به نام خدا

پروژه کارشناسی علوم کامپیوتر

استاد راهنما: دکتر میرزایی

نویسنده: میکاییل مایلی فریدنی

موضوع: بیت‌کوین و بلاک‌چین، از دید اقتصاد و علوم کامپیوتر

فهرست:

مقدمه: ۳

بیت‌کوین: سیستم پولی غیرمتمرکز ۴

بلاک‌چین: زیرساخت اصلی بیت‌کوین ۹

تراکنش‌ها و نمایش آن‌ها در بلاک‌چین ۱۱

فرایند ماینینگ و الحاق بلوک‌های جدید به زنجیره ۱۳

اعمال تغییرات در کد بلاک‌چین: هاردفورک و سافت‌فورک ۱۶

دیگر بلاک‌چین‌ها و نگاهی به آینده ۱۸

مطالعه بیشتر و منابع ۲۱

مطالعه بیشتر ۲۱

منابع ۲۱

مقدمه:

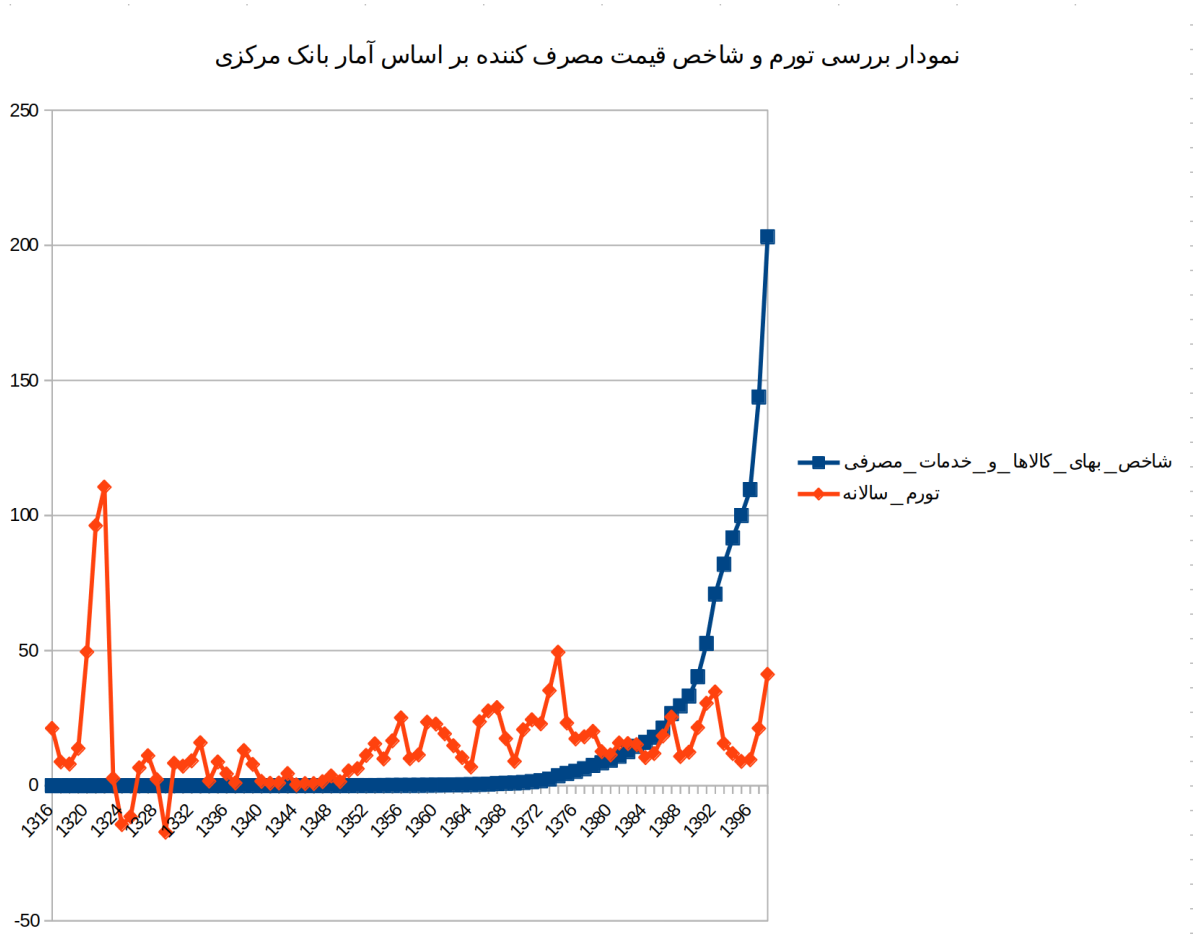
پس از تلاش‌های نافرجام دانشمندان علم رمزنگاری و علوم‌کامپیوتر برای ساخت یک پول دیجیتال، در سال ۲۰۰۹ فردی با نام مستعار ساتوشی ناکاموتو[1] مقاله‌ای را منتشر کرد که در آن با شرح یک سیستم پول دیجیتال نقطه به نقطه[2] مشکلات مربوط به ساخت و توزیع یک ارز دیجیتال را حل کرده بود. طبیعتا این موضوع از دو وجه قابل بررسی است. یک دید اقتصادی که در آن به پارامترها و تاثیرات اقتصادی این ارز دیجیتال پرداخته شود و یک دید علوم کامپیوتری که در آن به بررسی مشکلات و راه‌حل‌هایی که در این سیستم ارائه شده پرداخته شود.

در این مقاله نخست بیت‌کوین را از دید اقتصادی بررسی کرده و سپس آن را از دید علوم‌کامپیوتر بررسی می‌نماییم و در آخر آینده این فناوری و سیستم‌های جایگزین را معرفی خواهیم کرد.

1 Satoshi Nakamoto
2 Peer-to-Peer

بیت‌کوین: سیستم پولی غیرمتمرکز

به نمودار زیر توجه کنید:



شکل ۱ نمودار CPI و Infilation (با استفاده از داده‌های بانک مرکزی)

این نمودار بر اساس داده‌های بانک مرکزی جمهوری اسلامی ایران[3] (وبسایت بانک مرکزی جمهوری اسلامی ایران و خبرگزاری فارس)، بیانگر تورم سالانه و شاخص بهای کالاها و خدمات مصرفی است. برای درک بهتر این نمودار به تعریف این دو مفهوم می‌پردازیم:

شاخص بهای کالاها و خدمات مصرفی[4]: شاخص بهای کالاها و خدمات مصرفی بیانگر هزینه کلی کالاها و خدماتی است که یک مصرف‌کننده عام خریداری می‌کند.(Mankiw, 2017, p.496)

3 داده‌های سال‌های ۱۳۱۶ تا ۱۳۹۶ در سایت بانک مرکزی موجود است اما به دلیل دستور رئیس جمهور مبنی بر عدم انتشار این اطلاعات از سال ۱۳۹۶ به بعد، داده‌های دو سال ۱۳۹۷ و ۱۳۹۸ بر اساس نامه رییس بانک مرکزی به رییس قوه قضاییه موجود در خبرگزاری فارس نوشته شده است.

4 CPI(Consumer Price Index)

نرخ تورم: تورم با استفاده از شاخص بهای کالاها و خدمات مصرفی و به شکل زیر محاسبه می‌شود: (Mankiw, 2017, p.497)

$$YearlyInflationRate = \frac{CPI_{Year1} - CPI_{Year2}}{CPI_{Year1}} * 100$$

اهمیت طلا، مسکن، نقره و دیگر نگهدارنده‌ارزش‌ها به همین علت است. این دسته از کالاها به علت مقبولیتی که برای یک جامعه دارند و تولید آن‌ها به علت قوانین طبیعت محدود است، در نظام‌های پولی که از تورم رنج می‌برند یا برای افرادی که می‌خواهند دارایی‌های خود را از تصمیمات بانک مرکزی حفظ کنند، گزینه‌های مناسبی هستند. مهم‌ترین علت این موضوع، عدم امکان دخالت بانک مرکزی، در تعیین قیمت یا ارزش این دسته از کالاهاست.

مقاله اصلی بیت کوین در سال ۲۰۰۸ منتشر شد و با حل مشکلات مهمی که تا آن زمان از موفقیت ارزهای دیجیتال جلوگیری کرده بود (از مهمترین مشکلات حل همزمان غیرمتمرکز بودن و عدم امکان حمله دابل اسپندینگ است که بعداً به آن میپردازیم)، توانست نوع جدیدی از پول را خلق کند که خارج از کنترل بانک‌های مرکزی است و به سهولت توسط کاربران قابل استفاده است.

قبل از بیت‌کوین تلاش‌های زیادی برای ارائه یک ارز دیجیتال برای استفاده در شبکه جهانی وب[5] شده بود. یکی از مهمترین تلاش‌ها برای تولید چنین ارزی توسط دیوید چاوم[6] انجام شد. ایده این ارز دیجیتال که دیجی‌کش[7] نام داشت به این صورت بود: (A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, 2016)

۱. سیستم تولید پول، برای خلق پول جدید درخواست یک سریال از منحصربفرد از متقاضی می‌کند،
۲. متقاضی سریال را ارائه می‌دهد،
۳. سریال ارائه شده در پول ثبت می‌شود و توسط سیستم امضا می‌شود،
۴. حال برای هر بار استفاده از این پول، گیرنده از شما می‌خواهد که یک رشته رندوم از رشته امضا شده روی پول خود را رمزگشایی کنید تا وی بتواند در سیستم تحویل پول، این سریال را تحویل داده و ثابت کند آن را از شخص شما تحویل گرفته است و معادل آن دلار دریافت کند. در سیستم دیجی‌کش پرداخت کنندگان ناشناس می‌مانند اما اطلاعات دریافت کنندگان در سیستم می‌ماند.

---

5 Wrold Wide Web
6 David Chaum
7 Digicash

یکی از مشکلات اساسی دیجی‌کش عدم امکان پرداخت بین کاربران بود. درواقع دیجی‌کش تنها برای خرید مشتری از فروشندگان آنلاین طراحی شده بود. این باعث شد دیجی‌کش به علت عدم حمایت فروشگاه‌ها ازین سیستم به ورطه سقوط بیفتد. همچنین چاوم با پتنت کردن ایده‌های اصلی دیجی‌کش امکان پیشرفت و بهبود آن از سمت جامعه کاربران، برنامه‌نویسان و دانشمندان خارج از شرکت خود را گرفت.(Narayanan et al., 2016)

دیجی‌کش با اینکه در سال ۲۰۰۱ ورشکست شد، اما ایده‌های مهمی را در زمینه کریپتوکارنسی[8]ها مطرح و جزو اولین شرکت‌هایی بود که در این زمینه به شکل تجاری فعالیت کرد.(Narayanan et al., 2016)

در کنار دیجی‌کش، یک انجمن متشکل از علاقه‌مندان به این فناوری به نام سایفرپانک شکل گرفت که افراد حاضر در آن مایل به توسعه یک پول دیجیتال مانند دیجی‌کش بودند. جالب است بدانید که هشت سال بعد ساتوشی ناکاموتو[9] خود عضوی از این انجمن بود و طرح اولیه بیت‌کوین را برای اعضای این انجمن ارسال کرد. سه نفر از اولین توسعه‌دهندگان مهم بیت‌کوین به غیر از ساتوشی، هال فینی[10]، نیک زابو[11] و وی دای[12] بودند. .(Narayanan et al., 2016) از سال ۲۰۰۹ که اولین نود شبکه بیت‌کوین اجرا شد تا به امروز قیمت بیت‌کوین تغییرات زیادی داشته است، اما چه چیز باعث ارزشمند شدن بیت‌کوین می‌شود؟

---

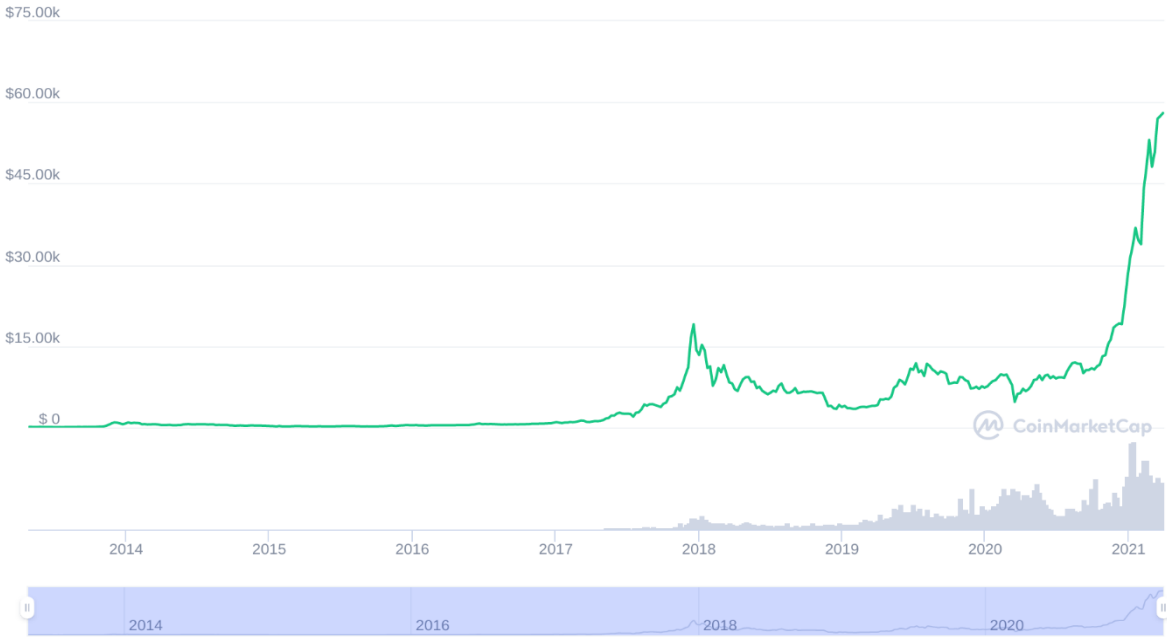
8 Cryptocurrencies

۹ Satoshi Nakamoto – اسم مستعار خالق بیت‌کوین است که کسی از هویت او خبری ندارد

۱۰ Hal Finney – یک برنامه نویس بسیار ماهر بود که به توسعه بیت‌کوین بویژه در مراحل اولیه بسیار کمک کرد.

۱۱ Nick Szabo – یک دانشمند علوم کامپیوتر و مبدع ایده قراردادهای هوشمند و بیت گولد، یکی از ارزهایی که بیت کوین بر آن پایه‌گذاری شده، است.

۱۲ Wei Dai – یک مهندس کامپیوتر و سازنده ارز دیجیتال بی-مانی. کوچکترین جز ارز شکه اتریوم به افتخار او wei نام‌گذاری شده است.



شکل ۲ نمودار قیمت بیت‌کوین از سال ۲۰۱۳

نمودار فوق نشان دهنده قیمت بیت‌کوین از سال ۲۰۱۳ تا این لحظه ویرایش این مطلب است. با وجود ریزش شدید قیمت در سال ۲۰۱۸ (از مرز ۲۰۰۰۰ دلار به مرز ۵۰۰۰ دلار) بیت کوین امروزه تقریباً به عنوان یک ذخیره ارزش به شمار می‌رود. علت این موضوع بخاطر ویژگی‌های ذاتی‌ای است که در قوانین بیت کوین گنجانده شده است:

۱. محدودیت عرضه: به علت شیوه تولید بیت‌کوین، تنها حدود ۲۱ میلیون از این رمزارز وجود خواهد داشت. این موضوع برخلاف سیستم ارزهای فیات[۱۳] است که امکان چاپ ارز رایج یک کشور در هر حجمی را برای بانک مرکزی آن کشور امکان‌پذیر می‌سازد. به همین علت عرضه محدود با افزایش سرمایه گنجانده شده در این بازار، قیمت این رمزارز روز به روز افزایش می‌یابد.
۲. عدم امکان سرقت: امکان دسترسی به سکه‌های یک حساب تنها و تنها با داشتن کلید خصوصی آن حساب ممکن است. بنابراین ازین جهت هر فرد می‌تواند با نگهداری کلید خصوصی خود در یک مکان امن، از امنیت حساب خودش مطمئن باشد و در هر زمان و مکان با وارد کردن کلیدهای خصوصی حساب خود، به سکه‌ها دسترسی داشته باشد.
۳. عدم امکان جعل: تمام تراکنش‌های بیت‌کوین در بلاک‌چین ثبت می‌شود. این موضوع به مشارکت‌کنندگان در این سیستم این امکان را می‌دهد تا به سهولت با بررسی بلاک‌چین از جعلی

13 Fiat Money

نبودن تراکنش مطمئن شوند. (برخلاف طلا و فلزات ارزشمند که نیاز به متخصص برای تعیین عیار و اصالت آن‌ها است.)

۴. امکان انتقال آنی: برخلاف طلا که نیاز به حمل فیزیکی برای انتقال از یک شخص به شخص دیگر دارد، انتقال مالکیت یک بیت‌کوین از یک حساب به حساب دیگر تنها با یک امضای دیجیتال قابل انجام است. این ویژگی باعث می‌شود هر کسی که به اینترنت متصل است بتواند به سهولت بیت‌کوین‌های خود را به شخصی در هر جای دنیا انتقال دهد.

۵. امنیت:با ثبت یک تراکنش در بلاک‌چین پس از گذشت ۶ بلاک آن تراکنش غیر قابل برگشت است (مگر اینکه شبکه تحت حمله ۵۱ درصد قرار بگیرد که در بخش‌های بعدی این موضوع را بررسی خواهیم کرد). این ویژگی باعث می‌شود پولی که به حساب شما واریز می‌شود توسط هیچ فردی به جز خود شما قابل برداشت نباشد.

۶. کارمزد کم: بلاک‌هایی که امروزه در بلاک‌چین ثبت می‌شوند، حجم قابل توجهی از سرمایه را با کارمزد بسیار پایین انتقال می‌دهند. این موضوع سیستم بیت‌کوین را گزینه بسیار مناسبی برای انتقال حجم‌های بزرگ پول می‌سازد.

۷. قراردادهای هوشمند[۱۴]: قراردادهای هوشمند به شبکه امکان تعریف اسکروها، چندامضایی ها و ... را می‌دهند که موجب ارائه راه‌حل‌های ساده برای مشکلات روزمره می‌شود.

این علل از جمله عواملی هستند که امروزه بیت‌کوین را به عنوان یک ذخیره ارزش و جایگزینی برای طلا مطرح می‌کند.

در ادامه به بررسی شبکه زیرساخت بیت‌کوین، یعنی بلاک‌چین می‌پردازیم.

Hash	00000000000000000029ce386c599cf970c9e14e36c60804f1d8d68cd36056d
Confirmations	1
Timestamp	2021-03-29 21:22
Height	676870
Miner	Unknown
Number of Transactions	2,583
Difficulty	21,865,558,044,610.55
Merkle root	d52a8046d5252f3607513ac326579210db7b2af9f1871adbfdc642bb72e5f917
Version	0x2000e000
Bits	386,719,599
Weight	3,993,171 WU
Size	1,279,362 bytes
Nonce	413,835,372
Transaction Volume	6716.10386240 BTC
Block Reward	6.25000000 BTC
Fee Reward	0.77082081 BTC

شکل ۳ جابه‌جایی ۴ میلیون دلار با تنها ۳۰ هزار دلار کارمزد

بلاک‌چین: زیرساخت اصلی بیت‌کوین

بلاک چین یک دفتر حسابرسی توزیع شده عمومی[15] است که تمامی تراکنش‌های انجام شده در شبکه بیت کوین در آن ثبت می‌شود. آنچه بلاک‌چین را از دیگر رقبای تاریخی خود متمایز می‌سازد، شیوه حل کردن مسئله دابل اسپندینگ[16] و ترکیب آن با ایده اثبات کار[17] برای رسیدن به یک اجماع در میان تمام دفاتر حسابرسی توزیع شده است.

مشکل دابل اسپندینگ هنگامی پیش می‌آید که یک سکه پرداخت شده مجدد توسط همان فرد اولیه به شخص دیگری پرداخت شود. برای مثال آرمین یک سکه دیجیتالی با کد"۱۲۳۴۵" دریافت می‌کند. او همین سکه را از طریق دو ایمیل به حسن و حسین می‌دهد. هر کدام از این دو نفر فکر می‌کنند که یک سکه منحصر به خود دریافت کرده‌اند، اما در صورت مواجهه با یکدیگر هیچ کدام نمی‌تواند اثبات کند که سکه متعلق به چه کسی است.

یکی از راهکارها برای حل این مشکل اتکا به یک سیستم متمرکز واسط است. این سیستم هر تراکنشی را رصد می‌کند و در صورت مشاهده یک دابل اسپند تنها یکی از تراکنش‌ها را تایید می‌کند.

مشکلات سیستم‌های این است که قدرت بسیار زیادی روی دارایی دیگران دارند. برای مثال می‌توانند دارایی‌های یک فرد را بلوکه کنند، از سرویس‌دهی به دسته‌ای از کاربران به علل مختلف خودداری کنند و ... . حال اگر بخواهیم این سیستم را غیرمتمرکز کنیم چه؟ چگونه می‌توان بدون اتکا به یک سیستم متمرکز مشکل تایید تراکنش‌ها را حل کرد؟

برای این منظور بیت کوین سیستم اثبات سهام را پیشنهاد می‌دهد:

فرض کنید در یک کلاس مدرسه، معلم می‌خواهد از بین دانش‌آموزان یک نفر را برای مبصری انتخاب کند. برای اینکار یک سوال ریاضی را روی تخته می‌نویسد و از دانش‌آموزان می‌خواهد که آن را حل کنند و اولین نفری که موفق به حل سوال شد را به عنوان مبصر برمی‌گزینند. اما برای اینکه قدرت همواره دست یک نفر نباشد، او هر زنگ یک مبصر جدید را به این شیوه انتخاب می‌کند.

---

15 Shared public ledger
16 Double Spending
17 Proof of Work

در سیستم بیت‌کوین، تراکنش‌ها توسط نودها جمع آوری شده و به ماینرها داده می‌شود، هر ماینر برای حل یک مساله ریاضی تلاش می‌کند که این مسئله تنها به شکل بروت فورس[۱۸] قابل حل شدن است. به همین علت آن سیستمی که سخت افزار قدرتمندتری دارد، شانس بیشتری دارد که پاسخ را بدست آورد. پس از حل شدن این مسئله، تراکنش‌ها به همراه راه‌حل مسئله به کل شبکه تعلام می‌شود. به مجموعه دسته تراکنش‌ها که در هر بار به واسطه حل یک مسئله ریاضی باهم اعلام می‌شوند تراکنش‌های یک بلوک یا به اختصار بلوک می‌گویند(بعدا می‌بینیم بلوک‌ها شامل داده‌های دیگری هم هستند). نودها در صورت مغایرت نداشتن تراکنش‌های ثبت شده در بلوک با قوانین بلاک‌چین آن‌ها را می‌پذیرند و ماینرها به سراغ حل مسئله بعدی برای بلوک جدید می‌روند.

حال فرض کنید یک نفر بخواهد دابل اسپند انجام دهد. در اینصورت باید اول سکه "۱۲۳۴۵" را به فرد A بفرستد و صبر کند تا تراکنش توسط شبکه ثبت شود. سپس یک لیست تراکنش جدید درست کند که در آن سکه مذکور به فرد B ارسال شده است و مسئله ریاضی را برای این بلوک جدید حل کند. تا بدینجا چون تراکنش‌های قبلی توسط شبکه پذیرفته شده، همچنان حمله وی ناموفق مانده است. پس باید مسئله ریاضی بلوک بعدی را سریعتر از بقیه ماینرها حل کند تا موفق به انجام حمله شود. اما این در صورتی امکان پذیر است که قدرت پردازش شخص حمله کننده از مجموع دیگر ماینرها بیشتر باشد که با توجه به قدرت هش امروزی شبکه بیت‌کوین عملا قابل انجام نیست. زیرا هزینه‌ای که برای خرید این مقدار توان پردازشی مورد نیاز است بسیار زیاد است.همچنین فرد با انجام این کار عملا ارزش سیستم را به عنوان یک پول به صفر می‌رساند و تمام سرمایه‌اش بی‌ارزش می‌شود.

با این مقدمه و دید کلی که به دست آوردیم به سراغ اجزای بلاک‌چین می‌رویم و هر یک از آن‌ها را عمیق‌تر بررسی می‌کنیم.

---

18 Brute-force

تراکنش‌ها و نمایش آن‌ها در بلاک‌چین

هر تراکنش بیت کوین سه بخش دارد:

۱. متادیتا[۱۹]: متادیتای تراکنش‌های بیت‌کوین شامل شماره نسخه (در حال حاضر ورژن ۱)، تعداد ورودی‌های تراکنش، تعداد خروجی‌های تراکنش و زمان قفل تراکنش (برای کاربردهایی مانند اسکروها) و کوین‌بیس[۲۰] است.

۲. ورودی‌ها: یک تراکنش می‌تواند یک یا چند ورودی داشته باشد. هر ورودی دارای خروجی تراکنش قبلی و شماره آن است. همچنین یک امضای دیجیتال که توسط پرداخت کننده انجام می‌شود تا ثابت شود سکه‌ای که در حال انتقال است،واقعا متعلق به وی است.

۳. خروجی‌ها:مقدارِ سکه‌ای که قرار است منتقل شود. و همچنین یک اسکریپت[۲۱] که به شما اجازه می‌دهد به غیر از آدرس گیرنده، ویژگی‌هایی همچون اسکرو[۲۲]ها یا آدرس‌های سبز[۲۳] را در پرداخت خود بگنجانید.


```
{
    "hash":"b6f6991d03df0e2e04dafffcd6bc418aac66049e2cd74b80f14ac86db1e3f0da",
    "ver":1,
    "vin_sz":1,
    "vout_sz":2,
    "lock_time":"Unavailable",
    "size":258,
    "relayed_by":"64.179.201.80",
    "block_height, 12200,
    "tx_index":"12563028",
    "inputs":[

            {
                "prev_out":{
                    "hash":"a3e2bcc9a5f776112497a32b05f4b9e5b2405ed9",
                    "value":"100000000",
                    "tx_index":"12554260",
                    "n":"2"
                },
                "script":"76a914641ad5051edd97029a003fe9efb29359fcee409d88ac"
            }

        ],
    "out":[

                {
                    "value":"98000000",
                    "hash":"29d6a3540acfa0a950bef2bfdc75cd51c24390fd",
                    "script":"76a914641ad5051edd97029a003fe9efb29359fcee409d88ac"
                },

                {
                    "value":"2000000",
                    "hash":"17b5038a413f5c5ee288caa64cfab35a0c01914e",
                    "script":"76a914641ad5051edd97029a003fe9efb29359fcee409d88ac"
                }

        ]
}
```


شکل ۴ نمونه‌ای از یک تراکنش در بلاک‌چین

19 Metadata

20 Coinbase : کوین‌بیس یک متغیر خالی برای قرار دادن اطلاعاتی است که شبکه آن را در نظر نمی‌گیرد. یکی از کاربردهای این متغیر قرار دادن متن دلخواه درون یک بلاک است. برای مثال‌در اولین تراکنش بیت‌کوین ساتوشی ناکوموتو یک خبر از روزنامه همان صبح لندن قرار داده است که در آن به تایید مجلس این کشور برای افزایش چاپ پول رای داده‌اند!

21 scriptPubKey

22 Escrow

23 Green Addresses

بنابراین بلاک‌چین بجای نگهداری بالانس هر حساب (در اینجا کلیدهای عمومی) ورودی‌ها و خروجی‌های یک تراکنش را نگه می‌دارد. این موضوع باعث می‌شود که برای انتقال یک سکه از یک فرد به فرد دیگر، تنها لازم باشد که خروجی تراکنش قبل توسط صاحب حساب امضا شده و به عنوان ورودی قرار داده شود.

علت انتخاب این روش برای افزایش سرعت تایید تراکنش به عنوان یک تراکنش معتبر است. زیرا در این حالت تنها کافیست تراکنش‌های بین تراکنش مبدا تا تراکنش حال حاضر بررسی شود. اما اگر قرار بود برای هر کلید عمومی حساب‌ها مجزا نگهداری شود، آن‌گاه می‌بایست هر دفعه از اولین تراکنش بلاک‌چین بررسی می‌شد تا بتوان یک تراکنش را رد یا تایید کرد. (Narayanan et al., 2016)

اسکروها و آدرس‌های سبز:

ویژگی اسکریپتی بودن خروجی هر تراکنش این امکان را به برنامه‌نویسان می‌دهد که تراکنش‌های برنامه‌ریزی شده‌ای را برای بیت‌کوین فراهم آورند.

یکی ازین تراکنش‌ها، اسکروها یا تراکنش‌های توافق شده هستند. در حالت عادی تنها امضای صاحب سکه باعث می‌شود تراکنش اجرا شود، اما در اسکروها دو یا چند امضا لازم است تا تراکنش اجرا شود.برای درک کاربرد این موضوع مثال زیر را در نظر بگیرید:

فرض کنید شما از یک فروشگاه آنلاین خرید انجام داده‌اید اما چون تراکنش‌های بیت‌کوین غیرقابل برگشت هستند نمی‌خواهید قبل از اطمینان از شرایط محصول هزینه آن را پرداخت کنید. اما فروشگاه آنلاین نیز طبیعتا بدون واریز وجه محصول را برای شما ارسال نمی‌کند. در اینجا یک اسکرو بین شما و فروشگاه آنلاین تشکیل داده می‌شود. در این اسکرو شما با فروشگاه آنلاین توافق می‌کنید که یک شخص ثالث مورد اطمینان را وارد قرارداد کنید و برای تایید تراکنش به دو امضا از شما سه نفر لازم باشد.

اگر کالا به دست شما رسید و محصول مدنظر شما بود، شما و فروشگاه تزاکنش را امضا می‌کنید و تراکنش تایید می‌شود.

اما اگر هر طرف به دلیلی تراکنش را تایید نکرد، شخص ثالث وارد قضیه می‌شود.

اگر بنظر شخص ثالث حق با فروشگاه باشد و پول باید به آن پرداخت شود، فروشگاه و شخص ثالث تراکنش را امضا می‌کنند و تراکنش انجام می‌شود.

در غیر اینصورت، شما و شخص ثالث تراکنش را امضا نمی‌کنید، این باعث منقضی شدن قرارداد و برگشت پول به حساب شما می‌شود.

آدرس‌های سبز برای سرعت بخشیدن به تراکنش‌هایی است که لازم است در لحظه انجام گیرند. به علت ساخت هر بلوک حدود ۱۰ دقیقه طول می‌کشد و برای اطمینان از انجام یک تراکنش در بدترین حالت تولید۶ بلوک لازم است، بعضی تراکنش‌ها نیازمند این هستند که در زمان کوتاه‌تری تایید شوبرای مثال اگر بخواهید در یک کافی شاپ پول سرویس را با بیت کوین بدهید باید یک ساعت صبر کنید تا تراکنش تایید شود و سپس قهوه شما سرو خواهد شد!

به همین علت بعضی شرکت‌ها به عنوان واسط عمل کرده و از سمت شما پرداخت را انجام می‌دهند. چون آدرس این شرکت‌ها برای همه شناخته شده است، کاربران شبکه بیت‌کوین می‌توانند با اعتماد به اینکه این آدرس‌ها تلاشی برای دابل اسپندینگ نمی‌کنند، تراکنش تایید نشده را بپذیرند و به این شکل از سیستم استفاده کنند.

در واقع آدرس‌های سبز به نوعی مانند کردیت کارت‌ها عمل می‌کنند. (Narayanan et al., 2016)

فرایند ماینینگ و الحاق بلوک‌های جدید به زنجیره

تا اینجا دیدیم هر تراکنش از چه اجزایی تشکیل شده و چه ویژگی‌هایی دارد. مهمترین بخش‌های یک بلاک شامل:

- یک اشاره‌گر به بلوک قبلی
- لیستی از تراکنش‌های تایید نشده
- جوابی برای یک سوال ریاضی که تنها به شیوه بروت فورس قابل حل است

نودهای نگهدارنده تراکنش‌های بیت‌کوین تنها زنجیره‌ای را معتبر می‌دانند که طولانی‌تر است. اگر دو ماینر همزمان دو بلوک متفاوت را ماین کنند، نودها صبر می‌کنند تا بلوک بعدی یافت شود، اولین بلوکی که به یکی از دو بلوک ساخته شده الحاق شود و زنجیره آن بلوک را بلندتر کند،آن زنجیره مورد قبول نودها قرار می‌گیرد.

ماینرها باید یک عدد پیدا کنند که با الحاق این عدد به هش بلاک قبلی و لیست تراکنش‌ها و هش گرفتن از این سه در یک فضای هدف کوچک باشد. به این نوع مسائل ریاضی هش پازل[۲۴] گفته می‌شود.

24 Hash Puzzle

$$hash(nonce + previousblockhash + transactions) < tragetspace$$

هر چه این فضای هدف کوچکتر باشد، یافتن جواب این مسئله نیازمند محاسبات بیشتر است. چون سیستم بلاک‌چین به گونه‌ای تعریف شده که در هر ۱۰ دقیقه تقریبا یک بلوک پیدا شود، در صورت افزایش توان محاسباتی ماینرها، سیستم خودبه‌خود سختی مسئله را افزایش می‌دهد تا کار پیدا کردن جواب سخت‌تر شود.

اما در ازای حل کردن این مسئله، سیستم به ماینرها پاداش می‌دهد. هر ماینری که بتواند یک بلوک را پیدا کند، ۱۲.۵ بیت کوین در حال حاضر به او تعلق می‌گیرد (مقدار اولیه این پاداش ۵۰ بیت‌کوین برای افزایش انگیزه و جذب ماینر بیشتر بود). پاداش ماینرها پس از هر ۲۱۰۰۰۰ بلوک که یافت می‌شود نصف می‌گردد. این فرمول باعث می‌شود از سال ۲۱۴۰ به بعد دیگر بیت‌کوین جدیدی ساخته نشود و همان خاصیت ضد تورمی است که در بخش اول آن را بررسی کردیم.

برای داشتن یک هش پازل مناسب شبکه بلاک‌چین سه ویژگی باید ارضا شود:

۱. سختی محاسبه: در صورت وجود یک راه‌حل ریاضیاتی چندجمله‌ای برای حل جواب مسئله، سیستم امنیت خود را از دست می‌دهد و هر فردی می‌تواند به راحتی زنجیرخ بلوک‌ها را تحت تاثیر قرار داده و حمله دابل اسپندینگ را انجام دهد. بنابراین توابع استفاده شده در سیستم برای حل مسئله نباید دارای راه‌حلی به جز بروت فورس باشد.
۲. هزینه متغیر:همانطور که گفته شد، سیستم باید بتواند در صورت افزایش تعداد ماینرها یا توان محاسباتی آن‌ها جوری خود را هماهنگ کند تا در زمان معین شده هر بلوک حل شود. بنابراین باید فضای جواب به پارامترهای مختلف تغییر کند.
۳. آسانی تایید جواب:راه‌حلی که توسط یک ماینر یافت می‌شود باید امکان تایید توسط دیگر اعضای شبکه در کمترین زمان ممکن را داشته باشدتا در صورت وجود اشکال سریعا رد شود و در صورت سحیح بودن مقادیر داخل بلوک، سریعا به زنجیره اضافه شده و ماینرها کار برای حل بلوک بعدی را آغاز کنند.

نکته قابل توجه این است که هر چه توان پردازشی ماینرها در یک سیستم بیشتر شود، سیستم امن‌تر می‌شود زیرا هزینه حمله ۵۱ درصد بیشتر و بیشتر می‌شود.

سیستم اثبات سهام[۲۵]

یکی از سیستم‌های جایگزین سیستم اثبات کار، سیستم اثبات سهام است.

25 Proof-of-stake

در این شیوه به جای حل یک مسئله به وسیله قدرت پردازشی،نودها مقدار مشخصی از ارز شبکه را در اختیار شبکه می‌گذارند و در صورت رفتار خلاف قوانین شبکه[۲۶] شبکه با کم کردن از حساب آن نود، آن نود را مجازات می‌کند.

این سیستم در بسیاری از شبکه‌های ارزهای دیجیتال کنونی از جمله اتریوم، کاردانو، پولکادات و ... استفاده می‌شود و می‌تواند جایگزینی برای سیستم اثبات سهام جهت کاهش هزینه مالی و انرژی‌ای سیستم اثبات کار باشد. در بخش آخر بیشتر به این شیوه می‌پردازیم.

26 Misbehaviour

اعمال تغییرات در کد بلاک‌چین: هاردفورک[۲۷] و سافت‌فورک[۲۸]

مانند هر سیستم کامپیوتری، بلاک‌چین نیز ممکن است نیاز به اصلاح، تغییر یا به‌سازی داشته باشد اما به علت غیرمتمرکز بودن سیستم، این تغییرات چالش‌هایی فراتر از سیستم‌های متمرکز ایجاد می‌کند. مهم‌ترین چالش، هماهنگ سازی نودها برای استفاده از نسخه جدید کدهاست. چون بلاک‌چین روی نودهای مختلف اجرا می‌شود، در صورت هماهنگ نبودن نسخه آن‌ها، این موضوع می‌تواند موجب دودستگی یا چنددستگی بین نودها و شبکه شود. به همین علت تغییرات در بلاک‌چین به دو دسته تقسیم می‌شوند:

۱. هاردفورک: در این تغییرات، نسخه جدید نرم‌افزار، بلاک‌هایی تولید می‌کند که توسط نسخه‌های قبلی نامعتبر شناخته می‌شود. این موضوع به معمولا به علت اضافه شدن ویژگی‌های جدید به کد اصلی است (برای مثال افزایش سایز بلاک‌ها یا ...). چون بلاک‌های تولید شده توسط نودهایی که نسخه جدید را اجرا می‌کنند توسط نودهای قدیمی رد می‌شود، این نودها شروع به ساخت بلاک‌های دیگری می‌کنند وزنجیره متفاوتی می‌سازند. این موجب دودستگی بین بلوک‌های درون شبکه می‌شود. به همین علت به این تغییرات، هارد فورک گفته می‌شود.
۲. سافت فورک: نوع دیگری از تغییرات هستند که باعث محدودتر شدن قوانین تایید بلاک‌ها می‌شود و چون مجموعه قوانین ورژن جدید، زیر مجموعه‌ای از قوانین ورژن قبلی است، نودهای قدیمی هم بلوک‌های تولید شده توسط نودهای جدید را می‌پذیرند. به این دسته از تغییرات سافت‌فورک گفته می‌شود زیرا از دودستگی کامل بین زنجیره نودهای قدیمی و جدید جلوگیری می‌کند.

هارد فورکینگ به علت ایجاد دودستگی بین اعضای شبکه بسیار به ندرت انجام می‌گیرد. یکی از معروفترین هاردفورک‌ها، در بلوک ۴۷۸۵۸۸، در تاریخ ۱ آگوست ۲۰۱۷ انجام شد. این هارد فورک به علت اعتقاد بعضی از اعضای جامعه بیت‌کوین از جمله راجر فر[۲۹] پیشنهاد شد که معتقد بودند برای افزایش مقیاس‌پذیری بیت کوین باید با افزایش محدودیت حجم هر بلاک، تعداد تراکنش بیشتری در ثانیه را امکان پذیر کرد. این موضوع موجب پدید آمدن ارز جدیدی به نام بیت‌کوین‌کش[۳۰] شد که امروزه نیز با یک شبکه مجزا از بیت کوین به فعالیت خود ادامه می‌دهد. (Narayanan et al., 2016)

27 Hard fork
28 Soft fork
29 Roger Ver
30 Bitcoin Cash

متن باز بودن[۳۱] این امکان را به هر فردی می‌دهد که با انجام تغییرات دلخواه خود، یک فورک جدید از بیت‌کوین ساخته و شبکه مورد نظرش را گسترش دهد.

31 Open-Source

دیگر بلاک‌چین‌ها و نگاهی به آینده

با اینکه بیت‌کوین تحول عظیمی در زمینه ارزهای دیجیتال را با خودبه همراه آورد، با حل شدن بعضی از مسائل کلیدی توسط ساتوشی ناکاموتو، این امکان به هر کس داده شد که پروژه و بلاک‌چین خود را تعریف و پیاده‌سازی کند. به همین علت در بین سال‌های ۲۰۱۱ تا ۲۰۱۵، تعداد بسیار زیادی پروژه توسط افراد و شرکت‌های مختلف اجرا شد. این فرصت بسیار مناسبی برای تبهکاران نیز بود تا با انجام عملیات پامپ و دامپ[۳۲] کلاهبرداری‌های عظیمی صورت دهند. اما در کنار این پروژه‌های تقلبی بعضی از فعالان این علم شروع به تولید ارزهای دیجیتال برای مصارف مختلف، یا جهت بهبود بیت‌کوین به آن نحو که بنظرشان درست می‌امد کردند. پروژه‌های غیر از بیت‌کوین که با نام آلت‌کوین[۳۳] شناخته می‌شوندبه دو دسته کلی تقسیم می‌شوند؛ یک دسته از کد بیت‌کوین با تغییر اندکی از پارامترها یا از بخشی از آن استفاده می‌کنند، و پروژه‌هایی که از نو و با دید دیگری شروع به توسعه محصول خود می‌کنند. تعدادی از آلت‌کوین‌های دسته اول شامل:

نیم‌کوین[۳۴]: نیم‌کوین اولین آلت‌کوینی بود که پس از بیت‌کوین ایجاد شد. هدف از این پروژه تولید یک DNS غیرمتمرکز بود که با ثبت آدرس‌های آی‌پی و دامنه‌نام‌ها این امکان را به مرورگرها می‌داد تا با کوئری گرفتن از این بلاک‌چین سرویس مورد نظر خود را پیدا کنند. این پروژه مورد استقال جامعه کاربری قرار نگرفت و عملا کاربردی ندارد.

لایت‌کوین[۳۵]: لایت‌کوین با تغییر بسیار کوچکی در پارامتر بیت‌کوین و تغییر الگوریتم پیدا کردن هش بلوک به وجود آمد. علت توسعه این ارز، جلوگیری از استخراج یک ارز دیجیتال با ارزش توسط GPU[۳۶] و ASIcها[۳۷] بود. این کار برای بیشتر غیرمتمرکز شدن این ارز انجام می‌شد. به همین علت لایت‌کوین با تغییر الگوریتم هش، ابتدا جامعه کاربری خوبی پیدا کرد. همین باعث شد پس از شکست خوردن هدف اصلی این پروژه (و امکان ماین شدن آن توسط کارت‌گرافیک و اسیک‌ها) همچنان جامعه کاربری خود را حفظ کند. به علت تولید سریعتر بلاک توسط بلاک‌چین لایت‌کوین، این ارز کارمزد کمتری از بیت‌کوین دارد. امروزه لایت‌کوین یکی از ده ارز برتر دیجیتال (از لحاظ مارکت‌کپ) است.

32 Pump-and-Dump
33 Altcoin
34 NameCoin
35 LiteCoin
36 Graphic Processing Unit
37 application-specific integrated circuit

شکل ۵ نمودار قیمت لایت‌کوین از سال ۲۰۱۳

پس از شیوه اثبات‌کار برای استخراج بلوک‌ها، شیوه جدیدی به نام اثبات سهام[۳۸] پیشنهاد شد که عملیات استخراج بلوک‌ها را با توان محاسباتی بسیار کمتری انجام می‌داد. در این شیوه هر فرد مقداری از دارایی خود را در اختیار شبکه قرار می‌دهد و شبکه با توجه به این دارایی وظیفه تایید بلوک‌ها را به نودهای مختلف تخصیص می‌دهد.در صورت تخدی یا ثبت تراکنش غیر مجاز، نود متخلف با از دست دادن مقداری از دارایی خود جریمه می‌شود. برای انجام حمله ۵۱ درصد، یک نود باید بیش از ۵۱ درصد از ارز یک شبکه را در اختیار داشته باشد که عملا غیرممکن است. در این روش نودها برای یافتن بلوک‌ها از شبکه جایزه دریافت نمی‌کنند و فقط کارمزد تراکنش‌های درون بلاک به آن‌ها داده می‌شود.

یکی از مهم‌ترین ارزهایی که پس از بیت‌کوین ساخته شد و ازین روش نیز استفاده می‌کند اتریوم[۳۹] نام دارد. ایده اتریوم در سال ۲۰۱۳ توسط ویتالیک بوترین[۴۰] داده شد و از مهم‌ترین اعضای اولیه این شبکه می‌توان به گوین وود[۴۱] اشاره کرد. برخلاف زبان اسکریپت بیت‌کوین که تورینگ-کامپیلیت[۴۲] نیست، زبان برنامه‌نویسی اتریوم تورینگ-کامپلیت است. این بدین معناست که شبکه اتریوم امکان اجرای هر برنامه‌ای که توسط کامپیوترهای مدرن قابل انجام است را دارد. حتی از لحاظ تئوری امکان ساخت بیت‌کوین درون اتریوم وجود

38 Proof-of-Stake
39 Ethereum
40 Vitalik Buterin
41 Gavin wood : یک دانشمند علوم کامپیوتراست که پس از ترک پروژه اتریوم، پروژه پولکادات را پایه‌گذاری نمود.
42 Turing-complete

دارد! همین امکان اجرای برنامه‌هایی با لوپ بی‌نهایت را روی شبکه اتریوم می‌دهد. توسعه‌دهندگان اتریوم برای مقابله با چنین مشکلی مفهومی به عنوان گاز[۴۳] را معرفی کردند. برای اجرای قراردادهای هوشمند[۴۴] نیاز است که کاربری که اجرا کننده است، مقدار گاز به سیستم پرداخت کند. این گاز در حین اجرای قرارداد هوشمند به تدریج از بین می‌رود و اگر پیش از اتمام قرارداد، گاز به پایان برسد، آن‌گاه قرارداد هوشمند متوقف می‌شود. هر گاز معادل ۱ گیگاوی[۴۵]، معادل 0.000000001 اتر [۴۶] می‌باشد.

سیستم قراردادهای هوشمند، اتوماسیون و دیجیتال‌سازی بسیاری از فعالیت‌های روزمره را ممکن می‌سازد. برای مثال توکن‌های غیرمتشابه[۴۷] امکان عرضه سندهای مالکیت را بر روی بلاک‌چین امکان‌پذیر می‌سازند.توکن‌های غیرمتشابه، توکن‌هایی هستند که برخلاف توکن‌های متشابه[۴۸] با یکدیگر متمایزند و یکسان نیستند. برای مثال هر یک بیت‌کوین ارزشی برابر با یک بیت‌کوین دیگر دارد و این دو با یکدیگر تمایزی ندارند اما سند خانه A با سند خانه B کاملا با یکدیگر متفاوتند. در صورت دیجیتال‌سازی این دو سند، به هر کدام ازین‌ها توکن غیرمتشابه می‌گویند. زیرا با اینکه هر دو از یک جنس (سند مالکیت) هستند اما ارزش یکسانی ندارند و محتوای آن‌ها با یکدیگر متفاوت است. توکن‌های غیرمتشابه امکان عرضه اسناد را بر روی بلاک‌چین امکان‌پذیر می‌سازند. با انتقال مالکیت یک توکن از یک شخص به شخصی دیگر، به علت ثبت شدن این تراکنش در بلاک‌چین، مالکیت این سند برای همگان واضح و غیرقابل‌تغییر خواهد بود. به همین علت بلاک‌چین بستر بسیار مناسبی برای دیجیتال سازی اسناد مختلف است.

یکی دیگر از کاربردهای آینده‌نگرانه بلاک‌چین، امکان اخذ عادلانه مالیات و توزیع عادلانه آن تحت این بستر است. به علت شفاف بودن تراکنش‌های روی بلاک‌چین، می‌توان با تنظیم قراردادهای هوشمند برنامه‌ای تعریف کرد، که به طور شفاف مقدار مالیاتی بر درامد افراد قرار دهد و همان مالیات گرفته شده را به جای اینکه با واسطه دولت برای مردم هزینه شود، مستقیما به حساب اشخاص واریز گردد.

این نشان می‌دهد کاربرد بلاک‌چین بسیار فراتر از صرف انجام تراکنش‌های مالی است و به کمک این فناوری می‌توان با شفافیت و امنیت کامل، به آینده‌ای بهتر دست پیدا کرد.

---

43 Gas

44 Smart Contracts – برنامه‌هایی که به صورت خودکار روی سیستم به واسطه صادق شدن یا نشدن بندی در یک قرارداد اجرا می‌شوند گفته می‌شود.

45 Gwei - gigawei

46 ether

47 NFT – Non-Fungible Token

48 Fungible Token

مطالعه بیشتر و منابع

مطالعه بیشتر

1. A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction,* 1st Edition, Princeton University Press, 2016
2. Andreas M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Crypto-Currencies*, 1st Edition, O'Reilly Media Inc., 2014.
3. C. Burniske, J. Tatar, *Cryptoassets: the innovative investor's guide to bitcoin and beyond*, 1st Edition, McGrow Hill Professional, 2018
4. S. Battilossi, Y. Cassis, K. Yago, *Handbook of the History of Money and Currency*, 1st Edition, Springer, 2018
5. C. Paar, J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*, 1st Edition, Springer Publishing Company Inc., 2009

منابع

منابع به ترتیب استفاده در متن:

i. وبسایت رسمی بانک مرکزی جمهوری اسلامی ایران https://www.cbi.ir/Inflation/Inflation_fa.aspx
ii. خبرگزاری فارس http://fna.ir/ewjn9v
iii. N. Gregory Mankiw, *Principles of Economics,* 8th Edition, Cengage Learning, 2017
iv. A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction,* 1st Edition, Princeton University Press, 2016