

بسم الله الرحمن الرحيم

تمدن در گذار

رمزارز پیچیده در پرده عدم قطعیت

اردوان مجیدی

مرداد ۹۹

تزلزل رمزارزها و رمزآلودگی آن، در کنار کاربردهای موثر آن، واقعیت‌هایی است که در مقابل جامعه و حکومت قرار دارد. رمزارزها، میدان بازی متفاوتی از حاکمیت و حکمرانی را پیش روی جامعه و حکومت قرار می‌دهند. جامعه و حکومت، ناخواسته درگیر یک تصمیم‌گیری و میدان پیچیده شده است، که باید آن را در معادلات خود لحاظ کند.

کلمات کلیدی: رمزارز، تمدن سایبری، حاکمیت و حکمرانی در تمدن سایبری، اقتصاد سایبری، عدم قطعیت، پیچیدگی، جوسازی فناورانه، اردوان مجیدی

در سلسله یادداشت‌هایی، به تحلیل ابعادی از تحول و چالش‌های این تمدن سایبری می‌پرداختیم. این سومین یادداشت از این مجموعه است. در یادداشت قبلی به عنوان یک نمونه از مسائل حاکمیت و حکمرانی در تمدن سایبری،

به مسئله رمزارز پرداختیم. در تبیین ماهیت رمزارز، دیدیم که رمزارز، در پس چند بار انتزاعی شدن مکرر، ارزش انتزاعی‌ای را در میدان جامعه به جریان می‌اندازد. بحث را در این یادداشت دنبال می‌کنیم.

رمزارزهای ذومراتب متنوع ذوفنون

در سال ۱۹۸۳ و پس از آن در سال ۱۹۹۰، دیوید شام^۱، طی دو مقاله، تبیینی از دو نوع پول مجازی را که امکان دنبال کردن معاملات آن وجود ندارد، با عناوین ای کش و دیجی کش، انجام داد^۲. در سال ۱۹۹۶ یک گزارش با عنوان «چگونه یک ضرابخانه بسازیم: رمزنگاری پول‌های الکترونیکی گمنام» توسط کارشناسان آژانس امنیت ملی آمریکا منتشر شد^۳. اما عملاً اولین رمزارز غیرمتمرکز در سال ۲۰۰۹ به نام بیت‌کوین توسط شخصی با نام مستعار ساتوشی ناکاموتو ایجاد شد. ماجرای مرموز این فرد نیز جالب است. کسی او را نمی‌شناسد. فردی که خود را ساکن ژاپن معرفی می‌کند، اما دیگران از روی نوشته‌های و خصوصیات پیامها او، او را فردی انگلیسی زبان، ساکن آمریکا می‌دانند. او در سال ۲۰۱۰ کاملاً مخفی شد و هیچ تعاملی از این تاریخ به بعد نداشته است^۴.

امروز انواع مختلفی از رمزارزها وجود دارند. رمزارزهایی که براساس زنجیره بلوکی^۵، توسعه بلوکهای رمزی آن توسط افراد مختلف انجام می‌شود^۶. یا می‌تواند توسط یک بانک یا موسسه راه اندازی و پشتیبانی و تامین اعتبار شود^۷، یا دارای پشتوانه طلا یا منابع ارزشی مشخص باشد^۸، یا رمزارزهای مبتنی بر سکوها^۹. هر کدام از این رمزارزها، مراتب مختلفی از انتزاع مورد بحث را در بردارند. تا کنون حدود ۲۰۰۰ رمزارز مختلف عرضه شده است.

رمزارزها مشخصه‌های زیادی دارند. اما آنچه که رمزارزها را جذاب و فراگیر کرده، ناشناس بودن، شفاف بودن سازوکارها (البته این شفافیت نسبی است)، فرامرزی بودن (و مسائل تراکنشهای بین المللی را آسان کردن)، ساده بودن معاملات (بدون تشریفات بانکهای موجود)، حل مشکل اعتماد یا بی اعتمادی به طرف مقابل، غیر قابل رهگیری بودن (مناسب برای فرار مالیاتی، فرار از تحریم، پولشویی، مشاغل غیر قانونی و نظایر آن) است^{۱۰}. البته یک دلیل برای گرایش به آن در سالهای گذشته هم، رشد ارزش آن بوده و افرادی به چشم بورس و سرمایه گذاری در بورس به آن نگاه می‌کنند^{۱۱}.

رمزارزها در پرده عدم قطعیت

ما هنوز در اولین روزهای استفاده از رمزارز قرار داریم، و هنوز ابعاد مختلفی از عدم قطعیت در مورد آن وجود دارد. اینکه چگونه رمزارزها ارزش گذاری شوند، به تصورات، فضا سازی‌های رسانه‌ای و شبکه‌های اجتماعی، هیجانات و عوامل مختلف دیگر بستگی دارد، و شکل گرفتن ارزشهای حبابی اتفاقی دور از انتظار نیست. همچنین سازوکارهای حکمرانی و مدیریت رمزارزها، نه هنوز به صورت کامل شناخته شده و معماری آن تبیین شده و شفاف

است، و نه هنوز ایجاد شده، و مسائل قانونی و ابعاد آن خلاءهای فراوانی دارد. حتی مسائل فنی آن هم به نظر من ابهامات فراوانی دارد، که در بسیاری از موارد افراد به آن توجه نمی‌کنند.^{۱۲}

درست است که از نظر سازوکارهای نظری، توضیحاتی در مورد قابلیت اطمینان آن داده می‌شود؛ اما فکر می‌کنم هنوز ابعاد ناشناخته‌ای در آن وجود دارد. یک سوی این ماجرا، ابهام و رمز آلود بودن ساختار و محتویات آن است. همان اتفاقی که در تعداد زیادی از نرم افزارهای متن باز می‌افتد، اینجا هم مصداق دارد. نرم افزارهای متن باز^{۱۳} نرم افزارهایی هستند که تمام متن نرم افزار را در اختیار استفاده کنندگان قرار می‌دهند. برخلاف نرم افزارهای معمولی که به صورت یک بسته کد شده در اختیار کاربران قرار می‌گیرد، و کاربران نمی‌توانند بدانند که در آن نرم افزار چه اتفاقی می‌افتد، و چگونه عملیات انجام می‌شود، نرم افزارهای متن باز تمام جزئیات متن برنامه^{۱۴} را در اختیار کاربران قرار می‌دهد. نرم افزارهای متن باز این اعتماد را در کاربران ایجاد می‌کنند که بدانند از اطلاعات و عملکرد آنها توسط برنامه نویسان این نرم افزار، استفاده‌های سوء نمی‌شود. همچنین این امکان برای کاربرانی که خود توان برنامه نویسی دارند ایجاد می‌شود که بتوانند بخشهایی از نرم افزار را آنگونه که خود می‌خواهند، تغییر دهند، و نسخه‌ای از نرم افزار را به صورت ویژه گرا شده و وارث نرم افزار اصلی، ایجاد کنند.

تا اینجای ماجرا خیلی خوب به نظر می‌رسد. اما مسئله این است که در اختیار گذاشتن متن یک برنامه چند صد هزار خطی به معنای آن نیست که شما بتوانید از همه آن متن سر در بیاورید. به عنوان یک برنامه نویسی که تجربه چند میلیون خط برنامه نویسی و مدیریت تولید چندین نرم افزار کاربردی را داشته‌ام، می‌دانم که اگر برنامه نویس اولیه یک نرم افزار متن باز، بخواهد سازوکاری را در برنامه اش بگنجانند که هیچ کس از آن سر در نیاورد، کار دشواری نیست. ضمن اینکه قطعا در بسیاری از قسمتها، متن برنامه به توابعی ارجاع می‌دهد که این توابع در کتابخانه‌های بیرونی و خارج از دسترس هستند (که در برنامه نویسی به صورت فراوان از آنها استفاده می‌شود)، و برنامه نویس می‌تواند هر چه را که بخواهد کسی متوجه آن نشود، در این توابع جانمائی کند. به عبارت دیگر متن باز بودن یک برنامه به معنای کاملا شفاف بودن و عدم امکان سوء استفاده در آن نیست.

به همین صورت نیز رمز آلود بودن، علیرغم باز بودن منابع یک زنجیره بلوکی، به معنای این نیست که این زنجیره از اختیار آغاز کننده آن خارج شده، و هیچگونه ابهامی در آن و احتمال فروپاشی آن وجود ندارد. تقریبا با هر کسی که در زمینه رمزارز فعالیت کاربردی یا تخصص تولیدی دارد صحبت کردم، چه آن کاربران و چه حتی آن تولید کنندگان، نتوانستند به تمام سوالاتی که از آنها پرسیدم پاسخ کامل و قاطع بدهند. مقالات و متون تخصصی هم که در این زمینه وجود دارند، همیشه در نقاطی به تبیین موضوعاتی می‌رسند که در آنجا روشن نیست، و به متون دیگر حواله شده، و در آن متون دیگر هم همین نقاط خلاء به صورت بازگشتی وجود دارد. البته شاید این به دلیل کم سواد و

فهم اندک بنده باشد. مسئله آن است که من به صورت قاطع، وجود مشکل در ماهیت رمزارزها را اظهار نمی‌کنم، فقط اعلام می‌کنم که در مورد آن، حداقل هنوز در ذهن خودم، سطحی از عدم قطعیت وجود دارد. این عدم قطعیت را در تمام سطوح افراد درگیر نیز احساس کرده‌ام.

به عبارت دیگر **کاربران رمزارزها با درجه بالایی از عدم قطعیت نسبت به سازوکار از آن استفاده می‌کنند.** و تولیدکنندگان بلاکهای بعدی هم فقط الگوریتمهایی را می‌شناسند که می‌توانند بلاک جدیدی را طبق روال مشخصی به زنجیره اضافه کنند، یا اعتبار یک بلاک مشخص را مورد سنجش قرار دهند؛ و حداقل با افرادی که من از آنها پرس و جو کردم، جوهری از ماجرا برای آنها نیز مبهم و ناشناخته بود. افراد متخصص نظری حوزه رمزنگاری نیز از منطق توابع و رمزگذاری صحبت می‌کنند، اما تا الان توضیح قانع کننده ای برای تبیین قطعیت کل سیستم نشنیده‌ام. بسیاری از استنادات به سرعت پردازشگرهای موجود و ممکن و حجم محاسبات بر می‌گردد، که آن هم به نظرم لایتغیر نیست.

حتی افرادی که در سطح راهبردی اقتصادی در مورد رمزارزها اظهار نظر می‌کنند، و من با آنها گفتگوی مختصری داشتم، به جوانب فنی و رمزهای پشت الگوریتمها و سازوکارهای رمزارز، آگاهی کاملی ندارند، و فقط به اظهارات متخصصان فنی رمزارز و رمزنگاری، اعتماد کرده‌اند. هر چند که مطمئن هستم به دلیل این اظهار نظری که اینجا می‌کنم، از سوی طیفهای مختلف متخصصان و مدافعان و کاربران رمزارز، مورد هجوم قرار می‌گیرم؛ اما واقعیت این است که فکر می‌کنم، **هنوز ابهامات زیادی در مسئله زنجیره بلوکی رمزارزها وجود داشته باشد، که بخشی از آن با چیزی که من "جوسازی فناورانه" می‌نامم، در هیاهوی مسائل فنی و هیجانات کاربری، گم می‌شود.**

خطر در کمین

فارغ از امکان فروپاشی فنی رمزارزها، رمزارزها از نظر بدون پشتوانه بودن، و تزلزل تقاضا در رقابت و رشد حبابی، منابع پرخطری هستند. با توجه به افزایش سطح انتزاع به پول متعارف، ریسک رمزارزها بیشتر و پیچیده‌تر است. وابسته شدن اقتصاد یک کشور در این فضای پر ریسک، خطری شدیدتر از آنچه که در بحرانهای تزلزل پول متعارف گریبانگیر کشورها شد را در پی دارد.

در دورانهای مختلف، کشورهای مختلف درگیر بحرانهای شدیدی به واسطه تغییر ناگهانی ارزش پول خود شدند. کشورما در سالهای اخیر، چند بار این را تجربه کرده. اما شاید به عنوان بهترین مثال بتوان از کشورهای آسیای جنوب شرقی (آسه آن) در سال ۱۹۹۷ نام برد^{۱۵}. اقتصاد حبابی، تکیه بر پول بدون پشتوانه، نقش تعیین کننده دلار در

اقتصاد کشورها و وابستگی به تبادلات دلاری، و بازی آمریکا با دلار بدون پشتوانه، بحرانهای زیادی را در اقتصاد بین المللی ایجاد کرده است.

اگر بحرانهای قبلی چند روزه می توانست اقتصاد یک کشور یا یک منطقه را نابود کند، بحرانهای رمزارزها ممکن است در چند ثانیه چنین فاجعه‌هایی را با شدت بیشتر رقم بزند. تصور کنید که بخش قابل توجهی از منابع اقتصادی بنگاهها و بانکهای یک کشور، بر رمزارزی قرار داشته باشد، و در یک اتفاق به هر دلیل (مثلا فروپاشی فنی، یا فروپاشی ارزش حسابی) آن رمزارز کاملاً از گردونه مبادلات خارج شود. تمام سرمایه آن بنگاهها و بانکها، در عرض چند ثانیه به صفر تبدیل خواهد شد. و این می تواند اقتصاد یک کشور را فلج یا ورشکست کند.

رمزارزها اما به کار می آیند

اما علیرغم تمام تزلزله‌ها و عدم قطعیتی که از آن صحبت کردیم، رمزارزها به کار می آیند. می توان در شبکه‌های غیر بانکی آن را جابجا کرد. در طیفی از آنها می توان مبادله به گونه ای انجام شود که ردگیری آن بسیار دشوار (و به ادعائی، غیر ممکن) باشد. این برای ناشناس ماندن خریدار و فروشنده در مبادلات غیر مشروع و پول شوئی یا مبادلاتی که برای مبارزه با یک نظام مالی - سیاسی انجام می شود (نظیر تحریمها علیه یک کشور) قابل استفاده خواهد بود. می توانید رمزارز را تقریباً به سادگی با پول نقد یا الکترونیکی رایج در کشورها مبادله کنید؛ حتی در برخی کشورها، دستگاههای خودپرداز برای این کار ایجاد شده است.^{۱۶} رمزارزها می تواند حتی ابزاری برای شکستن هژمونی دلار باشد.^{۱۷}

میدانی پیچیده، پیش روی مردم و حاکمیت

اما فارغ از عدم قطعیتی که از آن صحبت کردیم، واقعیت این است که در پارادایم تمدن سایبری، استفاده از رمزارزها، اجتناب ناپذیر است. اما اینکه در کجا و چه شرایطی از آن استفاده کنیم؟ چقدر از منابعمان را به صورت رمزارز مبادله کنیم، و چقدر از آن را با پولهای سنتی؟ چه مدت آن را به صورت رمزارز نگه داریم؟ چگونه رمزارزها و اقتصاد آن را فهم کنیم؟ چه نوع رمزارزی را انتخاب کنیم؟ چگونه فضای رمزارزها را مدیریت کنیم؟ چه مقرراتی برای استفاده از آن داشته باشیم؟ و سوالاتی از این دست، سوالاتی است که یک اقتصاد جامعه و ساختار حکومتی، در تعامل با رمزارز، پیش روی خود دارد. حداقل در شرایط کنونی، خریدن رمزارز به عنوان یک سرمایه دراز مدت کار غیرمنطقی‌ای به نظر می رسد؛ مگر برای کسی که سرمایه گذاری بسیار پر ریسک و قمارگونه‌ای را دنبال می کند. شاید منطقی باشد که امروز رمزارز را فقط برای تبادل

روزمره و محدود، و عبور دادن منابع در یک میدان استفاده کرد. اما بالاخره رمزارزها یک واقعیتند، که باید در معادلات خود آنها را ببینیم.

تزلزل رمزارزها و رمزآلودگی آن، در کنار کاربردهای موثر آن، واقعیت‌هایی است که در مقابل جامعه و حکومت قرار دارد. رمزارزها، میدان بازی متفاوتی از حاکمیت و حکمرانی را پیش روی جامعه و حکومت قرار می‌دهند. جامعه و حکومت، ناخواسته درگیر یک تصمیم‌گیری و میدان پیچیده شده است، که باید آن را در معادلات خود لحاظ کند.

رمزارزها، **پارادایم جدیدی را پیش روی حاکمیت** قرار می‌دهند. اگر حاکمیت پیش از این، در تعیین چرخه ارزش پول در نظام اقتصادی خود، نقش تعیین‌کننده و محوری داشت، امروز در شرایطی قرار می‌گیرد، که این چرخه تا حد زیادی، از حیطه اختیار و اقتدار او خارج می‌شود. **نظیر آنچه در بسیاری از حوزه دیگر نیز در تمدن سایبری، اتفاق می‌افتد.** حاکمیت در پهنه رمزارزها به چالش کشیده می‌شود.

در عین اینکه رمزارزها هر لحظه امکان فروپاشی دارند، اما در عین حال منابع و اعتماد عمومی را به خود جذب می‌کنند، و اقتصاد جامعه را به شدت درگیر خود می‌کنند. جریان متزلزل از یک سو، و پنهان از سوی دیگر را در پهنه اقتصادی جامعه ایجاد می‌کنند، که جامعه را به سمت یک اقتصاد متزلزل و آشفته، که عوامل پنهان فراوانی پشت آن وجود دارد سوق می‌دهد. عواملی که یکی از آنها، برای فروپاشی و شکست جبران‌ناپذیر اقتصادی یک جامعه و حاکمیت آن، کافی خواهد بود. **بازی رمزارزها** بازی پیچیده و دشواری را پیش روی حاکمیت و جامعه قرار داده است. تغییر میدان بازی، ورود به آن را اجتناب‌ناپذیر کرده است. **جذابیت‌های** آن آنچنان **دلفریب** است که هر دوی آنها به زحمت می‌توانند خود را از وسوسه آلوده شدن به آن، حفظ کنند. ولی در پشت این چهره دلفریب، ممکن است **هزار چهره متفاوت و بعضاً هولناک**، در میدان بازی جلوی چشمان بازیگران ظاهر شود.

مسئله اصلی این است که **حاکمیت برای حفظ اقتدار خود در این میدان، باید پارادایم جدید را فهم کند، سازوکارهای حکمرانی متفاوتی را اتخاذ کرده، و محاسبات خود را متناسب با معادلات این پارادایم انجام دهد.** میدان جدید، قواعد متفاوتی دارد، و بازی جدیدی در آن در حال وقوع است.

در این یادداشت و یادداشت قبل در مورد رمزارزها، و پیچیدگی و راز و رمز آنها در فضای تمدن سایبری سخن گفتیم. هدف ما تبیین نمونه ای از مسائل حاکمیت در فضای تمدنی جدید بود. بحث در مورد تمدن سایبری و حاکمیت در آن را در یادداشت‌های بعدی، دنبال می‌کنیم. ان شاء الله. الحمد لله رب العالمین.

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 خصوصیتی 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 - David Chaum

^۲ - (Chum, 1983) و (Chum et al. 1990).

^۳ - (Law et al. 1996).

^۴ - در این مورد از جمله نگاه کنید به (Lemieux, 2013)، (Economist, ۲۰۱۵) و (Wallace, ۲۰۱۸).

^۵ - Blockchain. به زبان ساده یک نوع سیستم ثبت اطلاعات و گزارش است، که اطلاعات ذخیره شده میان همه اعضای یک شبکه به اشتراک گذاشته می شود. اطلاعات به صورت تکه ها یا بلوک هایی مستقل ایجاد می شود، که یک دفتر کل توزیع شده با مدیریت نامتمرکز (تقریباً اینگونه که کپی این دفتر کل نزد همه باشد یا همه بتوانند به سادگی به آن دست پیدا کنند)، سوابق آن بلوکها را نگهداری میکند. در این مورد نگاه کنید به (زمانی و دیگران، ۹۸)، (Zibin et al ۲۰۱۸)، (Melanie, ۲۰۱۵). همچنین برای آشنائی با زبان ساده نگاه کنید به <https://arzdigital.com/what-is-blockchain-technology>.

^۶ - نظیر بیت کوین Bitcoin یکی از متداولترین رمزارزهای موجود.

^۷ - نظیر Central Bank Crypto-Currency CBCC - طبق ضوابط بانک مرکزی. از جمله نگاه کنید به (بانک مرکزی، ۹۷). مثال دیگر پترو (Petro) رمزارز بومی کشور ونزوئلا است. البته از یک منظر اگر یک رمزارز توسط یک بانک و با ضوابط یک بانک عمل کند، دیگر رمزارز نیست و فقط یک پول الکترونیکی است. مگر آنکه فقط پشتوانه بودن آن توسط بانک مذکور تامین شده، و سایر خصوصیات مبادله ای رمزارزها را داشته باشد.

^۸ - نظیر دیجیکس داثو DigixDAO با پشتوانه طلا، از جمله نگاه کنید به <https://bit.ly/2T3P5rg> و <https://arzdigital.com/coins/digixdao>.

^۹ - نظیر آتریوم Ethereum. از جمله نگاه کنید به <https://ethereum.org>.

^{۱۰} - از جمله نگاه کنید به (سلیمانی و دیگران، ۹۶)، (سیاه بیدی و محبی، ۹۸)، (اتاق بازرگانی صنایع ایران و فرانسه، ۹۸)، (Taskinsoy, 2018)،

<https://vrgl.ir/z8bKW>.

^{۱۱} - برای مشاهده به روز بورس ارزش در حال تغییر ۱۰۰ رمزارز متداول (از بین ۲۰۰۰ رمزارز موجود تا کنون) نگاه کنید به:

<https://coinmarketcap.com>.

^{۱۲} - از جمله در این مورد نگاه کنید به (Østbye, 2018)، (Ramadani et al. 2018)، (Bratspies, 2018) و (Baldoni, 2018).

^{۱۳} - OpenSource

^{۱۴} - Source

^{۱۵} - از جمله در این مورد نگاه کنید به (Euromoney, ۹۷).

^{۱۶} - از جمله نگاه کنید به (اتاق بازرگانی صنایع ایران و فرانسه، ۹۸)

^{۱۷} - در این مورد نگاه کنید به (Taskinsoy, ۲۰۱۸).