




# الگوریتم اثبات اعتبار چیست؟

 [www.kifpool.me](http://www.kifpool.me)

 Proof of Authority

وبلاگ کیف پول من 

## الگوریتم اثبات اعتبار (POA)

بدون شک تاکنون از خود پرسیده‌اید که امروزه قابل اطمینان‌ترین و امن‌ترین الگوریتم در انجام تراکنش‌های ارزی، چه الگوریتمی است یا به عنوان مثال کدام الگوریتم تراکنش‌های بیشتری را در ثانیه انجام می‌دهد؟ فضای ارزهای رمزنگاری شده روز به روز در حال تغییر است و مکانیسم‌های اجماع مختلفی برای دستیابی به اجماع در یک سیستم بلاک چین پیشنهاد می‌شود. با تغییر دنیای ارزها، دیگر الگوریتم اثبات کار (POW) که توسط بیت کوین استفاده می‌شود، مقیاس پذیر نیست و عملکرد محدودی دارد. در حال حاضر الگوریتم اثبات اعتبار (POA) به عنوان جایگزینی برای دو الگوریتم اثبات کار (POW) و الگوریتم اثبات سهام (POS) اجرا می‌شود و تراکنش‌های بیشتری را در ثانیه انجام می‌دهد. در این مطلب از وبلاگ کیف پول من به بررسی دقیق الگوریتم اثبات اعتبار و کاربردها و ویژگی آن به عنوان الگوریتمی که راه حلی موثر برای شبکه‌های بلاکچینی است، می‌پردازیم.

### آشنایی با الگوریتم اثبات اعتبار (Proof of Authority)

الگوریتم اثبات اعتبار (Proof Of Authority) که به اثبات صلاحیت نیز معروف است، به عنوان مکانیزمی برای افزایش مقیاس پذیری در شبکه‌های بلاک چین عمل

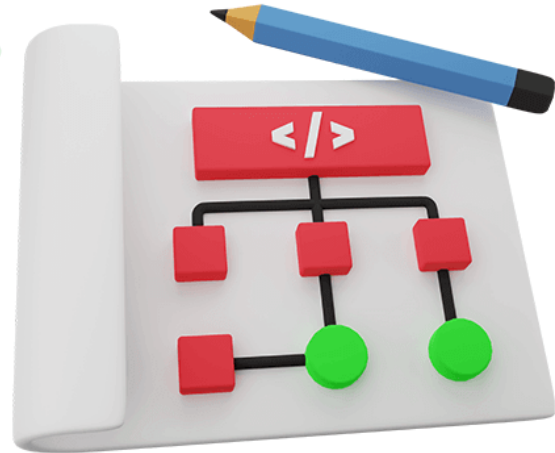
می‌کند. در الگوریتم اثبات کار (POW) انرژی بالایی برای امنیت و اعتبار شبکه مصرف می‌شود و در شبکه اثبات کار بیت کوین، هر تراکنش حداقل به 10 دقیقه زمان نیاز دارد تا انجام شود که بسیار کند است. در اثبات سهام نیز سپرده گذاری ارزها به تامین امنیت و اعتبار شبکه کمک می‌کند؛ اما در الگوریتم اثبات اعتبار (POA) به جای استفاده از سپرده گذاری ارزهای دیجیتال، سپرده گذاری اعتبار به کار می‌رود.

## **مطلب پیشنهادی : اطلاعات جامع و کاربردی شبکه بیت کوین**

### **عملکرد الگوریتم اثبات اعتبار (POA)**

الگوریتم اثبات اعتبار از اعتبار افراد به جای سپرده گذاری کوین‌ها یا توکن‌ها، برای تایید تراکنش‌ها و ساختن بلاک‌های جدید در شبکه استفاده می‌کند. در این الگوریتم برای کسب حقوق بلوک‌های جدید، یک گره باید احراز هویت کند. در گواه اثبات اعتبار، اعتبارسنج‌های شبکه یا همان ولیدیتورها (Validators) به صورت تصادفی و در طی فرایندی دشوار انتخاب می‌شوند و توسط سایر نودهای فعالیت کننده قدیمی، نودهای جدید نیز مورد تایید قرار می‌گیرند. این عملیات باعث می‌شود تا از دسترسی نودهای بدکار که سیستم را با مشکل مواجه می‌کنند، جلوگیری شود. این الگوریتم به عنوان نوعی مکانیسم توافقی برای شرکت‌ها و سازمان‌های خصوصی که قصد دارند زنجیره‌های خود را بسازند، کاربردی است.

## هدف الگوریتم اثبات اعتبار



هدف اصلی در سیستم‌های مبتنی بر اعتبار، اثبات هویت اعتبارسنج‌ها برای جلوگیری از حملاتی از جمله DOS است که البته مدت‌ها بعد به دلیل پتانسیل‌های آن، این الگوریتم در بلاک چین‌های خصوصی و شرکت‌ها به کار برده شد. پروسه انتخاب الگوریتم اثبات اعتبار :

### مزایای استفاده از الگوریتم اثبات اعتبار

الگوریتم اثبات اعتبار مزایای زیادی دارد که آن را به عنوان الگوریتمی بهتر و جایگزین تبدیل می‌کنند:

- الگوریتم اثبات اعتبار در برابر حملات 51 درصد و حملات داس مقاوم است.
- این مکانیزم سرعت بسیار بالایی در اعتبار سنجی و تایید تراکنش‌ها دارد.
- اثبات اعتبار به سخت‌افزارهای مخصوص برای ساخت بلاک‌های جدید نیاز ندارد.

- الگوریتم اثبات اعتبار در مقایسه با سایر شبکه‌های بلاک چین اثبات کار و اثبات سهام، بسیار مقیاس پذیر است.

- از روش اثبات اعتبار به دلیل کارایی بسیار بالای آن با عنوان روش اثبات اقتدار نیز یاد می‌شود.

- در این الگوریتم برای رسیدن به اجماع گره‌ها هیچ ارتباط خاصی مورد نیاز نیست.

### **معایب استفاده از الگوریتم اثبات اعتبار**

متمرکز بودن را می‌توان بزرگ‌ترین مشکل مکانیسم اثبات اعتبار در نظر گرفت؛ به دلیل اینکه برتری بلاک چین با توجه به تمرکز گریزی آن معنا می‌دهد. این الگوریتم علاوه بر ویژگی‌های برتر خود معایبی نیز دارد:

- شبکه‌های مبتنی بر این الگوریتم، فاقد تمرکززدایی لازم هستند و اثبات اعتبار تمرکز گریزی خود را فدای مقیاس پذیری می‌کند.

- مقاومت اثبات اعتبار در برابر سانسور تضمین شده نیست؛ به بیانی دیگر اطلاعات در این مکانیسم قابل دستکاری هستند.

- هویت تمامی اعتبار سنج‌ها برای هر فردی قابل دسترسی است که این موضوع می‌تواند دستکاری اطلاعات توسط اشخاص ثالث را رقم بزند.

## **مقایسه مکانیزم اثبات اعتبار با اثبات سهام**

### **مطلب پیشنهادی : الگوریتم اثبات سهام (POS) چیست ؟**

برخی کاربران فعال در این زمینه، مکانیزم اثبات اعتبار را تنها نسخه تعدیل یافته الگوریتم اثبات سهام می‌دانند که به جای هویت، از کوین استفاده می‌کنند. ماهیت اکثر شبکه‌های لاک چین غیرمتمرکز است و اثبات سهام نیز برای مشاغل خاص توصیه نمی‌شود؛ اما POA می‌تواند راه حل مناسب‌تری برای بلاک چین خصوصی باشد؛ چراکه عملکرد آن به طور قابل توجهی بالاتر است.

## پروژه‌هایی که از الگوریتم اثبات اعتبار استفاده می‌کنند



### پروژه‌هایی که از الگوریتم اثبات اعتبار استفاده می‌کنند



معروف‌ترین شبکه‌ای که از مکانیزم اثبات اعتبار استفاده می‌کند، POA Network است که ارز دیجیتال آن با نماد POA در بازار کریپتو عرضه می‌شود. در این پروژه نودها از اعتبارسنج‌های انفرادی تشکیل شده است که از دیتابیس‌های عمومی به عنوان مکانیزم شایستگی اعتبارسنج‌ها استفاده می‌شود. هایپرلجر بسو و هایپر فابریک نیز از این مکانیزم اجماع استفاده می‌کنند. هایپرلجر فابریک (Hyperledger Fabric) بر اساس تحمل خطای بیزانس (Byzantine Fault Tolerant) فعالیت می‌کند اما از اثبات اعتبار به عنوان بخشی از فریم ورک متن باز برای جامعه بلاک چین‌های خصوصی خود استفاده می‌کند. مدیریت زنجیره‌های تامین و لجستیک تخصص این شبکه است. پروژه **وی چین** (VeChain) یکی دیگر از پروژه‌های مشهوری است که از الگوریتم اثبات اعتبار استفاده می‌کند و ارز دیجیتال آن با نماد **VET** در بازار کریپتو عرضه می‌شود.

## الگوریتم اثبات اعتبار و دلیل اهمیت آن

الگوریتم اثبات اعتبار برای اولین بار در سال 2017 فعالیت خود را آغاز کرد و با گذشت زمان کاربردهای آن گسترش یافت. در حالت کلی می‌توان گفت هدف این مکانیزم اجماع، شرکت‌های بزرگ هستند و تعداد اعتبارسنج‌ها در این الگوریتم بسیار کم است. اثبات اعتبار در بلاک چین‌های عمومی کاربرد چندانی ندارد و برای شرکت‌ها و سازمان‌های خصوصی که قصد دارند زنجیره‌های خود را بسازند، کاربردی است. در این الگوریتم، بلاک چین توسط نودهای اعتبارسنج محافظت می‌شود و ارزش‌های دیجیتالی که از اثبات اعتبار استفاده می‌کنند، قابلیت استخراج ندارند. مقیاس پذیر بودن این الگوریتم و سرعت بسیار بالای آن در اعتبارسنجی و تایید تراکنش‌ها به عنوان یکی از مزایای بزرگ اثبات اعتبار در کنار سایر ویژگی‌های مثبت آن مانند مقاوم در برابر حملات 51 درصد و حملات داس در نظر گرفته می‌شود. در این مطلب از وبلاگ کیف پول من الگوریتم اثبات کار را به صورت دقیق بررسی کردیم. می‌توانید سوالات خود را در بخش نظرات با کارشناسان ما در میان بگذارید کارشناسان کیف پول من در اسرع وقت به سوال شما پاسخ دهند.