراد را تهدید کند. تلفن‌های ثابت و همراه، پیجوها و دیگر دستگاه‌های ارتباطی که نیازمند یک سیستم مرکزی هستند، عملاً در اختیار دولت‌ها قرار دارند و دولت بدون مجوزهای لازم و اختیاراتی خارج از چارچوب‌های حاکمیتی به هیچ کس اجازه انتقال بسته‌های پستی یا پیام‌ها را نمی‌دهد.

در جهان امروز نیز دولت‌ها، ارتباطات اینترنتی را تحت حاکمیت خود نگه داشته‌اند و سرویس‌هایی که شرکت‌های خصوصی ارائه می‌کنند باید در چارچوب‌های حکومتی باشد. در چنین فضایی است که رمزگذاری به کمک آنارشیسم می‌آید. برای جلوگیری از شنود، پیام در دو سر ارتباط رمزگذاری می‌شود و دیگر هیچ‌کس قادر به

مشاهده محتوای پیام مخابره شده نخواهد بود.

پروتکل‌های مختلفی با هدف تأمین امنیت ارسال پیام طراحی شده‌اند که معروفترین آن‌ها پروتکل‌های SSL[1] و TLS[2] می‌باشد. از این دو نوع پروتکل در تعداد زیادی از وب‌سایت‌ها استفاده می‌شود. این پروتکل‌ها بین سرویس‌دهنده (معمولاً وب‌سایت) و مشتری قرار می‌گیرد و از شنود ارتباط توسط مهاجمینی که بین راه ارتباط نشسته‌اند، جلوگیری می‌کنند. به عنوان یک نمونه همانطور که در تصویر زیر مشاهده می‌کنید ارتباطات بین یک سرویس‌دهنده ایمیل و مشتریانش توسط این پروتکل‌ها رمزنگاری شده است.



شکل ۱-۱- یک سرویس دهنده ایمیل که داده هایش را رمزنگاری می کند.

1. Secure sockets layer
2. Transport layer security

۳-۱. چالش‌های پیش روی رمزآنارشی

چالش‌های مختلفی در راستای تحقق آرمان‌های رمزآنارشی وجود دارد، از جمله مسائل سخت ریاضی که باید در راستای تحقق امنیت، طرح و حل شوند. در این میان مشکل اصلی، مقاومت حکومت‌ها در برابر رمزآنارشی است.

در برخی از کشورها، استفاده از رمزنگاری با سختگیری‌های قانونی روبه‌رو شده است. مثلا در انگلیس با درخواست دولت، شهروندان مجبور هستند که کلیدهای رمزنگاری خود را در اختیار حکومت قرار دهند، در غیر این صورت ممکن است تا دو سال به زندان محکوم شوند [۳]. همانطور که پیشتر اشاره شد، ممنوعیت فعالیت رمزارزها در برخی از کشورها، مانعی در راه تحقق رمزآنارشیسم تلقی می‌شود. البته آنارشیست‌ها در چنین جوامعی می‌توانند فعالیت‌های خود را محدود به خارج از کشور کنند.

۴-۱. آینده رمزآنارشی

هر چند لینوس تروالدز[1] سازنده سیستم عامل لینوکس در کتاب «فقط برای تفریح[2]» می‌گوید [۶]:

«آیا واقعا در جهان چیزی منزجرکننده‌تر از کسی هست که سعی می‌کند صنعت را پیشگویی کند؟ منظورم افراد خود بزرگ‌بینی هستند که سعی می‌کنند در این باره که قطار تفریحی تکنولوژی قرار است ما را به کجا ببرد، پُرچانگی کنند.»

1. Linus Torvalds
2. Just for fun

ا ما به هر حال انسان با نگاه به آینده است که می‌تواند قدم بردارد. رمزآنارشی در سی سال گذشته موفق شده است تا چندین چالش بزرگ و تاریخی را از پیش پای آنارشیسم بردارد. رمزآنارشی توانست سیستم‌های شنود دولتی را از کار بیاندازد، ارزی خارج از حیطه قانون و حکومت ایجاد کند، فضای تاریک نت را گسترش دهد و حتی بازار رمزآنارشیستی ایجاد نماید. در رابطه با این موارد در فصل آتی توضیحات بیشتری آورده شده است. پس از حل این مشکلات، اکنون وقت آن رسیده که به دو چالش بسیار مهم بپردازد. نخست طراحی پروتکلی برای رمزارزها که بتواند از اسکناس نیز پشتیبانی کند، چراکه وضعیت فعلی رمزارزها از جهان شمولی آنها جلوگیری می‌کند. چالش دیگر ایجاد تشکیلاتی آنارشیستی است. یعنی افراد بتوانند بدون آنکه نیازمند قانونی بالادستی باشند، شرکت‌های خود را تاسیس کنند، کارمند استخدام نمایند و قرارداد ببندند. شاید چنین رؤیای آنارشیستی بعید به نظر برسد. ولی به عنوان یک نمونه کردستان سوریه، در پی مستقر کردن یک سیستم خودمدیریتی است. این بدان معناست که دیر یا زود شاهد احساس نیاز به چنین ساختار رمزآنارشیستی خواهیم بود. چنین ساختاری احتمالاً برآمده از تکنولوژی بلاکچین و تائید فرایندهای روزانه شرکت توسط مدیران ارشد خواهد بود. مدیرانی که بر مبنای امتیاز، فعالیت و رای‌گیری محرمانه داخلی شرکت انتخاب شده‌اند (مانند آنچه در ویکی‌پدیا ادعا می‌شود). بنابراین افراد زیردست با تائید.

مدیـران رمزارزهـای داخلـی شـرکت را دریافـت می‌کننـد و می‌تواننـد بـا مبادلـه ایـن رمزارزهـا بـا دنیـای بیـرون بـه فعالیـت اقتصـادی بپردازنـد اهمـال کارکنـان منجـر بـه دریافـت امتیـاز منفـی شـده و بـا عـدم دریافـت سـهم رمـزارز بلـوک مربوطـه همـراه خواهـد بـود. چنیـن سـاختارهایی نـه تنهـا قـادر اسـت اهمـال و کـم‌کاری کارکنـان را کنتـرل کنـد، بلکـه از مرکزیـت شـرکت و شناسـایی کارکنـان نیـز جلوگیـری می‌کنـد. همچنیـن بـا طـرد از اجتمـاع (امتیـاز منفـی بـه کاربـر) از تخلفـات جلوگیـری می‌کند.

۵-۱. کردستان سوریه نمونه‌ای از یک نظام آنارشیستی

منطقـه خودمختـار کردنشـین سـوریه با نام رسـمی منطقه خـود مدیریتی غـرب کردسـتان یـا «روژاوا» شـناخته می‌شـود. مـردم ایـن منطقـه تحـت تاثیـر عبـدالله اوجـالان، رهبـر گـروه مسـلح و تروریسـتی پ.ک.ک سـعی دارنـد سیسـتم و سـاختارهای اجتماعـی را بـر پایـه نظامـی آنارشیسـتی بنـا کننـد. هیـچ حکومـت مرکـزی انتخـاب نکرده‌انـد و تـلاش دارنـد مناسـبات اجتماعـی را چنـان بنـا کننـد کـه نیازمنـد قـدرت مرکـزی نباشـد. دلایـل اجتماعـی - سیاسـی مختلفـی بـرای ایـن امـر می‌تـوان پیـدا کـرد. از جملـه ایـن دلایـل می‌تـوان بـه تجربـه تاریخـی کردسـتان‌های ایـران، ترکیـه و عـراق، جلوگیـری از درگیـری بـا دولت‌هـای مرکـزی سـوریه و ترکیـه، بدنامـی گروه‌هـای حامـی روژاوا و ... اشـاره نمـود. کردهـای سـوریه در پـی بهبـود روابـط بـا دولـت سـوریه و اعطـای تابعیـت بـه همـه کردهـا، کمتـر بـا دولـت مرکـزی سـوریه درگیـر شـده‌اند. دولـت سـوریه نیـز در عمـل

خودمختاری آن‌ها را به رسمیت می‌شناسد. . از طرفی با توجه به قدرت شاخه پ.ک.ک در سوریه موسوم به ی.پ.گ[1]، با تشکیل دولت مرکزی، احتمالاً این گروه جایگاه رسمی پیدا می‌کند. ولی با توجه به سابقه تروریستی پ.ک.ک در کشورهای مختلف، قطعاً با بی‌مهری همسایگان مواجه خواهد شد[۷].

به هر حال و بنابر هر دلیلی اهالی کردستان سوریه سعی کرده‌اند تا تحت لوای آنارشیسم و بدون تشکیل دولت به حیات سیاسی خود ادامه دهند. هر چند در طول تاریخ جوامع آنارشیستی مختلفی تشکیل شده‌اند، اما رژاوا یکی از مهمترین این جوامع است. در چنین جامعه آنارشیستی طبیعتا گرایش به بهره‌برداری از رمز آنارشیسم به صورت گسترده قابل مشاهده است.

ارسلان سردم[2] رهبر توسعه تکنولوژیک روژاوا در مصاحبه‌ای با مجله کوین‌دسک بیان می‌کند:

«ارز اصلی ما لیر سوریه است اما، اعتقاد رو به رشد مردم این منطقه این است که رمز ارزها می‌توانند جایگزین بهتری باشند.»[۸]

امیر تاکی از توسعه‌دهندگان اولیه بیت‌کوین و اوپن‌بازار به کمک ارسلان سردم و روژاوا شتافته و به آنها در پیاده‌سازی زیرساخت‌های مبتنی بر بلاک‌چین[3] یا همان زنجیره بلوکی برای مدیریت منابع آب و زمین کمک کرده است. او همچنین سعی کرده است تا کیف‌پول‌هایی به زبان محلی بسازد و حتی برای رمزارزها اسکناس‌های کاغذی نیز تولید کند وی (با نادیده گفتن سابقه

1. Erselan Serdem
2. Coindesk
3. Block-chain

تروریستی گروه‌های ی.پ.گ، پ.ک.ک و پژاک) مدعی است که روند آنارشیستی شدن جامعه، نه یک پروژه جمعی بلکه یک فرایند تکاملی و پروسه طبیعی است!

بخش دوم

گمنامی، گام استراتژیک رمز آنارشی

بخش دوم

گمنامی، گام استراتژیک رمزآنارشی

با استفاده درست از الگوریتم‌ها و پروتکل‌های مربوطه، سرویس‌های مخابراتی در شنود اطلاعات ناتوان می‌شوند و تنها به اطلاعاتی گنگ و مبهم از قبیل وجود پیام، حجم اطلاعات، زمان اتصال و هویت طرفین ارتباط دسترسی خواهند داشت. هرچند این اطلاعات دراغلب مواقع بیهوده و به درد نخور است، اما ممکن است همین اطلاعات برای دولت‌ها مهم باشد. فرض کنید یک مجرم در گوشه‌ای از کشور بیانیه‌ها و اطلاعیه‌هایی علیه حاکمیت (یا علیه امنیت عمومی کشور) منتشر می‌کند. هر چند بیانیه‌هایش (پیام‌هایش) را به صورت رمزگذاری شده برای دوستانش می‌فرستد و دوستانش این بیانیه‌ها را منتشر می‌کنند ولی دولت با بررسی منتشرکنندگان، اطلاعیه و افرادی که با آن‌ها در ارتباط هستند، می‌تواند نویسنده اطلاعیه‌ها را پیدا کند. درواقع دولت هنوز می‌تواند پیام‌ها را رهگیری کند و هویت طرفین ارتباط را بشناسد. پس هنوز آنچنان که باید گمنامی تأمین نیست[1]. اینجا بود که ایده محرمانه نگاه داشتن هویت طرفین

۱. آنارشیست‌ها دولت‌ها را فاقد مشروعیت لازم در برخورد با مجرمین می‌دانند. لذا حتی از مجرمین سایبری مانند کلاهبرداران، فروشندگان مواد مخدر و ... نیز همانند فعالین سیاسی حمایت می‌کنند

رابطه به ذهن رسید[1]. مخفی کردن مالکیت یک داده، پیچ تاریخی مهمی در رمزآنارشی محسوب می‌شود. بنابراین نسخه‌های اولیه از پروتکل‌های گمنامی ارائه شد و رمزنگارهای مختلفی از سرتاسر جهان آن‌ها را چکش کاری کردند تا ابزاری صیقلی و بی‌نقص ساخته شود.

پروتکل‌های گمنامی ارائه شده اعم از مسیریابی پیازی[2] یا شبکه مخلوط[3]، بر اساس ایده گم کردن پیام در میان تعداد زیادی از پیام‌ها شکل گرفتند. اکنون سعی می‌کنیم شاکله اصلی پروتکل گمنامی را با مثالی توضیح دهیم:

دو پستچی همکار را تصور کنید. پستچی اول هر لحظه ده‌ها بسته دریافت می‌کند. پستچی اول بسته‌ای که تنها شامل آدرس فرستنده است را باز می‌کند. داخل آن بسته، بسته‌ای کوچکتر است که پستچی اول آن را به پستچی دوم تحویل می‌دهد. پستچی دوم بسته دریافتی‌اش را باز می‌کند. داخل این بسته نامه‌ای است که فقط شامل آدرس گیرنده است. بنابراین به جز در حالتی که این دو پستچی با هم تبانی کرده باشند، هیچ حالت دیگری وجود ندارد که بتوان این پیام را رهگیری کرد. البته آنچه در عمل اجرایی شده است قطعاً ریزه‌کاری‌های بیشتر دارد، ولی می‌توان گفت که به طور شهودی روند فوق اجرا می گردد. نکته بسیار جالب ماجرا اینجاست که مخاطب نهایی، حتی اگر مبدأ نامه را نشناسد، می‌تواند به نامه دریافتی پاسخ دهد. روند به این صورت است که او پاسخ را به پستچی دوم می‌دهد و او نیز نامه را در همان بسته اولیه قرار

---

۱. شاید هم برای مخفی ماندن نیروهای اطلاعاتی دولتی از دید مخالفین داخلی و خارجی چنین ساختارهای مبتکرانه‌ای ایجاد شدند. برای مثال ابزار «تور» به عنوان معروفترین ابزار گمنامی، با پشتیبانی مالی نیروهای نظامی آمریکا آغاز به کار کرد. به هر حال گمنامی آبی بود که به آسیاب آنارشیست‌ها هم ریخته شد.

2. Onion Routing
3. Mix network

می‌دهد تا مبادا آدرس مقصد قابل شنود باشد. سپس این بسته را به پستجی اول می‌دهد. پستچی اول نیز مبدأ نامه را می‌شناسد. لذا به طرز جالبی طرفین ارتباط می‌توانند بدون شناخت هم با یکدیگر ارتباط برقرار کنند.

در واقعیت نیز برای محو کردن مبدأ ومقصد پیام‌ها از چنین ایده‌ای استفاده شده است. سامانه‌های گمنام فعلی شامل ده‌ها سرور است که به صورت تصادفی سه تا از آن‌ها به عنوان واسط انتخاب می‌شود. پیام‌های ارسالی کاربر، در لایه‌های رمزگذاری‌شده، بین این سه سرور جابجا می‌شود و هر کدام، یک لایه از رمز باز می‌کند و پیام را به مقصد می‌رساند.

البته پروتکل فوق مشکلاتی دارد. فرض کنید که دولت می‌تواند بسته‌های پستی خارج از اداره پست را رهگیری کند. دولت می‌داند که هر بسته از کجا می‌آید و به کجا می‌رود. تنها چیزی که از دسترس دولت خارج است زمانی است که یک پستچی، بسته را باز می‌کند. اگر اداره پست تنها یک مشتری داشته باشد دولت می‌بیند که فقط یک بسته به اداره پست وارد شده و فقط یک بسته از آن خارج شده است. بنابراین براحتی می‌تواند نتیجه بگیرد که بسته از کجا و به چه مقصدی ارسال می‌شود. لذا لازمه گمنامی این است که هر لحظه تعداد زیادی بسته به اداره پست ارسال شود و تعداد زیادی بسته نیز از آن خارج گردد. اینجاست که آنارشیست‌هایی غیر از متخصصین رمز به میدان می‌آیند. آن‌ها رایانه‌ها و خطوط

اینترنت خود را در اختیار سامانه قرار می‌دهند تا نقش پستچی را بازی کنند و به پیچیده‌تر کردن سیستم کمک کنند. به این ترتیب آنارشیست ها با توانمندی‌های مختلف، وظایف فردی خود را برای ناتوان کردن حکومت‌ها در شنود اطلاعات انجام می‌دهند.

ایده گمنام ماندن در بستر شبکه جهانی اینترنت، یک ایده تاریخی و اثرگذار در تاریخ رمزآنارشی محسوب می‌شود. این ایده به ایده پول‌های گمنام، بازارهای گمنام و شکل‌های دیگر گمنامی منجر شد که بعد از تدوین پروتکل‌های بلاک‌چین امروزه بخش‌های مختلف رمزآنارشی را تشکیل می‌دهند.

جدای از رمزآنارشی، مثال‌هایی از این دست در جهان حقیقی نیز وجود دارد که گمنامی در خدمت دولت‌ها و جوامع غیرآنارشیستی قرار دارد و یا با اهداف غیرآنارشیستی و غیرسیاسی پیاده‌سازی شده است. رای‌گیری و همه‌پرسی، نظرسنجی، آمارگیری‌های پزشکی و ... مثال‌هایی هستند که در جهان حقیقی و خارج از فضای سایبری، گمنامی را تأمین می‌کنند، تا نظام‌های سیاسی، پزشکی یا دیگر نهادها به اهداف خود برسند.

با وجود همه این توضیحات، باید در نظر گرفت که به صورت طبیعی بخش زیادی از فعالیت‌ها در فضای اینترنت به صورت گمنام صورت می‌گیرد. نظر دادن در خبرگزاری‌ها، وبلاگ‌ها، مشاهده توضیحات سایت‌های مختلف و ... به ندرت نیازمند تائید هویت[1] است. حتی اگر سرویس‌هایی مانند وبلاگ‌ها یا دایرة المعارف‌ها، تولیدکنندگان

---

۱. به عنوان مثالی از معدود سرویس‌های بلاگری که حتی استفاده از محتوای بلاگ‌ها نیازمند تائید هویت (از طریق پرداخت بانکی) است می‌توانید به https://hamsooo.com اشاره کرد. در این سرویس تقریباً هویت همه کاربران شفاف است و هیچ گمنامی وجود ندارد.

محتوا را ملزم به ثبت‌نام کنند، بازهم امکان ثبت یک اکانت گمنام و غیرقابل رهگیری وجود دارد. آنچه که در فضای اینترنت گمنامی را به خطر می‌اندازد پیام‌رسانی مبتنی بر آدرس شبکه‌ای (IP)[1] در اینترنت است. هر پیام در سطح شبکه نیز شامل آدرس مقصد و مبداء و احیاناً ایستگاه‌های میانی[2] است. مهمترین چیزی که گمنامی کاربران را تهدید می‌کند رهگیری همین IP است و معروف‌ترین ابزارهای گمنامی مانند Tor یا I2P نیز برای حل همین مشکل ساخته شده‌اند. در ادامه توضیحات بیشتری در مورد ابزارهای گمنامی ارائه می‌شود.

۱-۲. ابزارهای گمنامی

معروفترین سامانه‌های گمنامی عبارتند از تور[3]، فری‌نت[4]، آی۲پی[5] جوندونیم[6] و... البته نکته جالب ماجرا اینجاست که بیشتر ابزارهای گمنامی معروف با بودجه‌های دولتی و حکومتی تشکیل شده‌اند. همچنین به دلیل عدم استقبال سرویس‌دهندگان از کار کردن با مشتریان گمنام، اگر از طریق این شبکه‌ها (به خصوص تور) بخواهیم از برخی سرویس‌ها استفاده کنیم، با محدودیت‌های بسیار زیادی مواجه خواهیم شد. لذا ممکن است برخی کاربران ترجیح دهند به جای این ابزارهای معروف، از وی‌پی‌ان[7] یا پروکسی‌های[8] غیر تخصصی استفاده کنند. سرویس‌دهندگان وی‌پی‌ان و پروکسی‌ها معمولاً مشتری کمی دارند. برخی از انواع پروکسی‌ها اصلاً شامل

۲. مانند سرویس‌دهنده اینترنت

1. Internet Protocol
3. Tor
4. Freenet
5. I2P
6. Jondonym
7. VPN
8. Proxy

رمزنگاری نیستند و می‌توانند امنیت و حریم خصوصی کاربر را با تهدیدات جدی مواجه کنند.

بنابراین یک آنارشیست در هنگام استفاده از یک شبکه و با توجه به اهمیت داده‌های مبادله‌ای خود، باید حد عاقلانه‌ای از امنیت - کارکرد را انتخاب کند و برای یک وبگردی ساده و بی‌اهمیت سراغ ابزارهای سنگین و پرتنشی مانند تور یا جوندونیم نرود. به هر حال امروزه سرویس‌های مختلفی به ارائه خدمات گمنامی مشغول هستند و آنارشیست‌ها به راحتی می‌توانند حریم خصوصی خود را بیش از پیش حفظ کنند. در ادامه مختصری در مورد تعدادی از ابزارهای گمنامی توضیح خواهیم داد.

۱-۱-۲. رمزارزها

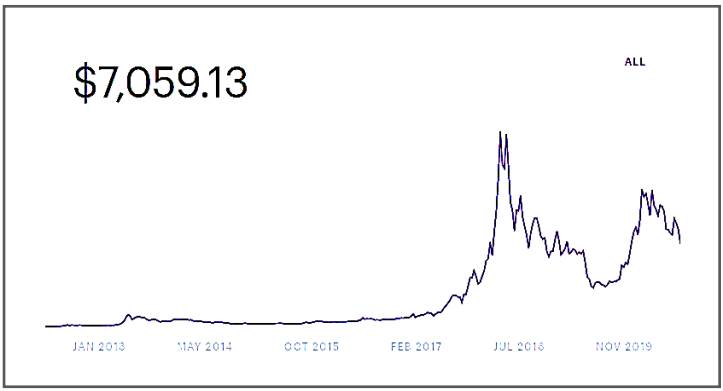
پس از تأمین گمنامی، آنارشیست‌ها نیازمند ابزاری بودند که به آن‌ها اجازه تبادلات مالی فارغ از محدودیت‌های دولتی را بدهد. دولت‌ها همواره در بازارهای مالی دخالت می‌کنند، مبادلات برخی اجناس را مجاز و برخی را غیرمجاز اعلام می‌کنند، کف و سقف قیمتی تعیین می‌کنند و از معاملاتی که دولت دخالتی در آن نداشته مالیات می‌گیرند. چنین رفتاری برای یک آنارشیست که قائل به عدم دخالت دولت در این امور است، قابل تحمل نیست. پول‌های کاغذی، مسکوکات و فلزات باارزش به راحتی قابل رهگیری نیستند. کسی شماره سریال پول‌هایش را یادداشت نمی‌کند، با میکروسکوپ

از همه سکه‌هایش تصویر برداری نمی‌کند و حتی اگر فردی هم چنین کاری کرد در عمل به درد رهگیری منشاء پول نمی‌خورد. اما زمین بازی در فضای مجازی کمی متفاوت است. تبادلات مالی بین افراد به راحتی قابل رهگیری است. حامیان مالی یک کنشگر سیاسی، به راحتی توسط سیستم بانکی شناسایی می‌شوند. سیستم بانکی به راحتی می‌تواند دارایی افراد را شناسایی کند، مالیات بر دارایی اعمال کند، یارانه نقدی وی را دستکاری کند یا حتی از دارایی وی برداشت و به حساب طلبکارانش واریز کند. برای یک آنارشیست همه این‌ها نقض حریم خصوصی محسوب می‌شود. با تکامل ابزارهای رمزنگاری اعم از الگوریتم کلید متقارن[1] و رمزنگاری کلید عمومی[2]، توابع درهم‌ساز[3]، روشهای احراز هویت و... کم‌کم زمینه ظهور ارزهایی که بدون پشتوانه‌های دولتی به بازار عرضه شوند، فراهم شد.

در سال ۲۰۰۹ شخصی با نام مستعار ساتوشی ناکاموتو ، یک ارز دیجیتال به بازار ارائه کرد و به این ترتیب افق جدیدی در پیش روی رمزآنارشی ایجاد گردید. با وجود اینکه ۱۰ سال از تولید بیت‌کوین می‌گذرد، هنوز هیچ حمله کارایی علیه آن گزارش نشده و همینطور هویت ساتوشی ناکاموتو[4] نیز مخفی مانده است. متخصصین حدس می‌زنند که ثروت شخصی وی حدود ۷۰۰ هزار دلار باشد و عجیب اینکه در این مدت برداشتی از آن صورت نگرفته است[۹]. هر چند افراد متعددی مدعی بودند که ساتوشی ناکاموتو هستند، ولی همگی

1. Symmetric key algorithm
2. Public key cryptography
3. Hash function
4. Satoshi Nakamoto

در اثبات ادعای خود شکست خوردند. بیت‌کوین از قیمت‌هایی نزدیک به ۰٫۳ سِنت شروع به کار کرد و مطابق نمودار زیر تا امروز فراز نشیب‌های بزرگی به خود دیده است.



شکل ۲-۱- نمودار نوسانات قیمت بیت‌کوین در طول ۱۰ سال گذشته

بیت‌کوین به عنوان اولین رمزارز، بسیار قدرتمند ظاهر شد. ولی نقاط ضعفی داشت که می‌توانست حریم خصوصی را مخدوش کند. دارایی حساب برای همگان قابل مشاهده بود، محل تراکنش‌ها قابل رهگیری بود و ... . معمولاً برای رفع این مشکلات، افراد حساب‌های بیت‌کوینی خود را صرفاً تحت سامانه‌های گمنامی استفاده می‌کردند و به جای استفاده از یک حساب برای همیشه، برای هر معامله یک حساب جدید باز می‌کردند. به این ترتیب می‌توانستند جلوی رهگیری و نقض گمنامی را بگیرند. اما به مرور زمان، رمزارزهای

دیگری به بازار عرضه شدند که این نواقص را نداشتند. به طوریکه پیش از معامله هیچ‌کس نمی‌تواند دارایی‌های دیگران را ببیند یا تراکنش‌های وی را رهگیری کند. اتریوم، بیت‌کوین گولد و... همگی از رمزارزهایی هستند که پس از بیت‌کوین وارد بازار شدند.

ساختاری که بیت‌کوین استفاده می‌کرد تا امنیت معاملات را تامین کند به بلاک‌چین یا زنجیره بلوکی مشهور شد. روند کار بلاک‌چین به این صورت است که هر بلوک تائید کننده صحت و درستی عملیات انجام شده در بلوک پیش از خود است و در هر گام از تایید معاملات، تنها نیاز به بررسی و تایید عملیات انجام شده درآخرین بلوک می باشد. با تائید هر بلوک (هر بلوک شامل معاملات انجام شده در طول یک بازه مشخص است) پول‌های ادعایی هر حساب تثبیت می‌شود. تائید هر بلوک نیازمند محاسبات بسیار زیاد و زمان‌بر است و در ازای محاسبات درست، بیت‌کوین‌های جدیدی دریافت می‌کنند. در اصطلاح علمی به افرادی که سعی دارند عمل تائید معاملات را انجام دهند معدن‌چی[1] گفته می‌شود. با توجه به غیرمتمرکز بودن معاملات، معدن‌چیان انگیزه‌ای برای دروغگویی ندارند، چرا که ممکن است ادعای کذب آن‌ها در تائید یک معامله توسط دیگر معدن‌چیان کشف شود. این سازوکار نه فقط دولت‌ها را حذف می‌کند بلکه، با حذف تمرکزگرایی انگیزه دروغگویی را نیز از معدن‌چی‌ها می‌گیرد.

هرچند ایده اولیه رمزارزها حذف نهاد دولت از معاملات و تبادلات

1. Miner

پولی بود، ولی این ایده در عمل حداقل تا کنون چندان موفق نبوده است.

در برخی کشورها مانند هند معامله رمزارزها عملی مجرمانه و افراد معدن‌چی مجرم محسوب می‌شوند[۱۰] و در برخی کشورها مانند ایران صرافی‌های رمزارز، تنها در صورت احراز هویت خدمات ارائه می‌دهند. تنها کسری از سایت‌ها حاضر به پذیرش رمزارزها شده‌اند و تنها تعداد معدودی فروشگاه در جهان حقیقی رمزارزها را به رسمیت شناخته‌اند. تا به امروز، رمزارزها در فضای دلالی و نوسان‌گیری دست و پا می‌زنند. هر چند بعید نیست در آینده‌ای میان‌مدت، رمزارزها بتوانند از فرش بلند شوند ولی روشن نیست که حتی در بلند مدت نیز بتوانند به عرش برسند.

۲-۱-۲. فضای تاریک نت

در ابتدای کار، ابزارهای گمنامی با این هدف ساخته شدند که مهاجم (یا همان دولت مرکزی در مکتب فکری آنارشیسم) در تشخیص مسیر ارتباطات مردم عادی ناتوان باشد. ولی ممکن است از نظر یک سرویس‌دهنده خود مشتری نیز مهاجم تلقی شود. یعنی لازم باشد که مشتری ندانند که از چه کسی سرویس می‌گیرد. ابزارهای گمنامی، به‌خصوص ابزار گمنامی تور، بستر مناسبی به این منظور مهیا کرده‌اند که امروزه آن را با نام فضای تاریک وب می‌شناسیم. این فضا صرفاً از داخل خود ابزار گمنامی در دسترس است و افراد

خارج از سامانه هیچ چیزی نمی‌بینند. این فضا این امکان را برای کاربران اینترنت فراهم می‌کند که بدون نظارت دولت بتوانند به فعالیت‌های خود بپردازند.[1]

۳-۱-۲. اپن بازار

پس از ظهور فروشگاه‌ها در فضای تاریک نت، عده‌ای به این فکر افتادند که با ایجاد بازارچه‌های تاریک غیرمتمرکز، امکان اعمال قدرت توسط مالک سایت را از آن بگیرند. همچنین با توجه به تجربه تلخ دستگیری مالک سیلک رود برای رمزآنارشیست‌ها، امکان اعمال قدرت توسط حکومت را نیز مرتفع سازند. سایت سیلک رود معروفترین سایت خرید و فروش در فضای تاریک نت (مبتنی بر تور) بود که افراد در آن بیشتر به خرید و فروش‌های غیرقانونی مانند مواد مخدر مشغول بودند. دولت آمریکا طی یک عملیات پیچیده امنیتی در یک مرحله موفق به مسدود کردن سایت و در مرحله دوم موفق به دستگیری گرداننده اصلی این وب‌سایت شد. پس از آن بود که یک فرد ایرانی تبار به نام امیرتاکی پروژه‌ای را شروع کرد تا بتواند پروتکلی غیرمتمرکز برای خرید و فروش ایجاد نماید. این پروتکل که نام اپن بازار برای آن در نظر گرفته شد، با هدف حذف نظارت حکومتی و آزادی در معامله ایجاد گردید. هر چند امیر تاکی رفیق نیمه‌راه اوپن بازار بود و آن را در میانه راه رها کرد، ولی گروه‌های برنامه‌نویس دیگر موفق شدند زیرساخت اوپن‌بازار را تکمیل و آن را

۱. معمولاً از فضای تاریک برای اعمال مجرمانه مانند خرید و فروش مواد مخدر، سلاح، پورنوگرافی، سفارش قتل و آدم‌کشی، جاسوسی و وطن‌فروشی و... استفاده می‌شود و کمتر شاهد رفتار قانونی اخلاق‌مدار در این فضا هستیم.

به مرحله عملیاتی برسانند.

۴-۱-۲. پیام‌رسان‌های گمنام

یکی دیگر از ابزارهای گمنامی، پیام‌رسان ها و پروتکل‌هایی هستند که قادرند اطلاعات را به صورت گمنام بین افراد رد و بدل کنند. در ادامه به بررسی تعدادی از پیام‌رسان‌های گمنام و بیان عملکرد آنان می‌پردازیم.

بیت مسیج:

یک پروتکل ارسال و دریافت پیام است که اولاً متمرکز نیست، ثانیاً گمنام است. این پروتکل بعد از ایمیل و پیش از بیت‌کوین معرفی شد و نهادهای امنیتی سعی کردند ابزارهای مبتنی بر این پروتکل را گسترش دهند. جالب است بدانید که پایه‌های رمزارز بیت‌کوین نیز مبتنی بر الگوریتم این پروتکل بنا شده است [۱۱].

تلگرام:

تلگرام پیام‌رسانی با قابلیت استفاده در سیستم عامل‌های اندروید[1] ios[2]، لینوکس[3]، ویندوز[4] و مک[5] می‌باشد. این پیام‌رسان به معنی دقیق کلمه گمنام نیست و ورود به نرم‌افزار نیازمند شماره تلفنی است که قابلیت دریافت پیامک داشته باشد. به دلیل ثبت نام اولیه و ذخیره اطلاعات افراد از جمله شماره تلفن آن‌ها که راه دسترسی به اطلاعات هویتی افراد را هموار می‌کند، در واقع مرتبه‌ای از تمرکز

1. Android
2. Iphone operating system
3. Linux
4. Windows
5. Mac

در ایـن پیام‌رسـان وجـود دارد. امـا هویـت کاربـران را از یکدیگـر پنهـان می‌کنـد. هـر چنـد یـک آنارشیسـت هرگـز نبایـد بـه یـک ابـزار متمرکـز اعتمـاد کنـد، ولـی بـه هـر حـال بـه عنـوان یـک ابـزار دم دسـتی می‌توانـد مفیـد باشـد.

شماره مجازی:

گفتیـم کـه یکـی از ابزارهـای دنیـای امـروز شـبکه‌های اجتماعـی مجـازی و پیام‌رسـان‌ها هسـتند. بیشـتر شـبکه‌های اجتماعـی و پیام‌رسـان‌های امـروزی جهـت جلوگیـری از حسـاب‌های کاربـری جعلـی و در نتیجـه فشـار بیشـتر روی سـرورها یـا فشـارهای اجتماعـی، خواسـتار شـماره تلفنـی هسـتند کـه کد احـراز هویـت را بـه آن شـماره تلفـن پیامک کننـد. چنیـن وضعیتـی کـه نیازمنـد لـو رفتـن هویـت کاربـر اسـت، بـرای آنارشیسـت‌ها پذیرفتـه شـده نیسـت. بنابرایـن ابزارهایـی سـاخته‌اند کـه شـماره‌هایی غیرواقعـی در اختیـار کاربـر قـرار می‌دهـد تـا بتوانـد پیامـک احـراز هویـت را بـه وسـیله آن دریافـت کنـد. ایـن شـماره‌ها نیازمنـد هیـچ سـیمکارتی نیسـتند و هویتـی بـرای آن‌هـا ثبـت نمی‌شـود. حتـی برخـی از سـرویس‌دهندگان شـماره مجـازی از رمزارزهـا نیـز پشـتیبانی می‌کننـد، تـا گمنامـی کاربـر را تضمیـن کننـد.

بخش سوم

عوارض رمز آنارشی

بخش سوم

عوارض رمزآنارشی

رمزآنارشی در طول تاریخ نوپایش عوارض شدید و مهلکی بر جای‌گذاشته است. امروزه پولشویی از طریق بیتکوین امری روزمره شده که حتی ساده‌ترین فیشینگرها که تنها با ابزارهای درگاه‌ساز می‌توانند کار کنند نیز از بیتکوین جهت پولشویی استفاده می‌کنند و در عملا پیگیری سرقتها و پولهای کثیف را مشکل می‌کنند. متاسفانه حتی رمزارزهایی نیز پس از بیتکوین ایجاد شده که از منظر رمزآنارشی نسبت به بیتکوین «ایمن» تر محسوب می‌شود و این در حکم امکانی قدرتمند در اختیار متخلفین از قوانین است. به بیان دقیق‌تر دیگر فروشندگان مواد مخدر، قاچاقچیان اعضای بدن، قاتلین مزدور و دیگر مجرمین بزرگ، نیازی به پولشویی‌های پیچیده ندارند، چرا که تنها با رد و بدل کردن رمزارز می‌توانند از نگاه دولت‌ها مخفی شوند. ابزارهای گمنامی نیز بیشتر به جای آنکه آزادی بیان را تامین کنند، به ابزاری جهت تخلف از سیاست‌های فرهنگی، اجتماعی و سیاسی کشورها تبدیل شده‌اند.

چنانچه ابزارهای گمنامی (فیلترشکن‌ها) حداقل در ایران به یک چالش جدی فرهنگی تبدیل شده است، در دیگر کشورها نیز وضعیت بهتر نیست، در ایالات متحده سایت‌های مجرمانه متعددی مثل سیلک‌رود به وجود آمدند و حتی مزدورهای گمنامی که با سفارش آنلاین اقدام به قتل می‌کردند در محافل هکری شهرت پیدا کردند. از سوی دیگر سرویس‌های ارائه شماره مجازی بیش از آنکه کارکردهایی جهت حذف مزاحمت‌های تلفنی داشته باشند به محلی برای ایجاد مزاحمت غیرقابل رهگیری تبدیل شده است.

متاسفانه رمزآنارشیست‌ها با هدف اعطای آزادی از قدرت متمرکز، هرج و مرج را در جهان واقعی افزایش داده‌اند و حداقل در رمزارزها حتی همین قدرت متمرکز نیز تنها از دولتها (که موظف به پاسخگویی هستند) به سمت شرکت‌های عظیم خصوصی پردازش(که تنها به سهامدارنشان پاسخگو هستند) جابجا شده و همان شعار پوسته‌ای آزادی نیز با اما و اگرهایی همراه شد. علاوه بر مشکلات هرج و مرج، تسلط شرکتهای خصوصی بر مردم، حامیان مالی برخی از ابزارهای رمزآنارشیستی مانند ماستادون صراحتا از شرکتهای فعال در صنعت پورن هستند که خود نشان‌دهنده سمت و سویی است که این ابزار بیشتر مورد استفاده قرار می‌گیرد[1] و قطعا در آینده نیز براحتی قادر به تخلف از آن نیستند.

در انتها باید تاکید داشت که با وجود معایب فوق حذف مطلق رمزآنارشی چندان سهل‌الوصول نیست، رمزنگاری یک فن و ابزار

---

http://csri.majazi.ir/index.php?module=cdk&func=loadmodule&system=cdk&sismodule=user/content_view.php&sisOp=view&ctp_id=697&cnt_id=87484&id=76

است که مانند هر ابزار دیگری می‌تواند خطرآفرین باشد. لذا مسئله تزاحم امنیت بین امنیت رمزنگاری و اهداف رمزآنارشی در جهان امروز باید ریزبینانه و موشکافانه بررسی شود و برخورد صرفا قهرآمیز با آن می‌تواند آسیب‌زا شود.

نتیجه گیری

نتیجه‌گیری و پیشـــنهادات راهبردی

نتیجه‌گیری

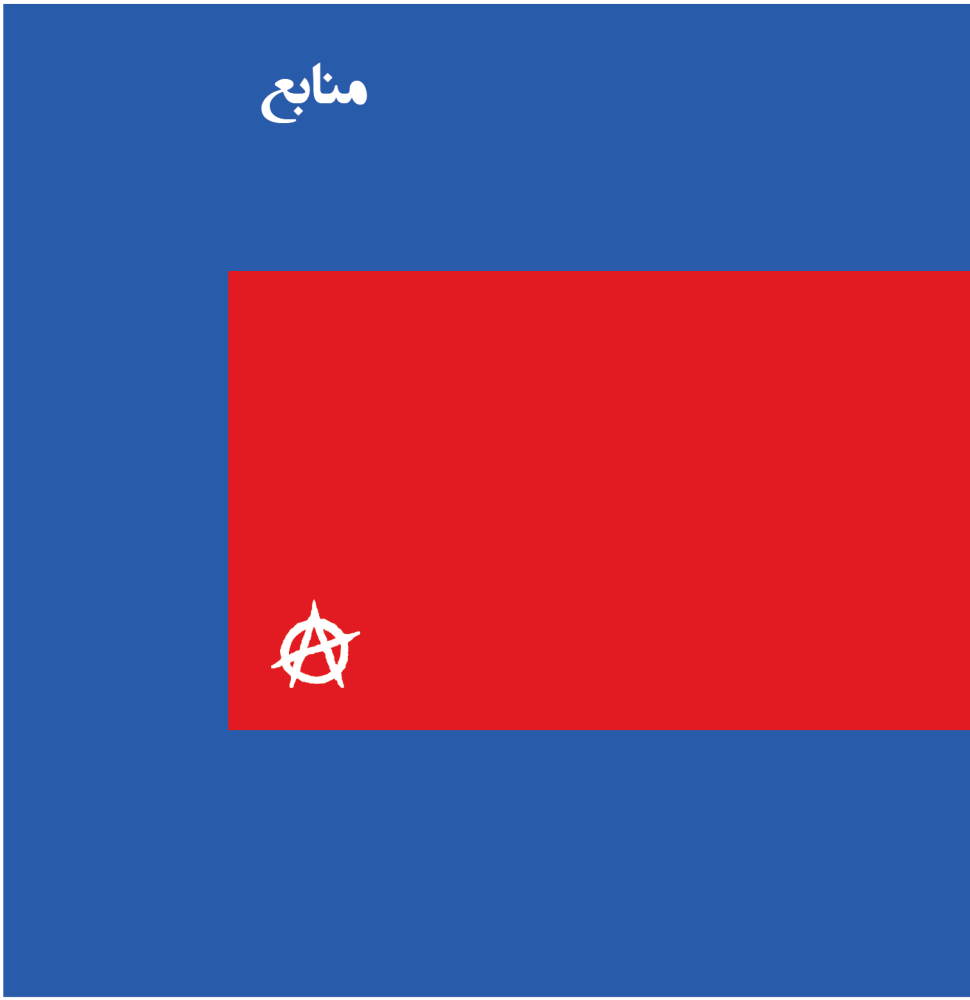
در ایـن گـزارش بـا چیسـتی رمزآنارشـی، اسـتفاده‌ای کـه بـه ویـژه آنارشیسـت‌ها از آن در جهـت گمنامـی می‌برنـد و برخـی ابزارهایـی کـه در خدمـت ایـن گمنامـی قـرار می‌گیرنـد آشـنا شـدیم.

بـا توجـه بـه ایـن نکتـه کـه ایـران بـا رمزآنارشیسـی بـه صـورت سـازمان یافتـه، تشـکیلاتی و ایدئولوژیـک مواجـه نیسـت و کنتـرل گسـترش ابزارهای مربوطـه بـه نظـر چنـدان دشـوار بـه نظـر نمی‌آیـد پیشـنهاد می‌شـود اطلاع‌رسـانی عمومـی و آگاه‌سـازی قشـر نخبگانـی جامعـه در زمینـه تعارض‌هایـی کـه رمزآنارشـی در جامعـه ایجـاد می‌کنـد در دسـتور کار قـرار گیـرد. زیـرا از طرفی شـاهد گسـترش برخـی ابزارهـای رمزآنارشیسـتی در جامعـه هسـتیم (ماننـد ابزارهـای گمنامـی از جملـه فیلترشـکن‌ها) و از طـرف دیگـر شـاهد هسـتیم مـردم و حتـی بعضـا نخبـگان نسـبت بـه عـوارض ایـن ابزارهـا آگاهـی چندانـی ندارنـد.

مطالعـه روی ویژگی‌هـای امنیتـی و فرهنگـی رمزآنارشیسـم بـا مولفه‌هـای سـازنده تمـدن اسـلامی-ایرانی می‌توانـد در بـازی بـه ظاهـر باختـی کـه

رمزآنارشی علیه دولتها و امنیت ملی حاکمیت‌ها ایجاد می‌کند با امتیاز مثبت و تبدیل تهدید به فرصت ظاهر شود. در حالت کلی شاید بتوان گفت هر چند رمزآنارشیسم به دلیل مبانی آن قرابتی با مبانی حاکمیتی ما ندارد ولیکن شاید برخی ابزارهای آن بتواند به صورت کاربردی مورد استفاده ما قرار گیرد. مثلا مطالعه در مورد طراحی سازوکارهای رمزآنارشیستی که بتواند مستکبرین را در اعمال تحریم ایران ناتوان سازد و برخی ابزارهای آنها را مختل کند باید در برنامه‌های آتی ملی گنجانده شود و مثلا باید بررسی شود که آیا می‌توان از رمزارزهای موجود در جهت دورزدن تحریم‌ها (حداقل به صورت جزئی) بهره برد یا خیر.

منابع



[1] https://en.wikipedia.org/wiki/Crypto-anarchism#Motives
[2] https://www.activism.net/cypherpunk/crypto-anarchy.html
[3] http://www.cryptolaw.org/cls2.htm#uk
[4] http://www.cryptolaw.org/cls2.htm#iran
[5] http://www.cryptolaw.org/cls2.htm#Egypt
[۶] فقط برای تفریح، نویسنده: لینوس تروالدز، مترجم: جادی
https://linuxstory.ir/chapters/road_ahead.html
[7] https://en.wikipedia.org/wiki/2019_Turkish_offensive_into_north-eastern_Syria
[8] https://finmag.ir
شورشیان-سوری-برای-قوی-کردن-خود-از-رمز-ار/
[9] https://cryptonews.com/news/how-many-bitcoins-does-satoshi-have2487-.htm
[10] https://akhbararz.com/
پلیس-هند-ممنوعیت-ارز-دیجیتال-بیت-کوین/
[11] https://bitmessage.org/wiki/
[12] http://webexpress.ir/News/753
[13] https://www.bloomberg.com/news/articles/23-08-2012/the-skype-killers-of-belarus

csri.majazi.ir

حـوزه فضـای مجـازی بـه انـدازه انقـلاب اسـلامی اهمیـت دارد. ایـن فضـا مثـل یـک رودخانـه پـر از آب و خروشـان اسـت کـه مـی آیـد و دائمـاً هـم بـر آب آن افـزوده و خروشـان تـر مـی شـود. اگـر مـا بـر ایـن رودخانـه تدبیـر کنیـم و برنامـه داشـته باشـیم، زه‌کشـی کنیـم و هدایـت کنیـم ایـن رودخانـه را تـا بـه سـد بریـزد، می‌شـود فرصـت. اگـر رهایـش کنیـم و برنامـه‌ای بـرای آن نداشـته باشـیم می‌شـود یـک تهدید.

csri.majazi.ir