# الگوریتم اثبات انجام کار در مقابل الگوریتم اثبات سهام

## Proof of Work Vs Proof of Stake

**سلمان صادقی**

**۱۳۹۸/۹/۱**

در دنیای رمز ارزها الگوریتم اجماع  یکی از مهمترین و حیاتی‌ترین ویژگی‌های هر شبکه بلاک‌چینی است چراکه این طراحی بهینه مکانیزم اجماع است که مسئولیت حفظ اصالت و امنیت این سیستم توزیع شده را بر عهده دارد.

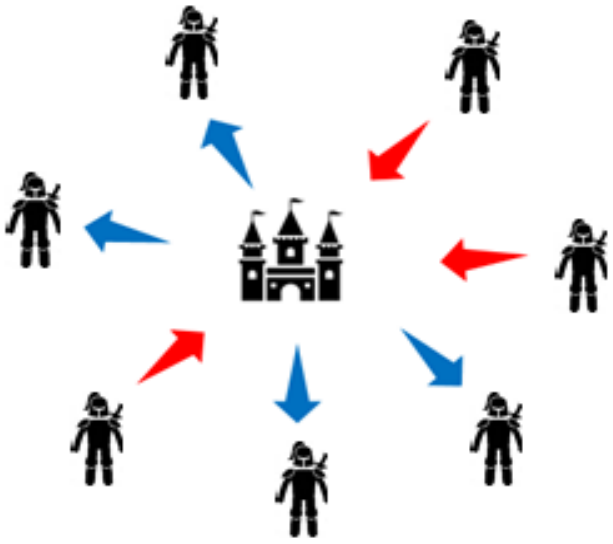
## فهرست مطالب

## مقدمه

در دنیای رمز ارزها الگوریتم اجماع[۱] یکی از مهمترین و حیاتی‌ترین ویژگی‌های هر شبکه بلاک‌چینی است چراکه این طراحی بهینه مکانیزم اجماع است که مسئولیت حفظ اصالت و امنیت این سیستم توزیع شده را بر عهده دارد. اولین الگوریتم اجماع رمز ارزها توسط ساتوشی ناکاموتو ساخته شد و در شبکه بیت‌کوین مورد استفاده قرار گرفت. طراحی مکانیزم اجماع مبتنی بر اثبات انجام کار[۲] در واقع تلاشی بود از سوی ساتوشی برای غلبه بر مسئله گسست بیزانس[۳].

در ابتدا شاید بهتر باشد پیش از ورود به بحث اصلی این متن که مقایسه ویژگی‌های دو الگوریتم اجماع مشهور و پر استفاده در دنیای رمز ارزها یعنی اثبات انجام کار و اثبات سهام[۴] است، مقدمه‌ای داشته باشیم پیرامون اینکه اساسا مسئله گسست بیزانس به چه مفهومی اشاره می‌کند و مکانیزم اجماع دقیقا چیست.

به طور مختصر مشکل فرماندهان بیزانسی[۵] یک دوراهی منطقی است که نشان می‌دهد چگونه یک گروه از فرماندهان بیزانسی ممکن است در ارتباط خود برای رسیدن به یک توافق برای ادامه مسیر فتح و پیروزی به مشکل بربخورند.



فرماندهان بیزانسی قبل از حمله

۱ Consensus Algorithm
۲ Proof of work
۳ Byzantine Fault
۴ Proof of stake
۵ Byzantine Generals problems

## گسست بیزانس چیست

مسئله زمانی آغاز می‌شود که  که فرض کنیم هرکدام از فرماندهان لشکر خود را دارند و هرکدام از این گروه‌ها در موقعیت‌های متفاوت پیرامون شهری مستقر هستند که قرار است آن را فتح کنند. این فرماندهان باید اجماع کنند که می‌خواهند به شهر حمله کنند یا قصد عقب نشینی دارند. مهم اینجا حمله و یا عقب نشینی نیست. مسئله رسیدن به یک اجماع برای انجام آن تصمیم است. خب برای شفافیت بیشتر فرض می‌کنیم:

- هر فرمانده باید یک تصمیم بگیرد.
- وقتی که تصمیم گرفته شد، هیچ کس حق ندارد تصمیم خود را عوض کند.
- تمام فرماندهان موظف هستند بر اجرای یک تصمیم اجماع کرده و بر اساس یک روش هماهنگ آن را اجرا کنند.

مسئله‌ی ارتباط ذکر شده بین فرماندهان بیزانسی از آنجا پررنگ می‌شود که بدانیم هرکدام از فرماندهان تنها از طریق پیام فرستادن توسط پیک می‌تواند با یک فرمانده دیگر ارتباط داشته باشد. مشخص است که پیام می‌تواند دیر به دست فرمانده دیگر برسد و یا گم و مخدوش شود. علاوه بر این حتی اگر پیام به طور موفقیت آمیز دریافت شود، ممکن است بعضی از فرماندهان جاسوس باشند و قصد ارسال پیام گمراه کننده و نامعتبر به دیگر فرماندهان داشته باشند.

اگر این استعاره از فرماندهان بیزانسی را به موضوع بلاک‌چین مرتبط کنیم، هرکدام از فرماندهان نقش یک گره را در شبکه ایفا می‌کنند. گره‌ها باید در رابطه با وضعیت سیستم به اجماع برسند. به بیان دیگر اکثریت مشارکت‌کنندگان در یک شبکه توزیع شده باید برای جلوگیری از شکست شبکه بر سر اجرای یک موضوع توافق حاصل کنند. بنابراین تنها راه رسیدن به توافق در این سیستم‌های توزیع شده این است که حداقل دو سوم از گره ها صادقانه عمل کنند. به این معنی که اگر تعداد زیادی از افراد شبکه بخواهند اطلاعات ناصحیح مخابره کنند، سیستم در معرض خطر شکست قرار خواهد گرفت. (مانند حمله ۵۱ درصدی در شبکه‌های اثبات انجام کار)

## تحمل خطای بیزانس چیست

به بیان ساده، تحمل خطای بیزانس ویژگی یک سیستم است که آن را از شکست به دلیل مشکل فرماندهان بیزانسی مصون می‌کند؛ به این معنی که سیستم بتواند درصورتی‌که برخی از گره‌ها صادقانه رفتار نکنند و قصد شکست سیستم را داشته باشند، به عملکرد خود ادامه دهد.

طبیعتا در دنیای بلاک‌چین پاسخ‌های متفاوتی به این مسئله وجود دارد و همین تفاوت پاسخ‌هاست که شیوه‌های گوناگون رسیدن به یک اجماع را ممکن می‌سازد؛ چیزی که به آن اگوریتم اجماع می‌گویند.

## الگوریتم اجماع و انواع آن

می‌توان الگوریتم اجماع را مکانیزمی تعریف کرد که توسط آن گره‌های شبکه به اجماع می‌رسند. مشهورترینِ این اگوریتم‌ها اثبات انجام کار و اثبات سهام هستند.

زمانی‌که ساتوشی ناکاموتو درحال طراحی اولین رمز ارز تاریخ بود، باید راهی پیدا می‌کرد که تراکنش‌ها بدون نیاز به وجود یک نهاد مرکزی و یا فرد واسط، تایید شوند. او به این مهم با ابداع اثبات انجام کار دست پیدا کرد.

در واقع اثبات انجام کار مشخص می‌کند که چگونه بلاک‌چین به اجماع می‌رسد. اجماع بر سر اینکه کسی در شبکه درحال انجام کار بدی نیست و برای مثال هیچکس یک پول را دوبار خرج نکرده است. اساس الگوریتم اثبات انجام کار بر ریاضیات پیچیده‌ای استوار است که از مشتقات علم رمزنگاری‌ست. به این دلیل است که بیت‌کوین و اتریوم را رمز ارز می‌نامند.

### اثبات انجام کار: چگونه تراکنش‌ها معتبر می‌شوند

همانطور که می‌توان تصور کرد، هزاران نفر درحال استفاده از بیت‌کوین و اتریوم در سرتاسر دنیا هستند. در اینجا برای توضیح بیشتر از الگوریتم اثبات انجام کار در شبکه بیت‌کوین صحبت می‌کنیم. واضح است که در بلاک‌چین‌های دیگر نیز روال مشابه بیت‌کوین است با تفاوت‌هایی در جزئیات.

تراکنش‌های بیت‌کوین ده دقیقه زمان نیاز دارند تا به طور کامل تایید شوند. در هر بازه زمانیِ ده دقیقه‌ای به اصطلاح یک بلاک جدید به زنجیره اضافه می‌شود. هر بلاک حاوی اطلاعات تراکنش‌هاست، تراکنش‌هایی که هرکدام به صورت مجزا نیز باید تایید شوند. در شبکه بیت‌کوین این مهم توسط افرادی انجام می‌شود که پردازنده‌های خود را به منظور حل یک الگوریتم رمزنگاری شده یا همان انجام اثبات کار اختصاص می‌دهند.

وقتی که این مهم انجام می‌شود، نه تنها تراکنش‌ها به طور کامل تایید می‌شوند، بلکه در بلاک‌چین نیز در معرض نمایش عموم قرار می‌گیرند. این افراد برای پرداخت هزینه محاسباتی خود به عنوان پاداش بیت‌کوین جایزه می‌گیرند. مسئله مهم این است که بدانیم هرکسی که کار محاسباتی انجام می‌دهد پاداش را دریافت

نمی‌کند. افراد بسیاری برای حل الگوریتم‌های رمزنگاری شده، پردازنده‌های خود را بـه رقابـت مـی اندازنـد و کسی که اولین بار معادله‌ای را حل می‌کند پاداش را دریافت خواهد کرد.

به خاطر طراحی ویژه این پازل‌های رمزنگاری شده، تنها از طریق آزمون و خطا می‌توان به پاسخ آنهـا رسـید. در ادامه به منظور روشن‌تر شدن این مسئله مثالی ساده را باز خواهیم کرد.

فرض کنید مسئله موجود در پازل، اثبات حل معادله ساده ۵ + ۷ باشد: استخراج‌کننـده اول بـه جـواب‌هـای ۱۳، ۱۱ و ۱۵ رسیده است. استخراج‌کننده دوم بـه جـواب‌هـای ۱۰، ۱۵ و ۱۲ رسـیده اسـت. همـانطور کـه مشخص است استخراج‌کننده دوم در تلاش سوم خود به جواب درسـت رسـیده اسـت و پـاداش اسـتخراج را دریافت خواهد کرد. در دنیای واقعی کامپیوترها قادرند محاسبات پیشـرفته‌ای را در کسـرهای زمـانی کوتـاه انجام دهند؛ محاسباتی که نیازمند حجم بالایی از الکتریسیته است.

به طورکلی هرچه سخت افزار بهتری داشته باشید، شانس بیشتری برای استخراج و حل پازل داریـد. عادلانـه به نظر نمی‌رسد. این طور نیست؟ هرچند تفاوت‌هایی در مکانیزم‌های مختلف اثبات انجام کار وجود دارد، امـا توضیحات فوق رفتار اصلی الگوریتم اثبات انجام کار را روشن می‌کند.

### اثبات سهام؛ چگونه تراکنش‌ها معتبر می‌شوند

اثبات سهام از یک الگوریتم متفاوت برای تایید تراکنش‌ها استفاده می‌کند. سیسـتم هنـوز از یـک الگـوریتم رمزنگاری شده استفاده می‌کند اما نوع مکانیزم متفاوت است.

در اثبات سهام ساخت بلاک جدید به جای حل معادلات پیشرفته توسط پردازنـده‌هـا، بـه مقـدار ارز سـپرده شده توسط افراد بستگی دارد. به این معنی که هرچه ارز بیشتری را سـپرده کـرده باشـید، شـانس بیشـتری برای ساخت بلاک جدید خواهید داشت.

در واقع این افرادِ حاضر در اثبات سهام، استخراج‌کننده نیستند؛ به آنها فورجر[۶] مـی‌گوینـد. بـرخـلاف اثبـات انجام کار، در اینجا از پاداش خبری نیست، بلکه کسانی که با سـپرده‌گـذاری ارزهـای خـود در اثبـات سـهام مشارکت می‌کنند هزینه ارسال تراکنش را دریافت خواهند کرد.

در ابتدا برای مشارکت در شبکه، افراد باید مقداری از ارزهای خود را در یک کیف پول مخصوص قرار دهنـد. کیف پول موجودی آنها را فریز می‌کند، از آن جهت که از ارزها قرار است برای اثبـات سـهام اسـتفاده شـود.

[۶] Forgers

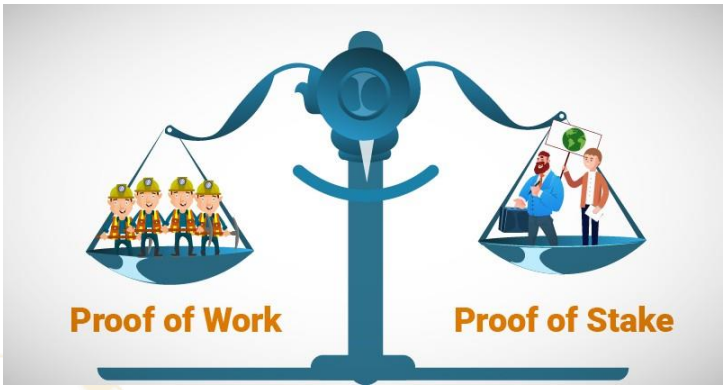
بیشتر بلاک‌چین‌هایی که از این الگوریتم استفاده می‌کنند محدودیت‌هایی را برای حداقل ارز سپرده شده قائل می‌شوند.

فرض کنید که شما مینیمم ارز مورد نیاز را مشارکت کرده‌اید. شانس شما برای دریافت هزینه تراکنش با درصد سپرده شما از کل ارزهای سپرده شده مرتبط است. مسئله مهمی که الگوریتم اثبات سهام را معتبر می‌کند این است که کسانی که ارزهای خود را سپرده می‌کنند، قطعا دنبال انجام درست امور هستند و اجازه خواهند داد که شبکه امن بماند. اگر کسی از فورجرها بخواهد سیستم را هک کند و یا اطلاعات نامعتبر وارد شبکه کند تمام ارزهای سپرده شده خود را از دست خواهد داد.

باتوجه به مطلب بالا هرچه سپرده بیشتری داشته باشید، پاداش بیشتری دریافت می‌کنید؛ درصورت بروز اعمال مجرمانه نیز هزینه بیشتری پرداخت خواهید کرد! ساده و شگفت انگیز است. این طور نیست؟

## کدام یک بهتر است؟ اثبات انجام کار یا اثبات سهام

در الگوریتم اثبات انجام کار مشکلاتی وجود دارد که باتوجه به آنها ما معتقد هستیم که اثبات سهام به مراتب الگوریتم بهینه‌تری برای تایید تراکنش‌هاست. در ادامه به برخی از این مشکلات پرداخته‌ایم.




### متمرکز سازی

همانطور که پیش‌تر اشاره شد، در الگوریتم اثبات انجام کار افرادی که پردازنده‌های قوی‌تری دارند شانس بیشتری برای دریافت پاداش خواهند داشت؛ چیزی که نهادهای متمرکز را ترغیب خواهد کرد تا با خرید دستگاه‌های استخراج بیشتر و ایجاد استخرهای استخراج شانس خود را برای دریافت پاداش افزایش دهند.

نتیجه این تمرکزگرایی این است که اکنون چهار استخر استخراج که اکثرا به دلیل برق ارزان در چین قرار دارند کنترل بیش از ۵۰ درصد استخراج شبکه بیت‌کوین را برعهده دارند. این یک مکانیزم ناعادلانه است

زیرا میانگین افراد شانسی برای دریافت پاداش استخراج ندارند. اینجا اثبات سهام تفاوت ایجاد می‌کند. اثبات سهام از ملحق شدن افراد به همدیگر برای افزایش شانس دریافت پاداش جلوگیری می‌کند. در واقع سلطه استخرها در الگوریتم اثبات سهام معنایی ندارد. افراد با توجه به نسبت ارز سپرده شده خود پاداش دریافت خواهند کرد.

### مصرف برق

در الگوریتم اثبات انجام کار به دلیل پیچیدگی معادلات رمزنگاری شده مقدار مصرف الکتریسیته بالاست. نتایج مطالعات اخیر نشان می‌دهد که مقدار برق مورد نیاز برای شبکه بیت‌کوین از مقدار مورد نیاز برای ۱۵۹ کشور دنیا بیشتر است. نه تنها این نشانی از آسیب‌رسانی به محیط زیست است، بلکه نشان دهنده عدم استقبال در پذیرش در آینده‌ای نزدیک می‌باشد. در الگوریتم اثبات سهام نیاز به حل این معادلات پیچیده وجود ندارد و در نتیجه برق بسیار کمتری مصرف می‌شود.

### خطر حمله ۵۱ درصدی

وضعیتی است که فرد یا گروهی کنترل بیش از ۵۰ درصد توان پردازشی شبکه را به دست آورند. در این صورت در شرایطی آنها خواهند توانست در اطلاعات ثبت شده در بلاک‌ها به نفع خود تغییراتی ایجاد کنند. مثال اخیر حمله‌ی ۵۱ درصدی، اتفاقی بود که در شبکه ورج (XVG) رخ داد. افراد مهاجم توانستند ۳۵ میلیون ورج معادل ۱,۷۵ میلیون دلار را به سرقت ببرند.

وقتی که از اگوریتم اثبات سهام استفاده می‌شود از نظر اقتصادی به صرفه نیست که فرد یا گروهی حمله ۵۱ درصدی را آغاز کنند؛ چراکه آنها باید ۵۱ درصد ارزهای در گردش را سپرده‌گذاری کنند. تنها راه تملک این مقدار ارز خرید آن از بازار است. با شروع خریدِ این مقدار به علت قانون عرضه و تقاضا قیمت ارز مورد نظر افزایش یافته و آن فرد یا گروه باید مبلغ بیشتری بابت خرید خود پرداخت کنند. با متوجه شدن سایر افراد شبکه از این قصد، فرد یا گروه مورد نظر دارایی‌های خود که صرف این خرید شده را نیز از دست خواهند داد.

## معایب الگوریتم اثبات سهام

بعضی‌ها فکر می‌کنند الگوریتم اثبات سهام نابرابری را افزایش می‌دهد. افراد ثروتمندتر کوین‌های بیشتری خریداری می‌کنند و با سپرده کردن آنها سود بیشتری نیز کسب می‌کنند. نکته قابل توجه این است که

چنین ایرادی به الگوریتم اثبات انجام کار نیز وارد است. افراد ثروتمندتر دستگاه‌های استخراج بیشتری خریداری می‌کنند و پاداش بیشتری نیز کسب می‌کنند.

بحث بعدی نحوه جلوگیری از خرج مجدد پول در این دو الگوریتم است. خرج مجدد پول حالتی است که فرد پول خود را به آدرس دیگری انتقال داده اما پیش از تایید شدن این تراکنش در شبکه قصد دارد مجددا پول خود را خرج نماید. در الگوریتم اثبات انجام کار این تلاش بی‌نتیجه خواهد ماند چراکه استخراج‌کننده‌ها با دیدن تراکنش تایید شده اول، تراکنش بعدی را به رسمیت نخواهند شناخت. در الگوریتم اثبات سهام به دلیل اینکه برای فورجر استخراج در زنجیره‌های مختلف هزینه‌بر نیست، اساسا امکان خرج مجدد پول وجود ندارد. در حالت کلی می‌توان گفت که خرج مجدد پول مشکل الگوریتم اثبات سهام نیست.

## نتیجه‌گیری

در پایان این مقاله باید توجه داشت که الگوریتم اثبات انجام کار که اکنون در شبکه‌های متعددی نظیر بیت‌کوین، اتریم و دش مورد استفاده قرار می‌گیرد دارای معایب زیادی است. از خطر حمله ۵۱ درصدی تا مصرف بالای انرژی و ایجاد قدرت خودمختاری برای استخرهای استخراج. با توجه به این مسائل الگوریتم‌های اجماع دیگری نظیر اثبات سهام توسعه پیدا کردند.

نگارنده معتقد است که الگوریتم اثبات سهام به مراتب موثرتر و کارآمدتر از الگوریتم اثبات انجام کار عمل می‌کند. اگر شما خواننده محترم با این نگاه هم عقیده نیستید، خواهشمندم نظرات خود را با ما در میان بگذارید.

## منابع

https://www.bitdegree.org/tutorials/proof-of-work-vs-proof-of-stake/

https://changelly.com/blog/what-is-proof-of-stake/

https://en.bitcoin.it/wiki/Proof_of_Stake#Double-spending_prevention

https://www.binance.vision/blockchain/byzantine-fault-tolerance-explained

**نویسنده**

نام نویسنده: سلمان صادقی

ایمیل نویسنده: salli.sadeghi@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