NOSTR: Сигурност, анонимност и независимост в една нецензурируема мрежа. Бъдещето на децентрализираната комуникация.

NOSTR (Notes and Other Stuff Transmitted by Relays) е децентрализирана платформа за съобщения, която позволява на потребителите да споделят и обменят информация директно, без нужда от централизирани сървъри или социални мрежи.

Какво представлява NOSTR?

Най-просто казано, NOSTR е протокол за децентрализирана комуникация. За разлика от традиционните платформи като Facebook или X (Twitter), където съобщенията преминават през централизирани сървъри, NOSTR използва мрежа от независими сървъри (наричани релейни сървъри), които предават съобщенията между потребителите. Това означава, че няма единна точка на контрол или цензура, и потребителите могат да комуникират свободно и директно.

Как работи?

- **Ключове и криптиране:**
  Всеки потребител в NOSTR генерира два ключа – публичен и частен. Публичният ключ се използва за идентификация, докато частният ключ е за подписване на съобщенията. Това осигурява автентичност и сигурност, тъй като само притежателят на частния ключ може да подпише съобщение, което другите могат да проверят чрез публичния ключ.

- **Релейни сървъри:**
  Вместо да изпращате съобщенията си към централен сървър, NOSTR използва множество релейни сървъри. Потребителите избират кои сървъри да използват и могат да изпращат своите съобщения към всички тях. Това позволява гъвкавост – дори ако един релеен сървър спре да работи, съобщенията могат да преминават през други сървъри. Получателите използват публичния ключ, за да проверят автентичността на съобщенията.

Защо е важно?

- **Цензура:** Понеже няма централизиран сървър или организация, която да контролира комуникацията, е изключително трудно съобщенията да бъдат цензурирани или изтривани.
- **Сигурност:** Поради използването на криптография с публични и частни ключове, съобщенията са трудни за подправяне.
- **Простота:** Протоколът е сравнително прост за имплементиране, което означава, че всеки може да създаде клиент или релеен сървър.

Реклами и монетизация

Една от ключовите характеристики на NOSTR е липсата на реклами. За разлика от повечето традиционни социални мрежи, които генерират приходи чрез показване на реклами и следене на поведението на потребителите, NOSTR няма централизирана платформа, която да монетизира данните на потребителите. Това означава, че няма нужда от проследяване и персонализирани реклами.

- **Интегрирани плащания със сатошита:**
  За да се осигури устойчивост и подкрепа за създателите на съдържание, NOSTR позволява микроплащания със сатошита (най-малката единица на Биткойн). Потребителите могат директно да подкрепят авторите на съдържание или конкретни публикации, които харесват, като им изпращат сатошита. Тази система премахва нуждата от трети страни и посредници, които често начисляват високи такси или налагат ограничения.

Чрез тези плащания NOSTR предоставя на създателите на съдържание възможност за по-директна и честна монетизация, като същевременно потребителите остават свободни от рекламния натиск и масовото следене на данни.

Известни приложения (клиенти)

Едни от най-известните приложения са Primal, Amethyst, Damus, Snort и др.

Как работи на техническо ниво

NOSTR използва следните основни компоненти:

- **Клиенти (Clients):** Това са приложенията, с които потребителите взаимодействат, за да изпращат и получават съобщения. Всеки клиент подписва съобщенията с частния ключ на потребителя и ги изпраща към релейни сървъри.
- **Релейни сървъри (Relays):** Те не са задължително доверени страни. Работата им е просто да предават съобщенията, без да извършват сложни проверки. Релейните сървъри могат да решат дали да предават или съхраняват дадени съобщения, но потребителите могат да използват различни сървъри за пълна децентрализация.
- **Формат на съобщенията:**
  Всяко съобщение съдържа:
  - ➔ Публичен ключ на потребителя
  - ➔ Съдържанието на съобщението
  - ➔ Подпис, генериран с частния ключ
  - ➔ Време на изпращане
- **Подписване и проверка:**
  При изпращане на съобщение, клиентът(приложението) го подписва с частния ключ на потребителя. Получателите и релейните сървъри могат да използват публичния ключ, за да проверят дали подписът е валиден, като по този начин се осигурява, че съобщението идва от правилния източник.
- **Скалируемост и устойчивост:**
  Тъй като няма централен сървър, NOSTR е много устойчив на атаки. Дори при загуба на няколко релейни сървъра, съобщенията все още могат да преминават през мрежата.

Заключение

NOSTR е протокол, който има за цел да осигури децентрализирана, устойчива на цензура комуникация. Простотата му и използването на криптография с публични ключове го правят привлекателен избор за тези, които искат по-свободен и сигурен начин за обмен на информация и изразяване на мнение.