Proof of History (PoH): Digitální časové razítko

Proof of History je sekvenční hashovací funkce (VDF - Verifiable Delay Function), která slouží k vytvoření historického záznamu prokazujícího, že se událost stala v konkrétním čase a v určitém pořadí. PoH řeší jeden z největších problémů distribuovaných sítí – synchronizaci času bez centrální autority.

1. Problém času v blockchainu

V tradičních blockchainech (např. Bitcoin nebo Ethereum) se uzly musí neustále ptát jeden druhého: „V kolik hodin tato transakce proběhla?“ a „Která byla první?“.

- **Zpoždění:** Tato komunikace zabírá obrovské množství šířky pásma a času.
- **Sekvenční výroba:** Validátor nemůže začít pracovat na bloku, dokud se nedohodne s ostatními na čase toho předchozího.

—

2. Jak PoH funguje: Vodoznak času

Proof of History funguje jako kontinuální proces hašování (SHA-256), který běží stále dokola. Výstup jednoho hashe se stává vstupem pro hash následující.

- **Sekvence:** Každý výpočet v tomto řetězci vyžaduje určitý čas, který nelze přeskočit ani urychlit (ani paralelizací).
- **Data v řetězci:** Pokud se do tohoto procesu vloží data transakce, stanou se součástí řetězce. Výsledný hash prokazuje, že data byla vytvořena **před** tímto hashem, ale **po** hashi předchozím.

Představte si to jako **digitální přesýpací hodiny**. Každé zrnko písku má na sobě unikátní ID. Pokud do písku vložíte vzkaz, přesně víte, kolik zrnek propadlo před ním a kolik po něm.

—

3. Paralelní ověřování (The Efficiency Leap)

Zatímco **vytváření** PoH řetězce musí být sekvenční (jeden krok za druhým), jeho **ověřování** může probíhat paralelně.

- Validátor rozdělí přijatý řetězec na tisíce malých kousků.
- Každé jádro procesoru (GPU/CPU) ověří jednu část nezávisle na ostatních.
- To umožňuje síti Solana potvrdit tisíce transakcí během milisekund.

—

4. Přínosy pro síť

Výhoda	Popis
Extrémní propustnost	Síť nemusí čekat na potvrzení času a může zpracovávat transakce „v plném proudu“.
Nízká latence	Doba bloku klesá na hranici fyzických limitů hardwaru (cca 400 ms).
Předvídatelnost	Validátoři přesně vědí, kdy je řada na nich, aby navrhli další blok (Leader Schedule).

—

5. PoH vs. PoS: Časté nedorozumění

Je důležité si neuvědomit, že **PoH není náhradou za Proof of Stake**.

- **PoH** je nástroj pro organizaci času a pořadí (synchronizace).
- **Proof of Stake** (PoS) se v Solaně stále používá pro výběr validátorů a hlasování o platnosti bloků (bezpečnost).

Související články:

- Solana: Architektura postavená na PoH
- Základy kryptografie: Hashovací funkce
- Paralelní zpracování: Sealevel

Tagy: it solana cryptography proof-of-history consensus blockchain

From:
https://serviceit.cz/ - **IT ENCYKLOPEDIE**

Permanent link:
https://serviceit.cz/doku.php?id=poh

Last update: **2026/01/02 20:22**