# Proof-of-Stake (PoS)

Пълна биография9-11 minutes 3.05.2017 г.

## Какво представлява Proof-of-Stake (PoS)?

Proof-of-stake е консенсусен механизъм за криптовалута за обработка на транзакции и създаване на нови блокове в блокчейн. Механизмът за консенсус е метод за валидиране на записи в разпределена база данни и поддържане на базата данни защитена. В случай на криптовалута, базата данни се нарича блокова верига - така че консенсусният механизъм защитава блоковата верига.

Научете повече за proof-of-stake и как се различава от proof-of-work. Освен това разберете проблемите, които proof-of-stake се опитва да реши в индустрията на криптовалутите.

### Ключови изводи

* С proof-of-stake (POS) собствениците на криптовалута валидират блокови транзакции въз основа на броя монети, заложени от валидатора.
* Proof-of-stake (POS) е създаден като алтернатива на Proof-of-work (POW), оригиналния консенсусен механизъм, използван за валидиране на блокчейн и добавяне на нови блокове.
* Докато PoW механизмите изискват миньорите да решават криптографски пъзели, PoS механизмите изискват валидаторите просто да държат и залагат токени.
* Proof-of-stake (POS) се счита за по-малко рисков по отношение на потенциала за атака в мрежата, тъй като структурира компенсацията по начин, който прави атаката по-малко изгодна.
* Следващият записващ блок в блокчейна се избира на случаен принцип, като по-високи коефициенти се присвояват на възли с по-големи позиции на залога.

0 seconds of 2 minutes, 12 secondsСила на звука 75%

00:00 часа

00:00 часа

02:12

#### Щракнете върху Игра, за да научите всичко за Proof-of-Stake

## Разбиране на Proof-of-Stake (PoS)

Proof-of-stake намалява количеството изчислителна работа, необходима за проверка на блокове и транзакции, които поддържат [блокчейна](https://www.investopedia.com/terms/b/blockchain.asp) и по този начин криптовалутата защитени. Proof-of-stake променя начина, по който блоковете се проверяват с помощта на машините на собствениците на монети. Собствениците предлагат своите монети като обезпечение за възможността да валидират блокове. Собствениците на монети със заложени монети след това стават „валидатори“.1

След това валидаторите се избират произволно за „копаене“ или валидиране на блока. Тази система рандомизира кой стига до „моето“, вместо да използва основан на конкуренцията механизъм като доказателство за работа.1

За да стане валидатор, собственикът на монети трябва да "заложи" определено количество монети. Например, [Ethereum](https://www.investopedia.com/terms/e/ethereum.asp) ще изисква 32 ETH да бъдат заложени, преди даден потребител да може да стане валидатор.1Блоковете се валидират от повече от един валидатор и когато определен брой валидатори потвърдят, че блокът е точен, той се финализира и затваря.

За да активирате свой собствен валидатор, ще трябва да заложите 32 ETH; обаче не е нужно да залагате толкова много ETH, за да участвате в валидирането. Можете да се присъедините към пулове за валидиране, като използвате „течен залог“ или заложите ERC-20 токен, който представлява вашия ETH.2

Различните механизми за доказване на дял може да използват различни методи за валидиране на блокове. Например, когато Ethereum въведе шардинг, валидатор ще провери транзакциите и ще ги добави към блок на сегмент, което изисква най-малко 128 валидатора в комисия3. След като шардовете са валидирани и блоковете са създадени, две трети от валидаторите трябва да се съгласят, че транзакцията е валидна, след което блокът се затваря.

За да обобщим процеса на Ethereum PoS, може да кажете, че това е споделяне на валидиране в мрежа за криптовалута, вместо състезание за валидиране.

## По какво се различава Proof-of-Stake от Proof-of-Work?

И двата консенсусни механизма помагат на блокчейните да синхронизират данни, да валидират информация и да обработват транзакции. Всеки метод се е доказал като успешен при поддържането на блокчейн, въпреки че всеки има плюсове и минуси. Двата алгоритъма обаче имат много различни подходи.

При PoS създателите на блокове се наричат ​​валидатори. Валидаторът проверява транзакциите, проверява дейността, гласува за резултатите и поддържа записи. Под PoW създателите се наричат ​​​​миньори. Миньорите решават сложни математически проблеми, за да проверят транзакции; в замяна.

За да „купят“ позицията да станат създатели на блокове, инвеститорите трябва само да закупят достатъчния лимит от монети или токени, необходими, за да станат валидатор за PoS блокчейн. За PoW миньорите трябва да инвестират в оборудване за обработка и да поемат големи такси за енергия, за да захранват машините, които се опитват да решат изчисленията.

Разходите за оборудване и енергия при PoW механизмите са скъпи, ограничавайки достъпа до копаене и укрепвайки сигурността на блокчейна. Въпреки това PoS блокчейните често позволяват по-голяма мащабируемост поради тяхната енергийна ефективност.

### Механизми за консенсус

Доказателство за залог

Създателите на блокове се наричат ​​валидатори

Участниците трябва да закупят монети или токени, за да станат валидатор

Енергийна ефективност

Позволява повече мащабируемост

Мрежовият контрол може да бъде закупен

Валидаторите получават такси за транзакции като награди

Доказателство за работа

Създателите на блокове се наричат ​​копачи

Участниците трябва да закупят оборудване и енергия, за да станат миньори

Не е енергийно ефективен

Не позволява повече мащабируемост

Стабилна сигурност поради скъпи предварителни изисквания

Копачите получават блокови награди

## Цели на Proof-of-Stake

Доказателството за залог е предназначено да намали [опасенията за скалируемост и екологична устойчивост](https://www.investopedia.com/nfts-and-the-environment-5220221) около протокола за доказателство за работа (PoW). [Доказателството за работа](https://www.investopedia.com/terms/p/proof-work.asp) е конкурентен подход за проверка на транзакции, което естествено насърчава хората да търсят начини да получат предимство, особено след като е включена парична стойност.

Копачите на биткойни печелят биткойни, като проверяват транзакции и блокове. Те обаче плащат оперативните си разходи като електричество и наем с [фиатна валута](https://www.investopedia.com/terms/f/fiatmoney.asp) . Това, което наистина се случва тогава, е, че миньорите обменят енергия за криптовалута. Количеството енергия, необходимо за копаене на криптовалута с доказателство за работа, влияе дълбоко върху пазарната динамика на ценообразуването и рентабилността. Има и аспекти на околната среда, които трябва да се вземат предвид, тъй като добивът на [PoW](https://www.investopedia.com/tech/how-does-bitcoin-mining-work/) използва толкова енергия, колкото една малка държава.4

PoS механизмът се стреми да разреши тези проблеми чрез ефективно заместване на залагането с изчислителната мощност, при което способността за копаене на индивида се рандомизира от мрежата. Това означава, че трябва да има драстично намаляване на потреблението на енергия, тъй като миньорите вече не могат да разчитат на масивни ферми от хардуер с едно предназначение, за да получат предимство.

Първата [криптовалута](https://www.investopedia.com/terms/c/cryptocurrency.asp) , приела PoS метода, беше [Peercoin](https://www.investopedia.com/terms/p/peercoin.asp) . Nxt, Blackcoin и ShadowCoin скоро последваха примера.

## Сигурност с доказателство за залог

Дълго рекламирана като заплаха за феновете на криптовалутата, [атаката от 51%](https://www.investopedia.com/terms/1/51-attack.asp) е проблем, когато се използва PoS, но е много малко вероятно. Атака от 51% е, когато някой контролира 51% от криптовалута и използва това мнозинство, за да промени блокчейна. В PoS група или индивид ще трябва да притежават 51% от заложената криптовалута.

Не само е много скъпо да притежавате 51% от заложената криптовалута – заложената валута е обезпечение за привилегията да „копаете“. Копачите, които се опитват да върнат блок чрез 51% атака, ще загубят всичките си заложени монети. Това създава стимул за миньорите да действат добросъвестно в полза на криптовалутата и мрежата.1

Повечето други функции за сигурност на PoS не се рекламират, тъй като това може да създаде възможност за заобикаляне на мерките за сигурност. Повечето PoS системи обаче разполагат с допълнителни функции за сигурност, които добавят към присъщата сигурност зад блокчейните и PoS механизмите.1

## Какво е Proof-of-Stake срещу Proof-of-Work?

Proof of Stake (POS) използва произволно избрани миньори за валидиране на транзакции. Доказателството за работа (POW) използва конкурентен метод за валидиране, за да потвърди транзакциите и да добави нови блокове към блокчейна.

## Сертификат ли е Proof-of-Stake?

Proof-of-stake е консенсусен механизъм, при който валидаторите на криптовалута споделят задачата да валидират транзакциите. Към момента няма издадени сертификати.

## Как печелите Proof-of-Stake?

Доказателството за залог (POS) е вграден консенсусен механизъм, който се използва от мрежата или валидаторите на криптовалута. Тя не може да бъде спечелена, но можете да помогнете за защитата на мрежа и да печелите награди, като използвате клиент за криптовалута, който участва в валидирането на PoS или става валидатор.5

## Може ли биткойн да се конвертира в Proof-of-Stake?

Възможно е Bitcoin да се промени на proof-of-stake. Etherum започна своето съществуване с помощта на PoW и преминава към PoS, но процесът може да отнеме години, за да се внедри във вече установена криптовалута.

Инвестирането в криптовалути и други първоначални предложения за монети („ICO“) е много рисковано и спекулативно и тази статия не е препоръка от Investopedia или автора да инвестирате в криптовалути или други ICO. Тъй като ситуацията на всеки индивид е уникална, винаги трябва да се консултирате с квалифициран специалист, преди да вземете каквото и да е финансово решение. Investopedia не прави декларации или гаранции по отношение на точността или навременността на информацията, съдържаща се тук.