# Proof of Work (PoW)

Пълна биография7-9 minutes 15.09.2016 г.

## Какво е доказателство за работа (PoW)?

Proof of work (PoW) describes a system that requires a not-insignificant but feasible amount of effort in order to deter frivolous or malicious uses of computing power, such as sending spam emails or launching denial of service attacks. The concept was subsequently adapted to securing digital money by Hal Finney in 2004 through the idea of "reusable proof of work" using the SHA-256 hashing algorithm.12

Following its introduction in 2009, Bitcoin became the first widely adopted application of Finney's PoW idea (Finney was also the recipient of the first bitcoin transaction).3 Proof of work forms the basis of many other [cryptocurrencies](https://www.investopedia.com/terms/c/cryptocurrency.asp) as well, allowing for secure, decentralized consensus.

### Key Takeaways

* Доказателството за работа (PoW) е децентрализиран механизъм за консенсус, който изисква членовете на мрежата да изразходват усилия за решаване на произволен математически пъзел, за да попречат на някой да изиграе системата.
* Доказателството за работа се използва широко в копаене на криптовалута, за валидиране на транзакции и копаене на нови токени.
* Благодарение на доказателството за работа, транзакциите с биткойни и други криптовалути могат да се обработват peer-to-peer по сигурен начин, без да е необходима доверена трета страна.
* Доказателството за работа в мащаб изисква огромно количество енергия, което само се увеличава, когато повече копачи се присъединят към мрежата.
* Доказателството за залог (POS) беше един от няколкото нови консенсусни механизма, създадени като алтернатива на доказателството за работа.

## Разбиране на доказателството за работа

Това обяснение ще се съсредоточи върху доказателството за работа, тъй като функционира в [биткойн](https://www.investopedia.com/terms/b/bitcoin.asp) мрежата. Биткойн е дигитална валута, която е подкрепена от един вид [разпределена книга](https://www.investopedia.com/terms/d/distributed-ledger-technology-dlt.asp) , известна като " [блокчейн](https://www.investopedia.com/terms/b/blockchain.asp) ". Тази книга съдържа запис на всички биткойн транзакции, подредени в последователни „блокове“, така че на нито един потребител не е позволено да харчи което и да е от притежанията си два пъти. За да се предотврати подправяне, счетоводната книга е публична или "разпространена"; променена версия бързо ще бъде отхвърлена от други потребители.4

Начинът, по който потребителите откриват подправяне на практика, е чрез [хешове](https://www.investopedia.com/terms/h/hash.asp) , дълги низове от числа, които служат като доказателство за работа. Поставете даден набор от данни чрез хеш функция (биткойн използва SHA-256) и той ще генерира само един хеш. Поради "ефекта на лавината" обаче, дори малка промяна в която и да е част от оригиналните данни ще доведе до напълно неразпознаваем хеш. Какъвто и да е размерът на оригиналния набор от данни, хешът, генериран от дадена функция, ще бъде със същата дължина. Хешът е еднопосочна функция: не може да се използва за получаване на оригиналните данни, а само за проверка дали данните, генерирали хеша, съответстват на оригиналните данни.1

Генерирането на произволен хеш за набор от биткойн транзакции би било тривиално за модерен компютър, така че за да превърне процеса в „работа“, биткойн мрежата задава определено ниво на „трудност“. Тази настройка се настройва така, че нов блок да бъде „ [копан](https://www.investopedia.com/terms/b/bitcoin-mining.asp) “—добавен към блокчейна чрез генериране на валиден хеш—приблизително на всеки 10 минути.5Трудността при задаване се постига чрез установяване на ["цел" за хеш](https://www.investopedia.com/terms/t/target-hash.asp) : колкото по-ниска е целта, толкова по-малък е наборът от валидни хешове и толкова по-трудно е да се генерира такъв. На практика това означава хеш, който започва с много дълъг низ от нули.

Доказателството за работа първоначално беше създадено като предложено решение на нарастващия проблем със спам имейлите.

## Специални съображения

Тъй като даден набор от данни може да генерира само един хеш, как миньорите се уверяват, че генерират хеш под целта? Те променят входа, като добавят цяло число, наречено [nonce](https://www.investopedia.com/terms/n/nonce.asp) ("номер, използван веднъж"). След като бъде намерен валиден хеш, той се излъчва към мрежата и блокът се добавя към блокчейна.6

Добивът е състезателен процес, но е по-скоро лотария, отколкото състезание. Средно някой ще генерира приемливо доказателство за работа на всеки десет минути, но кой ще бъде той, остава да се гадае.7Копачите се обединяват, за да увеличат шансовете си за копаене на блокове, което генерира такси за транзакции и, за ограничен период от време, награда от новосъздадени биткойни.

Доказателството за работа прави изключително трудно да се промени който и да е аспект на блокчейна, тъй като такава промяна би изисквала повторно копаене на всички следващи блокове. Това също така затруднява потребител или набор от потребители да монополизират изчислителната мощност на мрежата, тъй като машините и мощността, необходими за завършване на хеш функциите, са скъпи.

Ако част от мрежа за копаене започне да приема алтернативно доказателство за работа, това е известно като [хард форк](https://www.investopedia.com/terms/h/hard-fork.asp) .8

## Пример за доказателство за работа

Доказателството за работа изисква компютър произволно да се включи в функциите за хеширане, докато стигне до изход с правилното минимално количество водещи нули. Например, хешът за блок #660000, добит на 4 декември 2020 г., е 00000000000000000008eddcaf078f12c69a439dde30dbb5aac3d9d94e9c18f6. Блоковата награда за този успешен хеш беше 6,25 BTC.9

Този блок винаги ще съдържа 745 транзакции, включващи малко над 1666 биткойни, както и заглавката на предишния блок. Ако някой се опита да промени сумата на транзакция дори с 0,000001 биткойн, полученият хеш ще бъде неразпознаваем и мрежата ще отхвърли опита за измама.

## ЧЗВ за доказателство за работа

### Какво означава доказателство за работа?

PoW изисква възлите в мрежата да предоставят доказателство, че са изразходвали изчислителна мощност (т.е. работа), за да постигнат консенсус по децентрализиран начин и да попречат на лошите участници да превземат мрежата.10

### Как доказателството за работа валидира крипто транзакция?

Самата работа е произволна. За биткойн това включва итерации на SHA-256 хеширащи алгоритми. „Победителят“ от рунда на хеширане обаче събира и записва транзакции от mempool в следващия блок. Тъй като „победителят“ се избира на случаен принцип, пропорционално на свършената работа, това стимулира всички в мрежата да действат честно и да записват само истински транзакции.

### Защо криптовалутите се нуждаят от доказателство за работа?

Тъй като са децентрализирани и peer-to-peer по дизайн, блокчейните като мрежите за криптовалута изискват някакъв начин за постигане както на консенсус, така и на сигурност. Доказателството за работа е един такъв метод, който прави твърде ресурсоемки опити за изпреварване на мрежата. Съществуват и други механизми за доказване, които са по-малко ресурсоемки, но имат други недостатъци или недостатъци, като например [доказателство за залог (PoS)](https://www.investopedia.com/terms/p/proof-stake-pos.asp) и [доказателство за изгаряне](https://www.investopedia.com/terms/p/proof-burn-cryptocurrency.asp) . Без механизъм за доказване мрежата и данните, съхранявани в нея, биха били уязвими за атака или кражба.

### Биткойн използва ли доказателство за работа?

да Той използва PoW алгоритъм, базиран на функцията за хеширане SHA-256, за да валидира и потвърди транзакциите, както и да пусне в обращение нови биткойни.1

### По какво се различава Proof of Stake (PoS) от PoW?

PoS е механизъм за консенсус, който на случаен принцип определя възела, който ще копае или валидира блокиращи транзакции според това колко монети притежава този възел. Колкото повече токени се съхраняват в портфейла, толкова повече мощност за копаене му се предоставя ефективно. Въпреки че PoS е далеч по-малко ресурсоемък, той има няколко други недостатъка, включително по-голям шанс за [51% атака](https://www.investopedia.com/terms/1/51-attack.asp) при по-малки алткойни и стимули да трупате токени и да не ги използвате.11