Lightning Network

Motivace

Bitcoinový blockchain tvoří základ decentralizovaného finančního systému, který je nezávislý na centrálních institucích. Nicméně potvrzení transakcí na blockchainu trvá pro běžné používání neúnosnou dobu (blok je vytěžen zhruba každých 10 minut). To je pro běžné transakce, jako například nákup kávy, nepraktické. S řešením přichází **Lightning Network**, který umožňuje okamžité platby a zároveň podstatně zvyšuje objem bitcoinových plateb proveditelných za jednotku času.

Platební kanál

Platební kanál je základním stavebním prvkem sítě, technicky realizovaným jako **2-ze-2 multisig adresa**. K manipulaci s prostředky na této adrese je nezbytný digitální podpis obou stran. Kanál je iniciován **on-chain funding transakcí**, která uzamkne zdroje na adresu kanálu na blockchainu. Aby byla garantována bezpečnost prostředků i v případě nespolupráce protistrany, musí být ještě před zveřejněním funding transakce vytvořena a podepsána úvodní **commitment transakce**, která umožňuje zdroje kdykoliv jednostranně vybrat.

Commitment transakce reprezentují aktuální stav zůstatků v kanálu a standardně se nepouštějí do sítě (**off-chain**), čímž se šetří kapacita blockchainu. Tyto transakce využívají systém asymetrie a **revokačních klíčů** k zamezení podvodům (publikování starého stavu). Pokud strana A publikuje transakci jednostranně, okamžitě vyplatí stranu B, ale své vlastní prostředky má uzamčeny **časovým zámkem**. Pokusí-li se A publikovat neplatný starý stav, strana B může využít revokační klíč (který získala při přechodu na nový stav) a v rámci časového zámku zkonfiskovat veškeré prostředky kanálu. V případě vzájemné dohody (**kooperativní uzavření**) vzniká finální transakce bez časových zámků.

HTLC

Lightning Network je propojená síť platebních kanálů. Umožňuje směrovat platby přes více uzlů bez nutnosti mít přímý kanál mezi odesílatelem a příjemcem. Směrování je realizováno pomocí mechanismu **HTLC (Hashed Time-Locked Contracts)**, který zajistí, že všechny mezikroky proběhnou **atomicky**: buď zaplatí každý účastník v řetězci, nebo nikdo. Tím vzniká možnost okamžitých, levných a škálovatelných transakcí, aniž by byla obětována bezpečnost základní vrstvy.

HTLC jsou kontrakty kombinující **hash-lock** a **time-lock**. Hash-lock vyžaduje znalost určitého **preimage** (náhodně vygenerované číslo) k odemčení prostředků uzamčených v transakci, zatímco time-lock určuje časový limit pro vyplacení. Platba přes více uzlů probíhá tak, že příjemce vygeneruje tajný řetězec (preimage) a sdílí jen jeho hash. Každý mezilehlý uzel zablokuje prostředky s podmínkou, že budou uvolněny pouze při odhalení správného preimage. Pokud k odhalení nedojde včas, kontrakt se automaticky vrátí předchozí straně. Tím je zajištěno **atomické vypořádání** celé platby.