در جست‌وجوی پولِ نقدِ دیجیتال

داستان پیدایش بیت‌کوین از منظر
تلاش‌های آدام بَک و دیگر اعضای گروه سایفرپانک

سخنی با خوانندگان

در اوایل دهۀ ۱۹۹۰ میلادی دولت‌ها گنجینه‌ای از اطلاعات دیجیتال شهروندان خود را در اختیار داشتند. شرکت‌های ارائه دهندۀ خدمات دولتی و شرکت‌های خصوصی این اطلاعات را به دلایل مختلفی جمع‌آوری کرده بودند. جمع‌آوری و تجزیه و تحلیل چنین حجمی از اطلاعاتْ دورۀ تازه‌ای از شنود و جاسوسی از شهروندان را آغاز کرد که در دو دهه بعد به جنگی بسیار پیچیده تبدیل شد؛ جنگی که سوت‌زنِ مشهور آژانس امنیت ملی آمریکا ادوارد اسنودن در سال ۲۰۱۳ میلادی تنها گوشه‌ایَ از آن را افشا کرد.

فراهم آوردن ابزارهایی به‌منظور حفاظت از حریم خصوصی شهروندان در عصر دیجیتال، دغدغۀ گروهی از افراد بود که با نام «سایفرپانک» شناخته می‌شدند. جلسات حضوری این گروه در سال ۱۹۹۲ در شهر سانفرانسیسکو برگزار می‌شد و آن‌ها در این جلسات به‌کارگیری رمزنگاری برای رسیدن به آزادی‌های اجتماعی را مورد بررسی قرار می‌دادند. ایده‌های آنان در گروه ایمیلی سایفرپانک‌ها که به اختصار به «لیست» معروف است منتشر می‌شد، جایی که ایده‌های پشت بیت‌کوین توسعه یافت و سرانجام ۱۶ سال بعد توسط ساتوشی ناکاموتو منتشر شد.

با پیشرفت‌هایی که در اواسط دهۀ ۷۰ میلادی در علم رمزنگاری صورت گرفت و همچنین با ابداع روش رمزنگاری بر پایۀ کلید عمومی که در نهایت به ابزار رمزنگاری PGP

انجامید، پول نقد دیجیتال به چالش بعدی سایفرپانک‌ها تبدیل شد؛ مسیری که از اوایل دهۀ ۸۰ میلادی با تلاش‌های دیوید چام آغاز و در نهایت موجب خلق بیت‌کوین شد و همچنان ادامه دارد.

الکس گلداستین در این مقاله داستان پیدایش بیت‌کوین و پروژه‌هایی که قبل از بیت‌کوین برای خلق پول دیجیتال تلاش کرده بودند را از منظر فعالیت‌های آدام بَک و دیگر اعضای گروه سایفرپانک مورد بررسی قرار می‌دهد.

سایت منابع فارسی بیت‌کوین
پاییز ۱۴۰۰

در یکی از روزهای تابستانی اوت سال ۲۰۰۸ میلادی، آدام بَک[۱] ایمیلی از ساتوشی ناکاموتو[۲] دریافت کرد.

این اولین بار بود که ناکاموتو دربارهٔ پروژه‌ای که برنامه‌نویس یا برنامه‌نویسان آن نام بیت‌کوین را روی آن گذاشته بودند، با کسی صحبت می‌کرد. ایمیل ساتوشی، طرحی را شرح می‌داد که برای برنامه‌نویسان معتقد به حریم خصوصی که با نام سایفرپانک‌ها[۳] شناخته می‌شدند، حکم به حقیقت پیوستن یک رؤیای ناممکن را داشت: «پولِ نقدِ دیجیتالِ غیرمتمرکز.»[۴]

تا اواسط دههٔ ۲۰۰۰، متخصصین علوم رمزنگاری برای ایجاد نسخهٔ دیجیتالِ پول کاغذی با ویژگی حامل[۵] (وجه نقد) که حفظ حریم خصوصی کاربران خود را تضمین کند، تلاش‌های بسیاری کرده بودند. با وجود پیشرفت‌هایی که در علوم «رمزنگاری کلید عمومی»[۶] در دههٔ ۷۰ و همینطور blind signatures در دههٔ ۸۰ ایجاد شد، «پول نقد دیجیتال[۷]» رفته رفته تبدیل به چیزی فراتر از رؤیاهای علمی مطرح شده در کتاب‌هایی چون Snowcrash یا Cryptonomicon شده بود، و می‌رفت تا آرام آرام به واقعیت بپیوندد.

یکی از اهداف اصلی این پولِ دیجیتالْ قابلیت مقاومت در برابر سانسور[۸] بود، پولی که دولت‌ها و شرکت‌های بزرگَ کنترلی روی آن نداشتند. اما همهٔ پروژه‌های اولیه از یک نقطهٔ ضعف رنج می‌بردند و آن چیزی نبود جز تمرکز. ریاضیات پیشرفته‌ای که در این سیستم‌ها به‌کار گرفته شده بود اهمیتی نداشت، زیرا در نهایت تحت کنترل افراد یا

1 Adam Back
2 Satoshi Nakamoto
3 Cypherpunks
4 decentralized digital cash
5 Bearer
6 Public-key cryptography
7 e-cash
8 Censorship-resistance

نهادهایی بودند که قادر به سانسور برخی از تراکنش‌ها، یا ایجاد تورم از طریق تغییر سیاست‌های پولی بودند.

در دهه‌های ۹۰ و اوایل ۲۰۰۰، پیشرفت‌های زیادی در مسیر خلق «پول نقد دیجیتال»[1] صورت گرفت و هرکدام از این پروژه‌ها قدم بزرگی در مسیر حل مشکلات اساسی برمی‌داشتند. با وجود این تا پیش از سال ۲۰۰۸ همچنان یک مشکل بزرگ در حوزهٔ علوم کامپیوتر حل نشده باقی مانده بود و دنیا را از رسیدن به یک سیستم پولیِ غیرمتمرکز محروم می‌کرد: «مسألهٔ ژنرال‌های بیزانس»[2]

فرض کنید شما فرمانده ارتشی هستید که صدها سال پیش و در دوران امپراطوری عثمانی، قرار است به شهر بیزانس حمله کند. ارتش شما ۱۲ فرمانده دارد که در موقعیت‌های مکانی متفاوتی حضور دارند. چطور می‌توانید حمله‌ای غافلگیرانه در زمانی دقیق و مشخص ترتیب دهید؟ اگر جاسوس‌های دشمن به ارتش شما نفوذ کرده باشند و پیام شروع یا توقف حمله را زودتر از زمان تعیین شده به تعدادی از فرماندهان شما برسانند چه اتفاقی خواهد افتاد؟ در چنین شرایطی ممکن است تمام نقشه‌های شما نقش بر آب شود.

حال بیاید این مثال را به حوزهٔ علوم کامپیوتر ببریم؛ چگونه می‌توان بدون وجود یک هماهنگ‌کنندهٔ مرکزی میان افرادی که در مسافت‌های طولانی از یکدیگر قرار دارند اجماع برقرار کرد؟

این مانع بزرگی بود که دستیابی به پول نقد دیجیتال غیرمتمرکز را برای چندین دهه ناممکن کرده بود. اگر طرفین معامله نمی‌توانستند روی صحت دفتر حسابداری با یکدیگر توافق داشته باشند، از کجا می‌توانستند تراکنش‌های واقعی و معتبر را تشخیص دهند؟ در چنین شرایطی سیستم هم نمی‌تواند از دو بار خرج شدن یک پول جلوگیری کند. در نتیجه تمام نمونه‌های اولیه پول‌های دیجیتالی به یک فرد یا نهاد مسئول نیاز داشتند.

1 ecash
2 The Byzantine Generals Problem

راه حل جادویی در قالب یک پست اسرارآمیز و در یک گروه ایمیلی[1] نمایان شد؛ جمعه ۳۱ اکتبر سال ۲۰۰۸، زمانی که ساتوشی ناکاموتو وایت‌پیپر بیت‌کوین را منتشر کرد. عنوان ایمیلْ «مقالهٔ پول نقد دیجیتالی همتا-به-همتای بیت‌کوین»[2] بود. نویسنده دربارهٔ آن اینطور نوشته بود: «روی پروژهٔ پول دیجیتالی کار کرده‌ام که کاملا همتا به همتا است؛ و نیازی به اعتماد به شخص ثالث ندارد.»

Bitcoin P2P e-cash paper

Satoshi Nakamoto satoshi at vistomail.com
Fri Oct 31 14:10:00 EDT 2008

- Previous message: Fw: SHA-3 lounge
- **Messages sorted by:** [date] [thread] [subject] [author]

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
 Double-spending is prevented with a peer-to-peer network.
 No mint or other trusted parties.
 Participants can be anonymous.
 New coins are made from Hashcash style proof-of-work.
 The proof-of-work for new coin generation also powers the
    network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as honest nodes control the most CPU power on the network, they can generate the longest chain and outpace any attackers. The network itself requires minimal structure. Messages are broadcasted on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Full paper at:
http://www.bitcoin.org/bitcoin.pdf

Satoshi Nakamoto

The Cryptography Mailing List
Unsubscribe by sending "unsubscribe cryptography" to majordomo at metzdowd.com

---

انتشار مقالهٔ معرفی بیت‌کوین توسط ساتوشی ناکاموتو. منبع.

1 Email list
2 Bitcoin P2P e-cash paper

ساتوشی ناکاموتو برای حل «مسألهٔ ژنرال‌های بیزانس» و ارائهٔ سیستم مالی دیجیتال بدون نیاز به یک مرجع، پیشنهاد داد دفتر جامع سیستم اقتصادی را در اختیار هزاران کاربر در سراسر جهان قرار دهیم. هرکدام از این کاربران یک نسخهٔ مستقل در اختیار دارند که شامل تاریخچه تراکنش‌ها است و با تراکنش‌های جدید به‌روز می‌شود. ساتوشی نام آن را در ابتدا «تایم‌چین»[1] گذاشت. اگر یکی از این افراد تلاش می‌کرد تا پولش را «دو بار خرج»[2] کند همه با خبر می‌شدند و جلوی انجام آن تراکنش را می‌گرفتند.

ساتوشی ناکاموتو با انتشار وایت‌پیپر بیت‌کوین توجه‌ها را به‌خود جلب کرد، سپس بازخوردهای نهایی را بررسی و چند ماه دیگر روی پروژه کار کرد و سرانجام اولین نسخهٔ نرم‌افزار بیت‌کوین در ۹ ژانویه ۲۰۰۹ منتشر شد.

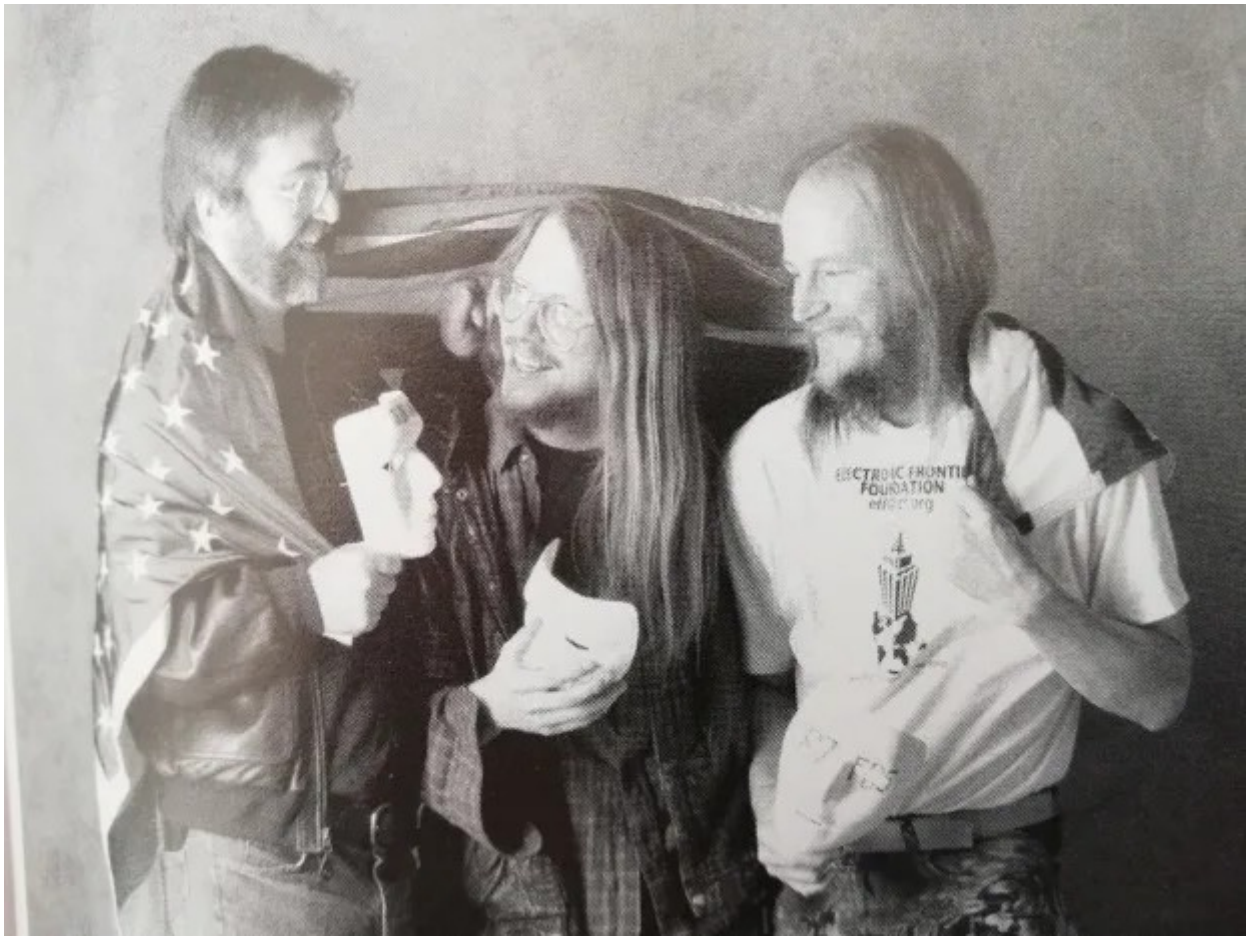
در زمان نگارش این مقاله هر واحد بیت کوین حدود ۵۵ هزار دلار ارزش دارد. حجم تراکنش‌های روزانه بازار بیت کوین از حجم GDP روزانه بعضی کشورها بیشتر، و ارزش بازار آن از مرز یک تریلیون دلار عبور کرده است. مخلوق ساتوشی ناکاموتو امروز توسط بیش از صد میلیون نفر و تقریبا تمام کشورهای چهار گوشهٔ جهان استفاده می‌شود. وال استریت، سیلیکون ولی و سیاستمدارهای ایالات متحده آمریکا بیت کوین را پذیرفته‌اند.

اما ساتوشی در آغازِ کار نیاز به کمک داشت و آدام بک اولین شخصی بود که ساتوشی برای دریافت کمکَ با او تماس گرفت.

1 timechain
2 double-spend

بخش اول – تولد سایفرپانک‌ها[1]

آدام بَک یک سایفرپانک بود؛ دانشجوی علوم کامپیوتری در دهه‌های ۸۰ و ۹۰ که می‌خواست از حقوق اولیهٔ انسان‌ها مانند حق برقراری ارتباط خصوصی با دیگران محافظت کند. فعالانی مثل بک می‌دانستند که فناوری‌هایی چون اینترنت قدرتی غیرقابل کنترل در اختیار دولت‌ها قرار می‌دهند. آن‌ها اعتقاد داشتند رمزنگاری بهترین دفاع شهروندان در مقابل این قدرت خواهد بود.



اولین اعضای گروه سایفرپانک: Tim May, Eric Hughes and John Gilmore

اوایل دههٔ ۹۰ دولت‌ها متوجه شدند گنجینه‌ای از اطلاعات و داده‌های شخصی شهروندان را به‌صورت دیجیتالی در اختیار دارند. این اطلاعات به دلایل متفاوتی ذخیره‌سازی شده بودند.

1 Cypherpunks

به عنوان نمونه سرویس‌دهنده‌های اینترنتی آدرس و شماره تلفن کاربران خود را به قصد ارسال صورت‌حساب‌های مالی ذخیره می‌کنند و اطلاعات جمع‌آوری شده را بدون نیاز به هیچ‌گونه حکم قانونی در اختیار ضابطین قضایی قرار می‌دهند.

دوران شنود و نظارت دیجیتالی [بر زندگی مردم عادی] با جمع‌آوری و تجزیه و تحلیل این نوع داده‌ها آغاز شد و دو دهۀ بعد به برنامه‌های پیچیده و مغایر با قانون اساسی ایالات متحدۀ آمریکا در جنگ با تروریسم منجر شد؛ برنامه‌هایی که سوت‌زنِ[1] مشهور آژانس امنیت ملی آمریکا یعنی اداورد اسنودن[2] از آن پرده برداشت.

دیود برنهام[3] روزنامه‌نگار نیویورک تایمز در کتاب «تولد دولتِ مبتنی بر کامپیوتر»[4] که در سال ۱۹۸۳ منتشر شد، هشدار داد که اتوماسیون سیستم‌های بین‌المللی حتما به شروع دوران تازه جاسوسی از شهروندان عادی منجر خواهد شد. او از شهروندان خواست در مقابل چنین وضعیتی به مطالبۀ حمایت‌های قانونی بپردازند. در مقابل این طرز فکر، سایفرپانک‌ها فکر می‌کردند راه حلْ لابی با دولت و تلاش برای ایجاد سیاست‌های بهتر نیست؛ راه حل این مشکل استفاده از فناوری‌های پیشرفته‌ای است که دولت نتواند در مقابل آن کاری از پیش ببرد.

سایفرپانک‌ها از رمزنگاری برای ایجاد تغییرات اجتماعی استفاده کردند. ایدۀ آن‌ها بسیار ساده بود: مخالفان سیاست‌های جاری از سراسر دنیا باید با اسم مستعار خود برای ایجاد تغییرات در راه آزادی و به چالش کشیدن قدرت با یکدیگر همکاری کنند. شعار آن‌ها «سایفرپانک‌ها کد می‌نویسند[5]» بود.

1 whistleblower
2 Edward Snowden
3 David Burnham
4 The Rise Of The Computer State
5 Cypherpunks write code

رمزنگاری که تا پیش از آن در انحصار ارتش‌ها و آژانس‌های جاسوسی نظامی قرار داشت در دهۀ ۷۰ میلادی به موضوعی عمومی تبدیل شد. افرادی مثل رالف مرکل[۶]، وایتفیلد دیفی[۷] و مارتین هلمان[۸] این علم را عمومی کردند. این سه نفر که در دانشگاه استنفورد همکار بودند در ماه مه ۱۹۷۵ کشف کردند که دو نفر چطور می‌توانند بدون نیاز به شخص ثالث، به‌صورت آنلاین باهم در ارتباط باشند و پیام‌های خصوصی برای یکدیگر ارسال کنند.

یک سال بعد دیفی و هلمان مقاله «مسیری جدید در رمزنگاری[۴]» را منتشر کردند. این مقاله حاصل تلاش‌های بسیار مهم این دو نفر در راه ایجاد سیستم پیام‌رسان ضد جاسوسی بود. این مقاله توضیح می‌داد که چطور شهروندان عادی می‌توانند پیام‌های دیجیتال خود را رمزنگاری و ارسال کنند؛ بدون اینکه ترسی از دخالت و نظارت دولت‌ها یا سازمان‌های بزرگی داشته باشند که همیشه می‌خواهند در زندگی آن‌ها جاسوسی کنند.

این مقاله به زبان ساده می‌گوید آوا یک کلید عمومی دارد که با دیگران به اشتراک گذاشته است. اگر بابک می‌خواهد برای آوا یک پیام خصوصی ارسال کند، می‌تواند از این کلید خصوصی برای رمزنگاری پیام خود استفاده کند. فقط آوا می‌تواند این پیام را رمزگشایی کند و بخواند. اگر کامران به‌عنوان نفر سوم حاضر در شبکه کلید خصوصی بابک را در اختیار نداشته باشد، نمی‌تواند محتوای آن را ببیند. همین مکانیزمِ ساده توازن قدرت اطلاعاتی افراد در مقابل دولت‌ها را تغییر داد.

دولت آمریکا پس از اینکه مقاله دیفی و هلمان منتشر شد تلاش کرد از گسترش این ایده جلوگیری کند. آن‌ها از طریق آژانس امنیت ملی آمریکا نامه‌ای به یک کنفرانس رمزنگاری نوشتند و هشدار دادند شرکت در چنین کنفرانس‌هایی ممکن است غیرقانونی

6 Ralph Merkle
7 Whitfield Diffie
8 Martin Hellman
4 New Directions In Cryptography

باشد. دولت فدرال البته زمانی که نسخه‌های چاپی این مقاله در سراسر آمریکا پخش شد و همه از محتوای آن با خبر شدند، مجبور به عقب‌نشینی شد.

در سال ۱۹۷۷ دیفی، هلمان، و مرکل «رمزنگاریِ کلید عمومی»[1] را با شمارهٔ ۴۲۰۰۷۷۰ ثبت اختراع کردند. این اختراع در حقیقت پایهٔ سیستم‌های پیام‌رسان و ایمیل محرمانه‌ای مثل PGP و اپلیکیشن‌های موبایلی مثل سیگنال بودند که ما امروزه از آن‌ها استفاده می‌کنیم.

دورهٔ کنترل دولت‌ها بر علم رمزنگاری در حال پایان بود و انقلاب سایفرپانک داشت شروع می‌شد.

بخش دوم – لیست

کلمه «سایفرپانک» تا سال ۲۰۰۶ جایی در فرهنگ لغات آکسفورد نداشت اما جامعهٔ سایفرپانک‌ها خیلی پیش از این تاریخ فعالیت خود را آغاز کرده بودند.

سال ۱۹۹۲ و یک سال بعد از ارائهٔ عمومی وبِ جهانی[2]، جان گیلمور[3] یکی از اولین مهندسان شرکت سان میکروسیستم به همراه اَریک هیوز[4] فعال حریم خصوصی، و تیموتی مِی[5] مهندس سابق اینتل در سانفرانسیسکو شروع به ملاقات کردند. آن‌ها می‌خواستند شرایط استفاده از رمزنگاری برای رسیدن به آزادی‌های اجتماعی را بررسی کنند. در همان سال آن‌ها «لیست ایمیلی سایفرپانک‌ها» یا به اختصار «لیست[6]» را منتشر کردند؛ جایی

1 public-key cryptography
2 World Wide Web
3 John Gilmore
4 Eric Hughes
5 Timothy May
6 The List

که ایده‌های پشت بیت‌کوین توسعه یافت و سرانجام ۱۶ سال بعد توسط ناکاموتو منتشر شد.

```
From: Eric Hughes <hughesNsoda.berkeley.edu>
Date: Mon, 21 Sep 92 22:47:51 PDT
To: cypherpunks@toad.com
Subject: No Subject
Message-ID: <9209220543.AA25094@soda.berkeley.edu>
MIME-Version: 1.0
Content-Type: text/plain


Welcome to the cypherpunks mailing list.

We have a real mailing list now, and not just a mail alias on my
account.  Thanks to John Gilmore for space on hoptoad and Hugh Daniel
for setting things up.

Mail to the list members at

        cypherpunks@toad.com

Request additions or deletions, talk to the list maintainer (me, Eric
Hughes) at

        cypherpunks-request@toad.com

Tell your friends about the list and have them join if they wish, and
have them do the same, but please do not post the list address yet.
We'd like to have a core group working before we advertise to avoid
diffusion of interest at the outset.

----------------------

ANNOUNCEMENT

Second Meeting -- October 10, 1992


The second meeting will be held at the new Cygnus offices.  Exact
address and directions to follow.

We do not have an exact agenda yet, but one should be arriving in the
next few days.  Please mark you calendars now and start telling your
friends.

For this meeting and until further announced, we are using a
transitive trust system for invitations.  Invite anybody you want and
let them invite anybody they want and so on.

The crypto-anarchy game we tried out at the first meeting was as good
a success as we could have hoped for from an untested idea.  The game
seems useful and fun enough to warrant continued play and play
testing, so we'll be playing again at this and future meetings.

We observed several interesting emergent behaviors in the first
session, including resellers and reputation behaviors.  We'll play a
two hour session this time and discuss it afterwards.


Eric
```

اعلام شروع به کار لیست از طرف اریک هیوز. منبع.

سایفرپانک‌هایی مثل مِی در این «لیست» دربارهٔ نقش رسانه‌های چاپی و اثرات دسترسی آزاد به اطلاعات روی از بین رفتن سیستم‌های پادشاهی اواخر قرون وسطی مطالبی منتشر می‌کردند. سایفرپانک‌ها در این لیست دربارهٔ تاثیر اینترنت آزاد و رمزنگاری روی دموکراتیزه کردن فناوری‌های مرتبط با حریم خصوصی و برهم زدن امپراطوری جاسوسی بین‌المللی از شهروندان عادی بحث و تبادل نظر کردند.

تحصیلات آدام بک هم مثل بیشتر سایفرپانک‌ها در حوزهٔ علوم کامپیوتر بود. اما خوشبختانه او قبل از وارد شدن به حوزهٔ علوم کامپیوتر و در سنین ۱۶ تا ۱۸ سالگی، در حوزهٔ اقتصاد به تحصیل علم پرداخت. او پس از اتمام دورهٔ علوم کامپیوتر در حوزهٔ سیستم‌های توزیع شده به درجهٔ دکتری رسید. اگر فقط یک نفر علم و آمادگی تبدیل شدن به یک دانشمند در حوزهٔ بیت‌کوین را داشت، آن فرد کسی جز آدام بک نبود.

بک در اوایل دههٔ ۹۰ میلادی و زمانی که در لندن علوم کامپیوتر می‌خواند، متوجه شد یکی از دوستانش روی پروژه‌ای کار می‌کند که هدفش افزایش سرعت کامپیوترها در پردازش الگوریتم‌های رمزنگاری است. بک از طریق دوست خود با شیوهٔ رمزنگاری مبتنی بر کلید عمومی که ۱۵ سال پیشتر توسط دیفی و هلمن اختراع شده بود آشنا شد.

بک معتقد بود این شیوه، تغییری تاریخی در روابط بین دولت‌ها و شهروندان ایجاد کرده است. با این شیوه شهروندان می‌توانند طوری که هیچ دولتی توانایی رمزگشایی آن را نداشته باشد به صورت آنلاین با یکدیگر ارتباط برقرار کنند. او می‌خواست اطلاعات بیشتری به دست آورد و این کنجکاوی در نهایت او را با «لیست» آشنا کرد.

بک در اواسط دههٔ ۱۹۹۰ میلادی یکی از فعال‌ترین سایفرپانک‌های «لیست» بود. کاربران این شبکه در زمان اوج فعالیت‌های آن روزانه ده‌ها پیام رد و بدل می‌کردند و بَک که به بحث و گفتگو در مورد تکنولوژی‌های پیشرفتهٔ آن دوران بسیار علاقه‌مند بود، یکی از فعال‌ترین اعضای این گروه بود.

بَک با ایدهٔ سایفرپانک‌ها که می‌خواستند با شیوه‌ای صلح‌آمیز سیستمی غیر قابل مهار بسازند و از این طریق موجب تغییر در جامعه شوند، بسیار موافق بود. سال ۱۹۹۳ هیوز رسالهٔ کوتاه اما بسیار مهمی با عنوان «مانیفست یک سایفرپانک»[1] نوشت:

«یکی از ضرورت‌های موردنیاز برای رسیدن به یک جامعهٔ آزاد در دورهٔ دیجیتال، حریم خصوصی است. حریم خصوصی به‌معنی محرمانگی نیست. یک امر خصوصی، چیزی است که صاحب آن [ممکن است آن را با افرادی که خودش صلاح می‌داند به اشتراک بگذارد، ولی] دوست ندارد همهٔ دنیا از آن خبردار شوند، اما یک امر محرمانه چیزی است که صاحب آن می‌خواهد از تک تکِ افراد جهان پنهان باشد. حریم خصوصی یعنی توان فاش کردن امور به‌صورت انتخابی...

«... ما نمی‌توانیم از دولت‌ها، سازمان‌ها یا تشکل‌های بسیار بزرگ و بی‌رحم انتظار داشته باشیم حریم شخصی ما را به منافع خود ترجیح دهند. ما اگر خواهان حریم خصوصی هستیم باید خودمان از آن دفاع کنیم. ما باید دور هم جمع شویم و سیستم‌هایی بسازیم که به ما امکان انجام تراکنش‌های ناشناس را بدهد. بشر در طول قرون گذشته همواره با استفاده از روش‌هایی مانند پچ‌پچ، فعالیت در تاریکی، ارسال نامه داخل پاکت، فعالیت پشت درهای بسته، روش‌های خاص برای دست دادن، و پیک‌های مورد اعتماد از حریم خصوصی خود دفاع کرده است. فناوری‌های الکترونیکی موجود برخلاف تکنولوژی‌های قدیمی امکان ایجاد ابزارهای مؤثری را به‌منظور حفظ حریم خصوصی فراهم می‌کنند.

«ما سایفرپانک‌ها خود را وقف ساخت سیستم‌های ناشناس کرده‌ایم. ما با استفاده از رمزنگاری، سیستم‌های ارسال‌کنندهٔ ایمیل به‌صورت ناشناس، امضاهای دیجیتال و پول الکترونیکی از حریم خصوصی خود دفاع می‌کنیم.

1 A Cypherpunk’s Manifesto

«سایفرپانک‌ها کُد می‌نویسند. می‌دانیم که یک نفر باید نرم‌افزاری بنویسد که بتواند از حریم خصوصی افراد دفاع کند و با توجه به اینکه برای رسیدن به حریم خصوصی، همهٔ افراد باید از آن برخوردار باشند به کدنویسی ادامه خواهیم داد... کدهای ما برای استفادهٔ عموم در سراسر جهان رایگان است. برای ما تایید شدن نرم‌افزارهایمان اهمیت زیادی ندارد چرا که می‌دانیم این نرم‌افزارها از بین نخواهند رفت؛ می‌دانیم که نمی‌توان سیستمی که در گسترهٔ جهان به‌کار گرفته می‌شود را متوقف کرد.»

بَک معتقد بود چنین تفکراتی قادر به ایجاد تغییر در جامعه خواهد بود. البته که با رأی‌گیری و لابی‌های پشت پرده نیز می‌توان تغییر ایجاد کرد اما چنین تغییراتی کُند، و تحت تاثیر سیاست‌های دولت خواهد بود.

راه جایگزینی که بَک آن را انتخاب کرده بود استراتژی بسیار بلندپروازانه‌ای بود؛ تغییر از راه به‌کارگیری سیستمی که برای استفاده از آن نیاز به اجازه از هیچ شخص یا نهادی نبود. او می‌دانست که این سیستم برای ایجاد تغییر لازم است.

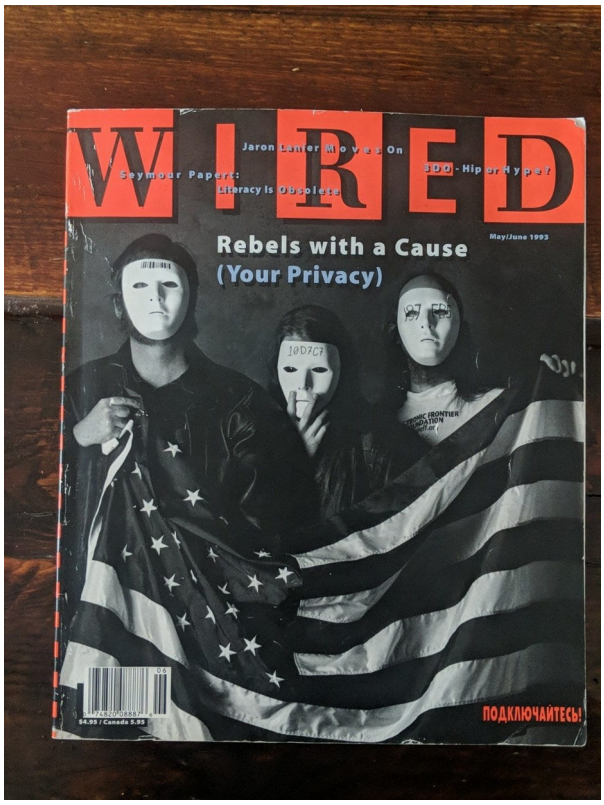
بخش سوم - جنگ با رمزنگاری

دشمنان اصلی سایفرپانک‌ها، دولت‌هایی بودند که نمی‌خواستند شهروندان از رمزنگاری استفاده کنند. بَک و دوستانش معتقد بودند حفظ حریم خصوصی یکی از حقوق اولیهٔ انسان‌ها است. در مقابلْ دولت‌های مرکزی معتقد بودند رمزنگاری به شهروندان اجازه خواهد داد کدهایی بنویسند که منجر به رهایی آن‌ها از کنترل و نظارت دولت‌ها شود.

قانون‌گذاران به قوانین قدیمیِ ارتش که رمزنگاری را به‌عنوان بخشی از ابزارهای جنگی در کنار هواپیماهای جنگنده معرفی می‌کند، استناد می‌کردند. آن‌ها با استناد به همین قوانین

تلاش می‌کردند رمزنگاری را برای شهروندان عادی غیرقانونی اعلام کنند تا با این کار از گسترش آن‌ها در دیگر نقاط جهان جلوگیری کنند. هدف دولت‌ها این بود که مردم را از استفاده از فناوری‌های مرتبط با حریم خصوصی بترسانند. این مناقشات با عنوان «جنگ با رمزنگاری»[1] شناخته می‌شوند و بَک در این جنگ یکی از سربازان خط مقدم بود.

بک می‌دانست نتیجهٔ شکست در چنین جنگی از بین رفتن بسیاری از موقعیت‌های شغلی بالقوه و همینطور در دسترس بودن اطلاعات حساس و مهم به‌صورت رمزنگاری نشده خواهد بود. دولت کلینتون نگاهی به آینده نداشت و آن‌ها فقط چند قدمی خود را می‌دیدند. مهم‌ترین هدف‌شان فیل زیمرمن[2] دانشمند علوم کامپیوتر بود. زیمرمن در سال ۹۱ میلادی اولین سیستم پیام‌رسان غیرقابل ردگیری که عموم مردم می‌توانستند از آن استفاده کنند را با نام Pretty Good Privacy یا به اختصار PGP منتشر کرده بود.



معرفی سایفرپانک‌ها در مقاله‌ای مفصل در مجلهٔ WIRED - اواسط دههٔ ۹۰ میلادی

1 Crypto Wars
2 Phil Zimmerman

PGP راه آسانی بود که دو نفر می‌توانستند برای برقراری یک ارتباط خصوصی بر روی بستر وب جهانی و با استفاده از کامپیوترهای شخصی از آن استفاده کنند. این ابزار به‌کارگیری از رمزنگاری را برای میلیون‌ها نفر در سراسر جهان امکان‌پذیر می‌کرد و به کنترل چند ده سالهٔ دولت‌ها بر روی ارتباطات خصوصی افراد پایان می‌داد.

زیمرمن به‌عنوان اصلی‌ترین فرد این پروژه هدف حمله‌های سنگین دولت‌ها و سازمان‌های بزرگ قرار داشت. در سال ۱۹۷۷ سه دانشمند موسسه فناوری ماساچوست[1] به نام‌های ریوست[2]، شمیر[3] و آدلمن[4]، ایده‌های دیفی و هلمان را در قالب الگوریتمی با نام RSA پیاده‌سازی کردند. موسسهٔ فناوری ماساچوست بعدها این اختراع را به نام جیم بیدزوس[5] و شرکت او به نام RSA Data Security ثبت اختراع کرد.

سایفرپانک‌ها با کنترل چنین ابزار مهمی توسط یک نهاد به‌هیچ وجه موافق نبودند و معتقد بودند این شرکت پاشنهٔ آشیل این تکنولوژی خواهد بود اما همچنان مسائل مربوط به مجوز بهره‌برداری و ترس از تعقیب قانونی ناشی از به‌کارگیریِ تکنولوژی‌های ثبت اختراع شده موجب شد که آنها در طول دههٔ ۸۰ میلادی نرم‌افزارهای جدیدی بر اساس این تکنولوژی خلق نکنند.

ابتدا زیمرمن از بیدزوس خواست به او اجازهٔ استفاده از نرم‌افزار را بدهد اما این درخواست رد شد. زیمرمن در مقابل PGP را به‌عنوان یک «نرم‌افزار رایگانِ نامتعارف[6]» و از طریق فلاپی دیسک‌ها و تالارهای گفتگوی آنلاین منتشر کرد. هال فینی[7] یک سایفرپانک جوان (که بعدها نقش بسیار بزرگی در داستان بیت کوین ایفا کرد) به زیمرمن ملحق شد تا پروژه را پیش ببرند. در سال ۱۹۹۴ یک مقاله در مجلهٔ WIRED چاپ، و در آن از دلیری

1 Massachusetts Institute of Technology (MIT)
2 Rivest
3 Shamir
4 Adelman
5 Bidzos
6 guerilla freeware
7 Hal Finney

زیمرمن به نیکی یاد شد و از انتشار PGP به‌عنوان «ضربه‌ای پیش‌گیرانه به یک آیندهٔ اورولی[1]» نام برده شد.

بیدزوس زیمرمن را دزد خطاب کرد و کارزاری برای جلوگیری از انتشار PGP به راه انداخت. زیمرمن در نهایت از کمک کریستوفر آلن[2] و تیمش برخوردار شد و نسخهٔ جدیدی از نرم‌افزاز PGP را با کمک بخشی از کدهای رایگان پروژهٔ بیدزوس منتشر کرد. او با این کار خطر تهدیدهای قانونی را از خود دور کرد.

اما دولت فدرال برای زیمرمن پرونده‌ای باز کرد و تحقیقات دربارهٔ فروش تسلیحات نظامی توسط او را بر اساس قانون منع صادرات سلاح شروع کرد. زیمرمن برای دفاع از خود اعلام کرد او کدهای متن‌باز را منتشر کرده و این کار بر اساس متمم اول قانون اساسی آمریکا حق قانونی اوست.

دولت کلینتون در آن زمان اعلام کرد شهروندان اجازه استفاده از رمزنگاری را ندارند. آن‌ها می‌خواستند از راه‌های قانونی شرکت‌های بزرگ را ملزم به به‌کارگیری «چیپ‌های شنود»[3] و ایجاد راه‌های مخفی[4] برای دولت کنند و از این راه به تمام پیام‌هایی که کاربران رمزنگاری می‌کنند دسترسی داشته باشند. کاخ سفید با حمایت نماینده‌های کنگره منجمله جو بایدن[5] اینطور ادعا کرد کرد که رمزنگاری باعث قدرت گرفتن خلافکارها، متعرضین به کودکان، و تروریست‌ها خواهد شد.

سایفرپانک‌ها در حمایت از زیمرمن که به یک ستاره تبدیل شده بود گرد هم آمدند. آن‌ها ادعا کردند قوانین ضد رمزنگاری آمریکا خلاف حق آزادی بیان است. فعالان آزادی‌خواه، سورس کُدهای PGP را در قالب کتاب چاپ، و به کشورهای دیگر پُست می‌کردند. زیمرمن و دیگران به این نتیجه رسیده بودند که با چاپ کدهای این نرم‌افزار بر

1 orwellian
2 Christopher Allen
3 clipper chips
4 backdoor
5 Joe Biden

روی کاغذ و در قالب کتاب، قوانین منع صادرات تسلیحات نظامی در مورد آن‌ها صدق نمی‌کند. کسانی که کد را در قالب کتاب دریافت می‌کردند، قادر بودند کُد را دوباره از راه اسکن کتاب بازسازی و اجرا کنند تا ثابت کنند کسی جلودارشان نیست.

بَک مجموعه‌ای از کدهای مختصری را نوشت که هر برنامه‌نویسی می‌توانست با به‌کارگیری آن‌ها ابزاری برای حفظ حریم خصوصی خود بسازد. بعضی از فعالان این حوزه بخش‌هایی از این کدها را روی بدن خود خالکوبی کردند. بَک تی‌شرت‌هایی به بازار عرضه کرد که روی آن بخش‌هایی از کدهای برنامه و در پشت آن نیز منشور حقوق شهروندی ایالات متحده چاپ شده بود که روی آن مهر «بی‌اعتبار» زده شده بود.

تی‌شرتی که آدام بک می‌فروخت. منبع.

فعالان این حوزه نسخه‌ای از کتاب را برای مدیران بخش قوانین نظامی آمریکا ارسال کردند و از آن‌ها پرسیدند که آیا ارسال این کتاب به خارج از کشور قانونی است یا نه. مدیران این بخش هرگز پاسخی به این پرسش ندادند. سایفرپانک‌ها حدس می‌زدند که کاخ سفید هرگز چاپ و نشر یک کتاب را ممنوع نخواهد کرد؛ حدس آن‌ها کاملا درست بود.

وزارت دادگستری آمریکا در سال ۱۹۹۶ شکایت خود از زیمرمن را پس گرفت. فشار برای به‌کارگیری چیپ‌های شنود نیز از روی شرکت‌ها برداشته شد. قاضی فدرال اعلام کرد رمزنگاری ذیل متمم اول قانون اساسی آمریکا یک حق طبیعی به‌شمار می‌رود. قوانین ضد رمزنگاری برداشته شدند و رمزنگاری پیام‌رسان‌ها به هستهٔ اصلی اینترنت آزاد تبدیل شد. PGP به پرمخاطب‌ترین سرویس ایمیل رمزنگاری شده در سراسر جهان تبدیل شد.

امروزه شرکت‌های بزرگ شامل آمازون، واتس‌اپ و فیسبوک از رمزنگاری برای امن کردن پرداخت‌ها و پیام‌های کاربران خود استفاده می‌کنند. میلیاردها نفر در جهان از مزایای آن بهره‌مند شدند. کُد در جهان تغییر به‌وجود آورد.

آدام بَک شکسته نفسی می‌کند و همیشه دربارهٔ نقش فعالیت‌های خود در ایجاد چنین تغییرات بزرگی با تردید صحبت می‌کند. اما بررسی تاریخ نشان می‌دهد جنگی که سایفرپانک‌ها به راه انداختند یکی از اصلی‌ترین دلایل شکست دولت آمریکا در جنگ با رمزنگاری بود. مقامات سیاسی تلاش کردند تا مانع از رشد و گسترش کُد شوند و شکست خوردند.

پذیرش چنین نقشی احتمالا ۱۵ سال بعد برای بَک راحت‌تر بود؛ زمانی که در سال ۲۰۰۸ اولین ایمیل را از ساتوشی ناکاموتو دریافت کرد.

بخش چهارم - از دیجی‌کَش تا بیت‌گُلد

استیون لِوی[1] تاریخ‌دان حوزهٔ کامپیوتر در سال ۱۹۹۳ گفته بود مهم‌ترین ابزار علم رمزنگاری «پول ناشناس دیجیتالی» خواهد بود. در واقع پس از پیروزی بزرگ و به‌دست آوردن حق برقراری قانونیِ ارتباط رمزنگاری شده و دور از نظارت دولت‌ها، چالش بعدی سایفرپانک‌ها پدید آوردنِ پول نقد دیجیتال بود.

برخی از سایفرپانک‌ها کریپتو-آنارشیست[2] و نسبت به سیستم‌های دموکراتیکِ امروزی به‌شدت بدبین بودند. گروهی دیگر همچنان امید داشتند که می‌توان با ایجاد تغییراتی در سیستم‌های دموکراتیک موجود از حقوق شهروندان حفاظت کرد. اما اغلبِ افراد صرف‌نظر از این اختلاف‌نظرها معتقد بودند هدف غایی جنبش سایفرپانک‌ها ساختنِ پول نقد دیجیتال است.

در دهه‌های ۱۹۸۰ و ۱۹۹۰ میلادی از نظر فرهنگی و فنی قدم‌های بزرگی در راه رسیدن به پول دیجیتال برداشته شد. در حوزهٔ فرهنگی نویسنده‌های علمی-تخیلی مثل نیل استفنسن[3] رویاپردازی‌های دانشمندان علوم کامپیوتر را دربارهٔ آینده‌ای که در آن پول فیزیکی حذف شده و انواع مختلفی از پول‌های دیجیتالی مورد استفاده مردم قرار می‌گیرد به‌نمایش درآوردند. در دوره‌ای که استفاده از کارت‌های اعتباری و پرداخت‌های دیجیتالی در حال افزایش بود، معامله با پول نقد که در آن فروشنده اطلاعاتی در مورد مشتری نگهداری نمی‌کرد و قادر به فروش این اطلاعات به دیگران نبود، یک نوع نوستالژی به حساب می‌آمد.

1 Steven Levy
2 cypherpunks
3 Neal Stephenson

در حوزهٔ فنی، دیوید چام[1] محقق رمزنگاری دانشگاه برکلی کالیفرنیا ایدهٔ قدرتمند «رمزنگاری کلید عمومی» را به خدمت گرفت و تلاش کرد تا آن را بر روی پول اعمال کند.

دیوید چام مخترع eCash

اوایل دههٔ ۸۰ میلادی دیوید چام نوعی از امضاهای دیجیتال را اختراع کرد که به آن‌ها blind signatures گفته می‌شد. این اختراع کلیدی قدم مهمی در راه امکان اثبات مالکیت بر یک دادهٔ دیجیتالی، بدون نیاز به ارائه مدارکی دال بر مالکیت بود. او در سال ۱۹۸۵ مقالهٔ «امنیتی که نیاز به شناسایی ندارد: سیستمی برای انجام تراکنش‌ها که منجر به منسوخ شدن برادر بزرگ[2] می‌شود» را منتشر کرد. مقاله‌ای پیشرو که توضیح می‌داد چگونه می‌توان با استفاده از پرداخت‌های دیجیتالیِ خصوصی، رشد پایش و نظارت دولت‌ها را کندتر کرد.

1 David Chaum
2 Big Brother

دیوید چام سال ۱۹۸۹ همراه دوستانش به آمستردام هلند نقل مکان کردند و در آنجا ایده‌هایشان را عملی، و شرکت دیجی‌کش[1] را راه انداختند. این شرکت کاربران را قادر می‌ساخت تا یورو و دلارهای خود را به توکن‌های پول دیجیتال تبدیل کنند. دارایی‌های موجود نزد بانک‌ها در این شرکت می‌توانست به «ای‌کش[2]» تبدیل و خارج از سیستم بانکداری میان کاربران جابجا شود. کاربران همچنین می‌توانستند این پول جدید خود را روی کامپیوترهای شخصی خود ذخیره، یا آن‌ها را دوباره نقد کنند. رمزنگاریِ بسیار موثری که در نرم‌افزار این سیستم پیاده‌سازی شده بود ردگیری مسیر نقل و انتقال پول از جانب دولت و نهادهای دیگر را غیرممکن می‌کرد.

سال ۱۹۹۴ و در روزهای اوج دیجی‌کش چام دربارهٔ این پروژه صحبت کرد و گفت هدف این بود که «سطح سیستم پرداخت موجود را به سطح مورد انتظار در قرن بعد برسانیم و در جریان رسیدن به این هدف می‌خواهیم سیستم‌های نظارتی آخرالزمانی برادر بزرگ را در هم بشکنیم و آن را با چیزی جایگزین کنیم که سهولت تراکنش‌های الکترونیکی را با پرداخت‌های نقدی ناشناس در هم می‌آمیزد.»

بَک می‌گوید سایفرپانک‌ها نسبت به پروژهٔ ای‌کش هیجان‌زده بودند. این سیستم اجازه ردگیری ارسال‌کنندگان و گیرندگان و همچنین مقادیر جابجا شده را به ناظران بیرونی نمی‌داد. همچنین با توجه به اینکه دارندهٔ این توکن‌ها به‌عنوان صاحب آن‌ها شناخته می‌شد، کاملاً شبیه به پول نقد بودند.

دیدگاه شخصی چام کاملاً با سایفرپانک‌ها هم‌خوانی داشت. او سال ۱۹۹۲ در مقاله‌ای نوشت: «بشریت در نقطهٔ تصمیم‌گیری است و باید میان مسیری که زندگی خصوصی افراد تحت نظارت و کنترل بی‌سابقه‌ای قرار می‌گیرد، یا راهی که در آن میان شهروندان و سازمان‌ها توازن امنی برقرار است یکی را انتخاب کند و این انتخاب شاکلهٔ جامعهٔ بشری در قرن بعد را شکل خواهد داد.»

1 DigiCash
2 eCash

با این حال شرکت دیجی‌کش موفق به جذب سرمایهٔ موردنیاز نشد و یک دهه بعد از تاسیس اعلام ورشکستگی کرد. این اتفاق درس بزرگی برای بَک و سایرین داشت: پول دیجیتال باید کاملاً غیرمتمرکز باشد.

بَک شخصاً برای ایجاد حریم خصوصی در جامعه تمام تلاش خود را کرده بود. او زمانی سرویسی به نام mixmaster اجرا می‌کرد که به افراد عادی کمک می‌کرد ارتباط‌های شخصی خود را از چشم دیگران دور نگه دارند. در این سرویس او ایمیل‌های کاربران را دریافت می‌کرد و با استفاده از روش‌های غیرقابل ردگیری، آن‌ها را برای مخاطبان مورد نظرشان ارسال می‌کرد. او سرور مورد نیاز را به قصد ناشناس ماندن از دوستی در سوئیس اجاره کرد و برای پرداخت هزینهٔ آن از لندن برای او پول نقد پُست می‌کرد. در نهایت پلیس فدرال سوئیس سراغ دوست بَک رفت و بَک نیز فردای آن روز سرویس خود را بالاجبار متوقف کرد. اما رؤیای خلق پول دیجیتال همیشه در پس ذهن او قرار داشت.

یک پول دیجیتال متمرکز ممکن است از سوی نهادهای تنظیم‌گر متوقف شود، یا مانند شرکت دیجی‌کَش ورشکسته شود. اما بزرگترین آسیب‌پذیری آن، ساز و کار خلق پول توسط یک نهاد ثالثِ مورد اعتماد است.

در تاریخ ۲۸ مارس سال ۱۹۹۷ میلادی، بَک بعد از سال‌ها برنامه‌ریزی و تحقیق موفق به اختراع و معرفی هَش‌کَش[1] شد. هَش‌کَش ایده‌ای برای مقابله با هرزنگاری[2] بود که بعدها ساتوشی ناکاموتو در وایت‌پیپر بیت‌کوین به آن ارجاع داد و یکی از ایده‌های زیربنایی در حوزهٔ استخراج بیت‌کوین است. هَش‌کَش ایدهٔ «اثباتِ کار»[3] را در حوزهٔ مالی کارآمد می‌کرد و پولی پدید می‌آورد که برای خلق آن می‌بایست انرژی صرف شود، پس تولید آن منصفانه‌تر و سخت‌تر است.

1 Hashcash
2 Spam
3 Proof of Work

دولت‌ها در طول تاریخ همواره از قدرت مطلقهٔ خود برای خلق پول سوءاستفاده کرده‌اند. از نمونه‌های دلخراشِ آن می‌توان به رُم باستان، ویمارِ آلمان، مجارستانِ شوروی، حوزهٔ بالکان در سال ۱۹۹۰، زیمبابوهٔ موگابه، و ۱.۳ میلیارد نفریِ که امروزه زیر فشار تورم‌های دو رقمی و سه‌رقمی و حتی چهار رقمی در چهار گوشهٔ دنیا از سودان تا ونزوئلا زندگی می‌کنند اشاره کرد.

در سال ۱۹۹۸، رابرت هتینگا[1] سایفرپانک مشهور در مقاله‌ای مرتبط با این موضوع، به این نکته اشاره کرد که با ظهور دارایی‌های دیجیتالِ واقعاً غیرمتمرکز اقتصاد دیگر دستاویزِ سیاستمداران نخواهد بود. او معتقد بود دیگر دولت‌ها نخواهند توانست با یک کلیک، حجم چشم‌گیری از پول نقد را روانهٔ بازار کنند و تورم‌های چندین رقمی بسازند.

یکی از نقاط ضعف هَش‌کَش این بود که اگر بر اساس قابلیت‌های ضد هرزنگاریِ آن یک پول طراحی و ساخته می‌شد، کاربرانی که کامپیوترهای سریع‌تری داشتند قادر به خلق پول بیشتر و در نتیجه ایجاد تورم‌های بالا بودند. یک دهه بعد ساتوشی ناکاموتو این مشکل را با اختراعی بسیار کلیدی حل کرد. او الگوریتم سختی[2] شبکه را طراحی کرد که هر دو هفته یک بار براساس حجم توان هش ماینرها، استخراج بیت‌کوین را برای آن‌ها سخت‌تر یا ساده‌تر می‌کند.

وی دای[3] مهندس کامپیوتر در سال ۱۹۹۸ ایدهٔ مشهور خود با نام بی-مانی[4] را به دنیا معرفی کرد. این مفهوم یک «سیستم مالی غیرمتمرکز و غیرقابل شناسایی» بود و «روشی ارائه می‌کرد که گروهی از افراد با نام مستعار بتوانند بدون نیاز به کمک یک نهاد بیرونی قراردادهایی را اجرا، و برای یکدیگر پول ارسال کنند.»

1 Robert Hettinga
2 Difficulty algorithm
3 Wei Dai
4 b-money

دای از هش‌کشِ بَک الهام گرفته بود و الگوریتم اثبات کار را در طراحی بی-مانی به‌کار برده بود. با وجودی که این سیستم قابلیت‌های محدودی داشت و بعدتر معلوم شد پیاده‌سازیِ آن عملی نیست، دای یادداشت‌های بسیار زیادی از خود بجا گذاشت که بازگو کنندهٔ نظرات هیوز، بک و سایر سایفرپانک‌ها بود.

دای در فوریه ۱۹۹۵ ایمیلی به لیست سایفرپانک‌ها ارسال، و در آن خاطرنشان ساخت که حقوق دیجیتالی افراد در آینده از راه تکنولوژی به‌دست خواهد آمد، نه از راه قانونگذاری:

«در نهایت همهٔ دولت‌های جهان برای کاهش آزادی شهروندان و یافتن راهی‌هایی برای به‌دست آوردن کنترل هرچه بیشتر روی آن‌ها تلاش خواهند کرد و هیچ استثنایی هم وجود نخواهد داشت. بنابراین ما به جای تلاش برای منصرف ساختن دولت‌ها از این تلاش‌ها، تکنولوژی‌هایی را توسعه خواهیم داد که رسیدن به این هدف را برای آن‌ها ناممکن می‌سازد.

«تلاش برای تحت تاثیر قرار دادن دولت‌ها از روش‌هایی چون (لابی‌گری یا تبلیغات گسترده) فقط از این نظر اهمیت دارند که می‌توانند اجرای سیاست‌های سرکوب‌گرانهٔ دولت‌ها را به تأخیر اندازند و برای تکمیل فن‌آوری‌ها و مورد استفادهٔ عموم قرارگرفتن آن‌ها زمان بخرند.

«حتی اگر معتقدید این موضوع درست نیست، از این زاویه به آن نگاه کنید: اگر شما زمان مشخصی برای بهبود حریم خصوصی افراد (یا آزادی مدنی، کریپتو-آنارشیزم یا هر شکل دیگر آزادی) داشته باشید، ترجیح می‌دهید این زمان را برای فراگرفتن رمزنگاری و توسعهٔ ابزارهایی که از حریم خصوصی محافظت می‌کنند صرف کنید، یا دولت‌ها را قانع کنید که به حریم خصوصی شهروندان احترام بگذارند؟»

همان سال یعنی در سال ۱۹۹۸، یک رمزنگار آمریکایی با نام نیک زابو[1] ایدهٔ بیت گُلد[2] را عرضه کرد. زابو بیت گُلد را بر مبنای ایده‌های دیگر افراد گروه سایفرپانک‌ها طراحی، و پیشنهاد ایجاد یک ساختار مالی موازی را داده بود که ارزش توکن مورد استفاده در آن به‌خودیِ خود ارزشمند باشد و نسبت به دلار یا یورو سنجیده نشود. زابو که سابقهٔ کار در شرکتِ دیجی‌کَش را داشت، آسیب‌پذیری‌های سیستمی که مسئولیت خلق پول در آن بر عهدهٔ یک نهاد متمرکز است را می‌دانست. از طرف دیگر او معتقد بود که طلا یک دارایی ارزشمند است و می‌توان آن را در فضایِ دیجیتال بازتولید کرد.

بیت گُلد از این جهت بسیار مهم بود که سرانجام پای دارایی‌های فیزیکی را به فعالیت‌های سایفرپانک‌ها باز کرد. این ایده تلاش می‌کرد تا ویژگی «اثبات‌پذیریِ هزینه‌بر بودن فرآیند خلق[3]» طلا را دیجیتالی کند. به عنوان مثال یک گردنبند طلا ثابت می‌کند که صاحب آن یا وقت و منابع قابل توجهی را صرف کرده و طلا را از دل زمین بیرون آورده و به جواهر تبدیل کرده، یا پول زیادی برای خرید آن پرداخت کرده است. زابو می‌خواست این ویژگی اثبات‌پذیر بودن را به فضای آنلاین آورد. بیت گُلد هرگز پیاده‌سازی نشد، اما سایفرپانک‌ها از آن الهام گرفتند.

چند سال بعد دنیا شاهد ظهور تجارت الکترونیک، حباب دات-کام و تولد اَبَر شرکت‌های اینترنت امروز بود. دنیای آنلاین در این چند سال از شلوغی به مرز انفجار رسید. اما در این پنج سال هیچ‌گونه پیشرفتی در حوزهٔ پول نقد دیجیتال ایجاد نشد. به این دلایل که اول، تعداد افرادی که بر روی این ایده مشغول به کَار بودند چندان زیاد نبود، و دوم، طراحی و اجرای یک سیستم بدون نقص امری بسیار چالش برانگیز بود.

1 Nick Szabo
2 Bit Gold
3 Provable Costliness

در سال ۲۰۰۴، هال فینی که سابقهٔ مشارکت در پروژهٔ PGP را داشت ایدهٔ اثباتِ کارِ چند بار مصرف[1] (به اختصار RPOW) را معرفی کرد که یکی از نوآوری‌های بسیار کَلیدیِ در مسیر به‌وجود آمدن بیت‌کوین بود.

فینی شبکه‌ای از سرورهای اپن سورس را بر روی ایدهٔ بیت گُلد سوار کرد، که وظیفهٔ تأیید تراکنش‌های شبکه را بر عهده داشتند. افراد می‌توانستند بیت گُلدهای خود را به‌همراه ایمیل برای دیگران ارسال کنند و گیرنده نیز از این راه صاحب پول نقدی -در وجه حامل- می‌شد که ارزشمند بودنِ آن اثبات‌پذیر بود.

هال فینی سیستم RPOW را روی سرورهای خودش به‌صورت متمرکز راه‌اندازی کرد، اما قصد داشت در نهایت معماری این شبکه را غیرمتمرکز کند. این قدم‌ها در مسیر رسیدن به بیت‌کوین کلیدی بودند اما برای تکمیل پازل نهایی هنوز به تکه‌های دیگری نیاز بود.

بخش پنجم - راه‌اندازی بیت‌کوین

آدام بَک در سال ۱۹۹۹ در رشته سیستم‌های توزیع شده مدرک PhD گرفت و در شرکت Zero Knowledge Systems در کانادا مشغول به کار شد. او در این شرکت در ساخت Freedom Network مشارکت داشت که به کاربران خود اجازه می‌داد به‌صورت خصوصی وب‌گردی کنند زیرا ردگیری آن‌ها ممکن نبود. بَک و همکارانش برای ساخت این ابزار از طرح "zero-knowledge proofs" استفاده کردند که بر اساس «امضای غیرقابل شناسایی»[2] دیوید چام بنا شده بود. آن‌ها از این ابزار برای رمزنگاری ارتباط‌های کاربران بر روی این شبکه استفاده می‌کردند و دسترسی به این سرویس را به کاربران به فروش می‌رساندند.

1 Reusable Proof of Work
2 Blind signatures

بعدها مشخص شد بَک با این نوآوری چشم‌گیر از زمان خود بسیار جلوتر بوده است. سه سال بعد یعنی در سال ۲۰۰۲ دانشمندان علوم کامپیوتر این ابزار را از طریق اپن سورس ساختنِ پروژه وب‌گردی خصوصی دولت آمریکا به نام «مسیریابی پیازی[1]» توسعه دادند. آن‌ها نام این پروژه را Tor نامیدند. پروژه‌ای که الهام‌بخش ظهور شبکه‌های خصوصیِ مجازی[2] شد و همچنان بهترین نمونه از شبکه‌های وب‌گردی خصوصی است.

بک اواسط دهۀ ۲۰۰۰ از شرکت کانادایی Zero Knowledge Systems جدا شد و برای دورۀ بسیار کوتاهی به‌عنوان محقق حوزۀ امنیت سایبری به استخدام مایکروسافت درآمد.او سپس به یک استارتاپ پیوست تا روی نرم‌افزاری که همکاری روی شبکۀ همتا به همتا را به‌صورت رمزنگاری انجام می‌داد مشغول شود. در تمام این مدت بک ایدۀ پول دیجیتال را در پسِ ذهن خود داشت و آن را فراموش نکرده بود

ایمیل ساتوشی ناکاموتو در اوت سال ۲۰۰۸ کنجکاوی او را برانگیخت. او با دقت ایمیل ساتوشی را مطالعه کرد و در پاسخ به او پیشنهاد داد سیستم‌های مالی دیجیتالی که تا آن روز ارائه شده بودند منجمله بی-مانی از وِی دای را بررسی کند.

ناکاموتو در روز ۳۱ اکتبر ۲۰۰۸ وایت‌پیپر بیت‌کوین را روی «لیست» منتشر کرد. او در اولین پاراگراف‌های این وایت‌پیپر وعده داده بود که رؤیای بزرگی که همگان به دنبال آن بودند را محقق کرده است: «یک نسخۀ کاملا همتا به همتا از پول الکترونیکی امکان پرداخت‌های آنلاین میان افراد را بدون وابستگی به نهادهای مالی محقق خواهد کرد.» هَش‌کَش از آدام بک، بی-مانی از دای، و تحقیقاتی که در گذشته در حوزۀ رمزنگاری انجام گرفته بود همگی در وایت‌پیپر بیت‌کوین ارجاع داده شده بودند.

1 Onion routing
2 Virtual Private Network

آرون ون ویردوم[1] از تاریخ‌نگارانِ حوزهٔ پولِ دیجیتال در این مورد می‌نویسد: «ساتوشی برای خلق بیت کوین با استفاده از ایده‌های هش‌کش با یک تیر دو نشان زد؛ هم مشکل دو بار خرج کردن در سیستم‌های غیرمتمرکز را حل کرد، هم امکان خلق توکن‌های جدید بدون نیاز به یک نهاد متمرکز را فراهم ساخت.» او خاطرنشان می‌کند که ممکن است هش‌کَش اولین سیستم پول دیجیتال نباشد، اما ایجاد یک سیستم پول دیجیتال غیرمتمرکز «بدون به‌کارگیری از هش‌کش احتمالاً ناممکن است.»

ناکاموتو در تاریخ ۹ ژانویه سال ۲۰۰۹ اولین نسخهٔ نرم‌افزار بیت‌کوین را عرضه کرد. هال فینی اولین نفری بود که این نرم‌افزار را دانلود و با آن کار کرد. او از اینکه می‌دید کسی الگوی اثبات کارِ چند بار مصرف (RPOW) او را برای چنین پروژه‌ای به‌کار گرفته، هیجان‌زده بود.

فردای آن روز یعنی در ۱۰ ژانویه، فینی توئیت تاریخی خود را نوشت: «بیت‌کوین را اجرا می‌کنم»[2] و این انقلاب صلح‌آمیز آغاز شد.

توئیت «بیت‌کوین را اجرا می‌کنم» از هل فینی. منبع.

1 Aaron van Wirdum
2 Running bitcoin

بخش ششم – بلاک آفرینش

ساتوشی ایدهٔ پشت فن‌آوری همتا به همتای بیت کوین را در یک انجمن گفتگوی آنلاین در فوریهٔ سال ۲۰۰۹ این‌گونه تشریح کرد:

«پیش از ظهور سیستم‌های رمزنگاری قدرتمند امروزی، کاربران برای محافظت از اطلاعات خصوصی خود راهی جز اعتماد به رمز عبورشان نداشتند. حریم خصوصی آن‌ها همیشه در معرض خطر تصمیمات مدیران شبکه یا افراد مافوق آن‌ها بود، زیرا ممکن بود شرایطی پیش آید که آن‌ها برخی از نگرانی‌ها را بر حفظ حریم خصوصی کاربران ترجیح دهند. سپس سیستم‌های رمزنگاری قدرتمند در دسترس همگان قرار گرفت و دیگر نیازی به اعتماد نبود. با استفاده از این روش‌ها می‌توان به‌گونه‌ای از اطلاعات محافظت کرد که گویی دسترسی به آن‌ها از نظر فیزیکی ممکن نیست. مهم نیست دلیل یا بهانهٔ شخصی که می‌خواهد به این اطلاعات دسترسی داشته باشد چقدر قوی باشد؛ مهم نیست او چرا می‌خواهد به این اطلاعات دسترسی داشته باشد؛ در نهایت این کار برای او ممکن نخواهد بود.

«زمان آن فرا رسیده است که ما چنین چیزی را برای پول نیز در اختیار داشته باشیم. با استفاده از پول‌های دیجیتالی که بر پایهٔ اثبات رمزنگاری[1] طراحی شده‌اند، می‌توان بدون نیاز به اعتماد به یک شخص ثالث به‌عنوان واسطه، تراکنش‌های بی‌دردسری انجام داد و امنیت پول را تأمین کرد. یک کوین دیجیتالی دربردارندهٔ کلید عمومی صاحبش است. صاحب یک دارایی دیجیتال برای انتقال آن باید توکن خود را با کلید عمومی صاحب جدید امضا کند. هرکسی که در شبکه حضور دارد می‌تواند صحت این امضا و زنجیرهٔ مالکیت آن را بازبینی کند. این روش برای تضمین مالکیت کوین‌ها به‌خوبی کار می‌کند، اما یک مشکل بزرگ همچنان حل نشده باقی می‌ماند: دوبار خرج کردن[2] کوین‌ها. مالکین کوین‌ها قادرند یکی از کوین‌هایی که قبلاً خرج کرده‌اند را امضاء و با ارسال آن به یک فرد جدید آن را

1 Cryptographic proof
2 Double-spending

دوباره خرج کنند. راه حل معمول این است که یک شرکت قابل اعتماد با یک پایگاه دادهٔ متمرکز را مسئول جلوگیری از دوبار خرج شدن کوین‌ها می‌کنند، اما این مدل دوباره پای اعتماد را به سیستم باز می‌کند. این شرکت با توجه به نقش مرکزی که دارد قادر است حقوق کاربران سیستم را پایمال کند...

«راه حل بیت کوین برای جلوگیری از دو بار خرج شدن، استفاده از یک شبکهٔ همتا به همتا است... در نتیجه، یک شبکهٔ توزیع‌شده بدون هیچ‌گونه نقطهٔ ضعفی خواهیم داشت. کاربران کلیدهای رمزنگاری پول خود را در اختیار دارند و بر روی شبکه‌ای همتا به همتا که وظیفهٔ جلوگیری از دوبار خرج شدن پول را بر عهده دارد، با یکدیگر معامله می‌کنند.»

ناکاموتو از ایده‌هایی که قبلاً توسط دیفی، چام، بک، دای، زابو، و فینی مطرح شده بود استفاده کرد و شبکهٔ غیرمتمرکز پول نقد دیجیتال را ساخت.

کلید موفقیت ساتوشی ترکیب امکان انجام معاملات خصوصیْ خارج از سیستم بانکی، و ایجاد یک کلاس دارایی جدید بود که امکان پایین آوردن ارزش آن از طریق مداخلات سیاسی ممکن نبود.

مورد دوم تا اواخر دههٔ ۱۹۹۰ مورد توجه سایفرپانک‌ها نبود. زابو در پیشنهاد بیت گُلد می‌خواست به آن دستیابی پیدا کند و افراد دیگری نیز وجود داشتند که با الهام از اقتصاددانان مکتب اتریش[1] مانند فردریش هایک[2] و موری راتبارد[3] در گذشته در مورد ایجاد پولی که دست دولت‌ها از آن کوتاه است، بحث کرده بودند. با این حال، به طور کلی، در دیدگاه‌های اولیهٔ سایفرپانک‌ها از پول نقد دیجیتال، حریم خصوصی بر سیاست‌های پولی اولویت داشت.

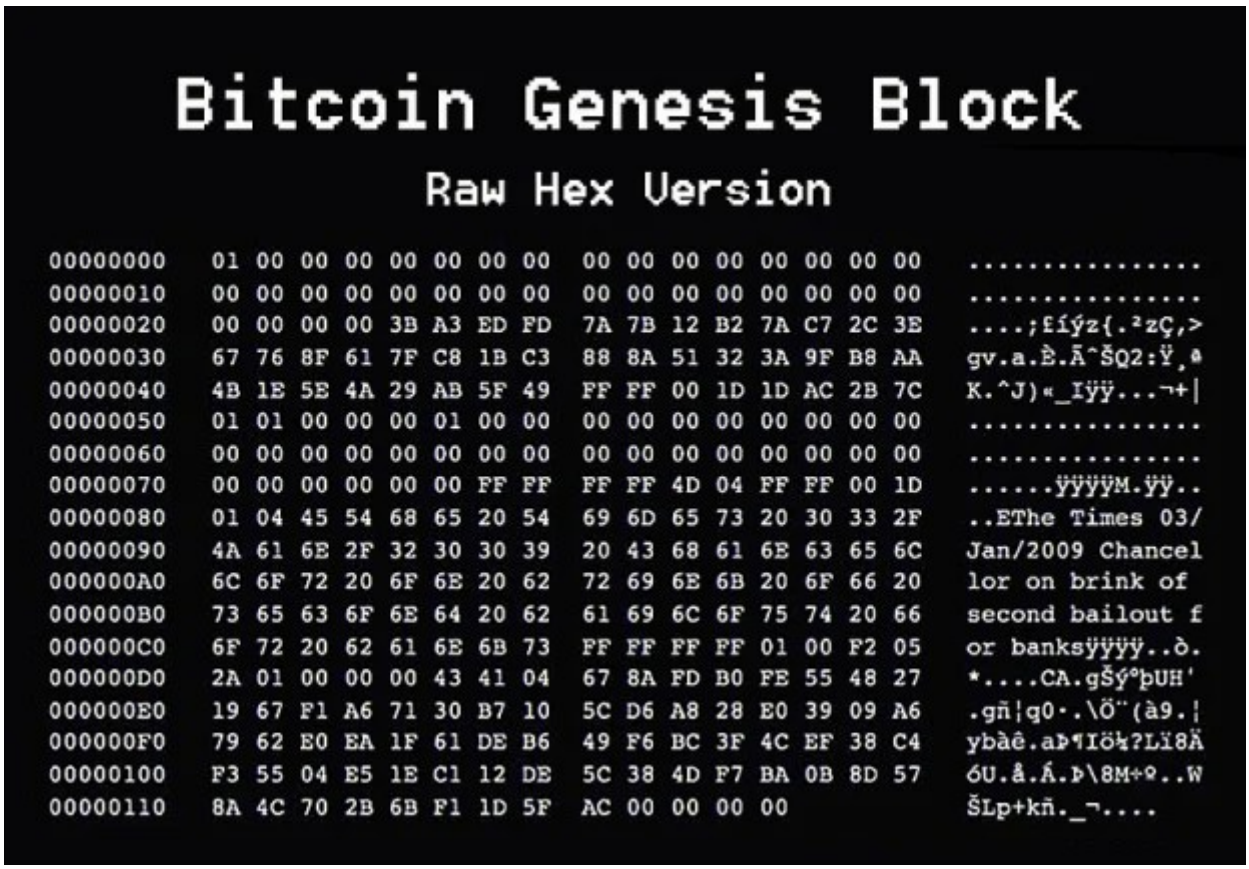
1 Austrian economists
2 Fredrich Hayek
3 Murray Rothbard

تردید حامیان حفظ حریم خصوصی نسبت به مقولهٔ سیاست‌های پولی همچنان مشهود است. بسیاری از گروه‌های آزادی‌های مدنی چپ‌گرا که در دو دههٔ گذشته از حقوق دیجیتال[1] شهروندان آمریکایی پاسداری کرده‌اند، یا به بیت‌کوین توجهی نکرده‌اند، یا با آن دشمنی دارند. محدودیت خلق ۲۱ میلیون کوین، کمیابی، و کیفیت «پول سخت»[2] (پولی که خلق یا تولید آن دشوار باشد. -م) لازمهٔ دستیابی به حریم خصوصی از راه به‌کارگیری پول نقد دیجیتال هستند. با این حال، گروه‌های مدافع حقوق دیجیتال، عمدتاً نقشی که ساز و کار اثباتِ کار، و سیاست پولی تغییرناپذیر می‌توانند در دفاع از حقوق بشر ایفا کنند را به رسمیت نمی‌شناسند.

ناکاموتو برای تأکید بر اهمیت ویژگی کمیابی، و سیاست پولیِ پیش‌بینی‌پذیر در مسیر پدید آوردن یک پول نقد دیجیتال، بیت‌کوین را پس از یک رسوایی ردگیری و نظارت دولت‌ها بر شهروندان منتشر نکرد، بلکه آن را در پی بحران مالی جهانی و آزمایش روش‌های مختلف چاپ پول در سال ۲۰۰۷ و ۲۰۰۸ منتشر کرد.

اولین رکورد ثبت شده در زنجیرهٔ بلاک بیت‌کوین –معروف به «بلاک پیدایش[3]»،- یک شعار سیاسی است. در میان اطلاعات قرار داده شده در این بلاک، پیامی قابل تأمل قرار گرفته است: «تایمز / ۳ ژانویه / ۲۰۰۹ در آستانهٔ دومین کمک مالی به بانک‌ها[4]»

1 Digital Rights
2 Hard money
3 Genesis Block
4 The Times / 03 Jan / 2009 Chancellor on brink of second bailout for banks



پیام مستتر در بلاک پیدایشِ بیت‌کوین

این پیام به تیتر روزنامهٔ تایمز چاپ لندن اشاره دارد که در آن توضیح می‌دهد که دولت بریتانیا چگونه قصد دارد از راه خلق پول، بخشِ خصوصیِ در حال ورشکستگی را نجات دهد. این بخشی از تلاش‌های بین‌المللی بود که در آن بانک‌های مرکزی برای نجات بانک‌های خصوصی از هیچ پول خلق می‌کردند و در ازای آن دارایی‌هایی چون اوراق بهادار با پشتوانهٔ وام مسکن و بدهی‌های شرکتی و دولتی را به‌دست می‌آوردند. بانک انگلستان[1] در بریتانیا پول بیشتری برای نجات اقتصاد چاپ می‌کرد.

بیانیهٔ ناکاموتو که در اولین بلاک زنجیرهٔ بیت‌کوین قرار گرفته، به کژمنشی[2] ایجاد شده توسط سیاست‌های پولی اتخاذ شده توسط بانک انگلستان اشاره داشت. این بانک قصد

1 Bank of England
2 Moral hazard

داشت با چاپ پول، آخرین راه چاره برای نجات شرکت‌های بریتانیایی باشد که با اجرای سیاست‌های بی‌پروای خود در خطر ورشکستگی قرار گرفته بودند.

بهای واقعی این اقدام‌ها را شهروندان قشر متوسط ساکن لندن پرداخت خواهند کرد، چرا که نخبگان و آقازاده‌ها همواره راهی برای محافظت از ثروت خود پیدا می‌کنند. در حالی که شهروندان طبقهٔ پایین و متوسط بریتانیایی از این سیاست‌ها آسیب می‌بینند، حتی یک بانکدار بریتانیایی در طول این بحران بزرگ به زندان نمی‌افتد. بیت‌کوین چیزی فراتر از پول نقد دیجیتال، بلکه جایگزینی برای بانکداری مرکزی بود.

ناکاموتو روش بوروکرات‌ها، یعنی نجات اقتصاد از راه افزایش بدهی را نمی‌پسندید. همانطور که نوشته:

> مشکلی ریشه‌ای پول‌های رایج این است که بدون اعتماد کار نمی‌کنند. باید به بانک مرکزی اعتماد کنیم که پول را بی‌ارزش نمی‌کند، اما در طول تاریخ بارها ثابت شده که قابل اعتماد نیستند. برای نگهداری و جابه‌جایی پول خود به‌صورت الکترونیکی باید به بانک‌ها اعتماد کنیم، اما آن‌ها با قرض دادن آن به روش بانکداری ذخیرهٔ کسری[1] موجب پدید آمدن موج‌هایی از حباب‌های اعتبار[2] می‌شوند.

ناکاموتو شبکهٔ بیت‌کوین را به‌عنوان رقیبی برای بانکداری مرکزی به‌راه انداخت. سیاست پولی بیت‌کوین خودکار است و دیگر خبری از اتاق‌هایی که تعداد انگشت‌شماری از نخبگان و آقازاده‌ها به‌جای مردم در مورد پول تصمیم می‌گیرند نیست.

1 Fraction in reserve
2 Credit bubbles

بخش هفتم – یک شاهکار در مهندسی

بَک از همان ابتدا تحت تاثیر بیت کوین قرار گرفت. او گزارش میدانی که هال فینی اوایل سال ۲۰۰۹ منتشر کرده بود را مطالعه کرد و متوجه شد که ساتوشی بسیاری از مشکلاتی که پیش از این از ایجاد پول نقد غیرمتمرکز جلوگیری می‌کرده را حل کرده است. چیزی که احتمالا بیش از هرچیزی بَک را تحت تاثیر قرار داد و از نظر او بیت‌کوین را نسبت به سایر پروژه‌هایی که تاکنون دیده بود مهم‌تر می‌کرد این بود که ساتوشی ناکاموتو اوایل سال ۲۰۱۱ برای همیشه ناپدید شد.

ناکاموتو طی سال‌های ۲۰۰۹ و ۲۰۱۰ در به‌روزرسانی نرم‌افزار و گفت‌وگو دربارهٔ بهبود بیت‌کوین حضور داشت و نظرش را دربارهٔ آیندهٔ شبکه با دیگران در تالارهای گفتگوی سایت Bitcointalk به اشتراک می‌گذاشت. سپس، یک روز ناپدید شد و از آن زمان تا به امروز کسی از او خبری قطعی ندارد.

در زمان حضور او، بیت‌کوین هنوز یک پروژهٔ نوپا بود و ساتوشی درواقع پاشنهٔ آشیل آن به‌حساب می‌آمد. اواخر سال ۲۰۱۰ او به‌عنوان دیکتاتورِ خیرخواه[1] پروژه عمل می‌کرد. او با ترک پروژه –و چشم‌پوشی از شهرت بی‌حد و حصر، جوایز، و ثروت،– امکان آسیب‌رساندن دولت‌ها به بیت‌کوین از راه دستگیری یا اعمال‌نفوذ روی خالق آن را از بین برد.

ناکاموتو پیش از ترک پروژه نوشت:

> «بسیاری از افراد بخاطر موفقیت‌آمیز نبودن تلاش‌های شرکت‌هایی که در مسیر خلق پول نقد الکترونیکی در دههٔ ۱۹۹۰ فعال بودند، این ایده را شکست‌خورده تلقی

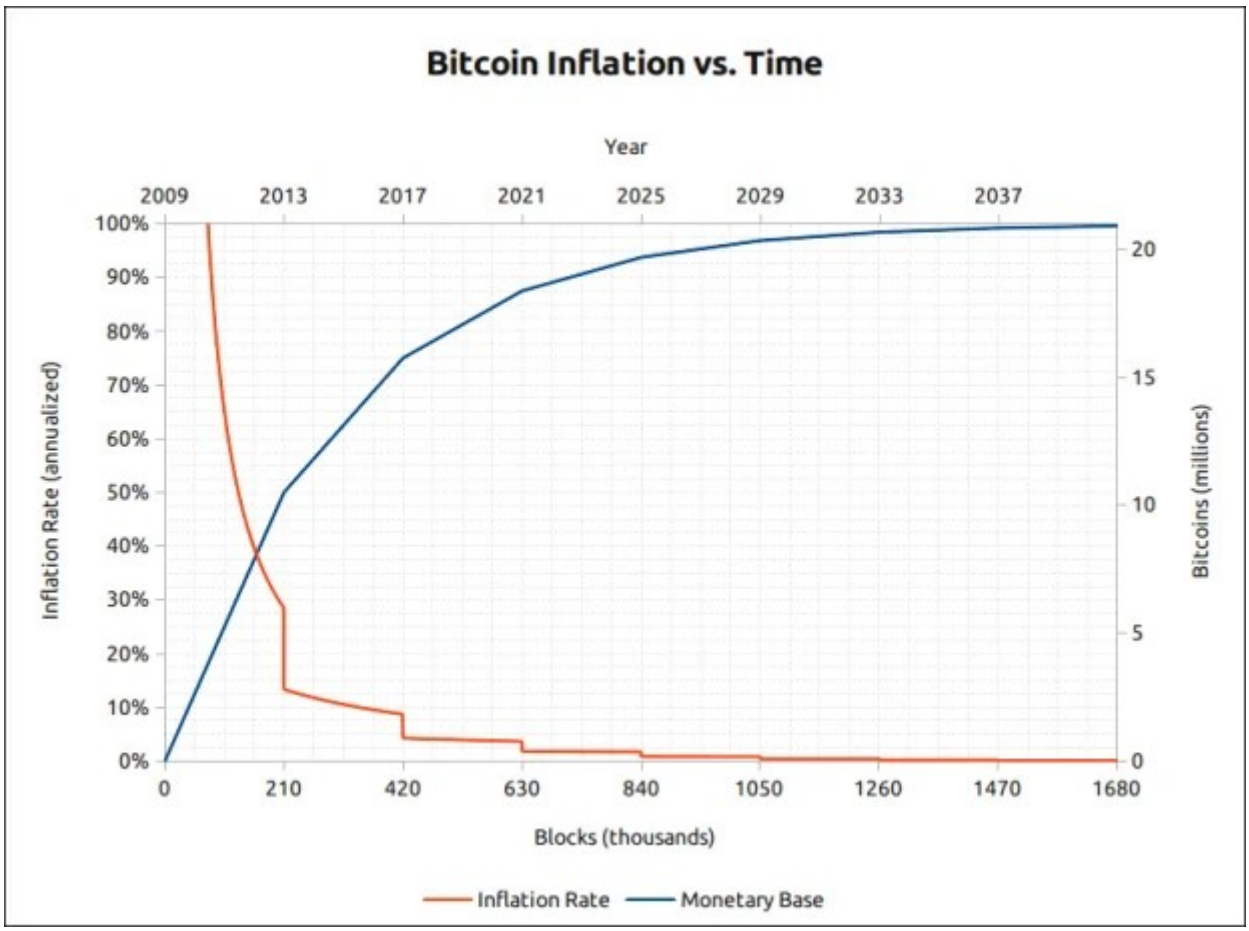
1 benevolent dictator

می‌کنند. امیدوارم این نکته واضح باشد که دلیل اصلی شکست آنها، ماهیت کنترل مرکزی این سیستم‌ها بوده است. من فکر می‌کنم این اولین بار است که ما سیستم غیرمتمرکزی که بر پایهٔ اعتماد بنا نشده است را امتحان می‌کنیم.»

بَک با این موضوع موافق بود. گذشته از اینکه او از نحوهٔ معرفی و سپس ناپدید شدن ناکاموتو به‌شدت تحت تأثیر قرار گرفته بود، او به‌ویژه شیفتهٔ سیاست پولی بیت‌کوین بود. سیاست پولی بیت‌کوین به‌نحوی برنامه‌ریزی شده است که تا دههٔ ۲۱۳۰ هر سال مقدار کمتری نسبت به سال‌های قبل بیت‌کوین تولید شود، تا اینکه در نهایت آخرین بیت‌کوین خلق و فرآیند تولید بیت‌کوین برای همیشه متوقف شود. تعداد کل کوین‌ها در شبکهٔ بیت‌کوین ۲۱ میلیون است.

هر چهار سال یارانهٔ ساخت بلاک یعنی مقدار بیت‌کوینی که به‌عنوان بخشی از پاداش ساختنِ بلاک به ماینرها داده می‌شود، در رویدادی که به «نصف شدن[1]» معروف است، به نصف مقدار دورهٔ قبل کاهش می‌یابد.

1 Halving



سیاست پولی پیش‌بینی‌پذیر بیت‌کوین. منبع.

زمانی که ناکاموتو در اوایل سال ۲۰۰۹ بیت‌کوین استخراج می‌کرد، یارانهٔ ساختِ هر بلاک ۵۰ بیت‌کوین بود. این دستمزد سال ۲۰۱۲ به ۲۵ بیت کوین رسید، چهار سال بعد به ۱۲.۵ بیت کوین رسید و در آوریل سال ۲۰۲۰ نصف این عدد شد. تا زمان انتشار این مقاله حدود ۱۹ میلیون بیت کوین استخراج شده است و تا سال ۲۰۳۵، ۹۹ درصد از کل بیت‌کوین‌ها خلق شده‌اند.

باقی کوین‌ها نیز در طول قرن بعد به‌عنوان انگیزه‌ای برای ماینرها که در گذر زمان باید سود خود را به‌جای یارانهٔ ساختِ بلاک از کارمزدهای تراکنش‌ها به‌دست آورند، در نظر گرفته می‌شود.

حتی در همان سال ۲۰۰۹ ساتوشی، هال فینی و دیگران حدس می‌زدند که سیاست پولی منحصربه‌فرد بیت‌کوین یعنی سقف عرضهٔ ۲۱ میلیون کوین ممکن است در صورتی که این پروژه رونق بگیرد، آن را بسیار ارزشمند کند.

بَک معتقد بود در کنار سیاست پولیِ نوآورانهٔ بیت‌کوین، «الگوریتم سختی»[1] نیز یک پیشرفت علمی بسیار مهم است. این ترفندْ یکی از نگرانی‌هایی را که بَک در مورد سیستم هَش‌کَش داشت، یعنی شرایطی که در آن افراد با کامپیوترهای سریع‌تر می‌توانستند سیستم را از پا دربیاورند برطرف می‌کرد. در بیت‌کوین، ناکاموتو با برنامه‌ریزی شبکه برای بازتنظیم سختی مورد نیاز برای ساخت یک بلاک و بر اساس زمانی که برای ساختن تعداد مشخصی از بلاک‌ها صرف شده، از این اتفاق جلوگیری کرد.

اگر بازار سقوط کند یا اتفاق فاجعه‌باری رخ دهد (به عنوان مثال، زمانی که حزب کمونیست چین نیمی از استخراج‌کنندگان بیت‌کوین را در ماه مه ۲۰۲۱ خاموش کرد)، و کل انرژی جهانی مصرف شده برای استخراج بیت‌کوین (همان «نرخِ هش»[2]) کاهش پیدا کند، در این شرایط ساختن بلاک‌ها بیشتر از حد معمول طول خواهد کشید.

با این حال، شبکه پس از گذشت مدت زمان کوتاهی (حدوداً دو هفته) و با اعمال الگوریتم [بازتنظیم] سختیْ جبران و ساختن بلاک‌ها را آسان‌تر می‌کند. برعکس، اگر توانِ هشِ جهانی برای مثال با اختراع تجهیزات استخراجِ کارآمدتر بالاتر رود، و ماینرها بلاک‌ها را در مدت زمان کوتاه‌تری بسازند، الگوریتم سختی پس از گذشت همان زمان کوتاه جبران و ساختن بلاک‌ها را دشوارتر می‌کند. این ویژگی به ظاهر ساده به بیت‌کوین قابلیت تاب‌آوری بالایی اعطا و به آن کمک کرده تا از آشفتگی‌هایی که با تغییر فصول در صنعت استخراج رخ می‌دهد، سقوط‌های شدید قیمتی، و تهدیدهای قانون‌گذاری جان

1 Difficulty algorithm
2 Hash rate

سالم به در برد. زیرساخت صنعت استخراج بیت‌کوین امروز بیش از هر زمان دیگری غیرمتمرکز است.

این نوآوری‌ها باعث شد تا بَک فکر کند که بیت‌کوین با برطرف کردن نقاط ضعف تلاش‌های قبلی که با شکست مواجه شده بودند، به‌طور بالقوه می‌تواند به موفقیت دست یابد. با این حال یک مشکل آشکار همچنان حل نشده باقی ماند: [نقل و انتقال روی زنجیرهٔ بلاک] بیت‌کوین خصوصی نبود.

بخش هشتم – مسألهٔ حریم خصوصی در بیت‌کوین

برای سایفرپانک‌ها، حریم خصوصی یک هدف کلیدی بود. تلاش‌های قبلی برای خلق پول نقد دیجیتال، مانند آنچه توسط شرکت دیجی‌کش ارائه شده بود، حتی حاضر به قربانی کردن تمرکززدایی به منظور دستیابی به حریم خصوصی شده بودند. ممکن است حریم خصوصی در این سیستم‌ها به نحو احسن پیاده شده باشد، اما کاربران می‌بایست به مرجع خلق پول اعتماد می‌کردند و پول آن‌ها در معرض خطر سانسور و کاهش ارزش قرار داشت.

برای جایگزین کردن مرجع خلق پول، ناکاموتو مجبور بود به یک سیستم دفتر کل حسابداری عمومی تکیه کند، سیستمی که در آن سابقهٔ همهٔ تراکنش‌ها در دسترس عموم قرار دارد. این تنها راه برای اطمینان از حسابرسی‌پذیری[1] الگوریتم خلق پول بود، اما حریم خصوصی کاربران را قربانی می‌کرد. بَک می‌گوید همچنان اعتقاد دارد که این یک تصمیم درست مهندسی بوده است.

1 Auditability

از زمان معرفی دیجی‌کَش کارهای بیشتری در حوزهٔ ارزهای دیجیتال انجام شده است. در سال ۱۹۹۹، محققان امنیتی مقاله‌ای با عنوان «پول نقد الکترونیکی ناشناسِ قابل حسابرسی»[1] را در مورد ایدهٔ استفاده از روش اثبات zero-knowledge منتشر کردند. بیش از یک دهه بعد، مقالهٔ Zerocoin که این ایده را بهبود می‌بخشید منتشر شد. اما این سیستم‌ها در تلاش برای دستیابی به حریم خصوصیِ کامل، ناچار بودند مصالحه کنند.

ریاضیات مورد نیاز برای این تراکنش‌های ناشناس به‌قدری پیچیده بود که سایز هر تراکنش را بسیار بزرگ، و نقل و انتقال آن‌ها را زمان‌بر می‌کرد. یکی از دلایلی که بیت‌کوین امروزه بسیار خوب کار می‌کند این است که میانگین سایز تراکنش‌های بیت‌کوین فقط چند صد بایت است. هرکسی می‌تواند با هزینهٔ کم یک نود در منزل خود اجرا کند و تاریخچهٔ بیت‌کوین و تراکنش‌های دریافتی را بازبینی کند، این موضوع قدرت را در دست کاربران سیستم قرار می‌دهد. این سیستم به تعداد معدودی از ابَرکامپیوترها متکی نیست، بلکه کامپیوترهای معمولی نیز قادرند زنجیرهٔ بلاک بیت‌کوین را ذخیره، و تراکنش‌ها را با توجه به پایین بودن سایز داده‌ها در شبکه، دریافت و منتشر کنند.

اگر ناکاموتو از مدلی شبیه به Zerocoin استفاده کرد بود، سایز هر تراکنش به بیش از ۱۰۰ کیلوبایت می‌رسید، در نتیجه سایز دفتر کل حسابداری بیت‌کوین به‌قدری بزرگ می‌شد که تنها تعداد انگشت‌شماری از افراد با تجهیزات مرکز دادهٔ تخصصی می‌توانستند یک نود بیت‌کوین اجرا کنند. در این صورت تبانی، سانسور، یا حتی تصمیم‌گیری گروه کوچکی از افراد برای افزایش عرضهٔ پولی بیت‌کوین بیش از ۲۱ میلیون کوین ممکن می‌شد. شعار جامعهٔ بیت‌کوین نیز بر همین اساس بیان می‌شود: «برای سنجیدن درستی امور به هیچکس اعتماد نکن، بلکه خودت آن‌ها را مورد بازبینی قرار بده»[2]

1 Auditable Anonymous Electronic Cash
2 don’t trust, verify

بَک می‌گوید حالا که فکرش را می‌کند، از اینکه مقالهٔ پول الکترونیکی ناشناس که در سال ۱۹۹۹ منتشر شده بود را در ایمیل‌های خود به ناکاموتو معرفی نکرده، خوشحال است. او معتقد است ایجاد پولِ نقد دیجیتالِ غیرمتمرکز مهم‌ترین ویژگی این اختراع است و حریم خصوصی را می‌توان بعداً به آن اضافه کرد.

بَک در سال ۲۰۱۳ میلادی به این نتیجه رسیده بود که بیت‌کوین به‌عنوان پایه و اساس پولِ نقدِ دیجیتال به اندازهٔ کافی با ثبات است. او فکر می‌کرد که زمان آن فرا رسیده که او برخی از تجربیات کاربردی رمزنگاری خود را به‌کار گیرد و به خصوصی‌تر شدن آن کمک کند. در این زمان بَک تقریباً ۱۲ ساعت از روز را به خواندن دربارهٔ بیت‌کوین اختصاص داده بود. او می‌گوید که در این دوره گذر زمان را حس نمی‌کرده، تقریباً غذا نمی‌خورده، بسیار کم می‌خوابیده، و ذهن او به‌شدت مشغول بیت‌کوین بوده است.

بَک در همان سال چند ایدهٔ کلیدی را از طریق IRC و تالارهای گفتگوی سایت Bitcointalk به جامعهٔ توسعه‌دهندگان بیت‌کوین پیشنهاد کرد. یکی از این پیشنهادها تغییر نوع امضاء دیجیتال به‌خدمت گرفته شده در بیت‌کوین، از ECDSA به Schnorr بود. با وجودی که امضاءهای نوع Schnorr انعطاف‌پذیرتر بودند و حریم خصوصی بهتری برای کاربران فراهم می‌کردند، ناکاموتو در طراحی اولیهٔ خود از آن استفاده نکرد، چرا که در آن زمان ثبت اختراع شده بود. اما این ثبت اختراع اکنون منقضی شده بود.

پیشنهاد بَک به‌عنوان بخشی از ارتقاء تَپ‌روت[1] در اواسط ماه نوامبر سال ۲۰۲۱ بر روی شبکه اعمال، و به قوانین شبکهٔ بیت‌کوین اضافه شد. هنگامی که تپ‌روت در مقیاس بزرگی توسط کاربران شبکه مورد استفاده قرار گیرد، اکثر تراکنش‌های کیف پول‌ها به چشم ناظران شبکهٔ عمومی بیت‌کوین (از جمله دولت‌ها)، یکسان به نظر می‌رسند و این ویژگی به مبارزه با دستگاه‌های نظارتی کمک می‌کند.

1 Taproot

بخش نهم - تراکنش‌های محرمانه[1]

برجسته‌ترین چشم‌اندازی که بَک برای بیت‌کوین متصور بود، قابلیتی بود که با نام تراکنش‌های محرمانه شناخته می‌شد. در حال حاضر مقدار بیت‌کوین انتقال یافته میان کاربران در یک تراکنش، به‌صورت آشکارا در مقابل دید همگان است. این ویژگی باعث می‌شود هرکس با اجرای نرم‌افزار بیت‌کوین روی یک کامپیوتر معمولی و بدون نیاز به اعتماد به شخص یا نهاد ثالث قادر به حسابرسی سیاست پولی و تعداد کوین‌های در گردش در شبکهٔ بیت‌کوین باشد، اما این قابلیت همچنین نظارت بر زنجیرهٔ بیت‌کوین را نیز امکان‌پذیر می‌سازد.

اگر یک دولت، قادر به شناسایی هویت صاحب یک آدرس بیت‌کوین باشد، در این صورت می‌تواند تمام دارایی‌های موجود در آن و تراکنش‌های انجام شده با آن را رهگیری کند. تراکنش‌های محرمانه می‌توانند مقدار دارایی جابه‌جا شده در یک تراکنش را مخفی کنند و کار نظارت و ردگیری تراکنش‌ها را دشوار، و در شرایطی که این روش در کنار تکنیک‌هایی مانند کوین‌جوین[2] به‌کارگرفته شود، حتی غیرممکن کند.

بَک در سال ۲۰۱۳ با تعدادی از مهندسان فعال در توسعهٔ هستهٔ بیت‌کوین (که او آن‌ها را جادوگران بیت‌کوین[3] می‌نامد) صحبت کرد. او به این نتیجه رسید که افزودن الگوریتم تراکنش‌های محرمانه به شبکه بسیار دشوار خواهد بود چرا که جامعهٔ بیت‌کوین امنیت و قابلیت حسابرسی‌پذیریِ سیاست پولی را بر حریم خصوصی ترجیح می‌داد و او این موضوع را به‌خوبی درک می‌کرد.

بَک همچنین متوجه شد که به دلیل طراحی یکپارچهٔ بیت‌کوین، امکان آزمایش سیستم‌هایی مانند تراکنش‌های محرمانه بر روی آن نیست، بنابراین ایده‌ای به فکرش خطور

1 Confidential Transaction
2 CoinJoin
3 Bitcoin Wizards

کرد که بستری برای انجام آزمون و خطا در حوزهٔ تکنولوژی بیت‌کوین فراهم می‌کرد، به‌گونه‌ای که او می‌توانست ایده‌هایی مانند تراکنش‌های محرمانه را بدون آسیب رساندن به شبکه روی آن آزمایش کند.

بَک خیلی زود به این نتیجه رسید که برای رسیدن به هدف راه زیادی در پیش دارد. او باید کتابخانه‌های نرم‌افزاری زیادی ایجاد، کیف پول‌ها و صرافی‌ها را با این سیستم سازگار، و رابط کاربرپسندی برای آن می‌ساخت. بَک برای انجام این کارها ۲۱ میلیون دلار سرمایه از شرکت‌های سیلیکون وَلی جذب، و یک شرکت تأسیس کرد.

بک با سرمایه‌ای که در اختیار داشت به همراه گرگ مکسول[1] توسعه‌دهندهٔ شناخته شدهٔ هستهٔ بیت‌کوین و با همکاری آستین هیل[2] به‌عنوان سرمایه‌گذار، شرکت بلاک‌استریم[3] را تاسیس کرد. این شرکت امروزه یکی از بزرگ‌ترین شرکت‌های فعال در زمینهٔ بیت‌کوین است. بک همچنان مدیرعامل این شرکت است. بلاک‌استریم روی پروژه‌هایی مانند Blockstream Satellite کار می‌کند. پروژه‌ای که کاربران بیت‌کوین را قادر می‌سازد بدون نیاز به دسترسی به اینترنت، از بیت‌کوین استفاده کنند.

بَک و مکسول در سال ۲۰۱۵ نسخهٔ تست[4] بیت‌کوینی که در نظر داشتند را به نام Element منتشر کردند. آن‌ها الگوریتم تراکنش‌های محرمانه را روی این زنجیرهٔ جانبی[5] راه‌اندازی کردند. این زنجیره در حال حاضر Liquid نام دارد و تاکنون صدها میلیون دلار تراکنش به‌صورت محرمانه بر روی آن انجام شده است.

کاربران بیت کوین بین سال‌های ۲۰۱۵ تا ۲۰۱۷ با ماینرها و شرکت‌های بزرگ فعال در حوزهٔ بیت‌کوین درگیر جنگی با هدف محدود کردن سایز بلاک بودند که به «جنگ بر سر سایز بلاک» مشهور است. بسیاری کاربران می‌خواستند اندازهٔ بلاک‌ها به یک محدودهٔ

1 Greg Maxwell
2 Austin Hill
3 Blockstream
4 testnet
5 sidechain

منطقی محدود، و قدرت در اختیار کاربران معمولی باقی بماند (اگرچه بیشینهٔ سایز بلاک در تئوری تا ۴ مگابایت افزایش یافت). بنابراین هر برنامه‌ای که در آینده قصد افزایش سایز بلاک را به مقدار قابل توجهی داشته باشد، به احتمال زیاد با مقاومت شدیدی مواجه خواهد شد.

بَک هنوز معتقد است که می‌توان کُد تراکنش‌های محرمانه را بهبود بخشید و سایز این تراکنش‌ها را به‌قدری کاهش داد که امکان ادغام آن در شبکهٔ بیت‌کوین فراهم شود. این کار [چه از نظر فنی، چه از منظر کسب توافق جامعهٔ کاربران بیت‌کوین] در بهترین حالت سال‌ها به‌طول خواهد انجامید اما بَک همچنان به تلاش خود ادامه می‌دهد.

در حال حاضر، کاربران بیت‌کوین می‌توانند با استفاده از تکنیک‌هایی مانند کوین‌جوین، کوین‌سواپ[1]، همچنین با استفاده از فناوری‌های لایهٔ دوم مانند شبکهٔ لایتنینگ[2] یا زنجیره‌های جانبی مانند Liquid و Mercury، از حریم خصوصی خود محافظت کنند.

به‌طور خاص، لایتنینگ -یکی دیگر از حوزه‌هایی که تیم بَک در شرکت بلاک‌استریم با توسعهٔ نود لایتنینگ c-lightning سرمایه‌گذاری جدی انجام داده است،- به کاربران کمک خواهد کرد تا بیت‌کوین‌های خود را با کارمزد بسیار پایین، سرعت بالا، و [در آینده با اضافه شدن تکنولوژی‌هایی که به خصوصی‌تر شدن این شبکه کمک می‌کنند،] به‌صورت خصوصی خرج کنند. با کمک نوآوری‌هایی مانند این، بیت‌کوین به پس‌اندازی مقاوم در برابر سانسور و کم‌ارزش شدن برای ده‌ها میلیون کاربر در سراسر جهان تبدیل خواهد شد، و می‌توان از آن در پرداخت‌های روزانه نیز استفاده کرد.

بیت‌کوین در آینده‌ای نه‌چندان دور به چشم‌انداز سایفرپانک‌ها یعنی پول نقد دیجیتالی که می‌توان آن به چهارگوشهٔ دنیا ارسال کرد، از تمام ویژگی‌های حفظ حریم خصوصی پولِ نقد برخوردار است، و مانند طلا ارزش دارایی دارندگانش را حفظ می‌کند، جامهٔ عمل

1 CoinSwap
2 Lightning Network

خواهد پوشاند. این موضوع با توجه به اینکه در حال حاضر دولت‌ها در حال آزمایش و بررسی راه‌های ایجاد ارزهای دیجیتال بانک مرکزی[1] هستند، می‌تواند یکی از مهم‌ترین رسالت‌های قرن حاضر باشد.

پول دیجیتالی بانک‌های مرکزی قصد جایگزینی پول کاغذی با اعتبارات الکترونیکی را دارد که می‌تواند به راحتی تحت نظارت، مصادره، کسر مالیات به‌صورت خودکار، و کاهش ارزش از طریق نرخ بهرهٔ منفی قرار گیرد. آن‌ها قصد دارند راه مهندسی اجتماعی، سانسور هدف‌مند، قطع دسترسی کاربران به سرویس‌ها و خدمات، و تعیین تاریخ انقضاء برای پول را هموار کنند.

اما اگر چشم‌انداز پول نقدِ دیجیتال برای بیت‌کوین به‌طور کامل محقق شود، در این صورت طبق گفتهٔ ناکاموتو: «می‌توانیم در این نبرد تسلیحاتی به یک پیروزی بزرگ دست پیدا کنیم و برای چندین سال قلمرو جدیدی از آزادی را به دست آوریم.»

این رؤیای سایفرپانک‌ها است و آدام بَک همچنان برای تحقق یافتن آن تلاش می‌کند.

1 Central Bank Digital Currency (CBDC)

این مقاله توسط الکس گلداستین تألیف و در سایت Bitcoin Magazine منتشر شده است. ترجمهٔ فارسی این مقاله توسط سجاد بیات (پادکست بلاک‌تایم)، بازبینی ویراست اول آن توسط یکی از مخاطبین ناشناس سایت، و صفحه‌بندی آن توسط «سایت منابع فارسی بیت‌کوین» انجام شده است.

سایت منابع فارسی بیت‌کوین
پاییز ۱۴۰۰