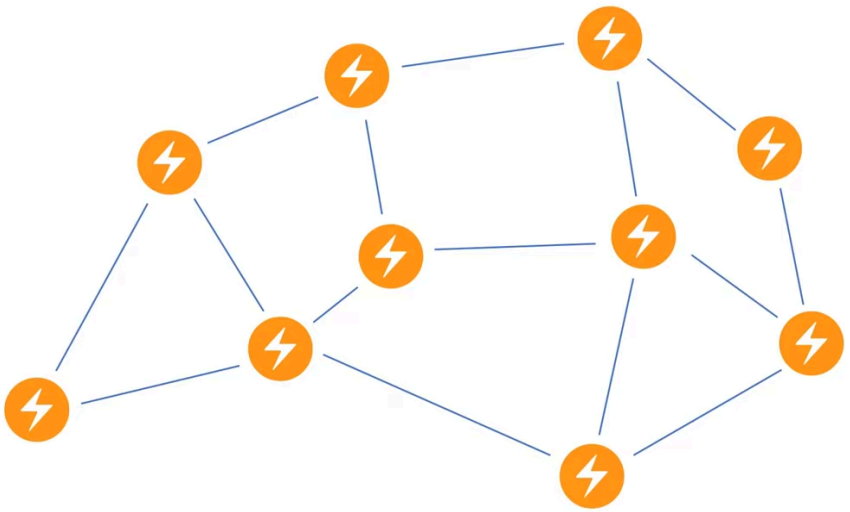
Разкриване на силата на Lightning Network - най-големият layer 2 в Bitcoin - Част 1

Нека създадем нашите участници в тази публикация – Алис и Боб, които са в бар. Алис иска да купи бира от Боб, като плати с Биткойн. За да направи това, Алис трябва да изпрати сумата на адреса на Боб, но транзакцията в блокчейна отнема поне 10 минути, така че Боб трябва да изчака, за да получи парите, а Алис трябва да плати такса за транзакцията. И ако Алис реши да изпие втора бира, ще трябва да повторят процеса. Това не е много ефективно за тях, а също така не е добра идея да се натоварва блокчейнът с толкова малки покупки. Затова те могат да използват силата на Lightning Network.

Какво е Lightning Network?

Lightning Network е втори слой за плащания, който работи върху Биткойн блокчейна. Създаден е, за да позволи по-бързи, по-евтини и мащабируеми транзакции извън веригата между участниците. Това е система от директна връзка (peer-to-peer) за извършване на плащания с Биткойн чрез мрежа от двупосочни платежни канали, без прехвърляне на контрола върху средствата в трета страна.



Как работи?

Платежни канали - отваряне и затваряне

Lightning Network работи чрез платежни канали, създадени между две страни. Каналите са по същество мултиподписни портфейли, създадени в Биткойн

блокчейна. За мултиподписните адреси се използват P2WSH адреси. Създаването им заключва средства и от двете страни в мултиподписен адрес, като са необходими подписи от двете страни, за да бъдат похарчени средствата върху блокчейна. За да се създаде платежен канал, и двамата участници заключват определено количество биткойн в мултиподписен портфейл чрез транзакция в блокчейна. Важно е и двете страни да заключат средства, защото каналът се нуждае от ликвидност и в двете посоки.

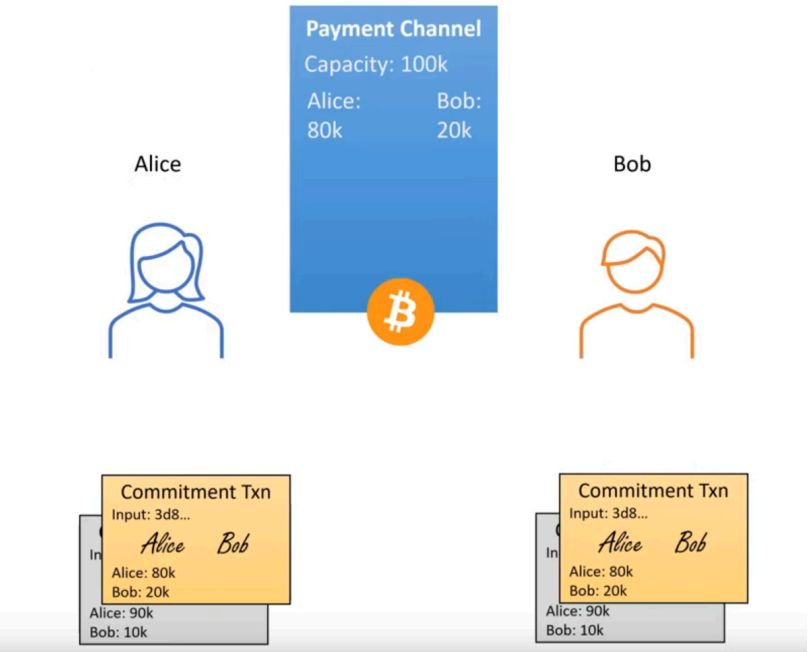
Тези средства са заключени в блокчейна и не се използват за всяка отделна транзакция. Представянето им се създава в Lightning Network (layer 2). Веднъж след като платежният канал е създаден, страните могат да извършват транзакции извън блокчейна, като актуализират баланса на канала. Те създават и обменят транзакции, които преразпределят средствата в канала, без всяка транзакция да бъде публикувана в блокчейна.

Каналите позволяват двупосочни транзакции, което дава възможност и на двете страни да извършват транзакции и в двете посоки, без всяка транзакция да бъде записвана в Биткойн блокчейна. Транзакциите в платежния канал са подписани от двете страни и могат да бъдат изпълнени мигновено.

Ликвидността на канала зависи от заключеното количество Биткойн.

Нека се върнем към Боб и Алис, които биха искали да използват Lightning Network. Те решават да отворят платежен канал помежду си, за да улеснят бъдещи транзакции, без да разчитат на Биткойн блокчейна за всяка покупка на бира. Те се съгласяват да финансират платежния канал с капацитет от 100 000 сатошита, създавайки мултиподписен портфейл, където и двете страни държат ключовете. След като е създаден каналът, Алис може да поръча бира от Боб, без да е необходимо всяка транзакция да бъде записана в Биткойн блокчейна. Алис изпраща транзакция за плащане на Боб за стойността на бирата, да кажем 10 000 сатошита. Алис създава плащане, подписва го и го хешира, за да генерира предварителен образ (preimage). Алис намира маршрут и предава предварителния образ на Боб през мрежата. Боб проверява предварителния образ, и след като получи плащането, средствата в платежния канал се актуализират, за да отразят плащането на Алис. Ако тя реши да купи втора бира, може отново да му изпрати сумата. За да подпише втората транзакция, Алис използва предварителния образ от предишната транзакция като хеш. Това позволява на Боб да провери валидността на втората транзакция и гарантира, че средствата се прехвърлят правилно.

Използват се Schnorr подписи и SHA256 хеш функция.



И Алис, и Боб съхраняват актуализираната транзакция, но без да е необходимо тя да бъде предадена на блокчейна. Те ще го направят, когато решат да затворят канала. Теоретично каналът може да остане отворен и да се използва, докато имат нужда от него, като съхраняват копия на транзакциите. По този начин, с Lightning Network, те могат да извършват безкрайно много транзакции, но само две ще бъдат записани в блокчейна – тази, която отваря канала, и тази, която го затваря.

Когато страните пожелаят да затворят канала, те предават най-новата транзакция на Биткойн блокчейна, за да уредят крайните баланси. Тази финална транзакция затваря канала, и двете страни получават съответните си дялове от средствата в техните лични адреси.

Има два варианта за затваряне на канала. Първият вариант е кооперативно затваряне, при което и двете страни се съгласяват да затворят канала и са онлайн. В този сценарий една от страните инициира заявка за затваряне на канала, а другата страна подпомага, като подписва транзакцията. По време на този процес се използват хеширащи алгоритми, за да се гарантира валидността и правилността на транзакцията. След това и двете страни получават своите средства на блокчейн адрес, спрямо крайното състояние на канала.

Вторият вариант е принудително затваряне, което се случва, когато един от възлите иска да затвори канала, но другият възел е или офлайн, или не желае да сътрудничи. При принудително затваряне не е необходимо съгласието на втората страна. Вместо това мрежата проверява средствата, налични в балансите на двете страни, използвайки алгоритми, и след това затваря канала. Въпреки това, този процес отнема повече време (около 2 седмици) в сравнение с кооперативното затваряне, за да има техническо време втората страна да провери за дали първата не се опитва да измами. Принудителните затваряния са по-рядко срещани и обикновено се използват като крайна мярка.

И в двата случая страните получават своите средства и актуализация, отразяваща крайното състояние на канала, което гарантира, че и двете страни имат запис на подробностите по транзакцията.

Onion Routing и отмяна, и заключване във времето

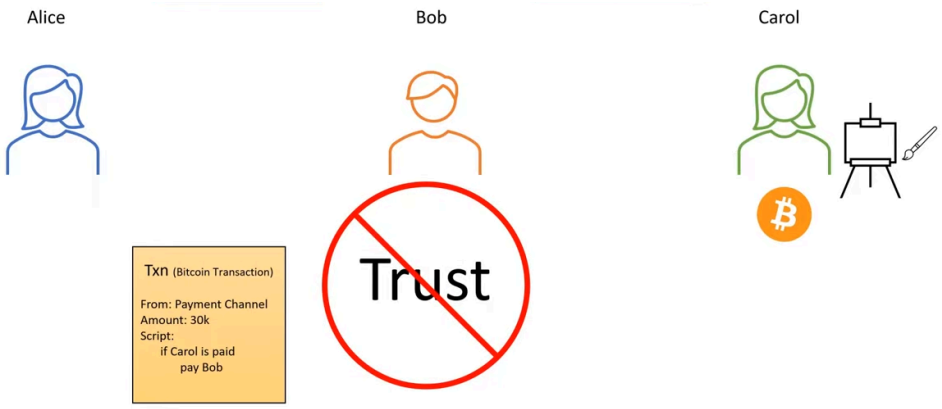
За да изпращат плащания към страни, с които нямат директен канал, Lightning Network използва механизъм за маршрутизация. Плащанията се маршрутизират през междинни възли, използвайки onion routing, при което всеки възел в пътя знае само самоличността(като адресен получател, а не физическа самоличност на човек) на предишния и следващия възел, което гарантира поверителността и сигурността на мрежата и нейните участници.

Нека разгледаме сценарий, в който Боб има канал с Карол, а Алис иска да изпрати биткойн на Карол, без да има директен канал с нея, използвайки връзката на Боб като посредник. Боб може да начисли такса за използването на своите връзки, но също така може и да не го направи.

Алис може да бъде сигурна, че нейните биткойни ще бъдат изпратени на Карол и че Боб не може да ги открадне. Lightning Network осигурява сигурност чрез използването на договори за възстановими последователности на падеж (RSMC) и транзакции със заключване във времето. Всяка страна държи копие на най-новата транзакция, и в случай на измама или опит за предаване на остаряла транзакция, контрагентът може да използва RSMC, за да изиска целия баланс на канала.

Ако Боб се опита да задържи средствата и да не ги предаде на Карол, Алис може да изчака предварително зададен период за изчакване (определен по време на процеса на плащане). Ако Боб не предаде плащането в рамките на този период, Алис може да изиска обратно средствата си, използвайки специална възстановителна транзакция. Това гарантира, че средствата на Алис са защитени, дори ако Боб действа нечестно.

Затова в света на LN доверието не е необходимо. И тук важи добре познатата от Биткойн максима - Не се доверявай, проверявай!



Приложения на Lightning Network

- **Микротранзакции**: Lightning Network улеснява микротранзакциите, което го прави подходящ за сценарии като монетизация на съдържание, плащане на гледане (pay-per-view) или дори покупки в приложения.
- **Търговски транзакции**: С мигновени и евтини транзакции, Lightning Network може да революционизира търговския сектор, предоставяйки безпроблемно и ефективно решение за плащания.
- **Микроплащания в IoT**: Мрежата може да се приложи в екосистемата на Интернет на нещата (IoT), като позволява на устройствата да извършват микро суми в реално време за услуги или данни.
- **Гейминг индустрия**: Lightning Network може да се интегрира в онлайн гейминг платформи, позволявайки покупки в игри, обмен на дигитални активи и други.
- **Децентрализирани финанси (DeFi)**: Lightning Network може да се разшири и в сферата на DeFi, като улеснява по-бързи и по-евтини транзакции за различни финансови услуги.

Заключение

Lightning Network предоставя ниво на анонимност, сравнимо с кеш транзакции, като същевременно предлага скоростта и ефективността на дигиталните плащания. То позволява на потребителите да извършват транзакции, без да оставят следи от лична идентификационна информация, което го прави жизнеспособна опция за хора, загрижени за своята поверителност.

Lightning Network е хвалена за "потенциала си да трансформира света на плащанията, правейки Биткойн по-достъпен, по-бърз и по-евтин за употреба" и е мащабируемото решение, което може да направи Биткойн още по-достъпен за обикновения човек.

Lightning Network е обещаваща технология, която има потенциала да революционизира плащанията с Биткойн. Тя предлага няколко предимства пред транзакциите в блокчейн, включително скорост, цена и мащабируемост. С развитието си, Lightning Network вероятно ще бъде приета от по-широк кръг бизнеси и потребители.