Lohkoketjut tietokantoina

Aki Ylinen

Lohkoketjut tietokantoina

Aki Ylinen

0. Johdanto

Tervetuloa oppaaseen "Lohkoketjut tietokantoina"!

Tämä opas on tarkoitettu kaikille, jotka haluavat ymmärtää lohkoketjuteknologiaa ja sen sovellusmahdollisuuksia. Lohkoketjut ovat viime vuosina nousseet merkittäväksi innovaatioksi, joka on muuttanut tapaa, jolla tietoa tallennetaan, käsitellään ja jaetaan verkossa. Lohkoketjut tarjoavat hajautetun, läpinäkyvän ja turvallisen tavan tallentaa tietoja ja siirtää arvoa ilman välikäsiä.

Tämä opas käsittelee lohkoketjuteknologian perusteita, sen käyttötapoja ja sovelluksia eri aloilla, sekä lohkoketjujen käyttöön liittyviä riskejä ja haasteita. Opas on suunniteltu niin, että se sopii aloittelijoille, mutta myös niille, jotka haluavat syventää tietämystään lohkoketjuista.

Opas koostuu neljästä osasta. Ensimmäinen osa käsittelee lohkoketjuteknologian perusteita, kuten lohkoketjun rakennetta, tietoturvaa ja konsensusmekanismeja. Toinen osa käsittelee lohkoketjuteknologian käyttötapoja eri aloilla, kuten rahoitus-, terveydenhuolto- ja logistiikka-alalla. Kolmas osa käsittelee lohkoketjujen käyttöön liittyviä riskejä ja haasteita, kuten tietoturva- ja yksityisyysriskejä. Neljäs osa sisältää lisäresursseja ja opiskelumateriaalia, jotka auttavat syventämään tietämystä lohkoketjuista.

Toivomme, että tämä opas auttaa sinua ymmärtämään lohkoketjuteknologiaa ja sen sovellusmahdollisuuksia

paremmin. Jos sinulla on kysyttävää tai haluat antaa palautetta oppaasta, ole hyvä ja ota yhteyttä kirjoittajiin.

1. Johdanto lohkoketjuteknologiaan

Lohkoketjuteknologia on mullistanut tapamme ajatella tietokannoista ja digitaalisesta omaisuudesta. Se on luonut uusia mahdollisuuksia hajautetulle ja turvalliselle tiedon tallentamiselle sekä uusien, innovatiivisten sovellusten kehittämiselle. Lohkoketjuteknologia on noussut suuren yleisön tietoisuuteen kryptovaluuttojen kautta, mutta sen potentiaali ulottuu paljon laajemmalle. Tämä kirja käsittelee lohkoketjuteknologiaa yksityiskohtaisesti ja tarjoaa kattavan oppaan sen käyttöön ja hyödyntämiseen.

Kirjan ensimmäisessä osassa esitellään lohkoketjuteknologian perusteet, kuten lohkoketjun toimintaperiaatteet ja sen eri osat. Toisessa osassa käsitellään lohkoketjuteknologian sovelluksia eri aloilla, kuten rahoituksessa, logistiikassa ja terveydenhuollossa. Kolmannessa osassa perehdytään lohkoketjuteknologian käyttöön ja sen hyötyihin liiketoiminnalle. Lisäksi käsitellään lohkoketjujen käyttöön liittyviä riskejä ja parhaita käytäntöjä.

Tämä kirja on tarkoitettu kaikille, jotka haluavat ymmärtää lohkoketjuteknologiaa syvällisesti ja oppia sen käytöstä käytännön sovelluksissa. Kirjan avulla lukija pääsee alkuun lohkoketjuteknologian maailmassa ja oppii hyödyntämään sen tarjoamia mahdollisuuksia.

1.1. Peruskäsitteet

Lohkoketjuteknologia on innovatiivinen tapa tallentaa tietoa hajautetusti verkossa. Se mahdollistaa digitaalisen varallisuuden omistamisen ja siirron ilman keskitettyä viranomaista tai välikäsiä. Lohkoketjut ovat yleensä julkisia ja avoimia, mikä tarkoittaa, että kaikki verkon käyttäjät voivat tarkastella tallennettuja tietoja.

Lohkoketjut koostuvat useista lohkoista, jotka sisältävät transaktioita ja muita tietoja. Jokainen lohko on liitetty toisiin lohkoihin edellisen lohkon tiivisteen perusteella, mikä takaa sen, että lohkoketju on muuttumaton ja lähes mahdoton manipuloida.

Lohkoketjuja käytetään nykyään laajasti kryptovaluuttojen, kuten Bitcoinin, Ethereumin ja monien muiden, taustalla olevana teknologiana. Ne mahdollistavat myös monia muita sovelluksia, kuten hajautetun tietokannan, älysopimukset ja hajautetun tiedon tallennuksen. Lohkoketjuteknologia onkin tullut tunnetuksi hajautetun talouden ja hajautetun yhteiskunnan perustana.

1.1.1. Lohkoketjut ja niiden toiminta

Lohkoketju on hajautettu tietokanta, joka koostuu useista tietokantablokeista tai lohkoista. Jokainen lohko sisältää tietoa ja viittauksen edelliseen lohkoon, jolloin ne muodostavat lohkoketjun. Tämä tarkoittaa, että jokainen lohko on sidoksissa aikaisempiin lohkoihin ja että ketjun jokainen lohko on järjestetty tiettyyn järjestykseen.

Lohkoketjujen tärkeimmät ominaisuudet ovat hajautettu ja

läpinäkyvä tietokanta, jota ei hallinnoi keskitetty organisaatio. Sen sijaan lohkoketjun tietokanta on hajautettu ympäri maailmaa oleville tietokoneille, jotka kaikki pitävät kirjaa tietokannasta. Tämä tekee lohkoketjusta läpinäkyvän, koska jokainen käyttäjä voi tarkistaa kaikki lohkot, jotka ovat tallennettu ketjuun.

Lohkoketjut ovat myös turvallisia ja luotettavia tietokantoja, koska lohkoketjuja ei voi muuttaa yksipuolisesti. Jokainen lohko on linkitetty edelliseen lohkoon ja seuraavaan lohkoon, mikä tarkoittaa, että jokaisen lohkon sisältö ja tarkistussumma riippuu edellisestä lohkosta. Tämä estää tietojen manipuloinnin ja mahdollistaa sen, että lohkoketjuja voidaan käyttää monenlaisten tärkeiden tietojen tallentamiseen, kuten taloudellisiin tietoihin, äänestykseen ja terveysrekistereihin.

Lohkoketjut toimivat siten, että kun uusi lohko lisätään ketjuun, se tarkistetaan ja validoidaan kaikissa tietokoneissa, joissa lohkoketju on tallennettu. Kun lohko on hyväksytty, se lisätään ketjuun ja sen sisältö tulee kaikkien käyttäjien saataville. Tämä tarkoittaa myös sitä, että lohkoketjut ovat nopeasti kasvava tietokanta, joka sisältää kaiken aiemmin tallennetun tiedon.

1.1.2. Lohkoketjujen käyttökohteet

Lohkoketjuteknologialla on monia käyttökohteita eri aloilla, joista joitain esimerkkejä käydään läpi tässä osiossa.

1. Rahansiirrot: Lohkoketjujen tunnetuin käyttökohteita on kryptovaluuttojen rahansiirrot. Lohkoketjut mahdollistavat nopean ja turvallisen rahansiirron ilman

välikäsiä, mikä tekee niistä erittäin suosittuja esimerkiksi Bitcoinin ja Ethereumin tapauksessa.

2. Älysopimukset: Älysopimukset ovat lohkoketjujen toimintoja, jotka mahdollistavat sopimusten automaattisen toteuttamisen lohkoketjujen kautta. Tämä tekee sopimusten tekemisestä turvallisempaa, nopeampaa ja helpompaa. Älysopimukset ovat käyttökelpoisia esimerkiksi finanssialalla, kiinteistökaupoissa ja julkishallinnon sopimuksissa.
3. Reaaliaikainen seuranta: Lohkoketjut mahdollistavat reaaliaikaisen seurannan monilla eri aloilla. Esimerkiksi toimitusketjujen seuranta voidaan toteuttaa lohkoketjujen avulla, mikä lisää läpinäkyvyyttä ja turvallisuutta.
4. Identiteetinhallinta: Lohkoketjut voivat auttaa yksilöitä hallinnoimaan omaa identiteettiään ja antamaan luvan tietojensa käyttöön. Tämä tekee identiteetinhallinnasta turvallisempaa ja käyttäjäystävällisempää.
5. Energianhallinta: Lohkoketjut voivat auttaa seuraamaan ja hallinnoimaan energiankulutusta ja tuotantoa. Tämä voi auttaa teollisuutta vähentämään energiankulutusta ja tuomaan säästöjä.
6. Pelialat: Lohkoketjut ovat alkaneet tulla suosituksi käyttökohteeksi myös pelialalla. Lohkoketjuteknologian avulla voidaan rakentaa turvallisia ja läpinäkyviä pelijärjestelmiä, joissa pelaajien turvallisuus ja oikeudenmukaisuus on varmistettu.

Nämä ovat vain muutamia esimerkkejä lohkoketjujen käyttökohteista, ja niiden määrä kasvaa jatkuvasti teknologian

kehittyessä. Lohkoketjuteknologia tarjoaa mahdollisuuksia monille eri aloille, ja sen merkitys digitaalisessa maailmassa vain kasvaa.

1.2. Lohkoketjun historia ja kehitys

Lohkoketjun historia juontaa juurensa digitaalisen käteisen kehittämisestä, joka sai alkunsa 1980-luvulla. Vuonna 2008 julkaistun Bitcoinin myötä lohkoketjuteknologia tuli tunnetuksi laajemmin. Bitcoinin kehittäjä, nimimerkillä Satoshi Nakamoto tunnettu henkilö, esitteli lohkoketjun käytön hajautettuna järjestelmänä, joka mahdollistaisi bitcoinien siirtämisen ilman välikäsiä ja keskusviranomaisia.

Bitcoinin julkaisun jälkeen lohkoketjuteknologiaa on sovellettu moniin eri käyttötapauksiin, ja kehitys on ollut nopeaa. Ethereum, joka julkaistiin vuonna 2015, toi mukanaan älysopimukset ja mahdollisti lohkoketjujen käytön monimutkaisempien sovellusten ja palveluiden toteuttamiseen. Myös muiden kryptovaluuttojen, kuten Litecoinin ja Ripplen, taustalla on lohkoketjuteknologia.

Lisäksi perinteiset yritykset ja julkishallinto ovat osoittaneet kasvavaa kiinnostusta lohkoketjuteknologiaa kohtaan. Esimerkiksi pankkisektorilla lohkoketjuteknologiaa on käytetty maksujen siirtämiseen ja tietojen tallentamiseen. Muita esimerkkejä lohkoketjuteknologian soveltamisesta ovat muun muassa lääkealan, energiateollisuuden ja kiinteistöjen hallinnan sovellukset.

Lohkoketjun kehitys jatkuu edelleen, ja teknologian sovellusmahdollisuudet näyttävät rajattomilta. Tulevaisuudessa lohkoketjuteknologiaa saatetaan hyödyntää

muun muassa älykaupungeissa, autonomisissa ajoneuvoissa ja Internet of Things -sovelluksissa.

1.2.1. Bitcoinin keksiminen

Bitcoinin keksiminen on yksi merkittävimmistä tapahtumista lohkoketjuteknologian historiassa. Vuonna 2008 julkaistun Satoshi Nakamoton kirjoituksen "Bitcoin: A Peer-to-Peer Electronic Cash System" myötä syntyi uusi hajautettu valuutta, joka perustui lohkoketjuteknologiaan.

Bitcoin toimii hajautetusti ilman keskitettyä valvontaa, mikä tekee siitä erittäin turvallisen ja anonyymin. Kaikki tapahtumat tallennetaan lohkoketjuun, jota ylläpitää hajautettu verkosto tietokoneita, eikä yksittäinen taho pysty manipuloimaan tietoja.

Bitcoinin käyttö on kasvanut merkittävästi sen keksimisen jälkeen, ja sitä voidaan käyttää maksuvälineenä verkkokaupoissa ja muissa palveluissa, joissa bitcoinin hyväksyminen on mahdollista.

Bitcoinin keksiminen on inspiroinut muita lohkoketjuprojekteja, ja se on ollut tärkeä lähtökohta lohkoketjuteknologian kehitykselle.

1.2.2. Ethereumin lanseeraus

Vuonna 2014 julkaistiin Ethereum, joka on toinen suuri lohkoketjuteknologia Bitcoinin jälkeen. Ethereumin perustaja, Vitalik Buterin, oli kriittinen suhteessa Bitcoinin

lohkoketjuteknologiaan ja päätti kehittää oman alustan, joka mahdollistaisi älykkäiden sopimusten luomisen lohkoketjuun.

Ethereumin avulla kehittäjät voivat luoda hajautettuja sovelluksia ja älykkäitä sopimuksia, jotka suorittuvat automaattisesti ja läpinäkyvästi ilman keskitettyä välikättäjää. Ethereumin lohkoketjussa toimii myös Ether-niminen kryptovaluutta, joka on toiseksi suurin Bitcoinin jälkeen.

Ethereum on luonut monia innovaatioita lohkoketjuteknologiassa, kuten älykkäät sopimukset, ERC-20-standardin, joka mahdollistaa lohkoketjupohjaisten kryptovaluuttojen luomisen, ja Ethereum Virtual Machinen, joka mahdollistaa koodin suorittamisen lohkoketjussa. Nämä innovaatiot ovat mahdollistaneet monia uusia sovelluskohteita lohkoketjuteknologialle, kuten hajautettujen rahoitussovellusten ja äänestyssysteemien kehittämisen.

Ethereum on myös ollut kiistojen kohteena sen jälkeen kun sen suosio kasvoi nopeasti. Lohkoketjun skaalautuvuus ja sen vaikutus ympäristöön ovat herättäneet huolta, ja myös lohkoketjun turvallisuus on ollut kyseenalaistettu. Ethereumin kehittäjät ovat kuitenkin jatkuvasti pyrkineet parantamaan lohkoketjun toimivuutta ja turvallisuutta uusilla päivityksillä ja innovaatioilla.

1.2.3. Lohkoketjuteknologian kehityksen merkittävät vaiheet

Lohkoketjuteknologian kehitys on ollut nopeaa ja merkittävää sen keksimisestä lähtien. Bitcoinin ja Ethereumin jälkeen on kehitetty lukuisia muita lohkoketjuteknologiaan perustuvia projekteja ja sovelluksia.

Yksi merkittävä vaihe lohkoketjuteknologian kehityksessä oli hajautettujen sovellusten (DApps) keksiminen. Ethereumin lanseeraus mahdollisti älysopimusten käytön lohkoketjuissa, jolloin lohkoketjuihin voitiin luoda ohjelmallisesti suoritettavia sopimuksia. Tämä avasi uusia mahdollisuuksia hajautettujen sovellusten kehittämiselle ja toteutukselle.

Toinen merkittävä vaihe lohkoketjuteknologian kehityksessä oli skaalautuvuuden ratkaiseminen. Aiemmin lohkoketjuteknologian skaalautuvuus oli ollut ongelmana, sillä lohkoketjujen kasvaessa niiden suorituskyky heikkeni. Tämä johti lohkoketjujen hitauteen ja tehottomuuteen, mikä rajoitti niiden käyttöä. Kuitenkin erilaiset skaalautuvuusratkaisut, kuten sharding ja off-chain ratkaisut, ovat auttaneet ratkaisemaan näitä ongelmia.

Kolmas merkittävä vaihe lohkoketjuteknologian kehityksessä on ollut yksityisyyden parantaminen. Alkuvaiheessa lohkoketjuissa tapahtuneet tapahtumat olivat täysin avoimia ja läpinäkyviä, mikä ei ollut toivottavaa kaikissa käyttökohteissa. Tämä on johtanut uusien yksityisyyteen liittyvien lohkoketjuteknologioiden kehittämiseen, kuten zk-SNARK ja Monero.

Neljäs merkittävä vaihe lohkoketjuteknologian kehityksessä on ollut lohkoketjujen käytön laajentuminen eri teollisuuden aloille. Alkuperäisen käyttötarkoituksen, eli rahansiirtojen ja transaktioiden käyttämisen lisäksi, lohkoketjuteknologiaa on alettu soveltaa monilla eri aloilla, kuten lääketieteessä, logistiikassa, äänestyksissä ja älykkäissä laitteissa.

Nämä ovat vain muutamia esimerkkejä merkittävistä vaiheista lohkoketjuteknologian kehityksessä, mutta osoittavat sen nopean kehityksen ja laajan käyttömahdollisuuden eri aloilla.

1.3. Lohkoketjujen merkitys digitaalisessa maailmassa

Lohkoketjujen merkitys digitaalisessa maailmassa on kasvanut huomattavasti sen jälkeen, kun Bitcoin ja sen lohkoketjuteknologia esiteltiin vuonna 2008. Lohkoketjut tarjoavat hajautetun ja luotettavan tavan tallentaa ja jakaa tietoa ilman keskitettyä valvontaa, mikä lisää turvallisuutta ja vähentää välittäjien tarvetta. Lohkoketjuja käytetään laajasti kryptovaluuttojen lisäksi esimerkiksi hajautetun tiedon tallentamiseen, älysopimusten suorittamiseen, äänestysten toteuttamiseen ja hajautetun rahoituksen (DeFi) sovelluksiin. Lohkoketjujen odotetaan vaikuttavan laajasti monilla aloilla, kuten terveydenhuollossa, vakuutusala, logistiikka, älykkäät kaupungit ja jopa vaalijärjestelmät.

1.3.1. Lohkoketjuteknologian vaikutus talouteen ja rahoitukseen

Lohkoketjuteknologialla on ollut merkittävä vaikutus talouteen ja rahoitukseen eri tavoin. Yksi merkittävimmistä vaikutuksista on ollut se, että lohkoketjut ovat mahdollistaneet uusien liiketoimintamallien syntymisen ja olemassa olevien liiketoimintamallien parantamisen. Tämä on johtunut siitä, että lohkoketjut tarjoavat uusia tapoja varmentaa ja siirtää arvoa.

Esimerkiksi rahansiirrot ovat yksi alue, jossa lohkoketjuteknologia on mahdollistanut nopeampia ja edullisempia transaktioita. Tämä johtuu siitä, että lohkoketjut mahdollistavat suorat henkilöiden väliset rahansiirrot ilman välittäjää, kuten pankkia. Lisäksi lohkoketjut tarjoavat lisäturvaa rahansiirroille, sillä lohkoketjuun tallennettuja transaktioita ei voi muuttaa tai manipuloida.

Toinen merkittävä vaikutus on ollut lohkoketjuteknologian soveltaminen pörssikaupassa. Lohkoketjut mahdollistavat

osakkeiden ja muiden arvopapereiden välittämisen ja kaupankäynnin ilman välikäsiä, kuten pankkeja tai pörssivälittäjiä. Tämä mahdollistaa nopeamman ja kustannustehokkaamman kaupankäynnin.

Lisäksi lohkoketjuteknologia mahdollistaa uusien rahoitusmuotojen syntymisen, kuten Initial Coin Offerings (ICO) ja Security Token Offerings (STO). Nämä muodot ovat mahdollistaneet uusien yritysten rahoituksen keräämisen lohkoketjuun perustuvien tokenien avulla, joita sijoittajat voivat ostaa.

Kaiken kaikkiaan lohkoketjuteknologia on muuttanut rahoitusalan perusteita, ja sen vaikutukset tulevat olemaan merkittäviä myös tulevaisuudessa.

1.3.2. Lohkoketjuteknologian käyttö mahdollistaa uusia sovelluskohteita

Lohkoketjuteknologian käyttö mahdollistaa monia uusia sovelluskohteita eri aloilla. Koska lohkoketju tarjoaa hajautetun ja läpinäkyvän tietokannan, sen käyttöä voidaan soveltaa monilla eri tavoilla, joita perinteiset keskitetyt järjestelmät eivät mahdollista. Tässä on joitakin esimerkkejä uusista sovelluskohteista:

1. Hajautetut digitaaliset omaisuudet: Lohkoketju mahdollistaa uusien digitaalisten omaisuuksien, kuten kryptovaluuttojen, luomisen ja vaihtamisen ilman välikäsiä. Tämä mahdollistaa entistä nopeamman, turvallisemman ja halvemman omaisuuden siirron ja vaihdon.
2. Älysopimukset: Älysopimukset ovat ohjelmia, jotka

toimivat automaattisesti lohkoketjussa määritettyjen ehtojen täyttymisen perusteella. Ne mahdollistavat sopimusten luomisen ja toteuttamisen ilman kolmannen osapuolen väliintuloa. Älysopimukset voivat olla hyödyllisiä esimerkiksi äänestysjärjestelmien ja äänestysselvitysten toteuttamisessa.

3. Hajautetut sovellukset (dApps): Hajautetut sovellukset ovat sovelluksia, jotka toimivat lohkoketjussa ja käyttävät sen ominaisuuksia, kuten hajautusta, läpinäkyvyyttä ja älysopimuksia. Ne voivat olla hyödyllisiä esimerkiksi hajautetun varastonhallinnan, hajautetun energiajärjestelmän ja hajautetun tietokannan toteuttamisessa.
4. Hajautetut identiteetit: Lohkoketju mahdollistaa hajautetun identiteetin luomisen ja käytön, joka voi olla hyödyllinen esimerkiksi henkilöllisyyden varmentamisessa, äänestysjärjestelmissä ja rahoituspalveluissa.
5. Supply Chain Management (SCM): Lohkoketjun avulla SCM voi olla läpinäkyvämpää ja tehokkaampaa. Esimerkiksi lohkoketjuun tallennettuun tietoon voidaan luottaa helpommin, jolloin tuotteiden jäljitettävyys on parempi.

Nämä ovat vain joitakin esimerkkejä lohkoketjuteknologian sovelluskohteista. Lohkoketjun käytön mahdollisuudet ovat käytännössä rajattomat ja uusia sovelluskohteita keksitään jatkuvasti.

1.3.3. Lohkoketjujen merkitys tulevaisuuden teknologiassa

Lohkoketjujen merkitys tulevaisuuden teknologiassa on merkittävä, sillä ne tarjoavat monia mahdollisuuksia eri alojen kehittämisessä ja digitalisaatiossa. Lohkoketjuteknologian avulla voidaan luoda hajautettuja ja läpinäkyviä järjestelmiä, joilla on korkea tietoturva ja luotettavuus. Tämä mahdollistaa uusien liiketoimintamallien syntymisen ja auttaa vähentämään kustannuksia ja lisäämään tehokkuutta.

Esimerkkejä tulevaisuuden sovelluskohteista ovat muun muassa hajautetut energiamarkkinat, älykaupungit ja -liikenne, digitaaliset terveyspalvelut sekä lohkoketjuun perustuvat älykkäät sopimukset. Lohkoketjujen käyttö voi myös parantaa datan hallintaa ja mahdollistaa turvallisemman tiedon jakamisen eri organisaatioiden välillä.

Lohkoketjuteknologia on vielä suhteellisen uusi keksintö, ja sen tulevaisuus riippuu osittain sen kehityksestä ja käyttöönotosta. On kuitenkin selvää, että lohkoketjut tulevat olemaan tärkeä osa tulevaisuuden teknologiaa ja vaikuttavat monilla eri aloilla, kuten taloudessa, terveydenhuollossa, logistiikassa ja energiantuotannossa.

2. Lohkoketjujen tekniset perusteet

Osiossa 2 käsitellään lohkoketjujen teknisiä perusteita ja rakennetta. Ensimmäisessä luvussa käydään läpi lohkoketjun rakennuspalikat, kuten transaktiot, lohkot ja hajautetut verkot. Toisessa luvussa keskitytään lohkoketjujen louhintaan, sen prosesseihin ja eri konsensusmekanismeihin. Kolmannessa luvussa tarkastellaan lohkoketjujen tietoturvaa ja yksityisyydensuojaa, sekä muita lohkoketjujen

haavoittuvuuksia ja riskejä. Lopuksi esitellään erilaisia lohkoketjujen sovelluskohteita ja käyttötapauksia. Osio tarjoaa lukijalle yleiskuvan lohkoketjuteknologian teknisistä ominaisuuksista ja sen toimintaperiaatteista.

2.1. Lohkot ja ketjut

Lohkoketjuteknologia perustuu lohkoihin ja ketjuihin. Lohkot ovat kuin tietokannan osia, jotka sisältävät tiivisteen edellisestä lohkosta, transaktiotiedot ja tiivisteen lohkon sisällöstä. Ketju puolestaan muodostuu näistä lohkoista, joita yhdistää tiivisteiden avulla syntynyt lohkoketju. Tämä ketju varmistaa, että lohkot ovat järjestyksessä ja että ketjua ei ole manipuloitu. Jokaisen uuden lohkon lisääminen lohkoketjuun varmistaa, että ketju laajenee edelleen ja että aikaisempien lohkojen sisältö säilyy muuttumattomana. Lohkot ja ketjut ovat keskeisiä lohkoketjuteknologian toiminnan kannalta, sillä ne varmistavat, että lohkoketju on hajautettu, turvallinen ja luotettava.

2.1.1. Lohkojen toiminta

Lohkot ovat keskeinen osa lohkoketjuteknologiaa, ja niiden toiminta on tärkeää ymmärtää, jotta lohkoketjuteknologian periaatteet ovat selkeät. Lohkot koostuvat tietueista, joita kutsutaan transaktioiksi, ja jokaisessa lohkossa voi olla useita transaktioita. Lohkojen toiminta perustuu siihen, että ne tallentavat tiedot siten, että ne ovat peruuttamattomia ja läpinäkyviä.

Kun uusi transaktio tehdään, se lisätään lohkoon, joka on tarkoitettu uusien transaktioiden vastaanottamiseen. Jokainen lohko on linkitetty edelliseen lohkoon, jolloin syntyy lohkoketju. Tämä tarkoittaa sitä, että lohkoketjussa olevat

lohkot ovat järjestyksessä aina vanhimmasta uusimpaan.

Lohkojen toiminnan kannalta tärkeä tekijä on niiden validointi. Kun uusi transaktio lisätään lohkoon, se tulee ensin validoida, jotta se voidaan hyväksyä lohkoon. Tämä tarkoittaa, että transaktion on oltava todennettavissa ja sen on täytettävä lohkoketjun asettamat säännöt. Kun transaktio on validointiprosessin läpäissyt, se lisätään lohkoon ja lohko lisätään lohkoketjuun.

Lohkojen toiminta on olennainen osa lohkoketjuteknologiaa, ja sen avulla voidaan luoda läpinäkyviä ja turvallisia tietokantoja, joita voidaan käyttää monissa sovelluskohteissa. Kun lohkoketjun lohkot ovat validointiprosessin läpäisseet, niiden sisältämät tiedot ovat peruuttamattomia, mikä takaa lohkoketjun turvallisuuden ja eheyden.

2.1.2. Lohkojen sisältö

Lohkot ovat tärkeä osa lohkoketjua, sillä ne sisältävät tietoa tapahtumista ja toimivat linkkeinä ketjussa. Jokainen lohko sisältää tietyn määrän transaktioita, eli tapahtumia, joita on tehty lohkon luomisen jälkeen. Tietojen tallentaminen lohkoihin tapahtuu monilla eri lohkoketjuilla samalla tavalla: jokaisessa lohkossa on otsikko, joka sisältää lohkon numeron, aikaleiman ja sen, mistä lohkosta se seuraa.

Lisäksi jokaisessa lohkossa on merkintä edellisestä lohkosta, joten lohkot ovat ketjussa peräkkäin ja niiden järjestys on tärkeä. Tämä mahdollistaa sen, että lohkoketjua ei voida muuttaa ilman että se vaikuttaa koko ketjuun. Lohkon sisältöön kuuluu myös tieto lohkon luojasta, joka voi olla esimerkiksi tietokoneohjelma tai ihminen, joka on ratkaissut

monimutkaisen matemaattisen ongelman.

Lohkojen sisältö voi vaihdella lohkoketjun tarkoituksesta riippuen. Esimerkiksi Bitcoinin lohkot sisältävät tiedon siirretyistä Bitcoineista ja niiden vastaanottajista sekä laskentatiedot, joiden avulla lohkon luonut tietokoneohjelma on ratkaissut matemaattisen ongelman. Ethereumilla lohkoissa on myös tietoa älysopimuksista, joiden avulla käyttäjät voivat luoda hajautettuja sovelluksia.

Lohkojen sisältö on suojattu salauksella, jotta niiden tietojen manipulointi ei olisi mahdollista. Tämä salaus takaa myös sen, että lohkoketjun tietoja voidaan käyttää luotettavasti ja turvallisesti. Salauksen purkaminen vaatisi valtavan määrän laskentatehoa, mikä tekee tietojen muuttamisesta lähes mahdotonta.

2.1.3. Lohkojen validointi

Lohkojen validointi on keskeinen osa lohkoketjuteknologian toimintaa. Kun uusi lohko lisätään lohkoketjuun, sen sisältö tulee olla validi ja kaikkien verkon osallistujien tulee olla yhtä mieltä sen validiudesta. Tämä tarkoittaa sitä, että lohkon sisältö tulee olla oikein ja sen pitää täyttää tiettyjä ehtoja, jotta se hyväksytään lohkoketjuun.

Yksi tärkeimmistä ehdoista on lohkon hash-arvon laskeminen. Jokaisessa lohkossa on hash-arvo, joka on laskettu lohkon sisällöstä. Hash-arvo muuttuu, jos lohkon sisältö muuttuu. Tämä tarkoittaa sitä, että jos joku yrittää manipuloida lohkon sisältöä, sen hash-arvo muuttuu ja muutos huomataan.

Lisäksi lohkon validoinnissa tarkistetaan lohkon allekirjoitus, joka varmistaa sen, että lohko on lähetetty oikealta lähettäjältä.

Tämä estää lohkoketjun turvallisuuden kannalta tärkeiden lohkojen manipuloinnin.

Validointiprosessi on automatisoitu lohkoketjussa, ja se toteutetaan konsensusmekanismin avulla. Verkon osallistujat tarkistavat lohkon validiuden ja hyväksyvät sen, jos se täyttää vaaditut ehdot. Konsensusmekanismi varmistaa sen, että kaikki verkon osallistujat ovat yhtä mieltä lohkon validiudesta ja sen lisäämisestä lohkoketjuun.

2.2. Hajautettu pääkirja

Hajautettu pääkirja (Distributed Ledger) on hajautetun järjestelmän perusta, joka tallentaa tietoja useisiin solmuihin ympäri verkkoa. Tämä mahdollistaa tietojen tallentamisen, jakamisen ja synkronoinnin ilman keskitettyä hallintaa. Lohkoketjut ovat yksi hajautettujen pääkirjojen tyyppi, ja ne tallentavat tietoja ketjussa oleviin lohkoihin siten, että uusi lohko linkitetään edelliseen lohkoon muodostaen ketjun. Tämä mahdollistaa tietojen tallentamisen turvallisesti ja läpinäkyvästi, koska lohkoketjuja ei voi muuttaa tai poistaa ilman muiden verkon solmujen suostumusta.

2.2.1. Pääkirjan merkitys lohkoketjussa

Pääkirja on tärkeä osa lohkoketjua, sillä se toimii kaikkien lohkojen keskitettynä tallennuspaikkana. Pääkirja sisältää kaikki lohkot kronologisessa järjestyksessä, ja sen avulla voidaan tarkistaa kaikki tapahtumat lohkoketjussa alkaen ensimmäisestä lohkosta. Pääkirjan tehtävänä on myös varmistaa lohkoketjun eheys ja estää mahdolliset virheet ja

petokset.

Pääkirja on hajautettu, mikä tarkoittaa että sen kopioita on useilla eri tietokoneilla ympäri maailmaa. Tämä tekee lohkoketjusta erittäin turvallisen, sillä jos yhdellä tietokoneella on ongelmia, muut kopiot voivat korvata sen. Pääkirjan hajautus takaa myös sen, että lohkoketjun tietoja on lähes mahdotonta väärentää, sillä kaikki tietokoneet pitävät kirjaa samasta pääkirjasta.

Pääkirjan merkitys korostuu erityisesti lohkoketjun turvallisuuden kannalta, sillä jos lohkoketjun pääkirja joutuu hakkeroinnin kohteeksi, lohkoketjun toiminta voi häiriintyä vakavasti. Pääkirjan eheyden ja turvallisuuden takaaminen on siis erittäin tärkeää lohkoketjun käyttökohteista riippumatta.

2.2.2. Lohkoketjun rakenne ja toiminta

Lohkoketju on hajautettu tietokanta, joka sisältää järjestetyn sarjan tietueita, joita kutsutaan lohkoiksi. Lohkot ovat yhdistetty edelliseen lohkoon kryptografisella tiivisteellä, mikä luo lohkoketjun, joka on mahdollista tarkastaa ja vahvistaa. Tämä tekniikka mahdollistaa hajautetun tietokannan, joka ei ole yhden yksittäisen osapuolen hallinnassa, vaan joka perustuu hajautettuun verkkoon, joka voi sisältää tuhansia tai jopa miljoonia tietokoneita.

Lohkoketjun rakenne koostuu useista eri osista, kuten pääkirjasta, transaktioista ja lohkoista. Pääkirja sisältää kaikki lohkoketjussa olevat tiedot ja toimii tärkeimpänä tietovarastona. Transaktiot sisältävät tiedot siitä, mitä tapahtuu lohkoketjussa, esimerkiksi rahan siirroista tai tietojen tallentamisesta. Lohkot puolestaan sisältävät transaktiot ja ne

liitetään edelliseen lohkoon kryptografisella tiivisteellä.

Lohkoketjun toiminta perustuu hajautetun verkon periaatteeseen, jossa useat eri tietokoneet ympäri maailmaa osallistuvat lohkoketjun ylläpitoon ja validointiin. Jokainen tietokone lohkoketjussa voi toimia verkon solmuna, joka validoi uusia transaktioita ja uusia lohkoja. Lohkoketjun toimintaperiaate mahdollistaa luotettavan ja turvallisen tavan tallentaa ja jakaa tietoa ilman keskitettyä valvontaa.

2.3. Konsensusmekanismit

Konsensusmekanismi on mekanismi, jonka avulla hajautettu pääkirja (distributed ledger) saadaan synkronoitua ja validoitua. Se on siis menetelmä, jolla hajautetun järjestelmän solmut pääsevät yhteisymmärrykseen siitä, mikä on totuus tiettyyn tapahtumaan tai transaktioon liittyen.

Lohkoketjujen konsensusmekanismit voivat perustua erilaisiin algoritmeihin, joista yleisimpiä ovat proof of work (PoW) ja proof of stake (PoS). Proof of work -algoritmissa solmujen tulee suorittaa laskentatehtävä, joka on tarpeeksi vaikea, jotta sen ratkaisemiseen tarvitaan huomattava määrä laskentatehoa. Proof of stake -algoritmissa sen sijaan solmut "panostavat" tiettyyn määrään kryptovaluuttaa, joka toimii takuuna niiden rehellisyydestä.

Konsensusmekanismit ovat keskeinen osa lohkoketjuteknologiaa, sillä niiden avulla estetään petoksia ja virheellistä tietoa lohkoketjuun tallentumasta.

2.3.1. Proof of Work

Proof of Work (PoW) on yksi lohkoketjujen konsensusmekanismeista, jota käytetään useissa tunnetuissa lohkoketjuissa, kuten Bitcoinissa ja Ethereumissa. Konsensusmekanismi on menetelmä, jolla lohkoketjussa varmistetaan, että lohko on pätevä ja luotettava, ennen kuin se hyväksytään ja lisätään lohkoketjuun.

PoW-konsensusmekanismi vaatii lohkoketjun validointiprosessin aikana ratkaistavan matemaattisen ongelman, joka vaatii huomattavaa laskentatehoa. Prosessi alkaa, kun louhija yrittää löytää lohkon hash-funktiolle tietyn yksilöllisen arvon. Tämä on erittäin laskennallisesti vaativa prosessi, ja vaadittava laskentateho kasvaa, kun lohkojen määrä lisääntyy.

Kun lohkon hash on löydetty, louhija lähettää lohkon lohkoketjuun, ja muut solmut tarkistavat sen. Tarkistusprosessi on yksinkertainen, sillä muiden solmujen tarvitsee vain suorittaa saman laskennallisen ongelman ratkaiseminen, jotta ne voivat varmistaa, että ratkaisu on oikea.

PoW-konsensusmekanismilla on joitain etuja, kuten sen luotettavuus ja turvallisuus, sillä lohkoketjuun ei voi lisätä väärennettyjä lohkoja ilman, että ratkaiseminen vaatii merkittävää laskentatehoa. Toisaalta PoW on myös erittäin energiavaltainen ja hidastaa lohkoketjun transaktioiden käsittelyä, koska ratkaisemisprosessi voi olla erittäin pitkä ja raskas. Tämä on johtanut useiden lohkoketjujen siirtymiseen muihin konsensusmekanismeihin, kuten Proof of Stake.

2.3.2. Proof of Stake

Proof of Stake (PoS) on toinen yleisesti käytetty konsensusmekanismi lohkoketjuissa, joka perustuu osallistujien osoittamaan panokseen sen sijaan, että se perustuisi laskentatehoon, kuten Proof of Work (PoW) -mekanismi. PoS-mekanismiin osallistuvat verkon käyttäjät, jotka laittavat lohkoketjuun panoksensa, jota kutsutaan nimellä ”stake” (panos). Mitä suurempi panos on, sitä suurempi on todennäköisyys, että käyttäjä valitaan seuraavaksi lohkon validointiin.

PoS-mekanismin tarkoituksena on vähentää lohkoketjun laskentatehon tarvetta, joka on PoW-mekanismin heikkous. Tämä johtuu siitä, että PoW vaatii valtavasti laskentatehoa ja sähköä, mikä tekee siitä kalliin ja ympäristöystävällisyydeltään heikon vaihtoehdon.

PoS-mekanismi vähentää myös 51% hyökkäyksen riskiä, koska hyökkääjän täytyy omistaa yli 51% lohkoketjun kaikista stakeista, jotta hän voisi manipuloida lohkoketjua. Tämä tekee lohkoketjusta turvallisemman ja vähentää sen altistumista hyökkäyksille.

PoS-mekanismia käytetään esimerkiksi Ethereum 2.0:ssa ja Cardanossa, jotka ovat kaksi suosittua lohkoketjua. PoS:n käyttöönotto on kuitenkin herättänyt myös keskustelua sen oikeudenmukaisuudesta, koska suuremmilla panoksilla on suurempi vaikutus lohkoketjun päätöksentekoon. Tämä onkin yksi PoS:n haasteista, jota pyritään ratkaisemaan esimerkiksi sattumanvaraisilla valinnoilla ja rangaistusmekanismeilla.

2.3.3. Delegated Proof of Stake

Delegated Proof of Stake (DPoS) on toinen suosittu konsensusmekanismi lohkoketjuteknologiassa, joka käyttää valittuja edustajia tarkistamaan transaktioita ja vahvistamaan lohkoja. DPoS:n avulla valittuja edustajia kutsutaan myös todistajiksi (witnesses) tai delegaateiksi (delegates).

DPoS-toimintaperiaate on yksinkertainen: omistajat voivat äänestää valitsemiaan edustajia, jotka ovat vastuussa lohkoketjun toiminnasta. Äänestyksessä käytetään yleensä kryptovaluutan tokeneita, joita omistajat voivat käyttää äänestysvoimansa mukaisesti. Mitä enemmän tokeneita omistajalla on, sitä enemmän äänestysvoimaa hänellä on.

Valitut edustajat vastaanottavat transaktiomaksuja lohkon validoinnista ja uusien tokenien luomisesta. Tämä kannustaa edustajia toimimaan oikein ja rehellisesti lohkoketjussa. DPoS:n etuna on myös sen skaalautuvuus, koska se voi käsitellä suuria määriä transaktioita nopeasti.

Toisaalta DPoS herättää kritiikkiä keskittymisestään valtaan ja demokratian puutteesta, koska suuret tokenin omistajat voivat hallita edustajien valintaa ja siten lohkoketjun toimintaa. Lisäksi DPoS jättää pois monet osallistumisen muodot, joita muut konsensusmekanismit tarjoavat.

2.4. Turvallisuus ja yksityisyys lohkoketjuissa

Lohkoketjujen turvallisuus ja yksityisyys ovat olennaisia osia teknologian toimivuudelle ja käytölle. Lohkoketjujen hajautetun luonteen takia jokainen lohkoketjun solmu voi pitää omaa kopioitaan pääkirjasta, mikä lisää turvallisuutta ja suojaa verkon manipuloinnilta. Jotta lohkoketju olisi todella turvallinen, sen on kuitenkin oltava immuuni hakkereiden

hyökkäyksille ja väärinkäytöksille.

Yksi tärkeimmistä lohkoketjujen turvallisuusmekanismeista on konsensusmekanismi, joka varmistaa, että jokainen solmu lohkoketjussa pitää saman sisällön. Lohkoketjun tietojen yksityisyys on myös tärkeää, ja siksi useat lohkoketjuteknologiat tarjoavat erilaisia salausmenetelmiä, joiden avulla tietoja voidaan suojata.

Käyttäjien yksityisyyden suojaaminen on erityisen tärkeää kryptovaluuttakäytössä, sillä lohkoketju tallentaa kaikki tapahtumat pysyvästi ja julkisesti. Monet lohkoketjuteknologiat tarjoavat kuitenkin myös yksityisyyden suojaamiseen tarkoitettuja työkaluja, kuten salattuja transaktioita ja anonyymejä osoitteita.

Lohkoketjujen turvallisuus ja yksityisyys ovat jatkuvan kehityksen kohteita, ja uusia ratkaisuja löydetään ja testataan jatkuvasti. On tärkeää, että lohkoketjujen käyttäjät ja kehittäjät seuraavat tarkasti uusimpia kehityksiä ja parhaita käytäntöjä tietoturvan ja yksityisyyden varmistamiseksi.

2.4.1. Lohkoketjujen turvallisuusmekanismit

Lohkoketjujen turvallisuus on yksi tärkeimmistä ominaisuuksista, joita lohkoketjuteknologialta odotetaan. Tämä johtuu siitä, että lohkoketju sisältää arkaluontoista tietoa, kuten transaktiotietoja ja henkilökohtaisia tietoja. Lohkoketjun turvallisuusmekanismit ovat suunniteltu suojaamaan tätä tietoa.

Yksi tärkeimmistä lohkoketjujen turvallisuusmekanismeista on konsensusmekanismi. Konsensusmekanismi on menetelmä, jonka avulla lohkoketjun käyttäjät voivat sopia siitä, mikä

lohko hyväksytään seuraavaksi lohkoketjuun. Tämä on erittäin tärkeää, koska se estää mahdollisuuden, että lohkoketjuun lisätään väärennettyjä lohkoja. Konsensusmekanismi perustuu yleensä matemaattiseen ratkaisuun tai verkon osallistujien äänestykseen.

Toinen tärkeä turvallisuusmekanismi on lohkoketjujen hajauttaminen. Hajauttaminen tarkoittaa, että lohkoketjun tietoja tallennetaan useisiin solmuihin tai verkon tietokoneisiin. Tämä tarkoittaa, että jos yksi solmu tai tietokone jostain syystä epäonnistuu, lohkoketju säilyy silti turvallisena, koska tietoja on tallennettu useisiin paikkoihin.

Lohkoketjujen turvallisuutta parantavat myös erilaiset salaustekniikat, kuten SHA-256, joka on käytössä Bitcoinissa. Näitä salaustekniikoita käytetään tietojen suojaamiseen ja estävät niiden muuttamisen.

Lisäksi lohkoketjuissa käytetään usein älysopimuksia, jotka ovat ohjelmia, jotka suorittavat toimintoja automaattisesti, kun tiettyjä ehtoja täyttyy. Älysopimukset ovat erittäin tärkeitä lohkoketjujen turvallisuuden kannalta, koska ne mahdollistavat sopimuksen täytäntöönpanon ilman kolmannen osapuolen väliintuloa.

Kaikkien näiden turvallisuusmekanismien avulla lohkoketjut ovat yleisesti ottaen hyvin turvallisia, mutta ne eivät ole täysin immuuneja hyökkäyksille. Siksi lohkoketjuihin liittyvien riskien ymmärtäminen ja niihin liittyvien turvatoimenpiteiden toteuttaminen on erittäin tärkeää.

2.4.2. Yksityisyys lohkoketjuissa

Yksityisyys on tärkeä tekijä lohkoketjuissa, koska lohkoketjut

ovat julkisia ja kaikki transaktiot tallennetaan pysyvästi. Tämä voi olla haitallista, jos henkilön henkilökohtaisia tietoja voidaan jäljittää lohkoketjun avulla.

Lohkoketjujen yksityisyyttä voidaan parantaa käyttämällä erilaisia tekniikoita, kuten salaus ja pseudonyymit. Salaus tarkoittaa tietojen salauksen käyttöä, joka tekee tiedoista lukukelvottomia ulkopuolisille. Pseudonyymit puolestaan tarkoittavat sitä, että käyttäjät eivät käytä todellisia henkilökohtaisia tietojaan, vaan käyttävät sijasta pseudonyymejä tai muita tunnisteita.

Lisäksi on olemassa kehittyneempiä yksityisyystekniikoita, kuten zk-SNARK, joka mahdollistaa yksityisten transaktioiden toteuttamisen julkisessa lohkoketjussa. Tällainen tekniikka mahdollistaa yksityisyyden ja turvallisuuden samanaikaisesti.

Yksityisyyden lisääminen lohkoketjuun voi kuitenkin vaikuttaa haitallisesti lohkoketjun avoimuuteen ja läpinäkyvyyteen. Tämä voi olla ongelmallista esimerkiksi julkisen hallinnon käyttäessä lohkoketjua. Siksi yksityisyyden ja avoimuuden tasapaino on tärkeä huomioida lohkoketjusovelluksia suunniteltaessa.

3. Lohkoketjut tietokantoina

Osiossa 3 "Lohkoketjut tietokantoina" käsitellään lohkoketjuteknologian käyttöä tietokantana. Tietokannat ovat olennainen osa tietojenkäsittelyä, ja lohkoketjut voivat tarjota uusia tapoja tallentaa, jakaa ja hallita tietoja. Osiossa tarkastellaan lohkoketjujen käyttöä tietokantoina ja niiden eroja perinteisiin keskitettyihin tietokantoihin. Lisäksi käsitellään lohkoketjuteknologian käytön riskejä tietokantana, sekä joitakin parhaita käytäntöjä lohkoketjujen käytössä

tietokantana.

3.1. Perinteiset tietokannat vs. lohkoketjut

Perinteiset tietokannat ovat keskitettyjä, kun taas lohkoketjut ovat hajautettuja ja läpinäkyviä. Lisäksi lohkoketjujen käytössä on tiettyjä riskejä, kuten tietoturvariskit ja skaalautuvuusongelmat, jotka on otettava huomioon. Tässä osiossa tarkastellaan myös joitain lohkoketjuteknologian käytön suosituksia ja parhaita käytäntöjä tietokantoina.

3.1.1. Perinteisten tietokantojen toiminta

Perinteiset tietokannat toimivat keskitetysti yhdessä paikassa, jossa on keskitetty tietokantapalvelin, joka vastaa tietokannan hallinnasta ja datan tallentamisesta. Tietokannan käyttäjät voivat lukea ja kirjoittaa tietokantaan vain tietokantapalvelimen kautta. Tämä tarkoittaa sitä, että tietokanta on yhden keskitetyn auktoriteetin hallinnassa, mikä lisää haavoittuvuutta yksittäisille hyökkäyksille ja mahdollisille tietoturvariskeille.

Perinteisten tietokantojen ylläpito on yleensä kallista, sillä tietokannan ylläpitäjän on hankittava laitteistoa, ohjelmistoja ja henkilökuntaa tietokannan hallitsemiseksi ja ylläpitämiseksi. Tietokannan koon kasvaessa, sen skaalautuvuus ja suorituskyky voivat myös aiheuttaa ongelmia.

Perinteisten tietokantojen tietoturvamekanismit ovat myös haavoittuvia, sillä tietoturvan ylläpitoon käytettävä ohjelmisto ja järjestelmät voivat olla vanhentuneita ja alttiita hyökkäyksille.

Lisäksi perinteisten tietokantojen käyttöönotto ja ylläpito vaatii usein keskitetyn tietokantapalvelimen asentamista, joka

voi olla este esimerkiksi hajautetuissa tai hankalasti saavutettavissa olevissa ympäristöissä.

3.1.2. Lohkoketjujen edut ja haasteet verrattuna perinteisiin tietokantoihin

Lohkoketjut ja perinteiset tietokannat ovat erilaisia tietojen tallennusjärjestelmiä, joilla on omat edut ja haasteet. Perinteiset tietokannat tallentavat tietoja keskitetysti yhdessä paikassa, kun taas lohkoketjut tallentavat tietoja hajautetusti useille tietokoneille. Lohkoketjut käyttävät myös hajautettua pääkirjaa, joka varmistaa tietojen eheyden ja turvallisuuden.

Yksi lohkoketjujen eduista verrattuna perinteisiin tietokantoihin on niiden läpinäkyvyys. Koska lohkoketjut tallentavat tietoja hajautetusti, kaikki osapuolet voivat nähdä saman tiedon, mikä vähentää väärinkäytösten riskiä. Lohkoketjut ovat myös turvallisempia, koska tietoja ei tallenneta yhteen paikkaan, johon ulkopuoliset pääsevät käsiksi. Tietojen tallentaminen hajautetusti usealle tietokoneelle myös parantaa tietojen saatavuutta, koska tietoja on saatavilla useammasta paikasta.

Toisaalta lohkoketjut ovat vielä kehittyvä teknologia, joka vaatii paljon resursseja ja osaamista sen käyttöönottoon. Lohkoketjuteknologia voi olla myös liian raskas tai monimutkainen joillekin sovelluskohteille, joissa perinteinen tietokanta riittää. Lohkoketjut myös vaativat suuren määrän laskentatehoa, mikä voi johtaa skaalautuvuusongelmiin suurissa verkoissa.

Kaiken kaikkiaan lohkoketjut ja perinteiset tietokannat ovat erilaisia tietojen tallennusjärjestelmiä, joilla on omat edut ja

haasteet. Lohkoketjut tarjoavat läpinäkyvyyden, turvallisuuden ja tietojen saatavuuden, mutta ne vaativat paljon resursseja ja osaamista niiden käyttöönottoon. Perinteiset tietokannat ovat helpompia käyttää, mutta ne eivät tarjoa samanlaista turvallisuutta tai läpinäkyvyyttä kuin lohkoketjut.

3.2. Etuja ja haittoja käyttää lohkoketjua tietokantana

Lohkoketjujen käyttö tietokantana tuo mukanaan monia etuja, mutta myös haasteita verrattuna perinteisiin tietokantoihin. Tässä on muutamia tärkeitä etuja ja haittoja:

Etujen joukossa ovat:

1. Hajautettu pääkirja: Lohkoketjut ovat hajautettuja järjestelmiä, jossa tietoa ei hallitse yksittäinen taho, vaan se jaetaan kaikkien verkon osapuolten kesken. Tämä tekee lohkoketjuista hyvin läpinäkyviä, turvallisia ja luotettavia.
2. Lohkojen ketjutus: Lohkojen ketjutus estää lohkojen manipuloinnin, sillä yhden lohkon muokkaaminen vaatisi kaikkien sen jälkeisten lohkojen uudelleenlaskennan. Tämä tekee lohkoketjuista turvallisia ja kestäviä.
3. Älysopimukset: Lohkoketjujen älysopimukset mahdollistavat suorien, automatisoitujen sopimusten tekemisen verkon osapuolten välillä. Tämä säästää aikaa ja kustannuksia ja vähentää mahdollisia virheitä.

4. Tietoturva: Lohkoketjujen tietoturva on yleensä korkeampi kuin perinteisissä tietokannoissa. Lohkoketjuissa käytetään monia erilaisia turvallisuusmekanismeja, kuten salauksia ja konsensusmekanismeja.

Haittojen joukossa ovat:

1. Skalausongelmat: Lohkoketjut voivat olla hitaita ja tehottomia, kun kyseessä on suuri määrä tietoa, mikä tekee niistä haastavia suurien organisaatioiden käyttöön.
2. Tietosuoja: Lohkoketjuissa kaikki tiedot ovat julkisia, mikä voi olla haaste tietyissä sovelluskohteissa, kuten terveydenhuollossa tai rahoitusalalla.
3. Hajautettujen sovellusten kehityksen haasteet: Kehittäjien on ymmärrettävä lohkoketjuteknologian monimutkaisuus ja erilaiset mekanismit, mikä voi vaatia erityistä koulutusta ja taitoja.
4. Virheiden vaikeus korjata: Lohkoketjuun tallennetut tiedot ovat peruuttamattomia, mikä tarkoittaa sitä, että jos virhe tapahtuu, sitä ei voi korjata helposti. Tämä voi olla haastavaa joissakin sovelluskohteissa, kuten rahoituspalveluissa.

3.2.1. Hajautettu ja läpinäkyvä pääkirja

Yksi merkittävimmistä eduista käyttää lohkoketjua

tietokantana on sen hajautettu ja läpinäkyvä pääkirja. Perinteisissä keskitetyissä tietokannoissa tiedot tallennetaan yhteen paikkaan, joka on altis tietoturvariskeille, kuten hakkeroinnille ja virheille. Lisäksi keskitettyjä tietokantoja hallinnoi yksi organisaatio, joka pystyy määrittämään, ketkä pääsevät tietoihin käsiksi ja kuinka tietoja käytetään.

Lohkoketjussa sen sijaan tietoja tallennetaan hajautetusti monelle eri tietokoneelle, jolloin tietojen häviäminen yhdeltä tietokoneelta ei vaikuta koko järjestelmän toimintaan. Lisäksi lohkoketjussa tallennetut tiedot ovat läpinäkyviä kaikille järjestelmän käyttäjille, mikä mahdollistaa avoimuuden ja luotettavuuden. Jokainen lohko tallentaa tiedon lisäksi myös sen luontihetken ajan, mikä takaa tiedon eheyden ja luotettavuuden.

Hajautettu ja läpinäkyvä pääkirja on erityisen hyödyllinen taloudellisissa sovelluksissa, kuten maksujärjestelmissä, joissa se mahdollistaa turvalliset, nopeat ja läpinäkyvät tapahtumat. Lohkoketjun avulla voidaan myös toteuttaa hajautettuja sovelluksia, joita ei tarvitse luottaa keskitettyyn palveluun.

Kuitenkin hajautettu pääkirja voi myös aiheuttaa haasteita, kuten skaalautuvuusongelmia ja suorituskyvyn hidastumista, kun tietoja tallennetaan monelle tietokoneelle. Lisäksi läpinäkyvyyden vaatimus voi johtaa tietoturvariskeihin, kuten henkilökohtaisten tietojen julkisuuteen tai liikesalaisuuksien paljastumiseen.

3.2.2. Tietoturva ja yksityisyys

Lohkoketjujen tietoturva ja yksityisyys ovat keskeisiä etuja verrattuna perinteisiin keskitettyihin tietokantoihin. Hajautetun

tietokannan luonteesta johtuen lohkoketju on immuuni yksittäiselle tietokoneelle tai solmulle kohdistuvia hyökkäyksiä vastaan. Tämä johtuu siitä, että tietokannan kopioita on useita hajautettuna verkossa, joten yhden tietokoneen kaatuminen tai tietojen muuttaminen ei vahingoita koko tietokantaa. Lisäksi lohkoketjujen kryptografiset turvallisuusmekanismit tekevät tietojen manipuloinnin erittäin vaikeaksi.

Yksityisyys on toinen keskeinen etu lohkoketjujen käytössä tietokantana. Koska lohkoketju on hajautettu ja läpinäkyvä, tietokannan käyttäjät voivat tarkistaa ja varmistaa, että kaikki tapahtumat ovat aitoja ja että kaikki tietueet ovat tarkkoja. Samalla kuitenkin käyttäjät voivat pitää henkilökohtaiset tiedot salassa käyttämällä yksityisiä avaimia.

Haasteena lohkoketjujen tietoturvassa ja yksityisyydessä on kuitenkin käyttäjien tarve pitää yksityiset avaimet turvassa, jotta ulkopuoliset eivät voi päästä käsiksi henkilökohtaisiin tietoihin. Lisäksi hajautettujen tietokantojen turvallisuusmekanismit ovat edelleen kehityksen alla, ja uusia haavoittuvuuksia voidaan löytää tulevaisuudessa. On tärkeää kehittää ja toteuttaa jatkuvasti uusia turvallisuusmekanismeja, jotta lohkoketjujen käyttö tietokantana voi olla turvallista ja tehokasta.

3.2.3. Älysopimukset ja hajautetut sovellukset

Lohkoketjuteknologia mahdollistaa myös älysopimusten luomisen ja käytön. Älysopimukset ovat ohjelmia, jotka toimivat automaattisesti sovittujen ehtojen täyttyessä. Älysopimuksia voidaan käyttää esimerkiksi rahoitustransaktioissa tai sähköisissä sopimuksissa.

Älysopimuksien käyttö lohkoketjuissa mahdollistaa hajautetun sovellusarkkitehtuurin käytön. Tämä tarkoittaa, että sovellus ei tarvitse keskitettyä palvelinta, vaan sen toiminta perustuu hajautettuun verkostoon, joka koostuu useista tietokoneista tai laitteista. Hajautettu sovellusarkkitehtuuri mahdollistaa nopeamman ja tehokkaamman tiedonsiirron, koska tietoa ei tarvitse siirtää yhden keskitetyn palvelimen kautta.

Hajautetut sovellukset ovat yksi lohkoketjuteknologian merkittävimmistä sovelluskohteista. Niitä voidaan käyttää monilla eri aloilla, kuten esimerkiksi äänestämisessä, logistiikassa tai kiinteistökaupoissa. Hajautetut sovellukset tarjoavat useita etuja perinteisiin sovelluksiin verrattuna, kuten nopeamman ja turvallisemman tiedonsiirron, sekä mahdollisuuden toteuttaa läpinäkyvyyttä ja avoimuutta vaativia sovelluksia.

3.3. Sovelluskohteita ja esimerkkejä

Lohkoketjuteknologiaa voidaan soveltaa moniin eri käyttötapauksiin eri aloilla. Tässä osiossa esitellään joitakin esimerkkejä lohkoketjuteknologian sovelluskohteista.

3.3.1. Lohkoketjuteknologian sovelluskohteet eri aloilla

Lohkoketjuteknologia tarjoaa monipuolisia sovellusmahdollisuuksia eri aloilla. Se mahdollistaa hajautetun ja läpinäkyvän tietokannan käytön, joka voi parantaa eri toimialojen tehokkuutta ja turvallisuutta. Tässä joitakin esimerkkejä lohkoketjuteknologian sovelluskohteista eri aloilla:

- Rahoitus: Lohkoketjuteknologiaa käytetään yleisesti kryptovaluuttojen ja muiden digitaalisten maksutapojen taustalla. Lisäksi se tarjoaa mahdollisuuden älykkäiden sopimusten käyttöön, joka voi automatisoida ja nopeuttaa rahoitusprosesseja.
- Vakuutus: Lohkoketjuteknologiaa voidaan käyttää vakuutusalalla esimerkiksi vahinkojen raportoinnissa ja korvausten maksamisessa. Lohkoketju mahdollistaa tehokkaan ja tarkemman tiedonkulun kaikkien osapuolten välillä.
- Logistiikka: Lohkoketjuteknologiaa voidaan käyttää logistiikka-alalla esimerkiksi tavaroiden seurannassa ja varastojen hallinnassa. Tämä parantaa läpinäkyvyyttä ja helpottaa tavaravirtojen seurantaa.
- Terveydenhuolto: Lohkoketjuteknologiaa voidaan käyttää terveydenhuollon alalla esimerkiksi potilastietojen tallennuksessa ja jakamisessa. Lohkoketju mahdollistaa potilastietojen turvallisen ja läpinäkyvän jakamisen eri terveydenhuollon toimijoiden välillä.
- Kiinteistöala: Lohkoketjuteknologiaa voidaan käyttää kiinteistöalalla esimerkiksi kiinteistöjen omistuksen ja hallinnan hallinnassa. Lohkoketju tarjoaa tehokkaan tavan hallita kiinteistöjen omistukseen liittyviä oikeuksia ja velvoitteita.
- Energia-alan: Lohkoketjuteknologiaa voidaan käyttää energia-alalla esimerkiksi sähköverkkojen hallinnassa ja energiankulutuksen seurannassa. Lohkoketju mahdollistaa älykkäiden mittareiden käytön ja sähköntuotannon seurannan.

Nämä ovat vain muutamia esimerkkejä lohkoketjuteknologian sovelluskohteista, ja uusia sovellusalueita löydetään jatkuvasti. Lohkoketjuteknologia voi parantaa toimialojen tehokkuutta, turvallisuutta ja läpinäkyvyyttä ja tarjota uusia mahdollisuuksia liiketoiminnalle.

3.3.2. Esimerkkejä lohkoketjua käyttävistä sovelluksista

Lohkoketjuteknologiaa voidaan hyödyntää monilla eri aloilla ja sovelluksissa. Tässä joitakin esimerkkejä:

1. Kryptovaluutat: Kryptovaluutat ovat yksi tunnetuimmista lohkoketjuteknologian sovelluskohteista. Bitcoin oli ensimmäinen lohkoketjupohjainen kryptovaluutta, mutta sittemmin muitakin kryptovaluuttoja, kuten Ethereum ja Litecoin, on kehitetty.
2. Supply chain management: Lohkoketjuteknologia mahdollistaa läpinäkyvän ja turvallisen tavan seurata tuotteiden liikkeitä ja varmistaa niiden alkuperä. Esimerkiksi elintarviketeollisuudessa lohkoketjua voidaan käyttää varmistamaan, että tuotteet ovat aitoja ja eettisesti tuotettuja.
3. Kiinteistömarkkinat: Lohkoketjuteknologiaa voidaan käyttää kiinteistökaupoissa ja vuokrasopimuksissa, mikä mahdollistaa läpinäkyvämmän ja turvallisemman prosessin. Esimerkiksi Ruotsissa on jo käytössä lohkoketjupohjainen kiinteistörekisteri.
4. Äänestysjärjestelmät: Lohkoketjuteknologia

mahdollistaa turvallisen ja läpinäkyvän äänestysprosessin. Äänestystulokset tallennetaan lohkoketjuun, jolloin manipulointi on lähes mahdotonta.

5. Identiteetin hallinta: Lohkoketjuteknologia mahdollistaa turvallisen ja läpinäkyvän tavan hallita henkilöiden identiteettiä. Esimerkiksi Dubai on kehittänyt lohkoketjupohjaisen identiteetin hallintajärjestelmän.
6. Musiikkiteollisuus: Lohkoketjuteknologiaa voidaan käyttää musiikin jakelussa ja lisensoinnissa. Esimerkiksi lohkoketjupohjainen Musiconomi-alusta mahdollistaa musiikin jakamisen ja lisensoinnin suoraan artistilta fanille.

Nämä ovat vain muutamia esimerkkejä lohkoketjuteknologian sovelluskohteista. Lohkoketjujen käyttömahdollisuudet ovat lähes rajattomat ja teknologiaa voidaan hyödyntää monilla eri aloilla.

4. Suosituimmat lohkoketjut tietokantakäyttöön

Osiossa 4 käsitellään suosituimpia lohkoketjuja, jotka ovat käytössä tietokantana. Lohkoketjujen käyttö tietokantana on suhteellisen uusi käsite, ja vaatii erilaisia ominaisuuksia kuin perinteinen tietokanta, joten on tärkeää valita sopiva lohkoketju sovelluskohteen mukaan.

4.1 . Ethereum ja älysopimukset

Ethereum on lohkoketjuteknologiaan perustuva avoimen lähdekoodin alusta, joka mahdollistaa hajautetun sovelluskehityksen älysopimusten avulla. Älysopimukset ovat itsenäisiä ja automaattisia ohjelmia, jotka toteuttavat sopimusehtoja lohkoketjussa. Ethereumin lohkoketjussa älysopimukset ovat toteutettuina Ethereum Virtual Machine (EVM) -ohjelmointikielen avulla. Älysopimusten avulla sovelluskehittäjät voivat rakentaa hajautettuja sovelluksia, joissa osapuolet voivat luottaa toisiinsa ilman keskitettyjä tahoja, kuten pankkeja tai muita välittäjiä.

Ethereumin lohkoketju tarjoaa monia etuja perinteisiin tietokantoihin verrattuna. Koska lohkoketju on hajautettu, tieto on kopioituna monelle tietokoneelle, eikä sitä pysty yksittäinen taho manipuloimaan. Lisäksi Ethereumissa on mahdollista käyttää älysopimuksia, jotka mahdollistavat ohjelmoitavan automaation ilman keskitettyjä tahoja. Tämä tekee hajautetun sovelluskehityksen mahdolliseksi ja tarjoaa uusia mahdollisuuksia esimerkiksi rahoitusalalla, jossa lohkoketjuteknologialla on jo monia käyttökohteita.

Esimerkkejä Ethereum-pohjaisista sovelluksista ovat esimerkiksi hajautettu pörssi, jossa käyttäjät voivat vaihtaa kryptovaluuttoja keskinäisesti ilman välittäjiä, sekä hajautetut ennustemarkkinat, joissa käyttäjät voivat lyödä vetoa tulevaisuuden tapahtumista. Lisäksi Ethereum on ollut perusta monille initial coin offeringeille (ICO), joissa yritykset ovat rahoittaneet toimintaansa myymällä kryptovaluuttoja.

Ethereumin lohkoketjua on kritisoitu sen skaalautumisongelmista, jotka rajoittavat sen käyttöä laajoissa sovelluksissa. Ethereumin kehittäjät ovat kuitenkin työskennelleet useiden ratkaisujen parissa, kuten sharding-tekniikan ja Proof of Stake -konsensusmekanismin, jotka voisivat parantaa Ethereumin skaalautuvuutta tulevaisuudessa.

4.1.1. Ethereumin toiminta ja rakenne

Olen tarkistanut tiedot useista luotettavista lähteistä ja voin kertoa seuraavaa:

Ethereum on hajautettu tietokonealusta, joka mahdollistaa älysopimusten suorittamisen lohkoketjussa. Ethereumin lohkoketju koostuu lohkoista, joissa tallennetaan tietoa tapahtumista, ja jokainen lohko on linkitetty edelliseen lohkoon muodostaen ketjun. Ethereumissa on myös oma kryptovaluutta, Ether, joka on tarpeen älysopimusten suorittamiseen ja siirtojen tekemiseen lohkoketjussa.

Ethereumin rakenne ja toiminta perustuvat hajautettuun pääkirjaan, jossa jokaisella solmulla on kopio lohkoketjusta ja pääsy kaikkiin tallennettuihin tietoihin. Älysopimukset ovat lohkoketjussa suoritettavia ohjelmakoodinpätkiä, jotka käyttävät lohkoketjun tallentamaa tietoa ja suorittavat tiettyjä toimintoja sopimuksen ehtojen mukaisesti.

Ethereumin lohkoketju mahdollistaa hajautettujen sovellusten kehittämisen ja käytön, joita voidaan käyttää esimerkiksi hajautettujen pörssien, ennustemarkkinoiden ja äänestysjärjestelmien toteuttamiseen. Ethereumia käyttäviä sovelluksia ovat esimerkiksi Golem, joka on hajautettu tietokoneresurssien jakamisalusta, ja Augur, joka on hajautettu ennustemarkkinapaikka.

4.1.2. Älysopimusten käyttö lohkoketjuissa

Älysopimukset ovat yksi lohkoketjuteknologian

keskeisimmistä sovelluksista, ja niiden käyttö on erityisen yleistä Ethereum-lohkoketjussa. Älysopimukset ovat itsenäisiä, ohjelmoitavia ja automatisoituja sopimuksia, jotka suorittavat toimintoja, kun ne täyttävät tiettyjä ehtoja. Älysopimukset ovat siis lohkoketjujen tapa toteuttaa itseään suorittavia sopimuksia, joiden toiminta ei ole riippuvainen keskusviranomaisesta tai kolmannesta osapuolesta.

Älysopimuksia käytetään laajalti esimerkiksi rahoitus- ja vakuutusalalla, joissa ne voivat suorittaa tiettyjä toimintoja automaattisesti, kuten maksuja tai vakuutuskorvauksia, kun tietyt ehdot täyttyvät. Älysopimuksia voidaan myös käyttää esimerkiksi äänestysten toteuttamisessa, jossa sopimus varmistaa, että äänestysprosessi suoritetaan turvallisesti ja oikeudenmukaisesti.

Älysopimuksien käyttöön liittyy kuitenkin myös haasteita. Koska sopimukset ovat ohjelmoitavia ja autonomisia, niiden turvallisuus on kriittisen tärkeää, sillä yksikin ohjelmointivirhe tai tietoturva-aukko voi johtaa merkittäviin taloudellisiin tappioihin. Lisäksi älysopimusten käyttöönotto vaatii usein erityisosaamista ja teknistä tietämystä, mikä voi olla este niiden laajamittaisemmalle käytölle.

Vaikka älysopimusten käyttö onkin vielä suhteellisen uutta, niiden potentiaali on valtava, ja tulevaisuudessa älysopimusten käyttö tulee todennäköisesti lisääntymään entisestään eri aloilla.

4.1.3. Ethereum-pohjaisten sovellusten esimerkkejä

Ethereum-pohjaisia sovelluksia on kehitetty monilla eri aloilla, kuten finanssialalla, äänestysjärjestelmissä, pelimaailmassa,

sähköisissä sopimuksissa ja jopa taiteessa. Alla on muutamia esimerkkejä Ethereum-pohjaisista sovelluksista:

1. Augur: Augur on hajautettu ennustemarkkina-alusta, joka mahdollistaa käyttäjien tekemään vetoja tulevaisuuden tapahtumista. Augur perustuu älysopimuksiin, jotka suorittavat vedonlyöntitoimintoja.
2. Golem: Golem on hajautettu tietokoneiden laskentatehon jakamisen alusta. Se mahdollistaa käyttäjien vuokrata laskentatehoa toisiltaan, mikä voi olla hyödyllistä esimerkiksi raskaan tietojenkäsittelyn tehtävissä, kuten animaatioiden renderöinnissä.
3. MakerDAO: MakerDAO on hajautettu finanssipalvelu, joka mahdollistaa käyttäjien luoda vakauden omaavia kryptovaluuttoja, joiden arvo on sidottu reaalimaailman omaisuuseriin, kuten Yhdysvaltain dollariin.
4. CryptoKitties: CryptoKitties on hajautettu peli, jossa käyttäjät voivat kerätä ja kasvattaa digitaalisia kissoja. Jokaisella kissalla on oma ainutlaatuinen "genetiikkansa", ja käyttäjät voivat myydä ja ostaa kissoja toisiltaan.
5. Civil: Civil on hajautettu journalismialusta, joka tarjoaa käyttäjille mahdollisuuden lukea ja kirjoittaa sisältöä ilman sensuuria tai valvontaa. Civilin älysopimukset auttavat hallinnoimaan sisältöä ja rahoitusta.

Nämä ovat vain muutamia esimerkkejä Ethereum-pohjaisista sovelluksista, ja Ethereumin suosio lohkoketjupohjaisena alustana on avannut monia mahdollisuuksia uusien sovellusten

kehittämiselle.

4.2. Hyperledger ja yksityiset lohkoketjut

Hyperledger on avoimen lähdekoodin projekti, joka on suunniteltu helpottamaan yksityisten lohkoketjujen kehittämistä ja käyttöönottoa. Hyperledgerin avulla organisaatiot voivat rakentaa yksityisiä ja hajautettuja järjestelmiä, joissa lohkoketju toimii tietokantana.

4.2.1. Hyperledgerin toiminta ja rakenne

Hyperledger on avoimen lähdekoodin lohkoketjuteknologia, joka on tarkoitettu yritysten käyttöön. Se on kehitetty Linux-säätiön toimesta ja se koostuu useista eri projekteista, joiden tarkoituksena on tarjota erilaisia lohkoketjuratkaisuja yrityksille. Hyperledgerin keskeinen tavoite on tarjota hajautettu alusta yrityksille, joka on skaalautuva, turvallinen ja modulaarinen. Hyperledgerin rakenne koostuu useasta eri komponentista, jotka tarjoavat eri palveluita, kuten identiteetin hallintaa, konsensusta ja älysopimusten toteutusta.

Hyperledgerin tärkein komponentti on Fabric, joka tarjoaa modulaarisen alustan yrityskäyttöön. Fabricin avulla käyttäjät voivat rakentaa lohkoketjuratkaisuja, joissa on erilaisia ominaisuuksia, kuten yksityisyyttä ja skaalautuvuutta. Fabricin avulla yritykset voivat myös hallita pääsyä tietoihin ja tarjota käyttäjille erilaisia käyttöoikeuksia.

Hyperledgerin toinen tärkeä komponentti on Sawtooth, joka tarjoaa hajautetun lohkoketjualustan, joka on suunniteltu skaalautuvaksi ja turvalliseksi. Sawtoothin avulla käyttäjät voivat kehittää hajautettuja sovelluksia, jotka käyttävät

älysopimuksia. Sawtoothin modulaarinen rakenne mahdollistaa myös sen, että käyttäjät voivat valita erilaisia konsensusmekanismeja, jotka sopivat parhaiten heidän tarpeisiinsa.

Hyperledgerin kolmas tärkeä komponentti on Iroha, joka on lohkoketjualusta, joka on suunniteltu erityisesti finanssi- ja pankkialan tarpeisiin. Irohan avulla käyttäjät voivat luoda hajautettuja sovelluksia, jotka tarjoavat turvallisen ja tehokkaan tavan käsitellä rahansiirtoja.

Hyperledgerin komponentit tarjoavat yrityksille monipuolisia tapoja hyödyntää lohkoketjuteknologiaa ja rakentaa omia lohkoketjuratkaisuja. Hyperledgerin avulla yritykset voivat hyötyä lohkoketjuteknologian eduista, kuten läpinäkyvyydestä, turvallisuudesta ja hajautuksesta, samalla kun ne voivat käyttää lohkoketjuteknologiaa omien tarpeidensa mukaan.

4.2.2. Yksityisten lohkoketjujen edut ja haasteet

Hyperledger on yksityisiin lohkoketjuihin erikoistunut alusta, joka on suunniteltu erityisesti yrityskäyttöön. Yksityiset lohkoketjut eroavat julkisista lohkoketjuista siinä, että niihin pääsy ja niiden käyttö on rajoitettu vain tiettyihin organisaatioihin. Tämä mahdollistaa tietojen luottamuksellisuuden ja yksityisyyden säilymisen.

Yksityisten lohkoketjujen käyttöä on ajettu erityisesti yritysten sisäisissä prosesseissa, joissa tarvitaan luotettavaa ja turvallista tietojen hallintaa ja jakamista. Tämä voi sisältää esimerkiksi erilaisia liiketoimintaprosesseja, rahoitusta, logistiikkaa tai henkilöstöhallintoa.

Yksityisten lohkoketjujen etuja ovat muun muassa parempi

tietoturva, luotettavuus ja läpinäkyvyys verrattuna perinteisiin keskitettyihin järjestelmiin. Yksityiset lohkoketjut ovat myös skaalautuvia ja tarjoavat mahdollisuuden älysopimusten käyttöön.

Haasteita yksityisten lohkoketjujen käytössä ovat muun muassa käytännön toteutus ja ylläpito, integraatiot muiden järjestelmien kanssa sekä se, että teknologia on vielä suhteellisen uutta ja sen käyttöönotto voi vaatia tietyn oppimiskynnyksen ylittämistä.

Hyperledger on yksi alusta, joka tarjoaa ratkaisuja yksityisten lohkoketjujen toteutukseen. Se tarjoaa erilaisia työkaluja, kirjastoja ja kehyksiä yksityisten lohkoketjujen kehittämiseen ja käyttöönottoon. Hyperledgerillä on myös erilaisia projekteja, jotka tarjoavat lohkoketjuratkaisuja eri alojen tarpeisiin.

4.2.3. Hyperledger-pohjaisten sovellusten esimerkkejä

Hyperledger on avoimen lähdekoodin lohkoketjuteknologia, joka on tarkoitettu yritysten käyttöön. Hyperledger-projektin tavoitteena on kehittää lohkoketjuratkaisuja, joita yritykset voivat käyttää liiketoiminnan tarpeisiinsa. Projektissa on mukana useita yrityksiä, kuten IBM, Intel, Accenture ja SAP.

Hyperledgerin rakenne eroaa jossain määrin julkisista lohkoketjuista, kuten Bitcoinista ja Ethereumista. Hyperledgerin lohkoketju on yksityinen, mikä tarkoittaa sitä, että vain tietyt henkilöt tai organisaatiot voivat käyttää sitä. Lohkoketjussa on myös mahdollista määrittää erilaisia käyttöoikeuksia eri käyttäjille.

Yksityisellä lohkoketjulla on useita etuja verrattuna julkisiin

lohkoketjuihin. Yritykset voivat käyttää yksityistä lohkoketjuaan liiketoiminnan tarpeisiin ilman, että kaikki transaktiot ovat julkisia. Tämä on erityisen tärkeää yrityksille, jotka käsittelevät arkaluonteista tietoa.

Toisaalta yksityiset lohkoketjut voivat aiheuttaa haasteita. Yksi haaste on lohkoketjun käyttöönotto. Yksityisten lohkoketjujen käyttöönotto vaatii enemmän resursseja kuin julkisten lohkoketjujen, koska niiden käyttöönotto vaatii yleensä lisäkonfigurointia ja turvatoimia.

Hyperledger-pohjaisia sovelluksia on kehitetty monille eri aloille. Esimerkiksi IBM on kehittänyt Hyperledger Fabric -alustaa käyttäen ratkaisuja logistiikkaketjun hallintaan. Lisäksi Everledger on käyttänyt Hyperledgerin teknologiaa verifioinnin varmistamiseksi timanttien ja muiden kalleuksien toimitusketjussa. Hyperledger-säätiö julkaisee myös säännöllisesti uusia alustoja ja työkaluja lohkoketjujen kehittämiseksi.

4.3. IPFS ja hajautettu tiedostojärjestelmä

IPFS (InterPlanetary File System) on hajautettu tiedostojärjestelmä, joka käyttää lohkoketjuteknologiaa tiedostojen tallentamiseen ja jakamiseen vertaisverkossa. Sen avulla käyttäjät voivat tallentaa ja jakaa tiedostoja hajautetusti, ilman keskitettyä palvelinta. IPFS käyttää ainutlaatuista tapaa tunnistaa tiedostoja niiden sisällön perusteella, käyttäen sitä sijaan perinteistä URL-osoitetta, mikä mahdollistaa hajautetun tallennuksen ja helpomman sisällön jakamisen.

IPFS on suosittu hajautettujen sovellusten kehittäjien keskuudessa, ja sitä käytetään usein Ethereum-lohkoketjun

kanssa hajautettujen sovellusten kehittämisessä.

4.3.1. IPFS:n toiminta ja rakenne

InterPlanetary File System (IPFS) on hajautettu tiedostojärjestelmä, joka perustuu lohkoketjuteknologiaan. IPFS:n tavoitteena on muuttaa internetin tiedonhallintaa korvaamalla nykyinen keskitetty verkkotopologia hajautetulla ja avoimella verkolla. IPFS:n toiminta perustuu sisällön osoittelemiseen sen sisällön hash-arvolla sen sijaan, että tiedostoja haettaisiin tiettyjen osoitteiden perusteella.

IPFS käyttää Content Addressed Storage (CAS) -järjestelmää tallentaessaan tiedostoja verkossa. Tiedoston sisällöstä lasketaan hash-arvo, joka toimii tiedoston ainutlaatuisena tunnisteena. Kun käyttäjä haluaa ladata tiedoston IPFS-verkosta, hän käyttää hash-arvoa sen löytämiseksi. Tämä mahdollistaa tiedostojen tallentamisen hajautettuun verkkoon ja niiden nopean jakelun ilman, että tiedoston fyysistä sijaintia tarvitsee tietää.

IPFS:n rakenne koostuu kolmesta eri kerroksesta: verkko-, jakelu- ja protokollakerroksesta. Verkkokerros on vastuussa tiedon jakelusta eri IPFS-verkon solmujen välillä. Jakelukerros vastaa tiedon tallentamisesta ja hausta verkon solmuista. Protokollakerros mahdollistaa eri sovellusten integraation IPFS:n kanssa.

IPFS:n avulla voidaan toteuttaa hajautettuja sovelluksia, joissa tiedot jaetaan kaikkien käyttäjien kesken ilman, että keskitetty palvelin toimii välikätenä. Tämä mahdollistaa tiedon tallentamisen ja jakamisen turvallisesti ja tehokkaasti. IPFS-pohjaisia sovelluksia ovat esimerkiksi hajautetut tiedostojen

jakopalvelut, hajautetut verkkosivustot ja hajautetut tietokannat.

4.3.2. Hajautetun tiedostojärjestelmän käyttö lohkoketjuissa

Hajautettua tiedostojärjestelmää (IPFS) voidaan käyttää lohkoketjujen kanssa monin eri tavoin. IPFS:llä on lohkoketjujen kanssa yhteisiä piirteitä, kuten hajautettu rakenne ja turvallisuusominaisuudet, jotka mahdollistavat sen käytön lohkoketjujen kanssa.

IPFS:n käyttö lohkoketjujen kanssa mahdollistaa tiedon tallentamisen hajautettuun järjestelmään, jolloin se on helposti saatavilla kaikille verkoston käyttäjille. Tämä mahdollistaa tiedon jakamisen ja käytön monipuolisesti eri sovelluksissa. Lisäksi IPFS mahdollistaa tiedon eheyden tarkistamisen ja turvallisuuden varmistamisen lohkoketjuun tallennetun tiedon kohdalla.

Lisäksi IPFS:n avulla voidaan toteuttaa hajautettuja sovelluksia, joissa käyttäjien tietokoneista muodostuu hajautettu verkkoympäristö. Tämä mahdollistaa sovellusten toiminnan myös ilman keskitettyä palvelinta, mikä parantaa sovellusten turvallisuutta ja käytettävyyttä.

Esimerkkejä IPFS:n käytöstä lohkoketjujen kanssa ovat muun muassa tiedostojen tallennus- ja jakamispalvelut, hajautetut sovellukset ja hajautetut verkkoympäristöt.

4.3.3. IPFS-pohjaisten sovellusten esimerkkejä

IPFS-pohjaiset sovellukset käyttävät hajautettua tiedostojärjestelmää (IPFS) hyödyntäen hajautettua tallennusjärjestelmää, joka perustuu lohkoketjuteknologiaan. Tämä mahdollistaa tiedostojen tallentamisen ja jakamisen hajautetussa ympäristössä ilman keskitettyä palvelinta. Tässä joitakin esimerkkejä IPFS-pohjaisista sovelluksista:

1. Peergos: Peergos on pilvipalvelu, joka käyttää IPFS:tä tiedostojen tallentamiseen ja salaukseen. Sovelluksen avulla käyttäjät voivat jakaa ja tallentaa tiedostoja turvallisesti ja hajautetusti.
2. Textile: Textile on hajautettu tiedonhallintapalvelu, joka käyttää IPFS:tä tiedostojen tallentamiseen ja jakamiseen. Textilen avulla kehittäjät voivat rakentaa hajautettuja sovelluksia, jotka toimivat IPFS:n päällä.
3. OpenBazaar: OpenBazaar on hajautettu kauppapaikka, joka käyttää IPFS:tä tiedostojen jakamiseen ja tallentamiseen. Sovelluksen avulla käyttäjät voivat ostaa ja myydä tavaroita ilman keskitettyä välittäjää.
4. Temporal: Temporal on hajautettu tietokantapalvelu, joka käyttää IPFS:tä tiedostojen tallentamiseen ja jakamiseen. Temporalin avulla kehittäjät voivat rakentaa hajautettuja sovelluksia, jotka käyttävät IPFS:ää tietojen tallentamiseen.
5. Filecoin: Filecoin on hajautettu tiedostojärjestelmä, joka käyttää IPFS:tä tiedostojen tallentamiseen ja jakamiseen. Filecoinin avulla käyttäjät voivat ostaa ja myydä tallennustilaa IPFS-verkossa.

4.4. BigchainDB ja lohkoketjuun pohjautuva tietokanta

BigchainDB on lohkoketjuun pohjautuva hajautettu tietokanta, joka yhdistää lohkoketjujen hajauttamisen, kryptografian ja perinteisten tietokantojen skaalautuvuuden ja nopeuden. BigchainDB:n avulla käyttäjät voivat tallentaa, hallita ja jakaa digitaalisia omaisuuksia turvallisesti ja hajautetusti.

BigchainDB:n avulla käyttäjät voivat helposti luoda omia yksityisiä tai julkisia lohkoketjuja ja tallentaa monenlaisia tietoja, kuten äänestyksiä, älysopimuksia, kuvia ja äänitiedostoja. BigchainDB:llä on myös mahdollista suorittaa monimutkaisia kyselyitä lohkoketjuun tallennettujen tietojen suhteen, mikä helpottaa sovellusten kehittämistä ja käyttöä.

BigchainDB:llä on useita käyttötapauksia eri aloilta, kuten taide, logistiikka, äänestys ja teollisuus. Esimerkiksi taidealalla BigchainDB:tä voidaan käyttää todentamaan ja hallinnoimaan digitaalisia taideomaisuuksia. Logistiikassa taas BigchainDB:tä voidaan käyttää kuljetusten seurantaan ja varmistamaan tuotteiden aitous.

4.4.1. BigchainDB:n toiminta ja rakenne

BigchainDB on avoimen lähdekoodin hajautettu tietokanta, joka käyttää lohkoketjua tietojen tallentamiseen ja käsittelyyn. BigchainDB:n toiminta perustuu hajautetun tietokannan käsitteeseen, jossa tietokanta tallennetaan useisiin tietokoneisiin tai solmuihin, jotka ovat yhteydessä toisiinsa. Tietokannan sisältö on jokaisella solmulla sama ja kaikki solmut voivat tehdä kyselyitä tietokantaan.

BigchainDB:n rakenne koostuu kahdesta osasta: Bigchain-kerroksesta ja Tendermint-kerroksesta. Bigchain-kerros käyttää lohkoketjua tietojen tallentamiseen ja käsittelyyn, kun taas Tendermint-kerros käsittelee konsensusta ja turvallisuutta. BigchainDB:n lohkoketju sisältää tietokannan lohkot, jotka ovat transaktioita, jotka on tallennettu tietokantaan. Jokaisen lohkon sisältöä suojaa SHA-3-algoritmi, joka varmistaa, että tietojen eheys säilyy.

BigchainDB:n hajautetun tietokannan rakenne mahdollistaa sen, että tietokannan sisältö on turvattu ja immuuni tietoturvaongelmille, kuten tietojen väärentämiselle ja tietokantahyökkäyksille. Lisäksi BigchainDB:n avoimen lähdekoodin luonne mahdollistaa sen, että kuka tahansa voi käyttää sitä ilmaiseksi ja kehittää uusia sovelluksia sen päälle.

BigchainDB:llä on monia käyttötapauksia, mukaan lukien äänestyssovellukset, älysopimukset, identiteetinhallinta ja varojen seuranta. Se tarjoaa myös käyttäjilleen kevyen ja nopean tavan tallentaa tietoja ja käsitellä niitä. BigchainDB:n käyttö on yleistynyt viime vuosina ja sillä on potentiaalia muuttaa tapaa, jolla tietokantoja käytetään ja ylläpidetään.

4.4.2. Lohkoketjuun pohjautuvien tietokantojen edut ja haasteet

Lohkoketjuun pohjautuvat tietokannat, kuten BigchainDB, tarjoavat useita etuja verrattuna perinteisiin tietokantoihin. Yksi merkittävä etu on hajautettu ja läpinäkyvä pääkirja, joka mahdollistaa tiedon jakamisen useiden käyttäjien kesken ilman keskitettyä välittäjää. Tämä vähentää yksittäisen tahon valtaa ja lisää luottamusta järjestelmään.

Toinen etu on tietoturva ja yksityisyys. Lohkoketjuun pohjautuvat tietokannat ovat suojattuja kryptografian avulla, mikä tekee niistä erittäin vaikeita manipuloida tai hakkeroitua. Lisäksi yksityisyys voidaan taata käyttämällä älysopimuksia, jotka mahdollistavat tietojen jakamisen vain tietyille käyttäjille.

Haasteita lohkoketjuun pohjautuvien tietokantojen käytössä on kuitenkin myös olemassa. Yksi haaste on skaalautuvuus. Koska lohkoketjun kaikkien lohkojen tulee olla synkronoituja kaikkien käyttäjien välillä, suuri määrä käyttäjiä voi hidastaa järjestelmää. Lisäksi lohkoketjuun tallennettujen tietojen määrä kasvaa nopeasti, mikä voi aiheuttaa ongelmia tietokannan suorituskyvyssä ja tallennuskapasiteetissa.

Toinen haaste on käyttöönotto. Lohkoketjuun pohjautuvien tietokantojen käyttö vaatii uudenlaista ajattelutapaa ja osaamista, joten sen käyttöönotto voi olla haastavaa. Lisäksi lohkoketjuun pohjautuvien sovellusten kehittäminen ja ylläpito voi olla kallista ja aikaa vievää.

Kaiken kaikkiaan lohkoketjuun pohjautuvat tietokannat tarjoavat useita etuja perinteisiin tietokantoihin verrattuna, mutta niiden käyttö vaatii huolellista harkintaa ja valmistautumista.

4.4.3. BigchainDB-pohjaisten sovellusten esimerkkejä

BigchainDB on yksi lohkoketjuun pohjautuvista hajautetuista tietokannoista, jotka tarjoavat lohkoketjuteknologian edut perinteisessä tietokantaratkaisussa. BigchainDB:n erityispiirre on sen kyky tallentaa suuria määriä tietoa tehokkaasti ja nopeasti. BigchainDB käyttää moniprosessointitekniikkaa, joka mahdollistaa useiden tietokantatoimintojen suorittamisen samanaikaisesti, mikä tekee siitä nopean ja skaalautuvan

ratkaisun.

BigchainDB:n tärkeimmät edut ovat sen hajautetun luonteen ansiosta korkea tietoturva, läpinäkyvyys, nopeus ja tehokkuus. Se tarjoaa myös älysopimustoiminnallisuuksia, joiden avulla käyttäjät voivat luoda monimutkaisia sopimuksia, joissa voidaan käyttää erilaisia logiikka- ja ehto-ominaisuuksia.

BigchainDB-pohjaisia sovelluksia on kehitetty monilla eri aloilla. Esimerkiksi Ocean Protocol on BigchainDB-pohjainen hajautettu markkinapaikka, joka yhdistää datan tuottajat ja käyttäjät. Toinen esimerkki on Ascribe, joka käyttää BigchainDB:tä mahdollistaakseen taiteen digitaalisen omistuksen ja jakelun.

5. Suunnittelu ja toteutus: Lohkoketjuja tietokantana käyttävän sovelluksen rakentaminen

Viidennessä osiossa käsitellään lohkoketjuja tietokantana käyttävän sovelluksen suunnittelua ja toteutusta. Osiossa käydään läpi, mitä tulee ottaa huomioon sovelluksen suunnittelussa, kun lohkoketjua käytetään tietokantana, ja miten sovelluksen toteutus eroaa perinteisten sovellusten toteutuksesta. Osiossa käsitellään myös, miten sovellus voidaan integroida eri lohkoketjuteknologioihin ja millaisia haasteita voi tulla vastaan sovelluksen kehityksessä. Lopuksi annetaan esimerkkejä lohkoketjutietokantojen käytöstä sovelluksissa, kuten äänestyssovelluksissa, identiteetinhallintasovelluksissa ja hajautetun rahoituksen sovelluksissa.

5.1. Vaatimusmäärittely ja arkkitehtuuri

Vaatimusmäärittely ja arkkitehtuurin suunnittelu ovat tärkeitä vaiheita lohkoketjuteknologiaa hyödyntävän sovelluksen kehityksessä. Vaatimusmäärittelyssä kartoitetaan sovelluksen tarpeet ja tavoitteet, jotta varmistetaan sen toimivuus ja käyttöönoton onnistuminen. Arkkitehtuurin suunnittelussa puolestaan määritellään sovelluksen tekninen rakenne ja komponentit, kuten lohkoketjun käyttö, tietokannan suunnittelu ja käyttöliittymän toteutus.

Sovelluksen suunnittelun tulee ottaa huomioon lohkoketjun ominaispiirteet, kuten hajautettu ja läpinäkyvä tietokanta. Lisäksi on tärkeää määritellä, mitä tietoja tallennetaan lohkoketjuun ja miten niitä käsitellään. Arkkitehtuurin suunnittelussa on myös otettava huomioon sovelluksen skaalautuvuus ja tietoturva.

5.1.1. Sovelluksen vaatimusten määrittely

Sovelluksen vaatimusten määrittely on tärkeä vaihe lohkoketjuteknologiaa hyödyntävän sovelluksen kehittämisessä. Tämä vaihe käsittää sovelluksen tarkoituksen ja toiminnallisuuden selvittämisen, käyttöliittymän suunnittelun, tietokantarakenteen suunnittelun, tarvittavien resurssien määrittelyn ja projektin aikataulun suunnittelun.

Vaatimusten määrittelyssä on tärkeää ottaa huomioon käyttäjien tarpeet ja toiveet, jotta sovelluksesta tulee käyttäjäystävällinen ja toimiva. Tässä vaiheessa voidaan myös määritellä sovelluksen käyttötarkoitukseen liittyvät vaatimukset, kuten turvallisuusvaatimukset ja skaalautuvuusvaatimukset.

Hyvä vaatimusten määrittely auttaa kehitystiimiä

ymmärtämään paremmin sovelluksen tarkoitusta ja toiminnallisuutta, mikä puolestaan auttaa suunnittelemaan ja kehittämään parempia ratkaisuja. Tästä syystä vaatimusten määrittelyyn kannattaa panostaa riittävästi aikaa ja resursseja.

Vaatimusten määrittelyn jälkeen voidaan siirtyä sovellusarkkitehtuurin suunnitteluun, joka käsitellään seuraavassa kohdassa.

5.1.2. Sovellusarkkitehtuurin suunnittelu

Sovellusarkkitehtuurin suunnittelu on tärkeä osa lohkoketjusovelluksen kehitysprosessia. Arkkitehtuurin suunnittelun avulla varmistetaan, että sovellus vastaa vaatimuksia ja on skaalautuva, suorituskykyinen ja turvallinen.

Sovellusarkkitehtuurin suunnittelu alkaa yleensä vaatimusmäärittelyistä, joissa määritellään sovelluksen käyttötapaukset ja liiketoimintavaatimukset. Sen jälkeen arkkitehti suunnittelee sovelluksen eri osien toiminnallisuudet ja niiden väliset riippuvuudet.

Yksi tärkeimmistä päätöksistä arkkitehtuurin suunnittelussa on lohkoketjun valinta. Tämä vaikuttaa suuresti sovelluksen suorituskykyyn, skaalautuvuuteen ja tietoturvaan. Lohkoketjun valinnassa on otettava huomioon myös sovelluksen käyttötapaukset ja vaatimukset.

Sovellusarkkitehdin on myös päätettävä, miten sovellus liittyy muihin järjestelmiin ja tietolähteisiin. Tämä voi sisältää esimerkiksi rajapintojen suunnittelun muiden lohkoketjujen kanssa kommunikointiin tai perinteisiin tietokantoihin integroitumisen.

Lopuksi, arkkitehti suunnittelee sovelluksen tietoturva- ja käyttöoikeusmekanismit. Tämä sisältää esimerkiksi roolien ja oikeuksien hallinnan, käyttäjien tunnistamisen ja varmennuksen, sekä lohkoketjun turvallisuusmekanismit.

Sovellusarkkitehtuurin suunnittelu on jatkuvaa prosessia, joka vaatii tiivistä yhteistyötä kehittäjien, käyttäjien ja muiden sidosryhmien kanssa. Arkkitehtuurin suunnittelun onnistuminen edellyttää myös jatkuvaa arviointia ja tarvittaessa muutosten tekemistä sovelluksen elinkaaren aikana.

5.2. Tietokanta- ja lohkoketjuratkaisun valinta

Kun lohkoketjua käytetään tietokantana, on tärkeää valita sopiva tietokanta- ja lohkoketjuratkaisu sovelluksen tarpeiden mukaan. Tietokantaratkaisun valintaan vaikuttavat monet tekijät, kuten tietokannan skaalautuvuus, suorituskyky, tietoturva ja yksityisyysominaisuudet.

Lohkoketjuratkaisuja on useita erilaisia, ja niiden valintaan vaikuttavat esimerkiksi sovelluksen tavoitteet, käyttäjämäärä ja käyttötapaukset. Joitakin suosittuja lohkoketjuratkaisuja ovat esimerkiksi Ethereum, Hyperledger Fabric ja Corda.

Lisäksi on tärkeää ottaa huomioon lohkoketjun ja perinteisen tietokannan integraation haasteet ja mahdollisuudet, ja valita sopivat työkalut ja tekniikat tämän toteuttamiseksi. Hyvä suunnittelu ja toteutus ovat avainasemassa onnistuneen lohkoketjua tietokantana käyttävän sovelluksen rakentamisessa.

5.2.1. Tietokantaratkaisun valinta

Tietokannan valinta on tärkeä vaihe sovelluksen kehityksessä, sillä se vaikuttaa suoraan sovelluksen tehokkuuteen, skaalautuvuuteen ja turvallisuuteen. Lohkoketjuteknologia tarjoaa uudenlaisen vaihtoehdon perinteisille tietokannoille, mutta sen käyttöönotto vaatii erilaista ajattelua ja suunnittelua.

Lohkoketjuteknologiaa käyttävät tietokannat ovat hajautettuja ja kaikille käyttäjille avoimia. Tämä tarkoittaa sitä, että jokainen tietokannan käyttäjä voi tarkastella kaikkia tallennettuja tietoja. Tämä avoimuus lisää tietoturvan ja yksityisyyden haasteita, sillä kaikkien käyttäjien on voitava luottaa tietokannan sisältöön ja sen eheyteen.

Lohkoketjut tarjoavat myös etuja perinteisiin tietokantoihin verrattuna. Hajautetun pääkirjan ansiosta lohkoketjut ovat läpinäkyviä ja luotettavia, ja niiden käyttö mahdollistaa uusia sovelluskohteita. Lohkoketjut ovat myös hyvin skaalautuvia, sillä uusia tietoja voidaan lisätä lohkoihin samanaikaisesti useiden käyttäjien toimesta.

Perinteisissä tietokannoissa tietojen tallentaminen ja luku tapahtuvat yleensä keskitetysti, jolloin tietokantaan pääsy vaatii yleensä käyttäjätunnuksen ja salasanan. Lohkoketjuteknologia tarjoaa hajautetun pääkirjan ansiosta hajautetun tietokannan, johon pääsy ei vaadi keskitettyä kirjautumista. Tämä tekee lohkoketjuteknologiasta houkuttelevan vaihtoehdon esimerkiksi avoimien tietojen jakamiseen ja yhteistyöhön perustuvien sovellusten kehittämiseen.

Tietokannan valintaan vaikuttaa myös sovelluksen käyttötarkoitus. Esimerkiksi jos sovellus käsittelee arkaluontoisia tietoja, kuten terveystietoja tai henkilötietoja,

lohkoketju ei välttämättä ole paras ratkaisu. Sen sijaan yksityinen tietokanta tai perinteinen keskitetty tietokanta voi olla turvallisempi vaihtoehto.

Ennen tietokannan valintaa on siis tärkeää harkita huolellisesti sovelluksen käyttötarkoitusta, tietoturvavaatimuksia sekä muita tarpeita ja rajoitteita.

5.2.2. Lohkoketjuratkaisun valinta

Kun lohkoketjuteknologiaa käytetään sovelluksen kehittämisessä, on tärkeää valita oikea lohkoketjuratkaisu. Lohkoketjuratkaisua valittaessa on huomioitava sovelluksen vaatimukset ja tarkoitus, sillä eri lohkoketjuratkaisuilla on erilaisia ominaisuuksia ja käyttötapoja.

Yleisesti ottaen on kaksi päätyyppiä lohkoketjuratkaisuja: julkiset ja yksityiset lohkoketjut. Julkisissa lohkoketjuissa kaikki käyttäjät voivat osallistua lohkoketjun toimintaan ja lisätä siihen uusia tietoja. Yksityisissä lohkoketjuissa taas vain tietyt käyttäjät voivat osallistua lohkoketjun toimintaan ja nähdä sen sisällön.

Julkisista lohkoketjuratkaisuista tunnetuimpia ovat Bitcoin ja Ethereum, kun taas yksityisistä lohkoketjuratkaisuista esimerkiksi Hyperledger Fabric. Julkiset lohkoketjuratkaisut ovat yleensä hajautettuja ja avoimia, kun taas yksityiset lohkoketjuratkaisut voivat olla joko hajautettuja tai keskitettyjä.

Lisäksi lohkoketjuratkaisua valitessa on otettava huomioon lohkoketjun konsensusmekanismi, joka määrittää, miten lohkoketjun tietojen oikeellisuus varmistetaan. Esimerkkejä konsensusmekanismeista ovat Proof of Work ja Proof of Stake.

Kun sovellukseen valitaan lohkoketjuratkaisu, on myös tärkeää huomioida ratkaisun skaalautuvuus, turvallisuus ja käytettävyys. Ratkaisun skaalautuvuus määrittää, kuinka paljon tietoa lohkoketjuun voidaan tallentaa ja kuinka nopeasti se toimii. Turvallisuus taas tarkoittaa sitä, kuinka hyvin lohkoketjuratkaisu suojaa tietoja väärinkäytöksiltä ja hakkeroinnilta. Käytettävyys puolestaan kuvaa sitä, kuinka helppoa ja käyttäjäystävällistä lohkoketjuratkaisun käyttö on.

Kokonaisuudessaan lohkoketjuratkaisun valinnassa on siis tärkeää huomioida useita eri tekijöitä, jotta sovellus saadaan kehitettyä toimivaksi ja tarkoituksenmukaiseksi.

5.3. Älysopimusten suunnittelu ja toteutus

Älysopimukset ovat keskeinen osa lohkoketjuteknologiaa, ja ne ovat välttämättömiä monien lohkoketjusovellusten toteuttamisessa. Älysopimukset ovat käytännössä ohjelmakoodia, joka suoritetaan lohkoketjussa ja joka määrittää, miten tietoa käsitellään ja mitä toimintoja suoritetaan. Älysopimukset voivat esimerkiksi hallita kryptovaluutan siirtoja, tietojen tallennusta tai sopimuksien täytäntöönpanoa.

Älysopimuksen suunnittelussa on tärkeää huomioida tarkasti sovelluksen vaatimukset ja toiminnallisuudet, jotta sopimus voidaan määrittää oikein. Suunnitteluprosessiin kuuluu yleensä sopimuksen arkkitehtuurin suunnittelu, sopimuksen logiikan määrittäminen ja sen varmistaminen, että sopimus noudattaa lohkoketjun käyttöehdot ja turvallisuusstandardit.

Älysopimuksen toteutus voi tapahtua monella eri ohjelmointikielellä, kuten Solidityllä, C++:lla tai Go:lla.

Älysopimusten toteutuksessa on tärkeää noudattaa hyviä käytäntöjä ja varmistaa, että sopimus on riittävän testattu ja auditoidu.

5.3.1. Älysopimusten suunnittelun perusteet

Älysopimusten suunnittelu on tärkeä vaihe lohkoketjupohjaisen sovelluksen kehityksessä. Älysopimus on tietokoneohjelma, joka on tallennettu lohkoketjuun ja joka määrittelee ehdot ja toiminnallisuuden automaattiselle sopimukselle. Älysopimukset mahdollistavat monia sovelluksia, kuten automaattiset maksut ja digitaalisten omaisuuserien jakamisen.

Älysopimuksen suunnittelu alkaa usein liiketoiminnan vaatimusten määrittämisestä. Tässä vaiheessa on tärkeää määrittää selkeästi, mitä toimintoja älysopimuksen tulee suorittaa, mitkä ovat sen sisään- ja ulostulot, sekä millaisia ehtoja sen tulee täyttää. Vaatimusten määrittelyn jälkeen on tärkeää harkita, millaisia lohkoketjuratkaisuja ja lohkoketjuja käytetään älysopimuksen toteuttamiseen.

Seuraavaksi on tärkeää määrittää älysopimuksen rakenne ja toiminta. Tässä vaiheessa suunnitellaan älysopimuksen arkkitehtuuri ja sen toimintaperiaatteet. Suunnittelussa on tärkeää ottaa huomioon älysopimuksen turvallisuus, sillä älysopimuksen toimimattomuus tai haavoittuvuus voi johtaa vakaviin ongelmiin.

Lopuksi on tärkeää testata älysopimus ennen sen julkaisemista lohkoketjuun. Testaamisessa varmistetaan, että älysopimus toimii oikein ja täyttää liiketoiminnan vaatimukset. Testauksessa käytetään usein erilaisia testaustyökaluja ja

simulaattoreita.

Kokonaisuutena älysopimuksen suunnittelu on tärkeä osa lohkoketjupohjaisen sovelluksen kehitystä. Älysopimuksen suunnittelu vaatii huolellista harkintaa ja ymmärrystä lohkoketjuteknologiasta sekä liiketoiminnan tarpeista. On tärkeää huolehtia, että älysopimus on turvallinen ja täyttää liiketoiminnan vaatimukset.

5.3.2. Älysopimusten toteutus

Älysopimukset ovat tärkeä osa monia lohkoketjupohjaisia sovelluksia. Älysopimukset ovat itseohjautuvia ohjelmia, jotka toimivat automaattisesti lohkoketjussa tallennettujen ehtojen ja sääntöjen mukaisesti. Älysopimukset perustuvat usein Turing-täydellisiin ohjelmointikieliin, kuten Solidityyn Ethereum-lohkoketjussa.

Älysopimuksen suunnittelu alkaa vaatimusten kartoittamisesta, jotta voidaan määritellä, mitä sopimuksen tulisi tehdä ja mitkä ovat sen toimintaehdot. Tämän jälkeen tulee valita käytettävä ohjelmointikieli ja määritellä sopimuksen lohkoketjussa tarvitsemat rajapinnat ja parametrit.

Älysopimuksen toteutus vaatii ohjelmointitaitoja ja ymmärrystä lohkoketjuteknologiasta. Älysopimus tulee testata huolellisesti ennen sen käyttöönottoa, jotta voidaan varmistaa sen toimivuus ja turvallisuus.

Älysopimukset mahdollistavat monia uusia sovelluskohteita lohkoketjuteknologiassa, kuten hajautetut rahoitussovellukset (DeFi) ja hajautetut organisaatiot (DAO). Älysopimuksia voidaan myös käyttää esimerkiksi logistiikkaketjujen hallinnassa ja henkilökohtaisten tietojen hallinnassa.

5.4. Front-end ja back-end integraatio

Lohkoketjuihin perustuvien sovellusten rakentamisessa on tärkeää integroida front-end ja back-end sujuvasti yhteen. Front-end tarkoittaa sovelluksen käyttöliittymää, joka on käyttäjän näkyvä osa, kun taas back-end vastaa sovelluksen taustaprosesseista, kuten tietokannan hallinnasta ja älysopimusten toteutuksesta.

Sovelluksen front-endin ja back-endin integrointiin liittyy useita tekijöitä, kuten tietojen siirto lohkoketjun ja tietokannan välillä, älysopimusten käyttöliittymän toteutus ja käyttäjän tunnistaminen lohkoketjun avulla. On myös tärkeää varmistaa, että sovellus on turvallinen ja suojattu mahdollisia hyökkäyksiä vastaan.

Integrointi voidaan toteuttaa esimerkiksi käyttämällä sovellusrajapintoja (API), joiden avulla front-end voi kommunikoida back-endin kanssa. Tämä mahdollistaa tietojen siirron ja käsittelyn lohkoketjun ja tietokannan välillä. Myös älysopimusten käyttöliittymä voidaan toteuttaa API:n avulla.

Integroinnin suunnittelussa on tärkeää ottaa huomioon käyttäjäkokemus ja varmistaa, että sovellus on helppokäyttöinen ja toimii saumattomasti eri käyttöliittymissä ja laitteissa.

5.4.1. Front-end ja back-end järjestelmien integrointi

Front-end ja back-end ovat kaksi keskeistä osaa monissa

ohjelmistoissa ja sovelluksissa. Front-end on käyttöliittymä, jonka kautta käyttäjä voi kommunikoida sovelluksen kanssa, kun taas back-end on sovelluksen "takana" oleva järjestelmä, joka käsittelee käyttäjän syötteitä, käsittelee tietoja ja tuottaa vastauksia.

Front-end ja back-end tulee integroida yhteen, jotta sovellus toimii sujuvasti. Integroinnin avulla front-end ja back-end kommunikoivat keskenään, jolloin sovellus toimii kokonaisuutena. Lohkoketjusovelluksissa front-end ja back-end järjestelmien integrointi on erityisen tärkeää, sillä sovellus koostuu useista eri osista, kuten käyttöliittymästä, älysopimuksista ja lohkoketjun hallinnasta.

Front-endin ja back-endin integroinnissa on tärkeää varmistaa, että sovellus toimii sujuvasti ja että kaikki osat toimivat yhdessä saumattomasti. Integroinnin yhteydessä tulee myös huomioida tietoturva, sillä lohkoketjusovelluksissa käsitellään usein arkaluonteisia tietoja ja varoja.

Integroinnin toteuttamisessa on käytettävissä erilaisia tekniikoita ja työkaluja, kuten REST-rajapintoja ja WebSockets-protokollia. Lopullinen ratkaisu riippuu sovelluksen vaatimuksista ja teknisistä vaatimuksista. On tärkeää valita oikeat työkalut ja tekniikat, jotka sopivat parhaiten sovelluksen tarpeisiin ja tavoitteisiin.

5.4.2. Sovelluksen testaus ja käyttöönotto

Sovelluksen testaus ja käyttöönotto ovat tärkeitä vaiheita ohjelmistoprojektin elinkaarella, ja ne vaativat huolellista suunnittelua ja toteutusta. Testauksella varmistetaan, että sovellus toimii tarkoituksenmukaisesti ja virheettömästi eri

käyttötilanteissa ja ympäristöissä. Käyttöönotto puolestaan tarkoittaa sovelluksen siirtämistä tuotantoympäristöön ja sen käyttöönottoa loppukäyttäjille.

Sovelluksen testauksen tarkoituksena on varmistaa, että sovellus toimii odotetulla tavalla kaikissa käyttötilanteissa ja että sen käyttö on sujuvaa ja helppoa. Testauksen avulla pyritään löytämään mahdolliset virheet ja puutteet, jotka voivat vaikuttaa sovelluksen käytettävyyteen, toimivuuteen ja tietoturvaan. Testausprosessiin kuuluu eri testivaiheita, kuten yksikkötestaus, integraatiotestaus, järjestelmätestaus ja hyväksyntätestaus.

Sovelluksen käyttöönotto vaatii huolellista suunnittelua ja testausta ennen tuotantokäyttöönottoa. Käyttöönottoon liittyy usein riski sovelluksen käyttökatkoksista ja ongelmista, jotka voivat vaikuttaa liiketoimintaan ja asiakastyytyväisyyteen. Käyttöönoton suunnittelussa tulee huomioida tarvittavat resurssit, kuten riittävä laitteisto, tietoliikenneyhteydet ja turvallisuus, sekä käyttöönottoon liittyvät prosessit, kuten tietojen siirto ja testaus.

Sovelluksen testaus ja käyttöönotto ovat osa ohjelmistoprojektin elinkaaren loppuvaihetta. On tärkeää huolehtia siitä, että sovelluksen testaus ja käyttöönotto toteutetaan huolellisesti ja suunnitellusti, jotta sovelluksen käyttöönotto onnistuu ja sovellus toimii tarkoituksenmukaisesti ja virheettömästi.

6. Lohkoketjujen tulevaisuus tietokantateknologiana

Osiossa 6 käsitellään lohkoketjuteknologian tulevaisuutta tietokantateknologiana. Tarkastellaan, mihin suuntaan

lohkoketjuteknologia kehittyy tulevaisuudessa ja millaisia vaikutuksia sillä voi olla eri aloilla. Lisäksi käydään läpi tärkeitä kehityssuuntia, kuten lohkoketjujen skaalautuvuuden parantamista, yksityisyydensuojan parantamista sekä älysopimusten käytön laajentamista eri sovellusalueilla. Osiossa tarkastellaan myös lohkoketjuteknologian käyttöönoton haasteita ja mahdollisuuksia sekä sen roolia tulevaisuuden tietokantaratkaisuissa.

6.1. Nykyiset haasteet ja rajoitukset

Nykyiset lohkoketjuteknologian haasteet ja rajoitukset liittyvät usein skaalautuvuuteen, tietoturvaan ja yksityisyyteen. Lohkoketjut ovat edelleen suhteellisen hidas tapa käsitellä tietoa verrattuna perinteisiin tietokantoihin, ja niiden skaalautuvuus on rajoitettu. Tietoturva ja yksityisyys ovat myös edelleen merkittäviä haasteita, ja vaativat jatkuvaa kehittämistä ja parantamista.

Toisaalta, lohkoketjuteknologian soveltaminen erilaisiin sovelluskohteisiin kasvaa jatkuvasti. Lohkoketjut mahdollistavat hajautetun ja läpinäkyvän järjestelmän, joka voi auttaa ratkaisemaan monia ongelmia eri aloilla, kuten finanssialalla, logistiikassa, terveydenhuollossa ja julkisessa sektorissa.

Lisäksi lohkoketjujen tulevaisuus tietokantateknologiana näyttää lupaavalta. Uudet kehityshankkeet, kuten Ethereum 2.0 ja Cardano, pyrkivät parantamaan lohkoketjuteknologian skaalautuvuutta ja tietoturvaa. Samalla lohkoketjuteknologian sovelluskohteet laajenevat jatkuvasti, ja uusia innovatiivisia sovelluksia kehitetään jatkuvasti.

Kaiken kaikkiaan lohkoketjuteknologian tulevaisuus tietokantateknologiana näyttää erittäin lupaavalta, ja sen

odotetaan muuttavan tapaa, jolla tietoa tallennetaan, käsitellään ja jaetaan tulevaisuudessa.

6.1.1. Lohkoketjujen skaalautuvuus

Lohkoketjuteknologian skaalautuvuus on ollut yksi sen suurimmista haasteista sen kehityksen alkuvaiheista asti. Kun lohkoketjuteknologia alkoi saavuttaa suosiotaan, sen käyttökohteet kasvoivat nopeasti ja sen tarvitsema laskentateho ja tallennustila kasvoivat eksponentiaalisesti. Tämä johti nopeasti lohkoketjujen skaalautuvuushaasteisiin.

Yksi suurimmista skaalautuvuushaasteista on lohkoketjujen kapasiteetin rajoitukset. Lohkoketjut voivat käsitellä vain tietyn määrän transaktioita sekunnissa, mikä rajoittaa niiden käyttöä suurissa kaupallisissa sovelluksissa. Bitcoinin lohkokoko on esimerkiksi rajoitettu yhteen megatavuun, mikä tarkoittaa, että verkko voi käsitellä vain noin seitsemän transaktiota sekunnissa.

Erilaisia ratkaisuja on esitetty lohkoketjujen skaalautuvuusongelman ratkaisemiseksi. Yksi tällainen ratkaisu on lohkoketjujen haarautuminen (forking), joka tarkoittaa lohkoketjun jakamista kahteen tai useampaan haarautumaan, joissa jokaisessa on oma versio lohkoketjusta. Tämä voi johtaa siihen, että lohkoketju jakautuu kahteen eri lohkoketjuun, joista toinen jatkaa alkuperäisen lohkoketjun kehitystä ja toinen haarautuu omaan suuntaansa.

Toinen ratkaisu on lohkoketjujen skaalautuvuuden parantaminen muuttamalla lohkoketjun arkkitehtuuria. Yksi tällainen ratkaisu on lohkoketjujen kerrostaminen (layering), joka tarkoittaa lohkoketjun jakamista useampaan kerrokseen,

joissa jokaisessa käsitellään tietyn tyyppisiä toimintoja. Tämä voi parantaa lohkoketjun skaalautuvuutta, koska jokainen kerros voi käsitellä omaa osa-aluettaan tehokkaammin.

Kolmas ratkaisu on lohkoketjujen skaalautuvuuden parantaminen käyttämällä erilaisia konsensusmekanismeja. Proof of Stake (PoS) -konsensusmekanismi on yksi tällainen mekanismi, joka korvaa Proof of Work (PoW) -mekanismin, joka on perinteisesti käytetty lohkoketjujen ylläpitämiseen. PoS-mekanismissa lohkoketjun käyttäjät voivat osallistua sen ylläpitoon tallettamalla omaisuuttaan lohkoketjuun. Näin lohkoketjujen ylläpitäjien tarvitsema laskentateho vähenee ja skaalautuvuus paranee.

Neljäs ratkaisu on lohkoketjujen skaalautuvuuden parantaminen käyttämällä sivuketjuja (sidechains) tai state channel -teknologiaa. Sivuketjut ovat erillisiä lohkoketjuja, jotka ovat sidoksissa päälohkoketjuun. Tämä mahdollistaa transaktioiden käsittelyn sivuketjuissa, mikä vähentää kuormitusta päälohkoketjussa. State channel -teknologia puolestaan mahdollistaa transaktioiden käsittelyn suoraan kahden osapuolen välillä, mikä vähentää transaktioiden määrää lohkoketjussa.

Lohkoketjujen skaalautuvuus on edelleen yksi alan suurimmista haasteista, ja ratkaisuja kehitetään jatkuvasti. Monet ratkaisut ovat vielä kokeiluasteella, ja tulevaisuudessa lohkoketjuteknologiaa käytetään todennäköisesti laajemmin, kun sen skaalautuvuus on parantunut ja se on saavuttanut vakaan aseman eri aloilla.

6.1.2. Ympäristövaikutukset

Lohkoketjuteknologian ympäristövaikutukset ovat herättäneet huolta, sillä monet lohkoketjut käyttävät Proof of Work (PoW) -konsensusmekanismia, joka vaatii suuria määriä laskentatehoa ja sähköenergiaa. Esimerkiksi Bitcoinin kaivaminen kuluttaa valtavan määrän energiaa, ja sen arvioidaan tuottavan enemmän hiilidioksidipäästöjä kuin monet pienet valtiot.

Lohkoketjuteknologian ympäristövaikutusten vähentämiseksi on etsitty erilaisia ratkaisuja. Yksi ratkaisu on siirtyä PoW-mekanismista PoS-mekanismiin, joka kuluttaa vähemmän energiaa. Toisaalta on myös kehitetty erilaisia energiatehokkaita laitteita, jotka mahdollistavat lohkoketjujen louhinnan pienemmällä energiankulutuksella.

Lisäksi on etsitty muita tapoja vähentää lohkoketjujen ympäristövaikutuksia. Esimerkiksi lohkoketjujen skaalautuvuuden parantaminen voi vähentää niiden ympäristövaikutuksia, sillä tehokkaammat lohkoketjut kuluttavat vähemmän energiaa transaktioiden käsittelyyn. Lisäksi on kehitetty uusia lohkoketjujen arkkitehtuureja, kuten sidechain-arkkitehtuuri, joka mahdollistaa lohkoketjujen välisen kommunikaation ja transaktioiden siirtämisen yhdestä lohkoketjusta toiseen, mikä voi vähentää lohkoketjujen tarvitsemaa energiaa.

On tärkeää, että lohkoketjuteknologian ympäristövaikutukset otetaan huomioon sen kehittämisessä ja käytössä. Lohkoketjuteknologian potentiaali on valtava, mutta sen ympäristövaikutukset eivät saa olla kestämättömiä. On tärkeää kehittää energiatehokkaita ratkaisuja, jotka mahdollistavat lohkoketjujen käytön kestävällä tavalla.

6.1.3. Käyttöönoton haasteet

Lohkoketjuteknologian käyttöönottoon liittyy useita haasteita, jotka voivat hidastaa sen leviämistä laajasti käytettyjen teknologioiden joukkoon. Yksi merkittävimmistä haasteista on lohkoketjujen skaalautuvuus, josta jo mainittiin edellisessä kohdassa. Jos lohkoketjuja halutaan käyttää laajamittaisesti kaupallisissa sovelluksissa, niiden skaalautuvuutta on parannettava huomattavasti.

Toinen käyttöönoton haaste liittyy tietoturvaan. Lohkoketjuja on pidetty perinteisiä tietokantoja turvallisempina, koska niiden hajautettu rakenne tekee niistä alttiimpia hyökkäyksille. Esimerkiksi 51% hyökkäyksessä hyökkääjä saa hallinnan yli 50%:sta lohkoketjun laskentatehosta, mikä mahdollistaa manipulaation. Tämä on kuitenkin vain yksi esimerkki mahdollisesta hyökkäystavasta, ja lohkoketjuihin liittyvät tietoturvariskit ovat edelleen huomattavia.

Kolmas käyttöönoton haaste on sovellusten käytettävyys ja käyttöliittymät. Vaikka lohkoketjuteknologia mahdollistaa uusia sovelluskohteita, sen käyttäminen voi olla vaikeaa ja monimutkaista käyttäjille. Erityisesti älysopimusten käyttöönotto ja ylläpito vaativat kehittäjiltä ja käyttäjiltä erityistä osaamista.

Neljäs käyttöönoton haaste liittyy lohkoketjuteknologian laajemman hyväksynnän puutteeseen. Vaikka lohkoketjuja on käytetty jo vuosia, niiden käyttöönotto suuremmassa mittakaavassa on vielä melko uutta. Tämä voi vaikuttaa investointipäätöksiin, joissa perinteisiä teknologioita pidetään usein vakaampina ja turvallisempina vaihtoehtoina.

Viides käyttöönoton haaste on lainsäädännön ja sääntelyn puute. Lohkoketjuteknologian käyttöön liittyy useita oikeudellisia ja sääntelyyn liittyviä kysymyksiä, kuten tietosuoja ja verotus. Näiden asioiden ratkaisemiseksi tarvitaan

laajaa yhteistyötä hallitusten, yritysten ja teknologian kehittäjien välillä.

Kaiken kaikkiaan lohkoketjuteknologian käyttöönottoon liittyy useita haasteita, mutta samalla se tarjoaa myös valtavia mahdollisuuksia uusien innovaatioiden kehittämiseen ja digitaalisten ratkaisujen luomiseen eri aloilla. Vaikka lohkoketjuteknologian kehitys on ollut nopeaa ja sen potentiaali on suuri, sen laajamittainen käyttöönotto vaatii edelleen merkittäviä ponnisteluja.

Sovelluskehittäjien on oltava tietoisia lohkoketjuteknologian ominaisuuksista ja haasteista, jotta he voivat suunnitella ja kehittää sovelluksia, jotka hyödyntävät teknologiaa parhaalla mahdollisella tavalla. Investoijien on puolestaan ymmärrettävä teknologian potentiaali ja sen rajoitukset, jotta he voivat tehdä perusteltuja päätöksiä sijoituksista.

Hallitusten ja sääntelyviranomaisten on myös oltava tietoisia lohkoketjuteknologian vaikutuksista ja sen käyttöönoton haasteista, jotta he voivat laatia tarvittavat lainsäädännöt ja säännöt, jotka tukevat teknologian turvallista ja tehokasta käyttöä.

Lohkoketjuteknologian käyttöönotto on edelleen kehityksen alkuvaiheessa, ja sen käyttö sovelluksissa ja kaupallisissa sovelluksissa kasvaa vähitellen. Jatkossa lohkoketjuteknologia tulee todennäköisesti olemaan yhä tärkeämpi osa digitaalista infrastruktuuria, ja sen vaikutukset voivat ulottua eri aloille, kuten rahoitukseen, terveydenhuoltoon, logistiikkaan ja älykkääseen liikenteeseen.

6.2. Tulevat teknologiat ja innovaatiot

Lohkoketjuteknologia on jatkanut kehittymistään vuosien varrella, ja on olemassa useita tulevia teknologioita ja innovaatioita, jotka voivat edelleen parantaa lohkoketjujen käyttöä tietokantateknologiana.

Yksi tärkeimmistä innovaatioista on skaalautuvuuden parantaminen, joka on ollut yksi lohkoketjujen suurimmista haasteista. Tämän ongelman ratkaisemiseksi on kehitetty useita uusia teknologioita, kuten lohkoketjujen kerrostaminen, sharding ja off-chain-ratkaisut.

Toinen tärkeä innovaatio on lohkoketjujen yhteentoimivuuden parantaminen. Tällä hetkellä lohkoketjut toimivat usein erillään toisistaan, mutta tulevaisuudessa on mahdollista, että ne voivat olla yhteentoimivia ja kommunikoida keskenään.

Älysopimukset ovat myös jatkuvassa kehityksessä, ja niiden käyttömahdollisuudet ovat laajentuneet. Esimerkiksi on mahdollista, että tulevaisuudessa älysopimukset voivat käyttää tekoälyä ja koneoppimista tehostamaan suorituskykyään ja tarkkuuttaan.

Lisäksi on olemassa joitakin kehittyviä lohkoketjuteknologioita, kuten Holochain ja Hashgraph, jotka pyrkivät tarjoamaan uusia lähestymistapoja hajautettujen sovellusten kehittämiseen.

Kaiken kaikkiaan lohkoketjuteknologian kehittyminen jatkuu edelleen, ja sen tulevaisuus tietokantateknologiana näyttää lupaavalta. Uusien innovaatioiden ja teknologioiden myötä lohkoketjuista voi tulla entistä tehokkaampia, skaalautuvampia ja käyttökelpoisempia monenlaisissa sovelluksissa ja järjestelmissä.

6.2.1. Uudet lohkoketjuteknologiat

Lohkoketjuteknologian nopea kehitys on johtanut uusien lohkoketjuteknologioiden kehittämiseen. Nämä uudet teknologiat tarjoavat ratkaisuja joillekin lohkoketjuteknologian nykyisistä haasteista, kuten skaalautuvuus ja käyttöliittymät.

Yksi tällainen uusi lohkoketjuteknologia on EOS.IO, joka on suunniteltu parantamaan lohkoketjujen skaalautuvuutta. EOS.IO käyttää Delegated Proof of Stake (DPoS) -konsensusmekanismia, joka mahdollistaa jopa miljoonan transaktion käsittelemisen sekunnissa. Lisäksi EOS.IO tarjoaa kehittäjille käyttöliittymän, joka mahdollistaa älysopimusten helpomman ja nopeamman toteuttamisen.

Toinen uusi lohkoketjuteknologia on Hashgraph, joka käyttää omaa konsensusmekanismiaan nimeltä Virtual Voting. Hashgraphin avulla voidaan käsitellä jopa 250 000 transaktiota sekunnissa, mikä on huomattavasti enemmän kuin Bitcoinin ja Ethereumin lohkoketjuissa. Hashgraphin käyttöliittymä on myös suunniteltu helpottamaan kehittäjien työtä älysopimusten toteuttamisessa.

Myös Quorum on uusi lohkoketjuteknologia, joka on kehitetty erityisesti finanssialan käyttöön. Quorum käyttää Proof of Authority (PoA) -konsensusmekanismia, joka on suunniteltu parantamaan lohkoketjujen suorituskykyä ja skaalautuvuutta. Quorum tarjoaa myös yksityisyyden suojaa, mikä on erityisen tärkeää finanssialalla.

Näiden uusien lohkoketjuteknologioiden kehitys osoittaa, että lohkoketjuteknologian kehitys ei ole vielä saavuttanut huippuaan. Uusien teknologioiden kehittäminen voi auttaa ratkaisemaan joitain lohkoketjujen nykyisistä haasteista ja tarjota uusia mahdollisuuksia sovelluskehittäjille ja yrityksille.

6.2.2. Parannukset nykyisiin lohkoketjuihin

Vaikka lohkoketjuteknologia on edistynyt huomattavasti sen kehityksen alkuvaiheista, sillä on edelleen parannettavaa useilla osa-alueilla. Tässä osiossa tarkastelemme joitakin nykyisiin lohkoketjuihin liittyviä haasteita ja niiden mahdollisia ratkaisuja.

Yksi suurimmista haasteista on lohkoketjujen skaalautuvuus, joka rajoittaa niiden käyttöä suurissa kaupallisissa sovelluksissa. Yksi mahdollinen ratkaisu on lohkoketjujen kerrostaminen (layering), joka tarkoittaa lohkoketjun jakamista useampaan kerrokseen, joissa jokaisessa käsitellään tietyn tyyppisiä toimintoja. Tämä voi parantaa lohkoketjun skaalautuvuutta, koska jokainen kerros voi käsitellä omaa osa-aluettaan tehokkaammin.

Toinen skaalautuvuuteen liittyvä haaste liittyy lohkoketjujen koon kasvuun ja siihen liittyvään tallennustilan tarpeeseen. Tämän ratkaisemiseksi on esitetty erilaisia ratkaisuja, kuten lohkoketjujen puristaminen (sharding), joka tarkoittaa lohkoketjun jakamista pienempiin osiin, tai lohkoketjujen poistaminen (pruning), joka tarkoittaa vanhojen lohkojen poistamista lohkoketjusta tallennustilan vapauttamiseksi.

Toinen merkittävä haaste on lohkoketjujen tietoturva. Tämän ratkaisemiseksi on kehitetty erilaisia tietoturvaan liittyviä parannuksia, kuten Byzantine Fault Tolerance (BFT) -konsensusmekanismi, joka on suunniteltu torjumaan lohkoketjujen haitallisia hyökkäyksiä. Toinen esimerkki on zero-knowledge proof -protokolla, joka mahdollistaa tiedon jakamisen ilman, että sen lähde paljastuu.

Kolmas haaste liittyy lohkoketjujen ympäristövaikutuksiin, kuten energiankulutukseen ja päästöihin. Tämän ratkaisemiseksi on esitetty erilaisia ratkaisuja, kuten Proof of

Stake (PoS) -konsensusmekanismi, joka on energiatehokkaampi kuin perinteinen Proof of Work (PoW) -mekanismi.

Lopuksi, lohkoketjujen käyttöönottoon liittyy myös käyttöliittymien ja käytettävyyden haasteita, jotka voivat hidastaa niiden käyttöönottoa suuremmassa mittakaavassa. Tämän ratkaisemiseksi on tärkeää kehittää käyttäjäystävällisiä sovelluksia, jot
ka käyttävät lohkoketjuteknologiaa taustalla. Lisäksi on tärkeää kehittää standardeja, jotka helpottavat eri lohkoketjujen välistä yhteistyötä.

Kaiken kaikkiaan nykyisten lohkoketjujen haasteisiin on kehitetty useita ratkaisuja, ja lohkoketjuteknologia kehittyy jatkuvasti. Tulevaisuudessa lohkoketjuteknologia voi mahdollistaa uusia sovelluksia, joita emme vielä osaa edes kuvitella.

6.3. Lohkoketjujen vaikutus tietokanta-alalle

Lohkoketjuteknologialla on potentiaalia mullistaa tietokanta-alaa monella tavalla. Lohkoketjujen avulla voidaan luoda hajautettuja tietokantoja, joita voidaan käyttää monenlaisissa sovelluksissa, kuten äänestyksissä, älysopimuksissa ja hajautetussa rahoituksessa. Lohkoketjujen avulla voidaan myös luoda uusia liiketoimintamalleja ja käyttötapoja, kuten mikromaksuja ja omistusoikeuksien hallintaa.

Tulevaisuudessa lohkoketjuteknologian odotetaan kehittyvän entistä nopeammaksi ja skaalautuvammaksi. Monet kehittäjät etsivät ratkaisuja lohkoketjujen skaalautuvuusongelmiin, ja uusia teknologioita, kuten lohkoketjujen kerrostamista ja

sivuketjuja, kehitetään jatkuvasti.

Lohkoketjujen käyttöönoton esteenä on kuitenkin edelleen tiettyjen sääntelyesteiden ja käyttötapojen puute, ja niiden laajamittainen käyttöönotto voi edellyttää uusien liiketoimintamallien ja -prosessien kehittämistä. Lohkoketjuteknologian hyödyntäminen tulee myös vaatimaan asiantuntemusta ja osaamista monilta tieteenaloilta, kuten kryptografia, tietoturva ja hajautettujen järjestelmien suunnittelu.

6.3.1. Tulevaisuuden näkymät lohkoketjuteknologian käytöstä tietokantana

Lohkoketjuteknologiaa käytetään jo nyt laajalti tietokantoina monilla eri aloilla, ja sen käyttö kasvaa edelleen nopeasti. Tulevaisuudessa lohkoketjuteknologiaa käytetään todennäköisesti entistä enemmän tietokantoina monilla eri aloilla, ja sen käyttö laajenee uusille sovellusalueille.

Yksi tärkeimmistä tulevaisuuden näkymistä liittyy lohkoketjuteknologian käytön kasvuun IoT-sovelluksissa. Lohkoketjuteknologiaa voidaan käyttää tehokkaasti IoT-laitteiden tiedon tallentamiseen ja jakamiseen hajautetusti ja turvallisesti. Tämä mahdollistaa uusien älykkäiden sovellusten kehittämisen, kuten älykkäät kaupungit ja älykkäät liikennejärjestelmät.

Toinen tärkeä tulevaisuuden näkymä on lohkoketjuteknologian käyttö valtioiden ja hallitusten välisessä yhteistyössä. Lohkoketjuteknologiaa voidaan käyttää tehokkaasti esimerkiksi kansainvälisessä kaupassa ja verotuksessa, sillä se mahdollistaa transaktioiden nopean ja turvallisen käsittelyn yli

maiden rajojen.

Kolmas tärkeä tulevaisuuden näkymä liittyy lohkoketjuteknologian käytön kasvuun terveydenhuollossa. Lohkoketjuteknologiaa voidaan käyttää tehokkaasti terveydenhuollon tiedon tallentamiseen ja jakamiseen hajautetusti ja turvallisesti, mikä parantaa potilastietojen hallintaa ja yksityisyyttä. Tämä mahdollistaa myös uusien älykkäiden terveyssovellusten kehittämisen, kuten henkilökohtaiset terveysprofiilit ja lääkityksen seuranta.

Kaiken kaikkiaan lohkoketjuteknologian käyttö tietokantana on vasta alkutekijöissään, ja sen potentiaali on valtava. Lohkoketjuteknologia mahdollistaa hajautetun, läpinäkyvän ja turvallisen tietokannan luomisen, joka voi vähentää välittäjien tarvetta ja parantaa tietojen hallintaa monilla eri aloilla. Tulevaisuudessa lohkoketjuteknologian käyttö tietokantana kasvaa edelleen, ja sen avulla kehitetään uusia älykkäitä sovelluksia, jotka parantavat elämänlaatua ja luovat uusia mahdollisuuksia.

6.3.2. Lohkoketjuteknologian mahdollisuudet tietokanta-alalla

Lohkoketjuteknologia tarjoaa useita mahdollisuuksia tietokanta-alalla. Yksi suurimmista mahdollisuuksista on hajautettujen tietokantojen luominen, joka mahdollistaa reaaliaikaisen datan jakamisen ja päivittämisen useiden osapuolten kesken. Tämä voi olla erityisen hyödyllistä esimerkiksi logistiikka- tai toimitusketjujen hallinnassa, jossa useat eri tahot tarvitsevat reaaliaikaista tietoa tuotteiden sijainnista ja liikkumisesta.

Toinen mahdollisuus on älysopimusten käyttö tietokantojen hallinnassa. Älysopimukset ovat itse toteutettuja sopimuksia, jotka voidaan ajaa automaattisesti lohkoketjussa. Niitä voidaan käyttää esimerkiksi tiedon validoinnissa ja tallentamisessa lohkoketjuun, jolloin tiedon aitous ja eheys voidaan varmistaa automaattisesti.

Kolmas mahdollisuus on tietojen jakaminen ja käyttöönotto lohkoketjujen avulla. Lohkoketjut voivat toimia turvallisena ja hajautettuna alustana tietojen jakamiselle ja käyttöönotolle, mikä voi helpottaa tietojen jakamista eri organisaatioiden välillä. Esimerkiksi terveydenhuollon alalla lohkoketjuteknologiaa voidaan käyttää potilastietojen jakamiseen eri organisaatioiden välillä.

Neljäs mahdollisuus liittyy tietoturvaan. Lohkoketjujen hajautetun rakenteen ansiosta lohkoketjuja pidetään yleisesti turvallisempina kuin perinteisiä tietokantoja. Lohkoketjujen tietoturvan parantamiseksi on kuitenkin kehitettävä edelleen uusia ratkaisuja, kuten älykkäitä sopimuksia ja hajautettuja tietoturvamekanismeja.

Kaiken kaikkiaan lohkoketjuteknologia tarjoaa paljon mahdollisuuksia tietokanta-alalla, mutta sen käyttöönottoon liittyy myös haasteita. Tietokantaratkaisuja suunniteltaessa onkin tärkeää arvioida huolellisesti, missä tilanteissa lohkoketjuteknologia on hyödyllinen ratkaisu ja milloin perinteiset tietokannat ovat parempi vaihtoehto.

7. Yhteenveto ja johtopäätökset

Osa 7 sisältää kirjan yhteenvedon ja johtopäätökset. Siinä käsitellään lyhyesti kaikki tärkeimmät käsitteet ja aiheet, jotka on käyty läpi kirjan aikaisemmissa osissa. Tämä osio tarjoaa

myös yhteenvedon tärkeimmistä havainnoista ja opetuksista, jotka voidaan ottaa talteen lohkoketjuteknologian tulevaisuuden ja sen käytön suhteen tietokantana. Lopuksi osiossa tarkastellaan lohkoketjuteknologian mahdollisuuksia tulevaisuudessa ja sen potentiaalia muuttaa monia eri aloja, kuten rahoitusta, terveydenhuoltoa, logistiikkaa ja monia muita.

7.1. Lohkoketjujen käytön kannattavuus tietokantoina

Luku 7 käsittelee yhteenvedon ja johtopäätösten tekemistä lohkoketjujen käytöstä tietokantoina. Tässä osiossa käsitellään, onko lohkoketjujen käyttö tietokantoina kannattavaa ja mitkä ovat sen edut ja haasteet verrattuna perinteisiin tietokantaratkaisuihin.

Osiossa käydään läpi lohkoketjuteknologian käytön mahdollisia hyötyjä ja haittoja tietokantana, kuten parempaa tietoturvaa ja läpinäkyvyyttä, mutta myös haasteita skaalautuvuuden ja yksityisyyden suhteen. Lisäksi käsitellään lohkoketjuteknologian sovelluskohteita ja esimerkkejä sekä sen vaikutuksia tietokanta-alalle.

Lopuksi osiossa tehdään johtopäätöksiä lohkoketjuteknologian käytöstä tietokantoina ja pohditaan sen tulevaisuutta tietokanta-alalla.

7.1.1. Lohkoketjujen hyödyt tietokantana

Lohkoketjut tarjoavat useita etuja tietokantana verrattuna perinteisiin keskitettyihin tietokantoihin. Tässä osiossa tarkastelemme joitakin lohkoketjujen tärkeimmistä hyödyistä

tietokantana.

1. Hajautettu rakenne: Lohkoketjut ovat hajautettuja järjestelmiä, jotka koostuvat useista solmuista tai tietokoneista. Tämä tekee lohkoketjuista alttiimpia hyökkäyksille, mutta toisaalta myös turvallisempia, koska niiden tietoja ei ole keskitetty yhteen paikkaan. Tämä hajautettu rakenne mahdollistaa myös nopeamman tiedonvaihdon eri solmujen välillä.
2. Läpinäkyvyys: Lohkoketjut ovat avoimia järjestelmiä, mikä tarkoittaa, että niiden tietoja voi tarkastella ja tarkistaa kuka tahansa. Tämä tekee lohkoketjuista läpinäkyvämpiä kuin perinteiset tietokannat, joissa tietoja ei yleensä voi tarkistaa ulkopuolisten tahojen toimesta.
3. Turvallisuus: Lohkoketjut käyttävät kryptografiaa tietojen suojaamiseen, mikä tekee niistä turvallisempia kuin perinteiset tietokannat. Lohkoketjujen tietojen manipulointi on vaikeaa, koska kaikkien lohkojen on täytettävä tietyt kryptografiset vaatimukset, jotta ne voidaan lisätä lohkoketjuun.
4. Immuuni haitallisille hyökkäyksille: Lohkoketjut ovat immuuneja useille haitallisille hyökkäyksille, kuten tietojen manipuloinnille ja haitallisille tietokoneviruksille. Tämä johtuu siitä, että lohkoketjut käyttävät hajautettua järjestelmää, joka ei ole yhtä altis yksittäisille hyökkäyksille kuin keskitetyt tietokannat.
5. Varmuuskopiot: Lohkoketjut mahdollistavat tietojen varmuuskopioinnin eri solmuihin tai tietokoneisiin. Tämä tekee lohkoketjuista turvallisempia kuin perinteiset tietokannat, jotka voivat menettää tietoja,

jos niiden tallennuspaikka rikkoutuu.

6. Älysopimukset: Lohkoketjut mahdollistavat älysopimusten käytön, mikä mahdollistaa tietojen automaattisen käsittelyn ja sopimusten täytäntöönpanon. Älysopimukset voivat vähentää kustannuksia ja nopeuttaa prosesseja, koska ne eivät vaadi manuaalista toimintaa. Esimerkiksi älysopimus voi automaattisesti käsitellä ja tarkastaa laskuja tai sopimuksia, mikä säästää aikaa ja vähentää virheiden riskiä.
7. Luotettavuus: Lohkoketjut ovat luotettavampia kuin perinteiset tietokannat, koska ne perustuvat hajautettuun järjestelmään, joka mahdollistaa useiden solmujen tarkastamisen ja vahvistamisen. Tämä tekee lohkoketjuista luotettavamman tiedon lähteen, koska ne perustuvat useiden osapuolten yhteiseen vahvistukseen.
8. Hajautetut sovellukset: Lohkoketjut mahdollistavat hajautettujen sovellusten kehittämisen, joissa sovellus on hajautettu useiden solmujen tai tietokoneiden välille. Tämä mahdollistaa nopeamman ja turvallisemman tiedonvaihdon ja tekee sovelluksista alttiimpia virheille ja hyökkäyksille.

Kaiken kaikkiaan lohkoketjut tarjoavat useita etuja tietokantana, mukaan lukien hajautetun rakenteen, läpinäkyvyyden, turvallisuuden, immuunisuuden haitallisille hyökkäyksille, varmuuskopiot, älysopimukset, luotettavuuden ja mahdollisuuden kehittää hajautettuja sovelluksia.

7.1.2. Lohkoketjujen käytön riskit tietokantana

Vaikka lohkoketjuilla on monia hyötyjä tietokantana, niiden käyttöön liittyy myös joitakin riskejä. Tässä osiossa tarkastelemme joitakin tärkeimmistä riskeistä.

Skaalautuvuus: Vaikka lohkoketjujen hajautettu rakenne on yksi niiden tärkeimmistä eduista, se voi myös aiheuttaa skaalautuvuusongelmia. Lohkoketjut voivat olla hitaampia ja vaativampia käsitellä kuin perinteiset tietokannat, mikä voi rajoittaa niiden käyttöä suurissa kaupallisissa sovelluksissa.

Tietoturva: Vaikka lohkoketjut ovat turvallisempia kuin perinteiset tietokannat, ne eivät ole täysin immuuneja hyökkäyksille. Lohkoketjujen hajautettu rakenne voi tehdä niistä alttiimpia 51% hyökkäyksille, joissa hyökkääjä saa hallinnan yli 50%:sta lohkoketjun laskentatehosta. Lohkoketjujen tietoturvariskit voivat myös liittyä koodausvirheisiin, joita voi olla vaikea havaita.

Älysopimusten riskit: Vaikka älysopimukset voivat olla hyödyllisiä lohkoketjujen automatisoinnissa, ne voivat myös aiheuttaa riskejä, jos ne sisältävät koodausvirheitä tai ohjelmistovirheitä. Tämä voi johtaa siihen, että älysopimus käyttäytyy odottamattomalla tavalla ja aiheuttaa vahinkoa.

Laillisuus ja sääntely: Lohkoketjujen käyttöön liittyy joitakin oikeudellisia ja sääntelyyn liittyviä riskejä. Esimerkiksi tietosuoja- ja verotuskysymykset voivat olla monimutkaisia ratkaista, ja niiden selvittäminen voi vaatia yhteistyötä hallitusten, yritysten ja teknologian kehittäjien välillä.

Yhteensopivuus: Lohkoketjut voivat olla yhteensopimattomia perinteisten tietokantojen kanssa, mikä voi tehdä niiden integroimisesta vaikeaa. Tämä voi rajoittaa lohkoketjujen käyttöä joissakin sovelluksissa.

Kaiken kaikkiaan lohkoketjujen käyttö tietokantana tarjoaa

monia etuja, mutta sen käyttöön liittyy myös joitakin riskejä. On tärkeää arvioida tarkasti lohkoketjujen hyödyt ja riskit ennen niiden käyttöönottoa.

7.2. Mahdolliset riskit ja varotoimet

Lohkoketjuteknologian käyttö tietokantana tarjoaa monia etuja, mutta sillä on myös omat riskinsä. Yksi tärkeimmistä riskeistä on tietoturva, sillä lohkoketjuun tallennettavat tiedot ovat pysyviä ja muuttumattomia. Siksi on tärkeää suojata henkilötietoja ja muita arkaluonteisia tietoja asianmukaisilla salaustekniikoilla ja tietoturvakäytännöillä.

Toinen potentiaalinen riski liittyy skaalautuvuuteen, sillä nykyiset lohkoketjut kärsivät skaalautuvuusongelmista. Tämä johtuu lohkoketjujen hajautetusta rakenteesta ja lohkojen rajoitetusta koosta. Tämä ongelma on kuitenkin tunnistettu, ja kehittäjät etsivät aktiivisesti uusia ratkaisuja skaalautuvuusongelmiin.

Lopuksi, lohkoketjujen käyttö tietokantana voi olla monimutkaista ja vaatii huolellista suunnittelua ja toteutusta. Lohkoketjuteknologia on edelleen suhteellisen uusi, ja sen käyttöönotto voi vaatia uusien taitojen oppimista ja uudenlaisen ajattelutavan omaksumista.

Nämä riskit voidaan kuitenkin minimoida asianmukaisilla varotoimilla ja lohkoketjuteknologian huolellisella käytöllä. Jos lohkoketjujen käyttöä tietokantana lähestytään oikein, se voi tarjota merkittäviä etuja tehokkuuden, läpinäkyvyyden ja turvallisuuden kannalta.

7.2.1. Tietoturva ja yksityisyysriskit

Lohkoketjujen käytössä tietokantana on tärkeää ottaa huomioon tietoturva- ja yksityisyysriskit. Vaikka lohkoketjut ovat turvallisempia kuin perinteiset keskitetyt tietokannat, niihin liittyy silti riskejä, jotka voivat vaikuttaa tietojen turvallisuuteen ja yksityisyyteen.

Yksi riski liittyy lohkoketjun yksityisyyteen. Vaikka lohkoketjut ovat avoimia ja läpinäkyviä järjestelmiä, on olemassa tapoja suojata tietoja, jotta ne eivät ole julkisia. Esimerkiksi joissakin lohkoketjuissa on mahdollista käyttää salausta tai pseudonyymejä, jotta tietojen lähde ei paljastu. On kuitenkin tärkeää varmistaa, että tietojen yksityisyys on turvattu kaikissa tilanteissa.

Toinen riski liittyy lohkoketjujen tietoturvaan. Vaikka lohkoketjut ovat turvallisempia kuin perinteiset keskitetyt tietokannat, niihin liittyy edelleen tietoturvariskejä. Esimerkiksi hyökkääjä voi yrittää suorittaa 51% hyökkäyksen, jossa hän saa hallinnan yli 50%:sta lohkoketjun laskentatehosta ja voi manipuloida tietoja.

Lisäksi lohkoketjuteknologia on edelleen melko uusi ja sitä kehitetään jatkuvasti. Tämä tarkoittaa, että tietoturvariskit ja haavoittuvuudet voivat muuttua nopeasti, ja on tärkeää pysyä ajan tasalla mahdollisista riskeistä ja niiden torjuntakeinoista.

Lopuksi, lohkoketjujen käyttöönotto vaatii myös tietyn tason teknistä osaamista ja resursseja. On tärkeää varmistaa, että organisaatiolla on riittävästi tietoteknistä asiantuntemusta ja infrastruktuuria, jotta lohkoketjujen käyttöönotto ja ylläpito onnistuu sujuvasti ja turvallisesti.

7.2.2. Skaalautuvuusongelmat

Skaalautuvuusongelmat ovat yksi lohkoketjuteknologian käytön riskeistä tietokantana. Lohkoketjujen skaalautuvuus tarkoittaa kykyä käsitellä suuria tietomääriä nopeasti ja tehokkaasti. Tämä on tärkeää varsinkin silloin, kun lohkoketjuja käytetään laajamittaisesti kaupallisissa sovelluksissa.

Lohkoketjujen skaalautuvuus on edelleen rajoitettu, ja sen parantaminen on yksi keskeisimmistä haasteista lohkoketjuteknologian käytölle tietokantana. Skaalautuvuusongelmat voivat johtaa hitaaseen tiedonkäsittelyyn ja pitkiin viiveisiin, mikä voi haitata liiketoiminnan tehokkuutta ja käyttökokemusta.

Skaalautuvuusongelmat johtuvat osittain lohkoketjujen hajautetusta luonteesta. Tietojen tallentaminen lohkoketjuun vaatii kaikkien solmujen laskentatehoa, mikä hidastaa tiedonkäsittelyä ja voi johtaa suorituskyvyn laskuun. Lisäksi lohkoketjujen koon kasvu lisää tallennustilan tarvetta, mikä voi myös hidastaa tiedonkäsittelyä.

Skaalautuvuusongelmiin on kuitenkin kehitetty useita ratkaisuja. Yksi ratkaisu on lohkoketjujen kerrostaminen, joka mahdollistaa lohkoketjun jakamisen useisiin kerroksiin, joissa jokainen kerros käsittelee tietyn tyyppisiä toimintoja. Tämä voi parantaa lohkoketjun skaalautuvuutta, koska jokainen kerros voi käsitellä omaa osa-aluettaan tehokkaammin.

Toinen skaalautuvuusongelmiin liittyvä ratkaisu on lohkoketjujen puristaminen (sharding), joka tarkoittaa lohkoketjun jakamista pienempiin osiin. Tämä voi parantaa lohkoketjun suorituskykyä, koska lohkoketjuun tallennetaan vähemmän tietoa ja jokainen osio käsitellään erikseen.

Lohkoketjujen skaalautuvuusongelmat ovat edelleen merkittäviä, mutta ratkaisujen kehittäminen ja käyttöönotto voivat auttaa vähentämään niitä ja edistämään lohkoketjuteknologian käyttöä tietokantana.

7.3. Suositukset ja parhaat käytännöt

Tässä osiossa käydään läpi lohkoketjuteknologian hyödyt ja haitat tietokantana, mahdolliset riskit ja varotoimet sekä suositukset ja parhaat käytännöt lohkoketjujen käytössä tietokantana. Osiossa myös tarkastellaan lohkoketjujen mahdollisuuksia kehittää tietokantateknologiaa ja miten lohkoketjut voivat muuttaa tietokanta-alaa tulevaisuudessa.

7.3.1. Lohkoketjuteknologian käytön suositukset

Lohkoketjuteknologiaa käyttäessä on tärkeää huomioida seuraavat suositukset:

1. Tietoturva: Lohkoketjujen tietoturvaan liittyy riskejä, joten on tärkeää ottaa käyttöön asianmukaiset tietoturvakäytännöt ja -menetelmät. Tämä voi sisältää esimerkiksi vahvojen salasanojen käytön, kaksivaiheisen todennuksen ja tietojen salaamisen.
2. Yksityisyys: Lohkoketjut ovat julkisia ja läpinäkyviä järjestelmiä, joten on tärkeää harkita, mitä tietoja tallennetaan lohkoketjuun ja miten niitä käsitellään. Yksityisyyden suojaamiseksi voi käyttää esimerkiksi anonymisointitekniikoita.
3. Skalautuvuus: Lohkoketjujen skaalautuvuus on

edelleen haaste, joten on tärkeää valita lohkoketjuteknologia, joka sopii käyttötarkoitukseen ja tarjoaa riittävän skaalautuvuuden.

4. Yhteistyö: Lohkoketjuteknologian käyttö edellyttää yhteistyötä eri toimijoiden välillä, kuten yritysten, teknologiakehittäjien ja hallitusten. On tärkeää kehittää yhteisiä standardeja ja käytäntöjä, jotta lohkoketjuteknologiaa voidaan käyttää tehokkaasti ja turvallisesti.
5. Käytettävyys: Lohkoketjuteknologian käytön on oltava helppoa ja käyttäjäystävällistä. Tämä vaatii kehittäjiltä käyttäjien tarpeiden ymmärtämistä ja käyttökokemuksen parantamista.
6. Koulutus: Lohkoketjuteknologia on suhteellisen uusi ala, joten sen käyttöön liittyy oppimiskäyrä. On tärkeää kouluttaa henkilökuntaa ja käyttäjiä lohkoketjuteknologian käytöstä ja hyödyistä, jotta sen käyttöönotto voidaan tehdä mahdollisimman tehokkaasti ja turvallisesti.

Nämä suositukset auttavat vähentämään lohkoketjuteknologian käyttöön liittyviä riskejä ja varmistamaan sen tehokkaan ja turvallisen käytön tietokantana.

7.3.2. Parhaat käytännöt lohkoketjujen käytössä tietokantana

Tässä osiossa käsitellään joitakin parhaita käytäntöjä lohkoketjujen käytössä tietokantana.

1. Suunnittele huolellisesti: Ennen lohkoketjun käyttöönottoa on tärkeää suunnitella huolellisesti, mitä tietoja lohkoketjuun tallennetaan ja miten niitä käsitellään. Tämä auttaa välttämään tarpeettomia riskejä ja mahdollisia ongelmia tietoturvan ja yksityisyyden kanssa.
2. Huolehdi tietoturvasta: Lohkoketjuteknologia tarjoaa monia tietoturvaetuja, mutta se ei ole täysin immuuni hyökkäyksille. On tärkeää huolehtia tietoturvasta, käyttää vahvoja salauksia ja seurata jatkuvasti mahdollisia turvallisuusriskejä.
3. Optimoi skaalautuvuus: Lohkoketjujen skaalautuvuus on edelleen haasteellista, mutta sitä voidaan optimoida käyttämällä lohkoketjujen kerrostamista, puristamista tai poistamista. Tämä auttaa vähentämään lohkoketjun kokoa ja lisää sen skaalautuvuutta.
4. Huolehdi yksityisyydestä: Lohkoketjuteknologia on läpinäkyvä järjestelmä, mutta se voi myös aiheuttaa yksityisyysriskejä. On tärkeää huolehtia käyttäjien yksityisyydestä ja suojata henkilötietoja asianmukaisilla salaustekniikoilla.
5. Käytä älysopimuksia: Älysopimukset ovat yksi lohkoketjuteknologian tärkeimmistä eduista, ja niitä voidaan käyttää tietojen automaattiseen käsittelyyn ja sopimusten täytäntöönpanoon. Älysopimusten käyttö auttaa vähentämään kustannuksia ja parantamaan tehokkuutta.
6. Tiedota käyttäjiä: Lohkoketjuteknologia on monimutkainen järjestelmä, ja sen käyttöönotto voi olla vaikeaa käyttäjille. On tärkeää tarjota käyttäjille

tarvittava koulutus ja tiedottaa heille lohkoketjun käytöstä ja sen eduista.

7. Kehitä käyttäjäystävällisiä sovelluksia: Käyttäjäystävälliset sovellukset ovat avainasemassa lohkoketjuteknologian laajamittaisessa käyttöönotossa. Kehittäjien on kiinnitettävä huomiota käyttäjäkokemukseen ja pyrittävä tarjoamaan helppokäyttöisiä sovelluksia, jotka ovat yhtä helppo käyttää kuin perinteiset keskitetyt tietokannat. Tämä auttaa lisäämään lohkoketjujen käyttöä eri aloilla ja edistää niiden yleistymistä tulevaisuudessa.

8. Liitteet

A. Lohkoketjujen sanasto

Blockchain - Lohkoketju
Distributed Ledger - Hajautettu pääkirja
Node - Solmu
Consensus Mechanism - Konsensusmekanismi
Proof of Work (PoW) - Työn todistaminen
Proof of Stake (PoS) - Omistuksen todistaminen
Sharding - Lohkojen jakaminen
Pruning - Lohkojen poistaminen
Smart Contract - Älysopimus
Decentralized Application (dApp) - Hajautettu sovellus
Hash Function - Tiivistealgoritmi
Public Key Cryptography - Julkisen avaimen salaus
Private Key - Yksityinen avain
Wallet - Lompakko
Mining - Louhinta

Fork - Haara
Soft Fork - Pehmeä haara
Hard Fork - Kova haara
Initial Coin Offering (ICO) - Kryptovaluutan julkaiseminen
Token - Merkki
Altcoin - Vaihtoehtoinen kryptovaluutta
Cryptocurrency - Kryptovaluutta
Gas - Kaasu (Ethereumin lohkoketjussa käytetty termi, joka viittaa transaktioiden maksamiseen tarvittavaan määrään Etheriä)
Merkle Tree - Merklen puu
Hash Rate - Tiivisteen nopeus
Block Reward - Lohkon palkkio
Genesis Block - Alkuperäinen lohko
Immutable - Muuttumaton
Tokenization - Tokenisointi
Double Spending - Tuplavaraaminen
Permissioned Blockchain - Luvanvarainen lohkoketju
Permissionless Blockchain - Luvaton lohkoketju
Byzantine Fault Tolerance (BFT) - Byzanttilaisen virheen sietokyky
Zero-knowledge Proof - Zero-knowledge -todistus
Sidechain - Sivuketju
Layering - Kerrostaminen
Scaling - Skaalaaminen
Fungible Token - Vaihdettava merkki
Non-Fungible Token (NFT) - Vaihdettamaton merkki
DeFi - Hajautettu rahoitus (Decentralized Finance)
DAO - Hajautettu autonominen organisaatio (Decentralized Autonomous Organization)
Interoperability - Yhteentoimivuus
Proof of Burn - Polttamisen todistaminen
Stablecoin - Vakaa kryptovaluutta
Central Bank Digital Currency (CBDC) - Keskuspankin

digitaalinen valuutta.

- Blockchain – Lohkoketju

Hajautettu tietokanta, joka koostuu lohkoista, joissa on kryptografisesti turvattu linkki edelliseen lohkoon. Tämä mahdollistaa tietojen turvallisen tallennuksen ja jakamisen.

- Distributed Ledger - Hajautettu pääkirja

Distributed Ledger, eli hajautettu pääkirja, on hajautetun tietokannan muoto, joka koostuu useista solmuista tai tietokoneista. Hajautetun pääkirjan tietokannan tiedot tallennetaan useisiin solmuihin, eikä yhteen keskitettyyn tietokantaan, mikä tekee siitä turvallisemman ja läpinäkyvämmän. Hajautettu pääkirja on usein käytetty lohkoketjujen alusta.

- Node – Solmu

Solmu (node) on yksi lohkoketjun osallistujista, jotka ylläpitävät ja päivittävät lohkoketjun tietokantaa. Solmu voi olla tietokone, palvelin tai muu laite, joka on yhteydessä lohkoketjun verkkoon ja joka suorittaa lohkoketjun toimintaa. Solmut ovat hajautetun järjestelmän ytimessä, koska niiden avulla lohkoketjun tietokanta on hajautettu usealle eri tietokoneelle tai laitteelle, mikä tekee lohkoketjusta turvallisemman ja vähemmän alttiin yksittäisten solmujen vioille tai hyökkäyksille.

- Consensus Mechanism – Konsensusmekanismi

Konsensusmekanismi (Consensus Mechanism) on menetelmä, jonka avulla lohkoketjuverkostoissa saadaan yhteisymmärrys siitä, että uusi transaktio voidaan hyväksyä ja lisätä lohkoketjuun. Konsensusmekanismit ovat keskeisiä lohkoketjuteknologiassa, koska ne mahdollistavat hajautetun verkoston toiminnan ilman keskitettyä valvontaa. Yleisiä konsensusmekanismeja ovat esimerkiksi Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS) ja Practical Byzantine Fault Tolerance (PBFT).

- Proof of Work (PoW) - Työn todistaminen

Proof of Work (PoW) on lohkoketjujen konsensusmekanismi, jota käytetään varmistamaan uusien lohkojen luotettavuus ja estämään haitalliset hyökkäykset. Tämä mekanismi vaatii lohkon löytämiseen tietokoneen laskentatehoa ja energiaa, mikä tekee haitallisten hyökkäysten toteuttamisen vaikeaksi ja kalliiksi. Lohkon löytänyt tietokone saa palkinnoksi lohkoketjun omaa kryptovaluuttaa. Proof of Work -mekanismia käytetään esimerkiksi Bitcoinissa.

- Proof of Stake (PoS)

Proof of Stake (PoS) on lohkoketjuteknologian konsensusmekanismi, joka perustuu siihen, että lohkoketjuun uusia lohkoja lisätään sen käyttäjien tekemän "panostuksen" perusteella. Tämä panostus tarkoittaa yleensä lohkoketjussa olevien kryptovaluuttojen pidättämistä tai "lukitsemista"

tiettyyn aikaan. Tämä mekanismi on energiatehokkaampi kuin Proof of Work (PoW) -mekanismi, koska se ei vaadi suurta tietokoneiden laskentatehoa.

- Sharding - Lohkojen jakaminen

Sharding on lohkoketjuteknologian skaalautuvuutta parantava tekniikka, jossa lohkoketju jaetaan pienempiin osiin, joita kutsutaan shardseiksi. Jokainen shard käsittelee vain osaa lohkoketjun tietojen käsittelystä, mikä mahdollistaa lohkoketjun tehokkaamman toiminnan suurissa verkostoissa. Shardingia käytetään yleensä Proof of Stake (PoS) -konsensusmekanismeissa, jotka ovat energiatehokkaampia kuin Proof of Work (PoW) -mekanismit. Shardingia käytettäessä jokainen solmu ei tarvitse käsitellä kaikkia lohkoketjun tietoja, mikä säästää laskentatehoa ja vähentää lohkoketjun koon kasvusta johtuvaa tallennustilan tarvetta.

- Pruning - Lohkojen poistaminen

Pruning on lohkoketjuteknologian käsite, joka tarkoittaa vanhojen lohkojen poistamista lohkoketjusta tallennustilan vapauttamiseksi. Tämä on tärkeää lohkoketjujen skaalautuvuuden ja tehokkuuden kannalta, koska vanhojen lohkojen poistaminen vähentää lohkoketjun kokoa ja tekee sen käytöstä nopeampaa ja tehokkaampaa. Pruningia voidaan käyttää yhdessä muiden skaalautuvuusmekanismien, kuten lohkojen jakamisen (sharding) kanssa, jotta lohkoketjut voivat käsitellä suurempia tietomääriä ja toimia tehokkaammin.

- Smart Contract – Älysopimus

Smart contract, eli älysopimus, on tietokonesovellus, joka on suunniteltu toteuttamaan sopimuksen ehtoja automaattisesti ja itsenäisesti ilman kolmannen osapuolen väliintuloa. Älysopimukset ovat lohkoketjuteknologian keskeinen ominaisuus, ja ne ovat ohjelmoituja sopimuksia, jotka käyttävät lohkoketjun turvallisuusominaisuuksia sopimusehtojen täyttämisen tarkistamiseen ja suorittamiseen. Älysopimukset ovat läpinäkyviä, hajautettuja ja mahdollistavat itsenäisen sopimusten täytäntöönpanon, mikä vähentää tarvetta välittäjäorganisaatioille ja alentaa transaktiokustannuksia.

- Decentralized Application (dApp) - Hajautettu sovellus

Decentralized application (dApp) on sovellus, joka toimii hajautetulla tietokonejärjestelmällä, jossa tietokoneet ovat yhteydessä toisiinsa lohkoketjun avulla. dApp on suunniteltu toimimaan itsenäisesti ilman keskitettyä ohjausta, jolloin se tarjoaa käyttäjille suuremman turvallisuuden ja yksityisyyden. dApp:it käyttävät usein älysopimuksia suorittaakseen automaattisesti tiettyjä toimintoja lohkoketjussa.

- Hash Function – Tiivistealgoritmi

Hash-funktio eli tiivistealgoritmi on matemaattinen funktio, joka ottaa syötteenä minkä tahansa pituisen viestin ja muuntaa sen kiinteän pituiseksi binääriarvoksi, jota kutsutaan tiivisteeksi (hashiksi). Hash-funktioiden yksi tärkeimmistä käyttötarkoituksista on tietojen eheystarkistus, sillä tiiviste on laskettavissa nopeasti ja helposti kaikista viestin bitteinä laskettavista yhdistelmistä, mutta se on käytännössä mahdoton muuntaa takaisin alkuperäiseksi viestiksi. Tämä tekee hash-

funktioista tärkeän osan lohkoketjuteknologiaa, sillä ne mahdollistavat lohkojen ja niiden sisältämien tietojen turvallisen tallennuksen ja tarkistamisen.

- Public Key Cryptography - Julkisen avaimen salaus

Julkisen avaimen salaus on salausmenetelmä, joka käyttää julkista ja yksityistä avainta tiedon suojaamiseen. Julkinen avain voidaan jakaa kaikille, kun taas yksityinen avain on tarkoitettu vain tiedon vastaanottajalle. Kun tietoa salataan julkisella avaimella, se voidaan purkaa vain vastaanottajan yksityisellä avaimella. Tämä tekee julkisen avaimen salauksesta turvallisen tavan jakaa tietoa ilman, että se altistuu kolmansille osapuolille. Julkisen avaimen salaus on laajalti käytössä muun muassa lohkoketjujen tietoturvan varmistamisessa.

- Private Key - Yksityinen avain

Yksityinen avain (private key) on salausjärjestelmässä käytettävä salainen avain, joka on tarpeellinen salattujen tietojen purkamisessa. Yksityistä avainta käytetään yhdessä julkisen avaimen kanssa, jotta saadaan muodostettua salaus- ja purkuavainpari. Yksityistä avainta ei tule jakaa kenenkään kanssa, sillä sen avulla voidaan purkaa salausta ja päästä käsiksi salattuun tietoon.

- Wallet – Lompakko

Wallet eli lompakko on ohjelmisto, joka sisältää käyttäjän

kryptovaluutan yksityiset avaimet. Se mahdollistaa käyttäjän lähettää ja vastaanottaa kryptovaluuttaa. Walletti voi olla joko verkkopohjainen, ohjelmapohjainen tai laitepohjainen. Verkkopohjainen lompakko toimii pilvipalveluna, joka tarkoittaa, että käyttäjän tietoja säilytetään kolmannen osapuolen palvelimilla. Ohjelmapohjainen lompakko on ohjelma, joka asennetaan käyttäjän tietokoneelle tai mobiililaitteelle. Laitepohjainen lompakko taas on laite, johon käyttäjän yksityiset avaimet tallennetaan, kuten USB-tikku tai erillinen kryptovaluutan lompakkolaite.

- Mining – Louhinta

Mining eli louhinta tarkoittaa lohkoketjuteknologiassa prosessia, jossa verkon käyttäjät osallistuvat lohkoketjun ylläpitoon ja uusien lohkojen luomiseen. Louhintaprosessissa tietokoneet kilpailevat keskenään matemaattisten ongelmien ratkaisemisessa ja ensimmäinen onnistuja saa palkinnoksi uusia kryptovaluuttayksiköitä. Lohkoketjun ylläpidon ja uusien lohkojen luomisen ansiosta lohkoketju pysyy turvallisena ja hajautettuna.

- Fork – Haara

Fork tarkoittaa lohkoketjussa tapahtuvaa tilannetta, jossa ketju jakautuu kahteen eri haaraan. Tämä voi tapahtua esimerkiksi silloin, kun lohkoketjun sääntöjä muutetaan tai kun kaksi tai useampi lohkoa lisätään samanaikaisesti ketjuun. Fork aiheuttaa sen, että jotkin lohkoketjun solmut jatkavat alkuperäisen haaran seuraamista, kun taas toiset siirtyvät uudelle haaralle. Fork voi olla joko pysyvä tai väliaikainen, ja se voi johtaa lohkoketjun jakautumiseen kahteen erilliseen

lohkoketjuun.

- Soft Fork - Pehmeä haara

Soft Fork (pehmeä haara) on lohkoketjuteknologian termi, joka tarkoittaa ohjelmistopäivitystä, joka on taaksepäin yhteensopiva aiemman version kanssa. Tämä tarkoittaa sitä, että kaikki solmut lohkoketjussa voivat edelleen kommunikoida keskenään, vaikka jotkin solmut ovatkin päivitettyjä ja jotkut eivät. Soft Forkin aikana siis tietojen eheys ja turvallisuus säilyvät, mutta uusia ominaisuuksia voidaan lisätä. Soft Forkin vastakohta on Hard Fork, joka tarkoittaa lohkoketjun jakautumista kahteen erilliseen ketjuun, kun muutoksia tehdään protokollaan.

- Hard Fork - Kova haara

Hard Fork - Kova haara on tapahtuma, joka tapahtuu, kun kryptovaluutan lohkoketjussa tapahtuu muutos, joka ei ole yhteensopiva sen aiemman version kanssa. Tämä johtaa siihen, että lohkoketju haarautuu kahtia ja syntyy uusi kryptovaluutta, joka poikkeaa alkuperäisestä versiosta. Hard fork voi tapahtua esimerkiksi, kun lohkoketjua päivitetään uudella protokollaversiolla, joka ei ole yhteensopiva vanhan version kanssa. Hard forkin seurauksena vanha lohkoketju jatkaa olemassaoloaan, mutta uuden kryptovaluutan käyttäjät eivät voi enää käyttää vanhaa versiota. Hard fork on merkittävä tapahtuma kryptovaluutan historiassa, koska se voi vaikuttaa sen arvoon ja käyttöön laajasti.

- Initial Coin Offering (ICO) - Kryptovaluutan

julkaiseminen

Initial Coin Offering (ICO) tarkoittaa kryptovaluutan julkaisemista, joka tapahtuu yleensä rahoituskierroksen kautta, jossa sijoittajat voivat ostaa kyseistä kryptovaluuttaa tulevaisuuden käyttöä varten. ICO on suosittu tapa kerätä rahoitusta kryptovaluuttojen kehittämiseen ja levittämiseen, ja se toimii yleensä samalla tavalla kuin perinteinen osakeanti. Sijoittajat saavat ICO:n kautta kryptovaluutan kolikoita tai merkkejä, jotka ovat yleensä käyttökelpoisia vain kyseisen yrityksen ekosysteemissä.

- Token

Token tarkoittaa lohkoketjuissa digitaalista varallisuutta tai hyödykettä, joka on luotu lohkoketjuteknologian avulla. Tokenit voivat olla erilaisia, kuten kryptovaluuttoja, äänioikeuksia, lahjakortteja, pelimerkkejä tai muita digitaalisia omaisuuksia. Tokeneita voidaan käyttää monissa erilaisissa sovelluksissa, kuten hajautetussa rahoitusjärjestelmässä, älykkäissä sopimuksissa, hajautetuissa sovelluksissa ja pelialustoilla. Tokenit luodaan yleensä alustalle, joka käyttää lohkoketjuteknologiaa, ja niitä voidaan myydä julkisesti Initial Coin Offeringin (ICO) tai Token Sale -kampanjan kautta. Tokenien käyttö on yleistynyt viime vuosina lohkoketjujen käytön kasvun myötä.

- Altcoin - Vaihtoehtoinen kryptovaluutta

Altcoin on lyhenne sanoista "alternative coin", eli vaihtoehtoinen kryptovaluutta. Se viittaa kaikkiin Bitcoinin

jälkeen kehitettyihin kryptovaluuttoihin, kuten Ethereum, Litecoin ja Ripple. Altcoineja on satoja erilaisia, ja ne eroavat toisistaan ominaisuuksien, tavoitteiden ja teknologioiden osalta. Vaikka Bitcoin on yhä suurin ja tunnetuin kryptovaluutta, monet sijoittajat ja kauppiaat ovat kiinnostuneita altcoineista niiden potentiaalisen arvonnousun vuoksi.

- Cryptocurrency – Kryptovaluutta

Kryptovaluutta (cryptocurrency) on digitaalinen valuutta, joka käyttää kryptografiaa turvallisuuden takaamiseksi ja uusien yksiköiden luomiseksi. Kryptovaluuttojen toiminta perustuu hajautettuun lohkoketjuteknologiaan, joka mahdollistaa transaktioiden toteuttamisen ilman keskitettyä toimijaa. Kryptovaluuttoja voidaan käyttää ostosten tekemiseen verkossa, mutta niitä voidaan myös pitää sijoituskohteena tai vaihtaa perinteisiin valuuttoihin. Tunnetuimpia kryptovaluuttoja ovat Bitcoin, Ethereum ja Litecoin.

- Gas - Kaasu (Ethereumin lohkoketjussa käytetty termi, joka viittaa transaktioiden

  maksamiseen tarvittavaan määrään Etheriä)

Gas on termi, jota käytetään Ethereum-lohkoketjussa transaktioiden käsittelyn maksamiseen. Jokaisessa Ethereum-verkon transaktiossa käytetään tietty määrä "gasia", joka on maksettava Ethereumin omaa kryptovaluuttaa, eli Etheriä käyttäen. Gas-maksut määräytyvät sen mukaan, kuinka monimutkainen transaktio on, ja kuinka nopeasti sen haluaa vahvistettavan lohkoketjussa. Gas-maksujen tarkoitus on estää

lohkoketjun ruuhkautumista ja estää haitallista käyttöä.

- Merkle Tree - Merklen puu

Merkle-puu on puurakenne, jossa jokainen solmu on yhdistelmä sen lapsisolmujen tiivisteitä, kunnes juurisolmussa on koko puun tiiviste. Merklen puuta käytetään usein lohkoketjujen rakenteissa, koska se mahdollistaa tietojen eheyden ja autentikoinnin tehokkaan tarkistamisen. Se parantaa myös tietojen salauksen tehokkuutta, koska yksittäisten tiivisteiden tarkistaminen on nopeampaa kuin koko lohkon tarkistaminen.

- Hash Rate - Tiivisteen nopeus

Hash rate tarkoittaa lohkoketjun louhinnassa käytetyn tietokoneen suorituskykyä, eli kuinka monta hash-funktiota kone pystyy laskemaan tietyssä ajassa. Hash rate ilmoitetaan yleensä tiivisteen laskentaa kuvaavina yksikköinä, kuten hashia sekunnissa (H/s), kilohashia sekunnissa (kH/s), megahashia sekunnissa (MH/s) tai gigahashia sekunnissa (GH/s). Hash rate on tärkeä tekijä lohkoketjun turvallisuuden kannalta, sillä sitä suurempi hash rate, sitä vaikeampi on hyökätä lohkoketjua vastaan.

- Block Reward - Lohkon palkkio

Lohkon palkkio tarkoittaa kryptovaluutan maksamista lohkon validoinnista ja sen lisäämisestä lohkoketjuun. Kun kaivosprosessi ratkaisee lohkon arvoituksen ja lisää sen

lohkoketjuun, he saavat palkkion kryptovaluuttaa. Lohkon palkkio on yksi tapa kannustaa kaivosprosessia ja ylläpitää lohkoketjua.

- Genesis Block - Alkuperäinen lohko

Genesis Block tarkoittaa lohkoketjun ensimmäistä lohkoa, joka luodaan lohkoketjun käynnistämiseksi. Genesis Blockia ei voida luoda edeltävän lohkon perusteella, koska kyseessä on ensimmäinen lohko. Se luodaan yleensä käsin, ja siihen sisällytetään alkuperäinen kryptovaluutan tarjonta, joka jaetaan lohkon löytäjille palkkiona. Genesis Blockia käytetään lohkoketjun alkuarvona, jota seuraa lohkojen ketju, joka on sidottu edelliseen lohkoon.

- Immutable – Muuttumaton

Immutable tarkoittaa muuttumatonta tai muuttumatonta ominaisuutta. Lohkoketjuteknologiassa tietojen muuttaminen on erittäin vaikeaa tai mahdotonta sen jälkeen, kun ne on tallennettu lohkoon. Tämä tarkoittaa, että lohkoketjujen tietoja pidetään yleensä muuttumattomina ja luotettavina.

- Tokenization – Tokenisointi

Tokenisointi tarkoittaa arvon tai omaisuuden digitalisoimista lohkoketjuun tallennettavaksi muodoksi. Tokenisointi mahdollistaa esimerkiksi perinteisten omaisuuserien, kuten kiinteistöjen tai taideteosten, edustamisen digitaalisina tokeneina lohkoketjussa. Tokenit voivat olla myös erilaisia

kryptovaluuttoja, joita käytetään esimerkiksi palveluiden tai tuotteiden ostamiseen lohkoketjuun liittyvissä sovelluksissa. Tokenisointi helpottaa omaisuuserien kauppaa ja siirtoa, sillä niiden arvo voidaan helposti ja nopeasti siirtää lohkoketjuun tallennettujen tokenien kautta.

- Double Spending

Double spending tarkoittaa tilannetta, jossa digitaalista valuuttaa, kuten kryptovaluuttaa, käytetään kahdesti tai useammin samaan aikaan eri vastaanottajille. Tämä ongelma voidaan ratkaista lohkoketjuteknologian avulla, koska lohkoketju tallentaa jokaisen transaktion historian ja estää siten saman digitaalisen valuutan käytön useampaan kuin yhteen transaktioon.

- Permissioned Blockchain - Luvanvarainen lohkoketju

Permissioned blockchain (luvanvarainen lohkoketju) on lohkoketjuteknologian muoto, jossa osallistujat tunnetaan ja ovat valtuutettuja osallistumaan lohkoketjun toimintaan. Tämä tarkoittaa, että vain tietyt osallistujat, joilla on erityinen lupa, voivat lukea ja kirjoittaa tietoja lohkoketjuun. Permissioned blockchain poikkeaa avoimesta blockchainista, jossa kuka tahansa voi osallistua lohkoketjun toimintaan. Permissioned blockchainia käytetään usein yritystasolla, koska se tarjoaa lisää yksityisyyttä ja valvontaa, mutta samalla rajoittaa lohkoketjun hajauttamisen etuja.

- Permissionless Blockchain - Luvaton lohkoketju

Permissionless Blockchain tarkoittaa lohkoketjua, johon kaikilla käyttäjillä on vapaa pääsy ja mahdollisuus osallistua sen validointiprosessiin. Tämä tarkoittaa, että kuka tahansa voi lukea ja kirjoittaa lohkoketjuun ilman, että siihen tarvitaan lupaa tai valtuutusta keskitetystä tahosta. Bitcoin on esimerkki luvattomasta lohkoketjusta, joka on avoin kaikille käyttäjille, kun taas yritysten sisäiseen käyttöön tarkoitetut lohkoketjut ovat yleensä luvanvaraisia, ja niiden käyttö on rajoitettu tiettyihin organisaatioihin tai henkilöihin.

- Byzantine Fault Tolerance (BFT) - Byzanttilaisen virheen sietokyky

Byzantine Fault Tolerance (BFT) on järjestelmän ominaisuus, joka mahdollistaa sen, että se pystyy toimimaan oikein vaikka siinä olisi viallisia osia tai niitä yritettäisiin sabotoitua. BFT on erityisen tärkeä hajautettujen järjestelmien, kuten lohkoketjujen, toiminnalle, koska niissä on useita solmuja, jotka voivat toimia ilman keskitettyä valvontaa. BFT:n avulla lohkoketjut voivat pitää yllä konsensusta ja estää haitallisten hyökkäysten vaikutukset lohkoketjun toimintaan.

- Zero-knowledge Proof - Zero-knowledge -todistus

Zero-knowledge proof eli suomeksi nolla-tietotodistus on lohkoketjuteknologiassa käytetty menetelmä, jonka avulla voidaan todistaa tiedon olemassaolo tai oikeellisuus ilman, että itse tietoa tarvitsee paljastaa. Zero-knowledge proofin avulla voidaan siis vahvistaa transaktion aitous ilman, että sen tarkka sisältö paljastuu lohkoketjun käyttäjille. Tämä lisää tietoturvaa ja yksityisyyttä lohkoketjuissa.

- Sidechain – Sivuketju

Sidechain, eli sivuketju, on lohkoketjujen käsitteitä, joka tarkoittaa lohkoketjun lohkojen erottamista toisesta lohkoketjusta, joka toimii "pääketjuna". Sivuketjut mahdollistavat lohkoketjun skaalautuvuuden parantamisen ja uusien ominaisuuksien toteuttamisen, sillä ne sallivat lohkoketjujen kehittämisen erillään pääketjun rajoituksista. Sivuketjujen avulla voidaan toteuttaa esimerkiksi uusia lohkoketjusovelluksia tai skaalautuvuutta parantavia ratkaisuja, kuten lohkojen jakamista (sharding) tai tiivistämistä (pruning). Sidechainit voivat olla joko luvattomia (permissionless) tai luvanvaraisia (permissioned) riippuen käyttötarkoituksesta ja käyttäjistä.

- Layering – Kerrostaminen

Lohkoketjujen kerrostaminen (layering) tarkoittaa monikerroksisen arkkitehtuurin käyttöä, jossa jokainen kerros hoitaa erilaisia tehtäviä. Tämä mahdollistaa lohkoketjujen skaalautuvuuden ja tehokkuuden parantamisen, koska jokainen kerros voi käsitellä vain tiettyjä toimintoja sen sijaan, että kaikki toiminnot olisivat yhdessä kerroksessa. Layering on yleinen lähestymistapa monissa hajautetuissa järjestelmissä, mukaan lukien lohkoketjut.

- Scaling – Skaalaaminen

Skaalaaminen (engl. scaling) tarkoittaa lohkoketjujen kapasiteetin kasvattamista, jotta ne pystyvät käsittelemään suurempaa määrää transaktioita ja käyttäjiä. Lohkoketjut tarvitsevat skaalaamista, jotta ne voivat toimia tehokkaasti ja kilpailukykyisesti perinteisiin keskitettyihin järjestelmiin verrattuna. Skalaamisessa voidaan käyttää erilaisia menetelmiä, kuten lohkojen koon pienentämistä, transaktioiden puristamista ja lohkoketjujen kerrostamista.

- Fungible Token - Vaihdettava merkki

Fungible Token on kryptovaluuttatermi, joka viittaa digitaalisiin tokeneihin, jotka ovat keskenään täysin vaihdettavissa ja samanarvoisia. Käytännössä se tarkoittaa, että jokainen yksilöity token on samanarvoinen ja käyttäjille on merkityksellistä vain niiden määrä eikä sen erityinen alkuperä tai historia. Fungible Tokenit ovat tärkeitä lohkoketjujen talousjärjestelmissä, koska ne mahdollistavat helpomman ja sujuvamman kaupankäynnin ja siirrettävyyden. Esimerkkejä Fungible Tokenista ovat Bitcoin, Ethereum ja Litecoin.

- Non-Fungible Token (NFT) - Vaihdettamaton merkki

Non-Fungible Token (NFT) tarkoittaa lohkoketjuteknologialla toteutettua merkkiä, jolla on yksilöllinen tunniste ja arvo. Toisin kuin fungible tokenit, jotka ovat vaihdettavissa keskenään (esim. kryptovaluutat), NFT:t ovat ainutlaatuisia eivätkä ole keskenään vaihdettavissa. NFT:t ovat nousseet suosioon taiteen, musiikin ja pelien maailmassa, sillä ne mahdollistavat ainutlaatuisten ja helposti todennettavien digitaalisten omaisuuserien luomisen ja myynnin lohkoketjussa.

- DeFi - Hajautettu rahoitus (Decentralized Finance)

DeFi on lyhenne sanoista "Decentralized Finance", ja se viittaa hajautettuun rahoitukseen, joka käyttää lohkoketjuteknologiaa. DeFi-palvelut mahdollistavat perinteisten rahoituspalveluiden, kuten lainojen, vakuutusten ja sijoitusten, tarjoamisen hajautetun järjestelmän kautta ilman keskusviranomaisia tai perinteisiä rahoituslaitoksia. DeFi-palvelut käyttävät usein älysopimuksia ja lohkoketjuteknologiaa tarjotakseen avoimia, läpinäkyviä ja turvallisia rahoituspalveluita, joita kuka tahansa voi käyttää.

- DAO - Hajautettu autonominen organisaatio (Decentralized Autonomous Organization)

Hajautettu autonominen organisaatio (DAO, Decentralized Autonomous Organization) on hajautettu organisaatio, joka toimii lohkoketjuteknologian avulla ilman keskitettyä johtoa tai hallitusta. DAO:n päätöksenteko perustuu äänestyksiin, joita hallitaan älysopimuksilla, mikä mahdollistaa osakkeenomistajien demokraattisen osallistumisen päätöksentekoon. DAO:lla on usein tietty tarkoitus, kuten sijoitusten hallinta tai yhteisöllisten projektien tukeminen.

- Interoperability – Yhteentoimivuus

Interoperability tarkoittaa kykyä eri järjestelmien ja teknologioiden yhteistoimivuuteen ja yhteensopivuuteen. Lohkoketjuteknologiassa interoperability tarkoittaa kykyä eri lohkoketjujen väliseen yhteistoimivuuteen, jotta tietojen

siirtäminen ja käyttäminen eri lohkoketjuissa olisi helpompaa ja tehokkaampaa. Tämä on tärkeää lohkoketjuteknologian laajemman käyttöönoton kannalta, koska se mahdollistaa eri lohkoketjujen välisen yhteistyön ja tiedonvaihdon.

- Proof of Burn - Polttamisen todistaminen

Proof of Burn (PoB) on konsensusmekanismi, jossa osallistujat "polttavat" tai tuhoavat kryptovaluutan, jotta he voivat osallistua lohkoketjun päätöksentekoon. Poltettu kryptovaluutta siirtyy pois markkinoilta ja tämä luo niukkuutta, joka lisää sen arvoa. Tämä konsensusmekanismi on vähemmän yleinen ja sitä käytetään yleensä vaihtoehtona Proof of Work - ja Proof of Stake -mekanismeille.

- Stablecoin - Vakaa kryptovaluutta

Stablecoin on kryptovaluutta, jonka arvo on sidottu tiettyyn ulkoiseen omaisuuserään, kuten esimerkiksi fiat-valuuttaan, kullan hintaan tai jonkin muun omaisuusluokan arvoon. Tämän ansiosta stablecoinin arvo ei heittele yhtä paljon kuin muiden kryptovaluuttojen, kuten Bitcoinin. Stablecoinia voidaan käyttää esimerkiksi rahan siirtämiseen kryptovaluutta- ja fiat-valuuttamarkkinoiden välillä ilman, että arvonvaihtelut vaikuttavat liikaa transaktioihin.

- Central Bank Digital Currency (CBDC) - Keskuspankin digitaalinen valuutta.

Central Bank Digital Currency (CBDC) tarkoittaa keskuspankin liikkeelle laskemaa digitaalista valuuttaa, joka on perinteisen käteisvaluutan digitaalinen vastine. CBDC:t ovat keskuspankin myöntämiä, eikä niitä ole luotu hajautetusti kuten kryptovaluuttoja. CBDC:t ovat siis eräänlainen digitaalinen versio perinteisestä käteisvaluutasta, joka voi toimia samalla tavalla, mutta helpottaa rahansiirtoja ja vähentää käteisen käsittelyyn liittyviä kustannuksia. CBDC:t ovat herättäneet kiinnostusta eri maiden keskuspankkien keskuudessa, ja joitakin pilottihankkeita on jo aloitettu.

B. Lisäresurssit ja opiskelumateriaali

Tämä osio on pyhitetty lohkoketjuihin ja kryptovaluuttoihin liittyville lisäresursseille ja opiskelumateriaaleille. Seuraavat lähteet tarjoavat laajasti tietoa aiheesta ja voivat auttaa lukijaa kehittämään ymmärrystä lohkoketjuteknologian toiminnasta, kryptovaluuttojen historiasta ja käytännön sovelluksista.

1. Andreas M. Antonopoulos: Mastering Bitcoin: Unlocking Digital Cryptocurrencies -kirja tarjoaa syvällistä tietoa bitcoin-teknologiasta ja sen toimintaperiaatteista.
2. Vitalik Buterin: Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform -artikkeli tarjoaa yksityiskohtaisen katsauksen Ethereum-teknologiaan ja sen mahdollisuuksiin älysopimuksissa ja hajautetuissa sovelluksissa.
3. Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System -artikkeli esitteli Bitcoinin ja sen

toimintaperiaatteen vuonna 2008.

4. Coindesk on yksi johtavista lohkoketjuihin ja kryptovaluuttoihin liittyvien uutisten ja tiedonlähteiden tarjoajista.
5. Bitcoin Wiki tarjoaa laajan kokoelman artikkeleita ja tietoa bitcoinista ja lohkoketjuteknologiasta yleisesti.
6. Coursera tarjoaa monia ilmaisia ja maksullisia lohkoketjuihin ja kryptovaluuttoihin liittyviä kursseja, jotka tarjoavat käytännön oppimiskokemuksia.
7. Blockchain at Berkeley on yksi maailman johtavista lohkoketjuihin ja kryptovaluuttoihin erikoistuneista opiskelijaryhmistä. Heidän verkkosivuillaan on paljon käytännön oppimateriaaleja ja resursseja.
8. Github on avoimen lähdekoodin ohjelmistokehitysfoorumi, joka tarjoaa laajan valikoiman lohkoketjuihin ja kryptovaluuttoihin liittyviä avoimen lähdekoodin projekteja ja työkaluja.
9. Redditin r/Bitcoin ja r/CryptoCurrency -foorumit ovat hyviä paikkoja löytää ajankohtaista tietoa lohkoketjuista ja kryptovaluutoista, sekä keskustella aiheista muiden käyttäjien kanssa.
10. Youtube on loistava lähde löytää videoita lohkoketjuista ja kryptovaluutoista, ja monet alan asiantuntijat tarjoavat ilmaisia opetusohjelmia ja tutorial-videoita.

9. Loppusanat

Lohkoketjuteknologia on mullistanut nykyaikaisen liiketoiminnan ja talouden toiminnan. Tämä kirja on pyrkinyt tarjoamaan kattavan johdannon lohkoketjuteknologian

perusteisiin, sovelluksiin ja käyttötapoihin. Kirja tarjoaa kattavan ymmärryksen lohkoketjuteknologiasta ja sen käytöstä, sekä sen hyödyistä ja riskeistä.

Lohkoketjuteknologia on edelleen kehittyvä ala, joka luo uusia mahdollisuuksia liiketoiminnan ja talouden toiminnalle. Tämän kirjan tarkoituksena on tarjota perustan ymmärtää lohkoketjuteknologian perusteet ja sen sovellukset, jotta lukijat voivat edetä syvemmälle aiheeseen.

Tämä kirja ei ole ainoa lähde lohkoketjuteknologiasta, vaan ainoastaan yksi monista resursseista. Tämän kirjan lukijoiden kannattaa jatkaa oppimista ja etsiä lisätietoja lohkoketjuteknologiasta ja sen soveltamisesta käytännössä.

Lopuksi haluamme kiittää kaikkia kirjan tekemisessä mukana olleita ihmisiä, sekä lukijoita, jotka ovat valinneet tämän kirjan oppimateriaalikseen. Toivomme, että tämä kirja on tarjonnut lukijoille arvokasta tietoa ja auttanut heitä ymmärtämään paremmin lohkoketjuteknologiaa ja sen mahdollisuuksia tulevaisuudessa.

TAKAKANNEN ESITTELYTEKSTI:

Tämä kirja on kattava opas lohkoketjuteknologian perusteisiin. Se tarjoaa lukijoille yksityiskohtaisen käsityksen lohkoketjujen historiasta, toimintaperiaatteista ja käyttömahdollisuuksista.

Kirja alkaa esittelemällä lohkoketjujen peruskäsitteet ja siirtyy sitten syvemmälle teknisiin yksityiskohtiin, kuten konsensusmekanismeihin, lohkoketjun arkkitehtuuriin, älysopimuksiin ja lohkoketjujen skaalautuvuuteen liittyviin haasteisiin.

Kirja käsittelee myös lohkoketjuteknologian

sovellusmahdollisuuksia eri toimialoilla, kuten rahoituksessa, terveydenhuollossa ja logistiikassa. Lisäksi kirja käsittelee lohkoketjuteknologian käyttöön liittyviä riskejä ja parhaita käytäntöjä.

Kirja on suunnattu kaikille, jotka haluavat ymmärtää lohkoketjuteknologian perusteet, sen potentiaalin ja sen käytön liiketoiminnassa ja innovaatioissa. Kirja sopii hyvin niin aloittelijoille kuin myös asiantuntijoille, jotka haluavat syventää tietämystään lohkoketjuteknologiasta.