Ana Zelaia Jauregi
UPV-EHUko Donostiako Informatika Fakultateko irakasle eta ikertzailea

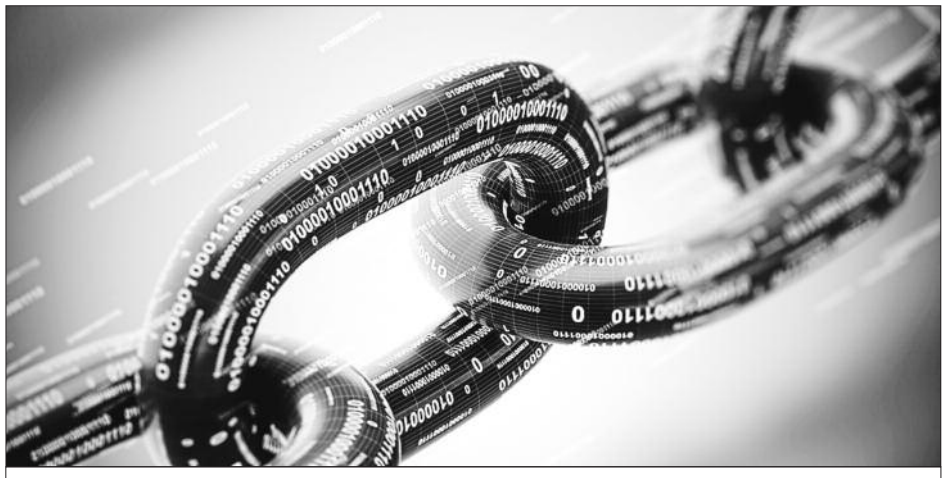
«Blockchain»: Interneten hurrengo belaunaldia ekar dezakeen teknologia

Internet sarearen sorrerak informazioa eskura jarri zigun. Haren protokoloei esker, mezuak, fitxategiak edo irudiak bidaltzea oso erraza bihurtu zen. Hala ere, badira oraindik bitartekari bidez egiten ditugun transakzioak. Dirua bidaltzea edo jabetzak erostea benetakotasuna egiaztatzea eskatzen duten ekintzak dira. Konfiantzaz jardun ahal izateko, transakzioan parte hartzen dutenen identitatea egiaztatu eta jabetzaren erregistroa fidagarria dela bermatzen duen entitate zentral baten beharra dugu: bankua, notarioa, etab. Bitartekari horrek datuak gordetzen ditu, eta datuak dituenak boterea du gaur egun.

Blockchain edo bloke-kateen teknologiak informazioaren benetakotasuna egiaztatzeko eta transakzioak modu seguruan eta bitartekaririk gabe egiteko aukera ematen du. P2P (*peer-to-peer*) motako konputagailu-sareen bidez kudeatzen da, hau da, deszentralizatutako sarea da; sareko nodoen artean ez dago hierarkiarik. Bloke-kate bakoitzean egin daitezkeen transakzioak kontratu adimendun (*smart contract*) batean definitzen dira. Kontratu hori sareko nodo guztiek onartu behar dute.

Blockchain teknologia 2009an eman zen ezagutzera, Bitcoin kriptomonetaren sorrerarekin batera. Ideia nagusiak hauek dira:

• **Bloke bat osatu:** Transakzioak digitalki sinatzen dira, egilearen benetakotasuna bermatzeko, eta blokeetan biltzen dira. Blokea bete denean, haren identifikatzailea izango den *hash* bat kalkulatzen da. *Hash* hori blokeko edukian oinarrituz kalkulatzen da *hash* funtzio bat aplikatuz. *Hash*-a blokearen laburpen moduko bat da, luzera finkoa duen eta bakarra den karaktere-kate bat. Ondoren, blokea sarean zabaltzen da.



Bloke-kateen teknologiaren ahalmena erreala da. Baina oztopo ugari ditu oraindik. GAUR8

• **Blokea kateatu:** Transakzioak kontratu adimendunari jarraituz egin daitezkeela egiaztatu ondoren, blokea balioztatu behar dute sarea osatzen duten nodoek. Blokeak kateatzeko estrategiaren arabera, nodo bat izango da blokea balioztatuko duen lehena. Lortzen duenean, gainerako nodoei jakinaraziko die, guztiek blokea katean lotu (aurreko blokearen *hash*-a gorde) eta luzatuz doan katearen kopia gorde dezaten.

• **Katea puskatu:** Kateko blokeren batean edukia aldatzean blokearen *hash*-a aldatuko denez, kateko lotura puskatuko da. Horrela lortzen da bloke-kateko transakzioen informazioa aldaezina izatea.

Teknologia honetan ez dago informazioaren monopolioa duen bitartekaririk eta iruzurrak antzeman egiten dira, bloke-katea puskatzen delako.

Hori guztia kudeatzeko, aplikazio deszentralizatuak garatu behar dira. Adibide ezagunena kriptomonetak dira (Bitcoin, Ether). Diru bidalketetarako aplikazio moduan, Jordaniako kanpamendu batean martxan dena aipa daiteke. Hango errefuxiatu siriarrek dendan erositakoa ordaintzeko, begietako irisa identifikatuz laguntza humanitarioa kudeatzen duen bloke-katea erabiltzen dute. Horrela, kudeaketa-gastuak nabarmen murrizten dira eta laguntza onuradunari iritsi zaiola bermatzen da. Gainera, errefuxiatuek identitate digital legala izatea lortzen dute. Izan ere, teknologia honekin identitate digitalaren burujabetza lor daiteke.

Bestelako aplikazioak asko dira: automobilgintzan edo elikagaien industrian produktuen trazabilitatea bermatzeko, titulu akademikoak balioztatzeko, energiaren gobernantza kooperatiboan laguntzeko, Gauzen Interneta kudeatzeko, Industria 4.0 garatzen laguntzeko...

Bloke-kateen teknologiaren ahalmena erreala da, baina oztopoak asko dira oraindik. Kriptografiak babesten duen arren, %100 segurua den teknologiarik ez da existitzen. Gainera, legegintza aldetik aldaketak behar dira teknologia onartua izateko. Oztopoak gainditzen badira eta bloke-kateen erabilera zabaltzen bada, Internet sarearen hurrengo belaunaldia izango dugu. Ematen diogun erabileraren arabera ikusiko da gizartearen ongizatean hobekuntza lortzeko balioko duen. •