

بسم الله الرحمن الرحيم

تمدن در گذار

رمزارز مرموز

اردوان مجیدی

مرداد ۹۹

اگر شما بتوانید یک سازوکار رمزگذاری را ایجاد کنید، که شخصی برای شکستن رمز آن مجبور به صرف انرژی و تلاش زیادی باشد، خود بسته رمزگذاری شده، حتی اگر محتوای آن خالی باشد، دارای ارزش خواهد بود. رمزارز تا زمانی که تقاضا و اقبال افراد به خرید آن وجود دارد، به صورتی انتزاعی ارزش پیدا می کنند. اما اگر به هر دلیل، این اقبال از بین برود، ارزش آن کاسته شده یا حتی در شرایطی به سرعت به ”هیچ“ تنزل می کند. و این، زمینه چالشی در حاکمیت در تمدن سایبری را فراهم می کند.

کلمات کلیدی: رمزارز، تمدن سایبری، حاکمیت و حکمرانی در تمدن سایبری، پول، اقتصاد سایبری، اردوان

مجیدی

در سلسله یادداشتهائی، به تحلیل ابعادی از تحول و چالشهای تمدن سایبری می‌پردازیم. این دومین یادداشت از این مجموعه است. در یادداشت قبلی به مسئله حاکمیت و حکمرانی در تمدن سایبری پرداختیم. به عنوان یک نمونه در این زمینه، در خلال این یادداشت و یادداشت بعدی، به مسئله رمزارز می‌پردازیم. ابتدا لازم است تا در این یادداشت به ماهیت انتزاعی رمزارز بپردازیم. سپس در یادداشت بعدی به بحث پیچیدگیها و عدم قطعیت آن، و تعیین کنندگی آن در حاکمیت و حکمرانی سایبری خواهیم پرداخت.

پول برای مبادله؛ انتزاع نخست

مس! احتمالا اولین فلزی که به صورت سکه با عنوان پولیس یا پولس در فنیقیه ضرب شد.^۱ چیزی که باعث شد مبادله پایاپای، و نیز مبادله با اشیاء ارزشمند نظیر طلا و جواهرات، به یک مبادله مبتنی بر شی قراردادی به نام فلوس یا پول تبدیل شود. مستقل از سکه‌ها، برخی از کالاها یا اشیاء در طول تاریخ به عنوان اشیاء دارای ارزش، برای مبادلات استفاده می‌شد. در زمان قدیم در خاورمیانه، جو، و در قاره آمریکا، صدف، به عنوان پول استفاده می‌شد.^۲ بتدریج با شکل‌گیری صرافی‌ها در شبکه شهرها، برگه حواله صرافی‌ها اعتبار مستقل پیدا کرد، و با تبدیل شدن صرافی‌ها به بانک، چک و اوراق بانکی به عنوان یک بستر مبادله شکل گرفت. اولین پولهای کاغذی در دوره مغولان چین ایجاد و استفاده شد.^۳ اینگونه بود که پول یک پدیده قراردادی و انتزاعی^۴ برای مبادله شد.

انتزاع در سطح دوم: بازی ارزش

معمولا سکه‌ها به واسطه ارزش ذاتی آن (مثلا ارزش طلا یا نقره) ارزش پیدا می‌کردند، اما بتدریج ارزش خود سکه (بواسطه اعتبار حکومتی ضرب کننده سکه)، با ارزش خود مواد سازنده آن متفاوت شد (بعضا بیشتر و بعضی اوقات حتی کمتر^۵). اینجا مسئله اعتبار پول جدی شد. به این ترتیب حکومتها از اعتبار خود برای چاپ یا ضرب پول بدون پشتوانه^۶ استفاده کردند.

با تنشهای جنگ جهانی اول و جنگ جهانی دوم، که یک سوی عوامل آن، مسائل اقتصادی بین کشورهای اروپائی-آمریکائی بود، تلاشهایی برای مدیریت این پدیده در کنفرانس ورسای و کنفرانس برتون وودز^۷ صورت گرفت، که بر اساس آن، کشورها طلا را به عنوان پشتوانه پول منتشر شده خود، محسوب کنند. در کنفرانس برتون وودز، دلار آمریکا به عنوان پشتوانه مبادلات مالی بین کشورها تعیین شد، و آمریکا متعهد شد که به مدت ۲۵ سال، برای پشتوانه دلار، طلا در خزانه خود نگهداری کند، و معادله ارزش دلار با ارزش طلا را ثابت نگاه دارد. به نحوی که هر کسی با دادن دلار آمریکا به خزانه داری آمریکا، بتواند معادل آن به مقدار ثابتی طلا دریافت کند. با این کار آمریکا توانست دلار را مبنای تمام مبادلات اقتصادی جهان قرار دهد.

اما بعد از چند سال وقتی که این اعتباریابی بین‌المللی دلار تثبیت شد، و نظامهای اقتصادی دنیا به آن وابسته شدند، در سال ۱۹۷۱، ریچارد نیکسون، رئیس‌جمهور آمریکا به صورت یکطرفه پیمان برتون وودز را لغو کرد. این اتفاق باعث شد تمام اقتصاد دنیا بر پایه پول بدون پشتوانه قرار بگیرد. کشورهای جهان از بازی آمریکا شوکه شدند؛ و از سوی دیگر بدلیل وابسته شدن نظامهای مالی شان، امکان حذف دلار را به سادگی نداشتند (که این مسئله تا امروز هم ادامه دارد). بنا بر این آنها هم شروع به چاپ اسکناس بدون پشتوانه کردند، و نظام پولی - ارزی بدون پشتوانه عجیب و غریب امروزی رقم خورد. اغلب مردم تصور می‌کنند که بابت اسکناسهایی که در دست دارند، طلا در خزانه به عنوان پشتوانه وجود دارد؛ اما واقعیت این است که تقریباً در اغلب کشورهای دنیا این فقط یک تخیل است^۱.

در واقع اتفاقی که افتاد، سطح دومی از انتزاع پول رقم خورد. پول که خود پدیده‌ای انتزاعی بود، مجدداً در سطح دیگر منتزع شد. پول که قبلاً خودش به عنوان یک شی قراردادی و انتزاعی برای مبادله بود، حالا به یک پدیده انتزاعی مضاعف تبدیل شد، که ارزش آن فقط به میزان ماهیت ارزش قراردادی آن بستگی نداشت؛ بلکه عوامل اعتباری دیگری در این تعیین ارزش نقش یافت.

این مثل آن می‌ماند که پدیده‌ای که مستقلاً دارای ارزش است، نه برای ارزش ماهوی خودش، بلکه برای ارزش مبادله‌ای آن، ارزشمند شود. در جنگ جهانی اول، در زندانهای اسرا، سیگار که به صورت قاچاق وارد زندان می‌شد، برای مبادله ارزش پیدا کرد. به دلیل عدم وجود پول در زندان، افراد معاملات خود را با سیگار انجام می‌دادند. مثلاً دو نخ سیگار برای یک تکه گوشت. سیگار به تدریج حتی توسط کسانی که سیگاری نبودند هم ارزشمند شد؛ چون آنها می‌توانستند از آن به عنوان یک دارایی خوب و دارای مشتری، برای مبادلات خود استفاده کنند. اینجا سیگار دیگر به دلیل ارزش ماهیتی آن برای افراد سیگاری ارزش پیدا نمی‌کند، بلکه به دلیل ارزش مبادله‌ای آن، و به میزان ارزشی که تقاضا برای آن تعیین می‌کند، ارزش خواهد داشت. پول هم اینگونه، به دلیل اعتبار انتزاعی آن، ارزش پیدا کرد.

اما تا اینجا ماجرا، هنوز کنترل دست کشورها بود. کشورها می‌توانستند ارزش پول خود را با سازوکارهایی مدیریت کنند. بانک مرکزی کشورها بالاخره پاسخگوی ارزش اسکناسی که چاپ کرده بودند، هستند. کم یا زیاد، اگر یک اسکناس را به بانک مرکزی چاپ‌کننده آن ببرید، معادلی برای ارزش آن، حداقل در خودش و بانکهای تابعش می‌شناسد.

سطح سوم انتزاع: تجسم در فضای الکترونیکی

اینجا اتفاقی جدید افتاد. با ایجاد شبکه‌های الکترونیکی، بتدریج تجارت الکترونیکی و خرید و فروش کالا از طریق بسترهای الکترونیکی موضوعیت پیدا کرد. بانکها اینجا نیز بیکار ننشستند، و سازوکارهای مبادله الکترونیکی

پول خودشان را در این فضا فراهم کردند. از طریق کارت بانکی، شما می‌توانستید مبلغی را که در حساب خود در بانک، مطابق ارزش پول آن بانک (مثلاً ریال یا یورو) داشتید، در شبکه مبادلات مالی الکترونیکی هزینه کنید. سطح دیگری از انتزاع در مورد پول اتفاق افتاد. پول الکترونیکی، انتزاعی از پول فیزیکی.

تا اینجا هنوز کنترل دست بانک است. در واقع تمام پول شما و فروشنده محصولات و خدمات به شما، و همه افراد دیگر در بانک و شبکه بانکی به هم پیوسته بانکهای کشور شما است. در واقع شما فقط یک تکه طلق به نام کارت بانکی، و شماره‌های ذخیره شده در آن در دست دارید، که شماره حساب شما را مشخص می‌کند. با خرید شما، اعتباری از حساب شما کم شده و به حساب فروشنده یا شخص دیگر منتقل می‌شود؛ ولی اصل پول در همان بانک است. پولها همه در همان فضای حسابهای بانکی جابجا می‌شود. البته بانک در صورت درخواست شما، به سادگی مبلغ الکترونیک حسابتان را به صورت پول نقد به شما تحویل می‌دهد^۹. پس تا اینجا هنوز اعتبار پول، همان اعتبار پول نقد است.

سطح چهارم: انتزاع مرموز

اما برای مبادله پیامهائی که نشان می‌دهد فلان خرید توسط فلان شخص به بهمان مقدار انجام شده است، نگرانی‌هایی وجود داشت. افرادی ممکن بود با نفوذ در این شبکه مبادله الکترونیک، در این پیامها دستکاری کرده، و پولها را به حساب خودشان جابجا کنند. برای جلوگیری از این اتفاق، رمزگذاری وارد میدان شد. پیامها رمز می‌شدند تا کسی نتواند در آنها دستکاری کند. روشها و سازوکارهای مختلفی برای رمزگذاری ایجاد شد.

بتدریج این سازوکارها و روشها پیچیده و پیچیده تر شدند. تا جایی که این فکر به ذهن برخی از افراد آمد که چطور است خود بسته‌های رمزگذاری شده، که کسی نمی‌تواند از آن رمزگشائی کند، به عنوان ارزش مستقل مالی محسوب شود. اگر شما بتوانید یک سازوکار رمزگذاری را ایجاد کنید، که شخصی برای شکستن رمز آن مجبور به صرف انرژی و تلاش زیادی باشد، به حدی که ارزش این تلاش و انرژی، بیش از ارزش محتوای مالی آن پیام باشد، خود این بسته رمزگذاری شده، مستقل از محتوای آن دارای ارزش خواهد بود. حالا که اینچنین است، اصلاً چرا در آن محتوایی (در ارجاع به پول فیزیکی یا الکترونیکی) بگذاریم. خود این پیام شبه پوچ (از این وجه پوچ که به هیچ حساب بانکی بیرونی با هیچ رقم پول مشخصی (در سطوح انتزاعی پائین تر که مطرح شد)، اشاره نمی‌کند) رمزگذاری شده، می‌تواند یک مبنای ارزش محسوب شود. اگر کسانی پیدا شوند که این بسته پوچ مالی رمزگذاری شده را بخرند، می‌توانند آن را به دیگران هم بفروشند. چیزی شبیه ماجرای آن سیگارها در زندان اسرا، با این تفاوت که سیگار بالاخره برای اشخاص سیگاری کارکردی دارد، اما محتوای این بسته‌ها عملاً به هیچ کار نمی‌آیند. به این ترتیب این بسته‌های پوچ مالی، خود از نظر مالی ارزش مستقلی پیدا خواهد کرد.

ارزش این بسته‌ها به میزان تقاضا (اقبال و تمایل افرادی که این بسته‌ها را می‌خرند)، بستگی دارد. ممکن است به هر دلیل مانند فضا سازی بازار و هیجانات آن، این ارزش بالا و پائین شود. اما تمام ماجرا در یک فضای کاملاً انتزاعی اتفاق می‌افتد. برای اینکه کمی بیشتر این فضا را احساس کنیم، یک مثال می‌زنم.

یک بازی رایانه‌ای مهیج اما دشوار نصب می‌کنید. درگیر بازی می‌شوید. دشواری بازی به شما اجازه نمی‌دهد که به مراحل بعدی بروید. یکی از دوستان شما که بازیگر حرفه‌ای است، حاضر می‌شود حساب کاربری^{۱۰} خودش را که تا مراحل بالاتر رفته، به شما در ازای مبلغی واگذار کند. برای لذت بردن از مراحل بعدی، حساب کاربری او را می‌خرید^{۱۱}. این اتفاقی است که امروز به صورتی واقعی می‌افتد. در سایتهای خرید و فروش مجازی می‌توانید آگهی‌های متعددی از این فروش را مشاهده کنید^{۱۲}.

این بازی و فروش حساب کاربری آن، یک پدیده انتزاعی است. اگر یک روز این بازی در سراسر دنیا از کار بیافتد و دیگر کار نکند، یا بازی مهیج تری به میدان بیاید، یا مثلاً دستورالعملی برای گذراندن مراحل آن بازی منتشر شود، که همه بتوانند به سادگی با استفاده از آن دستورالعمل، مراحل را بگذرانند، و یا اصولاً این بازی در سیستم عاملهای رایانه‌ها و گوشی‌های نسل جدید اجرا نشود، تمام حسابهای کاربری‌ای که خرید و فروش می‌شدند، ناگهان بی اعتبار و بی ارزش می‌شوند.

آن بسته‌های رمزگذاری شده پوچ مالی هم که حالا می‌توانیم اسم رمز ارز^{۱۳} را برای آن بگذاریم، وضعیتی مشابه دارند. تا زمانی که تقاضا و اقبال افراد به خرید آن وجود دارد، ارزش پیدا می‌کنند. اما اگر به هر دلیل این اقبال از بین برود، ارزش آن کاسته شده یا حتی در شرایطی به سرعت به “هیچ” تنزل می‌کند. شما با پدیده‌ای مواجهید که چهار بار متتزع شده است. اما هنوز واقعیت دارد، و به کار می‌آید.

حال باید دید، این بسته‌های هیچ، چگونه حاکمیت و حکمرانی را درگیر چالش می‌کند.

در بخش بعدی این یادداشت، در مورد پیچیدگی و بعضاً مخاطرات این پدیده، و نوع تاثیرگذاری آن در حاکمیت در تمدن سایبری، بیشتر صحبت می‌کنیم.

منابع

(شامل مراجع استفاده شده در بخش اول و دوم یادداشت)

(اتاق بازرگانی صنایع ایران و فرانسه، ۹۸). اتاق بازرگانی صنایع ایران و فرانسه. گزارش: دنیای رمزارزها چه خصوصیاتی دارد؟ مهر ۹، ۱۳۹۸، <https://bit.ly/2T4XryY>.

(بانک مرکزی، ۹۷). بانک مرکزی جمهوری اسلامی ایران، الزامات و ضوابط حوزه رمزارزها، ۱۳۹۷.

(تفقدی، ۲۰۱۳). حسین تفقدی اسراری، تاریخچه پول و روند تکامل آن؛ تاریخ پژوهی، دوره (۱۵)، شماره (۵۴)، سال (۲۰۱۳-۶)، صفحات (۱۱۵-۱۳۲).

(زمانی و دیگران، ۹۸). دسته بندی، مقایسه و تحلیل پلتفرم‌های زنجیره بلوکی از منظر کاربر نهایی؛ زمانی سیما، معز کریمی زهرا، گل میرزایی زهرا؛ کنفرانس بین المللی وب پژوهی، جهاد دانشگاهی دانشگاه علم و فرهنگ، ۱۳۹۸.

(سلیمانی و دیگران، ۹۶). بررسی فقهی پول مجازی، محمد مهدی سلیمانی پور ۱ حامد سلطانی نژاد ۲ مهدی پورمطهر ۳، تحقیقات مالی اسلامی، دوره ۶، شماره ۲ - شماره پیاپی ۱۲، بهار و تابستان ۱۳۹۶.

(سیاه بیدی و محبی، ۹۸). تأثیر ارز دیجیتال بر مقررات ارز (پول) سنتی، سعید سیاه بیدی کرمانشاهی ۱ رضا محبی ۲، پژوهشنامه حقوق فارس، دوره ۲، شماره ۲ بهار ۱۳۹۸.

(قدیری نژادیان و کریمی، ۹۵). محسن قدیری نژادیان، فائزه کریمی؛ چشم انداز بانکداری به مثابه پلتفرم، و الزامات؛ ششمین همایش سالانه بانکداری الکترونیک و و نظامهای پرداخت، دی ۱۳۹۵.

(مولانا، ۸۸). بزرگ‌ترین کلاهبرداری تاریخ؛ مسیح مولانا؛ ۳۰ فروردین ۱۳۸۸، نقل از وطن امروز.

(هدایتی، ۸۳). هرودوت، تاریخ هرودت. ترجمه با مقدمه و توضیحات و حواشی از هادی هدایتی. تهران: انتشارات دانشگاه تهران، ۱۳۸۳.

(هوا و جعفری مذهب، ۸۶). پول کاغذی در دوره مغولان چین، لو هوا، محسن جعفری مذهب، بررسی‌های نوین تاریخی سال سوم بهار ۱۳۸۶ شماره ۳.

(Baldoni, 2018). Baldoni, Sarina. "Cryptocurrencies: Myth vs. Reality." (2018).

(Bratspies, 2018). Bratspies, Rebecca M. "Cryptocurrency and the Myth of the Trustless Transaction." Mich. Tech. L. Rev. 25 (2018): 1.

(Cheung & Lee, 2010). Cheung.C.M,& Lee.M.K.. A theoretical model of intentional social action in online social networks; Decision Support Systems, 49, 2010, 2430.

- (Christofides et al. 2009). Christofides, E., Muise, A., & Desmarais, S. Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *CyberPsychology & Behavior*, 2009, 12(3), 341-345.
- (Chum et al. 1990). David Chum ;Amos Fiat ; Moni Nmr ; Untraceable Electronic Cash; S. Goldwasser (Ed.): *Advances in Cryptology - CRYPTO '88*, LNCS 403, pp. 319-327, 1990.
- (Chum, 1983). Chaum David; 1983; Blind Signatures for Untraceable Payments. In: Chaum D., Rivest R.L., Sherman A.T. (eds) *Advances in Cryptology*. Springer, Boston, MA; Archived in <https://bit.ly/2Ta7l2n> .
- (Economist, 2015). The Economist explains: Who is Satoshi Nakamoto? Nov 3rd 2015, 5:47 from The Economist explains.
- (Euromoney, 97). Euromoney Report: EMERGING MARKETS ASIA- Asian financial crisis: When the world started to melt By: Published on:Monday, December 01, 1997.
- (Folkerts et al. 2003). An Essay on the Revived Bretton Woods System; Michael P. Dooley, David Folkerts-Landau, Peter Garber; NBER Working Paper No. 9971; Issued in September 2003
- (Law et al. 1996). Laurie Law, Susan Sabett, Jerry Solinas ; "How To Make A Mint: The Cryptography of Anonymous Electronic Cash"; National Security Agency Office of Information Security Research and Technology- Cryptology Division; 18 June 1996
- (Lemieux, 2013). Lemieux, Pierre.Regulation; Washington Vol. 36, Iss. 3, (Fall 2013): 14-15.
- (Mason & Asher, 1973). Edward S. Mason and Robert E. Asher, "The World Bank Since Bretton Woods: The Origins, Policies, Operations and Impact of the International Bank for Reconstruction". Washington DC: Brookings Institution, 1973, 29.
- (Melanie, 2015). Swan, Melanie. *Blockchain: Blueprint for a new economy*. "O'Reilly Media, Inc.", 2015.
- (Østbye,2018). Østbye, Peder. "Model Risk in Cryptocurrency Governance Reliability Assessments." Available at SSRN 3195686 (2018).
- (Ramadani et al. 2018). Sejfuli-Ramadani, Nexhibe and Ramadani, Erenis and Idrizi, Florim and Misimi, Verda (2018) *Blockchain: General overview of the*

Architecture, Security and Reliability. Journal of Natural Sciences and Mathematics of UT, 3 (5-6). pp. 64-68. ISSN 2671-3039

(Taskinsoy, 2018). Taskinsoy, John. "Bitcoin Mania: An End to the US Dollar's Hegemony or another Cryptocurrency Experiment Destined to Fail?." Available at SSRN 3311989 (2018).

(Wallace, 2018). BENJAMIN WALLACE; "The Rise and Fall of Bitcoin". WIRED. Retrieved April 13, 2018.

(Zibin, et al. 2018). Zheng, Zibin; Hong-Ning Dai; Xiangping Chen, Huaimin Wang; "Blockchain challenges and opportunities: A survey." International Journal of Web and Grid Services 14.4 (2018): 352-375.

^۱ - از جمله در این مورد نگاه کنید به (شهاب، ۵۱). البته دیدگاههای دیگری هم وجود دارد. از جمله به نوشته هرودت، مردم لیدیا اولین کسانی بودند که به استفاده از سکه نقره روی آوردند. (هدایتی، ۸۳)

^۲ - <https://en.wikipedia.org/wiki/Money>

^۳ - (هوا و جعفری مذهب، ۸۶). همچنین در مورد تاریخچه پول نگاه کنید به (تفقدی، ۲۰۱۳).

^۴ - Abstract

^۵ - که برای اشخاص صرف می کند که سکه ها را از بازار جمع آوری و به مواد خام آن تبدیل کنند. این اتفاق در تاریخ بارها افتاده، و حتی در کشور خودمان در سالهای جاری نیز چنین وضعیتی وجود دارد. از جمله در این مورد نگاه کنید به گزارشهای تابناک <https://tabnak.ir/003Uwa> و روزنامه جام جم، یکشنبه ۲۵ شهریور ۱۳۹۷، شماره ۵۲۰۳، در <https://www.magiran.com/article/3803216>

^۶ - Fiat Currency

^۷ - Bretton Woods

^۸ - از جمله در این مورد نگاه کنید به (Mason & Asher, 1973)، (Folkerts et al. 2003) و (مولانا، ۸۸).

^۹ - البته صرفنظر از مسئله وجود آن مقدار پول نقد در آن شعبه.

^{۱۰} - Account

^{۱۱} - حساب کاربری فقط یک شناسه و کلمه عبور است که به صورت دو عبارت انتخاب شده توسط صاحب حساب شناخته می شود. خرید حساب کاربری یعنی اینکه او این دو عبارت را به شما بدهد، و شما مبلغی را به او بدهید.

^{۱۲} - مثلاً در مورد بازی clash of clans. این اتفاق شاید برای من و شما که احتمالاً اهل بازی رایانه ای نیستیم، قابل فهم نباشد. به من اگر پول هم بدهند، حاضر نیستم وقتم را صرف یک بازی رایانه ای کنم؛ چه رسد به اینکه برای مرحله بعدی آن پول بدهم. اما کسی که غرق آن شده، و به آن اعتیاد پیدا کرده است، همانند یک معتاد مواد مخدر، برای دریافت اثرات تخریبی مراحل بالاتر بازی، این کار را می کند.

^{۱۳} - Cryptocurrency