نویسنده

حمیدرضا عسگری

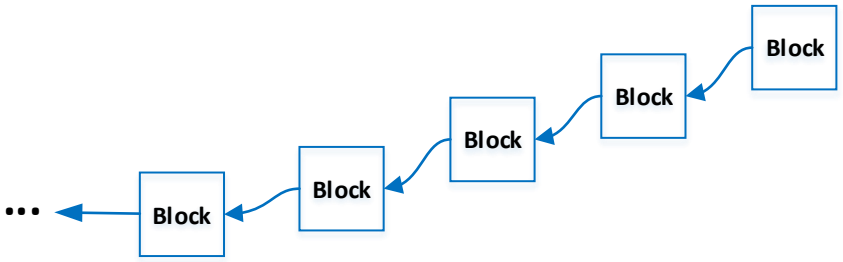
h.r.asgari52@gmail.com

منتشر شده توسط

کوین ایران

کوین ایران بزرگترین پایگاه خبری فارسی زبان در حوزه فناوری بلاکچین، ارزهای رمزنگاری شده و پلتفرم های مرتبط با بلاکچین است. این وب سایت در سال ۱۳۹۲ توسط بابک جلیلوند و آرش محبوب، با هدف اطلاع رسانی، آموزش و مشاوره به جامعه فارسی زبان علاقه مند به رمز ارزها راه اندازی شد و اولین مقاله آن در ۱۴ دی ماه همان سال، با عنوان «بیت کوین چیست؟» منتشر گردید . هدف کوین ایران از معرفی این فناوری ایجاد محیطی پژوهشی و آموزشی در راستای استفاده صحیح از این فناوری جهت ارائه تسهیلات و رفاه به جوامع فارسی زبان است.

www.coiniran.com



بلاکچین یا زنجیره بلوک ها چیست؟

امروزه هرگاه صحبت از بلاکچین به میان می‌آید، واژه های مختلفی به ذهن خطور می‌کند. از جمله ساختار داده، دفتر کل، بلوک های متوالی، رمزنگاری، توافق جمعی، امضای دیجیتال، و ...

در واقع هر کدام از این واژه ها به تنهایی نمی‌تواند بلاکچین را توصیف نماید، بلکه ترکیب همه آنهاست که بلاکچین را معنا دار و کاربردی می‌کند. لذا در خلال این کاتالوگ مباحث مختلفی مطرح می‌شود که در نگاه اول ممکن است ارتباطی با هم نداشته باشند اما در ساختار کلی بلاکچین، هرکدام از آنها یک پارامتر مهم محسوب می‌شود.

ساختار متمرکز در مقابل ساختار غیر متمرکز

فلسفه وجودی بلاکچین در واقع برای از بین بردن انحصار در مالکیت متمرکز است. به تعبیر دیگر بر اساس ماهیت و ساختار بلاکچین، کسی نمی‌تواند ادعای مالکیت روی زنجیره اطلاعات داشته باشد بلکه این مالکیت توزیع شده و طی فرایند های خاصی اطلاعات در آن قرار می‌گیرد که در ادامه مطالب به آن پرداخته خواهد شد.

تاریخچه پیدایش بلاکچین

مفهوم بلاکچین با پیدایش بیت کوین پا به عرصه وجود گذاشته است. در اکتبر سال ۲۰۰۸ مقاله ای (Bitcoin whitepaper) با نام "بیت کوین: سیستم پول الکترونیکی همتا-به-همتا توسط شخصی با نام مستعار **ساتوشی ناکاموتو**" در سایت metzdowd.com منتشر شد.در این مقاله او ساختار کلی این سیستم را بیان می‌کند. این مقاله به سرعت مورد توجه افراد متخصص و علاقمند در این حوزه واقع شد. در ژانویه ۲۰۰۹ او اولین نسخه نرام افزار بیت کوین را ارائه کرد. چندی نگذشت که شبکه بیت کوین شروع به کار نمود.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto

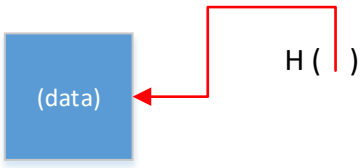
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third 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 a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast 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.

اگرچه مفهوم بلاکچین به نوعی در ابتدا بیت کوین را تداعی می‌کند اما این مفهوم تنها مربوط به رمز ارزها نبوده و در سالهای بعد از آن بسیار فراتر رفته است. این مفهوم امروزه کاربردهای بسیار متنوعی پیدا نموده است. در این نوشته برای درک بهتر و ساده تر بلاکچین، به ساختار بلاکچین بیت کوین پرداخته می‌شود.

بلاکچین به خودی خود یک ساختار داده است به این معنی که بیان می‌کند نحوه قرارگیری و ذخیره اطلاعات در کنار یکدیگر چگونه است. اما با ساختارهای ذخیره سازی معمول داده ها مانند دیتابیس ها، فایل های متنی و غیره متفاوت است. در دیتابیس های معمول، داده ها بصورت جداول و ردیف ها و ستون ها و ارتباط بین آنها تشکیل می‌شود، اما در بلاکچین، داده ها در یک توالی بهم پیوسته از بلاک ها ذخیره می‌شوند. مکانیزم نگهداری این توالی توسط نشانگرهای هش (Hash pointers) انجام می‌شود.

نشانگر هش (Hash pointer)

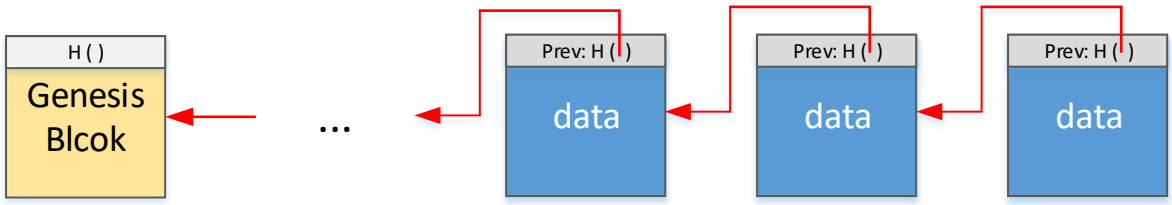


هر نشانگر هش از دو قسمت تشکیل شده است:

- یک نشانگر به محلی که اطلاعات در آن ذخیره شده
- یک هش رمزنگاری شده از آن اطلاعات

خاصیت نشانگر هش اطمینان از عدم دستکاری اطلاعات موجود در یک بلاک است.

بنابر این در بلاکچین پیوند بین بلاک ها و ترتیب و توالی آنها از روی نشانگر های هش معین می‌گردد. در هر بلاک یک block header وجود دارد که نشانگر هش در آن قرار می‌گیرد. خروجی هش بلاک قبل و همچنین آدرس بلاک قبل در این نشانگر قرار می‌گیرد.

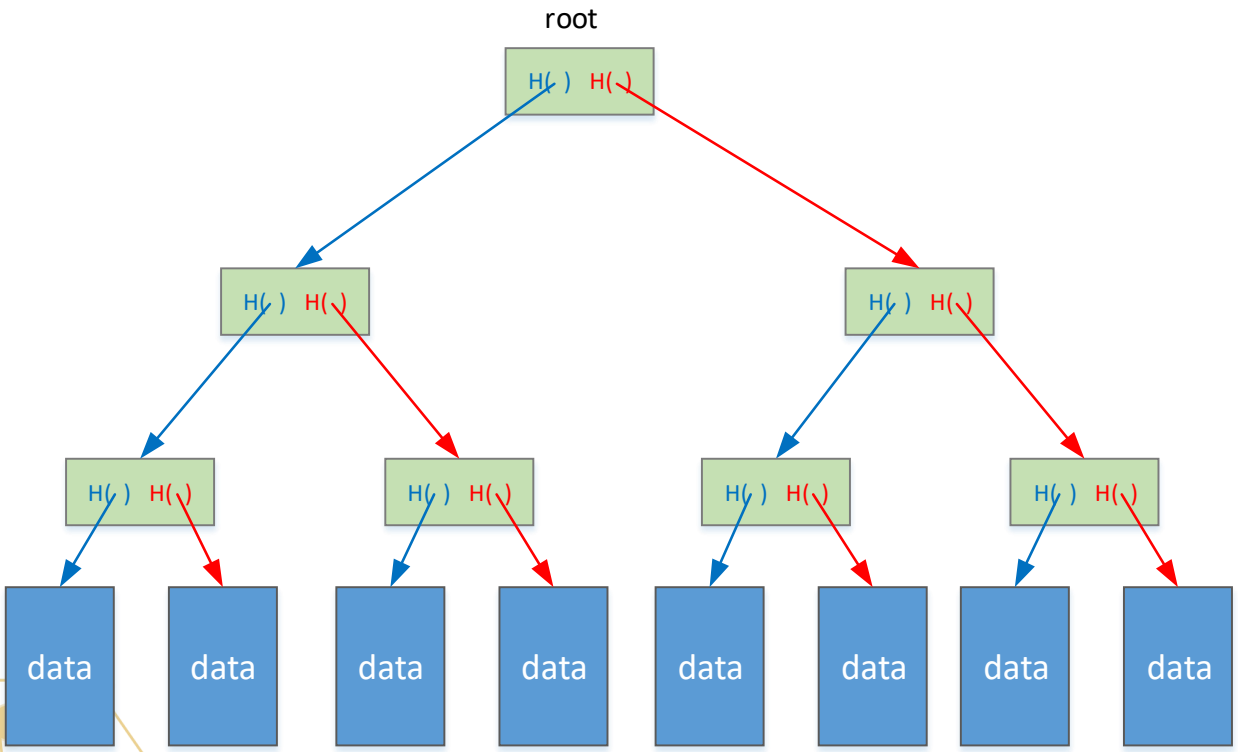


با این مکانیزم یکپارچگی و عدم دستکاری در بلاک ها بوجود خواهد آمد. هرگاه کسی به هر نحو بخواهد اطلاعات موجود در یک بلاک را تغییر بدهد این امر منجر به عوض شدن و نامعتبر شدن هش آن بلاک و بصورت زنجیروار هش های بلاک های بعدی خواهد شد. از این رو امکان این کار وجود ندارد.

از سوی دیگر اگر این فرد سعی در دستکاری و تغییر نشانگر های هش تمام بلاک ها، تا اولین بلاک (Genesis block) داشته باشد، در این صورت نیز بواسطه اینکه Genesis Block غیر قابل تغییر است، تلاش او به جایی نخواهد رسید. بدین ترتیب کل زنجیره از دستکاری مصون خواهد بود.

درخت مرکل (Merkle Tree)

یک ساختار کاربردی دیگر از ذخیره سازی با استفاده از نشانگر های هش، درخت مرکل نام دارد. این ساختار باینری که به نام خالق آن، Ralph Merkle ثبت شده است، یک درخت باینری است که داده ها در گروه های دو تایی قرار گرفته و هش این زوج، در نود بالاسری (parent) ذخیره و به همین ترتیب بالا می‌رود تا به نود اصلی یا ریشه می‌رسد. در پروتکل بیت کوین از این ساختار برای ذخیره سازی تراکنش های هر بلاک استفاده می‌شود.

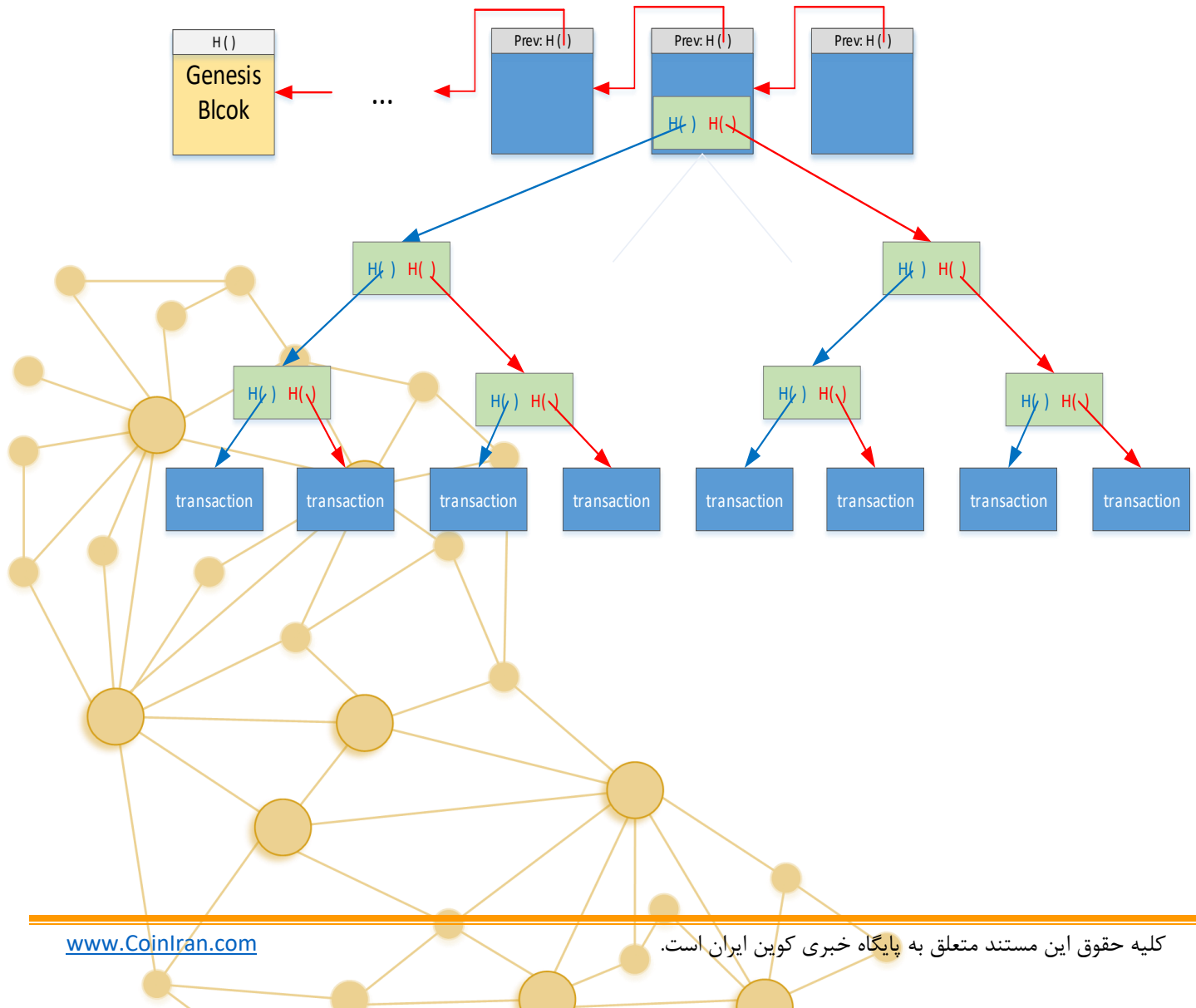


این ساختار نیز مانند ساختار قبلی، مصون از دستکاری است. با این ساختار حرکت در بین داده ها و مشخص کردن اینکه آیا یک داده خاص در این درخت قرار دارد یا خیر، بسیار سریع و تنها نیازمند صحت سنجی هش ها از آن شاخه تا ریشه است. به این خاصیت Proof of Membership گفته می‌شود.

به عنوان مثال فرض کنید یک درخت با تعداد ۱۰۰۰ تراکنش داشته باشیم و صحت سنجی هر کدام یک ثانیه طول بکشد، در حالت خطی و معمولی نیاز به صحت سنجی همه آنها داریم که ۱۰۰۰ ثانیه طول می‌کشد.

در ساختار درخت مرکل این زمان تنها Log(n) = Log (1000) = 3 یعنی **تنها ۳ ثانیه** طول می‌کشد. به همین خاطر سرعت جستجو در این ساختار بسیار سریع است.

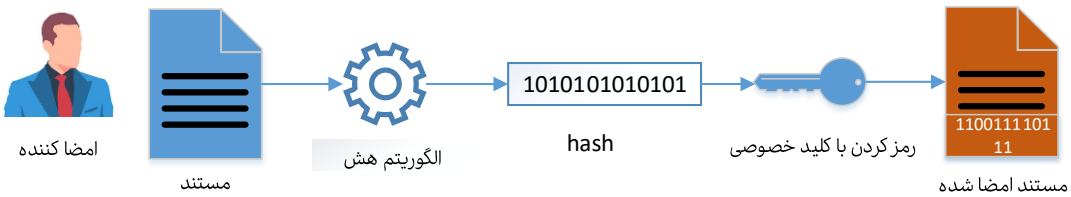
شمای کلی نشان گر هش و درخت مرکل در بلاکچین



امضای دیجیتال (Digital Signature)

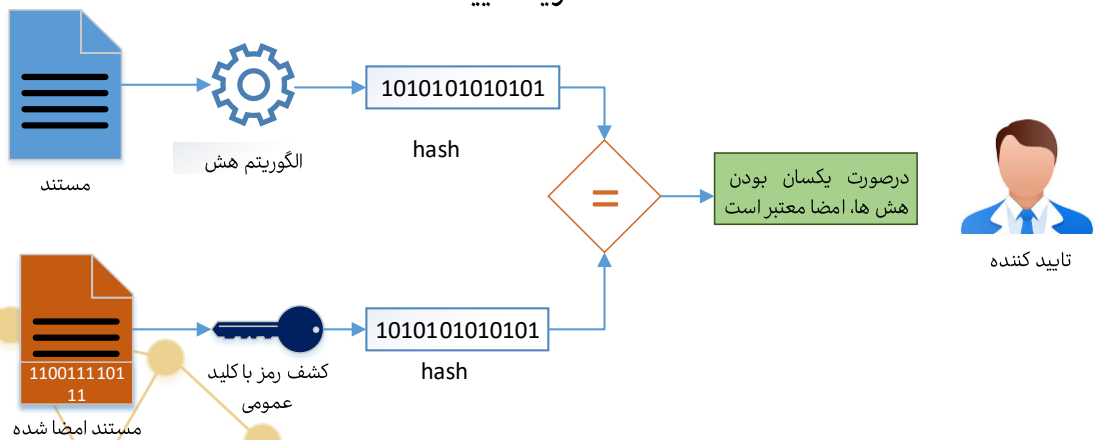
هدف از امضای دیجیتال، اطمینان از عدم دستکاری یک داده خاص است. در هر امضای دیجیتال دو خاصیت مهم مطرح است:

- تنها یک فرد می‌تواند امضا را بسازد و بقیه می‌توانند آن را صحت سنجی (verify) نمایند.
- هر امضا منحصر ا برای داده ای که امضای آن تولید شده، معتبر است و برای داده دیگری معتبر نیست.



فرآیند ایجاد امضا

فرآیند تایید امضا



مراحل یک امضای دیجیتال

۱. **تولید زوج کلید عمومی و خصوصی.** کلید خصوصی تنها در اختیار امضا کننده است و کلید عمومی برای تایید در اختیار دیگران قرار می‌گیرد.

۲. **متد امضا:** داده و کلید خصوصی به عنوان ورودی و مستند امضا شده به عنوان خروجی هستند.

۳. **متد تایید:** داده، کلید خصوصی و مستند امضا شده به عنوان ورودی هستند. نتیجه خروجی اگر درست بود امضا مورد تایید است.

نکته:

اگر داده ورودی طولانی باشد، امضای خروجی نیز طولانی بوده و مشکل ساز خواهد شد. برای این منظور یک راه حل هوشمندانه به کار گرفته شده است و آن اینکه اول داده ورودی را هش کرده و سپس هش بدست آمده امضا می‌شود و این متد به اندازه کافی امن خواهد بود.

متد مورد استفاده در بیت کوین، ECDSA (Elliptic curve Digital Signature Algorithm) است. در واقع نوع مشخصی از آن تحت عنوان Secp256k1 است که امنیت ۱۲۸ بیتی را فراهم می‌کند. شکستن این الگوریتم نیاز به حدس زدن از بین 2^{128} حالت مختلف دارد.

هویت (Identity)

در پروتکل بیت کوین، هویت در واقع همان آدرسی است که از کلید عمومی به دست می‌آید. به عبارت دیگر در پروتکل رمزنگاری، کلید عمومی (Public key) همان نقش هویت یا موجودیت را ایفا می‌کند اما چون طول کلید طولانی است، هش این کلید به عنوان هویت یا آدرس بیت کوین مورد استفاده قرار می‌گیرد.

$$H(P_k) = \text{Bitcoin Address}$$

به عنوان نمونه کلید عمومی و کلید خصوصی و آدرس بیت کوین به شکل زیر هستند:

Public Key (130 characters [0-9A-F]):

0483A76B32FAE3F7ED4D5B75DD464604B34E41095C49EA1671A111EEBB18DBF38104F70F320

9A93A57947 3B98039A5410FB66ED18D314 86AF8FCC5221D8A2B74869

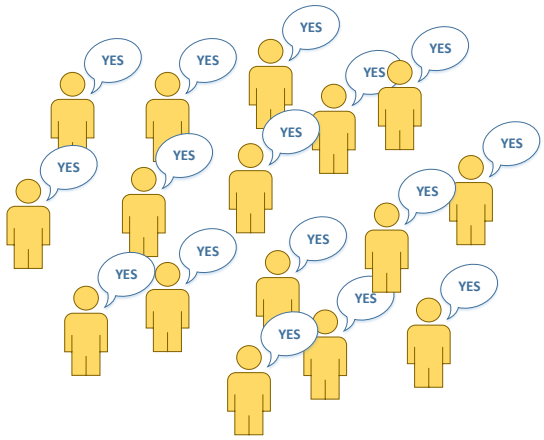
Private Key WIF Compressed, 52 characters base58, starts with a 'K' or 'L'

L5YTu7fwpEKgLDvMFGNa83chEB1RxuktrYqcvuT9zRR3y5R2TZ9t

Bitcoin Address

14WYnqg27a3SGDeeyubEtk9JWFZEKFTyB8

توافق جمعی (Consensus)



فرآیند اجماع و پذیرش یک بلاک به انتهای زنجیره را توافق جمعی می‌گویند. دستیابی به توافق جمعی در پروتکل بیت کوین در چند مرحله صورت می‌گیرد. در هر مرحله یک نود بصورت تصادفی انتخاب شده و این نود با حل مسئله ریاضی خاصی (پیدا کردن یک هش با مشخصات مورد نظر) یک بلاک برای اضافه شدن به زنجیره ارائه می‌کند (propose)، اما پذیرش یا عدم پذیرش این بلاک از طریق سایر نودها و توسط مکانیزمی در پروتکل بیت کوین انجام خواهد شد. به طور خلاصه مراحل به این ترتیب است:

۱. تراکنش های جدید برای همه نودها در شبکه ارسال می‌شود.
۲. هر نود تراکنش ها را در یک بلاک جدید تجمیع می‌کند.
۳. در هر مرحله -یک نود تصادفی- بلاک ساخته شده را برای بقیه ارسال می‌کند (انتشار بلاک ایجاد شده).
۴. سایر نود ها در صورت تایید و صحت سنجی تراکنش های داخل آن، آن بلاک را می‌پذیرند.
۵. نودها، پذیرفتن آن بلاک را با اضافه کردن هش آن بلاک به بلاک بعدی که ایجاد خواهند کرد، اعمال می‌کنند.

انواع حمله هایی که ممکن است در فرآیند توافق جمعی رخ دهد و نحوه مقابله با آنها

- **سرقت بیت کوین ها: (Bitcoin Stealing)**

هرگاه یک نود بخواهد تراکنش‌های داخل بلاک را -به مقصد آدرس خودش- دستکاری کند، ناچار است تراکنش جدیدی بسازد و در آن صورت می‌بایست آن تراکنش را از طرف قربانی امضا کند. با توجه به به استفاده از الگوریتم های رمزنگاری و نداشتن کلید خصوصی قربانی، عملا این کار غیر ممکن است.

- **عدم پردازش و ارسال تراکنش یک آدرس خاص (DOS (Denial Of Services**

بدین معنی است که یک نود در شبکه، تراکنش های یک آدرس خاص را به بلاکش اضافه نکند و در واقع از ارائه سرویس به آن فرد جلوگیری نماید. این حمله زیاد کارساز نخواهد بود زیرا با اندکی تاخیر تراکنش او توسط نود دیگری به بلاک اضافه خواهد شد.

- **خرج کردن دوباره یک بیت کوین خرج شده (Double Spending)**

به عبارت ساده یعنی اینکه یک فرد یک مقدار بیت کوین را که برای یک نفر ارسال کرده، دوباره به یک آدرس دیگر ارسال نماید. مثلا فرض کنید علی برای خرید یک کتاب از سایتی پرداخت خود را بصورت بیت کوین به آن سایت ارسال می‌کند و دوباره از همان بیت کوین، خرید دیگری از سایت دیگری انجام می‌دهد.

به خاطر وجود مکانیزم نشانگرهای هش تراکنش ها و مسئله ترتیب زمانی، تنها یک تراکنش او می‌تواند به بلاک بعدی اضافه شود و بنابر این از این حمله نیز جلوگیری می‌شود. یک مکانیزم دیگر برای جلوگیری از این حمله نیز اخذ تایید تراکنش ها است. بر اساس پروتکل بیت کوین و تجربه بدست آمده در اینخصوص (trade off) اگر یک تراکنش ۶ تاییدیه را اخذ کند (به عبارتی در ۶ بلاک بعدی که ایجاد می‌شود آن تراکنش معتبر باشد)، در آنصورت احتمال بروز وضعیت double spending تقریبا غیر ممکن خواهد بود. (این احتمال آنقدر نزدیک به صفر است که عملا می‌توان آن را صفر در نظر گرفت).

پاداش ایجاد یک بلاک (Block Reward) و کارمزد تراکنش (Fee)

ذات بلاکچین غیر متمرکز است و در کنترل کسی نیست. ادامه حیات زنجیره منوط به همکاری نود ها در پردازش و ایجاد بلاک های جدید به زنجیره است. این کار نیازمند وجود یک سیستم انگیزشی برای جبران هزینه های مختلف از جمله تجهیزات، انرژی، کولینگ و غیره است. از این رو مکانیزم پاداش و کارمزد برای ادامه حیات آن درنظر گرفته شده است.

در پروتکل بیت کوین به ازای هر بلاکی که ایجاد و به انتهای زنجیره اضافه می‌گردد، پاداشی برای آن نود منتخب در نظر گرفته شده است. به عبارت دیگر یک نود در هنگام ایجاد و ارائه یک بلاک، یک تراکنش خاص نیز در آن بلاک قرار می‌دهد که معروف به تراکنش ایجاد کوین است (coinbase transaction) و طبیعتا آدرس دریافت کننده تراکنش نیز همان نود است. به این ترتیب بیت کوین های جدید نیز وارد چرخه مالی زنجیره می‌شوند.

از ابتدای شروع بلاکچین بیت کوین، پاداش هر بلاک برابر با ۵۰ بیت کوین بود و بر اساس پروتکل بیت کوین پس از ایجاد هر ۲۱۰٫۰۰۰ بلاک یا تقریبا هر چهار سال یک بار این پاداش نصف می‌شود. با توجه به اینکه در پروتکل بیت کوین تعداد کل بیت کوین ها حداکثر به ۲۱٫۰۰۰٫۰۰۰ می‌رسد، لذا روند نصف شدن پاداش بر اساس محاسبات تا سال ۲۱۴۰ ادامه خواهد یافت و پس از آن دیگر بیت کوین جدیدی به چرخه وارد نشده و تنها کارمزد تعلق خواهد گرفت. در جدول زیر تاریخ های نصف شدن پاداش ها از ابتدا تا کنون آمده است.

تاریخ	تعداد بلاک	دوره	پاداش در هر بلاک	سال	تعداد کل بیت کوین در چرخه
2009-01-03	0	1	50.00	2009	2625000
2010-04-22	52500	1	50.00	2010	5250000
2011-01-28	105000	1	50.00	2011	7875000
2011-12-14	157500	1	50.00	2012	10500000
2012-11-28	210000	2	25.00	2013	11812500
2013-10-09	262500	2	25.00	2014	13125000
2014-08-11	315000	2	25.00	2015	14437500
2015-07-29	367500	2	25.00	2016	15750000
2016-07-09	420000	3	12.50	2016	16406250
2017-06-23	472500	3	12.50	2018	17062500
	525000	3	12.50	2019	17718750
	577500	3	12.50	2020	18375000
	630000	4	6.25	2021	18703125
	682500	4	6.25	2022	19031250
	735000	4	6.25	2023	19359375
	787500	4	6.25	2024	19687500

استخراج و اثبات کار (Mining & Proof of Work)

Image source

فرآیند قراردادن تراکنش ها و ایجاد بلاک و اضافه نمودن آن بلاک به انتهای زنجیره را استخراج می‌نامند. اما کدام بلاک را باید اضافه کرد و کدام نود مجاز است یک بلاک را به انتهای زنجیره اضافه کند. برای حل این مشکل، مکانیزم اثبات کار بوجود آمده است. این مکانیزم می‌گوید اگر یک نود بتواند در فاصله زمانی ایجاد بلاک ها (حدود ۱۰ دقیقه) یک هش با ویژگی خاص را محاسبه نماید، مجاز است تراکنش های ورودی را در یک بلاک قرار داده و آن بلاک را برای تایید و اضافه شدن به انتهای زنجیره، در شبکه منتشر کند. فرآیند تایید، همان مکانیزم توافق جمعی است. پس در واقع هر دو مکانیزم اثبات کار و توافق جمعی برای مقابله با انحصار ایجاد بلاک ها در زنجیره است.

نحوه تایید بلاک در توافق جمعی و محاسبه هش دارای جزئیات فنی است که در مستند دیگری درخصوص مکانیزم کاری بیت کوین، به آن پرداخته خواهد شد. در این جا تنها بصورت ساده اثبات کار تعریف می‌گردد.

$$H\ (\ nonce\ |\ prev\_hash\ |\ tx_1\ |\ tx_2\ |\ \dots\ |\ tx_n\ )\ <\ target$$

هر نود اگر بتواند هشی را محاسبه کند که ورودی آن شامل یک عدد nonce ، هش بلاک قبل و مجموعه ای از تراکنش های جدید باشد به طوری که خروجی هش از یک مقدار معین کمتر گردد و به طور مشخص مثلا با ۱۷ صفر شروع شود، در آنصورت مجاز است که بلاک را ایجاد و منتشر کند.

پیدا کردن مقدار nonce و هش مورد نظر نیاز به توان محاسباتی بسیار زیادی دارد و نیازمند محاسبه میلیاردها میلیارد هش مختلف است و و نیاز به تجهیزات و انرژی زیادی دارد. همین جنبه است که استخراج بیت کوین را بسیار مشکل نموده است.

هش و پارامترهای دیگر از که از یک بلاک نمونه استخراج شده، به شکل زیر است:

Summary	
Height	497913 (Main chain)
Hash	000000000000000000cc3185a8513c17b8fc0c6122913b35610e97939fae13f1
Previous Block	000000000000000000018864208e67492928a37ffd6c942eaa2df953752b0278f
Next Blocks	0000000000000000000b9386873d70422f5d8f878fb086fa67d9fa3b01e6bf7cb
Time	2017-12-06 11:17:38
Received Time	2017-12-06 11:17:38
Relayed By	AntPool
Difficulty	1,347,001,430,558.57
Bits	402706678
Number Of Transactions	2683
Output Total	14,756.50830944 BTC
Estimated Transaction Volume	1,782.85105533 BTC
Size	1053.611 KB
Version	0x20000000
Merkle Root	f89976d38e2cd295144467a51f3728c3905b40388975b8dc3151a78654ee1fde
Nonce	3739062621
Block Reward	12.5 BTC
Transaction Fees	1.15380209 BTC

تنظیم سختی شبکه (Network Difficulty)

به مقدار target سختی شبکه گفته می‌شود. در پروتکل بیت کوین تعیین و تنظیم مقدار سختی شبکه پیش بینی شده و مکانیزمی برای کنترل آن وجود دارد به طوری که ایجاد هر بلاک (پیدا کردن هش مورد نظر) در حدود ۱۰ دقیقه به طول بیانجامد. در این مکانیزم به ازای هر ۲۰۱۶ بلاک و به عبارتی هر دو هفته یک بار تنظیمات انجام می‌شود.

آیا استخراج مقرون به صرفه است؟

برای پاسخ به این سوال دو پارامتر مهم هستند:

- پاداش استخراج = پاداش بلاک + کارمزد تراکنشها
- هزینه استخراج = هزینه تجهیزات + هزینه عملیات (انرژی برق، کولینگ و ...)

حال چنانچه پاداش استخراج بیش از هزینه آن باشد در آن صورت مقرون به صرفه خواهد بود.

تئوری بازی (Game Theory) استخراج

نکته قابل تامل در هزینه های استخراج این است که هزینه سخت افزار حداقل برای یک بازه زمانی ثابت است اما هزینه های برق و کولینگ و ... متغیر است. از طرفی قیمت خود بیت کوین نیز بالا و پایین می‌شود و همین امر استخراج را تبدیل به یک بازی پیچیده می‌کند.