Blockchain

Transakzioen biltegiratze banatu, fidagarri eta manipulaezina

Blockchain edo bloke-kateen teknologia bitcoinarekin batera egin zen ezagun, kriptotxanpon entzutetsuak erabiltzen zuen transakzioen biltegiratze-sistema baita. Entitate ziurtatzaile zentralik gabeko sistema banatu hau segurua eta manipulaezina denez, beste arlo ugaritan aplikatzen hasi da. Iraultza berria omen da hurrengo urteetan noranahi hedatuko den bloke-kateen teknologia hau.

Bitcoin kriptotxanponaren sortzaileak berak asmatu du *Blockchain* edo bloke-kateen teknologia ere, Satoshi Nakamoto pertsona edo talde ezezagunak. Bitcoinaren kontzeptua deskribatu zuen artikulu berean deskribatu zuen bloke-kateen teknologia ere, 2008an; eta, 2009an, bitcoinarekin batera jarri zen martxan lehen inplementazioa. Izan ere, teknologia hori da txanponaren transakzioak biltegiratu eta ziurtatzeko erabiltzen den sistema.

Txanpon digital horren sorreraren oinarrian premisa bat zegoen: bere kasa funtzionatzea teknologia hutsez, inongo erakunderen parte-hartzerik edo gainbegiratzerik gabe. Eta, jakina, sistemak fidagarria eta iruzurren kontra babestua behar zuen izan. Hori guztia bermatzen du bloke-kateen diseinuak, eta agerian geratu da hori martxan izan den zortzi urteetan.

Bloke-kateen ezaugarriak

Edozer gauzaren erregistroa digitalki gorde behar denean, norbaiten kontrolpeko datu-base zentralizatuak izaten dira ohikoenak. Bloke-kateen teknologia, ordea, sistema banatua eta deszentralizatua da. Sare baten bidez konektatutako hainbat nodok osatzen dute sistema, eta nodo horietako bakoi-

Igor Leturia Azkarate
Informatikaria eta ikertzailea

tzean biltegiratzeko erabiltzen den bloke-katearen eta *Blockchain* softwarearen kopia bana dago. Horrek eragiten du sistema fidagarri izatea: izan ere, nodo bati zerbait gertatuz gero, beste asko daude sistemari martxan eusteko.

Sistema banatua izateak manipulaezintasuna ere bermatzen du. Izan ere, datu-base batean iruzurra egiteko, datu-base horretarako sarbidea besterik ez da behar. Erasotzaileek sarbide hori lortzea posible izateaz gainera, barruko hainbat pertsonak ere izan ohi dute sarbidea; beraz, sistema nahiko ahula da. Baina bloke-kateen sistema banatu batean, nodo guztien kontrola lortu beharko litzateke (edo gutxienez erdia baino gehiagorena), eta aldaketa bloke-kate guztietan egin. Askoz ere zailagoa da hori.

Are gehiago, bloke-kateen funtzionamenduak berak ere egiten du ia-ia ezinezkoa izatea iruzur egitea. Norbaitek bloke-kateetan transakzio bat erregistratu nahi duenean, nodo guztiek ziurtatzen dute transakzioa zilegia dela. Zehazki, bitcoinaren kasuan, diru-zorro batean kopuru bat sartu behar bada, ziurtatzen dute kopuru hori bera kenduko dela beste diru-zorro batetik edo diru-zorro horren jabeak meatzaritza bidez eskuratu duela diru hori (ordenagailuen bidez problema kriptografiko konplexuak ebaztea izan ohi da meatzaritza egitea txanpon digitaletan).

Baina, horrez gain, transakzioak bloketan antolatzen dira: blokearen edukiaren araberakoa den eta kalkulatzeko dezenteko kostu konputazionala duen

ARG.: WhiteMocca/Shutterstock.com

> *"Bloke-kateen funtzionamenduak ia ezinezko egiten du iruzurra"*

sinadura digital edo hash bat esleitzen zaio bloke horietako bakoitzari, eta bloke bakoitzak aurreko blokearen sinadura ere gordetzen du (horregatik bloke-katea, bloke bakoitzak aurrekoarekiko lotura gordetzen duelako). Hala, ahalmen konputazional handi samarra duen norbaitek akaso aldatu ahal izango luke azken edo azken-aurreko blokeko transakzio bat hurrengo blokea etorri aurretik (nahiz eta horretarako nodo guztien kontrola ere izan beharko lukeen); baina bloke-katean nahiko sakon dagoen bloke bateko transakzio bat ezingo litzateke aldatu munduko ordenagailu guztien ahalmena izanik ere.

Aplikazio ugari

Aipatutako ezaugarri horiengatik guztiengatik, bloke-kateen teknologia oso interesgarria da beste aplikazio askotarako. Izan ere, beste gauza askotan hasi dira erabiltzen, eta askoz gauza gehiagotan erabiliko omen da etorkizunean.

Kriptotxanponen sareak publikoak eta irekiak diren arren, bloke-kateekin sare pribatuak ere egin daitezke. Adibidez, enpresa-talde bateko enpresen arteko eragiketen erregistroa bloke-kate batean gorde daiteke, bakoitzak nodo bat izanik eta sarbidea berek bakarrik izanik. Edo enpresa bakarrak ere sor dezake bloke-kate bat, hainbat nodo jarrita. Gero eta gehiago ari dira erabiltzen finantzen munduan edota logistikan; lehenengoan, garrantzitsua delako iruzur egiteko aukerarik ez izatea, eta, bigarrenean, janarien, sendagaien eta halako beste produktu batzuen trazabilitatea bermatzen duelako.

Bestalde, herritarren informazioaren erregistroak gordetzeko ere erabil daiteke: erregistro medikoak; jaiotza, ezkontza eta heriotzenak... Edo notaritza-sistema gisa: lur eta etxeen salmenten erregistroak, kontratuak... Edota hauteskundeetako botoak gorde eta kontatzeko. Adibidez, Kataluniako urriaren 1eko erreferendumean erabili izan balute, behin bozka bat emanda, ezingo zatekeen bozka hori inola indargabetu, espainiar poliziak gero hautetsontziak lapurtzean ez bezala. Jakina, konfidentzialtasuna bermatu behar da kasu horietan, baina horretarako mekanismoak inplementa daitezke bloke-kateen teknologian.

Aipatu dugu dagoeneko transakzio bat onartzeko nodo guztiek transakzioaren zilegitasuna bermatu behar dutela lehenengo. Jakina, zilegitasuna erabakitzen duen algoritmoa egokitu egin behar zaio aplikazio-kasu bakoitzari. Adibidez, kriptotxanponen kasuan, esan dugu meatzaritza egin den edo kopurua beste zorro batetik kendu den begiratzen dela. Baina jaiotza-, heriotza- eta ezkontza-erregistroak gordetzeko erabili nahi bada, adibidez, ziurtatuko da horretarako baimena duen funtzionario batek eman duela agindua. Edo bozketa-sistema batean, sistemak ziurtatuko du bozkatzailea erroldan dagoela eta jada ez duela bozkatu.

Bloke-kateen teknologia erabiltzen duen aplikazio bat muntatu nahi izanez gero, hainbat sistema komertzial zein libre daude aukeran: Hyperledger, Openchain, IBM Blockchain... Itxura guztien arabera, etorkizun paregabea izango du bloke-kateen teknologiak. ●