

مقدمه‌ای بر بیت‌کوین از دید اقتصاد و علوم کامپیوتر

نویسنده: میکایل مایلی

فهرست:

مقدمه:	۳
بیت کوین: سیستم پولی غیرمتمرکز	۴
بلاک چین: زیرساخت اصلی بیت کوین	۹
تراکنش ها و نمایش آن ها در بلاک چین	۱۱
فرایند ماینینگ و الحاق بلوک های جدید به زنجیره	۱۳
اعمال تغییرات در کد بلاک چین: هاردفورک و سافتفورک	۱۶
دیگر بلاک چین ها و نگاهی به آینده	۱۸
مطالعه بیشتر و منابع	۲۱
مطالعه بیشتر	۲۱
منابع	۲۱

مقدمه:

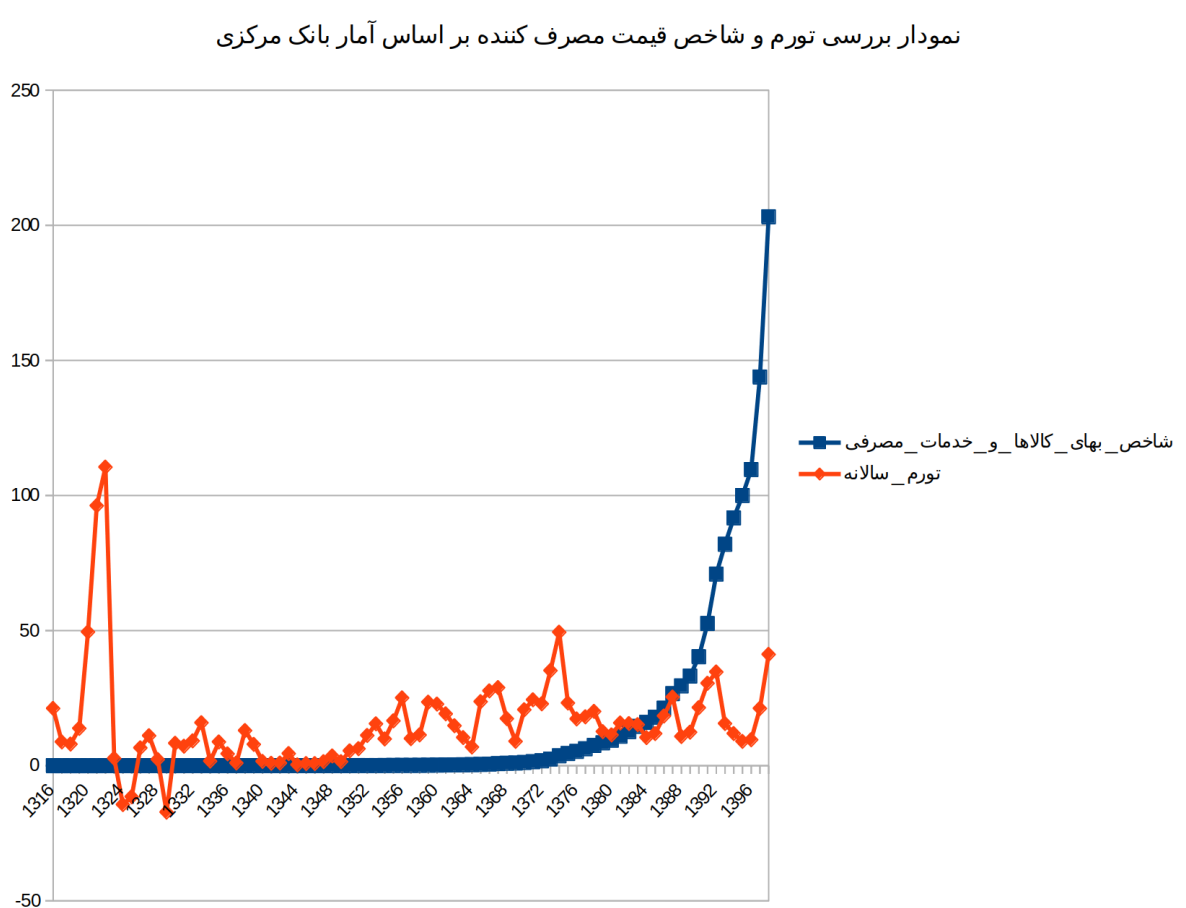
پس از تلاش‌های نافرجام دانشمندان علم رمزنگاری و علوم کامپیوتر برای ساخت یک پول دیجیتال، در سال ۲۰۰۹ فردی با نام مستعار ساتوشی ناکاموتو^۱ مقاله‌ای را منتشر کرد که در آن با شرح یک سیستم پول دیجیتال نقطه به نقطه^۲ مشکلات مربوط به ساخت و توزیع یک ارز دیجیتال را حل کرده بود. طبیعتاً این موضوع از دو وجه قابل بررسی است. یک دید اقتصادی که در آن به پارامترها و تأثیرات 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 علوم کامپیوتر بررسی می‌نماییم و در آخر آینده این فناوری و سیستم‌های جایگزین را معرفی خواهیم کرد.

1 Satoshi Nakamoto
2 Peer-to-Peer

بیت کوین: سیستم پولی غیر متمرکز

به نمودار زیر توجه کنید:



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

این نمودار بر اساس داده‌های بانک مرکزی جمهوری اسلامی ایران^۳، بیانگر تورم سالانه و شاخص بهای کالاها و خدمات مصرفی است. برای درک بهتر این نمودار به تعریف این دو مفهوم می‌پردازیم^۴:

3 داده‌های سال‌های ۱۳۱۶ تا ۱۳۹۶ در سایت بانک مرکزی موجود است:
https://www.cbi.ir/Inflation/Inflation_fa.aspx

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 رئیس بانک مرکزی به رئیس قوه قضاییه موجود در خبرگزاری فارس نوشته شده است:

<http://fna.ir/ewjn9v>

4 Mankiw, N. Gregory. 2016. *Principles of Economics*. 8th ed. Mason, OH: CENGAGE Learning Custom Publishing

شاخص بهای کالاها و خدمات مصرفی^۵: شاخص بهای کالاها و خدمات مصرفی بیانگر هزینه کلی کالاها و خدماتی است که یک مصرف‌کننده عام خریداری می‌کند.

نرخ تورم: تورم با استفاده از شاخص بهای کالاها و خدمات مصرفی و به شکل زیر محاسبه می‌شود:

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

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 بیت کوین تلاش‌های زیادی برای ارائه یک ارز دیجیتال برای استفاده در شبکه جهانی وب^۶ شده بود. یکی از مهمترین تلاش‌ها برای تولید چنین ارزی توسط دیوید چاوم^۷ انجام شد. ایده این ارز دیجیتال که دیجی کش^۸ نام داشت به این صورت بود:

۱. سیستم تولید پول، برای خلق پول جدید درخواست یک سریال از منحصر بفرد 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 دیجی کش پرداخت کنندگان ناشناس می‌مانند اما اطلاعات دریافت کنندگان در سیستم می‌ماند.

5 CPI(Consumer Price Index)

6 Wrold Wide Web

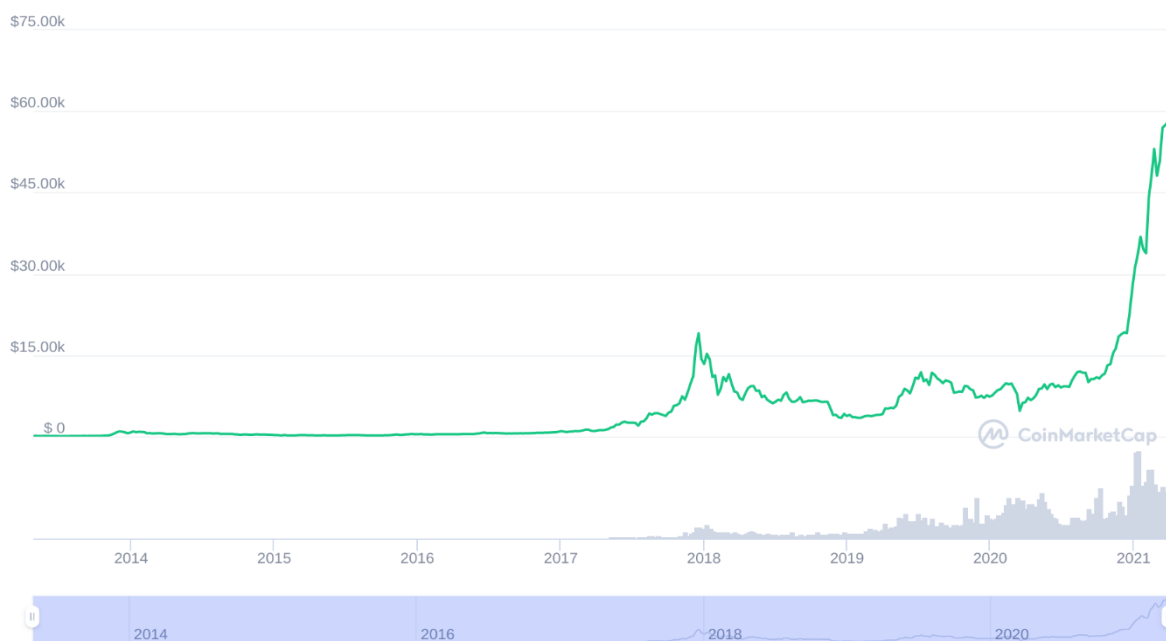
7 David Chaum

8 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 از این 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.

دیجی‌کش با اینکه در سال ۲۰۰۱ ورشکست شد، اما ایده‌های مهمی را در زمینه کریپتوکارنسی^۹ها مطرح کرد و جزو اولین شرکت‌هایی بود که در این زمینه به شکل تجاری فعالیت کرد.

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^{۱۰} 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^{۱۱}، نیک زابو^{۱۲} و وی دای^{۱۳} بودند. 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؟



شکل ۲ نمودار قیمت بیت‌کوین از سال ۲۰۱۳


9 Cryptocurrencies

- 10 Satoshi Nakamoto - اسم مستعار خالق بیت‌کوین است که کسی از هویت او خبری ندارد
- 11 Hal Finney - یک برنامه نویس بسیار ماهر بود که به توسعه بیت‌کوین علی‌الخصوص در مراحل اولیه بسیار کمک کرد.
- 12 Nick Szabo - یک دانشمند علوم کامپیوتر و مبدع ایده قراردادهای هوشمند و بیت‌گولد، یکی از ارزهایی که بیت‌کوین بر آن پایه‌گذاری شده، است.
- 13 Wei Dai - یک مهندس کامپیوتر و سازنده ارز دیجیتال بی-مانی. کوچکترین جز ارز شبکه اتریوم به افتخار او wei نام‌گذاری شده است.

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) بیت‌کوین امروزه تقریباً به عنوان یک ذخیره ارزش به شمار می‌رود. علت این موضوع بخاطر ویژگی‌های ذاتی‌ای است که در قوانین بیت‌کوین 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^{۱۴} 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 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.

در ادامه به بررسی شبکه زیرساخت بیت کوین، یعنی بلاک چین می پردازیم.

Hash	0000000000000000000029ce386c599cf970c9e14e36c60804f1d8d68cd36056d 
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

بلاک چین: زیر ساخت اصلی بیت کوین

بلاک چین یک دفتر حسابرسی توزیع شده عمومی^{۱۶} است که تمامی تراکنش‌های انجام شده در شبکه بیت کوین در آن ثبت می‌شود. آنچه بلاک چین را از دیگر رقبای تاریخی خود متمایز می‌سازد، شیوه حل کردن مسئله دابل اسپندینگ^{۱۷} و ترکیب آن با ایده اثبات کار^{۱۸} 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 برمی‌گزیند. اما برای اینکه قدرت همواره دست یک نفر نباشد، او هر زنگ یک مبصر جدید را به این شیوه انتخاب می‌کند.

در سیستم بیت کوین، 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^{۱۹} 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 راه حل 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 (بعدها 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 بیت کوین عملاً قابل انجام نیست. زیرا هزینه‌ای که برای خرید این مقدار توان پردازشی مورد نیاز است بسیار زیاد است. همچنین فرد با انجام این کار عملاً 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.

تراکنش‌ها و نمایش آن‌ها در بلاک‌چین

هر تراکنش بیت کوین سه بخش دارد:

۱. متادیتا^{۲۰}: 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^{۲۱} 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: مقدار سکه‌ای که قرار است منتقل شود. و همچنین یک اسکریپت^{۲۲} که به شما اجازه می‌دهد به غیر از آدرس گیرنده، ویژگی‌هایی همچون اسکرو^{۲۳}ها یا آدرس‌های سبز^{۲۴} را در پرداخت خود بگنجانید.

```
{
  "hash": "b6f6991d03df0e2e04daffcd6bc418aac66049e2cd74b80f14ac86db1e3f0da",
  "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

20 Metadata

²¹ 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 مثال در 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!

22 scriptPubKey

23 Escrow

24 Green Addresses

بنابراین بلاک چین 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 بلاک چین بررسی می‌شد تا بتوان یک تراکنش را رد یا تایید کرد.

اسکروها و آدرس‌های سبز:

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

یکی از این 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 طبیعتاً 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 تراکنش 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 این صورت، شما و شخص ثالث تراکنش را امضا نمی کنید، این باعث منقضی شدن قرارداد و برگشت پول به حساب شما می شود.

آدرس های سبز برای سرعت بخشیدن به تراکنش هایی است که لازم است در لحظه انجام گیرند. به علت ساخت هر بلوک حدود ۱۰ دقیقه طول می کشد و برای اطمینان از انجام یک تراکنش در بدترین حالت تولید بلوک لازم است، بعضی تراکنش ها نیازمند این هستند که در زمان کوتاه تری تایید شو برای 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 شرکت ها به عنوان واسطه عمل کرده و از سمت شما پرداخت را انجام می دهند. چون آدرس این شرکت ها برای همه شناخته شده است، کاربران شبکه بیت کوین می توانند با اعتماد به اینکه این آدرس ها تلاشی برای دابل اسپندینگ نمی کنند، تراکنش تایید شده را بپذیرند و به این شکل از سیستم استفاده کنند.

در واقع آدرس های سبز به نوعی مانند کردیت کارت ها عمل می کنند.

فرایند ماینینگ و الحاق بلوک های جدید به زنجیره

تا اینجا دیدیم هر تراکنش از چه اجزایی تشکیل شده و چه ویژگی هایی دارد. مهمترین بخش های یک بلاک شامل:

- یک اشاره گر به بلوک قبلی
- لیستی از تراکنش های تایید نشده
- جوابی برای یک سوال ریاضی که تنها به شیوه بروت فورس قابل حل است

نودهای نگهدارنده تراکنش های بیت کوین تنها زنجیره ای را معتبر می دانند که طولانی تر است. اگر دو ماینر همزمان دو بلوک متفاوت را ماین کنند، نودها صبر می کنند 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 می گیرد. ماینرها باید یک عدد پیدا کنند که با الحاق این عدد به هش بلاک قبلی و لیست تراکنش ها و هش گرفتن از این سه در یک فضای هدف کوچک باشد. به این نوع مسائل ریاضی هش پازل^{۲۵} گفته می شود.

$$\text{hash}(\text{nonce} + \text{previousblockhash} + \text{transactions}) < \text{targetspace}$$

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 تقریباً 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 بیت کوین 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 زنجیر 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 باشد تا در صورت وجود اشکال سریعاً رد شود و در صورت صحیح بودن مقادیر داخل بلوک، سریعاً 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^{۲۶}

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

در این شیوه به جای حل یک مسئله به وسیله قدرت پردازشی، نودها مقدار مشخصی از ارزش شبکه را در اختیار شبکه می‌گذارند و در صورت رفتار خلاف قوانین شبکه^{۲۷} شبکه با کم کردن از حساب آن نود، آن نود را مجازات می‌کند.

این سیستم در بسیاری از شبکه‌های ارزشهای 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.

اعمال تغییرات در کد بلاک چین: هاردفورک^{۲۸} و سافت فورک^{۲۹}

مانند هر سیستم کامپیوتری، بلاک چین نیز ممکن است نیاز به اصلاح، تغییر یا به سازی داشته باشد اما به علت غیرمتمرکز بودن سیستم، این تغییرات چالش هایی فراتر از سیستم های متمرکز ایجاد می کند. مهم ترین چالش، هماهنگ سازی نودها برای استفاده از نسخه جدید کدهاست. چون بلاک چین روی نودهای مختلف اجرا می شود، در صورت هماهنگ نبودن نسخه آن ها، این موضوع می تواند موجب دودستگی یا چنددستگی بین نودها و شبکه شود. به همین علت تغییرات در بلاک چین به دو دسته تقسیم می شوند:

۱. هاردفورک: در این تغییرات، نسخه جدید نرم افزار، بلاک هایی تولید می کند که توسط نسخه های قبلی نامعتبر شناخته می شود. این موضوع به معمولاً به علت اضافه شدن ویژگی های جدید به کد اصلی است (برای مثال افزایش سایز بلاک ها یا ...). چون بلاک های تولید شده توسط نودهایی که نسخه جدید را اجرا می کنند توسط نودهای قدیمی رد می شود، این نودها شروع به ساخت بلاک های دیگری می کنند و زنجیره متفاوتی می سازند. این موجب دودستگی بین بلوک های درون شبکه می شود. به همین علت به این تغییرات، هارد فورک گفته می شود.

۲. سافت فورک: نوع دیگری از تغییرات هستند که باعث محدودتر شدن قوانین تایید بلاک ها می شود و چون مجموعه قوانین ورژن جدید، زیر مجموعه ای از قوانین ورژن قبلی است، نودهای قدیمی هم بلوک های تولید شده توسط نودهای جدید را می پذیرند. به این دسته از تغییرات سافت فورک گفته می شود زیرا از دودستگی کامل بین زنجیره نودهای قدیمی و جدید جلوگیری می کند.

هارد فورکینگ به علت ایجاد دودستگی بین اعضای شبکه بسیار به ندرت انجام می گیرد. یکی از معروفترین هاردفورک ها، در بلوک ۴۷۸۵۸۸، در تاریخ ۱ آگوست ۲۰۱۷ انجام شد. این هارد فورک به علت اعتقاد بعضی از اعضای جامعه بیت کوین از جمله راجر فر^{۳۰} پیشنهاد شد که معتقد بودند برای افزایش مقیاس پذیری 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 بیت کوین کش^{۳۱} شد که امروزه نیز با یک شبکه مجزا از بیت کوین به فعالیت خود ادامه می دهد.

28 Hard fork

29 Soft fork

30 Roger Ver

31 Bitcoin Cash

متن باز بودن^{۳۲} 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.

دیگر بلاک چین ها و نگاهی به آینده

با اینکه بیت کوین 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 بلاک چین خود را تعریف و پیاده سازی کند. به همین علت در بین سال های ۲۰۱۱ تا ۲۰۱۵، تعداد بسیار زیادی پروژه توسط افراد و شرکت های مختلف اجرا شد. این فرصت بسیار مناسبی برای تبهکاران نیز بود تا با انجام عملیات پامپ و دامپ^{۳۳} کلاهبرداری های عظیمی صورت دهند. اما در کنار این پروژه های تقلبی بعضی از فعالان این علم شروع به تولید ارزهای دیجیتال برای مصارف مختلف، یا جهت بهبود بیت کوین به آن نحو که بنظرشان درست می آمد کردند. پروژه های غیر از بیت کوین که با نام آلت کوین^{۳۴} شناخته می شوند به دو دسته کلی تقسیم می شوند؛ یک دسته از کد بیت کوین با تغییر اندکی از پارامترها یا از بخشی از آن استفاده می کنند، و پروژه هایی که از نو و با دید دیگری شروع به توسعه محصول خود می کنند. تعدادی از آلت کوین های دسته اول شامل:

نیم کوین^{۳۵}: نیم کوین اولین آلت کوینی بود که پس از بیت کوین ایجاد شد. هدف از این پروژه تولید یک DNS غیرمتمرکز بود که با ثبت آدرس های آی پی و دامنه نام ها این امکان را به مرورگرها می داد تا با کوئری گرفتن از این بلاک چین سرویس مورد نظر خود را پیدا کنند. این پروژه مورد استقبال جامعه کاربری قرار نگرفت و عملاً کاربردی ندارد.

لایت کوین^{۳۶}: لایت کوین با تغییر بسیار کوچکی در پارامتر بیت کوین و تغییر الگوریتم پیدا کردن هش بلوک به وجود آمد. علت توسعه این ارز، جلوگیری از استخراج یک ارز دیجیتال با ارزش توسط GPU^{۳۷} و ASIC^{۳۸} ها بود. این کار برای بیشتر غیرمتمرکز شدن این ارز انجام می شد. به همین علت لایت کوین 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 کارت گرافیک و اسیک ها) همچنان جامعه کاربری خود را حفظ کند. به علت تولید سریعتر بلاک توسط بلاک چین لایت کوین، این ارز کارمزد کمتری از بیت کوین دارد. امروزه لایت کوین یکی از ده ارز برتر دیجیتال (از لحاظ مارکت کپ) است.

33 Pump-and-Dump

34 Altcoin

35 NameCoin

36 Litecoin

37 Graphic Processing Unit

38 application-specific integrated circuit



شکل ۵ نمودار قیمت لایت کوین از سال ۲۰۱۳

پس از شیوه اثبات کار برای استخراج بلوک‌ها، شیوه جدیدی به نام اثبات سهام^{۳۹} 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 عملاً 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 بیت کوین ساخته شد و ازین روش نیز استفاده می‌کند اتریوم^{۴۰} نام دارد. ایده اتریوم در سال ۲۰۱۳ توسط ویتالیک بوتیرین^{۴۱} داده شد و از مهم‌ترین اعضای اولیه این شبکه می‌توان به کوین وود^{۴۲} اشاره کرد. برخلاف زبان اسکریپت بیت کوین که تورینگ-کامپلیت^{۴۳} 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 بیت کوین درون اتریوم وجود

39 Proof-of-Stake

40 Ethereum

41 Vitalik Buterin

42 Gavin wood : یک دانشمند علوم کامپیوتر است که پس از ترک پروژه اتریوم، پروژه پولکادات را پایه‌گذاری نمود.

43 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^{۴۴} را معرفی کردند. برای اجرای قراردادهای هوشمند^{۴۵} 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^{۴۶}، معادل 0.000000001 اتر^{۴۷} می‌باشد.

سیستم قراردادهای هوشمند، اتوماسیون و دیجیتال‌سازی بسیاری از فعالیت‌های روزمره را ممکن می‌سازد. برای مثال توکن‌های غیرمتشابه^{۴۸} امکان عرضه سندهای مالکیت را بر روی بلاک‌چین امکان‌پذیر می‌سازند. توکن‌های غیرمتشابه، توکن‌هایی هستند که برخلاف توکن‌های متشابه^{۴۹} 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 کاملاً با یکدیگر متفاوتند. در صورت دیجیتال‌سازی این دو سند، به هر کدام از این‌ها 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 غیرقابل تغییر خواهد بود. به همین علت بلاک‌چین بستر بسیار مناسبی برای دیجیتال‌سازی 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 درآمد افراد قرار دهد و همان مالیات گرفته شده را به جای اینکه با واسطه دولت برای مردم هزینه شود، مستقیماً 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.

44 Gas

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

46 Gwei - gigawei

47 ether

48 NFT – Non-Fungible Token

49 Fungible Token

مطالعه بیشتر و منابع

مطالعه بیشتر

1. Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016:

This is a great theoretical introduction in order to understand bitcoin, blockchain and a little history on the subject

2. Andreas M. Antonopoulos. 2014. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (1st ed.). O'Reilly Media, Inc.:

This is a great introduction for anyone who wants to learn bitcoin and blockchain from a more technical point-of-view

3. Bitcoin.org:

The official website of bitcoin developers! With lots of great articles and a great developer guide

4. Burniske, Chris, and Jack Tatar. 2018. *Cryptoassets: the innovative investor's guide to bitcoin and beyond*: An introduction with more focus on finance and economics
5. Battilossi, Stefano & Cassis, Youssef & Yago, Kazuhiko. (2020). *Handbook of the History of Money and Currency*. 10.1007/978-981-10-0622-7.
6. Christof Paar and Jan Pelzl. 2009. *Understanding Cryptography: A Textbook for Students and Practitioners* (1st. ed.). Springer Publishing Company, Incorporated.

منابع

منابع به ترتیب استفاده در متن:

- i. https://www.cbi.ir/Inflation/Inflation_fa.aspx
- ii. <http://fna.ir/ewjn9v>
- iii. Mankiw, N. Gregory. 2016. *Principles of Economics*. 8th ed. Mason, OH: CENGAGE Learning Custom Publishing
- iv. Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.
- v. <https://bitcoin.org>