BLOCKCHAIN: KRIPTOTXANPONEZ HARATAGO, TEKNOLOGIA EZAGUTU ETA TREBATZEKO TAILERRA

1. Deskribapena.

Hurrengo dokumentuan Blockchain teknologia zer den azaltzen da, bere historia, oinarri teknologiko eta egun ezagutzen diren inplementazioetako batzuk aipatuz. Ondoren, Ethereumekin aplikazio deszentralizatu bat garatzen jarraitu beharreko pausoak jasotzen dira, horretarako egun existitzen diren tresna ezberdinak azalduz.

2. Edukia.

2.1. ZER DA BLOCKCHAIN?

Blockchain teknologia 2008tik ezagutzen dugu, Satoshi Nakamotok “Bitcoin”en [1] paperra argitara eman zuenetik. Bitcoin, Blockchain teknologiaren gainean inplementatutako kriptotxanpon bat da. Blockchain teknologia algoritmo eta arkitektura multzo bat da, teknika kriptografiko eta deszentralizazioan sostengatzen dena.

Bitcoin, Blockchain teknologia erabiliz eraikitako lehen kriptotxanpona bada ere, asko izan dira Nakamotorenaren atzetik garatu eta argitara eman diren bestelako kriptotxanponak. Horrek izan zezakeen eraginaren jakitun, banketxeak ere laster sartu ziren teknologia honen ikerketan. Kriptotxanponen eta banketxeen ondotik, Blockchain teknologiari bestelako erabilerak ematen hasi zitzaizkion.

Hasierako aplikazio eta inplementazio horiek ordea, kriptoaktibo konkretu bat sortu eta beronen hartu emanera mugatzen ziren. Hori dela eta, Blockchain teknologiaren bestelako inplementazioak garatzen hasi ziren. Horien artean, hurrengo ataletan azaltzen diren Ethereum [2] eta Hyperledger Fabric [3] aipatuko genituzke. Hauek, kriptoaktiboak sortu eta hauen hartu emana ahalbidetzeaz gain, bestelako logikak garatzeko aukera ematen digute, horretarako Smart Contractak [4] (kontratu adimenduak) erabiltzen dituztelarik.

Gaur egun askok Blockchain teknologiaren eragina gutxiesten badute ere, sektore ezberdinetako erakunde ugari ari dira berau ikertzen. Gainera, era isolatu batean lan egin beharrean, enpresa hauek partzuergo edo aliantza ezberdinak sortu dituzte. Horien artean, batzuk aipatzeagatik, hurrengoak nabarmenduko genituzke: Ethereum Aliance, Hyperledger Foundation, R3, B3i eta Enerchain.

2.2. OINARRI TEKNOLOGIKOAK.

Blockchain teknologiak informazioa deszentralizatu eta sare banatuak sortzeko aukera ematen digu. Blockchainen erregistratzen den informazioa aldaezina izateaz gain, sareko nodo guztietan eguneratuta mantentzen da. Horretarako, ezinbestekoa da P2P (Peer to peer) sare bat izatea, baita parte-hartzaile guztien arteko kontsentsua, guztiek informazio berbera izan dezaten. Blockchain, teknologia berri bat baino, teknologia ezberdinen arteko mix batetik sortutako mekanismo bat dela esan dezakegu. Ondoren, berau eraikitzeko erabiltzen diren teknologiak azaltzen dira.

2.2.1. Kriptografia

Hurrengo atal honetan Blockchainen erabiltzen diren teknika kriptografiko esanguratsuenak deskribatzen dira, era labur eta sinple baten.

2.2.1.1 Hash algoritmoak

Arrasto bakarra sortzeko asmoz garatutako algoritmoa. Eduki konkretu bati Hash algoritmo bat aplikatuz gero, emaitza beti izango da arrasto berbera. Arrasto hauek luzera berdina dute guztiek. Arrasto eskuartean izanik, hasierako edukia lortzea ezinezkoa da. Algoritmo hauek bi abantaila nagusi ematen dizkigute:

- Alde batetik, informazioaren integritatea bermatzen digute. Edukian aldaketa minimo bat egiten badugu eta berriz algoritmo berbera aplikatu, emaitza guztiz ezberdina izango da.
- Bestetik, edukiak konprimatzeko balio digu.

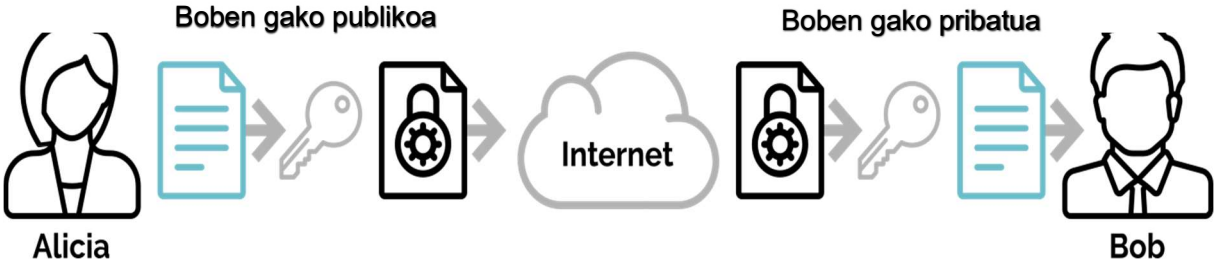
2.2.1.2 Kriptografia simetrikoa

Informazioa zifratzeko eta deszifratzeko gako berdina erabiltzen da. Blockchainen bezero mailan erabiltzen da kriptografia simetrikoa, norbere informazioa era seguruan zifratzeko. Azken finean, teknika honen oinarria gakoen segurtasunean datza. Hori dela eta, lokalean soilik erabiltzen da,d gakoa ez baita saretik bidali behar.

2.2.1.3 Kriptografia asimetrikoa

Informazioa asimetrikoak gako ezberdinak erabiltzen dira zifratu eta deszifratzeko, gako pribatua eta gako publikoa. Gako publikoa, gako pribatutik sortzen da. Gako publikoa, bere izenak dioen bezala, publikoki banatzen da, gako pribatua ordea, norbera gordetzen du. Kriptografia asimetrikoak, ondorengo erabilerak ditu:

- Batetik, mezuak zifratzeko erabiltzen da. Horretarako, mezuaren hartzailearen gako publikoa erabiltzen da. Mezu hau zifratzeko erabili den gako publikoarekin lotutako gako pribatuarekin soilik deszifratu daiteke. Kasu honetna, mezuaren hartzaileak soililik deszifratu dezake.

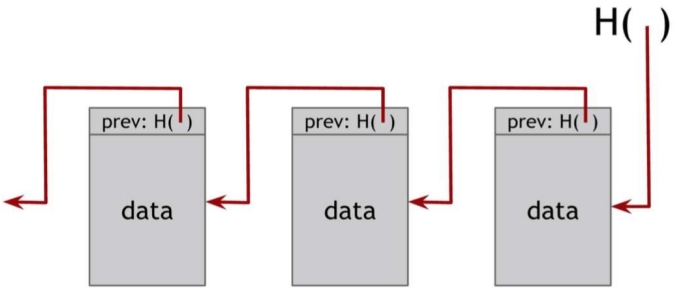


1. irudia: gako publiko eta pribatuaren erabileraren adibidea mezuak zifratzean

- Bestalde, mezuak sinatzeko erabiltzen da, mezuaren igorlea ezagutzeko. Igorleak bere gako pribatuarekin sinatzen du mezua. Mezuaren sinatzailea balioztatzeko, sinatzeko erabili den gako pribatuarekin lotutako gako publikoa erabili beharko da.

2.2.2. Blokeen katea

Blokeen kate (Blockchain) bat, datuak era banatu batean gordetzeko mekanismo bat da. Datuak blokeka biltzen ditu, bloke bakoitza aurrekoarekin matematikoki lotuz. Era honetan, informazioa berreskuratu eta datuen integritatea bermatzen laguntzen du. Horretarako, bloke bakoitzak biltzen duen eduki guztia hartu eta Hash algoritmo bat aplikatzen dio, bloke horren identifikatzailea sortuz.



2. irudia: blokeen katea

Bloke berri bat sortzen denean, honen, beharrezkoa den datu eta erregistro guztiak jasotzeaz gain, aurreko blokearen identifikatzailea ere biltegiratzen du. Era honetan, bloke bakoitza aurrekoari lotuta geratzen da, eduki guztia oinarritzat hartuz sortutako hashak aurreko blokearen identifikatzailearekiko dependentzia baitu. Era honetara, katearen apurtu ezin bat sortzen da, bloke batean egiten den edozein aldaketak katea apurtuko bailuke. Bloke berri bar sortzen den bakoitzeko, berau sareko kide guztiei banatzen zaie.

2.2.3. Kontsentsua

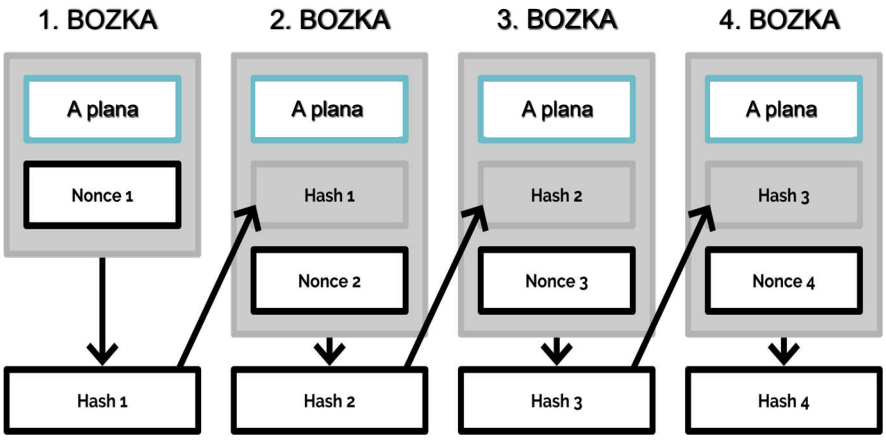
Blockchain teknologiak kontsentsuaren arazoarentzako irtenbide bat planteatzen du sistema banatuetan. Blockchainek erabiltzen duen kontsentsu mekanismoa azaltzeko, sistema banatuetan erabiltzen den arazo bat hartuko dugu oinarritzat: “jeneral bizantinoen arazoa”. Arazo horren ezaugarri nagusiak ondorengoak dira:

- Inperio zahar horretako jeneral multzo bat daukagu sakabanaturik, 4 ditugula suposatuko dugu.
- Haien artean komunikatzeko aukera dute, baina ez dago komunikazioak koordinatzen dituen entitate zentralik. Hala era, guztiek duten besteekin era zuzenean komunikatzeko aukera.
- Komunikazioen helburua, adostasun bat bilatzea da: erasoaldiaren ordua adostu behar dute jeneralek, edo ea erretiratuko diren. Jeneral guztiek berdin jokatzen badute, gerra irabaziko dute.
- Dena den, komunikazio horietan arazoak izan ditzakete, edo jeneral birek plan ezberdinak proposatu. Gainera, bidaltzen ari diren mezuak harrapatu eta aldatu ditzakete.
- Jeneral bakoitzak ordenagailu bat dauka, mezuak bidali eta jasotzeko aukera ematen diona, hashak kalkulatzeko gaitasuna izateaz gain. Haien helburua ados jartzea da, bakoitzak proposatu dezakeen planaren gainetik.

Bitcoin protokoloa ezagutzera eman zenera arte ez zen arazo hau konpontzen zuen irtenbide praktikorik ezagutzen. Horretarako, Blockchain erabiltzen da, edo kasu honetan “lan frogen kate” bezala era ezagutu daitekeena. Jeneralek haien bozkak bidaliko dituzte proposatutako planen gainean. Horrela, plan bat baino gehiago jasoz gero, horietako bakarrari emango liokete bozka.

Jeneral bakoitzak bozka bat bidali ahal izango du bere ordenagailuak hash konkretu bat kalkulatzen duenean. Hash hori sortuko den bloke berriaren identifikatzailea izango da. Hash hori kalkulatzeko, aurreko blokearen hasha (identifikatzailea), bozkatzen ari den plana eta zenbaki aleatorio bat erabiliko ditu (nonce-a). Helburua, kalkulatzen duen hasharen balioa aurretik definitu duten zailtasun maila bat baino txikiago izatea izango da. Horrela, jeneralak zenbaki aleatorioa aldatu eta hasha kalkulatzen jarraitu beharko du baldintza hau bete arte.

Zailtasun maila bat definitzeak, bozka bakoitza bidaltzeko behar den denbora mugatzea du helburu. Horretarako, 4 jeneralek dituzten ordenagailuen konputazio gaitasuna hartu da kontuan. Hori horrela izanik, zehaztu den zailtasun mailari esker bloke berri bakoitza 10 minutuan behin sortuko dela aurreikusten da.



3. irudia: kontsentsuaren metodologia

Jeneral batek bere plan proposamena bidaltzea lortzen duenean, lehendabiziko balizko bozka izango da. Beste jeneralek lehen bozka jasotzen dutenean, hori oinarritzat hartu jarraituko dute haien bozkak kalkulatzen. Azken finean, helburua bakoitzak bere iritzia ematea baino, adostasun batetara heltzea da. Horrela, bozken katea sortzen joango gara.

Jeneral batek bloke berri bat jasotzen duen bakoitzean, hurrengo balidazioak egingo ditu:

1. Bloke berriaren identifikatzailea (hash), zehaztutako zailtasun maila baina txikiagoa da?
2. Hash hori, blokearen edukia hartuz sortzen ahal da (nonce-a, bozka eta aurreko blokearen identifikatzailea edo hasha)?
3. Plan hau, aurreko planaren berdina ahal da?

Aurrerako ere aipatu dugu ordea, jeneral bakoitzak bozka edo bloke bi jaso ditzakela. Kasu horietan, kate baten gainean hasiko litzateke lanean. Beranduago, beste katean bozka edo bloke gehiago izango balitu, katez aldatuko luke. Azken finean, eta lehenago adierazi bezala, helburua adostasun batera heltzea bada.

Aurreko lerroetan, Bitcoinek erabiltzen duen kontsentsu algoritmoa azaldu da, Proof of Work (PoW) deiturikoa. Gaur egun ordea, algoritmo ezberdinak daude. Horietan artean, Ethereumek erabiltzen duen Proof of Stake (PoS) edo Hyperledger Fabricen inplementatuko den Practical Byzantine Fault Tolerance (PBFT) aipatuko genituzke.

2.2.4. Smart Contractak

Smart Contractak aipatutako Blockchainen oinarrietako azkena da. Smart Contract edo kontratu adimenduak Blockchainean exekutatuko den logika jasotzen duten programak dira. Hauek, Blockchain sareko nodo guztietan integratzen dira. Horrela, ekintza bakoitzaren emaitzak ez du exekutatzen den lekuarekiko menpekotasunik, hau da, emaitza beti izango da berdina.

Horri esker, exekutatutako ekintza guztiak balioztatzeko aukera dute sareko nodo guztiek. Horrela, okerreko datu edo kalkulurik egiten ez dela balioztatzen da. Kontratu adimendu hauek, gure logika propioa garatu eta Blockchainean integratzeko aukera ematen digute.

2.3. BLOCKCHAIN MOTAK eta INPLEMENTAZIOAK

Hurrengo atal honetan Blockchainen inplementazio ezberdinak sailkatzeko erabiltzen den katalogazio sistema tipikoa azaltzen da. Sistema bera azaldu baino, sailkapen horretan banatzen diren mota ezberdinen ezaugarri nagusiak deskribatzen dira: alde batetik Blockchain publikoak ditugu, bestetik, pribatuak. Horrez gain, gaur egun autorearen ustez esanguratsuenak diren inplementazioak deskribatzen dira: Hyperledger Fabric eta Ethereum.

2.3.1. Blockchain publikoak

Blockchain publikoak Bitcoinen esentzia jarraituz garatu diren inplementazio guztiak dira. Blockchain mota hauen ezaugarri nagusiak ondorengoak dira:

- Parte-hartze askea: ez dago sare hauetan parte-hartzea kontrolatzen duen inor. Blockchain hauetara edonor batu daiteke.
- Informazio publikoa: Blockchain hauetan informazioa mundu guztiaren eskura dago.
- Anonimotasuna: era honetako sareetara gehitzeko ez da beharrezkoa identifikatzerik

2.3.2. Blockchain pribatuak

Era honetako Blockchainak aurrekoan kontrako ezaugarriak dizute. Dena den, egun badaude bakoitzeko ezaugarri batzuk hartu eta erdi-bidean kokatzen diren inplementazioak ere. Horiek Blockchain hibrido bezala ezagutzen dira. Pribatuen ezaugarriak hurrengoak lirateke:

- Parte-hartze mugatua: entitate bat edo entitate multzo baten baimena behar da era honetako Blockchainekin bat egiteko. Gainera, askotan bakoitzaren aktibitatearen berri jakiten da.
- Informazioaren pribatutasuna: sare hauetan partekatzen den informazioa berau osatzen duten kideen artean soilik elkartrukatzen da.

2.3.3. Inplementazioak

2.3.3.1. Hyperledger Fabric

Hyperledger Fabric, Hyperledger Fundazioaren barruan garatutako proiektu bat da. Proiektu honek merkatuen Blockchaina izatea du helburu. Horretarako, parte-hartzaileen kontrola eta kudeaketa ahalbidetzen du. Dena den, entitate ezberdinak Blockchain berdinean parte-hartuta ere, informazioa era konfidentzial batean partekatzeko mekanismoak eskaintzen ditu.

2.3.3.2. Ethereum

Ethereum aldiz, Blockchain publiko bat da. Zure nodo propioak martxan jarri eta zure Blockchain pribatua sortzeko aukera ematen badu ere, gaur egun sare publiko ugari ditu. Ethereumek bere burua plataforma deszentralizatu bezala definitzen du. Gaur egun, Blockchainekin garatutako proiektu publiko gehienak inplementazio hau erabiliz egin dira.

2.5. APLIKAZIO DESZENTRALIZATU BATEN GARAPENA ETA INPLEMENTAZIOA ETHEREUMEN

Hurrengo atal honetan Ethereumen aplikazio deszentralizatu bat (DAPP) garatzeko jarraitu beharreko pausoak aipatzen dira. Bestalde, egun Ethereumekin lan egiteko dauden tresna nagusiak ere zerrendatzen dira.

2.5.1. Tresnak

2.5.1.1. Solidity

Ethereumeko Smart Contractak garatzeko erabiltzen den programazio lengoaia dugu.

2.5.1.2. Remix

Ethereumerako garapen ingurune bat da, tresna ezberdinak barnebiltzen dituena. Remixen gure Smart Contractak garatu, konpilatu eta hedatu ditzakegu. Baita probak egin ere.

2.5.1.3. Metamask

Ethereumeko sareetara konektatzea ahalbidetzen digun tresna.

2.5.1.4. Truffle & Ganache

Truffle Ethereum garapenerako ingurune bat da, Framework bat. Smart Contractak konpilatu eta hedatzeko aukera ematen digu. Truffleren tresnen artean Ganache dugu, gure makina lokalean probak egiteko baliogarria den Ethereumeko Blockchain bat martxan jartzen duen tresna, bere esploratzaile eta guzti.

2.5.1.5. Web3

Web3 liburutegi bat da. Programazio lengoaia ezberdinetan garatuta dago eta hauei esker, Ethereumeko Blockchainera konektatzen diren aplikazioak era erraz batean garatu ditzakegu.

2.5.2. Garapen manuala

Ondoren, era labur batean DAPP baten garapenerako jarraitu beharreko pausoak zerrendatzen dira:

- Smart Contractaren garapena: norberaren aplikazioaren logika jasotzen duen kontratu adimendua garatu beharko litzateke lehendabizi. Solidity programazio lengoaia erabiliz egin beharko litzateke. Ondoren, Remix eta Ganache erabili daitezke probatzeko.
- Aplikazioaren garapena: gure Smart Contractaren logika eta metodoen arabera funtzionatuko duen aplikazio bat beharko genuke. Aplikazio hau nahi dugun programazio lengoaian egin dezakegu. Gero ordean, Ethereumeko Blockchainarekin komunikatzeko Web3 liburutegia integratu beharko genuke.
- Smart Contractaren hedatzea: dagokion Ethereumeko sarea aukeratu eta Smart Contracta

Blockchain: kriptotxanponez haratago, teknologia ezagutu eta trebatzeko tailerra bertan zabaldu beharko litzateke. Ondoren, gure Smart Contractaren helbidea hartu eta aplikazioan sartu beharko genuke.

3. Bibliografia.

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system

[2] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151, 1-32.

[3] Cachin, C. (2016, July). Architecture of the hyperledger blockchain fabric. In Workshop on Distributed Cryptocurrencies and Consensus Ledgers (Vol. 310).

[4] Szabo, N. (1997). The idea of smart contracts. Nick Szabo's Papers and Concise Tutorials, 6.

4. Kredituak eta baimenak.

Egilea: Urko Larrañaga Piedra

Data: 2018eko uztailaren 4a.