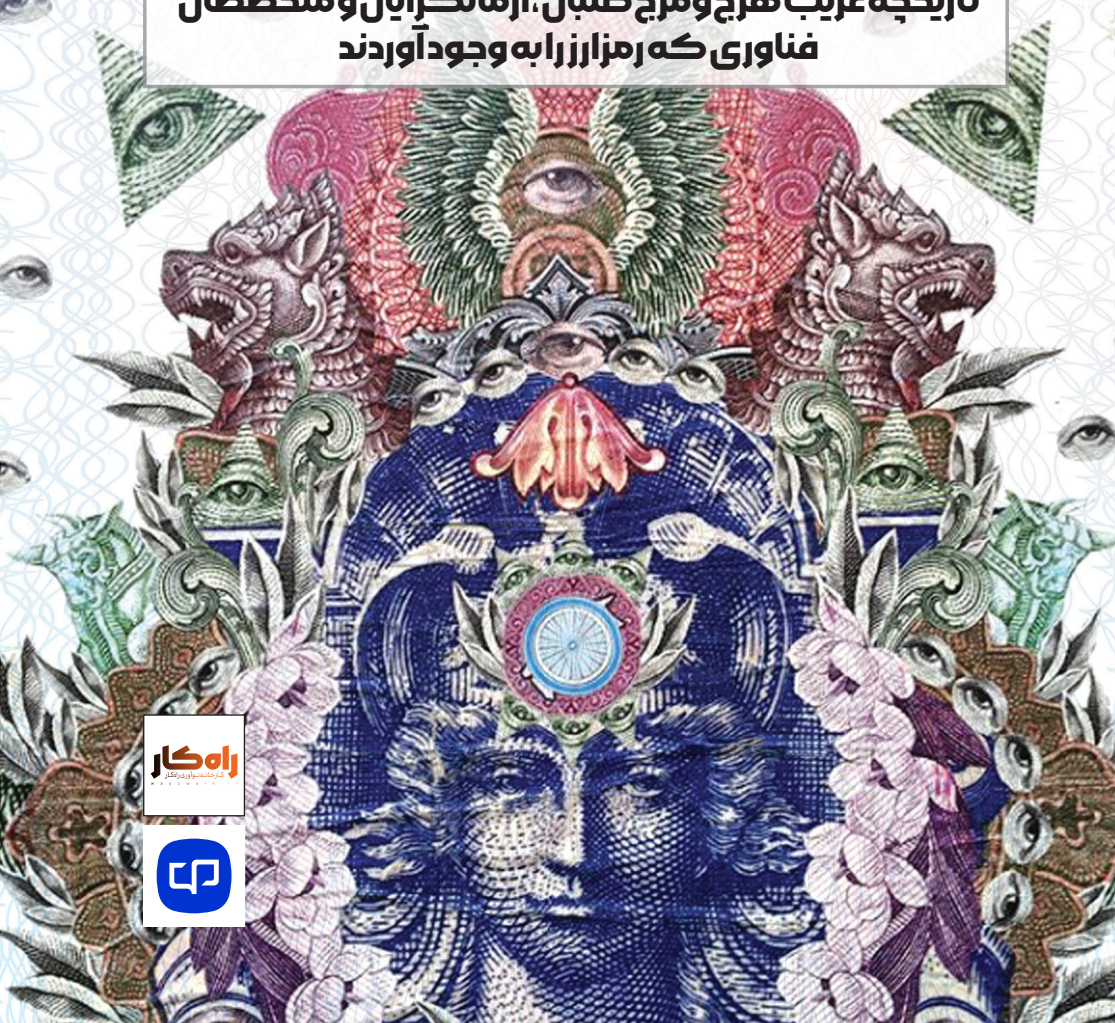
پول نقد دیجیتال

فین برونتون

مترجم: علی قربان‌زاده

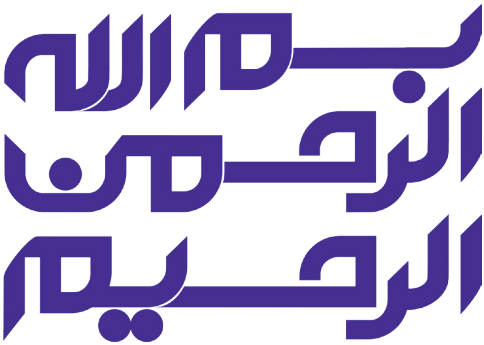
چاپ سوم

تاریخچه غریب هرج و مرج طلبان، آرمانگرایان و متخصصان فناوری که رمزارز را به وجود آوردند



راه کار

انتشارات راه پرداخت


بسم الله
الرحمن
الرحيم

The mark of responsible forestry
FSC® C009732

سرشناسه : برانتون، فین / Brunton, Finn
عنوان و نام پدیدآور : پول نقد دیجیتال: تاریخچه غریب هرج و مرج‌طلبان، آرمانگرایان و متخصصان فناوری که رمزارز را به وجود آوردند
نویسنده : فین برونتون
مترجم: علی قربان‌زاده
مشخصات نشر : تهران: راه‌پرداخت، ۱۴۰۰
مشخصات ظاهری : ۲۲۸ ص.؛ ۱۴/۵×۲۱/۵ س‌م
شابک: ۹۷۸-۶۲۲-۹۷۲۲۰-۷-۷
وضعیت فهرست نویسی : فیپا
یادداشت : عنوان اصلی : Digital cash : the unknown history of the anarchists, utopians, and technologists who created cryptocurrency ,2019.
عنوان دیگر : تاریخچه غریب هرج و مرج‌طلبان، آرمانگرایان و متخصصان فناوری که رمزارز را به وجود آوردند
موضوع : ارز مجازی
موضوع: Digital currency
موضوع : بیت‌کوین
موضوع : Bitcoin
شناسه افزوده : قربان‌زاده، علی، ۱۳۷۵-، مترجم
شناسه افزوده : والی، مینا، ۱۳۶۳
شناسه افزوده : سرافرازی، قاسم، ۱۳۶۶-، ویراستار
رده بندی کنگره: HG۱۷۱۰
رده بندی دیویی : ۳۳۲/۱۷۸
شماره کتابشناسی ملی : ۷۳۲۷۵۰۰

پول نقد دیجیتال

فین برونتون

مترجم: علی قربان‌زاده

چاپ سوم

تاریخچه غریب هرج و مرج طلبان، آرمانگرایان و متخصصان فناوری که رمزارز را به وجود آوردند

راه کار

عنوان: پول نقد دیجیتال
ناشر: راه‌پرداخت
نویسنده: فین برونتون
مترجم: علی قربان‌زاده
ویراستار ارشد: مینا والی
ویراستار محتوایی: قاسم سرافرازی
ویراستار فنی: یلدا شایسته‌فر
بازبینی نهایی متن: رضا قربانی
صفحه‌آرا: علیرضا کیوان
ناظر چاپ: قادر شهبازی
نوبت چاپ: سوم ۱۴۰۴
شمارگان: ۱۰۰ نسخه
شابک: ۹۷۸-۶۲۲-۹۷۲۲۰-۷-۷
تلفن: ۰۲۱-۴۴۴۴۳۹۶۶
دورنگار: ۸۹۷۸۴۹۰۲
ایمیل: info@way2pay.press
وب‌سایت: way2pay.press
لیتوگرافی: هنر اشکان
چاپ و صحافی: واژه

نشانی فروشگاه انتشارات راه‌پرداخت: تهران، جنت‌آباد جنوبی، خیابان لاله غربی، روبه‌روی پاساژ سمرقند، خیابان حدیث، کوچه حدیث دوم، پلاک ۸

way2pay.press w2ppress.ir way2paypress

فهرست

یادداشت ۱۱

[یادداشت ناشر]

بیت‌کوین و دیگر رمزارزها داستان ناگفته‌ای دارند که کتاب «پول نقد دیجیتال» برای اولین‌بار آن را روایت می‌کند. این روایت به فراتر از تاریخچه مرسوم ارزهای دیجیتال می‌پردازد و تلاش‌هایی که به خلق بیت‌کوین منجر شد را مرور می‌کند. بسیاری تصور می‌کنند بیت‌کوین یک فناوری انقلابی است که تاریخچه‌ای ندارد؛ در حالی که واقعیت چیز دیگری است. تاریخچه بیت‌کوین به سال‌های ابتدایی قرن بیستم بازمی‌گردد و حدود ۱۰۰ سال است که آرمان‌گراهای دنیای فناوری و آنارشیست‌ها با ایده‌هایشان راهی را پیموده‌اند که به خلق بیت‌کوین منجر شده است. ایده‌هایی مانند حفظ حریم خصوصی، کاهش قدرت دولت‌ها، دنیای آخرالزمانی و ساختن جهانی رؤیایی در این کتاب مرور می‌شوند و نویسنده به‌خوبی توضیح می‌دهد که چطور این ایده‌ها به خلق بیت‌کوین منجر شد.

در این کتاب قصه‌های زیادی از گروه‌های گوناگون در طول ۱۰۰ سال گذشته مرور می‌شود؛ برخی از آنها شبیه داستان‌های علمی-تخیلی هستند و باورکردنی نیستند! و سخت است قبول کنیم که پشت بیت‌کوین و فلسفه آن چنین آدم‌هایی وجود داشته‌اند. سؤالی که نخ تسبیح همه گروه‌هایی است که در کتاب به آنها پرداخته شده، این پرسش است: ما چگونه می‌توانیم به هم اعتماد کنیم و از انواع دیگری از پول استفاده کنیم؟ چه چیزی اشیای دیجیتال را ارزشمند می‌کند؟ چگونه یک ارز خودش را به ما ثابت می‌کند؟ چه چیزی یک موجودیت دیجیتال را معادل پول نقد می‌کند؟ چیزی که می‌تواند خلق، اما نمی‌تواند کپی شود!

«فین برونتون»، استاد دانشکده رسانه، فرهنگ و ارتباطات دانشگاه نیویورک است. او پیش از این،

کتاب «اسپم: تاریخ در سایه اینترنت» را نوشته است. درباره کتابی هم که اکنون در دست شماست، باید بگویم که کتابی به‌شدت سهل و ممتنع است؛ با اینکه روایتی جذاب و پیوسته دارد، ولی تعدد ارجاع‌های آن ممکن است خوانش کتاب را سخت کند. کتاب توسط انتشارات دانشگاه پرینستون در ژوئن ۲۰۱۹ منتشر شده است. بنابراین باید در تمام مدت توجه داشته باشید که با یک کتاب عامه‌پسند بازاری سروکار ندارید؛ بلکه یک کتاب پژوهش‌محور دانشگاهی در دست گرفته‌اید که قرار است شما را با بخش‌هایی از دنیای ارزهای دیجیتال آشنا کند که کمتر جایی ممکن است چیزی درباره آن بشنوید.

نکته مهم کتاب این است که یادآوری می‌کند پدیده‌ای مانند بیت‌کوین یک پدیده سطحی و موقتی نیست؛ بلکه فلسفه و تلاش‌های اجتماعی سنگینی پشت آن وجود دارد؛ نکته مهم دیگر نیز این است که این کتاب بار دیگر اهمیت مفهوم پول را یادآوری می‌کند؛ به طرز عجیبی با وجود اهمیت پول در زندگی روزمره تلاش برای ندیدن این مفهوم در دنیای فلسفه و جامعه‌شناسی جالب است.

ظهور پول‌ها (و شاید ارزها و ابزارهای پولی و هر واحد اندازه‌گیری ارزش) مانند بیت‌کوین به یکباره ما را متوجه دانش اندک‌مان درباره پول کرد. اهمیت کتاب حاضر در این است که به‌خوبی نشان می‌دهد ارزهای دیجیتال نه با ابزارهای فناورانه؛ بلکه با دیدگاه‌های فلسفی و اجتماعی شروع شده‌اند.

ذکر این نکته درباره متن کتاب اصلی هم لازم است که کتاب متن سختی دارد و همین موضوع ترجمه کتاب را دشوار کرد؛ لازم است از مترجم کتاب؛ آقای علی قربان‌زاده تشکر کنم که سخت‌گیری‌های ما در انتشارات راه پرداخت را قبول کرد و اگر همکاری صمیمانه او برای چند بار ترجمه و بازنویسی کتاب نبود این کتاب به این نقطه نمی‌رسید. آقای قاسم سرافرازی و خانم یلدا شایسته‌فر نقش مهمی در تولید کتاب داشتند. سرکار خانم مینا والی در بازنویسی کتاب و روان‌شدن آن نقش بارزی داشت و آقای علیرضا کیوان هم با حوصله مسئولیت صفحه‌آرایی کتاب را به‌دوش گرفت.

لازم است از حامی محترم کتاب یعنی تیم بیت‌راه تشکر کنم؛ امیدوارم در آینده نزدیک شاهد رشد کسب‌وکارهای نوآورانه‌ای باشیم که در زمینه‌های نوین مالی در ایران خلق شده‌اند. قطعاً با رشد نوآوری و فناوری‌های مالی شاهد توسعه بیش از پیش ایران خواهیم بود.

در این مسیر ما در گروه راه پرداخت و به‌طور خاص در انتشارات راه پرداخت تلاش می‌کنیم زمینه نشر دانش را فراهم کنیم و امیدواریم این تلاش‌ها مفید باشد.

رضا قربانی / انتشارات راه پرداخت

مقدمه

جریان موجود

این کتاب، داستان ناگفته پول دیجیتال و افرادی را تعریف می‌کند که به‌دنبال ساختن آن بودند. هدف بعضی از آنها زمین‌زدن دولت‌ها و ملت‌ها و ایجاد آرمانشهری رمزنگاری‌شده بود و هدف برخی دیگر این بود که با از میان رفتن نظم جهانی، پاداشی دریافت کنند، برخی نیز می‌خواستند ماشینی را پدید بیاورند که بتوانند با آن تا ابد زندگی کنند. عوامل به وجود آمدن رمزارزها از این قرار اســـت: پیش‌نیازها، فناوری‌ها و خرده‌فرهنگ‌ها، ایده‌ها، خیال‌ها، داستان‌ها و مدل‌های آینده‌ای که پشت اولین معرفی بیت‌کوین وجود داشت.

بحث اصلی این کتاب با بیان این حقیقت آغاز می‌شود که به جای پول الکترونیکی که کلی‌تر است، قرار است داستان پول دیجیتال را تعریف کنیم. دیجیتالی کردن پول، یعنی چیزی را ایجاد کنیم که به‌راحتی در شبکه‌های کامپیوتری معامله شود و بررسی و تایید هویت آن آسان باشد، اما نتوان آن را جعل یا تکثیر کرد، همچنین باید اطلاعاتی را در مورد هویت و ارزش خود به همراه داشته باشد، ولی در مورد چگونگی استفاده و کسی که از آن استفاده می‌کند، اطلاعاتی ندهد.

این مجموعه شـــرایط، ظاهرا متناقض و غیر ممکن به نظر می‌رسند؛ پول دیجیتال مورد نظر ما باید موجود باشد، اما کمیاب؛ منحصر به‌فرد و ناشناس باشد، اما قابل شناسایی و مطمئن؛ به‌راحتی منتقل شود، اما قابل تکثیر نباشد و تمامی این ویژگی‌ها باید در قالب فناوری‌هایی ارائه شود که قابلیت تکثیر بدون هزینه، فوری و بدون هیچ ایرادی را داشته باشند.

استدلالی که برای شما می‌آورم این است که داستان پول دیجیتال از طریق آشنایی با تاریخچه پول بهتر درک می‌شـــود. از کجا می‌توان فهمید که پول خاصی اعتبار دارد (یعنی می‌توان آن را به شخص دیگری داد و دیگران آن را از شـــما قبول می‌کنند و می‌توان آن را پرداخت و دریافت کرد؟ در کل در مورد ارزش پول حرف می‌زنیم). ایـــن میکروتکنولوژی فرهنگی پیچیده، این ابزار اجتماعی از باورهای قدرتمند و غالبا انتزاعی در مورد ماهیت کنونی و آتی اشـــیا نشات می‌گیرد. این موارد که در فصل اول کتاب به تفصیل بررسی خواهند شد، عبارتند از: پیش‌بینی، شـــرط‌بندی و امید به اینکه نوع خاصی از پول برای پرداخت مالیات پذیرفته شود، نوع دیگری از پول با ورود فلزات یا مواد کمیاب به بازار بی‌ارزش نشـــود و شبکه هدایا، تعهدات و تقابل‌ها در جامعه باقی بماند.

حال از دیدگاه عملی به ارز، پول نقد و سکه نگاه کنید. ارزش یک نوع خاص از پول را چگونه می‌توان تشـــخیص داد؟ چگونه از هویت آن اطمینان حاصل کرده و چگونه اعتبار آن را تایید

می‌کنید؟ می‌توان این موارد را با بررسی شکل‌پذیری، رسانش گرمایی و صدای سکه فهمید؛ مثلا با گاز گرفتن سکه، مشاهده سرعت ذوب‌شدن یخ روی آن، تست پینگ و بررسی صدای آن پس از ضربه. در مورد چای می‌توان از طریق بررسی عطر و وزن آن این کار را انجام داد؛ در مورد سیگار از طریق برند و طرح آن و در مورد اسکناس، اعتبارنامه یا چک مسافرتی با بررسی شماره سریال، امضا، ضخامت کاغذ، نخ‌های امنیتی و واترمارک آن. ما همه این موارد را در قالب آموزش، عادت و تجربه یاد گرفته‌ایم. با در نظر داشتن این موارد، چگونه می‌توان ارز دیجیتال تولید کرد؟

می‌خواهم شما را متقاعد کنم که پول دیجیتال را باید بخشی از چالش ارزشمندسازی داده‌های دیجیتال در نظر بگیریم. وقتی از نقطه‌نظر اعتبار، مالکیت، قطعیت و گواه اشیای دیجیتال به پول دیجیتال نگاه کنیم، بسیاری از جنبه‌های گیج‌کننده آن به خودی خود حل می‌شود. همان‌گونه که تاریخچه موجود در این کتاب نشان خواهد داد، دو پروژه مشابه مالکیت دیجیتال و پول دیجیتال همیشه در کنار یکدیگر ظاهر می‌شوند؛ از ساخت فروشگاه‌های اطلاعاتی گرفته تا بررسی اظهارنامه‌های ناشناس، اعتبارسنجی کار و زمان و مبارزه با جعل و تکثیر. به عبارت دیگر، این کتاب تاریخچه‌ای است از اینکه داده‌ها چگونه عملا و مجازا به پول تبدیل شدند.

بحث دیگری که مطرح می‌کنم این است که تاریخچه پول دیجیتال می‌تواند مثال واضحی از به‌کارگیری پول و فناوری برای پیش‌بینی آینده باشد. این پیش‌بینی‌ها نوعی استدلال، پیش‌خرید، شرط‌بندی، هم‌پیمان‌شدن و در دست گرفتن قدرت حال حاضر است. در این کتاب چند پروژه پولی آرمانی و تئوری کوچک و بزرگ را توصیف خواهم کرد. هر کدام از آنها دوره زمانی، داستان‌ها، ماجراهای تاریخی و آتی و فناوری‌های مرتبط خود را دارند (منجمدسازی، انواع رمزنگاری، شهرهای زیر آب) که ارزش خود را از آن می‌گیرند. همه آنها با مشکل انتقال معنی و ارزش نیز روبه‌رو هستند؛ زیرا برای افراد خارج از گروه‌های کوچک و همگن به‌وجودآورنده این پول‌ها قابل درک نیستند. مثلا مردان آمریکایی سفیدپوست به نسبت جوانی که سابقه مهندسی یا ساخت نرم‌افزار داشتند، بیشترشان در ساحل کالیفرنیا زندگی می‌کردند، باورهای سیاسی مشترکی داشتند و از طریق لیست‌های ایمیلی و شرکت در رویدادها با یکدیگر آشنا شده بودند [از بیت‌کوین استقبال کردند، ولی دیگر گروه‌ها مفهوم بیت‌کوین را به‌راحتی نپذیرفتند].

تمامی ســـازندگان پول که در این کتاب آمده‌اند، شـــرایط تاریخی خاص خود را داشته‌اند؛ تکنوکرات‌هایی که نمودار پیشـــرفت را روی کاغذ گراف اتود می‌زدند، سایفرپانک‌هایی که به دولت‌های دیکتاتور آسیب می‌زدند، کســـانی که به‌دنبال بهبود شرایط زندگی انسانی بودند[1] و بدن‌های منجمدشان مانند کشتی‌های فرعون به تاریخ پیوست، آزادی‌خواهان و آگوریست‌ها[2] و هرج‌ومرج‌طلبان کاپیتالیست[3] و خرده‌ناسیونالیست‌ها[4] و عینیت‌گرایان[5] و اقتدارطلبانی که منتظر فروپاشی هســـتند تا تصمیمات و باورهای خود را وارد جامعه کنند و قدرت را به دست بگیرند. تلاش آنها برای آینده سفت‌وســـخت بود، اما به جدیت در زمان حال نیاز داشت؛ از به‌کارگیری جوامع اولیه تا طراحی کوپن‌های ایده، جمع‌آوری تسلیحات به امید آماده‌شدن برای پایان دنیا، همه و همه نیازمند ایجاد یا پذیرش ارزهای تئوری و پول دیجیتال بود. آنها چارچوب زمانی مشترکی با طرفداران پول فلزی قرن هفدهم داشـــتند که هدف‌شان «توضیح‌دادن و اثر گذاشتن، قانع‌کردن و رسیدن به نیروی جنبش بود؛ بنابراین اگر می‌توانستند مخاطبان خود را به عمل‌کردن متقاعد کنند، می‌توانستند آینده را به دست بیاورند.»

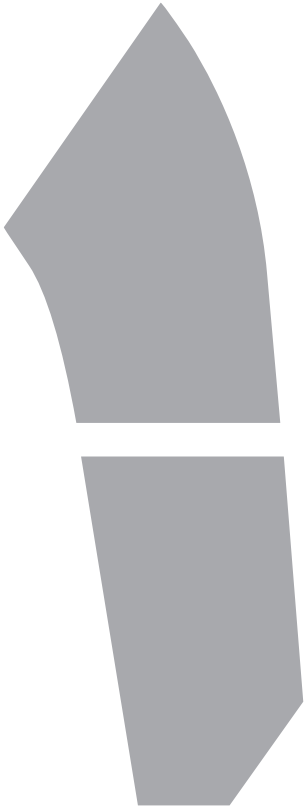
هدف این کتاب را می‌توان تنها در یک جمله جمع‌بندی کرد؛ «وجه رایج» عبارتی است که در دنیای ارز برای پولی استفاده می‌شود که عموما برای معامله پذیرفته شده و از شخصی به شخص دیگر منتقل می‌شود. پول موجود در جیب شما به این دلیل «وجه رایج» محسوب می‌شود که در جامعه پذیرفته شده است. این پول را به هر کسی که بدهید آن را قبول می‌کند و در نهایت می‌توان برای پرداخت مالیات یا وام از آن استفاده کرد. «ارز» بودن و قابلیت انتقال آن در حال حاضر به این دلیل است که آینده‌ای برای آن وجود دارد. «وجه رایج» در علوم دیگر نیز دیده می‌شود که در ساخت سخت‌افزار کامپیوتری و ایجاد پول دیجیتال مورد استفاده قرار می‌گیرد. این کتاب تا حدودی به این موارد نیز می‌پردازد. «وجه رایج» در نهایت ما را به یاد گذر زمان می‌اندازد؛ گذر زمان حال بین گذشته‌ای که به تاریخ پیوسته و آینده مطلوب، پیش‌بینی‌شده یا هراسناک. داستان پول دیجیتال در محل تقاطع سه حوزه قرار دارد؛ «مســـائل اجتماعی مربوط به پول»، «تاریخ فناوری و کامپیوتر» و «احساس ما نسبت به شرایط گذشته و آینده».

1. Extropians
2. Agorists
3. Anarcho-capitalists
4. Micronationalist
5. Objectivists

بنابراین این کتاب دو هـــدف دارد. با مطالعه ایـــن کتاب از اجزا، مفاهیـــم و ایده‌های پول دیجیتال (از آزمایش‌های دهه ۱۹۸۰ گرفته تا ایجاد بیت‌کوین) یک ذهنیت پیدا خواهید کرد. به این ترتیب چگونگی به‌کارگیری داده‌ها و توافق‌ها و تلاش‌هایی را که طی این فرایند صورت گرفت (به‌خصوص نظارت بر پرداخت‌ها و تراکنش‌ها) خواهید دید. همچنین تاریخچه‌ای از پول‌های آزمایشی را خواهید دید که تا نزدیکی موفقیت رفتند، ولی در نهایت شکست خوردند. این موضوع از تاریخچه ارزهای آرمانی، نمونه‌های اولیه، تصاویر، داســـتان‌ها، سیستم‌های کاربردی و طراحی‌های مربوط به آینده که پیش‌تر «تکنیک‌های آینده»[1] محســـوب می‌شدند، فراتر خواهد رفت. امیدوارم دانش شما را در رابطه با ارزها (دیجیتال و غیردیجیتال) و همچنین محاسبات افزایش دهم و با کمک پول، ماشین و داســـتان به شما نشان دهم چه انتظارات قابل توجهی از آینده وجود داشته و دارد.

با در نظر گرفتن تمامی این موارد امیدوارم این کتاب تجربه خوبی برای شما به همراه بیاورد؛ مجموعه‌ای از سیســـتم‌های مختلف آرمانی، آینده‌نگری‌هـــای خیال‌آمیز و زندگی تجربی به انضمام طرح مختصری از شخصیت‌ها و شیوه‌هایی که ممکن است بعضی از آنها لجبازانه، خطرناک و حتی زشـــت به نظر برســـند. در این مجموعه، موارد زیر را بررسی خواهیم کرد: کشورهای پیشرو و چالش‌های محاسباتی، سیســـتمی مالی که سازنده‌اش را دوباره به زندگی برگرداند، کالاهایی که حکم پول نقد را داشـــتند، پروژه زانادو[2]، پـــول کاغذی، ارزش عینی، وحشت‌زدگی ارزی، سفینه‌های شـــخصی، تصادفی‌بودن همگانی، تکنوکرات‌های قهرمان آمریکایی، رمزنگارهای مسلمان، نواحی خودمختار برون‌مرزی، گریس هاپر[3] در حال بازی بســـکتبال، نقره آزادی‌خواهان، طرح‌های ژئودزیک، ماشـــین زمان خراب، کوپن‌های ایده، امضاهای جعلی، دیواری از لامپ لاوا و مخزنی پر از سر منجمد انسان‌ها.

1. Techniques of futurity
2. Xanadu hypertext
3. Grace Hopper



فصل اول

پول‌های فرضی

کار خود را با پروژه‌ای آرمانی در ایالات متحده و در قلب رکود بزرگ، با طرحی عجیب برای کنترل قاره آمریکای شمالی به‌عنوان یک واحد صنعتی آغاز می‌کنیم. با صعود و سقوط تکنوکراسی یاد می‌گیریم پول یک فناوری برای مدیریت زمان (آینده، اعتقادات و پیش‌بینی‌ها) است و الگویی از جامعه را شامل می‌شود. از میان اشکال ناپایداری که پول به خود گرفت، «ارزهای معاملاتی» نیازمند توجه ویژه هستند. آنها مانند سیستمی برای رویکردهای آرمانی عمل می‌کنند (کازموگرام[1]؛ مفهومی که در ادامه کتاب به‌تدریج توضیح داده می‌شود).

تکنوکرات

«هاوارد اسکات» دو نوع لباس می‌پوشید. در دهه ۱۹۲۰ مهندس بود. در دهکده گرینویچ نیویورک پوتین سنگینی به پا داشت، شلوار مخصوص سوارکاری و کاپشن چرم می‌پوشید، دستمال‌گردن گل‌دار قرمز می‌بست، کلاه لبه‌دار به سرش می‌گذاشت و خط‌کش مهندسی و نقشه‌های ساختمان به همراه داشت. این لباس مخصوص این بود که در محل ساخت آسمان‌خراش یا باند فرودگاه یا بازدید از یک سد، آفتاب به چشمانش نتابد. «آین رند»[2] هنوز نوجوانی بود که در روسیه زندگی می‌کرد و رمان او به نام «سرچشمه»[3] در سال ۱۹۴۳ منتشر شد، اما اسکات حتی قبل از چاپ‌شدن آن کتاب شبیه «هاوارد رورک»، قهرمان آن داستان، لباس می‌پوشید که آماده بود تا کاپشنش را دربیاورد و با دستگاه «جک همر» در معدن گرانیت مشغول به کار شود. البته او چه از نظر طرز فکر و چه در عمل شباهتی به رورک نداشت.

هاوارد اسکات شخصی واقعی بود، اما نقش شخصیت دیگری را بازی می‌کرد؛ او نه مهندس بود، نه معمار. هیچ چیزی نداشت که بخواهد با خط‌کش‌اش آن را محاسبه کند. او شخص عجیبی بود که همه اهل محل او را می‌شناختند. کسی بود که در مورد اقتصاد دستوری نطق می‌کرد و در کافی‌شاپ‌های دهکده در مورد اهمیت توجیه عقلانی زندگی و افزایش بازده صنعتی سخنرانی می‌کرد.

در دهه ۱۹۳۰ با گسترش رکود در سراسر کشور و تعطیل‌شدن کارخانه‌ها، خالی‌شدن میادین و شهرها و سرریز شدن مهاجران در خیابان‌ها و راه‌آهن، لباس اسکات نیز عوض شد؛ کت و

1. Cosmogram
2. Ayn Rand
3. The Fountainhead

شلوار خاکستری شیکی می‌پوشید و کراوات آبی می‌زد. او دیگر مهندس خشنی نبود که انگار تازه از سکوی نفتی آمده است؛ بلکه مردی منطقی و رسمی بود که نمایندگی شرکتش را بر عهده داشت. لباسی که او به تن کرده بود لباس تکنوکالچر بود؛ برنامه صنعتی مشخصی که قرار بود با جنبش سیاسی خود یعنی تکنوکراسی آن را به واقعیت تبدیل کند.

ایالات متحده آن زمان از نظر نقدینگی با مشـــکل مواجه بود. ورشکستگی و فرار بانک‌ها باعث شـــده بود مردم پول‌هایشـــان را داخل «جوراب، گاوصنـــدوق، صندوقچه، زیر زمین، دستشویی، آســـتری کت، پالان اســـب، توده زغال و تنه درخت» پنهان کنند. می‌توان مورد مشـــابهی را در خط اول کتاب «زندگی اجتماعی پول ـ ۲۰۱۴» از «نایجل داد» مشاهده کرد. او می‌نویسد: «در یونان پول منجمد وجود داشت.» در سال ۲۰۰۸-۲۰۰۷ بحران اقتصادی از کنترل خارج شد و مردم پول‌های خود را در «فریزر، جاروبرقی، کیسه‌های آرد، ظرف غذای حیوانات خانگی، لابه‌لای تشک و زیر موزاییک کف زمین» جاسازی می‌کردند. در سال ۱۹۳۳ روزولت، ریاست‌جمهوری را به دســـت گرفت و یک روز را برای بانک‌ها تعطیلی اضطراری اعلام کرد که باعث شد جریان نقدینگی از قبل هم کندتر شود (به این ترتیب برای خودش زمان خرید تا نوعی بیمه سپرده فدرال را تصویب کند).

صدها شـــهر کوچک و بزرگ گواهی‌های مختص خـــود را صادر و با اســـتفاده از منیزیم سکه‌هایی ضرب کردند. مغازه‌های دیترویت با شانه‌های تخم‌مرغ و عسل، مبادله کالا به کالا انجام می‌دادند، مغازه‌داران، پزشـــکان و داروخانه‌ها به مشتریان خود نسیه می‌دادند. روزنامه دانشجویی Daily Princetonian با مشارکت بازرگانان پرینستون ۵۰۰ دلار ارز مخصوص خود را به‌صورت ۲۵ سنتی منتشر کرد. رقصنده‌های تالار رزلند نیویورک (به قول آهنگ راجرز و هارت «رقصنده‌های ۱۰سنتی») حاضر بودند به جای ۱۰ ســـنتی از مشتری‌ها برگه IOU[1] بگیرند؛ البته باید دفترچه حساب خود را نشان می‌دادند تا ثابت کنند پول دارند. بوکسورهای آماتوری که در تورنمنت‌ها شرکت می‌کردند، حاضر بودند سیگار، شانه یا کیسه‌ای سیب‌زمینی را به جای دستمزد خود قبول کنند. حمل‌ونقل عمومی نیز با ســـکه پنج‌سنتی کار می‌کرد؛ در نتیجه خوشگذران‌های شیک‌پوش و کسانی که رفت‌وآمد زیادی داشتند، دستگاه‌های اتومات منهتن را دوره می‌کردند تا از آن پول خرد بیرون بکشند.

1. I owe you (من به شما بدهکارم)

امکان نداشـــت زمان‌بندی بهتر از این برای تکنوکراســـی وجود داشته باشـــد. اسکات و دستیارانش به شرایط بلاتکلیفی مالی عمیقی قدم گذاشتند که آرمانشهری از اقتصاد علمی به نظر می‌رسید و اگر قدرت می‌یافت، می‌توانست رکود بزرگ را به پایان برساند. آنها به مدت چند سال توانستند توجه رسانه‌های ایالات متحده را به خود جلب کنند، بعضی از این رسانه‌ها جدی بودند و بعضی دیگر آنها را مسخره می‌کردند که به هر حال همگی تبلیغ محسوب می‌شدند. نقطه اوج آنها وقتی رقم خورد که ایالات متحده بیش از هر زمان دیگری به ســـازندگی گرایی و ماشین‌پرستی دهه ۱۹۲۰ شوروی نزدیک شد. آنها نسخه آمریکایی نظریه‌پرداز بلشویک حوزه مدیریت علمی الکسی گاستو و همراهانش بودند و هدف‌شان این بود که با استفاده از زیست ـ فیزیک و کرونوفوتوگرافی؛ جامعه، مردم و خطـــوط کارخانه‌ها را از نو طراحی کنند و تمدنی علمی ـ تخیلی از مینیمالیسم انبوه به وجود بیاورند که انسان‌ها اجزای بی‌عیب‌ونقص و دائمی موتور آن باشند. البته تکنوکراسی بر خلاف بلشویک‌ها خودش را «فراتر از سیاست» معرفی می‌کرد و ادعا داشت از چارچوب مهندسی کاربردی و مهم‌تر از همه «علم» نشات می‌گیرد. شعار آنها این بود: «حکومت علمی و کنترل جامعه توسط قدرت فناوری».

برای نجات دموکراسی آمریکا از دست رکود بزرگ، لازم بود که افراد، ماشین‌ها، مواد و پول ملت به شکلی اجباری به کار گرفته شود. این برنامه‌ای بود که «کمونیسم جنگی» بلشویک‌ها را تحقیر می‌کرد و قدرتمند بودن آمریکایی‌ها و عملکرد مهندسی آنها را به همگان نشان می‌داد. تکنوکرات‌های دوآتشه بازو بندهایی می‌بستند و سنجاق‌هایی به لباس خود می‌زدند که روی آنها «موناد»[1] (نماد یگانگی، بـــه معنی وحدت مصرف و تولید) وجود داشـــت و به یکدیگر سلام شبه‌نظامی می‌دادند. آنها به‌صورت گروهی با خودروها و موتورسیکلت‌هایشان حرکت می‌کردند، گروه جوانان آنها «فاراد» نام داشـــت که تعدادی نیروی علاقه‌مند و جدید عضو آن بودند. نام این گروه از واحد اندازه‌گیری ظرفیت خازن‌های الکتریکی الهام گرفته شده بود.

هدف آنها ایجاد اقتصاد پساکمیابی[2] به نام تکنوکراســـی بود که ایالات متحده، کانادا و در برخی موارد مکزیک را شامل می‌شد و مهندسان ارشد به‌صورت استبدادی آن را اداره می‌کردند. هر فعالیت سیاســـی، هنری، اخلاقی، اجتماعی، فکری و ســـرگرمی غیرضروری نیز کاهش

1. Monad
2. Post-scarcity economy

یافته یا به‌کلی قطع می‌شد. ضامن این دگرگونی، ارز جدیدی بود که مستقیما به انرژی متصل بود، واحد آن «ارگ»[1] بود و به‌صورت گواهی رسمی صادر می‌شد. اسکات در سال ۱۹۳۳ در مقاله‌ای با عنوان «فناوری سیستم قیمت‌گذاری را نابود خواهد کرد»[2] برای مجله هارپرز نوشت: «ارزش دلار (برای خرید انرژی) ممکن است هر روز تغییر کند، اما واحد کار یا گرما در سال ۱۹۰۰، ۱۹۲۹، ۱۹۳۳ یا ۲۰۰۰ ثابت می‌ماند. پولی که «ارزش عینی» داشته باشد، هم قابل اندازه‌گیری است و هم با اصول اجتماعی مطابقت دارد.»

بیایید نگاهی به ترفند «گواهی‌های انرژی» بیندازیم (که در آینده به روش‌های زیرکانه‌تری اجرا شد). این گواهی‌ها واقعی‌تر از دلار بودند؛ زیرا به «کار یا گرمای» موجود در جهان وابسته بودند. از همه نظر واقعی‌تر بودند، ولی وجود خارجی نداشتند؛ اما طبق برنامه‌ریزی‌های موجود قرار بود به وجود بیایند. نقاشی‌هایی از این گواهی‌ها ترسیم شده بود و با جزئیات قابل توجهی توصیف می‌شدند: «کاغذ دارای واترمارک و... به شکل قطعات باریکی که در دفترچه‌های مستطیلی کوچک جا شوند و به قدری کوچک باشند که بتوان به‌راحتی آنها را در جیب گذاشت». گواهی انرژی واقعی‌تر از دلار بود (اندوخته ارزشی و واحد محاسبه بهتر، برتر و بدون تغییر)؛ زیرا به آینده‌ای تعلق داشت که تمام جامعه به‌طور مناسب برای آن آماده شده بود. گواهی انرژی تکنوکرات‌ها که نه می‌توان آن را طرح پیشنهادی نامید، نه نمونه اولیه (به همراه همه طرح‌های پول فرضی دیگر که در این کتاب آمده است)، چیزی است که «جان ترش»، مورخ، آن را کازموگرام می‌نامد. کازموگرام در عین حال «علمی، هنری، فنی و سیاسی» است؛ چیزی است که طرحی از جهان و نقشه‌ای برای سازمان‌دهی زندگی و تنظیم جامعه مطابق با آن را شامل می‌شود.

نحوه انجام کارها در آینده

کتاب «جان ترش» تحت عنوان «ماشین رمانتیک: علم و فناوری آرمانی پس از ناپلئون» دوره زمانی سقوط ناپلئون در سال ۱۸۱۴ و پیروزی ناپلئون سوم در سال ۱۸۵۲ در فرانسه را بررسی می‌کند؛ وقتی ماشین، آثار علمی اثبات‌گرا، کمیت‌پذیری و صنعت، به سبک زندگی

1. Erg
2. Technology Smashes the Price System

تبدیل شدند و طرز تفکر رمانتیک را به وجود آوردند. او لحظه‌ای را توصیف می‌کند که مفاهیم علمی و فنی و اشیا، نقطه شروعی برای دانش تجربی جهان و همچنین اخلاقیات، دگرگونی‌های اجتماعی، زیبایی‌شناسی، ارزیابی جایگاه ما در تاریخ و لذت محض تجربیات شدند.

چنین استدلالی «ترش» را در جایگاه حساسی قرار می‌دهد تا در مورد چیزهایی صحبت کند که به‌صورت همزمان کارکردهای مختلفی داشتند؛ ساختمان‌های جدید، تقویم‌ها و طرح‌های سازمانی، دستگاه‌های نظام‌مند و چشم‌اندازهای عمومی مانند پانوراما و فانتازماگوریا[1]. همگی اینها نظم خاصی از جهان را توصیف می‌کردند؛ مجموعه‌ای از نظام‌ها و روابط، راهنمایی برای گذشته و آینده و اینکه رفتار فردی و اجتماعی ما باید چگونه باشد. هم انتزاعی بودند و هم عینی؛ بناهایی که می‌توان واردشان شد، مناظری که بر پایه فناوری کار می‌کنند و می‌توان از آنها لذت برد، نقشه‌ها و ابزارهایی که می‌توان اســتفاده کرد. او در مورد این اشکال مختلف می‌نویسد: «دلیل مهم تفاوت کازموگرام با گیتی‌شناسی[2] این است که در مورد موضوعی صحبت می‌کنیم که نتیجه آن کارکردها و مجموعه مقاصد مشخصی است که در کنار یکدیگر فهرست یا نقشه کاملی از جهان ارائه می‌کنند.» این اسناد و اشیا در قالب فناوری فرهنگی عمل می‌کنند.

کازموگرام شامل مواردی است که به جهان و جایگاه ما در آن نظم می‌دهند و نظامی از روابط، نقش‌ها و فعالیت‌هــا را در عملکرد خود جای می‌دهند. برای مثال می‌توان از پرستشــگاه‌ها، مناسک قوم دوگون[3] و ماندالای بودایی‌های تبت گرفته تا دایره‌المعارف، پروژه‌های علمی خاص و نقشه‌های راهنمای کتابخانه را نام برد. چیزی که کازموگرام را تعریف می‌کند، اهمیت آن در تاریخ جهان نیست؛ بلکه مجموعه نقش‌هایی است که ایفا می‌کند. از دید یک کاربر، کازموگرام زمان و مکان ما را مشــخص می‌کند (در چه زمانی و کجا هستیم؟)، سطوح هستی‌شناسی را معین می‌کند (چه چیزی حائز اهمیت اســت؟) و روش‌ها و الگوهایی را فراهم می‌کند (چه کاری باید انجام دهیم و درک‌مان چگونه باشــد؟)؛ همچنین ملاک‌هــا و معیارهایی را برای اعضای گروه‌ها تعیین کرده و روابط و به‌هم‌پیوستگی‌هایی را بین دسته‌بندی‌های مختلف ایجاد می‌کند (مهم و کم‌اهمیت؛ برتری و پستی؛ پاکی و ناپاکی). علاوه بر این، تصویری از جهانی ارائه می‌دهد که می‌توانست وجود داشته باشــد و با کمک مجموعه‌ای از روش‌ها این تصویر

1. Phantasmagoria
2. Cosmology
3. Dogon

را تثبیت می‌کند تا ما را برای تصمیم‌گیری در این جهان راهنمایی کند. در حقیقت کازموگرام نمونه‌ای از یک جهان هدفمند و پروژه‌ای آرمانی اســت که از طریق اشیا و نمادهای خاصی خودش را نشان می‌دهد.

نهایتا کازموگرام علاوه بر موارد ذکرشــده، زمان و تاریخ را برای کاربران خود سازمان‌دهی می‌کند، به‌خصوص آنچه در آینده رقم خواهد خورد؛ همچنین روش‌هایی را برای حفظ تاریخ و رسیدن به این آینده ارائه می‌کند و با استفاده از گیتی‌شناسی دینی، منطق مارکسیست قرن نوزدهم یا مقایسه نمودارهای قرن بیستم در مورد گذشته‌ها (بخش‌های مهم تاریخ) و آنچه در آینده رخ خواهد داد صحبت می‌کند. «حال» را از گذشته، آینده و شرایط احتمالی، تمییز می‌دهد و کمک می‌کند با توجه به زمانی که در آن قرار داریم، رفتار کنیم. این پروژه‌ای اســت که علم به آینده را در اختیار ما قرار می‌دهد.

پول‌های فرضی

گواهی‌های انرژی تکنوکراســی، کازموگــرام تمام‌عیاری بودند کــه کل جامعه و جهان را به‌صورت خلاصه دربر می‌گرفتند و بــرای جهانی ارزش قائل بودند کــه در آن بازده صنعتی از ماهیت و فعالیت تمام انسان‌های پیشــین مهم‌تر بود. این گواهی‌ها از سیستم حسابداری پیچیده‌ای برخوردار بودند (نوعی سیستم رده‌بندی ده‌دهی دیوئی اصلاح‌شده) که حامل وجه و خریدهای احتمالی او را از نظر وجودی در میان تمامی نقش‌ها، خدمات و محصولات موجود در هســتی قرار می‌داد. این گواهی‌ها برخی رفتارها را تایید و از برخی رفتارها نهی می‌کردند، همچنین نوعی برنامه زمانی محسوب می‌شدند؛ زیرا تمام گواهی‌های انرژی باید ظرف مدت دوساله «دوره کامل بار متعادل»[1] مصرف می‌شدند.

این چرخه دوســاله، نوعی تاریخ مصرف را به گواهی‌ها اضافه می‌کرد که باعث می‌شــد در تاریخ خاصی طبق برنامه ارزش خود را از دســت بدهند تا به جای پس‌انداز و سفته‌بازی؛ سرمایه‌گذاری و مبادله را ترویج کنند. این برنامه خاص برای سایر ارزهای آزمایشی که در دوره رکود بزرگ در جریان بود نیز وجود داشت. برای مدت کوتاهی آلبوم‌های تمبر و طرح‌های اعتبار اجتماعی در اتریش، کانادا و ایالات متحده رونق پیدا کردند و ســپس ارزش‌شان را از دست

1. Full balanced load period

دادند؛ مگر اینکه مورد استفاده قرار می‌گرفتند («مثل روزنامه تاریخ مصرف‌شان تمام می‌شد، مثل سیب‌زمینی پوسیده می‌شدند و مثل آهن زنگ می‌زدند»). اما پول تکنوکرات‌ها نوعی ویژگی زمانی دیگر نیز داشت؛ یکی از خصوصیات عمومی پول این است که ابزاری برای آینده تلقی می‌شود، یعنی به زمانی که در آن مبادله خواهد شد، تعلق دارد.

بسیاری از پژوهشگران حوزه پول، داستان‌های کلاسیکی را که از زمان قدیم در مورد منشاء پول گفته شده است، تایید یا تکذیب کرده‌اند. مثلا پول به‌صورت کالا و سکه بود، مالیات و خراج بود، هدیه بود، واحد شمارش بود، ضایعات بود. کتاب «زندگی اجتماعی پول»[1] اثر داد[2]، شش نوع مفهوم اولیه را برای پول در نظر می‌گیرد و به بسیاری مفاهیم دیگر نیز اشاره می‌کند. در تئوری و عمل، منشاء داستان‌هایی که در مورد پول گفته می‌شود، نقش آن را در زندگی ما مشخص می‌کند، البته پیش‌بینی‌های ما از آینده نیز در این امر تاثیر دارند. پولی که ما دریافت می‌کنیم «پول رایج» است، یعنی می‌دانیم اشخاص دیگری (اعم از بازرگانان، ماموران جمع‌آوری مالیات و بانک‌ها) وقتی زمان خرج‌کردن برسد، آن را از ما قبول می‌کنند. پولی که در جیب ماست، در آینده به آثار باستانی تبدیل خواهد شد.

این حقیقتی است که در حوزه مالی و پولی، بدیهی محسوب می‌شود. مطمئنا مردم دارایی‌ها و بدهی‌های خود را با در نظر گرفتن ثبات و عدم ثبات «گذشته، آینده پیش‌بینی‌شده و زمان محاسبه‌شده» تنظیم می‌کنند. هر چقدر هم عقب برویم، پول همیشه به شکل خاصی عمل می‌کرده است. برای مثال می‌توانیم به رسیدهای تخفیف انبارهای غلات در مصر، یا وام‌ها و سیستم بهره پیچیده‌ای به نام «مش» در بین‌النهرین اشاره کنیم که با تغییرات سلسله‌ای و مرتبه‌های ارثی قدرت در هم تنیده شده بود. سرمایه‌گذاران معاملات خود را به‌صورت کوتاه‌مدت و با ترکیبی از مدل‌ها، الگوریتم‌ها و غریزه انجام می‌دادند؛ زمان تسویه‌حساب در معاملات مالی می‌تواند از نوسانات چند میکروثانیه‌ای تا قبض‌های یک‌ماهه یا تعهد ۳۶۷ساله دانشگاه ییل را شامل شود (که هنوز بهره آن را پرداخت می‌کنند). چنین چیزی به آینده نامشخصی وابسته است که نظامی از تغییرات غیرقابل پیش‌بینی را شامل می‌شود، مثل اینکه متعهد شویم وعده‌های ما عملی نخواهند شد و همین‌طور هم بشود. در عین حال، افراد

1. The Social Life of Money
2. Dodd

و خانواده‌ها از حقوقی که قرار است در آینده بگیرند، برای بچه‌ها، سلامتی، هزینه رهن، هزینه تحصیل و بازنشستگی پول کنار می‌گذارند. بخشی از این کار به‌صورت حدسی است و باید پیش‌بینی کرد در آینده دیگران چه اتفاقاتی می‌افتد و این احتمال را باید در نظر گرفت که حدس اشتباه دیگران می‌تواند حدسیات شما را هم تحت‌الشعاع قرار دهد.

متخصصان امور مالی، بدهی را بر اســـاس نرخ تورم ارز متداول، در نظر می‌گیرند و اینکه ارزش پول در آینده و طی مدت بدهی چگونه تغییر خواهد کرد. اگر به بانک‌ها اعتماد نداشته باشـــیم، می‌توانید پول نقد، طلا، جعبه‌های سیگار یا شـــوینده انبار کنید؛ ترکیبی از چند نوع اندوخته، صرفا جهت اطمینان، مانند خانه‌ای که برق دارد، اما در آن شـــمع هم پیدا می‌شود. سرمایه‌گذاران با بررسی‌های بلندمدت، ارزش خالص کنونی سرمایه‌گذاری را در قالب «ارزش پول در گذر زمان» مشخص می‌کنند؛ اینکه ارزش پول در آینده چقدر کاهش پیدا خواهد کرد. مدل‌های این چنینی تصور ما را از اقتصاد آینده تغییر داده‌اند.

ترکیب معمول پول، اعتبار، سکه و گواهی‌ها، علاوه بر ابزار رفاهی، نماینده دوره زمانی حال و آینده نیز هست، همان‌طور که «ربکا اسپنگ» در پژوهشی در رابطه با پول در دوران انقلاب فرانسه می‌گوید: «پول نشانگر چیزی بود که مردم از آینده انتظار داشتند. طبق فعالیت‌های مکرر و انتظارات معمول، این شیء بی‌جان و مقبول، درکی از نحوه عملکرد طبیعی جهان و مردم آن به ما ارائه کرد. به این ترتیب، پول یک نهاد یا میکروفناوری برای تولید و تکثیر هنجارهای مشترک و پیوستگی اجتماعی محسوب می‌شود.»

ورود پول به روابط، نقش‌ها و معاملات روزانه ما نوع دیگری از ناپایداری را نیز نشان می‌دهد؛ روابطی که با نزدیکان، قوم و خویش، جامعه و دوستان خود داریم (در اینجا کلمه «ناپایداری» زمان را توصیف نمی‌کند؛ بلکه به روابط و ایده‌های مرتبط با آن اشـــاره دارد). به گفته «ویویانا زلیزر»[1]، جامعه‌شناس اقتصادی، این همان زمانی است که پول «سایه گذشته و آینده را روی تعاملات کنونی می‌اندازد؛ زیرا مجموعه معانی روابط و منافع طرفین در آینده، روی آنچه امروز رخ می‌دهد، تاثیر می‌گذارد». به وام‌های شـــخصی، دارایی‌ها و حساب‌های مشترک، وعده میراث و عشق به فقیر و غنی، دریافت کمک‌هزینه یا کنار گذاشتن پول برای روز مبادا فکر کنید. در حقیقت با توجه به انتظارات، امید و ترسی که در روابط و موقعیت‌های شخصی داریم، پولی

1. Viviana Zelizer

را کنار می‌گذاریم. پول را به امید خوشبختی آینده پس‌انداز می‌کنیم یا هدیه می‌دهیم؛ حتی برای شخصی که فوت کرده، خیرات می‌کنیم یا بخشی از یک سهام را وقف می‌کنیم.

وقتی یک قدم از این روابط فراتر برویم، می‌بینیم شبکه‌ای از جوامع، خویشاوندی‌ها و روابط بزرگ‌تر وجود دارد. «کریستین دسان» در کتاب «پول‌سازی» تحلیل دقیقی از پیدایش و گسترش سرمایه‌داری در اوایل دوره انگلیس مدرن ارائه می‌کند تا نشان دهد پول، هرچه باشد، عرفی گروهی است که توسط جوامع خاصی «برای سازمان‌دهی جهان مادی طراحی شده است». کار آن «اندازه‌گیری، جمع‌آوری و توزیع مجدد منابع» برای گروه‌های خاص است که اغلب چارچوب قدرت موجود در منطقه را نشان می‌دهد. پول‌سازی چیزی فراتر از یک ایالت است. دسان می‌نویسد: «این جوامع ممکن است مردم یک ایالت باشند، یا جمعی باشند که حول محور وفاداری، دین یا سودمندی اشخاص به‌صورت عملی یا اهدای کالا سازمان‌دهی شده باشند» و در چارچوب‌های مختلف زمانی، تاریخی و آینده مورد انتظار جای گرفته باشند.

در نهایت، بحران و فاجعه نیز نوع دیگری از ناپایداری پول است. وقتی پول با شکست مواجه می‌شود «تمام روابط نزدیک، با شفافیت غیرقابل تحمل و نافذی آشکار می‌شود که البته این امر مانع دوام پول می‌شود... پولی که به شکل خانمان‌براندازی در مرکز تمامی موارد حیاتی قرار می‌گیرد». والتر بنجامین، فیلسوف و منتقد، در یادداشت‌هایش در رابطه با زندگی در تورم پس از جنگ جهانی اول در آلمان چنین نوشت: «با فرو ریختن آینده؛ پس‌انداز، حقوق مستمری، انحصارات و تمام دادوستدهای حساس، عمل به تعهدات، ترس‌ها و واقعیت‌های مربوط به دوستان و آشنایان آسیب دید و تنها بقا بود که ضرورت داشت.» این هم بخشی از تاریخ پول است که در آن آرامش «پول واقعی» به هم خورده است. جان مینارد کینز در این باره می‌گوید: «این همان چیزی است که بی‌قراری‌های ما را فرو می‌نشاند و بدگمانی ما نسبت به آینده را از میان می‌برد» (همان‌طور که انتظار می‌رود، حدود یک‌چهارم آخر این کتاب به چنین زمانی اختصاص دارد).

با در نظر گرفتن چشم‌انداز و آینده پول، چه چیزی باعث ناپایداری گواهی انرژی تکنوکرات‌ها می‌شود؟ این گواهی فقط از نظر مالی یک ارز فرضی نبود؛ بلکه ارزی فرضی ـ تخیلی بود که آینده را تصور و روایت می‌کرد. این گواهی نه وسیله سرمایه‌گذاری بود و نه ابزاری برای معامله، نه گاوصندوقی از سکه‌های طلا بود و نه راهی برای سازمان‌دهی جهان؛ چیزی که «ترش» اسم

آن را «تصویری از جهانی که می‌توانست وجود داشته باشد» می‌گذارد؛ جهانی با آداب و رسوم و جوامع خاص خود که در زمان حال توسط قدرت فرهنگی پول به ما نشان داده می‌شود. آنها پلتفرمی برای آینده و رویه‌های آرمانی بودند که به آینده پل می‌زدند. اکنون به جای شرط‌بندی روی برداشت زیتون (مانند تالس) یا شرط‌بندی روی شـــرافت اقتصادی رژیم اسپانیا (مانند بانکداران بزرگ هلند) می‌توان از پول برای طرح‌های فرهنگی استفاده کرد که در آینده سودمند خواهد بود و ثمره‌ای خواهد داشت.

شورش دانشمندان

ارزهای فرضی ثمره آینده نیســـتند، اما آینده خاص و مشخصی را نشان می‌دهند که به زمان خودش تعلق دارد. با اینکه تکنوکراسی همیشـــه عملکرد خود را مطابق با آینده تنظیم می‌کرد، تشکیلات آنها از همه نظر نشانگر حساسیت علمی ـ تخیلی دوره رکود بزرگ در ایالات متحده بود. آینده مورد انتظار آنها نیز که با گواهی انرژی آن آشنا شدیم، مانند ساختمان امپایراستیت یا کتاب «آفاق» نوشته «نورمن بل گدس» که به آینده نزدیک می‌پردازد، ثمره همان زمان است. در سال ۱۹۳۲، «ویلیام ادیسون دوییگینز» (خطاط و طراح حروف) در مورد طراحی مجدد ارز ایالات متحده نوشت: «با توجه به وضعیت نیمه اول قرن بیستم این کار از قبل انجام شده است... چنین طرحی از ســـرعت می‌گوید، از اینکه هوا، بزرگراه جدید ماست، از جهانی که ناگهان به شکل ترسناکی بزرگ شده اســـت.» این دقیقا همان وضعیتی بود که در تکنوکراسی و پول آن وجود داشت. دوییگینز می‌گوید: «پول آمریکا در سال ۱۹۳۲ باید نشان‌دهنده رشد بالای انرژی مکانیکی باشد که برای حفظ قالب دموکراسی خود تلاش می‌کند.»

آینده تکنوکراسی که هاوارد اسکات مطرح کرد، زیبایی آن از سندی حقوقی می‌آمد که برای تمامی جنبه‌های زندگی آینده طراحی شده بود، همچنین چارچوبی یکپارچه و خشن داشت و کنترل مطلق را به دست دانشمندان، متخصصان و مهندسان می‌داد. رستوران‌های این آرمانشهر توسط شیمیدانان نظری اداره می‌شد که جنبش غذایی جدیدی را راه‌اندازی می‌کردند تا طبیعت را به «زنجیره‌ای از کارخانه‌ها و یک خـــط تولید بزرگ» تبدیل کننـــد؛ روغن‌ها و چربی‌های خوراکی را به‌صورت مصنوعی تولید کنند؛ کل قاره آمریکا را به شـــکل یک شـــرکت فناورانه درآورند و انحصار نهایی را رقم بزنند.

در آن دوره زمانی خاص، چنین نتایجی اجتناب‌ناپذیر به نظر می‌رسید. اسکات از پیروان «تورستین وبلن» بود؛ اقتصاددان و جامعه‌شناسی که کتاب «تئوری طبقه مرفه» را نوشت و برای اولین بار از اصطلاح «مصرف آشکار»[1] استفاده کرد. او همچنین کتاب «مهندسان و نظام قیمت‌گذاری» را در سال ۱۹۲۱ نوشت که به‌نوعی اجرای آزمایشی تکنوکراسی بود. این کتاب تصویری از «هیات حاکمه متخصصان» و الگویی از دگرگونی اجتماعی ارائه می‌کرد که مبتنی بر اعتصاب متخصصان بود و نسخه‌ای سوسیالیست از اعتصاب «مغزهای خلاق» در کتاب «اطلس شورید» آین رند محسوب می‌شد.

در سال ۱۹۳۳ کتاب «شکل چیزهایی که می‌آیند»[2] از «اچ جی ولز» جهانی اجتناب‌ناپذیر را به نمایش گذاشت که متخصصان، دانشمندان و خلبانانی آن را کنترل می‌کردند که قصد داشتند دین را از میان ببرند، زبان انگلیسی را در همه‌جا رواج دهند و «پولی کاملا انتزاعی را بنیان‌گذاری کنند؛ پولی انتزاعی و آزاد از قیدوبندهای ماده مثل وزن و اندازه». قرار بود اسم این پول انتزاعی، «دلار هوایی»[3] باشد؛ واحدی یکپارچه که محموله‌های در حال ترانزیت را نشان می‌داد و از اسکناس‌های کاغذی استفاده می‌کرد که وزن و حجم محموله و سرعت و فاصله هواپیما را شرح می‌دادند. برای ولز نیز، مانند سایر مخترعان آرمانگرای پول‌های فرضی، «امکان نداشت یک تئوری پولی وجود داشته باشد که تئوری کاملی از یک سازمان اجتماعی (کازموگرام) نباشد». سازمان‌دهی مجدد جهان و امور انسانی با توجه به یک نظام فناورانه جدید و صدور اسکناس‌های جدید انجام می‌شد؛ «دلار هوایی» که «با قطعیت نشان می‌داد مفهوم ایستا و کهنه زندگی بشری با منابع محدود جای خود را به ایده‌های پرجنب‌وجوش زندگی جدیدی می‌داد که دائما در حال گسترش بود».

درست در همان سال، کتاب «داستان‌های حیرت‌انگیز» نوشته «هوگو گرنزبک» مجموعه داستان‌هایی از «شورش دانشمندان» را در خود جای داد که یک کودتای مالی تکنوکراتیک را توصیف می‌کرد که در آن تکنوکرات‌های شورشگر با استفاده از فناوری‌های شیمیایی و انواع اشعه‌هایی که می‌توانست طلا را به قلع تبدیل کند و نوشته‌های روی اسکناس‌ها را پاک کند، تمام بدهی‌ها را از میان بردند و قبل از اینکه کنترل را به دست بگیرند، اقتصاد را زمین زدند. این قضیه

1. Conspicuous consumption
2. The shape of things to come
3. Air-dollar

موضوع منحصربه‌فردی نبود. داستان‌های کیمیاگری یا بی‌ارزش‌کردن طلا و نقره به‌صورت صنعتی و هرج‌ومرج مالی پس از آن، از ابتدای قرن، ذهن مردم را به خود مشغول کرده بود، به‌خصوص در کتاب‌های علمی ـ تخیلی عامه‌پسند. در همان اوایل در سال ۱۹۰۰، «گرت سرویس»[1] کتاب «فلز ماه» را نوشت که در آن یافتن منابع بزرگی از طلا در قطب جنوب اقتصاد را به نابودی می‌کشاند تا اینکه «دکتر سیکس»[2] فلز جدیدی به نام «آرتمیسیوم»[3] را معرفی کرد که جایگزینی مصنوعی برای پشتیبانی از پول بود. در سال ۱۹۲۲، قهرمان کتاب «نبرد برای طلا» نوشته «راینهولد آیچکر»[4] طلا را به‌صورت مصنوعی تولید می‌کند تا هم غرامت جنگ آلمان را بپردازد و هم به اقتصاد متحدین ضربه بزند (اما «آلمان آیچکر» که از این موضوع آگاه بود، از پلاتین به‌عنوان پشتیبان پول خود استفاده کرد). داستان‌های تکنوکرات‌ها تفاوتی ندارند؛ به‌جز اینکه تفرقه و کودتا برای آنها مشکل مالی تلقی نمی‌شد؛ بلکه به معنای رهایی بود تا جهان را تحت کنترل دربیاورند و آینده‌ای را ایجاد کنند که قرار بود از طریق بحران فناوری پول ایجاد شود.

افرادی که در این کتاب بررسی می‌کنیم، پول‌های فرضی‌شان را به‌عنوان نقشه‌ای قدرتمند برای آینده می‌بینند. این نقشه‌ها شباهتی به شرط‌بندی منطقی روی بهره‌وری در آینده یا وضع مالیات در آینده که دسان در تضاد با شمش‌های نقره آنها را بررسی می‌کرد، ندارند؛ بلکه تخیلات فناورانه و علمی ـ تخیلی هستند که می‌توانند باعث از هم گسیختگی کامل و جبران‌ناپذیر جامعه شوند؛ البته پول، فقط بخشی از این دگرگونی و راه فرار از حال به آینده خواهد بود. پول آنها فقط آرمانی نیست؛ بلکه پول جهانی موازی است، همان‌طور که «راینهایت کسلک»، تاریخدان، می‌گوید: «جامعه برتر در مکانی روی کره زمین به واقعیت بدل نمی‌شود؛ بلکه باید در زمان دیگری به‌دنبال آن گشت؛ زمانی که در حال حاضر می‌توان نشانه‌هایش را در ارزهایی دید که بعدها کنار گذاشته خواهند شد.»

بعد از دسته ماشین‌های خاکستری دارای سمبل «موناد»، بعد از پیش‌بینی‌های آخرالزمانی و وسواس توطئه (مخصوصا کارهایی که واتیکان انجام می‌دهد) و نیاز به شورشگران دانشمند؛ تکنوکرات‌ها به قدری دوام آوردند که خودشان را تنها دیدند (به قول کسلک در آینده‌ای مانده‌اند

1. Garrett Serviss
2. Dr. Syx
3. Artemisium
4. Reinhold Eichacker

که گذشته است). آنها در زمان گیر افتاده‌اند، اما در دوران خودشان نقش ارزهای فرضی، آرمانی و جهان‌های موازی را به نمایش گذاشتند؛ چیزی که آینده را برای آنها رقم می‌زد.

فصل دوم

کاغذ مطمئن

در این فصل خواهیم دید پول نقد و ارز در عمل چگونه کار می‌کنند؛ تاریخچه ژرفی از تولید، ایمن‌سازی و رسمیت‌بخشیدن به پول کاغذی را خواهیم دید (دسته‌ای غریب از اسناد چاپی که همگی معنی آن را یاد گرفته‌ایم). پول جعلی و رقبای آن را دنبال می‌کنیم، به مشکل اعتماد به اسناد می‌پردازیم، مقاله‌ای ضمنی در رابطه با اســتقلال در تراکنشی معمولی را می‌خوانیم و با منظومه‌ای پنهانی آشنا می‌شــویم که همه آن را دیده‌ایم و تقریبا هیچ‌کدام قادر به شناسایی آن نیستیم.

اشیای تولیدشده به روش‌های جدید

احتمالا در عین حال که این مطلب را می‌خوانید، امضاهای زیادی را با خود به همراه دارید. در ایالات متحده ایــن امضاها احتمالا متعلق به «تیموتی گیتنــر»، «آنا کابرال» یا «جاکوب لو» هستند؛ در برزیل متعلق به «هنریک میرلس»؛ در مالزی «داتوک محمد بن ابراهیم»؛ در لهستان «آدام گلاپینسکی» و در اروپا «ماریو دراگی» یا «ژان کلود تریشه». این امضاها نمونه‌ای از پرتکثیرترین نوشته‌های موجود هستند که در گوشه اسکناس‌های جهان در کنار بناهای ملی، پرتره‌های افراد برجسته غرق در تفکر، اعداد تاریخی، تاج‌گل‌های اشراف و معماری‌های وزین، سپرها، تزئینات طوماری‌شکل و پایتخت‌هایی با سبک معماری یونانی جای گرفته‌اند. «والتر بنجامین» در زمان تورم شدید آلمان در رابطه با اسکناس چنین نوشت: «قهرمانان تنومندی که شمشیر خود را در مقابل واحد پول غلاف کرده و سردر جهنم را تزئین کرده‌اند.»

امضاهای مقامــات خزانه‌داری و روســای بانک‌های مرکزی بخشــی از قدمت تدریجی اسکناس‌ها هســتند که به منزله دندان عقل یا آپاندیس آنها محســوب می‌شوند؛ یادگاری از حواله‌های قدیم. حواله، ابزاری در زنجیره پیچیده اعتبار بود که تجارت اروپا را قرن‌ها پایدار نگه داشت. توصیف فناوری‌ها و رویه‌های پیشین با استفاده از فناوری‌های جدید می‌تواند مدگرایانه و گمراه‌کننده باشد، اما حواله‌ها چیزی شبیه به شبکه‌های اجتماعی را تشکیل می‌دادند که در آن مجموعه‌ای از روابط و برنامه‌ها قابل تعیین بود.

بازرگانی در یک شهر حواله‌ای را در اختیار یک کارگزار قرار می‌دهد و متعهد می‌شود مبلغی را در زمان مشخصی در آینده به شــخص دیگری پرداخت کند. شخصی که قرار است پول را دریافت کند، می‌تواند این حواله را پشت‌نویسی کرده و آن را با نرخ کمتری به شخص دیگری

پرداخت کند و این شخص نیز می‌تواند به نوبه خود از آن استفاده کند. نرخ و ارزش این مبادلات (به گفته ریکا اسپنگ) بر اســـاس «حجم حواله‌هایی که باید در شهری مشخص و بر اساس شهرت پرداخت‌کننده اولیه و تمامی کسانی که حواله را طی مبادلات پشت‌نویسی کرده‌اند» تعیین شود.

از آنتورپ تا ژنو، پاریس تا فرانکفورت و استانبول تا لیســـبون هر قرارداد جدید حلقه‌ای به زنجیره امضاها اضافه می‌کرد و هر امضا شخص خاصی را مسئول می‌کرد. همان‌طور که اسپنگ گفت، امضاهای مکتوب «به ما این امکان را می‌داد که تصور کنیم حتی افراد ناشناس پیشین را نیز می‌توان پیدا کرد و در صورت نیاز آنها را مسئول دانست.» هر حواله منحصربه‌فرد نشانگر قرارداد خاصی از افراد و رویدادها و کالاها بود (لوازم منزل، کنیاک، موسیو X، دکتر Y، آقای Z، شش ماه بعد، در نمایشگاه لایپزیگ) و به خودی خود شیء منحصربه‌فردی بود. دارنده حواله می‌توانست در صورت گم‌شدن آن آگهی منتشر کند؛ «انگار سگش یا چترش را گم کرده باشد». از آنجا که احتمال ورشکستگی هر یک از اشخاص زنجیره وجود داشت، بنابراین تعداد امضای بیشتر به معنی امنیت مالی بود؛ زیرا اشخاص بیشتری درستکاری یکدیگر را تایید می‌کردند.

این ســـازوکار مدیریت جریان ارزش، تعادل را بین تکرارپذیری اســـتاندارد و مشخصات منحصربه‌فرد اشخاص، معاملات و زمان معین برقرار می‌کرد. شکنندگی این تعادل خودش را در بحران امضاها در هنگام تولید اسکناس[1] در انقلاب فرانسه نشان داد. اسکناس واحد پول نظام جدید بود که در تئوری و در ابتدا به دارایی‌های ملی متصل بود. تولید و گردش آنها نهایتا بسیار بیشتر از حواله‌ها شد، در حالی که هنوز اعتبار خود را از امضاهای خاصی می‌گرفتند؛ از کارمندان اولیه تا زنجیره کسانی که آن را پشت‌نویسی می‌کردند. البته افکار شومی در رابطه با کارمندان فاسد جریان داشت. رفته‌رفته مشکل محدودیت صدور پول‌های جدید هم ظاهر شد که منشـــاء آن محدودیت توانایی و وقت کارمندانی بود که به‌صورت دستی پول‌ها را امضا می‌کردند؛ در واقع امضاهای حک‌شده و چاپی معنی پول را عوض کردند. علاوه بر دارایی‌ها، هویت و نامی که به اسکناس داده می‌شد، پشـــتیبان آن بود. این امکان وجود داشت که مامور دولتی خاصی را با قلمش، نشانی خانه‌اش و سه رنگ انقلابی پین‌شده به کلاهش پیدا کرد و او را مسئول دانست (اصطلاح «بوروکرات» نیز در همین دوره زمانی اختراع شد و در هنگام انقلاب

1. Assignat

استقلال پیدا کرد؛ نظارت در دفتری اداری که نماینده منابع اطلاعاتی و نظام عملیاتی بود).

بررسی اسپنگ از این دوره، تغییر عمیق و ظریفی را ثبت کرده است؛ به‌کارگیری تکنیک‌ها و فناوری‌های جدید در چاپ به‌منظور تایید هویت اسکناس به جای پشت‌نویسی توسط اشخاص. این اسکناس‌ها به «اشیای تولیدشده به روش‌های جدید» تبدیل شده و به گونه‌ای طراحی شدند که خودشان هویت خود را تایید کنند و به تایید اشخاص سرمایه‌دار نیازی نباشد.

می‌توانیم این مورد را با ایالات متحده مقایسه کنیم. تشریفات اداری نظام‌های اعتباری (اعم از دستور پرداخت به نمایندگان، کارگزاران، عمده‌فروشان و واسطه‌ها در برابر کالاهای تحویلی، رسید انبارداری، بارنامه و اسناد مزایده) با اسکناس‌هایی که بانک‌ها صادر می‌کردند، رابطه پشتیبانی دوطرفه داشتند و به یک ساختمان خاص، جامعه کشاورزان یا معدنچیان یا گاوصندوق پر از شمش طلا محدود می‌شدند. به‌تدریج شبکه‌های اعتباری همگانی رواج پیدا کردند؛ چنانچه در قرن نوزدهم، باغداران فلوریدایی و کسانی که پیش‌تر به آنجا رفته بودند، گردشگرانی را که از شمال می‌آمدند، پذیرفتند. این گردشگران اغلب از چک‌هایی استفاده می‌کردند که نقد کردن آنها بسیار وقت‌گیر بود. بنابراین خود چک‌ها به جای پول دست‌به‌دست می‌شد و مجموعه‌ای از پشت‌نویسی‌ها را شامل می‌شد که نمایانگر نظام اجتماعی «ایندین ریور»[1] بود. «توماس اش»[2]، گردشگر ایرلندی در سال ۱۸۰۸ می‌نویسد: «کل کسب‌وکار آن حوالی بدون استفاده از پول صورت می‌گرفت.»

زندگی تجاری آمریکای شمالی، از اسکله‌های اقیانوس اطلس تا امپراتوری بردگان در مزارع پنبه جنوب، از ماهی‌گیران و مسافران رودخانه‌های کانادا تا قطارها و راه‌آهن‌های غرب، همگی در ابتدا با سیستمی سازمان یافتند که برای خانواده بازرگانان ونیزی قرن پانزدهم آشنا بود. این سیستم بر شبکه‌ای از روابط و تجارت خارجی دقیق با حسابداری دوطرفه مبتنی بود که در «حساب‌های مخاطرات و کالاها» ثبت می‌شد. گاهی اوقات نیز از سکه و اسکناس و روش‌های امضامحور برای مدیریت افراد، اسناد و سرمایه‌گذاری‌ها استفاده می‌شد.

در این فرهنگ مالی، سکه و مسکوکات (از جمله سکه‌های نقره، شلینگ انگلیس و ریال اسپانیا)، حواله سربازانی که از کبک (ایالتی در کانادا) برگشته بودند، بارنامه‌های کشتی‌های

1. Indian River
2. Thomas Ashe

زغال‌سنگ یا پنبه، اســکناس‌های محلی و کالاهایی مانند خز، موم، کتان، چای و باروت که معادل پول نقد بودند، مورد استفاده قرار میرفتند. بنابراین مطرح‌شدن مفهوم و عملکرد اسکناس ملی موضوع جدیدی بود (با همان پیچیدگی هستی‌شناسی که اسپنگ توصیف می‌کند). نظام اعتباری، از بارنامه تا اسکناس‌های نهادهای محلی، همگی شبکه‌ای از اعتماد جمعی و تجربه را در منطقه تشکیل می‌دادند (یکی از شخصیت‌های کتاب «مرد مخفی» نوشته «ملویل»[1] در سال ۱۸۵۷، در حالی که یکی از اسکناس‌های موسسه مالی ـ اعتباری ویکسبورگ را بررسی می‌کند، می‌گوید: اســکناس خوب باید بعضی جاهایش برجستگی داشته باشد و همچنین چند نقطه موج‌دار قرمز داشته باشد). سکه‌ها و اسکناس‌ها از نظر فیزیکی بررسی می‌شدند؛ از وزن‌کردن در ترازو گرفته تا بررسی ظرافت رشته‌های پارچه یا چشیدن، لمس‌کردن، وزن‌کردن، انعطاف‌پذیری و ظاهر فلزات. اسکناس ملی خودش باید هویتش را به‌عنوان شکل جدیدی از پول ثابت می‌کرد و علاوه بر ایده‌های جدید، روش‌های جدیدی را نیز برای ارزیابی اشیا و درک ارزش آنها به افراد نشان می‌داد.

باید بتوان بدون دانستن شیوه تولید اسکناس، به‌راحتی اســکناس واقعی را تشخیص داد؛ چالش کاغذ مطمئن. تولید اســکناس باید برای سازنده اولیه کار راحتی باشد (پس از عبور از موانع مهندسی اولیه، هزینه نهایی آن باید نزدیک به صفر باشد) و در عین حال باید به گونه‌ای باشد که کســی نتواند از طریق مهندسی معکوس آن را بازســازی کند. یکی از طرفین (مانند ایالات متحده) باید بتواند مواد باطله را به اسکناس‌های تازه تبدیل کند و این کار را طوری انجام دهد که طرف مقابل نتواند مشابهش را تولید کرده یا آن را تکثیر کند. «لیزا گایتلمن»[2] در مورد دوره‌ای در قرون نوزدهم و بیستم صحبت می‌کند که تکنیک‌ها و فناوری‌های نوشتاری پیشرفت عظیمی کرده بود و راه‌های جدیدی برای ایجاد اسناد به وجود آمده بود. برای مثل گواهی فوت را در نظر بگیرید؛ امضاهای متعدد، مهرها و حاشیه‌ها، چاپ تصویر به‌صورت حک‌شده، بارکد، واترمارک، جوهر حرارتی، ریزچاپ[3] و خود گواهی به‌عنوان «نسخه اصلی موجود در پرونده». پول کاغذی نیز باید سطح مشابهی از امنیت داشته باشد تا بتواند در بافت‌های مختلفی مانند بازار و در هر معامله‌ای هویتش را برای طرفین اثبات کند.

1. Melville
2. Lisa Gitelman
3. Microprinting

اکنون کار سخت‌تر شده و این کار باید در بافت بزرگ فناوری‌های دیجیتال و رشد «اشیای تولیدشده به روش‌های جدید» بر اساس سیستم بی‌عیب‌ونقص و دقیق تکثیر نیز انجام شود.

آموزش خواندن اسکناس یک‌دلاری

اسکناس یک‌دلاری ایالات متحده یکی از اشیایی است که بیشترین تولید صنعتی موجود را داشته و ده‌ها میلیارد عدد از آن وجود دارد. البته مشخص کردن تعداد دقیق آن دشوار است: هرچند می‌دانیم که بانک مرکزی هر سال چه میزان از آن را به گردش می اندازد (مثلا حدود ۱۱ میلیارد و ۷۰۰ میلیون در سال ۲۰۱۶)، اما طول عمر این اسکناس خیلی کوتاه و بین یک تا پنج سال است. از نظر قانونی و اقتصادی همه آنها دقیقا یکی هستند، با یکدیگر قابل تعویض بوده و هیچ‌کدام ارزش‌شان بیشتر یا کمتر نیست، می‌توان از آنها به‌عنوان ابزاری برای سنجش و مقایسه قیمت کالاهای مختلف استفاده کرد، ولی اگر این اسکناس‌ها را به‌صورت شیء در نظر بگیریم، هر کدام‌شان بر اساس شرایط، منحصربه‌فرد هستند.

داده‌های فراوانی به‌صورت عددی روی اسکناس خاصی که در موردش صحبت می‌کنیم، چاپ شده است؛ مثل اینکه کجا چاپ شده است (سنت‌لوئیس)، شماره سری و سریال چاپش چیست، دقیقا از چه قالبی برای چاپ آن استفاده شده است (FW A 81) و در کدام قسمت از صفحه ۳۲عددی چاپ قرار داشته است. البته ممکن است این اسکناس مچاله یا کمی کهنه شده باشد یا گوشه‌اش پاره شده باشد. وقتی آن را در دست می‌گیریم، در واقع به وسیله‌ای دست می‌زنیم که شاید چندین هزار نفر آن را لمس کرده‌اند؛ مجموعه‌ای مشارکتی از باکتری‌ها. پول کاغذی باکتری‌ها را دست‌به‌دست منتقل می‌کند، مثل کشتی حمل باری که فاضلاب را از بندری به بندر دیگر برده و در آنجا تخلیه می‌کند.

در واقع اسکناس یک‌دلاری شیئی است که برای خواندن طراحی شده است. ظاهری نمادین دارد و هم برای انسان و هم برای ماشین به‌سرعت قابل تشخیص است. ظاهر آن ثابت است؛ رنگ سبز، عدد مشخص، منظره سرد و مخوف پشت آن با هرم ناتمام و هوشیاری که مانند نقاشی‌های «رنه ماگریت» تنها ایستاده و ۱۲ مورد دیجیتال و عددی دیگر که به منحصربه‌فرد بودن آن در مقایسه با سایر اسکناس‌ها اشاره دارند. من محکم پای این طرز فکر هستم که این اسکناس باید خوانده شود؛ زیرا عضو مجموعه بزرگ‌تری از اسناد ارزشمند محسوب می‌شود؛

نماد تاثیرگذاری که به طرق خاصی معنی آن را فهمیده‌ایم.

«فرانسیس رابرتسون»، متخصص تاریخ طراحی، رابطه نزدیک توسعه اولین اسکناس‌های امروزی و طراحی و چاپ با استفاده از قالب‌های فولادی را شرح می‌دهد: همان فناوری‌هایی که باعث پیشرفت تکثیر صنعتی شدند (فرایند دقیق و مفصل تولید انبوه قطعات و ماشین‌های پیچیده)، برای تولید اسکناس قابل قبول و بی‌رقیب بودند. ابزار خودکاری که نیاکان دستگاه‌های تراشکاری پیچیده، ماشین‌ها و کنترل عددی کامپیوتری (CNC)، دستگاه‌های فرز و برش محسوب می‌شدند، از نظر هندسی تولیدات دقیقی را ممکن ساختند که می‌توانست جایگزین کارهای دستی شود که نیاز به مهارت داشتند. این دستگاه‌ها با الگوهای حرکتی دایره‌ای و مارپیچ در تولید قطعات مورد نیاز لوکوموتیو، کشتی‌ها، پل‌ها و اسکناس استفاده می‌شدند.

محصولاتی که توسط ابزار مکانیکی، صنعتی و پیشرفته تولید می‌شوند باید معتبر نیز باشند و این اعتبار در پیچیدگی تکثیر آنها ریشه دارد. این محصولات، مانند قطعات قابل تعویض اسلحه یا لوکوموتیو، دقیقا مشابه یکدیگرند و به همان اندازه هم قابل اطمینان هستند. هم از نظر فلسفی و هم از نظر فنی «واقعی» هستند، مانند چرخی که به‌دقت تولید و بازرسی می‌شود. بنابراین با همان اطمینانی که از روی یک پل آهنی رد می‌شوید، می‌توانید از اسکناس هم استفاده کنید.

«ماری پووی»، تاریخ‌دان فرهنگی اظهار می‌کند که اسکناس بخشی از دامنه بزرگ خواندنی‌ها محسوب می‌شود که دیگر از دید ما مخفی شده است. هم برای پول و هم برای سایر مکتوبات می‌توان از این عبارت استفاده کرد: «ارزش نوشته‌ها با کاغذ استفاده‌شده یکی نیست.» از نظر پووی، پذیرش اسکناس‌های صنعتی به‌صورت گسترده و الگوهای «شایستگی ادبی» در زمان و مکان مشخصی در قرون هجدهم و نوزدهم در بریتانیا و اروپا تصادفی نبود؛ همان‌طور که برگه نثر یا شعر ارزشمند بود، اسکناس نیز دارای ارزش بود، به این ترتیب روش‌های مختلفی برای تعریف ارزش کاغذ چاپی وجود داشت. او می‌نویسد: «پول به قدری شناخته‌شده است که انگار نوشته‌هایش نامرئی شده و پیشینه‌اش را به‌عنوان نوشته از دست داده است.» این استدلال به قدری پیچیده است که اینجا نمی‌توان آن را تماما بررسی کرد، اما جنبه دیگری از دلار را به ما نشان می‌دهد؛ دلار سندی است که مجموعه‌ای از مفاهیم پیدا و پنهان را با خود حمل می‌کند.

دلار «مسئول قانونی رسیدگی به بدهی‌های عمومی و خصوصی است» و هر بار که با آن معامله می‌کنیم، وفاداری خود را به کشورمان نشان می‌دهیم. دوویگینز، طراحی که در فصل اول با او آشنا شدیم و پیشنهاد طراحی مجدد اسکناس‌ها را مطرح کرده بود، می‌نویسد: «پول کاغذی نمونه بارزی از کیفیت محصولات دولت فدرال است که خودش را روی کاغذ نشان می‌دهد؛ ارز ملی و تمبر فدرال نماد ایالات متحده هستند که بیشترین توزیع را دارند.» می‌توانید این نماد را از کیف پول‌تان بیرون بیاورید و در چیزی مشارکت داشته باشید که «لانا سوارتز»، انسان‌شناس و پژوهشگر سیستم‌های پرداختی، آن را «اجتماع معاملاتی» می‌نامد. مثلا برای دلار آمریکا، این اجتماع از مرزهای کشور فراتر می‌رود؛ از کشورهایی مانند اکوادور که اقتصاد آن بر پایه دلار استوار است تا دسته‌های صددلاری که در پلاستیک پیچیده شده و حکم پس‌انداز نقدی یا تسویه‌حساب برای عملیات‌های عمومی و مخفی را در سراسر جهان دارند.

وقتی اسکناس یک‌دلاری مچاله‌شده را صاف می‌کنم که دستگاه فروش اتوماتیک آن را از من قبول کند، در واقع یک سند تاریخی زنده را باز می‌کنم؛ سندی که «فرانکلین روزولت» طراحی‌اش را تایید کرده و «لینکلن» ارزش ملی‌اش را افزایش داده؛ ارزشی که طی تورم دوره «نیکسون» و حکم بانک مرکزی در رابطه با فعالیت بازار با نوسان روبه‌رو شده، «امیلی گیلبرت»[1]، جغرافیدان آن را «تایید هر روزه دولت ملی» نامیده، یک‌صدم متر مربع مساحت دارد و همه مردم کشور آن را با خود حمل می‌کنند. در ادامه شرحی فلسفی از مفهوم قدرت ارائه خواهم کرد که معنی آن به چالش کشیده شده است.

زشت‌ترین تی‌شرت جهان

با در نظر داشتن اینکه چقدر می‌توانیم اسکناس یک‌دلاری را بررسی کنیم، بیایید از نردبان ارزش دلار بالا برویم و به اسکناس ۲۰ دلاری برسیم که باید با چالش فنی دیگری مواجه شود. دیگر کسی سعی نمی‌کند اسکناس یک‌دلاری را جعل کند، در واقع مدت‌هاست که دوره جعل پول خرد به پایان رسیده است. گروه‌های جدی و ماهر بسیاری روی جعل ۲۰ دلاری کار می‌کنند. این اسکناس، علاوه بر تمام اشتراکاتی که با یک‌دلاری دارد، باید از فناوری‌هایی استفاده کند که قابل خواندن باشد، اما نتوان آن را به‌صورت دیجیتال تکثیر کرد؛ یعنی خودش

1. Emily Gilbert

مرز آنالوگ و دیجیتال را حفظ کند.

اسکناس ۲۰ دلاری شیء بسیار خاصی است که باید به تمام ۲۰ دلاری‌های موجود دیگر شبیه باشد، اما کمی تفاوت داشته باشد؛ اگر اسکناس دیگری وجود داشته باشد که دقیقا شبیه آن باشد، یکی از آنها جعلی است. هیچ اسکناسی مشابه اسکناسی که اکنون جلوی من است وجود ندارد (شماره سریال JB9557548B سری ۲۰۰۹، امضای «تیموتی گیتنر» و خط خطی کوچکی که روی سرسرای کاخ سفید دیده می‌شود)، اما ۶/۴ میلیارد اسکناس دیگر وجود دارد که بسیار به آن شباهت دارند. این اسکناس‌ها در کیف پول‌ها، پاکت‌ها، مخزن دستگاه‌های خودپرداز و بانک‌ها و ماشین‌های حمل پول وجود دارند، در انبارها پنهان شده‌اند یا در پارکینگ‌های حومه شهر در میان لوله‌های PVC مدفون شده‌اند.

این اسکناس خاص در عین حال، هم ارزشمند است و هم بی‌ارزش؛ اگر آن را به چهار قسمت تقسیم کنیم معنی آن عوض می‌شود و ارزشش را از دست می‌دهد (البته جرم تخریب اموال را نیز مرتکب شده‌ایم، مثل اینکه پول من متعلق به خودم نیست). این اسکناس از وقتی دست من است تا زمانی که به شخص دیگری داده شود، ارزش دارد. تنها دلیلی که برای من ارزش دارد، این است که می‌توانم آن را خرج کنم. کمیتی انتزاعی است که می‌تواند هر کاربردی داشته باشد، می‌توان آن را بخشید یا با آن آتشی را خاموش کرد، در هر صورت از نظر کیفیت عینی دارای موجودیت است (البته من به‌شخصه اسکناس خودم را کنار گذاشتم تا در آینده خرج کنم، پس انداز کنم یا کار دیگری با آن انجام دهم). علاوه بر تمام این همزمانی‌ها، می‌توان به آنالوگ و دیجیتال‌بودن همزمان این اسکناس هم اشاره کرد.

مرز ظریف بین آنالوگ و دیجیتال در دهه ۱۹۹۰ از میان رفت و بحران پول نقد نزدیک می‌نمود. زیاد شدن اسکنرهایی با وضوح بالا، چاپگرهای لیزری و رنگی دقیق و نرم‌افزارهای ویرایش عکس، ناگهان زمینه را برای جعل فراهم کرد. دیجیتالی‌شدن، نظمی را که باعث بقای پول نقد می‌شد، به هم زد. البته استراتژی‌های جدیدی برای حل این مشکل به کار بسته شد؛ جوهر حرارتی و نوار امنیتی، حقه‌های بصری، بافت متفاوت کاغذ، واترمارک، حتی نوشته‌های مخفی که با تابش نور لیزر می‌توان آن را دید. برجسته‌ترین آنها صورت فلکی یوریون بود.

هر جای جهان که باشید، احتمالا این صورت فلکی را در کنار مجموعه‌ای از امضاها در کیف یا جیب خود حمل می‌کنید. به‌عنوان مثال، اگر اسکناس ۲۰ پزویی مکزیکی داشته باشید،

می‌توانید آن را در دایره‌های کوچک زردرنگ پشت سر «بنیتو خوارز»[1] ببینید؛ درهم امارات معمولا این دایره‌ها را نزدیک نقاط برجسته‌ای مانند ستاره‌های موجود در پس‌زمینه قرار می‌دهد، در اسکناس ۱۰ یورویی در انعکاس بصری طاق ساختمان قرار دارد، اسکناس ۲۰ دلاری آمریکا آنها را در «۲۰»های کوچک زردرنگی پنهان می‌کند. این الگو از نقطه‌ها توسط پرینترهای رنگی، اسکنرها، درایور پرینتر و اجزای موجود در نرم‌افزارهای ویرایش عکس (مانند فتوشاپ) شناخته می‌شوند و سیستم تشخیص پول را راه‌اندازی می‌کنند که مانع دیجیتالی‌کردن یا تکثیر اسکناس می‌شود.

«ویلیام گیبسون»[2] در رمان «تاریخچه صفر» خود شیئی را مطرح می‌کند که آن را «زشت‌ترین تی‌شرت جهان» می‌نامد: «طرح‌های بزرگی با سایه‌رنگ سیاه ملال‌آوری در سراسر آن کشیده شده بودند، چشمان نامتقارنی در قسمت سینه، دهانی ترسناک در پایین آن... خطوط اریبی در کناره‌ها که به پشت لباس کشیده می‌شد، آستین‌های شل.» شبیه چهره‌ای خشن به همراه یک کیوآرکد که صلیبی به آن اصابت کرده باشد. این الگو «معماری عمیق» نظارت ویدئویی به‌صورت دیجیتال را نشان می‌دهد. دوربین‌های مداربسته تصویر شخصی را که این لباس را پوشیده ضبط می‌کنند، اما هنگام بازیابی، او را از ویدئوها حذف می‌کنند. «آنها شخصی را که تی‌شرت زشت را به تن دارد، فراموش می‌کنند، سرش را، پاهایش را، دست‌ها و بازوهایش را فراموش می‌کنند.»

در رمان «قرارداد شرافتمندانه» محرز می‌شود که این نماد مرموز در نرم‌افزار دوربین مداربسته اختلال به وجود می‌آورد. این شیء یک ابزار جادویی تاثیرگذار است؛ شخصیت‌های گیبسون از آن تحت عنوان «نشان» یاد می‌کنند؛ نمادی که دارای قدرت ماوراءالطبیعی است. هر کسی که از پول نقد استفاده کرده باشد، نمادی وسیع‌تر از این را در دست داشته است؛ صورت فلکی که نشانگر توافق بین‌المللی است که از دیجیتالی‌کردن برخی اشیا به روش‌های مختلف جلوگیری می‌کند. زشت‌ترین تی‌شرت جهان فقط برای سیستم دوربین مداربسته جواب می‌دهد؛ صورت فلکی نیز فقط روی سیستم‌های ذخیره، ویرایش و چاپ تصویر با وضوح بالا جواب می‌دهد (می‌توانید بدون هیچ مشکلی با تلفن همراه خود از آن عکس بگیرید).

---

1. Benito Juárez
2. William Gibson

نرم‌افزار سیستم تشخیص جعل به‌صورت رایگان موجود است، اما متن‌باز نیست (یعنی حتی شرکت‌هایی که از آن اســتفاده می‌کنند، نمی‌توانند سازوکار آن را بررسی کنند). سازوکارهای تشخیص دیگری نیز وجود دارند که به شکل نامشخصی عمل می‌کنند. حتی اگر صورت فلکی را بپوشانید، برخی سیستم‌های دیجیتال اپتیکال با استفاده از سرنخ‌هایی که پژوهشگران به‌دنبال پیدا کردن آنها هستند، باز هم تصویر پول را ذخیره یا ویرایش نخواهند کرد. این مجموعه نمادها برای ماشین ساخته شده، نه برای انسان. این سیستم‌ها به گونه‌ای کار می‌کنند که پول را از اشیای دیگر تشخیص دهند؛ نه برای اینکه ارزش آن را حفظ کنند؛ بلکه به این منظور که آن را یک شیء نگه دارند، از دیجیتالی‌شدن آن جلوگیری کنند و آن را در جبهه آنالوگ حفظ و نگهداری کند.

پول دیجیتال چطور؟ چطور می‌توان آن را ایمن‌سازی و اعتبارش را تایید کرد؟ چطور می‌توان آن را خواند و فهمید؟

فصل سوم

قابل تشخیص
اما غیر قابل شناسایی

در ادامه، با پیشروی در عصر کامپیوتر بررسی می‌کنیم که پول نقد چیست، چطور به وجود آمده و چگونه اعتبار پیدا کرده است. در این فصل ایجاد رمزنگاری نامتقارن، به‌خصوص فناوری‌های تایید اعتبار مورد استفاده برای «امضای دیجیتال» را بررسی می‌کنیم و می‌بینیم چگونه در اسناد تاییدشده موجود (از جمله پول نقد) به کار می‌روند و اشکال مرکب غریبی را طی این فرایند به وجود می‌آورند.

درد رمزنگاری[1]

در سال ۱۹۴۴، «نانسی ویک» مسیری ۴۰۰ کیلومتری را به‌صورت شبانه‌روزی با دوچرخه طی کرد. وقتی به خواب نیاز داشت، پشت بوته‌ها دراز می‌کشید یا در چاله‌ای پنهان می‌شد. او لوازم آرایش به همراه داشت تا بتواند در طول مسیر سر و وضعش را مرتب کند و چنین به نظر برسد که برای گردش کوتاهی بیرون آمده یا کاری برای انجام‌دادن در آن محل دارد. دلیل این کار این بود که او مامور متفقین در فرانسه اشغالی بود که گشتاپو نامش را «موش سفید» گذاشته بود و برای سرش جایزه‌ای پنج میلیون فرانکی تعیین شده بود. شخصی دارای شجاعت و جرات فوق‌العاده که هزاران مبارز چریکی را در «اوورنی»[2] سازمان‌دهی و تجهیز کرد و یک نگهبان اس‌اس را با دست خالی کشت. او باید این مسیر را طی می‌کرد؛ وگرنه خودش و نیروهایش به دام می‌افتادند. بی‌سیم‌چی آنها «دنیس ریک» از ترس اسیر شدن هنگام عقب‌نشینی تجهیزات رادیویی‌اش را دفن کرده بود و کتاب رمزنگاری‌اش را از بین برده بود.

بدون داشتن رمزها راهی برای ارتباط با پشتیبانی در بریتانیا و درخواست غذا، نیرو، اسلحه، مهمات و تجهیزات دیگر و همچنین هماهنگی با سایر مبارزان وجود نداشت. ویک موقعیت نزدیک‌ترین بی‌سیم‌چی که کتاب رمز را داشت، می‌دانست؛ پس به این امید به راه افتاد که قبل از تمام‌شدن غذا یا شکست‌خوردن، بازگردد. زمانی که برگشت نه می‌توانست راه برود و نه بدون کمک از دوچرخه‌اش پیاده شود، اما رمزها را به دست آورده بود.

ویک عضو سازمانی به نام SOE[3] بود. این سازمان مبارزان چریکی پشت خطوط نیروهای محور را آموزش می‌داد، هماهنگ می‌کرد و از آنها پشتیبانی می‌کرد. این سازمان، آشفته،

1. The agony of coding
2. Auvergne
3. Special Operations Executives

جدید، نامتعارف و فاقد عمومیت بود. ماموران SOE به ابزار ارتباطی امن و سیستم رمزنگاری نیاز داشتند که قابل اطمینان و قابل حمل باشد، به‌راحتی پنهان شود و سریع باشد. این ماموران افرادی مانند «آد استارهایم»[1] را شامل می‌شدند که به «ابردین»[2] فرار کرد تا عملیات تخریبی و پیام‌رسانی رمزی را آموزش ببیند (درد رمزنگاری) تا بتواند با پاراشوت به نروژ برگردد و به تیمی از SOE کمک کند تا تاسیسات آب‌سنگین نازی‌ها را از بین ببرد. این امکان وجود نداشت که او را با دستگاه رمزنگاری ۱۱ کیلویی مستقیم وسط میدان بفرستند (مثلا در نیمه‌شب او را از هواپیما پایین بیندازند)؛ زیرا اگر او را پیدا می‌کردند، فورا دستگیر و بازجویی می‌شد.

روش استاندارد آنها استفاده از «رمزنگاری شعری»[3] بود. حروف شماره‌گذاری‌شده در شعری که از پیش بین فرستنده و گیرنده مورد توافق قرار گرفته بود، کلید رمزگشایی پیام‌ها محسوب می‌شد. خوبی این روش این بود که به هیچ تجهیزاتی نیاز نداشت، چون شعر قابل حفظ کردن بود (اما ماموران این عادت بد را داشتند که شعرهایی از کیتز، مولیر، شکسپیر و غیره را انتخاب می‌کردند که شناخته‌شده بودند).

انجام رمزنگاری به‌صورت ذهنی به اشتباهاتی ختم می‌شد که باعث می‌شد پیام‌شان برای گیرنده گنگ یا نامفهوم باشد؛ استفاده از شعرهای تکراری (یا حتی جدید) امنیت را پایین می‌آورد. مسئولان SOE اغلب یک متن را برای ماموران مختلف می‌فرستادند و برای هر کدام از رمز شخصی‌شان استفاده می‌کردند. اگر یکی از این رمزها کشف می‌شد، دشمن می‌توانست آن را با سایر رمزها مقایسه کند و هر یک از آنها را رمزگشایی کند. نهایتا اگر این رمزها یک بار کشف می‌شدند، امکان کشف مجدد آنها نیز وجود داشت؛ زیرا خود کدها تغییری نمی‌کردند.

«لئو مارکس»[4] مسئول رمز SOE با این روش مخالفت کرد (بله، اسم او واقعا مارکس بود، نکته جالب دیگر اینکه دفتر آنها در خیابان بیکر بود؛ جایی که شرلوک هلمز مشغول کشف رمزهای دیگری بود). او در کوتاه‌مدت بسیاری از ماموران SOE را متقاعد کرد که خودشان شعر بگویند یا حداقل از شعرهای غیرمتداول استفاده کنند. مثلا نانسی و یک از شعری عاشقانه استفاده می‌کرد که با عادت غلط املایی خود آن را عاشقانه‌تر کرده بود. مارکس در بلندمدت

1. Odd Starheim
2. Aberdeen
3. Poem cipher
4. Leo Marks

به‌دنبال راه‌حل کامل‌تری بود.

او راه‌حل را در «پد یک‌بار مصرف» پیدا کرد و آن را به‌صورت «پد یک‌بار مصرف الفبایی»[1] (LOP) درآورد و روی ورقه‌ای ابریشمی چاپ کرد. LOP شبکه‌ای از حروف بود که به‌صورت تصادفی تولید شده بودند و به همراه «جدول جانشینی»[2] اســتفاده می‌شدند. شبکه‌ای برای سهولت ارجاع، ۲۶ سطر و ۲۶ ستون، شــامل مجموعه‌ای از قواعد جانشینی (به جای A به علاوه A بنویسید P، به جای I به علاوه D بنویسید U). ابریشمی‌بودن ورقه‌ها، پنهان‌کردن و از بین بردن آنها را آسان می‌کرد، می‌شد آنها را در آستری کت دوخت یا به شکل توپ کوچکی درآورد، قورت داد، آتش زد یــا در توالت انداخت (وقتــی ک گ ب از پدهای یک‌بار مصرف استفاده می‌کرد، آنها را روی نیتروسلولز چاپ می‌کرد تا بلافاصله پس از مصرف منهدم شوند). ابریشم گران بود، اما مارکس ایده‌اش را به این صورت برای مافوق‌هایش مطرح کرد؛ «یا ابریشم یا سیانور» (یعنی یا بودجه را خرج ابریشم کنند یا خرج قرص‌های خودکشی برای ماموارنی که اسیر شده بودند یا به خطر افتاده بودند).

مثلا پیام شما با AT MIDNIGHT و پد حروف تصادفی با OPXCA PLZDR شروع می‌شود. جدول جانشینی را چک کنید؛ به جای A به علاوه O بنویسید J، به جای T به علاوه P بنویسید X و الی آخر. دو کلمه اول پیام شما JXFZD YXQZK خواهد بود. وقتی رمزنگاری انجام شــد، می‌توانید پیام‌تان را بفرســتید و حروف تصادفی پد را منهــدم کنید (این حروف یک‌بار مصرف هستند و هرگز دوباره استفاده نمی‌شــوند). استفاده مجدد از جدول جانشینی امنیت را به خطر نمی‌اندازد؛ بدون داشتن پد اصلی حروف تصادفی، جدول جانشینی نمی‌تواند متن پیام را به شما لو دهد؛ بلکه فقط برای رمزنگاری سریع‌تر و دقیق‌تر از آن استفاده می‌شود. شخص رمزگشــا نیز همین فرایند را از آخر به اول انجام می‌دهد. تا وقتی که فرستنده و گیرنده از پد و جدول جانشینی مشابهی استفاده کنند و از جای مشابهی در رشته حروف تصادفی کار خود را شروع کنند، پد یک‌بار مصرف می‌تواند به‌سرعت و با امنیت بالا پیام‌ها را رمزنگاری و رمزگشایی کند.

همان‌طور که «کلاود شــانون»، رمزنگار معروف آمریکایی در سال ۱۹۴۵ (و «ولادیمیر

1. Letter one-time pad
2. Substitution square

کوتلنیکف» در سال ۱۹۴۱ به‌صورت جداگانه) اثبات کرد، اگر اعداد واقعا تصادفی باشند و از کلیدها استفاده مجدد صورت نگیرد، پد یک‌بار مصرف کاملا امن است. متن رمز هر اندازه هم که زیاد باشد، هیچ حرف یا رشته حروفی در آن، به حرف متناظرش اشاره نمی‌کند. تنها چیزی که دشمن می‌تواند بفهمد طول پیام است؛ طبیعتا بسیاری از کاربران پدهای یک‌بار مصرف، رشته حروفی به پیام خود اضافه می‌کردند تا حتی طول پیام واقعی هم مشخص نباشد.

همه این ابزارها و تکنیک‌ها (کتاب‌های رمز بی‌سیم، دستمال‌های ابریشمی، شعرهای حفظ‌شده) با میزان سودمندی متفاوت، یک مشکل عمیق داشتند؛ تقارن. تمامی این روش‌ها؛ از پدهای یک‌بار مصرف امن گرفته تا شعرهای رمزنگاری‌شده شکسپیر، به این متکی بودند که گیرنده و فرستنده «کلید مشابهی» را داشته باشند. این کلید می‌توانست شعر، صفحه‌ای از یک کتاب یا خطی از یک صفحه پد یک‌بار مصرف باشد که برای رمزنگاری و رمزگشایی استفاده می‌شد. برای تایید اعتبار طرفین گفت‌وگو نیز از همین کلید استفاده می‌شد؛ رمزنگاری صحیح پیام عموما به این معنی بود که پیام از طرف شخص درستی آمده است.

این کلیدهای مشابه باعث می‌شدند خطر کشف رمز توسط دشمن در مراحل ذخیره‌سازی، اشتراک‌گذاری، ارسال و به‌روزرسانی کلیدها چندبرابر شود. کافی است چمدان‌های افراد را در گمرک متوقف کنید، از تمام صفحات رمز به‌صورت مخفیانه عکس بگیرید و در کشور خودتان به‌راحتی پیام‌های مامور مورد نظر را بخوانید (و وقتی آنها را از صحنه کنار زدید، به جای آنها پیام بفرستید). تقارن باعث می‌شد فرستنده، گیرنده و تمامی نقاط بین آن دو آسیب‌پذیر شود. سیستم رمزی نیروی دریایی آلمان (که به ماشین انیگمای معروف متکی بود)، کتابچه‌هایی داشت که با استفاده از آنها می‌توانستید دستگاه خود را با سایر بخش‌های سازمان همگام‌سازی کنید (کلیدها را متقارن نگه دارید) و از کدهای کوتاهی برای کاهش احتمال شناسایی‌شدن استفاده کنید؛ این کتابچه‌ها با جوهر قرمز روی کاغذ جوهرخشک‌کن صورتی‌رنگ چاپ می‌شدند تا با ریختن کمی آب روی آن فورا ناخوانا شود و از افتادن آن به دست دشمن جلوگیری شود.

نانسی و یک چندصد کیلومتر دوچرخه‌سواری کرد، در حالی که برای پیدا کردن کتاب رمز، احتمال دستگیر شدن، شکنجه و مرگش وجود داشت. اوضاع همین‌طور بود تا اینکه یک روز بعدازظهر در بهار سال ۱۹۷۵ کسی که وظیفه مراقبت از خانه «جان مک‌کارتی»[1]، متخصص

1. John McCarthy

کامپیوتر، در برکلی را داشت، همه چیز را تغییر داد.

دریچه مخفی

«چیزی که دقیقا به خاطر دارم، این است که در اتاق نشیمن نشسته بودم که برای اولین‌بار به ذهنم خطور کرد، بعد از پله‌ها پایین رفتم تا نوشابه‌ای بردارم و نزدیک بود یادم برود.»

«ویتفیلد دیفی» ذهنش مشغول مساله کلیدهای متقارن بود. اگر بخواهیم سیگنالی که بین دو کامپیوتر ارسال می‌شود «واضح» نباشد و هر کسی نتواند آن را بخواند، کامپیوترها باید از کلیدهای مشابه برای رمزنگاری و رمزگشایی استفاده کنند، اما این کلیدها چگونه فرستاده می‌شوند؟ اگر بتوان این کلیدها را هم در میان راه خواند، انتقال اطلاعات به‌صورت ایمن بین دو کامپیوتر (و امکان برقراری ارتباط دیجیتال مطمئن با تایید اعتبار طرفین و ایمن‌ماندن پیام) به‌شدت دشوار می‌شود.

خود شخصیت اصلی چندین بار این داستان را چه به‌صورت شفاهی و چه در چند کتاب برجسته تعریف کرده است. دیفی سوار بر ماشین داتسون ۵۱۰ خود در کشور گشت می‌زد، به کتابخانه‌ها سر می‌زد و با پژوهشگران ملاقات می‌کرد تا به دو سوال مرتبط به هم پاسخ دهد: چگونه می‌توانیم اعتبار خودمان و دستگاه‌مان را تایید کنیم (مساله‌ای که در تجهیزات نظامی، شناسایی دوست از دشمن یا IFF نامیده می‌شود) و چگونه می‌توانیم ثابت کنیم که ارتباط‌مان محرمانه است. او در نهایت وظیفه مراقبت از خانه مک‌کارتی را بر عهده گرفت، در حالی که مسیر دیگری را برای حل مساله رمزنگاری مدرن در پیش گرفته بود. آن روز بعدازظهر در ماه مه، چند مساله مختلف را با استفاده از رمزنگاری کلید نامتقارن حل کرد؛ با اینکه نزدیک بود به خاطر یک نوشیدنی راه‌حلش را فراموش کند، در آن نقطه از اتاق نشیمن تاریخ متحول شد.

این به آن معنی نیست که رمزنگاری کلید نامتقارن (یا عمومی) هرگز کشف نمی‌شد. افراد مختلفی در حال بررسی این مساله از جهات مختلف بودند. «مارتین هلمن»، همکار و کمک‌نویسنده دیفی نیز در حال بررسی آن بود؛ «ریچارد شروپل» که زندگی خود را وقف رمزگذاری کرده بود نیز همین‌طور. «رالف مرکل»، دانشجوی کارشناسی دانشگاه برکلی هم روی ایده‌های مشابهی کار می‌کرد؛ مجموعه‌ای از پیچیدگی‌ها که کلید محرمانه مشترکی را بین طرفین ایجاد کند، بدون اینکه کلید مشترکی از قبل وجود داشته باشد. او برای اولین‌بار این ایده

را در سال ۱۹۷۴ مطرح کرد. مرکل به‌عنوان یک ریاضی‌دان برجسته و متخصص رمزنگاری، طرفدار منجمد کردن انسان و پیشرفت بشری، بارها در این کتاب ظاهر می‌شود؛ آثار او در رابطه با داده‌های جفت‌درهم[1] یا درخت مرکل[2]، اساس بلاکچین بیت‌کوین را پایه‌گذاری می‌کند.

آیا می‌توان بدون کلید مشترک اولیه، پیامی را به شکلی ایمن رمزنگاری کرد که فقط طرفین مجاز قادر به خواندن آن باشند؟ «جیمز الیس»، «کلیفورد کاکس» و «مالکوم ویلیامسون» پیش‌تر در بریتانیا رمزنگاری نامتقارن را به‌طور مستقل تحت عنوان «رمزنگاری غیرمحرمانه» کشف کرده بودند. این کشف طی پیشرفت‌های اولیه سال ۱۹۶۹ و راه‌حل ریاضیاتی نظریه اعداد، در سال ۱۹۷۳ صورت گرفت. آنها برای سازمان مرکزی ارتباطات دولت (GCHQ) کار می‌کردند که معادل آژانس امنیت ملی ایالات متحده (NSA) است، به همین خاطر دستاورد آنها تا مدت‌ها محرمانه ماند.

آنچه دیفی، الیس، کاکس، ویلیامسون، هلمن، مرکل و دیگران درصددش بودند، دو نیم کردن کلید بود. تقارن به این معنی است که از یک کلید برای رمزنگاری و رمزگشایی استفاده شود؛ اگر بتوان این عملکردها را به دو کلید مختلف، اما مرتبط تبدیل کرد، می‌توان به‌راحتی یکی را در اختیار دیگران گذاشت، بدون اینکه خطر لو رفتن کلید دیگر وجود داشته باشد. این موضوع می‌توانست مساله دشوار مبادله کلیدهای متقارن را در کسری از ثانیه حل کند.

آرایش نامتقارن به این معنی است که می‌توانید به‌راحتی کلید «عمومی» خود را به اشتراک بگذارید، بدون اینکه امنیت ارتباط خود را به خطر بیندازید. پیام‌هایی که با این کلید عمومی رمزنگاری شده باشند، تنها از طریق یک کلید «خصوصی» قابل خواندن هستند که در اختیار کاربر است. این کلیدها به یکدیگر شباهت دارند، اما نمی‌توان یکی را با داشتن دیگری به دست آورد، یعنی نمی‌توان کلید خصوصی را از کلید عمومی استخراج کرد. به جای اینکه نگران لو رفتن امنیت کلیدهای متقارن به خاطر حلقه‌های ضعیف زنجیره حفاظت باشیم و به کلیدهای متقارن عامل خارجی برای ارتباط ایمن بین کامپیوترها اعتماد کنیم، خودمان می‌توانیم یک جفت‌کلید ایجاد کنیم، کلید عمومی را با هر کسی که می‌خواهیم به اشتراک بگذاریم و کلید خصوصی را فقط برای خودمان به‌صورت محرمانه نگه داریم. دیفی می‌گوید:

1. Hashing paired data
2. Merkle Tree

«کمال رمزگذاری در این است که مجبور نباشید مستقیما به کسی در ارتباط خود اعتماد کنید.»

به این منظور، متخصصان رمزگذاری باید مجموعه‌ای از «توابع یک‌طرفه» را پیدا می‌کردند. آنها باید محاسبه یک تابع و رسیدن به نتیجه را بسیار آسان و در عین حال به‌عقب‌برگشتن از نتیجه، یعنی معکوس کردن تابع را بسیار دشوار («از نظر محاسباتی غیر ممکن») می‌کردند. این کار به‌صورت یک‌طرفه انجام می‌شود؛ مانند دری که اجازه ورود می‌دهد، ولی اجازه خروج نمی‌دهد. می‌توانیم با قلم و کاغذ و محاسبات بسیار ابتدایی دو عدد صحیح بسیار بزرگ را در یکدیگر ضرب کنیم، اما مشخص کردن اینکه از ضرب کدام دو عدد اول به این عدد رسیده‌ایم، کار بسیار دشواری است؛ جست‌وجوی فراگیر طولانی در فضایی بی‌کران. اگر کلیدی داشته باشیم که به اندازه کافی قوی باشد، فرایند یافتن راه‌حل آن از طول عمر ما، تاریخ پیدایش خط، تکامل بشری و تاریخ زمین‌شناسی نیز بیشتر طول می‌کشد!

این تابع جزء مهم دیگری نیز دارد؛ یک دریچه مخفی. اگر به اعداد نیمه‌اول[1] برسید، می‌توانید به‌سرعت درستی آنها را بررسی کنید. وجود دریچه مخفی به این معنی است که با داشتن اطلاعات درست، می‌توان به‌راحتی تابع را معکوس کرد. دیفی و هلمن می‌نویسند: «سیستم رمزی دارای دریچه مخفی را می‌توان برای تولید سیستم توزیع کلید عمومی به کار برد.» یعنی در عمل و در سطوح بالا با داشتن مجموعه درستی از توابع می‌توانید پیامی را رمزنگاری کنید، بدون اینکه از کلید مورد نیاز برای رمزگشایی آن اطلاع داشته باشید. کسی که این کلید را دارد، می‌تواند به‌سرعت و با کمک «سخت‌افزار دیجیتال ارزان‌قیمت» رمزگشایی را انجام دهد و حتی اگر دشمن بتواند پیام رمزنگاری‌شده و کلید عمومی را به دست بیاورد، باز هم نمی‌تواند کلید خصوصی را پیدا کرده و پیام را بخواند. دیفی و هلمن تابع مشخصی را برای این نوع عملیات یک‌طرفه در نظر نداشتند و تلاش‌های اولیه به‌راحتی با استفاده از محاسبات سریع قابل حل بود. «ران ریوست»، «ادی شمیر» و «لئونارد ادلمن» چند سال بعد در سال ۱۹۷۸ حوزه خاص فاکتورگیری اعداد اول را دگرگون کردند[2] و چیزی را آغاز کردند که «جان فرانسوا بلانشت» (متخصص زیرساخت‌های محاسباتی و رمزنگاری) آن را این‌گونه توصیف می‌کند: «هجوم همگانی برای کشف مسائل مقتضی دیگری که حول کشف فرضیات محاسباتی مختلف

1. Semi-prime numbers

۲. نام الگوریتم و شرکت RSA از این سه نفر گرفته شده است.

(فرض‌های متمایز در رابطه با دشواری محاسبه توابع معکوس) می‌گردد.»

استفاده از تشبیه در این حوزه می‌تواند گمراه‌کننده باشـــد. خصوصیاتی وجود دارد که فقط مختص اعداد اول و نیمه‌اول و توابع هم‌ارز مختلف اســـت که باعث می‌شـــود برخی اعداد و عملیات‌ها برای این هدف چندان مناسب نباشند. اما این سوال ساده هنوز باقی می‌ماند: این عدد چگونه به وجود آمده است؟

۱۲۴۶۲۰۳۶۶۷۸۱۷۱۸۷۸۴۰۶۵۸۳۵۰۴۴۶۰۸۱۰۶۵۹۰۴۳۴۸۲۰۳۷۴۶۵۱۶۷۸
۸۰۵۷۵۴۸۱۸۷۸۸۸۳۲۸۹۶۶۶۸۰۱۱۸۸۲۱۰۸۵۵۰۳۶۰۳۹۵۷۰۲۷۲۵۰۸۷۴۷۵
۰۹۸۶۴۷۶۸۴۳۸۴۵۸۶۲۱۰۵۴۸۶۵۵۳۷۹۷۰۲۵۳۹۳۰۵۷۱۸۹۱۲۱۷۶۸۴۳۱۸۲۸۶
۳۶۲۸۴۶۹۴۸۴۰۵۳۰۱۶۱۴۴۱۶۴۳۰۴۶۸۰۶۶۸۷۵۶۹۹۴۱۵۲۴۶۹۹۳۱۸۵۷۰۴۱۸
۳۰۳۰۵۱۲۵۴۹۵۹۴۳۷۱۳۷۲۱۵۹۰۲۹۲۳۶۰۹۹

وقتی دیفی و هلمن روی جزئیات سیستم دو نیم کردن کلید کار می‌کردند، مشخصه دیگری از این سیستم را کشـــف کردند. اگر یک کلید دوتایی (عمومی ـ خصوصی) به همراه دریچه مخفی وجود داشته باشد، می‌توان از کلید خصوصی برای رمزنگاری پیام استفاده کرد و با کلید عمومی متناظر آن پیام را رمزگشایی کرد. این کار به هیچ‌وجه محرمانه نبود، اما اعتبارسنجی را ممکن می‌کرد؛ کلید عمومی باید بین چندین نفر توزیع شود و هر کسی که آن را داشته باشد، می‌تواند پیامی را که با استفاده از کلید خصوصی رمزنگاری شده، بخواند. رمزگشایی پیام با کلید عمومی اثبات می‌کرد که پیام با کلید خصوصی رمزنگاری شده است. اگر کلید خصوصی محافظت شده باشد (به‌صورت محرمانه تنها در دست سازنده‌اش وجود داشته باشد) به این معنی است که می‌توان مطمئن بود پیام از طرف دارنده کلید خصوصی تولید شده و آن را در مسیر تغییر نداده‌اند. پس این امکان وجود داشت که معادل امضای کتبی و پاکت نامه مهروموم‌شده برای پیام فراهم شود.

این سیستم می‌توانست در عین حال واقعی بوده و نتایج قابل اثباتی داشته باشد. دیفی و هلمن در مورد قرارداد و رسید حرف می‌زدند؛ ریوست، شـــمیر و ادلمن در مورد «امضا»، «اثبات» و «قضاوت» حرف می‌زدند و بلانشـــت اشـــاره می‌کند: «نمی‌توان به‌راحتی الگوریتم‌های رمزگذاری را به نوشتن اسم شخص روی کاغذ تشـــبیه کرد.» اول از همه مشکل تکثیر وجود داشت. دیفی و هلمن می‌نویسند: «از آنجا که هر سیگنال دیجیتالی قابل تکثیر است، امضای

دیجیتال حقیقی باید قابل تشخیص باشد، اما قابل شناسایی نباشد.»

قابل تشخیص اما غیرقابل شناسایی؛ این دستور دشـــواری بود که در اسکناس‌ها هم با آن مواجه بودیم. چطور می‌توان شیء قابل تکثیری را تولید کرد (پول چاپی و امضا) که طرف دیگر نتواند آن را تکثیر کند؟ باید قابلیت اعتبارسنجی داشته باشد، اما قابل کپی‌کردن نباشد؛ به‌راحتی تولید شود، اما تکثیر نشود؛ قابل تشخیص باشد، اما قابل شناسایی نباشد و در نهایت بتوان قابل اطمینان بودن آن را اثبات کرد (پس از گذشت دهه‌ها، بیت‌کوین به سیستمی تبدیل شد که کاملا از امضاهای دیجیتال رمزگذاری‌شده تشکیل شده اســـت). دیفی و هلمن می‌نویسند: «برای ایجاد سیستمی که بتواند ارتباطات کاملا الکترونیکی را جایگزین قراردادهای کتبی کند، باید پدیده‌ای دیجیتال را کشف کنیم که خصوصیاتی مشابه امضای کتبی داشته باشد.» بلانشت در جواب، این سوال را مطرح می‌کند که «اصلا امضای کتبی چیست؟»

خصوصیاتی مشابه امضای کتبی

وقتی «سیلویا هالند» در سال ۱۸۶۵ فوت کرد، از خودش وصیت‌نامه‌ای به جا گذاشت که در آن بخشی از ثروت هنگفت خود را به خواهرزاده‌اش «هتی رابینسون» واگذار کرده بود. رابینسون به‌صورت مخفیانه وصیت‌نامه دیگری درست کرد و تمام دارایی او را به نام خود زد. مامور اجرای وصیت‌نامه این موضوع را نپذیرفت و کار به دادگاه کشید. وصیت‌نامه دوم به دستخط رابینسون بود که از طرف خاله پیر و ناتوانش نوشـــته بود. فقط امضای انتهای برگه متعلق به هالند بود (یا نبود). میلیون‌ها دلار پول به این موضوع بستگی داشت.

سه کلمه «سیلویا آن هالند» یکی از دستخط‌هایی در طول تاریخ بود که بررسی زیادی روی آن انجام گرفت. از نظر زمان و تخصص صرف‌شده، تنها چند اثر هنری وجود دارد که به این اندازه مورد توجه قرار گرفته باشد؛ تصویر امضا بزرگ‌نمایی شده و زیر میکروسکوپ بررسی شد، متخصصان خط، بانکداران، دانشمندان، عکاسان و حکاکان آن را به‌دقت موشکافی کردند.

مشکل این نبود که دو امضا با یکدیگر تفاوت زیادی داشته باشند، مشکل این بود که بیش از حد شبیه یکدیگر بودند. آنها دقیقا مشابه یکدیگر بودند، نقطه‌به‌نقطه، حتی محل قرارگیری و فاصله آنها از حاشیه صفحه یکسان بود. امضا اصل به نظر نمی‌رسید؛ بلکه انگار کپی شده بود. ده‌ها نمونه دیگر از امضای هالند اختلافاتی را نشان می‌داد، اما این امضاها مربوط به زمان‌های

مختلف بودند. امضای شما روز به‌روز، ساعت به‌ساعت و از کاغذی تا کاغذ دیگر چقدر فرق می‌کند؟ بانکداران و حسابداران (کسانی که در تایید امضاها سابقه داشتند) در مورد درستی آن نظرات مختلفی داشتند. «لوئیس آگاسیز»[1] با استفاده از فناوری میکروسکوپ پیشرفته‌ای رد نوک مداد را دنبال کرد، اظهارات او به جست‌وجوگری شباهت داشت که به‌وسیله بالون بر فراز طبیعتی بیگانه پرواز کرده باشد؛ او آثار اندکی از جوهر پیدا کرد که مانند گل در بستر رودخانه رسوب کرده بودند و هیچ ردی از لایه‌های پاک‌کن نیز مشاهده نمی‌شد.

«بنجامین پیرس» (ستاره‌شناس) و پسرش چارلز سندرز پیرس (دانشمند، فیلسوف و منطق‌دان) رویکرد بسیار متفاوتی را در پیش گرفتند؛ آنها به سمت ریاضی و احتمالات رفتند و از پاسخ حسی افرادی که در زمینه امضا سابقه داشتند، دوری کردند. پدر و پسر در امضای هالند دقیقا ۳۰ ضربه را روی کاغذ شناسایی کردند، ده‌ها نمونه دیگر را بررسی کرده و تغییرات آنها را ثبت کردند و در نهایت مدلی آماری از احتمال واقعی‌بودن امضای موجود در وصیت‌نامه مورد بحث ارائه کردند. بنجامین پیرس در روزی در ماه ژوئن در دادگاه حاضر شد تا احتمال واقعی‌بودن امضا را به‌صورت عددی بیان کند، گفت: «احتمال امضاهایی چنین مشابه فراتر از تجربه بشری است.»

چارلز پیرس بعدها به بنیان‌گذاری فلسفه عمل‌گرایی و رشته نمادشناسی در ایالات متحده کمک کرد. او به منطق نمادین علاقه داشت و به‌طور خاص علاقه داشت بداند چگونه بین نمادهایی که به اشیای خاص دلالت می‌کنند و نمادهایی که خودشان یک شیء هستند، تمایز قائل می‌شویم: معنی عدد صفر یا علامت دلار یا متر یا عقربه فشارسنج چیست و چگونه کار می‌کند؟ او و پدرش در پرونده وصیت‌نامه هالند باید امضا را از تصویر امضا تشخیص می‌دادند و توضیح می‌دادند چطور می‌توان حضور انسان و رضایت آگاهانه او را در سندی کتبی تشخیص داد و وجود آن را از معنی‌اش تمییز داد.

قابل تشخیص، اما غیر قابل شناسایی

امضا را با یک روش واحد می‌توان شناسایی کرد؛ اینکه شاخصی از یک رویداد است،

1. Louis Agassiz

شخصی که چیزی را می‌نویسد. چارلز سندرز پیرس به‌عنوان یک نمادشناس عنوان می‌کند برای اینکه شیء یا نشانه‌ای بتواند «علم به چیز دیگری را منتقل کند که نماینده یا نشانگر آن است» سه راه وجود دارد؛ یکی از آنها «شاخص» است؛ نشانه‌ای که علمی را از طریق ارتباط فیزیکی با مصداق خود به ما منتقل می‌کند. می‌توانید آن را به شکل انگشت اشاره در نظر بگیرید که به چیزی اشـــاره می‌کند. به این ترتیب بدون حرف‌زدن ارتباط برقرار می‌کنید. مشاهده دود از راه دور، ستاره قطبی، حباب موجود در تراز بنایی، شاقول، نقشه، طرز راه رفتن ملوانان در خشکی، اثر انگشت باقی‌مانده روی شیشه؛ همگی شاخص محسوب می‌شوند (نشانه‌هایی که از طریق ارتباط فیزیکی اطلاعاتی را منتقل می‌کنند). امضا مجموعه‌ای از نمادهای مکتوب مبتنی بر قرارداد و کاربرد آن اســـت (همان‌طور که پنج حرف «هـ»، «ا»، «ل»، «ن» و «د» نمادهایی قراردادی هســـتند)، اما شاخص نیز محســـوب می‌شود؛ زیرا چیزی اســـت که توسط دستی ثبت شده که زمان و رویداد خاصی را به شخص ربط می‌دهد. وقتی «کوییکوئگ»[1] در رمان «موبی‌دیک» برای زوبین‌داری کشتی نام‌نویسی می‌کند «قلمی را که به دستش دادند، گرفت و روی کاغذ، در محل مناسب، شکل دایره عجیبی را کشید که روی بازویش خالکوبی شده بود.»

مهر خاتم، مهر چینی، مهر ژاپنی (اینکان)، مهر کره‌ای (دوجانگ و گوکسائه)، اثر انگشت و طغرای منحصربه‌فرد سلاطین عثمانی: تاریخ هزاران‌ساله چنین اشیایی که برای تایید اعتبار استفاده می‌شوند، به تضاد شیئی وابسته اســـت که منحصربه‌فرد، اما قابل تکرار بوده و هر بار نمایانگر لحظه‌ای خاص از وجود باشد. باید آن‌قدر شبیه خودش باشد که بدون شباهت کامل هم قابل تایید باشد (قابل تشخیص، اما غیرقابل شناسایی). امضا کردن یا اعتبار بخشیدن را می‌توان به دیگران نیز محول کرد؛ از کابینه رئیس‌جمهور یا نخست‌وزیر گرفته تا ماشین امضای خودکار و مهر پلاستیکی. «هیلل شـــوارتز»[2]، متخصص تاریخ فرهنگی، می‌گوید امضا پس از روزهای خوش جنبش رمانتیک اروپا ارزش فرهنگی پیدا کرد؛ چراکه روی سبک و استعداد شخصی تمرکز داشت. شـــوارتز می‌نویســـد: در زمانی که چاپ و تکثیر ممکن بود «هرکس نگارش خاص خود را داشت که با ابزار چاپ قابل تکثیر نبود، مانند خط مارپیچی که در انتهای امضا کشیده می‌شـــود». این خط مارپیچ اقدامی احتیاطی برای جلوگیری از جعل امضا بود؛

1. Queequeg
2. Hillel Schwartz

قابل تشخیص، اما غیرقابل تکثیر، سبک انسانی منحصر به هر فرد.

امضای دیجیتال به‌عنوان امری به‌ظاهر مشابه برای اعلام حضور فردی، پدید آمد تا به پیامی که با کلید خصوصی متناظر کلید عمومی ارسال می‌شود، اعتبار ببخشد و همان‌طور که دیفی و هلمن انتظار داشتند به «پدیده‌ای دیجیتال با خصوصیات مشابه امضای کتبی تبدیل شود.» اما امضای دیجیتال دقیقا «خصوصیات مشـــابه» امضای کتبی را نداشت. امضاهای کتبی به یکدیگر شباهت دارند، اما دقیقا یک‌شکل نیستند. چیزی که امضای معتبر را از جعلی متمایز می‌کند، اختلاف جزئی شخصی است که دســـتگاه فتوکپی قادر به ارائه آن نیست. امضا، در موقعیت‌هایی مانند شهادت‌دادن، مقامات رســـمی مانند دفاتر اسناد رسمی و وکلا و سیستم اسنادی مانند چک، قرارداد و فرم‌ها از نظر فنی نقشی ساده و از نظر اجتماعی نقشی پیچیده دارد.

«پدیده دیجیتال» امضای رمزنگاری‌شده، خانواده در حال رشدی از موضوعات ریاضیاتی جالب توجه، فرایندهای نرم‌افزاری و مدل‌های مختلف بود. به قول بلانشت، این عناصر «به شـــکل خلاقانه‌ای کنار یکدیگر قرار گرفته‌اند و جهشـــی را در امضای دیجیتال رقم زده‌اند»؛ داستانی عجیب از روش‌های جدیدی برای تایید، اعتباربخشی، تصدیق یا بازبینی؛ افسانه‌هایی با نام‌هایی مانند امضای یک‌بارمصرف، امضای چندپروکسی، امضای حلقوی، امضای کاملا مخفی، امضای انکارناپذیر، امضای فوروارد ایمن، امضای بدون خرابی، امضای سرحدی، امضای چندگانه و امضای مخصوص تاییدکننده.

گاهی اوقات نیز متخصصان مجبور می‌شدند از تشبیهات غیردیجیتال استفاده کنند؛ جوهر نامرئی، پاکت امضاشده، تمبر قطعی، قفل و کلید، صندوق امانات، چک بانکی، اوراق قرضه حامل و اسکناس. «دیوید چام» (کارآفرین و رمزنگار) می‌نویسد: «پاکت سربسته‌ای را فرض کنید که در آن کاغذ کربن گذاشته شده و حاوی یک سند نامعلوم است؛ پشت آن نیز تمبر دفتر اسناد رسمی خورده است.» او اولین طرح پول دیجیتال را با اســـتفاده از این مفهوم عجیب به وجود آورد؛ پول دیجیتالی که انتظار داشت از آینده‌ای مبتنی بر دیکتاتوری پیشگیری کند.

فصل چهارم

عامل محرمانگی

کار خود را با کابوس نظارت و کنترل جمعی شـــروع می‌کنیم که پول الکترونیکی در ســـال ۱۹۷۵ آن را رقم زد. با در نظر گرفتن پیش‌بینی تراکنش‌های الکترونیکی و تجارت کامپیوتری و ترس از آنها، کار دیوید چام را بررســـی می‌کنیم. پروژه دیجی‌کش او پروتکلی پولی بود که بانک‌های موجود می‌توانســـتند آن را به‌صورت دیجیتال صادر کرده و بازخرید کنند. شکست این پروژه چارچوبی را برای کسانی بر جای گذاشت که هدف‌شان ایجاد انواع جدیدی از پول دیجیتال بود؛ نه فقط انتقال آن.

انرژی سازمان‌یافته

پیش از هر چیز بیایید رویاها را بررسی کنیم

«مارتین گرینبرگر» در ســـال ۱۹۶۴ در مقاله «کامپیوترهای فردا» با عنوان فرعی «جوامع کامپیوتری‌شده» آن را «بهتر از پول» خواند. او مقاله‌اش را در مجله آتلانتیک منتشر کرد؛ همان مجله‌ای که در سال ۱۹۴۵ پیش‌بینی برجســـته «وانوار بوش»[1] از سیستم پروتوهایپرتکست را با عنوان «آن‌گونه که فکر می‌کنیم»[2] منتشـــر کرده بود. گرینبرگر از روی قرائن، «سودمندی اطلاعاتی»[3] آینده و کاربردهای آن را پیش‌بینی می‌کرد: «سیســـتم‌های اطلاعات پزشکی»، «کتابخانه‌های اتوماتیک»، «ســـرویس‌های شبیه‌ســـازی»، «طراحی و اصلاح کنسول‌ها... جوامع کامپیوتری». کلید همه اینها دستیابی به پلتفرمی «بهتر از پول» است: «این کارت که بعضی‌ها آن را «کلید پول» می‌نامند، در کنار پایانه‌ها و انتقال اطلاعات ساده، می‌تواند نیاز به ارز، چک، صندوق فروشگاهی، فاکتور خرید و پول خرد را به‌کلی از بین ببرد.»

منظور گرینبرگر این بود که زیرساختی شـــبیه کارت اعتباری ایجاد شود که بر سیستمی از خطوط تلفن همگانی و بانک‌ها و شرکت‌های پرداختی موجود مبتنی باشد، البته به‌علاوه اندکی جادوی آینده. او وعده دیگری نیز داد: «ضمنا فرایند پذیرش پول الکترونیکی مزیت دیگری نیز دارد؛ دست دزدهای مختلف از پول شما کوتاه می‌شود. ممکن است افرادی که بیکار شده‌اند از طریق تقلب در امور حسابداری به‌دنبال اختلاس باشند، اما راه‌هایی وجود دارد که کامپیوتر می‌تواند بدون سروصدا و بدون احتمال فساد، پلیس را از عملیات خود مطلع کند.»

1. Vannevar Bush
2. As We May Think
3. Information utility

«جان مک‌کارتی»، متخصص کامپیوتر، شش سال بعد در کنفرانسی در شهر بوردو در مورد چیزی مشابه «کنسول‌هایی» صحبت می‌کرد که گرینبرگر وعده داده بود، در حالی که برای عملی کردن آنها عزم بیشتری داشت (جان مک‌کارتی همان شخصی است که «ویتفیلد دیفی» وظیفه مراقبت از خانه‌اش در برکلی را بر عهده گرفته بود و به ایجاد رمزنگاری با کلید عمومی کمک کرد). مک‌کارتی صریحا در مورد نقش «پول» سخن می‌گفت. پول الکترونیکی اشکال جدیدی از تجارت الکترونیکی را ممکن می‌ساخت. او تبلیغات، پرداخت پول برای اطلاعات و مقالات و انواع ناشناخته‌ای از تراکنش را در نظر داشت و «تاثیری پیچیده روی خریدوفروش» را پیش‌بینی می‌کرد. اما چگونه می‌توان صحت این تراکنش‌ها را بررسی کرد؟ با اینکه اکنون ممکن است ساده به نظر برسد، ولی بررسی یک تراکنش ظرافت‌های خاصی از قبیل هویت، اعتبار، رسید و گواهی را شامل می‌شود.

«دی هاک»[1]، مدیرعامل ویزا، پنج سال بعد به‌دنبال جوابی برای این سوال بود. هاک به شرکتی تعلق داشت که افرادی مانند «باکمینستر فولر»[2]، معمار گنبدهای ژئودزیک و شبکه‌های جهانی و «استفرد بیر»[3]، متخصص ارتباطات و مشاور مدیریتی عضو آن بودند. هاک که مجذوب نظم و سازمان‌دهی خودکار فرایندهای طبیعی شده بود، تمایل نداشت فقط کسب‌وکاری را راه‌اندازی کند که به «انتقال وجه الکترونیکی» (EFT) اختصاص داشته باشد. نظر او بر این بود که «مبادله الکترونیکی ارزش» (EVE) را از نظر اجتماعی دگرگون کند. EVE آینده پول بود. او می‌نویسد: «داده‌های حرفی-عددی تضمین‌شده» با «انرژی سازمان‌یافته» که به‌راحتی در شبکه‌های کامپیوتری در سراسر دنیا منتقل می‌شوند.

هاک، EVE را سیستمی مشابه اینترنت می‌دید که تازه به وجود آمده بود و آن را شبکه‌ای جهانی با مجموعه فرضیات آرمانی می‌پنداشت. طرح او برای سازمان مرکزی EVE دفتری دایره‌وار بود که به شکلی نمادین چهار گوشه کره زمین را نشان می‌داد و به هر منطقه فرهنگی بخشی اختصاص داده شده بود و اتاقک‌هایی برای ترجمه همزمان زبان‌های مختلف در آن وجود داشت. قرار بود EVE عصر جدیدی را در جامعه سایبری رقم بزند.

اما نکته دیگری نیز وجود داشت؛ چه چیزی داده‌های حرفی-عددی را که قرار بود

1. Dee Hock
2. Buckminster Fuller
3. Stafford Beer

معادل پول باشـــند، «تضمین می‌کرد»؟ چه چیزی آن جریان انرژی پول را هدایت یا متوقف می‌کرد؟ نظارت.

بهترین سیستم نظارت قابل تصور

اکنون به بخش کابوس‌ها می‌رسیم

«پاول آرمر»، متخصص کامپیوتر دانشگاه استنفورد در سال ۱۹۷۵ برای ژورنال «کامپیوتر و مردم» مقاله‌ای می‌نویسد. او مقاله‌اش را بر اساس شـــهادتی که در مجلس داده بود، نوشته بود. کتاب‌های پیشنهادی‌اش «۱۹۸۴» از جورج اورول، یادداشت‌های نیکسون در رابطه با اجتماع هوش داخلی و «جنگ علیه یهودیان ۱۹۴۵-۱۹۳۳» نوشته «داویدوویتز»[1] را شامل می‌شد. مقاله آرمر به طرز شگفت‌آوری مشکل نظارت را که از اعتبارسنجی پول الکترونیکی ناشی می‌شد، پیش‌بینی کرده بود. او می‌نویسد: «فرض کنید می‌خواهید کتابی بخرید، کارت خود را به فروشنده می‌دهید. فروشنده آن را در پایانه‌ای قرار می‌دهد که با بانک شما ارتباط برقرار می‌کند.» بانک تراکنش را تایید یا رد می‌کند و مشکل از همین جا آغاز می‌شود.

وقتی شما با کارت اعتباری خود کتاب را می‌خرید، سیستم پرداختی موقعیت مکانی شما را به دست می‌آورد و آن را به همراه «اطلاعات زیادی درباره تراکنش‌های مالی و همچنین زندگی شـــما» به گزارش فعالیت‌هایتان اضافه می‌کند. اگر از قبل تحت نظر پلیس بودید چه؟ «شک ندارم که از چنین سیســـتم‌هایی سوءاستفاده می‌شـــود.» وقتی کاگ‌ب در سال ۱۹۷۱ وظیفه ساخت یک دستگاه نظارت را به عهده آرمر و گروهی از متخصصان کامپیوتر و نظارت گذاشت، آنها نسخه‌ای از سیستم انتقال وجه الکترونیکی را ابداع کردند: «این سیستم علاوه بر اینکه تمام اطلاعات مالی و آماری را برای یک اقتصاد کنترل‌شده فراهم می‌کرد، بهترین سیستم نظارتی بود که بدون ایجاد مزاحمت کار می‌کرد.»

او به‌عمد یک کتاب را برای خرید فرضی‌اش مثال می‌زند؛ فرض کنید تحت نظر نیســـتید، اما خرید یک کتاب خاص شما را به فهرست افراد مظنون اضافه می‌کند. اگر مقامات تصمیم بگیرند که شما نباید این کتاب را بخوانید، آیا سیستم به‌طور خودکار خرید شما را رد می‌کند؟ یعنی پول شما فقط برای خرید کالاهای محدودی جواب می‌دهد؟

---

1. Dawidowicz

رمان «سرگذشت ندیمه»[1] نوشته «مارگارت اتوود»[2] تا حدودی یک داستان دیستوپیایی در مورد پول الکترونیکی است. حساب‌های کامپیوتری و اعتباری که به زنان تعلق دارد، از کار افتاده است. همان‌طور که اتوود می‌گوید: «اکنون که کارت‌های اعتباری وجود دارند، به‌راحتی می‌توان دسترسی به اعتبار را از مردم گرفت.» او از میان سیستم‌های سلطه، «جبر پولی» را انتخاب کرد؛ سیستمی که در آن برای هر شیء کوپن خاصی وجود داشت که قدرت انتخاب و تصمیم‌گیری را از فرد می‌گرفت. شخصیت اصلی داستان او، «آفرد»، با خود فکر می‌کند: «به پرتقال‌ها نگاه می‌کنم، هوس پرتقال کرده‌ام، اما کوپن آن را با خود نیاورده‌ام.» صورت‌های مشابهی در دنیای واقعی نیز وجود داشته و وجود خواهد داشت؛ از شهرهای شرکتی گرفته تا کوپن‌های جیره‌بندی غذایی که برای هر ایالت با رنگ خاصی مشخص می‌شود یا اعتبارات رفاهی که در ایالات متحده از طریق «انتقال الکترونیکی منافع» (EBT) منتقل می‌شود؛ مثلا از پولی که فقط مخصوص خرید مواد غذایی است، نمی‌توان برای خرید کالاهای خاصی استفاده کرد و جمع‌آوری و تحلیل داده روی آن صورت می‌گیرد.

پول الکترونیکی می‌تواند در نقش ابزاری کنترلی عمل کند که بازار را به یک سیستم پاسخگویی سریع برای نیروهای پلیس، گزارش موقعیت مکانی و جعبه اسکینر تبدیل می‌کند و شهروندان را مجبور می‌کند کاری را انجام دهند که دولت یا شرکت‌ها می‌خواهند. «ژیل دلوز»[3]، فیلسوف، در سال ۱۹۹۰ متن کوتاهی با عنوان «یادداشتی در مورد جوامع کنترل‌شده» نوشت. دلوز کار خود را با گذار میشل فوکو آغاز کرد (گذار از جامعه سلطه‌گر به جامعه منظم که نشان می‌دهد قدرت چگونه خود را در هر مرحله از زندگی نشان می‌دهد) و پرسید: آیا مردمی که در جوامع پساصنعتی، شبکه‌ای و کاپیتالیستی زندگی می‌کنند، در تلاش برای گذار و کنترل جامعه هستند؟ او برای توضیح‌دادن مقصود خود، شگرد قدرت را مثال می‌زند: «شاید پول بهتر از هر چیز دیگری تفاوت بین دو جامعه را مشخص کند.»

جامعه منظم قبلی مانند یک حصار عمل می‌کرد و سازوکارهای تثبیت‌کننده و استانداردکننده‌ای برای سازمان‌دهی نیروهای مولد داشت تا بتواند خروجی‌هایی مثل بیسکویت، شهروند، روزنامه، سرباز، ماشین فورد، جبهه راست و قطعات قابل تعویض

1. The Handmaid's Tale
2. Margaret Atwood
3. Gilles Deleuze

تولید کند. او می‌نویسد: «جامعه این کار را به‌عنوان مبنا و سازوکاری قاعده‌مند، در چارچوب پول فیزیکی انجام می‌داد که پشتوانه آن طلا بود.» جامعه کنترل‌شده در حال حاضر و در آینده نزدیک، ارزش را بر اساس «نرخ ارز شـــناور تعیین می‌کند که با توجه به نرخ مجموعه ارزهای استانداردی تنظیم شده است». سیستم کنترل می‌تواند با دانستن «موقعیت هر عنصر در فضای باز در هر لحظه» در جامعه‌ای اعمال قدرت کند که افراد آن به چشم «اعداد و ارقام» و داده‌های دیجیتالی دیده می‌شوند که به‌سادگی قابل مدیریت، ارائه، تحلیل و استفاده هستند.

دلوز (گویی گویندگی یک فیلم علمی ـ تخیلی دیستوپیایی را بر عهده دارد) می‌نویسد: «بشر دیگر بشر محدود نیست؛ بلکه بشر مقروض است.» پول در قالب کارت (پول در قالب داده) می‌تواند همه چیز را کنترل کند؛ یک جا قابل پرداخت است و جای دیگر قابل پرداخت نیست، برای خرید یک چیز قابل استفاده است و برای خرید چیز دیگری قابل استفاده نیست و اطلاعات آنی در مورد کار بر را برای رسیدگی آتی ثبت می‌کند. دلوز در اندیشه خود موارد زیر را در یک ردیف قرار می‌دهد؛ پابند مخصوص حبس خانگی و آزادی مشروط، تولید به‌موقع و زنجیره تدارکات، تلفن‌های همراه و موقعیت جغرافیایی، شناسایی اشخاص و مکان‌ها، دسترسی به پلتفرم‌های فناوری‌های ممنوعه، پرداخت دیجیتال و پول الکترونیکی؛ حوزه وسیعی که مختصری از نوع جدیدی از سلطه و نمایش و اعمال قدرت را تعریف می‌کند.

نظام سلطه منسوخ شده است

دیوید چام نیز از آینده‌ای می‌ترســـید که در آن کیف پول‌های آنلاین و سیستم‌های اعتباری به پرونده شخصی تبدیل شـــوند: «اطلاعات مربوط به پرداخت‌ها، اندک‌اندک روی هم انباشته می‌شوند.» چام نیز در سال ۱۹۸۳، هشت سال پس از آرمر، در مورد کتاب خریدن و تراکنش‌های دیگری می‌نویســـد که «اطلاعات زیادی را در مورد موقعیت، روابط و سبک زندگی فرد آشکار می‌کنند.» همان ســـازوکاری که موجب اعتماد به پرداخت‌های دیجیتال شد، می‌تواند زمان و موقعیت جغرافیایی شخص را ثبت کند که می‌توان اطلاعات زیادی را از آن به دست آورد؛ البته هنوز دستکاری کیف پول‌های آنلاین برای تعیین محدودیت، ثابت کردن یا افزایش قیمت و سازوکارهای دیگر محرومیت مالی را در نظر نگرفته‌ایم. هنگامی که چام در سال ۱۹۹۵ در مجلس صحبت می‌کرد، در مورد زندان‌های پیشرفته، وضعیت پلیس و نظام سلطه حرف زد؛ او کارت‌های اعتباری

را مانند پایانه فروش اطلاعات برای جمعیتی از انسان‌ها می‌دید که همانند «حیواناتی بودند که در مزرعه به‌صورت الکترونیکی ردیابی می‌شدند»؛ البته او راه‌حلی نیز داشت.

پیشنهاد او به جای مزارع حیوانات این بود که «خریداران و فروشندگان در میدان اصلی شهر» خرید‌وفروش کنند تا هر یک از طرفین بتواند «از منافع خود محافظت کند». او به‌منظور اینکه «برابری بین افراد و سازمان‌ها رعایت شـــود» از فناوری رمزنگاری با کلید عمومی و امضای دیجیتال استفاده کرد تا پولی را ایجاد کند که هویت خود را تایید کرده و در عین حال هویت کاربر را مخفی نگه دارد. شرکت او با نام «دیجی‌کش» که در هلند مستقر بود، این پول را «e-cash» نامید (که گاهی تحت عناوین eCash، Ecash و e-Cash نیز از آن نام برده می‌شـــود). آنها اولین پول دیجیتال واقعی و کارآمد را ایجاد کردند که جایگزینی برای سیســـتم‌های اعتباری نظارتی بود. رویکرد، اختراعات و نظریه‌های چام زمینـــه را برای بیش از یک دهه پژوهش در زمینه پول دیجیتالی فراهم کرد.

چام مجذوب ایده‌هایی مانند «سرقت اطلاعات، امنیت اسناد، هشدار سرقت، گاوصندوق، قفل‌ها و روش‌های جاسوسی» بود (از دیگر اختراعات او می‌توان به قفلی الکترونیکی اشاره کرد که می‌توانست جنس فلز کلید را تشخیص دهد، او سیستم‌های مخصوص رای‌گیری را نیز اختراع کرد). او ایده‌ای داشت که طرح کلی‌اش به امنیت اسناد قدیمی شباهت داشت. فرض کنید قصد دارید برای سندی تایید رسمی دریافت کنید، ولی نمی‌خواهید محتوای آن را نشان دهید؛ مثلا اکتشافی انجام داده‌اید و آن را یادداشت کرده‌اید و قصد دارید بدون اینکه آن را با دیگران به اشتراک بگذارید، حق امتیازش را دریافت کنید. «ماریو بیاگیولی»[1]، متخصص تاریخ علم، مساله مشابهی را در علوم رنسانس توصیف کرده است؛ مثلا وقتی «کریســـتیان هایگنز»[2] اختراع فنر مویی را در قالب یک آناگرام خبر داد («abce-filmnorstux 41353731234324 2») یا گالیله مشاهده شکل غیرطبیعی زحل را به‌صـــورت «smaismrmilmepoetaleumibunenugtauiras» اعلام کرد. چاره‌کار پیدا شد؛ یادداشت‌های مهروموم‌شده‌ای که از طریق نهادهای قابل اطمینانی مانند آکادمی علوم ارسال می‌شد. البته امکان فراتر رفتن از پاکت‌های مهروموم‌شده نیز وجود داشت.

نامه خود را به همراه کاغذ کاربن داخل پاکت بگذارید، درب پاکت را مهروموم کنید، سپس

1. Mario Biagioli
2. Christiaan Huygens

امضا و تاریخ را پشت پاکت بنویسید یا از مهر رسمی استفاده کنید. کسی که پشت پاکت را امضا می‌کند یا مهر می‌زند، خبر ندارد که به چه چیزی سندیت می‌بخشد؛ «امضای نهانی»؛ مجموعه نشانه‌هایی که به زمان خاصی اشاره کرده و محرمانه‌بودن خود را حفظ می‌کند. کاغذ کاربن، پاکت نامه و امضای پشت آن باعث می‌شود خود نامه گواه محرمانه‌بودنش باشد، نه پاکت آن؛ به این ترتیب احتمال تعویض یا بخار دادن پاکت، چراغ حرارتی و سایر ابزارهای جاسوسی باز کردن نامه هم از میان می‌رود. خود نامه می‌تواند بدون آشکار کردن هویتش، حقانیت خود را اثبات کند؛ قابل تشخیص، اما غیر قابل شناسایی.

چام روش مشابهی برای پول دیجیتال ابداع کرد. همان‌طور که می‌توانستید پول خود را به‌صورت نقدی از دستگاه خودپرداز بردارید، امکان برداشت دیجیتال نیز از آن وجود داشت، اما به این صورت که باید از کارت خاصی برای تراکنش استفاده می‌کردید یا به‌صورت اینترنتی و با استفاده از برنامه‌ای در کامپیوترتان این کار را انجام می‌دادید. با در دست داشتن کارت یا با استفاده از برنامه کامپیوتر می‌توانستید از پول دیجیتال مانند پول نقد استفاده کنید، بر خلاف تراکنش در کیف پول آنلاین که سیستم باید از راه دور اعتبار حساب شخص را چک می‌کرد و برای یکی بدهکاری و برای دیگری بستانکاری ثبت می‌کرد.

پول شما در کارت یا کیف پول دیجیتال‌تان خواهد بود، بنابراین اگر آن را گم کنید، پول‌تان را هم از دست می‌دهید، درست مثل اینکه پاکتی پر از پول را در مسیر برگشت از سر کار در مترو جا گذاشته باشید. وقتی کارت خود را در اختیار فروشنده‌ای قرار می‌دهید یا تراکنش آنلاین را در کامپیوترتان مجاز می‌کنید، سیستم آنها می‌تواند بدون نیاز به تایید هویت شما یا هماهنگی با بانک‌تان پول مورد نظر را از حساب‌تان بردارد؛ «داده‌های امن که معادل پول است» می‌تواند هویت خودش را تایید کند، درست مانند پول نقد. در نهایت، آنچه برای چام بیشترین اهمیت را داشت، این بود که e-cash به کسی که آن را برداشت و خرج می‌کرد، متصل نمی‌شد؛ فناوری اثبات بدون شناسایی که چام امیدوار بود «نظام سلطه را از بین ببرد».

عامل محرمانگی

قرار نبود e-cash منبع ارزش دیجیتال مستقلی باشد؛ چام ارز جدیدی را مطرح نکرده بود؛ بلکه سازوکاری را به بانک‌ها ارائه کرده بود تا بتوانند ارزهای موجود را به پول دیجیتال تبدیل کنند

و برعکس. «هال فینی»، برنامه‌نویسی که در پدید آمدن بیت‌کوین نقشی کلیدی داشت، وقتی در سال ۱۹۹۳ این پروژه را توضیح می‌داد، مقایسه خوبی انجام داد: بیش از یک قرن پیش و قبل از به وجود آمدن ارزهای ملی و منطقه‌ای، بانک‌های محلی بر اساس دارایی‌های خود اسکناس صادر می‌کردند. تاجری که این اسکناس‌ها را قبول می‌کرد، فرضش بر این بود که «می‌تواند ارزش معادل اسکناس را در بانک مربوطه» در قالب سکه، شمش یا هر چیز دیگری دریافت کند. بانک «کالای ارزشمند» را نزد خود نگه می‌داشت و اسکناس‌ها را به‌عنوان ابزار به گردش درمی‌آورد. تاجران در سیستم چام نیز e-cash را قبول می‌کنند؛ زیرا می‌دانند امکان نقد کردن آن به‌صورت ارز ملی در بانک مربوطه وجود دارد.

بیایید سازوکار چام را به چهار بخش تقسیم کنیم؛ خواهیم دید که هر راه‌حل به نوبه خود مساله دیگری را ایجاد می‌کند.

۱. چطور می‌توان فهمید که این پول واقعی است؟

فرض کنید می‌خواهید آنلاین خرید کنید. از بانک خود یک اسکناس ۲۰ دلاری e-cash درخواست می‌کنید. بانک این پول را از حساب شما برداشت می‌کند (درست همان‌طور که از دستگاه خودپرداز پول برداشت می‌کنید) و اسکناس e-cash جدیدی تولید کرده و به شما ایمیل می‌کند یا آن را روی یک کارت هوشمند ذخیره می‌کند. اسکناس ارزش خود را این‌گونه شرح می‌دهد: «این اسکناس به ارزش ۲۰ دلار از بانک ولزفارگو صادر شده که با درخواست کاربر پرداخت خواهد شد.» قبل از اینکه بانک اسکناس را برای شما بفرستد، آن را با استفاده از کلید خصوصی رمزنگاری می‌کند. به یاد داشته باشید هر کسی که کلید عمومی متناظر را داشته باشد، می‌تواند پیام را رمزگشایی کند، بنابراین پیامی که با کلید خصوصی رمزنگاری شده حکم نوعی امضا را دارد. بانک ولزفارگو نسخه‌ای از کلید عمومی را به‌طور گسترده بین بازاریان توزیع می‌کند؛ رستوران‌ها، فروشگاه‌ها، رانندگان تاکسی، کافی‌شاپ‌ها و تمامی فروشگاه‌های آنلاین نسخه‌ای از آن را دارند تا نرم‌افزار تراکنش بتواند فورا تعیین کند که بانک اسکناس e-cash را امضا کرده و ارزش آن چقدر است.

۲. چرا نمی‌توان آن را جعل کرد؟

رمزنگاری کلید عمومی باعث می‌شود چیز مخفیانه‌ای وجود نداشته باشد. امضای بانک که با کلید خصوصی انجام می‌شود، نشان می‌دهد که اسکناس توسط بانک صادر شده و جعل آن

را غیر ممکن می‌کند (کسی نمی‌تواند اسکناس جدیدی تولید کند که مشابه اسکناس‌های بانک باشـــد). امضا نمی‌تواند جلوی جعل را بگیرد، اما جلوی تکثیر اسکناس e-cash صادرشده را می‌گیرد. در واقع هر اسکناس فقط رشته‌ای از داده‌هاست که می‌توان در میان راه جلوی آن را گرفت و آن را تکثیر و خرج کرد، مانند کسی که برای هر یک از مغازه‌های محل، چکی به ارزش ۲۰۰ دلار می‌نویسد. به همین دلیل بانک به هر برگه از چک شـــماره سریال منحصر به‌فردی اختصاص می‌دهد. وقتی شـــیفت کاری راننده تاکسی تمام می‌شود، اسکناس‌های e-cash را که در کارت هوشمندش جمع شده، به بانک برده و به حسابش واریز می‌کند. بانک صحت امضا و ارزش اسکناس‌ها و همچنین شماره سریال‌های منحصر به‌فرد آنها را بررسی می‌کند تا مطمئن شود پیش از این به حساب واریز نشده باشند (یعنی یک اسکناس چند بار خرج نشده باشد)، سپس دلارها را به حساب او واریز می‌کند. البته این شماره سریال منحصر به‌فرد، حریم خصوصی پرداخت‌کننده را از میان می‌برد. وقتی شـــخص دریافت‌کننده آن را به حساب خود واریز می‌کند، شماره سریال نشان می‌دهد که از چه حسابی صادر شده است.

۳. آیا می‌توان از این شماره سریال برای ردیابی شخص استفاده کرد؟

راه‌حلی که چام ارائه کرد «عامل محرمانگی» بود. کاربر برای هر اســـکناس شماره سریال خاصی تولید می‌کند و آن را به بانک فرســـتاده و درخواســـت e-cash می‌کند؛ بانک با کلید خصوصی خود اسکناس ۱۰ دلاری را امضا می‌کند و همان مقدار از حساب شما کسر می‌کند. مانند گذشته می‌توانید e-cash خود را هر جا که خواستید، خرج کنید. البته با استفاده از یک حقه ریاضیاتی، شماره ســـریالی که ارســـال کرده‌اید، در عددی تصادفی ضرب شده که فقط خودتان از آن اطلاع دارید (عامل محرمانگی) و وقتی که بانک اســـکناس e-cash را به شما تحویل می‌دهد، می‌توانید قبل از خرج‌کردن، آن را بر عددی که می‌دانید تقســـیم کنید. بانک مسئولیت ایجاد اسکناس‌هایی را بر عهده دارد که می‌توانید خرج‌شان کنید یا آنها را به ارز ملی (فیات) تبدیل کنید، اما دیگر نمی‌داند (و نیازی نیست بداند) که این اسکناس‌ها از حساب شما می‌آیند. کسی که اسکناس را از شما می‌پذیرد نیز این موضوع را نمی‌داند. بانک شماره سریال اسکناس‌هایی را که گیرنده برای نقد کردن به بانک برده، بررسی می‌کند تا مطمئن شود که قبلا خرج نشده‌اند. این اعداد به هیچ داده دیگری اشـــاره نکرده و تراکنش‌های شما را به هویت‌تان متصل نمی‌کنند. مانند نامه‌ای که با کاغذ کاربن در پاکت گذاشته و پشت آن را مهر زده باشند که

نشان می‌دهد می‌توان محتویات آن را به شکل یک ۱۰دلاری نقد کرد، بدون اینکه به ثبت‌کردن نامه داخل پاکت نیازی باشد.

۴. کلاهبرداری از طریق خرج‌کردن آفلاین چطور؟

در تراکنش‌های آفلاین (برای مثال پرداخت کرایه تاکسی) این امکان وجود دارد که پیش از بررسی شماره سریال توسط بانک، یک اسکناس چند بار خرج شود (معادل دیجیتال چک برگشتی). به این ترتیب بانک اولین پرداختی e-cash را انجام داده و از انجام سایر پرداخت‌ها خودداری می‌کند و با در نظر گرفتن عامل محرمانگی راهی برای پیدا کردن شخص کلاهبردار وجود ندارد. مطمئنا چنین موضوعی بازاریان را از به کار بردن این سیستم جدید دلسرد می‌کند و در حوزه‌های پرداختی بسیاری مشکلاتی را ایجاد می‌کند؛ از فروش آفلاین (مانند دست‌فروشان و بازارهای محلی) گرفته تا سیستم‌هایی که به پرداخت آنی نیاز دارند؛ مانند گیشه دریافت عوارضی که با اسکن برچسب الکترونیکی ماشین شما، پرداخت را انجام می‌دهد. (دیجی‌کش روی ایجاد یک سیستم زیرساختی پرداخت عوارض برای هلند هم کار می‌کرد). چام، «جیل براسارد»[1] و «کلاد کریپو»[2] ضربه آخر را نیز وارد کردند و سازوکاری ریاضیاتی ایجاد کردند که طبق آن هر تراکنش e-cash یک سوال را شامل می‌شد؛ سوالی عددی در مورد اسکناس که نرم‌افزار شخص خرج‌کننده باید به آن پاسخ می‌داد. این سوال ارزش خاصی نداشت و ناشناس‌بودن اسکناس را به خطر نمی‌انداخت، اما پاسخ تکراری هویت خرج‌کننده را به دریافت‌کننده نشان می‌داد و او را از حالت ناشناس‌بودن خارج می‌کرد؛ زیرا پاسخ تکراری به این معنی بود که شخص سعی دارد یک اسکناس را دو بار خرج کند.

با مشاهده کل این سیستم می‌بینیم کسی که e-cash را نقد می‌کند، ناشناس نمی‌ماند. پس باز هم امکان رشوه و معاملات بازار سیاه وجود نداشت. در واقع چنین فعالیت‌هایی محدودتر می‌شدند؛ زیرا پولشویی در سیستم e-cash بسیار دشوارتر از پولشویی با اسکناس و مسکوکات است. چام راهی پیدا کرده بود تا نوعی پول دیجیتال تولید کند که الگوی نظارت کامل بر پول الکترونیکی را از میان ببرد. او فناوری جدیدی ایجاد کرد که از حریم شخصی افراد حفاظت می‌کرد و در عین حال به معاملات مواد مخدر، رشوه‌خواری و موارد دیگر کمکی

1. Gilles Brassard
2. Claude Cripeau

نمی‌کرد. خرج کردن آن غیر قابل ردیابی بود؛ مگر اینکه خرج‌کننده سعی می‌کرد سیستم را فریب دهد که در این صورت شخص سوءاستفاده‌کننده هویت خود را آشکار می‌کرد.

از نظر فنی، e-cash هنوز مشکلات پیچیده‌ای داشت (مانند پول خرد، استرداد وجه و غیره) و موارد بسیاری باید در آینده بهبود می‌یافتند، اما ساختار این سیستم کارآمد و منسجم بود؛ پول دیجیتال ناشناس که در برابر نظارت، جعل و تقلب ایمن بود، همان‌طور که چام در مجلس عنوان کرد: «این سازوکار از کدهای پیشرفته‌ای استفاده می‌کند که مشابه‌شان برای حفاظت از مواد هسته‌ای، اطلاعات سری و انتقال وجه مورد استفاده قرار می‌گیرد.» این پول بسیاری از چالش‌های مرتبط با حریم خصوصی را پشت سر گذاشت و این کار را به گونه‌ای انجام داد که زیرساختی برای فعالیت‌های مجرمانه ایجاد نکرده باشد.

وعده او تهدیدی ضمنی نیز به همراه داشت؛ او اخطار می‌دهد: «اگر ما به‌درستی ارزهای ملی را به شکل الکترونیکی تبدیل نکنیم، بازار آنها را دور زده و ارزهای دیگری ایجاد می‌کند.» این پیش‌بینی چیزی بود که اکنون شاهد عواقبش هستیم.

فضای طراحی مخصوص

در اوایل دهه ۱۹۹۰، دیجی‌کش که در هلند مستقر بود، برنامه‌ای آزمایشی را در بانکی در سنت‌لوئیس اجرا کرد. این شرکت به‌شوخی، نوعی «دلار سایبری» بدون پشتوانه را معرفی کرد که می‌شد برای خرید تی‌شرت، مقالات دانشنامه بریتانیکا، متن روتین قدیمی «مانتی پایتون»[1] و آثار پیشین چام از آن استفاده کرد. چام در حال عقد قرارداد با دو یچه‌بانک بود و پژوهش‌های مختلفی؛ از سنگاپور گرفته تا انگلستان در حال انجام بودند. نرم‌افزار دیجی‌کش برای تمامی سیستم‌عامل‌های رایج وجود داشت و در مرورگر موزاییک[2] نیز قرار گرفته بود. آی‌ان‌جی، ویزا، مایکروسافت و مجموعه‌ای از بانک‌ها سعی می‌کردند با دفاتر دیجی‌کش در آیندهوون[3] ارتباط برقرار کنند.

پیش از اینکه دهه ۱۹۹۰ به اتمام برسد، دیجی‌کش ورشکسته شد.

دلایل این ورشکستگی پیچیده بوده و هنوز مورد بحث است، اما فناوری و میراثی که

1. Monthy Python
2. Mosaic
3. Eindhoven

دیجی‌کش برای ســازندگان ارزهای دیجیتال و پول‌های فرضی به جا گذاشت، مشخص بود؛ یک الهام و یک اخطار. «جان فرانسوا بلانشــت» در این‌باره می‌گوید: «چام مسیر پایداری را برای پژوهش و مهم‌تر از آن فضای طراحی مخصوصی را آشــکار کرد. این فضا نشان داد که لزومی ندارد کامپیوترها با نظارت و کنترل اجتماعی پیوند بخورند و اینکه برنامه‌های پژوهشی علمی منســجم و خلاقانه را می‌توان به‌وضوح از طریق اهداف اجتماعی پیش برد (که در این مورد، حفاظت از حریم شخصی، ناشناس ماندن و مشارکت دموکراتیک را شامل می‌شود).» این فضای طراحی و اهداف اجتماعی زمینه آزمایش‌های بعــدی را فراهم کردند؛ افرادی که ناشناس‌بودن همه‌جانبه را می‌خواســتند، یا به‌دنبال پولی با ویژگی‌های جدید بودند یا به‌دنبال این بودند که پول دیجیتال را دائمــی کنند؛ به گونه‌ای که دیگر به بانک‌ها (یا حتی کشــورها) وابسته نباشد.

تلاش‌های چام و همکارانش و صعود و ســقوط دیجی‌کش نقطه مبنایی را برای طرح‌های دیگری فراهم کرد. پس از e-cash «قراردادهای هوشــمند»، «گواهی‌های حامل دیجیتال» و ســازوکارهای پولی جدیدی به وجود آمدند که نه‌تنها از حریــم خصوصی افراد محافظت می‌کردند؛ بلکه برابری بین اشخاص و ســازمان‌ها را نیز حفظ می‌کردند و اساس پروژه‌های بیشتری را بنا می‌گذاشــتند؛ چام و e-cash به سرمشــق و عبرتی برای دیگران تبدیل شدند و ابتکاری واقعی در تحقیق و توســعه در خدمت پیش‌بینی و پیشگیری آینده‌ای ناخوشایند قرار گرفت. هال فینی در ســال ۱۹۹۲ بیان کرد که رمزنگاری و e-cash برای او چه ارزشی دارد. فینی می‌نویسد: «راهی که چام باز کرد، قدرت را بین افراد و سازمان‌ها متعادل می‌کند... اگر همه چیز خوب پیش برود، ممکن است بتوانیم به گذشته نگاه کنیم و ببینیم این مهم‌ترین کاری بوده که انجام داده‌ایم.»

e-cash داســتانی آموزنده هم بود. چام با نگاه‌کردن به گذشــته می‌گوید: «من از جهان می‌خواســتم شــیوه کاری خود را تغییر دهد تا حریم خصوصی کاملا رعایت شــود.» برای پذیرفته‌شــدن این ابزار باید از ســد مشــکلات زیادی عبور می‌کردیم. «آروین نارایانان»[1]، متخصص کامپیوتر، برای توصیف ایده‌های بلندپروازانه‌ای مانند ایده چام از عبارت «پذیرش

1. Arvind Narayanan

اجتماعی»[1] اســـتفاده می‌کند: «حجم عظیمی از کاربران بالقوه که از وضعیت کنونی راضی نیستند» و سیستم جدید باید کاملا و فورا جایگزین آن شود. افراد و گروه‌های کوچک می‌توانند سیستم‌هایی مانند رمزنگاری ایمیل را قبول کنند، اما سیستم چام تغییری عمده را می‌طلبید. به عبارت دیگر، فناوری به‌تنهایی کافی نیست. حتی با ریاضیات پیشرفته، اکتشافات علمی، گردش آزاد ایده‌ها، سخت‌افزار قابل اطمینان و کدهای در حال اجرا باز هم باید اشتیاق، رویا، نارضایتی، داستان یا خیالی در سر داشته باشید. درخشش آرمان‌شهری در افق و کاز موگرامی برای رسیدن به آن.

چه می‌شـــد اگر برای رد شـــدن از این چالش می‌توانســـتید ابتدا جامعه و پس از آن پلتفرم مناســـب را ایجاد کنید؟ چه می‌شـــد اگر می‌توانستید دنیایی بســـازید که فناوری در آن امری اجتناب‌ناپذیر باشد؟

1. Societal buy-in

فصل پنجم

سقوط دولت‌ها

در دهه‌های ۱۹۸۰ و ۱۹۹۰ در حالی که کریپتوآنارشیست‌ها[1]، سیستم تبادل اطلاعات آمریکا[2] و پروژه زانادو[3] سعی داشتند داده دیجیتال را ارزشمند کرده و بازارهای آتی را پی‌ریزی کنند، سایفرپانک‌ها پول جدیدی را به وجود آوردند. ایجاد پول دیجیتالی که کاملا ناشناس باشد، سه مساله اساسی را حل می‌کرد؛ هماهنگی، تکثیر و پذیرش. این فصل به توضیح دو مساله اول می‌پردازد و نشان می‌دهد آینده احتمالی با پول دیجیتال به چه شکل در می‌آمد.

سیاه‌چاله

روز جمعه ۲۵ سپتامبر ۱۹۹۲ در کلوپ «سیاه‌چاله» در سان‌فرانسیسکو، «سنت جود»[4] با سفیران آینده ملاقات کرد.

او می‌دانست آنها از جهانی در آینده می‌آیند و بخشی از «انقلابی هستند که همان موقع نیز جریان داشت»؛ زیرا ناشناس و مبهم بودند، چادر پوشیده بودند و عینک‌های سه‌چشمی زده بودند. وقتی حرف می‌زدند، صدایشان از فیلتری عبور می‌کرد و به ترکیب صدای آزاردهنده‌ای از ساکسیفون و ویولن‌سل تبدیل می‌شد که آن را غیرقابل تشخیص می‌کرد و از بلندگوهایی که روی سرشان تعبیه شده بود، خارج می‌شد. دیگران از طریق بلندگوهایی حرف می‌زدند که صدایی مشابه ترمین[5] یا آب خروشان داشت. عینک سه‌چشمی لنزی بود که به وسیله آن با شبکه‌ای از مردم ارتباط برقرار می‌کردند. وقتی او لطیفه‌ای برایشان تعریف کرد، چادرها از مناطق جغرافیایی مختلف «ارکستری از خنده» سر دادند. با خودش فکر کرد: «یعنی در سطح جهانی معروف شده‌ام؟»

سفیران خیلی از او بلندتر بودند، قد هر دویشان یکی بود و کفش کوتورنی[6] به پا داشتند؛ کفشی سنگین با کفی ضخیم و پاشنه مخفی. مانند غواصانی که به کف آب می‌روند، در کفش‌های سربی خود به اطراف حرکت می‌کردند و با هر حرکت و اشاره‌ای لباس‌شان مانع حرکت آنها می‌شد. وقتی از میان دود در کلوپ سیاه‌چاله ظاهر شدند (کلوپی که حتی یک

1. Crypto anarchists
2. American Information Exchange
3. Xanadu
4. St Jude
5. Theremin
6. Cothurni

فوتون اطلاعات هم نمی‌توانســت از آن فرار کند) او گفت: «فکر کنم شما کریپتوآنارشیست باشید. البته من سایفرپانک را ترجیح می‌دهم!... هدف شما این است که جهان را تسخیر کنید.» صدای آزرده‌خاطری شبیه به ویولن‌سل با لهجه هلندی با او مخالفت کرد: «ما به تسخیر کردن اعتقادی نداریم. در واقع ما سعی داریم همه‌چیز را غیر قابل تسخیر کنیم.»

دو چادری و صداهای متعددی که همزمان از آنها خارج می‌شــد (و کسی نمی‌دانست در حقیقت متعلق به چه کسانی بود) برنامه را توضیح داد: اقتصاد وابسته به نام مستعار که همه چیز در آن رمزگذاری شده است، شهرت آنلاین و سیستم همگانی رتبه‌بندی اعتبار و پول دیجیتال ایمن «حساب بانکی ســوئیس برای میلیون‌ها نفر». و با صدای رباتیک خود ادامه داد: «برای ایجاد یک سیستم پولی جهانی که دولت‌ها را منسوخ می‌کند.»

«سنت جود» نوشت: «نه، خیالاتی نشده‌ام.» او واقعا با سایفرپانک‌ها ملاقات کرده بود، در واقع خودش این نام را به آنها داده بود. این اتفاق، شنبه قبل در روز روشن و در سواحل کالیفرنیا، شهر برکلی و منزلی شخصی به وقوع پیوســته بود؛ نه در دود و تاریکی کلوپ سیاه‌چاله. اما او حقیقت امر را به کمک اشباح تخیلی چندصدایی منتقل کرد؛ شبکه‌ای از تیرگی که دستکش میخ‌دار پوشیده بودند، باتوم برقی به همراه داشتند و نقشه رمزگذاری همه چیز را کشیده بودند. او در خط آخر مطلبش گفت: «اینها شــایعه‌ای بیش نبود. می‌توانیــد از طریق آدرس ایمیل cypherpunks@toad.com با انقلابی‌ها ارتباط برقرار کنید.» (این آدرس شما را عضو یک فهرست ایمیل واقعی می‌کند که همان هفته آغاز به کار کرد و اولین پیش‌نویس‌های داستانش را از طریق آن منتشر می‌کرد).

دهه‌ها قبل، «جود میلهان» ملقب به «سنت جود» از بنیان‌گذاران یکی از اولین شبکه‌های اجتماعی دیجیتال به نام Community Memory بود که بــا کیبوردهای تله‌تایپ[1] موجود در سی‌دی‌فروشــی‌ها و کتابخانه‌های عمومی از آن اســتفاده می‌کردند. این برنامه پیشرفت شخصیت‌هایی مانند دکتر بنوی[2] را شاهد بود که از نام مستعار استفاده می‌کردند. این سیستم بدون امنیت نیازی به حساب کاربری نداشت و هر کسی می‌توانســت از طرف دکتر بنوی یا شخص دیگری مطلب بنویسد. جود می‌گوید: «عده‌ای از نقض‌کنندگان قانون کپی‌رایت اعلام

1. Teletype keyboards
2. Dr. Benway

کردند که قصد دارند لوگوی دکتر بنوی را تکثیر کنند. از نظر من اشـــکالی ندارد... به هر حال آن هم جزء اموال عمومی است.» چه اهمیتی دارد که چه کسی پشت آن بلندگوها و با آن اسم صحبت می‌کند؟ یکی از دوســـتان میلهان پس از فوت او در سال ۲۰۰۳ می‌نویسد: «یکی از فلسفه‌های زندگی «جود» این بود که نیازی نیست هویت خود را برای کل جهان آشکار کنید.»

ســـنت جود از یکی از چادری‌های داســـتان سیاه‌چاله می‌پرســـد: «پس در واقع از هویت فیزیکی خودتان محافظت می‌کنید، نه؟» و در عین حال این سوال را از مخاطبان واقعی خود نیز می‌پرسد؛ کسانی که اخیرا به جرگه سایفرپانک‌ها پیوسته‌اند. «از هرگونه توضیح، پیشنهاد، تصحیح یا حتی سوءاستفاده و تهدید استقبال می‌شود.» او داستان «جنبش سایفرپانک‌ها»[1] را در ستون «روزنامه‌نگار بی‌مسئولیت» برای مجله سایبری «موندو ۲۰۰۰» می‌نوشت (این مجله حکم خواهر بزرگ و یاغی مجله وایرد را داشت که علاوه بر مطالبی در رابطه با واقعیت مجازی، مواد روان‌گردان، رمزنگاری و داستان‌های تجربی، مواردی از قبیل شایعات، مصاحبه با باندهای موسیقی و عکاسی مد را نیز شامل می‌شد). او پیش‌نویس داستانش را به افرادی که الهام‌بخش او بوده‌اند، اولین اعضای فهرست ایمیل cyberphunk@toad.com و گروهی که هفته قبل به شکل حضوری در خانه «اریک هیوز» گرد آمده بودند، تقدیم کرد. میلهان در آن جلسه حضور داشت و از ایده‌های مختلف یادداشـــت‌برداری می‌کرد و اکنون فقط نگران این بود که یادداشت‌هایش «صحیح و واضح» باشند و حس آینده‌ای را که بر پایه رمزنگاری، ناشناس‌بودن و «پول دیجیتال ایمن» مبتنی بود، به‌درستی منتقل کند. سایه مبهم از میان هاله‌ای از نور با صدای زنگ‌دارش گفت: «مرگ بر دولت‌ها.»

سقوط دولت‌ها

«تیموتی می» نیز در کنار سنت جود در دورهمی روز شنبه در برکلی حضور داشت؛ همان جایی که گروهی از مهندســـان، برنامه‌نویســـان و علاقه‌مندان به رمزنگاری به ســـایفرپانک تبدیل شدند.

او مهندسی بود که پس از محاســـبه دقیق پول مورد نیاز برای حفظ استقلالش تا آخر عمر، خودش را در ۳۴ سالگی بازنشسته کرده بود. او در شرکت اینتل مساله حساسی را حل کرده بود

1. The Cypherpunk Movement

که به خطای میکروچیپ‌ها ناشی از نشر ذرات آلفا از پوشش سرامیکی مربوط می‌شد. او مانند یک فیزیک‌دان، جهان را به شکل یک واقعیت می‌دید (رادیواکتیویته، رادیواکتیویته است، چه انسان‌ها از وجود آن در کپه‌ای شن یا تکه‌ای سنگ کوارتز اطلاع داشته باشند، چه نداشته باشند) و به لایه‌لایه‌بودن انسان و ماشین به شکلی طعنه‌آمیز و با دیده تحقیر نگاه می‌کرد. در مقاله‌ای که در مورد ذرات آلفا نوشته بود، پس از چندین صفحه شواهد و استدلال‌های دقیق در مورد طراحی چیپ‌ها و فروپاشی هسته‌ای، جمله آخری که نوشت این بود: «از نقطه‌نظر مهندسی انسانی تا حدودی خوشایند است که توجه داشته باشیم ربات‌های قرن بیست‌ویکم که میکروکامپیوترها کنترل‌شان می‌کنند نیز ممکن است دچار مشکلاتی مشابه انسان شوند؛ ربات‌ها نیز ممکن است مثل انسان دچار اشتباه شوند.»

«می» نیز مانند بسیاری از افرادی که آن روزها آنلاین وقت می‌گذراندند، کادر امضای خود را داشت؛ فایلی با فرمت sig. که متنی را شامل می‌شد که به‌صورت خودکار به ایمیل‌ها و پست‌های ارسالی‌اش در تالارهای گفت‌وگو الحاق می‌شد. کادر امضا جایی بود که برای نوشتن شماره تلفن و سایر اطلاعات استفاده می‌شد (جولیان آسانژ، یکی دیگر از اعضای فهرست ایمیلی سایفرپانک‌ها، نقل‌قولی کنایه‌آمیز از نیکسون را در کادر امضای خود نوشته بود).

امضای می، متن یکی از ترانه‌های Talking Heads بود؛ جناسی ریاضیاتی در مورد ۱۰ عدد اول بزرگ کشف‌شده و خط زمانی آینده، داستان علمی ـ تخیلی مینیاتوری که کریپتوآنارشیسم، رمزنگاری، پول دیجیتال، شبکه‌های افراد ناشناس، نام‌های مستعار دیجیتال، دانش صفر، شهرت اینترنتی، بازارهای اطلاعاتی، بازارهای سیاه و سقوط دولت‌ها را شامل می‌شد. فهرستی از مولفه‌های مورد علاقه او به همراه شرحی از آینده فرضی که به‌ترتیب ظاهر می‌شدند و می‌توان آن را در قالب داستان آغاز عصر کریپتوآنارشیست‌ها نوشت. مجموعه‌ای از پیشرفت‌های بنیادین در رمزنگاری و دهه‌ها طراحی و پژوهش که دولت هزینه آن را تامین کرده است، موجب نابودی خودش می‌شود. آزمایش‌هایی که در زمینه شبکه‌های افراد ناشناس، نام‌های مستعار دیجیتال، دانش صفر و شهرت اینترنتی صورت گرفته است، زیرساخت را برای پول دیجیتال مهیا می‌کند. تنها به بازاری اطلاعاتی نیاز است که عملکرد این اجزا را نشان دهد و کاربران جدیدی را جذب کرده و آموزش دهد. این امر امکان ایجاد شبکه‌های جهانی بازار

سیاه برای معامله غیر قابل ردیابی و بدون پرداخت مالیات را فراهم می‌کند که لزوما پس از آن دولت‌ها سقوط خواهند کرد.

وظیفه او این بود که این داستان را به واقعیت بدل کند، اما نمی‌توانست این کار را به‌تنهایی انجام دهد؛ بلکه به شریک، جنبش و توطئه ریاضیاتی اولیه‌ای نیاز داشت. او برای گروهی که آن روز شنبه در ماه سپتامبر گرد هم آمده بودند (و جود میلهان هم در میان‌شان بود) چنین خواند: «روح سرگردانی جهان مدرن را به وحشت انداخته است، روح کریپتوآنارشیسم.» او سخنانش را این‌گونه آغاز کرد: «مانیفست کریپتوآنارشیسم.»

جامعه سایفرپانک‌ها از همان ملاقات اول آینده‌های مختلفی را در ذهن داشت که با یکدیگر هم‌پوشانی داشتند. آنها فرضیه‌هایی منطقی داشتند، مثلا «به محض اینکه پول وارد شبکه‌هایی شود که تنها به نام‌های مستعار متصل است (و نه به افراد واقعی) هویت‌های صرفا مجازی بسیاری به وجود خواهد آمد.» آنها همچنین در مورد «واقعیت مجازی سه‌بعدی»[1] به‌عنوان «محل سکونت دائمی» فرضیاتی داشتند. آنها در تکنیک‌ها و فناوری‌های مورد استفاده خود به‌دنبال نشانه‌هایی از آینده بودند تا یک روز به‌صورت گسترده در شبکه‌ها مورد استفاده قرار بگیرند. «موضوع بحث ما به‌کارگیری بلندمدت این ایده‌هاست.»

ظریف‌ترین و مهم‌ترین اشکال تاریخی پروژه سایفرپانک زمان‌بندی نامناسب آن بود. این زمان‌بندی به دو علت نامناسب بود؛ اول اینکه پروژه جلوتر از فرارسیدن بافت تاریخی‌اش ایجاد شده بود و دوم اینکه پیشرفت بسیار کندی داشت. بین اثبات موارد بنیادی رمزنگاری (الگوریتم‌های سطح پایین مطمئن) و به‌کاربستن آنها در قالب یک شبکه کارآمد فاصله زیادی وجود داشت. «می» می‌پرسد: «چرا بیشتر چیزهایی که سایفرپانک‌ها در موردشان حرف می‌زنند، به وقوع نپیوسته است؟» حتی مانیفستی که او آن روز شنبه در اولین ملاقات‌شان خواند، به چهار سال قبل تعلق داشت و در سال‌های ۱۹۸۸، ۱۹۸۹ و ۱۹۹۰ بین «تکنوآنارشیست‌های[2] همفکر» دست‌به‌دست می‌شد. «به دلایل تاریخی آن را همان‌طور که هست، کنار می‌گذارم. ما اکنون در شرف این هستیم که توانایی ارتباط و تعامل را به شکلی کاملا ناشناس در اختیار افراد و گروه‌ها قرار دهیم.» چرا این کار به این اندازه زمان‌بر بود؟

---

1. Spatial VR
2. Techno-anarchists

پیشـــرفت در حوزه‌هایی مانند ایمیل، بـــا مجموعه پروتکل‌های رایج و پذیرفته‌شـــده، کار دشـــواری نبود، اما برای مواردی مانند پول دیجیتال که مســـتقل نبـــوده و اغلب پروتکل‌های چندجانبه، تاخیر، پردازش آفلاین و غیره را شـــامل می‌شـــدند، اوضاع بدتر بود. ساخت پول دیجیتال هم از نظر فنی پیچیده و هم از نظر معناشناسی گیج‌کننده بود. «می» می‌نویسد: «معنی رمزنگاری یا توزیع‌کننده ایمیل کاملا مشخص است؛ اما بانک دیجیتال به چه معنی است؟» بررسی آسیب‌پذیری ایمیل یا نقاط قوت و ضعف سیستم‌های رمزنگاری گوناگون تفاوت زیادی با پول دارد که به شکل غیرمستقیم مجموعه‌ای از ارزش، زمان، تاریخ و ساختار اجتماعی را دربر می‌گیرد. منظور شما از «بانک دیجیتال» بخشی از یک کاز موگرام است (راهی برای دانستن، سازمان‌دهی و توضیح‌دادن جهان). تعریف آن نیازمند ایجاد توافقی است که پیش از توافق بر سر زبان برنامه‌نویسی، پایگاه داده، فرمت، ابزار همکاری و سیستم نسخه‌بندی مطرح می‌شود که برای شروع کار به آنها نیاز دارید.

برای ساخت یک بانک دیجیتال هماهنگی عمیقی نیاز اســـت که (همان‌طور که «یوچای بنکلر»[1] در مورد ساخت نرم‌افزارهای رایگان و متن‌باز می‌گوید) معمولا از طریق سیستم‌های قیمت‌گذاری یا ساختارهای مدیریتی انجام می‌شـــود. می‌توانید بازاری داشته باشید که برای فعالیت‌های خاصی جایزه یا مشوق تعیین کند یا شرکت‌ها و نهادهایی داشته باشید که حقوق پرداخت می‌کنند، تیم‌هایی تشـــکیل می‌دهند و دســـتورالعمل‌هایی را تعیین می‌کنند؛ دو راه مختلف اما سازگار با یکدیگر که مردم را کم‌وبیش در یک جهت به حرکت وامی‌دارند. ایجاد یک پلتفرم بانکداری دیجیتال معمولا تحـــت امر و یزا یا بانک مرکزی یـــا نهاد بزرگ دیگری صورت می‌گیرد که حکم قانونی، فضای دفتری و ردیفی از مدیران و هیات اجرایی را برای حل ناسازگاری‌های داخلی در اختیار دارد. در مقابل آن، ســـایفرپانک‌ها تنها گروهی دورقمی از افراد بسیار باهوش و یک فهرست ایمیل در اختیار داشتند. «ما، افراد این فهرست، برای ساخت هیچ چیز پولی دریافت نمی‌کنیم، از کسی کمک نمی‌گیریم و پشتیبانی مالی موسسات را در اختیار نداریم.»

داستان نرم‌افزار رایگان و متن‌باز، داســـتان جوامع فناورانه جدیدی است که از سد تمام این نابرابری‌ها عبور می‌کنند تا از سیســـتم‌عامل گرفته تا پلتفرم‌های ســـروری را بسازند که اساسا

1. Yochai Benkler

اینترنت روی آن استوار است. در حالی که همه این پروژه‌ها اختلاف‌نظرهای زیادی را تحمل کرده‌اند، پیچیدگی گفت‌وگوهای مورد نیاز برای ایجاد چیزی مشابه بانک دیجیتال از نوع دیگری بود. این گفت‌وگوها از سوالات فنی سرگرم‌کننده شروع نمی‌شـــدند؛ بلکه از تعهد فلسفی و اجتماعی نسبت به مقامات، نظام و ماهیت ارزش شروع می‌شدند.

وضعیت برای مدتی طولانی به همان شکل باقی ماند؛ گفت‌وگوهایی که کند پیش می‌رفتند و امید رسیدن به توافق در آنها دیده نمی‌شد. شاید می‌شد حجم قابل توجهی از حمایت‌کنندگان، کاربران و شرکت‌کنندگان را دور هم جمع کرد تا بتوان یکی از این طرح‌ها را پیش برد. اگر امکان رسیدن به سطحی که هیوز در نظر داشت، ممکن بود و «پول در شبکه‌ای جریان پیدا می‌کرد که فقط به نام‌های مستعار متصل بود و نه به اشخاص واقعی»، بنابراین سیستم تنها به خودش متکی می‌شد و کاربران آن جمعیتی بودند که تشویق شده بودند تا از نوع جدیدی از نظام قیمتی استفاده کنند و از آن حمایت کرده و آن را بســـازند؛ به این ترتیب جزئی از جریان موجود می‌شدند. با تعداد افراد کافی می‌توان در عمل و به صورت مجازی نیروی مورد نیاز را برای ایجاد فناوری‌های جدید و تعریف یک داستان فراهم کرد.

فصلی از داستانی که «می» می‌خواست تعریف کند (داستان پیروزی پول دیجیتال و سقوط دولت‌ها) به پدید آمدن «بازارهای اطلاعاتی» اختصاص داشـــت که پلتفرمی برای داده‌های ارزشـــمند و بافتی اقتصادی برای پول دیجیتال ایجاد می‌کرد. بـــازار اطلاعاتی آنلاین چطور می‌تواند کار خود را آغاز کند؟ دو شرکت نزدیک به هم در حوزه فعالیت «می» سعی کردند به این سوال پاسخ دهند و سیستم‌ها، تعهدات و شرکایشان چیزی را به وجود بیاورند که قرار بود پول دیجیتال را شکل دهد. یکی از آنها، شرکت تبادل اطلاعات آمریکا بود که «فیلیپ سالین» آن را بنیان گذاشته بود. چنانچه اولین گفت‌وگوی «می» با گروهی از افراد همفکر در مورد پروژه کریپتوآنارشیسم در سال ۱۹۸۸ در اتاق نشیمن خانه سالین رخ داد.

شرکت موشکی آمریکایی[1]

فیلیپ سالین در انتهای جاده‌ای زندگی می‌کرد که یکصد مایل طولش بود و از همان‌جایی

1. American Rocket Company

که او ایستاده بود، مستقیم به خارج از جو زمین متصل می‌شد. او از «پالو آلتو»[1] تا مدار نزدیک زمین مسیری را طراحی کرده بود. تیم او در «آرک تکنولوژیز»[2] (که بعدها نام آن به «استارز ترک» و در نهایت به شـــرکت موشـــکی آمریکا با مدیریت جدید تغییر کرد) روی ساخت سوخت موشک «راکت کندی»[3] بر پایه مواد قندی کار می‌کردند تا ســـوخت ارزان‌تری را برای وسیله پرتاب موشک بســـازند. آنها بودجه خود را از «مایکل اسکات»، اولین مدیرعامل شرکت اپل دریافت می‌کردند. سالین مهندس هوافضا نبود؛ بلکه متخصص علم اقتصاد با مدرک ام‌بی‌ای بود که مکتب اتریشـــی بازار محور «فریدریش هایک»[4] را دنبال می‌کرد. او باور داشت قدرت عملیات‌های بازار به‌تنهایی برای ایجاد تغییر کافی است. از نظر سالین بزرگ‌ترین چالشی که فضا می‌توانست در آینده با آن مواجه شود، نیرویی قدرتمندتر از جاذبه یا تحمل‌پذیری فلزات بود و آن چیزی نبود به‌جز استفاده نامناسب از پول.

او در کمیسیون مجلس اعلام کرد که شاتل‌ها بســـیار ارزان هستند، هزینه‌هایشان مشمول یارانه شـــده و به‌طور مصنوعی کاهش پیدا می‌کند؛ این موضوع مانـــع کارآفرینی در صنعت موشکی می‌شود. جابه‌جایی پول به‌تنهایی می‌تواند ما را از سلطه این نیرو خارج کند. او اظهار کرد: «پیشـــرفت بزرگ بعدی که در فضا حاصل می‌شود، پیشـــرفتی اقتصادی خواهد بود.» سالین مجذوب بازارهای اطلاعاتی بود که پول و اطلاعات در آنها در گردش بود (پول مساوی اطلاعات بود و اطلاعات مساوی پول).

ســـالین در ســـال ۱۹۸۴ وقتی پروژه فضایی‌اش با مشکلاتی مواجه شـــد، پروژه جدیدی را راه‌اندازی کـــرد که از دهه ۱۹۷۰؛ وقتی آثـــار هایک و کارل پوپـــر را مطالعه می‌کرد و روی سیســـتم‌های کامپیوتری اشـــتراک زمان کار می‌کرد، به فکر آن بود. این پروژه، ایجاد بازاری دیجیتال برای مالکیت معنوی بود. او نام آن را سیســـتم تبادل اطلاعات آمریکایی (AMIX) گذاشـــت و آن را مکانی برای فروش انواع اطلاعات می‌دید. این سیستم علاوه بر اطلاعات، راه‌حلی برای همه چیز محسوب می‌شد؛ از نظرسنجی، تحلیل بازار و حق امتیاز تا پروژه‌های اتوکد، حل مســـائل و انواع فرمول‌ها. ســـالین می‌گفت: «ما ســـعی داریم هزینه‌های اضافی

1. Palo Alto
2. Arc Technologies
3. Rocket Candy
4. Friedrich Hayek

معاملات را کاهش دهیم؛ هزینه‌هایی که مردم را از معامله اطلاعات‌شان باز می‌داشت.»

به این منظور، آنها باید سیستم مزایده و فروشی می‌ساختند که حساب کاربری، قابلیت امتیازدهی، بخش نظرات و مدیران بازاری داشته باشد تا شغل جدید «واسطه اطلاعاتی» را به گردن بگیرند. آنها برای رسیدگی به امور حسابداری، تنظیم صورت‌حساب‌ها و معاملات و پرداخت‌ها به یک پلتفرم نیاز داشتند. همچنین لازم بود کامپیوترهای شخصی در سراسر ایالات متحده از نرم‌افزار مخصوص AMIX استفاده کنند (که رسانه‌ها استفاده از آن را «طاقت‌فرسا» نامیدند) تا هر مشتری بتواند به سرورهای یونیکس[1] متصل شود که مجموعه‌ای از موضوعات اصلی و فرعی و اقلام مربوط به دنیای تخصصی محصولات و خدمات اطلاعاتی را در بر می‌گرفتند. همان‌طور که «داک سیرلز»[2]، روزنامه‌نگار حوزه فناوری می‌نویسد: «تیم AMIX سعی داشت سرویس آنلاینی را از صفر ایجاد کند»؛ نسخه‌ای قراردادی از زیرساختی که اینترنت در آینده ارائه خواهد کرد. «فیلیپ می‌خواست اینترنت خودش را داشته باشد.» حتی پیش از حل این مسائل، AMIX باید توضیح می‌داد که چرا اطلاعات دیجیتال ارزشمند است.

«استر دایسون» در سال ۱۹۹۰ ایراد آن را به این شکل عنوان کرد: «قانون عرضه‌وتقاضا برای محصولی مانند اطلاعات جواب نمی‌دهد؛ چراکه بدون هیچ هزینه‌ای می‌توان اطلاعات را تکثیر کرد.» در آن زمان دایسون روزنامه‌نگاری در حوزه پیشرفت‌های کامپیوتری بود که از توسعه بازارهای اطلاعاتی دیجیتال حمایت می‌کرد. این بازارهای آزاد سایبری با مشکلی مواجه بودند که از طرح کسب‌وکار سالین سرچشمه می‌گرفت. دایسون به‌کرات در مورد AMIX مطالبی نوشت و سعی می‌کرد مشکل تکرارشونده‌ای را که در مورد ارزش رسانه‌های دیجیتال وجود داشت، حل کند: «پس از تولید، بدون هیچ هزینه‌ای می‌توان آنها را تکثیر کرد.»

در سال ۱۹۷۲ «استوارت برند»، نویسنده پیرو مکتب مشاء و طرفدار هنر با خرده‌فرهنگ خوره‌های کامپیوتر آشنا شد که وقت خود را صرف برنامه‌نویسی و بازی ویدئویی Spacewar! می‌کردند. او ایده دیجیتالی کردن رسانه‌های آنالوگ را به‌وضوح مطرح کرد: «داده‌های زیادی را می‌توان با استفاده از کامپیوتر به شکل دیجیتال درآورد و انتقال داد؛ مثلا علاقه‌مندان به موسیقی می‌توانند در این شبکه، موسیقی‌های خود را با جزئیات دقیق با یکدیگر مبادله کنند که

1. Unix
2. Doc Searls

البته برای فروشندگان موسیقی خبر خوبی نیست.» جمله‌بندی او یک ایراد مهم دارد؛ ایرادی معناشناسانه که امروزه زیاد شاهدش هستیم. علاقه‌مندان به موسیقی، فایل‌هایشان را با یکدیگر «مبادله» نمی‌کنند و آنها را به هم قرض نمی‌دهند؛ بلکه تکثیر می‌کنند؛ زیرا هر نسخه از آن (در کامپیوتر من و شما، ذخیره‌شده روی سرور، در حافظه پنهان و در دستگاه پخش موسیقی) یک کپی دقیق از فایل اصلی است؛ مگر اینکه خودمان روی آن فیلتری اعمال کنیم، فشرده‌اش کنیم یا تغییرش دهیم.

بیشتر تاریخچه کامپیوتر و ارتباطات در قرن بیستم مربوط به چالش‌های صحت، دقت و اصلاح خطاست که هدف آن ذخیره‌سازی و انتقال کپی‌های بی‌عیب‌ونقص اطلاعات از طریق رسانه‌های معیوب و کانال‌های شلوغ بود؛ از خطوط تلفن گرفته تا امواج رادیویی و سیم‌کشی بین واحدهای حافظه، پردازش و نمایشگر یک کامپیوتر. می‌توان گفت کار کامپیوترها، به‌خصوص کامپیوترهای تحت‌شبکه، این بود که دوره جدیدی از دستگاه‌های تکثیر را ایجاد کنند که ظرفیت تکثیر آنها بسیار فراتر از صنعت چاپ و عکاسی بود. صفحه رو به‌رویی مطلبی که دایسون در مورد AMIX در مجله فوربس نوشته بود، تبلیغی تمام‌صفحه از یک دستگاه زیراکس بود که برنده‌شدن «جایزه کیفیت ملی» را اعلام می‌کرد. مانند برنامه‌های کامپیوتری اولیه‌ای که «کنراد زوسه»[1] ساخته بود و از دستورالعمل‌های دیجیتالی استفاده می‌کرد که روی یک فیلم قدیمی ۳۵ میلی‌متری پانچ شده بود؛ او در واقع دو رسانه مختلف را به شکل آراسته‌ای کنار هم قرار داده بود.

این قدم دیگری در بحران چندقرنی موضوع «مالکیت معنوی» بود؛ دیجیتالی‌شدن، برای سوالات قدیمی در رابطه با چرایی و چگونگی ارزشمند بودن اطلاعات، پاسخ‌های جدیدی ارائه کرد. پاسخ سالین در چارچوب AMIX نوعی سادگی فریبنده بازاری داشت؛ اطلاعات دیجیتال به این دلیل ارزشمند است که مردم حاضرند برای آن پول بدهند. کسی دلیل آن را نمی‌داند. دایسون در یکی از مقالاتش در رابطه با AMIX می‌نویسد: «چیزی که برای «خوان» عادی محسوب می‌شد، برای «آلیس» کشفی هیجان‌انگیز بود. بگذارید بازار خودش تصمیم بگیرد.» اما این پاسخ، سوال ژرف‌تری را مطرح می‌کرد. AMIX در واقع بازار و پلتفرمی برای معامله و فروش اطلاعات دیجیتال بود. «اطلاعات دیجیتال» خود پول پرداختی را نیز شامل می‌شد. چه چیزی باعث می‌شد پول دیجیتال این بازار دیجیتال ارزشمند باشد؟

1. Konrad Zuse

همان سازوکاری که انتقال و ذخیره اطلاعات را در قالب مجموعه‌ای از بیت‌ها ممکن کرده و آنها را از حسابی به حساب دیگر منتقل می‌کرد، کار را برای پول دیجیتال دشوار می‌کرد. تیموتی می، اشاره کرد که می‌توان از تکنیک پنهان‌نگاری[1] (مخفی کردن داده در داده‌ای دیگر) برای پنهان کردن پول دیجیتال در فایلی صوتی یا عکسی با وضوح بالا استفاده کرد. می‌توان یک ماشین حمل پول کامل را در یک عکس دیجیتال ساده پنهان کرد، اما این پول نیز مانند خود عکس ایرادی اساسی داشت و قابل تکثیر بود. دایسون برای حمایت از AMIX دو دلیل می‌آورد؛ اول اینکه عموما تکثیر اطلاعات دیجیتال رایگان بوده، اما پیدا کردن آن دشوار است و دوم اینکه داده‌های ارزشمند به‌صورت گسترده در دسترس همگان قرار نمی‌گیرند. این موضوع برای رسانه دیجیتالی که آن را پول می‌نامیم، چگونه عمل خواهد کرد؟

سالین به‌قدری زنده نماند که نتیجه این پروژه‌ها را ببیند و در دسامبر ۱۹۹۱ در ۴۱ سالگی بر اثر سرطان کبد درگذشت؛ درست چند ماه پس از اینکه شرکت طراحی کامپیوتری اتودسک، پروژه AMIX را خریداری کرد. او پنجاه‌ونهمین فردی بود که فرایند انجماد پس از مرگ را طی کرد؛ با جراحی عصبی سرش را جدا کرده و منجمد کردند تا توسط جامعه‌ای که پیش‌بینی کرده بود، به زندگی بازگردانده شود یا به‌صورت دیجیتالی بازسازی شده و بدنش را کلون کنند یا به‌صورت مصنوعی جایگزین کنند. او در مورد یکی از مشکلات این کار با «می» صحبت کرد: شخص چگونه می‌تواند دارایی‌هایش را هم مثل خودش ابدی کرده و به آینده انتقال دهد؟ اگر قیمت‌گذاری دقیق روی شاتل فضایی و انتقال وجه بین افراد در سیستم AMIX کار چالش‌برانگیزی بود، فرض کنید که انتقال پول به آینده‌ای ناشناخته و غیرقابل تشخیص چقدر می‌تواند دشوار باشد؛ به‌خصوص وقتی در تابوتی در آریزونا منجمد شده باشید و شما را در قالبی پساانسانی به زندگی بازگردانده باشند.

یادداشت‌های «می» در سال ۱۹۹۳ در رابطه با «پروتکل‌های رمزنگاری زمان‌دار» (روش‌های فرضی برای رمزنگاری پیام به گونه‌ای که فقط پس از گذشت زمانی مشخص یا پس از وقوع رویدادی خاص بتوان آن را خواند) از موردی استفاده کرد که سال‌ها پیش در گفت‌وگویش با سالین مطرح شده بود: «در درجه نخست، ارسال پول به آینده و در عین حال حفاظت از آن در مقابل سرقت، مالیات و غیره برای طرفداران انجماد مطرح می‌شود؛ کسانی

1. Steganographic

که می‌خواهند ترتیبی بدهند که در آینده دوباره به زندگی برگردند.» (جولیان آسانژ نیز یک دهه بعد همین مساله را در جمع سایفرپانک‌ها مطرح می‌کند، البته برای ایمن‌سازی انتشار رمزها). باید حساب بانکی مخصوصی وجود داشته باشد که گذر زمان روی آن اثر نگذارد و برای کسانی که اشخاص را به زندگی برمی‌گردانند، جایزه تعیین کند؛ مثلا اولین گروهی که صاحب حساب را به زندگی برگرداند، پس از رمزگشایی داده‌ها جایزه تعیین‌شده را دریافت می‌کند. معامله‌گران داده در آینده‌ای که سالین می‌خواست ایجاد کند، بیشترین بهره را از این موضوع می‌برند؛ نظام قیمتی که می‌تواند سازنده‌اش را دوباره به زندگی برگرداند.

سفر در زمان و ورود به دنیای خوره‌های فناوری

مسیر حرکت نامتعارف سالین باعث شـــد او و «گیل پرگامیت»[1] (همکار، هم‌بنیان‌گذار و همســـرش که مدافع فناوری نانو نیز بود) به مرزهای فرضی صنایعی نزدیک شوند که ممکن بود آینده خوبی داشته باشند؛ از کامپیوتر اشتراک زمان و تحلیل‌های اقتصادی برای فروپاشی انحصار تلفن تا برنامه فضایی خصوصی و بـــازاری برای اطلاعات دیجیتال؛ اما عجیب‌ترین عنوان شغلی که برای او ثبت شد در «شرکت عملیاتی زانادو» (XOR) بود؛ «شتاب‌دهنده» (عنوان شغلی پرگامیت در این پروژه «متغیر پنهان» بود). زانادو پروژه‌ای شبیه به AMIX بود؛ ابتکاری برای دیجیتالی‌کردن تمام دانش بشـــری و وارد کردن پول در بنیادی‌ترین سطوح آن. برای تیم زانادو (و سالین) پول بهترین سوخت و نیز انگیزه‌ای برای آینده بود. «تئودور نلسون» (از کارکنان XOR که عنوان شغلی‌اش «کارگردان» بود) خودش و «گروه اجرایی نهایی» که برای انجام پروژه در پنسیلوانیا گرد هم آمده بودند را این‌گونه توصیف می‌کند: «همگی حامی کاپیتالیســـم بودیم...؛ من به‌دلیل نفرت از کمیته‌ها، نبود خلاقیت و رقـــت افکار و دیگران به خاطر اینکه دوست داشتند شاتل فضایی خودشان را داشته باشند.» اطلاعات دیجیتال و پول دیجیتال در صورتی که به‌درستی به کار گرفته شوند، می‌توانند آنها را از صندلی‌هایشان جلوی کامپیوترهای PDP-11 در کینگ آو پراشا[2] در پنسیلوانیا به ستاره‌ها ببرند.

شرکت طراحی کامپیوتری اتودسک نیز از طریق سرمایه‌گذاری در پروژه زانادو با AMIX

1. Gayle Pergamit
2. King of Prusia

آشنا شد و در آن سرمایه‌گذاری کرد. این دو شرکت با یکدیگر همراستا بودند، ولی دلیل آن فقط افراد مشترک‌شان (از جمله سالین) نبود. هدف هر دوی آنها پیدا کردن، پیش‌بردن و مهم‌تر از همه قیمت‌گذاری روی اطلاعات دیجیتال بود. «جان واکر»، بنیان‌گذار اتودسک در یادداشتی به مدیران اجرایی خود می‌گوید: «به امید روزی که همه بپذیرند در عصر ما اطلاعات نیز مانند گندم، دام و طیور، فرانک سوئیس یا شاخص اس اند پی ۵۰۰ کالایی ملموس است.» اطلاعات به‌نوعی پول بود (یا می‌توانست باشد) و شبکه‌ای که از آن استفاده می‌کرد، می‌توانست کاربردی «بدیهی مانند عملکرد پول در دوره پس از برتون وودز» داشته باشد. واکر در پروژه‌های زانادو و AMIX راهی برای ایجاد بازارهای اطلاعاتی می‌دید که عملکرد و قیمت‌گذاری آن می‌توانست به رشد نوع جدیدی از تحقیق و توسعه مناسب سیستم‌های دیجیتال سرعت ببخشد (نوعی شتاب‌دهنده برای کل جامعه فناورانه).

سازوکار AMIX ایجاد بازاری سرراست (و به‌شدت بلندپروازانه) برای اطلاعات را شامل می‌شد. سیستم زانادو بسیار گسترده‌تر بود، الگویی برای تمام فرهنگ‌های انسانی، گذشته و آینده که در آن اطلاعات دیجیتال و پول جدایی‌ناپذیر بوده و از یکدیگر قابل تشخیص نیستند. در واقع پول دیجیتال اختراع دوباره همه چیزهایی بود که ساخته شده بود و قرار بود ساخته شود. واکر گفت‌وگوهایی خیالی با تیم زانادو داشت که هدف‌شان «طراحی تمام و کمال سیستمی بود که بتواند در زمان حال و آینده همه نوع اطلاعاتی را برای چندین میلیارد نفر در گذر زمان ذخیره کند». او می‌نویسد: «این پروژه در زمان سفر کرده و وارد دنیای خوره‌های فناوری شده بود.»

او از اصطلاح مناسبی استفاده کرده است. نلسون اصطلاح «هایپرتکست» را برای اولین‌بار در سال ۱۹۶۵ به کار برد. او مدام وعده سیستمی را می‌داد که تصوری را که ذهن‌ها در ذهن داشت، به واقعیت بدل کند. این سیستم که زانادو نام داشت، قرار بود به شبکه‌ای جهانی از پایانه‌هایی تبدیل شود که اجازه و ابزار دسترسی به تمام متونی را ارائه کند که تاکنون نوشته شده‌اند یا در آینده نوشته خواهند شد؛ علاوه بر این رابطه‌ای بین تمام متن‌ها، فایل‌های صوتی، ویدئوها، «تصاویر چندبعدی»، اشیا، اشخاص، مکان‌ها و «DNA/RNA» برقرار می‌کرد.

زانادو قرار بود به چیزی تبدیل شود که همه چیز را به همه کس متصل کند. به گونه‌ای که هیچ نوع خاتمه، نهایت یا نقطه پایانی برای هیچ چیز وجود نداشته باشد، به‌جز خود زانادو که طراحی‌اش نهایی بود. نلسون می‌نویسد: «دلیل طولانی‌شدن این پروژه این است که تمامی

ویژگی‌های نهایی آن جزئی از طراحی‌اش محسوب می‌شود. دیگران ابتدا سیستمی را طراحی می‌کنند که کار زیادی انجام نمی‌دهد و سپس مواردی را به آن اضافه می‌کنند، ولی ما این سیستم را به شکل ساختاری یکپارچه طراحی کرده‌ایم که بتواند همه کار انجام دهد.»

سیســـتمی چنین بلندپرواز در این مقیاس به این معنی بود که گزینه‌های طراحی از معنای ضمنی و ماورایی برخوردار بودند. نلســـون می‌گفت که طرح این سیستم نمایانگر الهامی از «ساختار واقعی ایده‌ها» بود. این ســـاختار واقعی، دارایی، مالکیت و گردش پول دیجیتال را شامل می‌شود. ایده‌های بدیع نلســـون درباره جابه‌جایی و نمایش متن دیجیتال (و همچنین پروژه ناتمام و غیرقابل تکمیل چهاردهه‌ای زانادو) بســـیار مورد بحث قرار گرفته‌اند، اما زانادو در عمیق‌ترین سطوح فنی خود یک سیستم پرداختی (و زیرســـاخت بازار) بود که این امکان وجود داشت که فعالیت‌های متنی جدیدی بر اساس آن ایجاد شود. نلسون این سیستم را تحت عنوان «ساختار فنی و قرارداد مالکیت» تعریف می‌کند. پیش از این امکان واگذاری حق تالیف و مالکیت با پرداخت پول وجود نداشـــت. کاربر آینده زانادو (یکی از میلیاردها نفری که طی میلیاردها سال از سیستم دانش بی‌عیب‌ونقصی استفاده خواهد کرد) «مالک حقیقی حق نشر اثر است یا از مالک آن مجوز دارد و برای ذخیره اثر پول می‌پردازد». پایه و اساس شبکه زانادو که از پایانه‌های متصل‌به‌هم تشکیل می‌شد، این بود که «برای هر بایت داده‌ای که منتقل می‌شود، حق نشر پرداخت شود.»

«مارک میلر» یکی از مهم‌ترین برنامه‌نویسان پروژه XOR (که عنوان کاری‌اش «هکر» بود) برای عملی‌کردن این موضوع، توسعه یک سیســـتم آدرس‌دهی را پیش می‌برد[1] که می‌توانست موقعیت و مالک هر بایت از داده را مشخص کند. نلســـون می‌نویسد: «طبق سنت مالکیت[2] هر سندی مالکی دارد؛ بنابراین باید مطابق قوانینی که برای رعایت عدالت تنظیم شده است، در اســـناد دیگر از مالک آن نام برد یا لینکی ارائه کرد.» میلر که نام خود را به شـــکل $amuel می‌نوشـــت تا وفاداری خود به قدرت پول را نشـــان دهد، این جمله قصار را در صفحه اصلی وب‌سایتش نوشته بود: «اگر چیزی در بازار وجود نداشته باشد، می‌توان نتیجه گرفت که ارزش آن بیشتر از پول است.» او بعدها سیستم کامپیوتری و عقد قرارداد هوشمندی به نام «Agorics»

---

۱. سیستم tumbler که عملکرد آن بر خصوصیات اعداد نامحدود مبتنی بود.

۲. با توجه به اینکه حق نشر و مالکیت به‌تازگی به وجود آمده بودند، این سوال مطرح می‌شود که منظور نلسون از «سنت مالکیت» چیست.

را به وجود آورد؛ در ادامه این کتاب او را جزء اکسترو پین‌ها[1] خواهیم دید.

بنیان مالکیت، حق نشر و پرداخت خاصی در این سیســـتم به وجود آمد. قرار دادن مطلب در زانادو به این معنی بود که شما هم مانند دیگران مالک چیزی هستید و برای سرور باید پولی پرداخت کنید. این «ساختار یکپارچه» با شرایط مشخص و «تمامی ویژگی‌های نهایی‌اش» که از ابتدا وجود داشـــتند، همه «مجموعه متن‌های پیچیده (یا افـــکار را)» به کالایی نایاب و کنترل‌شـــده تبدیل می‌کند که تکثیر آن غیر ممکن اســـت. نقل‌قول کردن یک متن آن را تکثیر نمی‌کند؛ بلکه آن را از مکانش در حافظه و حساب کاربری ســـازنده «تراگنجانش»[2] می‌کند (زنجیره‌ای از ارجاع و حق امتیاز). این سیستم فقط داده را نمی‌فروشد؛ بلکه در عمل خود آن را به پول تبدیل می‌کند. مبادله اطلاعات به‌طور کلی به‌صورت تراکنش مالی صورت می‌گیرد. نوشتن و خواندن معادل دریافت و پرداخت وجه است.

اینکه زانادو چطور می‌خواست انتقال وجه را انجام داده و انبوهی از خرده‌پرداخت‌های کمتر از یک سنت را گروه‌بندی و واریز کند، هنوز هم مانند بســـیاری دیگر از جنبه‌های این سیستم در هالـــه‌ای از ابهام قرار دارد. البته مشـــخص بود که به چه چیزی نیاز اســـت. خود اطلاعات دیجیتال باید به یک بازار تبدیل می‌شـــدند و در عین حال، هم خودشان واحد قیمت بوده و هم قیمت‌گذاری می‌شدند. آینده بیش از اینها از ما انتظار داشت. میلر پس از وقفه‌ای، در سال ۱۹۸۸ به پروژه زانادو برگشت و نوشت: «با توجه به ترسی که از فناوری نانو وجود دارد، در کنار شور و هیجانی که نویدش را می‌دهد...، با ایجاد رسانه‌ای بهتر برای گفت‌وگو و تصمیم‌گیری اجتماعی شانس بهتری برای بقا در مقابل خطرات فناوری‌های جدید در اختیار داریم.» مسیر آینده به بازار اطلاعاتی و تصمیمات مرتبط با آن وابسته بود. «رابین هانسون»[3]، اقتصاددان آزادی‌خواهی که مشـــاور تیم بود، یک بازار پیش‌بینی داخلی برای زانادو ایجاد کرد که کارکنان می‌توانستند روی رویدادهای آینده شرط‌بندی کنند، مثلا «قبل از اینکه «دنگ ژیائو پینگ»[4]، رهبر چین بمیرد، زانادو وارد بازار خواهد شد.» هانسون توضیح داد: «آنها امیدوار بودند این محصول بتواند پس از مرگ دنگ برای رســـیدن به دموکراسی به چین کمک کند» (هانســـون نیز در این کتاب جزء

1. Extropians
2. Transcluded
3. Robin Hanson
4. Deng Xiaoping

اکستروپین‌ها مطرح می‌شود و ارزی به نام «ایده‌های آینده»[1] را به وجود می‌آورد).

زانادو عضو ثابت آینده بود؛ از «گروه پیاده‌سازی نهایی» در پنسیلوانیا در سال ۱۹۷۹ گرفته تا وعده‌های واکر در سال ۱۹۸۸ که باور داشت تیم جدید، «نسخه اولیه سیستم زانادو را ظرف ۱۸ ماه به بازار می‌رساند». زانادو که همیشه به تعویق می‌افتاد، قرار بود از شش ماه بعد تا میلیون‌ها سال عملیاتی شود. AMIX باید اینترنت خودش را به وجود می‌آورد و زانادو (که از سرزمین خوره‌های فناوری آمده بود) باید ساختار یکپارچه‌ای ارائه می‌کرد که بتواند تا ابد خودش را با تفکرات مختلفی تطبیق دهد. گفتنی است اتودسک دو سال پس از سرمایه‌گذاری‌اش سعی داشت سهم ۸۰ درصدی خود از AMIX و زانادو را بفروشد و کسب‌وکاری را که به‌دنبال راهی برای ارزشمندسازی اطلاعات دیجیتال بود، رها کند.

AMIX و زانادو هردو سیستم‌هایی عمومی بودند که حول مالکیت صریح متن، فایل و لینک به وجود آمده بودند و به حساب بانکی و هویت ثابت وابسته بودند. تیموتی می به‌خوبی می‌دانست که اگر امکان مخفی‌کردن یا رمزنگاری هویت وجود داشت، در آن صورت چنین سیستمی چه کاربردهایی پیدا می‌کرد. چند نفر از برنامه‌نویسان کلیدی زانادو عضو فهرست ایمیل سایفرپانک‌ها بودند که پس از اولین ملاقات در سال ۱۹۹۲ به وجود آمد؛ آنها کسانی بودند که در داستان جود میلهان سفیران آینده بودند. وقتی «می» با «سالین» در مورد AMIX صحبت می‌کرد، اشاره کرد که این سیستم خیلی زود الگویی برای بازار سیاه می‌شود یا خودش به یک بازار سیاه تبدیل می‌شود. وقتی «می» در مورد طراحی و ساخت میکروچیپ فکر می‌کرد، با سوالی فنی برای AMIX روبه‌رو شد (که در واقع جزء اسرار بازرگانی بود). «چقدر طول می‌کشد تا شخصی که در یک شرکت تولید چیپ کار می‌کند، اطلاعات پژوهشی چندین میلیون دلاری شرکتش را در ازای یکصدهزار دلار بفروشد؟»

این سیستم راهی برای ارزشمندسازی اطلاعات دیجیتال و گامی به سمت پیدایش کریپتوآنارشیسم بود؛ نسخه‌ای متفاوت از بازار که جهان را تغییر می‌داد و ریشه در یک داستان داشت. «می» می‌گوید: «فکر من به‌شدت تحت تاثیر داستان «اسامی حقیقی»[2] نوشته «وینج»[3] بود.»

1. Idea futures
2. True Names
3. Vinge

فصل ششم

مرزهای نامحدود

بانک دیجیتال سایفر پانک‌ها علاوه بر مشـــکل هماهنگی (توافق بر اینکه چه چیزی بسازند) و مشکل تکثیر (کاری کنند که داده به‌راحتی تکثیر نشود) با مشکل پذیرش نیز مواجه بود؛ یعنی افراد کافی از این سیستم استفاده کنند. سایفر پانک‌ها شروع به ساخت بازار، سیستم معاملاتی و نمونه‌های اجتماعی اولیه کردند که هر دولتی را که سر راه جامعه رمزنگاری قرار می‌گرفت، نابود می‌کرد.

آنها برای اینکه سیستم فرضی‌شان مورد پذیرش اجتماعی واقع شود، به جامعه آزمایشی، طبقات بازاری و داستان‌هایی در مورد آینده نیاز داشتند؛ داستان‌هایی از جهان دیگر، مرزهای نامحدود، ستون ایکس و بلک‌نت.

مستر اسلیپری[1]

تیموتی می یک سال پس از اینکه اتودسک، زانادو را از خود جدا کرد، در مورد «تئودور نلسون» نوشت: «او به مسائل رمزنگاری علاقه نشان می‌داد و با چند نفر از تیم ما در مورد گردهمایی هکرها و مفاهیم مربوط به آن صحبت کرده بود.» گردهمایی هکرها یک «شبکه گفت‌وگو» بود؛ «فردترنر» متخصص ارتباطات در تاریخچه محاسبات پادفرهنگی، برای درک اینکه جوامع فنی مختلف در چه حوزه‌هایی می‌توانند همکاری داشته باشند، ایده‌های مشترک پیدا کنند و پروژه‌های مشترکی را کشف کنند، از این عبارت استفاده کرده بود. می در این گردهمایی سخنرانی کرده و برگه‌هایی با محتوای کریپتوآنارشیسم را توزیع کرد؛ واکر در همین گردهمایی با اشخاص کلیدی پروژه زانادو آشنا شد که منجر شد روی زانادو و AMIX سرمایه‌گذاری کند. «جان گیلمور» در مورد رمزنگاری و «اریک هیوز» در مورد پول دیجیتال صحبت کردند. «رودی راکر»، ریاضی‌دان و نویسنده که برای اتودسک کار می‌کرد و با «جود میلهان» برای مجله «موندو ۲۰۰۰» مطلب می‌نوشت، در مورد «حیات مصنوعی»[2] سخنرانی کرد. برنامه‌نویسان و مهندسان الکترونیک با «هکرهای قانونی»[3] (وکلایی که بیشترشان عضو بنیاد مرزهای الکترونیکی بودند) و «هکرهای متنی»[4] که داستان‌های علمی-تخیلی می‌نوشتند، آشنا شدند. یکی از این هکرهای متنی به نام «ورنر وینج» در سن‌دیه‌گو

1. Mr. Slippery
2. Artificial life
3. Legal hackers
4. Prose hackers

ریاضیات تدریس می‌کرد.

وینج در مورد آغاز دوره‌های جدید داستان می‌نوشت. مضمون داستان‌های او زمان و فضایی غیرقابل بازگشت داشتند و همه چیز در آنها متفاوت بود. او در مورد حباب سکون می‌نوشت که زمان را متوقف می‌کرد؛ کسی که وارد آن شده و سپس از آن خارج می‌شد، در یک لحظه، برای همیشه و به شکل غیرقابل بازگشتی به آینده سفر می‌کرد. او همچنین نسخه معاصر و محبوبی از «تکینگی»[1] را در کارگاه ناسا در سال ۱۹۹۳ مطرح کرد؛ مجموعه‌ای از پیشرفت‌های فناوری خودکار و با شتاب بالا (به‌خصوص در حوزه هوش مصنوعی) که فورا از تمامی مدل‌ها و سیستم‌های قبلی پیشی می‌گیرد. او توضیح داد: «پیشرفت فناوری باعث پیدایش قریب‌الوقوع موجوداتی باهوش‌تر از انسان می‌شود که خود به پیشرفت‌های تصاعدی دیگری منجر شده و از کنترل انسان خارج می‌شود... در چنین نقطه‌ای، تمام الگوهای موجود رها شده و دنیای جدیدی به وجود می‌آید.» گویی در تاریخ توسعه فناوری مانعی وجود داشت که با گذر از آن، جهان به‌سرعت از قوه درک انسان فراتر می‌رود؛ مرزی که آن سوی آن غیرقابل تصور است.

او در رمان کوتاه «اسامی حقیقی» که در سال ۱۹۸۱ در مورد شبکه‌های ارتباطی نوشت، کامپیوتر را دروازه‌ای برای ورود به محیطی مجازی به نام «جهان دیگر»[2] می‌دید. هدف هکرها در آنجا این بود که «اسامی حقیقی» خود را پنهان کنند و در برابر خطری که از سوی دولت، تبهکاران و یکدیگر تهدیدشان می‌کرد، از خود محافظت کنند. قهرمان داستان وینج «مستر اسلیپری» نام دارد که با موجودی مرموز و احتمالا غیرانسانی به نام «میل من» درگیر می‌شود. در این کتاب عبارات معذب‌کننده‌ای در گفت‌وگوهای مربوط به جهان دیگر استفاده می‌شود که نشان‌دهنده دهه‌ها تلاش برای کنترل مرزهای آنلاین و آفلاین است.

افسانه‌ها و داستان‌های عامیانه پر از دروازه‌های مرموز، فضاهای خارج از تصور و جهان‌هایی با قوانین متفاوت‌اند؛ مثلا شخصی وارد سرزمین پریان می‌شود که در شرق خورشید و غرب ماه قرار دارد. یک شب آنجا می‌ماند و وقتی به دنیای خود برمی‌گردد، قرن‌ها گذشته است. وینج از چنین سبکی برای روایت داستانش استفاده کرد؛ داستانی که هکرهایش از یک زبان استعاری جادوگری استفاده می‌کردند (البته برخی هکرهای واقعی هم از این زبان استفاده می‌کردند). هکرهای

1. Singularity
2. Other Plane

جادوگر وینج می‌دانستند که (مثل داستان‌های دیو و پری) دسترسی به اسم حقیقی هکر دیگر باعث می‌شود نسبت به آنها برتری داشته باشید. این عنصر عامیانه و کلاسیک در جهان امروزی تجربه‌ای عملی است از حمله به هویت اشخاص، افشای اطلاعات خصوصی، باج‌گیری و استراتژی‌هایی که برای شناسایی و هک سازمان‌ها که نمونه بارز آن گروه آنانیموس[1] است. در چنین جهانی دانستن اسم افراد مساوی قدرت است.

چادرپوش ناشناس هم با صدای رباتیکش در سال ۱۹۹۲ در کلاب پر از دود و سروصدا به سنت جود گفته بود: «در واقع نشان‌دادن هویت واقعی‌ات تضمینی برای شکنجه و مرگت خواهد بود.» وقتی «وی‌دای»[2]، برنامه‌نویس و رمزنگار مبتکر و پرکار، در سال ۱۹۹۸ پروژه پول دیجیتالی بی‌مانی را معرفی می‌کرد، طرح خود را این‌گونه توضیح داد: «من واقعا تحت تاثیر کریپتوآنارشیسم تیموتی می قرار گرفته‌ام... جایی که خشونت در آن بی‌معنی است؛ زیرا نمی‌توان اسامی حقیقی یا موقعیت مکانی افراد را پیدا کرد.»

آینده‌ای که وینج در «اسامی حقیقی» به تصویر می‌کشد، آینده‌ای سرزنده است که احتمال رمزنگاری دیجیتال در آن وجود دارد؛ البته یک چیز از قلم افتاده است؛ «کاون‌ها»[3] (هکرهای توطئه‌گر داستان وینج) می‌توانند بدون ترس از شناسایی‌شدن و «مرگ حقیقی» حاصل از آن آنلاین شوند (بر خلاف دنیای واقعی که آفلاین‌بودن در آن نماد مرگ است). آنها به‌راحتی می‌توانند ملت‌ها، شرکت‌ها، مافیا و خدمات مالی آسیب‌پذیر را بازیچه خود قرار دهند. در اواخر داستان، وقتی مستر اسلیپری سیستم عصبی خود را با شبکه ارتباطات جهانی ترکیب می‌کند، انتقال پول را نیز بخشی از نظارت همه‌جانبه‌اش می‌بیند: «امکان نداشت چکی نقد شود و او در شبکه ارتباطی بانکی متوجه آن نشود.» در آینده‌ای که وینج می‌سازد، ذهن‌هایی که از جسم خود خارج شده‌اند، در واقعیتی مجازی شبیه به سرزمین ارباب حلقه‌ها[4] پرسه می‌زنند و با استفاده از حسگرهای ماهواره‌ای ماورای بنفش همه جا را می‌بینند، اما پول هنوز هم پول است، چک‌ها هنوز برداشت می‌شوند، پولشویی هنوز هم صورت می‌گیرد و بانک‌ها پابرجا هستند؛ اما پول دیجیتال وجود ندارد.

---

1. Anonymous
2. Wei Dai
3. The Covens
4. Lord of the Rings by J.R.R. Tolkien

میراث دوران قبل از فضای مجازی

یک شب در سال ۱۹۹۳، می قبل از بحثی در رابطه با فناوری نانو، برای خودش داستان تخیلی کوتاهی نوشت؛ داستانی که یک قدم از داستان وینج فراتر رفت. می داستان علمی ـ تخیلی خود را به شکل رویدادی واقعی[1] و به سبک «ادگار آلن پو» نوشت. می دعوت‌نامه‌ای از طرف یک سازمان مخفی به نام بلک‌نت نوشت که این طور آغاز می‌شد: «ما از اسم شما اطلاع داریم.»

او پس از گفت‌وگویش با فیلیپ سالین در مورد AMIX در سال ۱۹۸۷، به این ایده و نام مهیجی برای آن می اندیشید. «من نقش وکیل مدافع شیطان را بازی کردم و توضیح دادم که چرا فکر می‌کنم شرکت‌های بزرگ آمریکایی (که هدف اصلی‌شان جذب مشتری است) از چنین سیستمی دوری می‌کنند.» وجود بازار اطلاعاتی به این معنی است که بازار سیاهی نیز وجود خواهد داشت؛ در اوایل دهه ۱۹۹۰ تمام قطعات پازل فناوری کنار یکدیگر قرار گرفته بودند تا این موضوع آشکار شود و تنها جای یک قطعه خالی بود.

تصورات می از چنین سازمانی جزئیات اختراع او را تکمیل می‌کرد. اپراتورها و کاربران بلک‌نت برای یکدیگر ناشناس بودند. بلک‌نت یک کلید عمومی ارائه می‌کرد که با استفاده از آن پیام‌هایی که برایشان فرستاده می‌شد، رمزگذاری می‌شدند تا فقط خودشـــان بتوانند پیام‌ها را بخوانند، اما جایی برای ارسال چنین پیام‌هایی وجود نداشت؛ بلکه کاربر پیام رمزگذاری‌شده را با استفاده از یک توزیع‌کننده ایمیل ناشناس به گروه‌های خبری یا فهرست‌های ایمیل آنلاین ارسال می‌کرد تا به‌عنوان ارسال‌کننده پیام شناخته نشود (گروه‌های خبری، تالارهای گفت‌وگوی عمومی بودند که قبل از پیدایش اینترنت در سیستمی به نام Usenet وجود داشتند). کارمندان بلک‌نت مجموعه‌ای از چنین گروه‌هایی را تحت نظارت داشتند. دعوت‌نامه ارسالی باید توضیحاتی در مورد محصول، ارزش بالقوه آن، یک کلید عمومی مخصوص برای پاسخ‌دادن و «شرایط پرداخت» را شامل می‌شد.

وقتی گروه بلک‌نت پیامی را می‌دیدند که برای آنها رمزگذاری شده است، آن را رمزگشایی کرده و می‌خواندند. از آنجا که پیام به‌صورت مستقیم در مکانی عمومی به اشتراک گذاشته شده بود، برای مدیران بازار بلک‌نت راهی برای پیداکردن کاربر بالقوه وجود نداشت. اگر گروه بلک‌نت به محصول علاقه‌ای داشت، مانند کاربر پیام رمزگذاری‌شده‌ای را از طریق توزیع‌کننده ایمیل به گروه خبری یا

---

۱. همان‌طور که داستان علمی ـ تخیلی ژول ورن از عبور سه روزه مانک میسون شجاع از اقیانوس اطلس در سال ۱۸۴۴ در روزنامه نیویورک سان تحت عنوان «اخبار شگفت‌انگیز!» منتشر شد.

فهرست ایمیل می‌فرستاد؛ رویکردی که «مایرون کوپر من» آن را «استخر پیام» نامید (کوپر من در آن زمان دانشجوی مهندسی کامپیوتر دانشگاه سیمون فریزر بود که در AMIX حساب کاربری داشت و به «آزادی عمل ابدی در فضای مجازی و کامپیوتری»[1] اعتقاد داشت؛ او همچنین فناوری بیت‌کوین را برای انجام امور مالی سازمانی مناسب‌سازی کرد). اگر رمزنگاری و سیستم ناشناس توزیع‌کننده ایمیل پابرجا می‌ماندند، این سیستم می‌توانست یک کانال ارتباطی دوطرفه و غیرقابل ردیابی را برای کسب‌وکار بلک‌نت فراهم کند.

این سیستم نسخه دیجیتالی از تبلیغات خصوصی محرمانه بود که در گذشته در روزنامه‌های دوره ویکتوریایی و ادواردی چاپ می‌شد؛ به این ترتیب که یکی از شماره‌های روزنامه تایمز لندن حاوی پیامی رمزی در قالب حروف («Zanoni Yboko z jo wnm?») و پیام دیگری در قالب اعداد («۵۳۸۵۲۸۴ ۲۸۲۳۰») منتشر می‌شد تا نویسنده و خواننده مد نظر او توسط شخص سومی قابل شناسایی نباشند. کدهایی که در روزنامه چاپ می‌شد، فقط حروفی جایگزین‌شده و قابل پیش‌بینی بودند (مثلا خوانندگان پیام «ozye wpe ud dpp jzf wzzv le logpcefdpxpye» را به محض انتشار در روزنامه دیلی تلگراف رمزگشایی کردند[2])؛ اما بلک‌نت از سیستم رمزنگاری با کلید عمومی استفاده می‌کرد که اگر به‌درستی از آن استفاده می‌شد، به شکل اثبات‌پذیری غیرقابل رمزگشایی بود.

تمام فناوری‌ها و ابزارها، به غیر از یک مورد، برای بدل‌شدن بلک‌نت به واقعیت وجود داشتند. می‌وعده می‌داد: «بلک‌نت می‌تواند به‌صورت ناشناس به حساب بانکی مورد نظر شما پول واریز کند، همچنین اگر قوانین بانکداری محلی اجازه دهد، می‌تواند مستقیما پول نقد را برایتان پست کند (البته مسئولیت به سرقت رفتن آن به عهده خودتان خواهد بود) یا پول شما را در قالب کریپتوکردیت[3] (ارز داخلی بلک‌نت) به شما بدهد. این ایده از AMIX گرفته شده بود؛ بدین نحو که امکان پس‌انداز کریپتوکردیت و خرج‌کردن آن برای خرید اطلاعات محرمانه از دیگر کاربران بلک‌نت وجود داشت. کریپتوکردیت قدمی بزرگ بود که به سمت دنیای خیالات برداشته شده بود؛ مثل اینکه قهرمان داستان ژول ورن با بالن خود به ماه سفر کند.

دعوت‌نامه می‌به یک سازمان غیرواقعی نیز مانند داستان وینج، داستان ژول ورن و ادبیات تخیلی

1. Immortalcybercomputinglaissezfaire
2. [Don't let Js see you look at advertisement]
3. CryptoCredit

و آرمانی دیگر، داستان مرزهایی بود که با عبور از آنها به جهانی دیگر وارد می‌شدید. در واقع این جهان دیگر، یک ناکجاآباد بود (یا همان‌طور که «توماس رید» می‌گوید: «صدایی ناشناس از یک فضای مجازی تهی»). البته این ناکجاآباد، مانند ناکجاآباد داستان «آرمان‌شهر» نوشته «توماس مور» نبود که در جای مشخصی از جهان (در دماغه‌ای کنار جریان آب) قرار داشت (مسافری در داستان مور به ما می‌گوید که این آرمان‌شهر را دقیقا کجا می‌توان پیدا کرد، اما شخصی سرفه می‌کند و مور نشانی آن را کامل نمی‌شنود). «گالتس گالچ»[1] در کتاب فانتزی آزادی‌خواهانه «اطلس شورید» نوشته «آین رند» نیز در رشته‌کوه راکی قرار داشت، ولی با استفاده از ابزاری تخیلی استتار می‌شد؛ او این شهر را از شهر واقعی «اوری» در کلرادو الهام گرفته بود. از طرف دیگر، بلک‌نت ناکجاآبادی هدفمند است که تنها نقطه ثابت آن آدرسی است که به کلید عمومی آن متصل است: «nowhere@cyberspace.nil».

«کن آدام»، طراحی است که اتاق جنگ فیلم «دکتر استرنج‌لاو» و تعدادی از پایگاه‌های مخفی فیلم‌های جیمز باند را با نمایشگرها و نقشه‌های بزرگ، پنل کنترل و تجهیزات و مهمات‌شان طراحی کرده است. «کریستوفر فریلینگ»، منتقد، در گفت‌وگویی که در سال ۲۰۰۸ با آدام داشت، این سوال را مطرح کرد که امروزه مقر تبهکاران فیلم‌های جیمز باندی به چه شکلی طراحی می‌شود. او عنوان کرد که چنین مقری اصلا شبیه مرکز فرماندهی نخواهد بود؛ بلکه می‌تواند یک تلفن همراه یا کیف دستی باشد (الزاما استحکامات نظامی محافظت‌شده‌ای نیست؛ بلکه یک نقطه دسترسی برای شبکه‌ای نامرئی و فراگیر است). طراحی‌های آدام، فانتزی‌های اواسط قرن بیستم را نشان می‌دهد که قدرت را به شکل پناهگاه‌های مدرن با کارمندان شیک‌پوش به تصویر می‌کشد. دعوت‌نامه بلک‌نت می طرحی متعلق به دهه ۱۹۹۰ بود که به جای خودبزرگ‌بینی می‌توان نام پارانویا را روی آن گذاشت. این طرح، جمعیتی از جاسوسان بالقوه را وعده می‌داد که از سلسله‌مراتب کنترل و فرماندهی استفاده نمی‌کردند؛ بلکه از روابط «دوسوکور»[2] استفاده می‌کردند که بر شبکه‌های کامپیوتری، داده‌های رمزنگاری‌شده و پول دیجیتال ناشناس مبتنی بودند.

آنها نیازی به یک مکان خاص نداشتند و از شبکه‌هایی استفاده می‌کردند که از قبل وجود داشت.

---

1. Galt's Gulch
2. Double-blind

بلک‌نت بدون نیاز به هیچ پایگاه یا قلمرویی می‌توانست در زیرساخت نهادهای موجود جریان پیدا کند؛ مانند قطرات باران که از دیوار خانه‌ای قدیمی به داخل چکه می‌کنند. «می» می‌نویسد: «بلک‌نت مواردی از قبیل دولت ملی، قوانین صادراتی، قوانین حق ثبت اختراع، مسائل امنیت ملی و امثالهم را میراث دوران قبل از فضای مجازی می‌داند.» بلک‌نت فقط در آینده‌ای فعالیت می‌کرد که نوع جدیدی از ناکجاآباد بود.

الگوی اجتماعی[1]

دعوت‌نامه بلک‌نت «می» با اینکه حالتی مسخره‌آمیز داشت و لطیفه‌هایی را شامل می‌شد که فقط افراد حوزه فناوری نانو آنها را می‌فهمیدند، همچنان پابرجا ماند و برای گروه‌های مختلف ارسال می‌شد؛ تا اینکه حدود ۲۰ سال پس از افشای اسناد دیپلماتیک آمریکا توسط ویکی‌لیکس بدنامی اندکی هم متوجه این دعوت‌نامه شد. این دعوت‌نامه بخش‌هایی از برنامه‌ای را پیش‌بینی کرد که جولیان آسانژ برای ویکی‌لیکس در نظر داشت و در مقاله «توطئه به نام حکومت»[2] در مورد آن صحبت کرد؛ ایجاد یک چارچوب رمزنگاری برای افشای اطلاعات به‌صورت ناشناس و از کار انداختن سازمان‌ها با تبدیل هر یک از کارمندان به یک افشاگر بالقوه.

ناگهان همه سایفرپانک‌ها به برنامه‌نویسان و کاربرانی تبدیل شدند که در نسخه‌ای آزمایشی از آینده مورد انتظار خود زندگی کرده، آن را امتحان می‌کردند و به سمت آینده پیش می‌رفتند. حتی فهرست ایمیل آنها نمونه اولیه از آینده‌ای بود که فعالیت‌های سایفرپانک‌ها از جمله پول دیجیتال را در بر می‌گرفت. افرادی که عضو دائمی این فهرست بودند، لایه‌لایه‌بودن پلتفرم خود را مشکلی می‌دیدند که باید حل می‌شد تا پول دیجیتال دوام داشته باشد؛ نشانه زودهنگامی که از راه دور، سخت‌افزارهای قدرتمندی را پیش‌بینی می‌کرد. جلسات آنها، گفت‌وگوهایشان، بازی‌هایشان، سناریوهایی که مطرح می‌کردند و داستان‌هایی که می‌نوشتند؛ همگی همین‌طور بودند. گردهمایی‌های سایفرپانک‌ها زمینه را برای تفحص در آینده فراهم می‌کرد. آنها می‌توانستند با کمک یکدیگر «رفتارهای جالب توجهی را که در آینده پدید می‌آمد» استنتاج، ثبت و کشف کنند و خودشان روی فناوری‌هایی کار کنند، «با آنها آزمایش‌هایی انجام دهند، ببینند چه نوع

1. Social prototype
2. Conspiracy as Governance

رفتار جدیدی به وجود می‌آید، چه کاستی‌ها و موانعی پدید می‌آید و چگونه می‌توان از سد آنها گذشت و غیره.»

این جامعه متن‌باز شکلی به خود گرفته بود که «کریس کلتی»، پژوهشگر علم و فناوری، آن را «جامعه بازگشتی»[1] می‌نامد. جامعه بازگشتی، دائما به فناوری‌هایی باز می‌گردد که موجب پیدایش آن شده‌اند و آنها را اصلاح می‌کند. «لاناسوارتز» با بررسی توسعه‌دهندگان رمزارزها به ایده مرتبطی دست پیدا کرده که گام بعدی جامعه بازگشتی است؛ «همکاری زیرساختی»؛ گروه‌هایی که «برای ایجاد و پشتیبانی پلتفرمی برای معامله در همکاری با یکدیگر ارزش قائل‌اند، پلتفرمی که از دخالت‌ها و گمانه‌زنی‌های واسطه‌های حقوقی در امان است» و محیطی پربار برای الگوهای اجتماعی محسوب می‌شود.

«الگوی اجتماعی» عبارتی است که «فردترنر» از آن استفاده می‌کند. او در مورد سیلیکون‌ولی می‌نویسد: «این مدل گردهمایی‌ها (از دفاتر استارت‌آپی گرفته تا فستیوال برنینگ‌من) فناوری‌هایی را در دل خود دارند که به خودی خود الگویی از یک جامعه ایده‌آل هستند.» ترنر روش‌های ساخت نمونه را در مهندسی نرم‌افزار بررسی کرد و اظهار کرد که این روش‌ها فقط احتمالات فنی را نشان نمی‌دهند؛ بلکه گروه‌های جدیدی از افراد را در کنار یکدیگر قرار می‌دهند. آنها فقط یک شیء به وجود نمی‌آوردند؛ بلکه جامعه‌ای را به وجود می‌آوردند که از آن شیء استفاده کند. «این اشخاص می‌توانند کمک کنند فناوری وارد بازار شود، اما به خودی خود نشان‌دهنده احتمالات اجتماعی جدیدی نیز هستند.» البته بخشی از کسب‌وکار سیلیکون‌ولی در اوایل قرن بیست‌ویکم این بود که جوامع جدیدی را شناسایی کرده و آنها را با ظاهری جذاب رواج دهد. این جوامع از محصول، پلتفرم یا خدمات خاصی مثل همکاری و زندگی مشترک، پیام‌های تصویری موقت، هولوکراسی[2]، رقابت‌های ورزشی بازی‌گونه یا پیاده‌روی و گشتن به‌دنبال پوکیمون‌ها[3] در موقعیت‌های جغرافیایی مختلف، استفاده می‌کردند. الگوها بر پایه گذشته و آنچه از قبل موجود است، ساخته می‌شود، ولی در نقش حیطه‌ای برای نمونه‌سازی و کنترل آینده احتمالی عمل می‌کند؛ یعنی یک نوع کاز موگرام که تصویر خودش را بازتاب می‌دهد. فضایی که برای کار کردن روی کامپیوترها وجود داشت،

1. Recursive Publics
2. Holacracy
3. Pokemons

مانند نسخه‌ای از یک اتاقک حباب[1] بود که با استفاده از ردیاب نوترینو[2] قابل شناسایی بود که در آن به‌دنبال اثرات محسوس چیزهای نامحسوس و سنجش آینده غیرقابل سنجش بودند.

مرزهای نامحدود

«جان پری بارلو» می‌گوید: «وقتی با تلفن حرف می‌زنید، در فضای مجازی هستید.» از نظر فیزیکی همین‌جا حضور دارید، ولی با استفاده از یک دستگاه به فضای دیگری وارد شده‌اید. «ویلیام گیبسون» اصطلاح «فضای مجازی» را تحت عنوان وضعیت آتی فناوری اختراع کرد (او در مصاحبه‌ای در سال ۱۹۸۵ عنوان کرد: «فضای مجازی همان جایی است که بانک پول شما را نگه می‌دارد»). «بارلو» که پیش از این مشغول تماشای بازی !Spacewar بود، در تابستان سال ۱۹۹۰ و در شبکه اجتماعی WELL (که «استوارت برند» آن را ساخته بود) این اصطلاح را به زمان حال وارد کرد. بارلو آغاز فعالیت «بنیاد مرزهای الکترونیکی» را اعلام می‌کرد؛ سازمانی قانونی که در خدمت آزادی مدنی در دنیای دیجیتال بود. او می‌نویسد: «در این جهان ساکت، همه مکالمات تایپ می‌شوند. برای ورود به این جهان، شخص باید جسم و مکان خود را فراموش کند و جزئی از کلمات شود... این جهان در سراسر حوزه وسیع حالت الکترون، ریز موج، میدان مغناطیسی، حرکت نوری و به قول ویلیام گیبسون فضای مجازی گسترش می‌یابد.» این «حوزه وسیع» دستاورد بنیاد مرزهای الکترونیکی بود.

فضای مجازی گیبسون همانند پیدایش زیرساخت مدنی بود که شرکت‌های بزرگ، خدمات شهری و حتی کهکشان‌های دوردست و سیستم‌های نظامی بر آن حکم‌فرما بودند. بارلو این فضا را نویدبخش محیط خارجی بزرگی می‌دانست که موجود بوده و از این جهان امکان دسترسی به آن وجود داشت؛ مانند صفحه سفید پشت یک نقشه که افرادی زمین‌های آن را تصاحب کنند. هر جا که آنتن‌دهی خطوط تلفن همراه یا امکان نصب مودم وجود داشت، می‌توانستید مانند هاکلبری‌فین «به سرزمین پیش روی خود قدم بگذارید». زمان تعیین‌کننده‌ای بود که «فردترنر» آن را «یکی از سوءتفاهم‌های برپایی اینترنت» می‌نامد. این سوءتفاهم این بود که مردم به جای اینکه اینترنت را مجموعه‌ای از زیرساخت‌های جهانی بدانند که در کنار یکدیگر کار می‌کنند، فکر می‌کردند که

1. Bubble Chamber
2. Neutrinodetector

«اینترنت یک مکان است» (مخصوصا مکانی در آمریکا).

بخشی از تصور این مکان غیرواقعی (و محیط خارجی وسیع) از هویت ناشناس و رمزنگاری‌شده و ارزش‌های آن ناشی می‌شود. تیموتی می می‌نویسد: «این قضیه مانند یک سوپاپ اطمینان عمل می‌کند؛ شخص می‌داند که امکان حرکت به سمت مرزهایی را دارد که در آنجا مسئولیت گذشته‌اش را بر عهده نخواهد داشت.» چنین موضوعی باعث ایجاد جامعه‌ای می‌شود که «مرزها را حفظ کرده و روحیه کالوینیستی[1] فاش‌نکردن مسائل خصوصی در آن وجود دارد.» هدف از این برنامه برق‌رسانی به مناطق روستایی نیست؛ بلکه سکنی‌دادن به جامعه الکترونیکی در فضایی بزرگ و بی‌قانون است که مواردی از جمله اسم مستعار و خوش‌نامی، دزدی، اعتمادبه‌نفس و دفاع از خود در فضای فناوری و کیسه‌هایی از پول غیرقابل ردیابی را شامل می‌شود؛ در حالی که بانکی به چشم نمی‌خورد.

می در مانیفستی که در سال ۱۹۹۲ برای جود میلهان خواند، اعلام کرد که این سرزمین فکری رفیع آماده تصاحب است؛ «تنها اختراع به‌ظاهر کوچکی مانند سیم خاردار لازم است که امکان فنس‌کشی به دور مراتع و مزارع وسیع این سرزمین را فراهم کند و برای همیشه مفهوم حق مالکیت زمین را در غرب دچار تغییر کند؛ به همین ترتیب، کشف کوچکی در شاخه ریاضیات به مثابه سیم‌بری خواهد بود که سیم خارداری را که به دور مالکیت معنوی کشیده‌شده از بین می‌برد.» او در دعوت‌نامه بلک‌نت خود شرایط سخت‌تری را عنوان کرده و دو نوع مالکیت معنوی را مطرح می‌کند که سرعت پیشرفت فناوری رمزنگاری را کاهش می‌دادند؛ «قوانین صادرات و حق ثبت اختراع علنا برای نشان‌دادن قدرت ملی و امپریالیستی و فاشیسم دولت استعمارگر استفاده می‌شوند.»

بارلو در سال ۱۹۹۶ «بیانیه استقلال فضای مجازی»[2] را منتشر کرد. متن این بیانیه که در گردهمایی قدرت‌های جهانی در شهر داووس سوئیس تهیه شده بود، به گونه‌ای بود که باید سوار بر اسب خوانده می‌شد و مناسب زمین‌های بربادرفته کشور آزادی بود که می در نظر داشت: «ای دولت‌های جهان صنعتی، ای غول‌های ملالت‌بار گوشت و فولاد، من از فضای سایبری می‌آیم؛ منزلگاه جدید ذهن. از جانب آیندگان از شما مردم گذشته درخواست می‌کنم که ما را به حال خودمان بگذارید. شما در میان ما جایی ندارید. در مجمع ما حق حاکمیتی برای شما وجود

1. Calvinist
2. Declaration of the Independence of Cyberspace

ندارد... شما سعی دارید با تخلیه پست‌های نگهبانی مرزهای فضای مجازی، از خودتان در برابر ویروس آزادی محافظت کنید.»

رابطه این زنجیره از استعاره‌ها، تشبیهات و ارجاعات با تاریخ حقیقی غرب و آمریکا، همانند رابطه فضای مجازی گیبسون با سرورهای واقعی، ارتباط از راه دور یا مرورگر اینترنت بود؛ آنها فقط افسانه‌های تاریخی بودند که داستان علمی‌ـ‌تخیلی پلتفرم‌های احتمالی آینده مانند بلک‌نت را تکمیل می‌کردند. مهاجران اولیه (مانند کسانی که به غرب مهاجرت کرده بودند) به دولت وابسته بودند و قصد فرار از آن را نداشتند؛ دولتی که با چارچوب قانونی و توسعه نظامی، حمل‌ونقل و نیروی دریایی؛ نقشه‌ها و وعده‌های سیاسی و طرح‌های سرمایه‌گذاری و سوبسید آنها را خریده بود. این افراد به جای اینکه حق حاکمیت را بین همگان توزیع کنند، به آن خدمت می‌کردند. البته هدف این نبود که همه چیز دقیقا توضیح داده شود. داستان‌هایی که سایفرپانک‌ها تعریف می‌کردند، صحت نداشتند، اما اشتباه هم نبودند؛ هدف این داستان‌ها استدلال تاریخی نبود؛ بلکه انتقال یک حس بود.

مقایسه‌هایی که دو حالت فرضی بسیار متفاوت (غرب وحشی و فضای سایبری) را در کنار هم می‌گذاشتند، متقاعدکننده‌تر می‌شدند؛ چراکه هیچ‌کدام «واقعی» نبودند؛ بلکه آینده بالقوه‌ای را نشان می‌دادند که می‌توانست به واقعیت تبدیل شود. دلیل متقاعدکننده‌بودن این «مرزهای» تاریخی خیالی در دهه ۱۹۹۰ این بود که مهندسانی با مدرک دکتری آن را مطرح می‌کردند؛ کسانی که یکشنبه‌ها به صرف صبحانه در برکلی گرد هم می‌آمدند تا در مورد رمزنگاری بحث کرده و پس از آن به تمرین تیراندازی بپردازند (بارلو مزرعه‌ای به نام Bar Cross Ranch در «وایومینگ»[1] داشت که عموی پدرش آن را تاسیس کرده بود). می‌نویسد: «این مرزهای جدید و غیرقابل دسترس برای دولت‌های ظالم، داستان اسامی حقیقی و ینج را به واقعیت تبدیل کرده بود.»

مرز دیجیتال تصوری بود که تجربه زندگی بدون ماده را ممکن می‌کرد؛ محیط خارجی شبکه‌ای غیرمادی که در زندگی هر روزه افراد نفوذ کرده بود. بارلو به‌مانند پیام‌آوری روحانی چنین می‌نویسد: «جهان ما در عین حال همه جا هست و هیچ جا نیست؛ اما هر کجا که باشد، از این دنیای مادی خارج است. هویت ما جسم ندارد، پس بر خلاف شما نمی‌توانیم با تهدید و اجبار نظم را برقرار کنیم.»

1. Wyoming

چه کسی حاضر است به قطار مهاجران بدون جسمی بپیوندد که به سمت مرزهای همه جا و هیچ جا در حرکت است تا اقتصاد خود را بر پایه پول دیجیتال بسازد؟ «اغلب افرادی که در این حوزه‌ها پیش‌قدم می‌شوند، افراد خطرپذیری هستند که به امید پاداش، فناوری‌های جدید را می‌پذیرند.» برای جذب این افراد پاداش‌هایی نیاز بود. همچنین مکان‌هایی لازم بود که جوامع آزمایشی بتوانند آغاز به کار گروه‌هایی را پنهان کنند که قرار بود در این فضا پیشرفت کنند. علاوه بر این به افرادی نیاز بود که برای ساخت شبکه‌ای نامطمئن، گاهی مصیبت‌بار و بعضی اوقات خطرناک، برای پول و مبادلات رمزی دلیلی داشته باشند.

آزادی اطلاعات

می برای یگان ضربت کریپتوآنارشیسم و دارندگان پول دیجیتال نام «ستون ایکس» را انتخاب کرد. او این نام را با تغییر اصطلاح «ستون پنجم»، برای جامعه توطئه‌گری، انتخاب کرده بود که به دشمن خدمت کرده و کشور را از درون نابود می‌کنند. خرابکاران و جاسوسان او به وسیله یک متغیر نشان داده می‌شدند و برای عنصر ناشناخته‌ای کار می‌کردند. او می‌نویسد: «برای جذب افراد در ستون ایکس به فشار خارجی نیاز بود. نیاز به کالاهای غیرقانونی مانند مواد مخدر، یکی از این محرک‌ها را فراهم می‌کرد. سایر بخش‌ها عبارت بودند از: فروشندگان، خریداران و مدیران، انتقال مخفیانه اطلاعات و برنامه‌های محرمانه برای آزمایش کیفیت و اعتبار» (دهه‌ها بعد، «راس اولبریکت» اعلام کرد که این ایده به او الهام بخشید که بازار سیاه «سیلک‌رود» را در دارک‌وب به وجود بیاورد). اما چیزی که می واقعا به آن علاقه داشت، افشای اطلاعات در ازای دریافت پول دیجیتال بود.

جامعه سایفرپانک (فارغ از اینکه جزء پروژه کریپتوآنارشیسم بودند یا نه) همگی طرفدار «آزادی اطلاعات» بودند؛ زیرا حوزه علاقه‌مندی و پژوهش مشترک‌شان به‌شدت تحت نظارت بود. «گیلمور» که فهرست ایمیل را راه‌اندازی کرده بود، وقت خود را به تحقیقات کتابخانه‌ای و درخواست برای «قانون آزادی اطلاعات» اختصاص داده بود تا آثار «الیزابت» و «ویلیام فریدمن» و «رالف مرکل» را از حالت محرمانه خارج کرده، به شکل دیجیتال درآورد و منتشر کند. مقالات مرتبط دیگری که در ژورنال‌های آکادمیک و تخصصی منتشر شده بودند نیز باید امانت داده می‌شدند تا بتوان از آنها عکس گرفت یا اسکن کرد، یا در صورت نیاز دوباره تایپ کرد و در شبکه

به اشتراک گذاشت.

اریک هیوز می‌گوید: «سایفرپانک‌ها کدنویسی می‌کنند» و این کار را با ذهنیت انسان‌هایی انجام می‌دهند که از آسیب‌پذیری محصولات رمزنگاری‌شده اطلاع دارند که بدون بررسی عمومی منتشر شده‌اند. البته آنها سابقه مشترکی نیز با هکرهای یونیکس داشتند که راهنمای یک سیستم‌عامل اختصاصی را تکثیر و منتشر کردند و همچنین خوره‌های تلفنی که فهرست سیگنال‌های تلفن را از مجله تخصصی تلفن بل[1] استخراج کردند. بسیاری از سایفرپانک‌ها عضو جنبش نرم‌افزارهای رایگان و متن‌باز بودند که هدف اساسی‌اش این بود که نرم‌افزار باید لزوما سرگشاده و رایگان باشد و بتوان آن را مطالعه و بررسی کرد، به اشتراک گذاشت، عیب‌یابی کرد و بهبود بخشید. «ریچارد استالمن» در این‌باره می‌گوید: نرم‌افزارها باید برای همگان آزاد و رایگان باشند؛ «درست مثل آزادی بیان. موضوع آزادی است، نه قیمت» (در سال ۱۹۹۷ وقتی می در کنفرانس حریم خصوصی دیجیتال در مورد اهمیت معاملات غیرقابل ردیابی صحبت می‌کرد، استالمن داستانی علمی‌ـتخیلی به نام «راه تایکو»[2] منتشر کرد. داستان کتاب در جامعه‌ای دیستوپیایی اتفاق می‌افتد که خواندن کتاب دیگران سرقت محسوب می‌شود و از جایی که تمام کتاب‌ها فقط به‌صورت دیجیتال موجود هستند، این امر به‌راحتی قابل شناسایی است).

اطلاعات محرمانه، مخاطبان دیگری نیز داشتند؛ از جمله پژوهشگران خارجی که به کتابخانه‌ها یا نشریات دسترسی نداشتند، کارگزاران سهام که می‌خواستند سهام غیرقانونی خریدوفروش کنند، دانش‌آموزان متقلبی که می‌خواستند به اوراق امتحانی دست پیدا کنند، وام‌دهندگانی که به‌دنبال گزارش‌های اعتباری غیرقانونی بودند، نمایندگی‌های بیمه‌ای که به‌دنبال سوابق پزشکی افراد بودند، کارفرمایانی که به‌دنبال سوءپیشینه افراد بودند، کارمندانی که از کارشان اخراج شده یا بیرون آمده بودند و سعی داشتند با نقض «پیمان‌نامه عدم افشا» داده‌های دزدی خود را به پول تبدیل کنند، افرادی که به‌دنبال آموزش اورکلاکینگ[3] کامپیوتر، آموزش کاشت ماریجوانا در خانه، تولید شیشه، برقراری تماس راه دور به‌صورت رایگان یا تعمیر یخچال بدون باطل کردن ضمانت آن هستند. دوستداران فیلم، گیمرها، طرفداران انیمیشن، کلکسیونرهایی که کتاب‌های فکاهی قدیمی جمع می‌کنند، خوانندگان کتاب‌های قدیمی که چاپ‌شان متوقف شده، کسانی

1. Bell Telephone technical journal
2. The Road to Tycho
3. Overclocking

که به‌دنبال صفحات موسیقی قدیمی هستند، طرفداران موسیقی جاز، طرفداران دوآتشه اپرا (که بسیاری از اجراهای زنده قدیمی را به‌صورت غیرقانونی روی گرامافون ضبط کرده‌اند) و طرفداران بازیگران فیلم‌های پورن.

فعالان سیاسی، معترضان و کسانی که اخبار را در بوق و کرنا می‌کنند، به اطلاعات محرمانه و ابزاری برای مخابره آن نیاز دارند. بیشترین کاربران اولیه سیستم‌های توزیع‌کننده ناشناس ایمیل، کسانی بودند که از فرقه ساینتولوژی[1] خارج شده بودند یا علیه آن فعالیت می‌کردند و اسناد مربوط به افراد سطح بالای این فرقه را با یکدیگر تبادل می‌کردند. به درخواست کلیسا برای پیدا کردن هویت یکی از افشاگران اطلاعات، پلیس بین‌الملل به سیستم پنهان‌کننده هویت Usenet در فنلاند (anon.penet.fi) حمله کرد. «یوهان هلسینگیوس»، متخصص اینترنت فنلاندی در ابتدای پروژه خود گفته بود: «اگر پلیس یا دستگاه‌های محرمانه دولتی با حکم قضایی به خانه من بیایند و پایگاه داده را از من بخواهند، می‌توانم با آنها همکاری کنم.» اما آیا راه دیگری نیز وجود داشت؟

او اخطار داد: «تنها راه این است که هر کس یک سیستم رمزنگاری مانند PGP با کلید عمومی مخصوص خود داشته باشد تا از سوءمدیریت در امان باشد.» PGP نرم‌افزاری برای رمزگذاری و امضای پیام‌ها بود. این نرم‌افزار در زمان عقد پیمان منع گسترش سلاح‌های هسته‌ای ایجاد شده بود که اعضای آن اغلب تحت نظارت خانگی بودند. توصیه هلسینگیوس به استدلالی شباهت داشت که به نفع «تمامی» کسانی بود که از چنین سیستمی استفاده می‌کردند و با اعتراض سیاسی خود زمینه را برای کریپتوآنارشیسم فراهم می‌کردند. «سمیر پارخ»، سایفرپانک و کارآفرین حوزه فناوری که بعدها روی پول دیجیتال و رمزنگاری مالی کار کرد، در سال ۱۹۹۱ وقتی دانش‌آموزی دبیرستانی بود کتاب «نافرمانی مدنی» نوشته «ثورو» را با استفاده از کامپیوتر IIGS اپل تایپ کرد و نقطه تحولی را در تاریخ به‌اشتراک‌گذاری آنلاین در آمریکا رقم زد (امروزه هم اگر به نسخه آنلاینی از این کتاب برخوردید، یادداشت «تایپ‌شده توسط سمیر پارخ» را در انتهای آن خواهید دید). در ادامه، هنگامی که از راه‌اندازی یک پناهگاه داده[2] دریایی روی شناوری فرضی در دریای شمال صحبت می‌کنیم، با او بیشتر آشنا می‌شویم.

همه این گروه‌ها برای نیاز خود به سیستم معاملاتی با پول دیجیتال، دلایلی منطقی داشتند.

---

1. Scientology
2. Data haven

فروشندگان مواد مخدر، بازیگران فیلم‌های مستهجن، کسانی که فایل‌ها را به‌صورت غیرقانونی دانلود می‌کردند، فروشندگان اطلاعات محرمانه یا غیرقانونی و مشتریان و حمایت‌کنندگان آنها؛ همگی به ابزاری برای تجارت محرمانه نیاز داشتند. فعالان سیاسی و معترضان هم برای تهیه اسباب کار خود به راهی نیاز داشتند تا بتوانند کار خود را انجام داده و در شرایط سخت از یکدیگر محافظت کنند. همان‌طور که گذر زمان نشان داده اســـت، این نگرانی‌ها فرضی نبوده‌اند؛ از شرکت‌های اعتباری که کمک مالی به ویکی‌لیکس را ممنوع کردند تا پلتفرم‌هایی مانند پی‌پال و Patreon که دارایی‌ها و معاملات مرتبط با «مسائل جنسی» و روسپی‌گری را مسدود کردند.

جامعه دیگری نیز وجود داشت که نیازش به اطلاعات محرمانه و پول دیجیتال چندان آشکار نبود، ولی بعدها آشکار شـــد؛ جاودانه‌گرایان[1]. می به تفصیل در مورد آنها صحبت کرده است: «کسانی که اهل تحقیقات پزشـــکی ممنوعه و به‌دنبال زندگی پس از مرگ بودند. این افراد وقت خود را به جمع‌آوری، اشتراک‌گذاری و آزمایش تکنیک‌های افزایش طول عمر و جلوگیری از پیری اختصاص دادند. چنین گروهی به‌دنبال سیستم‌های معتبر ناشناسی خواهد بود که نتایج مطالعات علمی ممنوعه را در آن منتشر کرده و ابزاری را برای درجه‌بندی کلینیک‌های مخفی فراهم کند. آنها برای داروهای آزمایشی، گردشگری پزشکی و پیدا کردن جوامع حامی فعالیت‌های غیرقانونی یا تاییدنشده، به یک بازار نیاز دارند.»

این جامعه به ابزار مالی خاصی نیاز دارند، از جمله طرح‌های بیمه غیرمعمول، سرمایه‌گذاری مشـــارکتی برای گروه‌هایی که ممکن است اعضایشـــان خیلی زود بمیرند یا قرن‌ها عمر کنند، وصیت‌نامه، سرمایه‌گذاری معمولی و دارایی تخصیص‌یافته برای کسانی که برای ورود موقتی به «کمای سوخت‌وساز»[2] آماده می‌شوند (یعنی خودشان را منجمد می‌کنند تا در آینده دوباره به زندگی برگردانده شوند). آنها به نوعی از پول نیاز دارند تا بتوانند با آن هزینه آزمایش‌ها و نگهداری بدن‌شان را پرداخت کنند، پس‌انداز و معامله کنند و پرداخت‌های بلندمدت را انجام دهند.

تعریفی که می از این گروه ارائه می‌کند تا حدودی تخیلی است، ولی چنین گروهی واقعا وجود داشت. پول آزمایشی که آنها برنامه‌ریزی و طراحی کرده بودند، قدمی بود به سمت زندگی جاودان. اما پول دیجیتال هنوز هم با مشکلاتی اساسی مواجه بود که باید حل می‌شد.

---

1. Immortalists
2. Metabolic coma

هیچ‌کس هیچ‌چیز مدنیوز

روایتی تاریخی و کمتر دیده و شنیده شده از پول؛ تلاشی برای معرفی تاریخچه ناشناخته رمزارزها و روایتی از رسیدن به مفهوم پول نقد دیجیتال!

پول دیجیتال، مفهومی است که در عصر ما به‌وفور به کار برده می‌شود. هنگامی که صحبت از پول دیجیتال به میان می‌آید، **بیت کوین** اولین چیزی است که به ذهن بسیاری می‌رسد، اما آیا در واقعیت بیت کوین اولین پول دیجیتالی است که ایجاد شده است؟

برخی تصور می‌کنند رمزارزهایی مانند بیت کوین مفهومی جدید هستند؛ چیزی که این کتاب تلاش می‌کند آن را رد کند و با استناد به وقایع تاریخی نشان می‌دهد که بیت کوین ریشه تاریخی بیش از آن چیزی دارد که ما در ذهن خود متصور هستیم. این کتاب، داستان ناگفته پول دیجیتال و افرادی را تعریف می‌کند که به‌دنبال ساختن آن بودند. هدف بعضی از آنها زمین‌زدن دولت‌ها و ایجاد آرمانشهری رمزنگاری‌شده بود. برخی نیز می‌خواستند ماشینی را پدید بیاورند که بتوانند با آن تا ابد زندگی کنند.

این کتاب تلاشی است برای پاسخ به سوالاتی مانند اینکه: **ما چگونه یاد گرفتیم که اعتماد کنیم و انواع متفاوت پول را استفاده کنیم؟** چه چیزی اشیای دیجیتال را ارزشمند می‌کند؟ ارزها چگونه به عنوان یک واقعیت پذیرفته می‌شوند؟ چگونه دیجیتال معادل پول نقد می‌شود؟ این کتابی متفاوت است و برای کسانی مناسب است که می‌خواهند **فلسفه و تاریخچه رمزارزها** را بدانند.

ایجاد و درست کردن یک واحد پول، نیاز و واقعیتی ذهنی است که در ذهن و تصورات افراد ریشه دارد.

PRINCETON UNIVERSITY PRESS

کتاب پول نقد دیجیتال با حمایت کارخانه نوآوری راه‌کار منتشر شده و ناشر اصلی آن انتشارات دانشگاه پرینستون است

راه‌کار
کارخانه نوآوری راه‌کار
way2work.ir

ISBN 978-622-97220-7-7

۵۰۰ هزار تومان

انتشارات راه پرداخت
ناشر فناوری و نوآوری
way2pay.press