Proof of History (PoH)

Proof of History (PoH), v překladu důkaz historie, je inovativní kryptografická technologie a výpočetní koncept navržený pro synchronizaci uzlů v blockchainových sítích. Tuto technologii vytvořil Anatoly Yakovenko a stala se základním stavebním kamenem a hlavním technologickým tahákem kryptoměny Solana.

Častým omylem je přesvědčení, že Proof of History je mechanismus konsensu (podobně jako Proof of Work u Bitcoinu nebo Proof of Stake u Etherea). Ve skutečnosti PoH není mechanismus pro dosahování shody sítě, ale funguje jako decentralizované a kryptograficky zabezpečené hodiny. Tyto hodiny pomáhají primárnímu mechanismu (v případě Solany upravenému Proof of Stake) fungovat s extrémní rychlostí a efektivitou.

Problém synchronizace času v blockchainu

V tradičních distribuovaných systémech (jako jsou Bitcoin nebo starší blockchainy) neexistují žádné centrální hodiny. Když uzel (těžař nebo validátor) vytvoří nový blok a zařadí do něj transakce, přidá k nim vlastní časové razítko (timestamp).

Problém nastává, když se síť musí shodnout na tom, v jakém přesném pořadí se transakce udály. Uzly si musí informace vzájemně přeposílat, ověřovat a čekat na sebe, aby se ujistily, že nedošlo k podvodu. Toto neustálé čekání na síťovou shodu a latence při komunikaci vytváří obrovské úzké hrdlo (bottleneck), které drasticky omezuje propustnost sítě (TPS - transakce za sekundu).

Proof of History tento problém řeší tím, že do sítě zavádí univerzální časovou osu, které mohou všechny uzly kryptograficky důvěřovat, aniž by spolu musely neustále komunikovat.

Jak Proof of History funguje (Technologický princip)

Jádrem Proof of History je matematická funkce zvaná Verifiable Delay Function (VDF). PoH konkrétně využívá vysokofrekvenční sekvenční hashovací funkci algoritmu SHA-256.

Sekvenční hashování: Systém neustále generuje hashe, přičemž výstup předchozího hashe je použit jako vstup pro hash následující. Tento proces tvoří nepřerušený řetězec operací.

Nemožnost paralelizace: Protože každý další krok vyžaduje výsledek toho předchozího, nelze tento výpočet urychlit rozdělením na více procesorových jader (nelze jej paralelizovat). Výpočet prostě vyžaduje určitý fyzický čas. Tím pádem délka vygenerovaného řetězce hashů matematicky dokazuje, že od bodu A do bodu B uplynul konkrétní a nezpochybnitelný úsek času.

Vkládání událostí: Pokud chce uživatel odeslat transakci, systém vloží data této transakce přímo do aktuálního stavu hashovacího řetězce. Výsledný hash pak slouží jako nezpochybnitelný důkaz, že transakce se stala přesně v tento moment – po předchozí události, ale před tou následující.

Okamžité ověření: Zatímco samotné generování hashovacího řetězce (tvorba času) je záměrně sekvenční a pomalé, samotné ověření tohoto řetězce ostatními uzly je naopak extrémně rychlé a lze jej plně paralelizovat na vícejádrových procesorech.

Vztah k Proof of Stake

Jak již bylo zmíněno, Proof of History nedokáže sám o sobě zabezpečit síť proti útokům. Proto vždy spolupracuje s mechanismem Proof of Stake (PoS).

V síti Solana funguje PoH jako časomíra pro protokol nazvaný Tower BFT (kastomizovaná verze byzantské tolerance chyb). Díky tomu, že všechny uzly v síti přesně znají kryptografický čas, vědí přesně, kdy jsou na řadě s tvorbou nového bloku. Nemusí na sebe čekat a mohou transakce chrlit neustále (tzv. streaming), což sráží dobu vytvoření bloku na neuvěřitelných 400 milisekund a teoretickou propustnost sítě až na 65 000 transakcí za vteřinu.

Výhody a nevýhody technologie

Výhody: Hlavní a absolutní výhodou je bezkonkurenční rychlost a propustnost. Technologie umožňuje smazat prodlevy vznikající při komunikaci uzlů. Transakce jsou potvrzovány téměř okamžitě, což činí sítě s PoH ideální pro decentralizované burzy (DEX) a aplikace vyžadující vysokofrekvenční obchodování. Díky obrovské kapacitě sítě jsou také transakční poplatky zcela minimální (zlomky haléřů).

Nevýhody a kritika: Hlavní nevýhodou jsou extrémní hardwarové požadavky. Generování i bleskové ověřování PoH vyžaduje od validátorů velmi drahé servery s výkonnými vícejádrovými procesory a obrovským množstvím RAM. Tento fakt vyvolává kritiku ohledně centralizace, protože provozovat uzel nemůže běžný uživatel doma na notebooku (jak je tomu často u Bitcoinu nebo Etherea). Rychlost a komplexnost PoH architektury také v minulosti vedla k několika softwarovým chybám, které způsobily dočasné výpadky celé sítě Solana.

Související pojmy: Solana, Blockchain, Proof of Stake (PoS), Proof of Work (PoW), SHA-256, Verifiable Delay Function (VDF), Konsensus algoritmus, TPS (Transactions Per Second).