Electronic Ledger o Llibre de Comptes Digital

Un *electronic ledger*, o llibre comptable electrònic, és un registre digital que emmagatzema i manté un historial de transaccions o esdeveniments. També es coneix com a llibre major electrònic o llibre comptable digital.

En lloc d'utilitzar un llibre físic o registres en paper, un *electronic ledger* utilitza tecnologia informàtica i bases de dades per a mantindre un seguiment de les transaccions de manera segura i transparent. Aquestes transaccions poden incloure transferències d'actius financers, registres de propietat, intercanvis comercials, registres d'esdeveniments i més.

Un exemple popular de *electronic ledger* és la tecnologia *blockchain*, que s'utilitza en criptomonedes com Bitcoin. En la *blockchain*, les transaccions es registren en blocs enllaçats mitjançant criptografia, creant una cadena immutable de transaccions. Això proporciona seguretat i transparència, ja que cada participant en la xarxa té una còpia del llibre major i pot verificar les transaccions.

Blockchain, Cadena de Blocs

Una blockchain és una tecnologia de registre distribuït que s'utilitza per a emmagatzemar i verificar de manera segura transaccions o registres d'esdeveniments. La blockchain és la base de funcionament de moltes criptomonedes, sent Bitcoin una de les més conegudes.

En el cas de Bitcoin, la blockchain és una cadena de blocs enllaçats, on cada bloc conté un conjunt de transaccions. Cada transacció representa l'intercanvi de Bitcoins entre participants de la xarxa.

Una característica fonamental de la blockchain de Bitcoin és el mecanisme de consens anomenat "*Proof of Work*" (Prova de Treball). Aquest mecanisme garanteix la seguretat i confiabilitat de la xarxa.

El *Proof of Work* implica que els participants, anomenats miners, han de fer un esforç computacional per a validar i agregar nous blocs a la cadena. Per a fer-ho, els miners han de resoldre un problema matemàtic complex, conegut com "hash puzle". Aquest problema requereix una gran quantitat de poder computacional i es basa en algorismes criptogràfics.

El primer miner a resoldre el hash puzle rep una recompensa en forma de Bitcoins acabats de crear, i el bloc validat s'agrega a la blockchain. Això es coneix com a "mineria" i és una manera de crear nous Bitcoins i assegurar la integritat de la xarxa.

Una vegada que un bloc s'agrega a la blockchain, és extremadament difícil modificar-lo a causa de l'estructura criptogràfica de la cadena. Cada bloc conté una referència al bloc anterior, creant un enllaç que s'estén fins al bloc inicial, conegut com a "bloc gènesi". Qualsevol modificació en un bloc requeriria canviar tots els blocs posteriors, la qual cosa seria computacionalment inviable i requeriria un consens de la majoria dels participants de la xarxa.

Aquesta estructura descentralitzada i resistent a modificacions fa que la blockchain de Bitcoin siga segura i de confiança, ja que els registres són transparents i poden ser verificats per qualsevol participant de la xarxa. A més, en utilitzar el Proof of Work, es dificulta l'atac maliciós a la xarxa, ja que un atacant necessitaria controlar la majoria del poder computacional de la xarxa per a alterar els registres.

Algorismes de consens

Consens *Proof of Work* (PoW): L'algorisme de consens *Proof of Work* (Prova de Treball) s'utilitza en moltes blockchains, incloent Bitcoin. En PoW, els participants, anomenats miners, han de fer un esforç computacional significatiu per a validar i agregar nous blocs a la cadena. Resolen problemes matemàtics complexos (hash puzles) per a demostrar que han fet el treball necessari. El primer miner a resoldre el puzle guanya el dret d'agregar el bloc i és recompensat. PoW és conegut per ser segur i resistent a atacs, però requereix un alt consum energètic a causa de la competència per resoldre els puzles.

Consens *Proof of Stake* (Post): L'algorisme de consens Proof of Stake (Prova de Participació) assigna el dret a crear i validar blocs basat en la participació o "stake" que un participant té en la xarxa. En lloc de resoldre problemes computacionals, els participants bloquegen una quantitat de criptomonedes en una cartera digital com a garantia. La probabilitat de ser triat per a validar un bloc es basa en la quantitat de criptomonedes que han bloquejat. Post és més eficient energèticament que PoW, ja que no requereix un alt poder computacional, però alguns argumenten que pot portar a una major centralització, ja que els participants amb més criptomonedas tenen més possibilitats de ser triats.

Consens *Proof of Authority* (*PoA): L'algorisme de consens *Proof of Authority* (Prova d'Autoritat) es basa en la confiança en un grup d'autoritats o nodes de confiança que són seleccionats per a validar transaccions i crear blocs. Aquestes autoritats són identitats conegudes i de confiança en la xarxa. A diferència de PoW i PoS, PoA no requereix un gran consum energètic i s'utilitza en blockchains d'ús empresarial o consorcis on la identitat i confiança són fonamentals.

Altres algorismes de consens: A més de PoW, PoS i PoA, existeixen altres algorismes de consens utilitzats en diferents blockchains. Alguns exemples inclouen:

1. Delegated *Proof of Stake* (DPoS): És una variant de Post on els participants trien a representants o delegats per a validar els blocs en el seu nom. Aquests delegats s'encarreguen de validar les transaccions i agregar blocs a la cadena. DPoS s'utilitza en blockchains com EOS i Tron.
2. Practical Byzantine Fault Tolerance (PBFT): És un algorisme de consens dissenyat per a sistemes distribuïts en els quals els participants han d'aconseguir un acord fins i tot si alguns d'ells són maliciosos o fallen. PBFT se centra en la tolerància a fallades i s'utilitza en blockchains com Hyperledger Fabric.

Cal destacar que cada algorisme de consens té els seus avantatges i desavantatges, i la seua elecció depén de les necessitats i objectius específics de la blockchain en qüestió.

Llavors i claus

Una llavor aleatòria, en el context de la criptografia i les criptomonedas, és una seqüència de bits generada de manera completament aleatòria. Aquesta llavor s'utilitza com a base per a derivar claus privades i públiques en un procés conegut com a generació determinista de claus.

Un estàndard àmpliament utilitzat per a generar llavors aleatòries i derivar claus és el BIP39 (Bitcoin Improvement Proposal 39). BIP39 defineix un mètode estàndard per a crear una llavor aleatòria de 12, 18 o 24 paraules mnemotècniques (conegudes com a "frase de recuperació" o "*seed phrase*" en anglés). Aquestes paraules són seleccionades d'una llista predefinida de paraules en el BIP39 *Wordlist*, que consta de 2048 paraules en total.

El procés de generació de claus privades i públiques a partir de la llavor aleatòria BIP39 es realitza en diversos passos:

1. Generació de la llavor: Es tria una quantitat de paraules mnemotècniques segons la longitud desitjada (per exemple, 12 paraules). Aquestes paraules es converteixen en una seqüència binària de 128 bits, coneguda com a llavor.
2. Càlcul de la llavor mestra: La llavor es passa a través d'una funció de derivació determinista coneguda com a funció hash (com HMAC-SHA512) per a generar una "llavor mestra". Aquesta llavor mestra té una longitud de 512 bits.
3. Derivació de claus: A partir de la llavor mestra, es poden derivar múltiples claus privades i públiques. Això es realitza mitjançant una funció de derivació jeràrquica (HD) com s'especifica en l'estàndard BIP32.
4. Derivació de la clau privada: La llavor mestra s'utilitza per a generar una clau privada arrel. A partir d'aquesta clau privada arrel, es poden derivar claus privades addicionals utilitzant rutes i números d'índex específics.
5. Derivació de la clau pública: A partir de cada clau privada, es pot generar una clau pública corresponent utilitzant algorismes de criptografia asimètrica, com l'algorisme de corba el·líptica (per exemple, l'algorisme secp256k1 utilitzat en Bitcoin). La clau pública es pot compartir àmpliament i s'utilitza per a rebre fons en una direcció de criptomoneda.

És important destacar que la llavor aleatòria i la frase de recuperació són crítiques per a accedir i restaurar les claus privades en un moneder o cartera de criptomonedes. Per tant, és fonamental mantindre-les segures i realitzar còpies de seguretat adequades. A més, l'ús de BIP39 i l'estàndard HD permet la generació determinista de claus, la qual cosa facilita la recuperació i la creació de múltiples claus a partir d'una sola llavor aleatòria.

Transaccions bàsiques en Bitcoin i Ethereum

El procés de realitzar transaccions en les blockchains de Bitcoin i Ethereum involucra diverses etapes, des de la iniciació de la transacció en un moneder (*wallet) fins que es confirma en un bloc. Ací està el procés general pas a pas:

1. Creació d'una cartera (wallet): L'usuari crea una cartera digital en la blockchain respectiva (Bitcoin o Ethereum). La cartera genera un parell de claus criptogràfiques: una clau privada i una clau pública.
2. Generació d'una transacció: L'usuari inicia una transacció en la seua cartera. La transacció inclou detalls com l'adreça del destinatari, la quantitat de criptomoneda a enviar i, opcionalment, una tarifa de transacció.

3. Signatura de la transacció: La cartera utilitza la clau privada del remitent per a signar digitalment la transacció. Això proporciona la prova criptogràfica que el remitent és el propietari legítim dels fons i permet que la transacció siga verificada pels nodes de la xarxa.
4. Difusió de la transacció: La cartera difon la transacció signada a la xarxa blockchain. La transacció es propaga a través dels nodes de la xarxa, que la transmeten a altres nodes, creant així una xarxa de difusió.
5. Validació i propagació de la transacció: Els nodes de la xarxa verifiquen la validesa de la transacció. Això inclou verificar la signatura digital i comprovar si el remitent té suficients fons per a completar la transacció. Una vegada validada, la transacció es propaga a altres nodes de la xarxa.
6. Inclusió en un bloc: Els miners (en el cas de *Bitcoin) o validadores (en el cas de Ethereum) recopilen diverses transaccions i les agrupen en un bloc. Aquests miners o validadores competeixen per a resoldre un problema criptogràfic (proof-of-work en Bitcoin, proof-of-stake en Ethereum) que els permet agregar el bloc a la cadena.
7. Confirmació de la transacció: Una vegada que el bloc és minat o validat, el bloc s'agrega a la cadena de blocs. La transacció ara es considera confirmada i permanent en la blockchain. En general, es recomana esperar múltiples confirmacions (és a dir, blocs addicionals agregats després del bloc inicial) per a major seguretat, ja que cada confirmació redueix la possibilitat d'una reversió de la transacció.

Cal esmentar que el temps que porta confirmar una transacció pot variar segons la congestió de la xarxa i les tarifes de transacció pagades. En períodes d'alta demanda, pot portar més temps perquè les transaccions siguen incloses en blocs i confirmades.

Smart contracts, contractes intel·ligents

Ethereum i Bitcoin són dos blockchains amb diferents enfocaments i característiques. Una de les principals diferències que permet que Ethereum permeta l'execució de codi en contractes intel·ligents, a diferència de Bitcoin, es deu a la diferència en el seu disseny i funcionalitat:

1. Llenguatge de programació Turing complet: Ethereum utilitza un llenguatge de programació *Turing complet,que s'executa en una màquina virtual anomenada EVM (*Ethereum Virtual Machine*), i pot programar-se en llenguatges d'alt nivell com l'anomenat Solidity amb una sintaxi basada en Java/C++ o Vyper, amb sintaxi basada en Python. Permet la creació de contractes intel·ligents amb lògica i funcionalitats més complexes. En contrast, Bitcoin té un llenguatge de scripting més simple i limitat, que està dissenyat principalment per a realitzar operacions bàsiques de transaccions.
2. Màquina virtual Ethereum (EVM): Ethereum compta amb una màquina virtual anomenada *Ethereum Virtual Machine* (*EVM). La EVM és una plataforma d'execució de contractes intel·ligents que permet la interpretació i execució de codi en la blockchain de Ethereum. Els contractes intel·ligents escrits en Solidity o Vyper es compilen en bytecode de la EVM, que pot ser interpretat i executat pels nodes de la xarxa Ethereum.
3. Flexibilitat i personalització: Ethereum es va dissenyar per a ser una plataforma de computació descentralitzada i programable. Permet als desenvolupadors crear aplicacions descentralitzades (DApps) i contractes intel·ligents personalitzats que poden realitzar una àmplia gamma de funcions, des de transaccions financeres fins a votacions, jocs i més. Bitcoin, d'altra banda, se centra principalment a ser una moneda digital i una reserva de valor, amb un enfocament més limitat en l'execució de codi.
4. Gas i tarifes de transacció: Ethereum utilitza un sistema de tarifes de transacció anomenat "gas". Cada operació en la xarxa Ethereum, inclosa l'execució de contractes intel·ligents, requereix un consum de gas que ha de ser pagat en Ether (la criptomoneda nadiua de Ethereum). Aquestes tarifes de gas cobreixen els recursos computacionals utilitzats i eviten l'abús de la xarxa. Bitcoin no té un sistema similar de tarifes de gas, i les tarifes de transacció es basen en la competència d'oferta i demanda en la xarxa.

Aquestes particularitats en el disseny de Ethereum, com el seu llenguatge de programació Turing complet, la EVM i l'enfocament en l'execució de contractes intel·ligents, han permés que Ethereum es convertisca en una plataforma líder per al desenvolupament d'aplicacions descentralitzades i contractes intel·ligents més complexos en comparació amb Bitcoin, que se centra principalment a ser una forma de diners digitals.