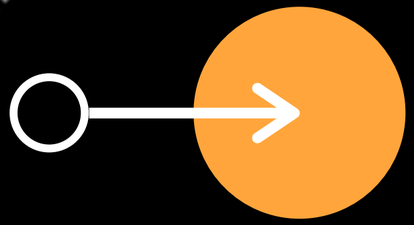
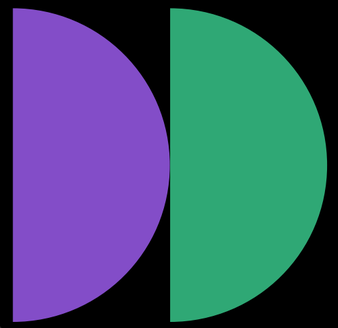
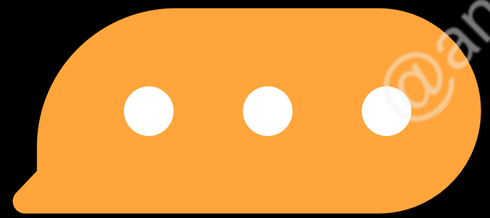
короткий посібник

PoW проти PoS: який алгоритм консенсусу краще?







Алгоритм консенсусу є невід'ємною складовою блокчейну. **Алгоритм консенсусу — це нібито набір правил та вимог, своєрідна Конституція, якої необхідно дотримуватися всім учасникам блокчейну.** Існують сотні **блокчейнів** з різними **"конституціями"**. Кожна має свої переваги та недоліки — швидкість, масштабованість, безпека та рівень децентралізації. Найбільш розповсюдженими **алгоритмами**, які ми розглянемо в даній статті, є **Proof-of-Work** та **Proof-of-Stake**

Proof-of-Work - (PoW) (від англ. proof of work – дослівно: «доказ роботи») — це децентралізований механізм консенсусу, який вимагає від членів мережі (майнерів) докладати зусиль шляхом вирішення складної математичної головоломки, щоб запобігти будь-якому обману системи.

Proof-of-Stake - (**PoS**) (від англ. **proof of stake**, умовно: «підтвердження долі») — це механізму консенсусу, який дозволяє власникам депозитити криптовалюти і створювати валідаційні ноди, що дає їм право перевіряти нові блоки транзакцій, додавати їх до блокчейну та отримувати за це винагороду.

Proof-of-Work та **Proof-of-Stake** це два основні консенсус механізми, які використовують криптовалюти для перевірки нових транзакцій, додавання їх до блокчейну та створення нових токенів. **Proof-of-Work**, розроблений для системи біткоїна, використовує майнінг для досягнення цих цілей. **Proof-of-Stake**, консенсус алгоритм **Cardano**, **Eth 2.0** та інших, використовує депозитування криптовалют для досягнення тих же цілей.

Механізм Proof-of-Work (PoW) вважається безпечним та ефективним алгоритмом досягнення консенсусу в мережі блокчейн. DDoS-атаки на блокчейн, що використовують цей алгоритм, неможливі з сучасними обчислювальними технологіями. Проте, висока вартість електроенергії, негативний вплив на навколишнє середовище і пов’язане з цим несприятливе висвітлення у ЗМІ, зростаюча централізація в майнінгу та низька пропускна спроможність транзакцій, ймовірно, зроблять його нежиттєздатним у довгостроковій перспективі.

Однак Proof-of-Stake (POS) також не є ідеальним. Наприклад, під час стейкінгу зловмисник може підтвердити хибні транзакції. Проект Ethereum в рамках запланованого переходу на PoS розробив протокол Casper. Casper карає шахраїв конфіскацією криптовалют і позбавленням їх можливості стейкати коли-небудь знову.

Якщо запланована реалізація PoS у такому відомому протоколі, як Ethereum, пройде добре, то крипто-спільнота, вірогідно, буде достатньо впевнена у здатності алгоритму PoS забезпечувати безпеку мережі. Це може схилити чашу терезів на користь PoS, але тільки час покаже, яким буде алгоритм консенсусу блокчейна в майбутньому.

Чому Proof-of-Stake краще, ніж Proof-of-Work?

Модель Proof-of-Stake краща, ніж Proof-of-Work, тому що вона вирішує багато проблем:

Централізація. Чотири **майнінг** пули контролюють понад **50%** загальної потужності **майнінгу біткоїну**. Це несправедлива система, оскільки вона означає, що звичайна людина майже не має шансів коли-небудь отримати нагороду за майнінг. У цьому відмінність **Proof-of-Stake**. Ця модель запобігає об’єднанню груп людей для домінування в мережі для отримання прибутку. Натомість ті, хто робить внесок у мережу, заморожуючи свої монети, отримують винагороду пропорційно до суми, яку вони вклали.

Майнінг - (англ. **mining** – “видобування корисних копалин”) – виробництво криптовалюти за рахунок потужностей комп’ютерного обладнання.

Споживання електроенергії. Деякі блокчейни **Proof-of-Work**, такі як **Біткоїн**, використовують велику кількість електроенергії. Нещодавнє дослідження показало, що загальна кількість електроенергії, необхідна для підтримки працездатності мережі Біткоїн, перевищує кількість, яку використовують більш ніж **159** окремих країн! З іншого боку, у **Proof-of-Stake** витрати на електроенергію для перевірки транзакцій значно нижчі.

Атака 51%. Відносно нещодавно відбувся приклад атаки 51% проти блокчейна Verge, що дозволило хакеру викрасти 35 мільйонів монет XVG. На момент атаки реальна вартість становила $1,75 мільйона доларів! При використанні механізму консенсусу Proof-of-Stake немає фінансового сенсу намагатись виконати атаку 51%. Для цього зловмисник має мати у своєму розпорядженні не менше 51% від загальної кількості криптовалюти в обігу. Єдиний спосіб зробити це – купити монети на відкритому ринку. Якби зловмисник вирішив купити таку значну суму, то реальна вартість монети по ходу збільшилася б. В результаті він витратить значно більше, ніж отримає від атаки.

Зараз деякі блокчейни застосовують обидві технології для формування нових блоків (наприклад, у криптовалютах PeerCoin і Reddcoin метод PoW використовується для початкового розподілу, а PoS — для підтвердження транзакцій). Це зв’язано з тим, що кількість монет кожної криптовалюти фіксована і рано чи пізно закінчиться. Тоді при розгадуванні блоку доведеться переходити на PoS технологію, за якої не відбувається введення нових монет в обіг.


GOOD LUCK!