Tampereen ammattikorkeakoulu

Yleiskatsaus Ethereumiin ja älykkäisiin sopimuksiin

Ville Ekholm

OPINNÄYTETYÖ
Joulukuu 2023

Tietojenkäsittely
Ohjelmistotuotanto

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittely
Ohjelmistotuotanto

EKHOLM, VILLE:
Yleiskatsaus Ethereumiin ja älykkäisiin sopimuksiin

Opinnäytetyö 36 sivua, joista liitteitä 0 sivua
Joulukuu 2023

Lohkoketjuteknologia on mullistanut digitaalisen tiedon tallennuksen ja jakamisen tavan. Erityisesti Ethereum-ekosysteemi on viime vuosien aikana noussut esiin tarjotessaan alustan älykkäille sopimuksille ja hajautetuille sovelluksille. Muutoksen taustalla on selkeä tarve ymmärtää näiden teknologioiden toimintamekanismeja ja niiden potentiaalista vaikutusta tulevaisuuden digitaalisiin järjestelmiin.

Opinnäytetyön tavoitteena oli tarjota syvällinen ja kattava katsaus Ethereumiin, sen historiaan, päivityksiin ja keskeisiin komponentteihin, kuten Ether-kryptovaluuttaan ja älykkäisiin sopimuksiin. Työssä käytiin läpi Ethereum verkon toimintaa ja kehitystä ja erityisesti Ethereum 2.0 -fuusion vaikutuksia.

Opinnäytetyön tuloksena selvisi, että Ethereum on monimutkainen ja monipuolinen järjestelmä, joka on jatkuvassa muutoksessa. Älykkäät sopimukset, jotka ovat yksi sen keskeisistä komponenteista, mahdollistavat automatisoidun ja luotettavan transaktioiden käsittelyn, minkä vuoksi ne ovat herättäneet suurta kiinnostusta eri toimialoilla. Kehitystyökalujen ja kielten, kuten Solidityn ja Vyperin, ymmärrys on kriittistä näiden sopimusten luomiseksi ja julkaisemiseksi.

Johtopäätöksenä voidaan todeta, että Ethereum saattaa olla merkittävässä roolissa tulevaisuuden digitaalisessa taloudessa. Sen toiminnan ymmärtäminen ja sen tuomat mahdollisuudet voivat olla avainasemassa monien digitaalisten järjestelmien ja liiketoimintamallien innovaatioissa. Opinnäytetyössä on myös esitetty ehdotuksia siitä, miten Ethereumia ja sen komponentteja voidaan kehittää edelleen tehokkaammin ja turvallisemmin.

Asiasanat: ethereum, kryptovaluutta, lohkoketju

ABSTRACT

Tampere University of Applied Sciences
Degree Programme in Business Information Systems
Software Production

EKHOLM, VILLE:
Overview of Ethereum and Smart Contracts

Bachelor's thesis 36 pages, appendices 0 pages
December 2023

Blockchain technology has revolutionized the way digital information is stored and shared, with the Ethereum ecosystem emerging prominently as the platform for smart contracts and decentralized applications.

This work aims to provide an in-depth overview of Ethereum, by focusing on its history, updates, and essential components, such as the Ether cryptocurrency and smart contracts. The study covers the functions and evolution of the Ethereum network, especially the impacts of the Ethereum 2.0 upgrade.

It was discovered that Ethereum is a complex and diverse system undergoing constant change. Smart contracts are a pivotal component, which enable automated and trustworthy transaction processing, which in turn has led to considerable interest across various sectors. A thorough understanding of development tools and languages, such as Solidity and Vyper is crucial for developing and deploying these contracts.

In conclusion, Ethereum may play a significant role in the future of digital economy. Understanding its operations and potential can be significant for innovations in digital systems and business models. The thesis also suggests ways to further develop Ethereum and its components more efficiently and securely.

Key words: ethereum, blockchain, cryptocurrency

SISÄLLYS

ERITYISSANASTO

Lohkoketju	Hajautettu ja turvallinen tietokanta, joka tallentaa transaktiot ketjuksi.
Konsensus	Mekanismi, jonka avulla lohkoketjun osallistujat pääsevät yhteisymmärrykseen verkon tilasta.
DAO	Organisaatio, joka toimii lohkoketjuteknologian varassa ilman keskitettyä ohjausta.
Louhija	Osallistuja Proof of Work -lohkoketjussa, joka ratkaisee matemaattisia ongelmia vahvistaakseen transaktioita ja lisätäkseen uusia lohkoja.
DeFi	Hajautettu rahoitus, joka viittaa rahoitusratkaisuihin lohkoketjuteknologian varassa.
ICO	Alkuperäinen kolikkotarjous, tapa hankkia rahoitusta kryptovaluutan luomiseen.
Kaasu (Gas)	Maksuyksikkö, jota käytetään Ethereum-verkossa kompensoimaan laskentaresurssien käyttöä.
Solmu (Node)	Tietokone, joka osallistuu lohkoketjun verkkoon ja vahvistaa tapahtumia.
NFT	Tulee sanoista Non-Fungible Token. Ainutlaatuinen digitaalinen tunnus, joka edustaa omistajuutta ja todistaa digitaalisen esineen, kuten taiteen, keräilyesineen tai muun digitaalisen omaisuuden yksilöllisyyttä lohkoketjussa.

1 JOHDANTO

Tulevaisuuden taloudessa ja yhteiskunnassa digitaaliset teknologiat näyttelevät yhä keskeisempää roolia. Erityisesti lohkoketjuteknologia on noussut merkittäväksi innovaatioksi, jolla on potentiaalia mullistaa monia perinteisiä toimialoja aina pankkitoiminnasta kiinteistökauppaan. Ethereum, yhtenä johtavista lohkoketjupohjaisista alustoista, on ollut eturintamassa tuomassa näitä muutoksia käytäntöön. Sen tarjoamat älykkäät sopimukset avaavat oven automatisoituun, luotettavaan ja läpinäkyvään digitaaliseen maailmaan.

Ethereum on paitsi teknologinen innovaatio, myös ilmentymä siitä, kuinka yhteiskuntamme voi uudistua digitaalisessa aikana. Sen ymmärtäminen on välttämätöntä paitsi teknologia-alan ammattilaisille, myös yrityksille, sijoittajille ja yksilöille, jotka haluavat pysyä ajan hermolla. Kuitenkin, vaikka Ethereumista on paljon tietoa hajallaan, kokonaisvaltaisen, yksityiskohtaisen ja selkeän lähteen puute on ollut ilmeinen. Tämä työ pyrkii paikkaamaan tuon aukon, tarjoten lukijalleen kattavan yleiskatsauksen Ethereumiin ja sen merkitykseen.

Työ keskittyy ymmärtämään lohkoketjuteknologian roolia nyky-yhteiskunnassa ja selvittämään, miten Ethereum on erottunut tässä kentässä. Se tarkastelee, kuinka Ethereum on kehittynyt vuosien varrella ja pyrkii antamaan kuvan sen tulevaisuuden näkymästä, erityisesti ottaen huomioon Ethereum 2.0 -fuusion. Työ pyrkii myös ymmärtämään älykkään sopimuksen merkitystä ja potentiaalia, sekä tutkimaan, miten se on vaikuttanut ja tulee vaikuttamaan digitaaliseen talouteen ja yhteiskuntaan. Lisäksi työ vertailee Ethereumia muihin kryptovaluuttoihin, erityisesti Bitcoiniin, ja analysoi, mikä tekee siitä ainutlaatuisen. Lopuksi työssä käydään läpi erilaisia kehitystyökaluja ja -käytäntöjä, joiden avulla Ethereum-alustalla voidaan kehittää älykkäitä sopimuksia ja tarkastellaan miten ne vaikuttavat sen ekosysteemiin.

Tavoitteena on tarjota lukijalle kattava ja syvällinen ymmärrys Ethereumista, sen kehityksestä, potentiaalista ja merkityksestä tulevaisuuden digitaalisessa yhteiskunnassa.

2 LOHKOKETJUTEKNOLOGIA

Lohkoketjuteknologia on digitaalinen innovaatio, joka on saanut alkunsa kryptovaluutoista, kuten Bitcoin, ja laajentunut moniin muihin toimialoihin. Se perustuu hajautetun kirjanpitojärjestelmän (distributed ledger) käsitteeseen, jossa digitaaliset tiedot tallennetaan lohkoiksi kutsuttuihin yksiköihin, jotka on liitetty toisiinsa muodostaen ketjun. Lohkoketjun avulla voidaan saavuttaa läpinäkyvyys, pysyvyys ja manipuloinnin kestävyys, mikä tekee siitä erittäin houkuttelevan ratkaisun monille sovelluksille. (Nakamoto 2008.)

Proof of Work (PoW) ja Proof of Stake (PoS) ovat kaksi yleisintä konsensusmekanismia, joita käytetään lohkoketjuissa. Niiden tarkoituksena on mahdollistaa verkon osallistujien yhteisymmärrys sekä estää mahdollinen huijaaminen tai manipulointi.

2.1 Työntodistus (Proof of Work)

Työntodistus eli Proof of Work tai PoW on konsensusalgoritmi, jota käytetään kryptovaluutoissa ja lohkoketjuteknologiassa siirtojen validoimiseen ja uusien lohkojen luomiseen. Käsite esiteltiin ensimmäisen kerran Cynthia Dworkin ja Moni Naorin toimesta vuonna 1993 roskapostin ja palvelunestohyökkäysten torjumiseksi. (Hooda 2023) Myöhemmin, vuonna 2008, Satoshi Nakamoto toteutti Bitcoin-verkon, jonka keskeisenä osana algoritmi toimii. Tämän jälkeen monet muut kryptovaluutat ovat myös alkaneet käyttämään sitä. PoW turvaa verkkoa vaatimalla sen käyttäjiltä, joita kutsutaan louhijoiksi, monimutkaisten matemaattisten ongelmien ratkaisemista, mikä puolestaan validoi verkon sisällä tehtävät valuutan siirrot ja luo uusia lohkoja mikä generoi kryptovaluuttaa. (IBM n.d.)

2.1.1 Työntodistuksen toiminta

Algoritmi perustuu kryptografisiin pulmiin varmistaakseen siirtojen turvallisuuden ja pätevyyden. Nämä pulmat edellyttävät louhijoilta tietyn syötteen löytämistä,

joka yhdistettynä siirtotietoihin tuottaa hajautusarvon, joka on tietyn tavoitteen alapuolella. Tavoite määrittää pulman vaikeuden, ja matalammat tavoitteet tekevät ongelmasta haastavamman ratkaista. (Nakamoto 2008) Tämä prosessi on resurssi-intensiivinen ja vaatii merkittävää laskentatehoa. Tästä johtuen esimerkiksi bitcoinin SHA-256 algoritmiin on kehitetty normaalia näytönohjainta huomattavasti tehokkaampia laskentatehoa omaavia ASIC piirejä. (Hooda 2023.)

Louhijat kilpailevat näiden kryptografisten pulmien ratkaisemisesta, ja ensimmäisenä pulman ratkaissut palkitaan uudella luodulla kryptovaluutalla (esim. Bitcoin). Tätä prosessia, jota kutsutaan louhinnaksi, ei ainoastaan käytetä siirtojen validoimiseen, vaan se tarjoaa myös kannustimen louhijoille omistaa resurssinsa verkon ylläpitämiseen. Mitä enemmän louhijoita liittyy verkkoon, sitä vaikeammaksi pulma muuttuu, mikä varmistaa, että lohkoja luodaan johdonmukaisella nopeudella. (Hooda 2023.)

PoW-mekanismi toimii myös tärkeässä roolissa verkon turvallisuuden ylläpitämisessä ja kaksinkertaisen siirron estämisessä. Vaatimalla louhijoita investoimaan laskentaresursseja kryptografisten pulmien ratkaisemiseen PoW-järjestelmä tekee taloudellisesti kannattamattomaksi hyökkääjälle yrittää hallita yli 50 % verkon louhintatehosta. Tämä johtuu siitä, että tarvittavan laitteiston ja sähkön hankkimiseen liittyvät kustannukset ylittäisivät verkon hyökkäämisestä saatavat potentiaaliset voitot. (Hooda 2023.)

2.1.2 Työntodistuksen hyvät ja huonot puolet

Hyvät puolet

- Turvallisuus: PoW tarjoaa vahvan turvallisuuden lohkoketjuverkoille, tehden järjestelmän kompromisoinnin vaikeaksi.
- Hajauttaminen: PoW edistää hajauttamista antamalla kenelle tahansa riittävien laskentaresurssien omaavalle mahdollisuuden osallistua louhintaprosessiin.
- Kannustimet: Louhijoita palkitaan heidän panoksestaan, mikä kannustaa heitä ylläpitämään verkkoa ja validoimaan siirtoja.

Huonot puolet

- Energiankulutus: PoW vaatii toimiakseen huomattavan määrän sähköä, mikä johtaa suureen energiankulutukseen ja ympäristöhuoliin.
- Keskittymisriskit: Korkeat louhintalaitteiston kustannukset voivat johtaa louhinnan keskittymiseen, koska aloituskustannukset ja tarvittavan infrastruktuurin määrä kasvavat jatkuvasti.
- Skaalautuvuus: PoW-mekanismi voi olla hidas eikä välttämättä pysty käsittelemään suuria siirtomääriä, mikä puolestaan voi johtaa hitaampiin siirtojen vahvistusaikoihin ja kasvaviin siirtomaksuihin.

Työntodistus on edelleen monien lohkoketjuverkkojen kriittinen osa, joka tarjoaa turvallisuutta ja hajauttamista, näistä ehkä tunnetuimpana järjestelmänä on Bitcoin. Sen resurssi-intensiivinen luonne ja skaalautuvuusrajoitukset ovat kuitenkin johtaneet vaihtoehtoisten konsensusmekanismien tutkimiseen. Lohkoketjualueen kehittyessä on vielä nähtävissä, pysyykö PoW hallitsevana konsensusalgoritmina vai jatkavatko vaihtoehtoiset menetelmät kuten Proof of Stake nopeaa kasvuaan ja ennen pitkää ohittavat jo hieman vanhemman PoW järjestelmän omien hyötyjensä kautta. (Hooda 2023.)

2.2 Proof of stake

Proof of Stake (PoS) on lohkoketjuteknologiaan perustuva konsensusmekanismi, joka on kehitetty tarjoamaan vaihtoehto Proof of Work (PoW) -mekanismille. Sen perusperiaatteena on, että sen sijaan, että käytettäisiin laskentatehoa kilpailun kautta, kuten PoW:ssa, lohkoketjun validointi ja päätöksenteko perustuvat osallistujien eli validointisolmujen omistamaan panokseen. Panos on tietty määrä kryptovaluuttaa, jonka validointisolmu on sitonut järjestelmään. PoS sai alkunsa vuonna 2011, kun kryptovaluuttojen varhaiset kehittäjät alkoivat hahmottaa vaihtoehtoisia tapoja saavuttaa konsensus lohkoketjuissa. Sen kehitys alkoi osana pyrkimystä löytää ratkaisu Proof of Work –mekanismin suurimpiin ongelmiin, kuten energiankulutukseen ja keskittymisriskiin. (Hooda 2022.)

2.2.1 Perustoiminta

PoS-mekanismissa lohkojen validointiprosessi, joka tunnetaan myös nimellä "forging" tai "minting", on keskeinen toiminto. Validointisolmut, jotka haluavat osallistua prosessiin, lukitsevat tietyn määrän kryptovaluuttaa panokseksi. Tämä panos antaa validointisolmulle mahdollisuuden päästä validointiin mukaan ja siten saada palkkio, joka on yleensä osa lohkopalkkiosta tai transaktiomaksuista. (Hooda 2022.)

PoS-mekanismissa järjestelmä valitsee validointisolmut satunnaisesti tai painotetusti panoksen mukaan. Yleensä mitä suurempi panos, sitä suurempi todennäköisyys on tulla valituksi seuraavan lohkon validointiin. Kun validointisolmu valitaan, se voi ehdottaa ja validoida seuraavaa lohkoa lohkoketjuun. Muiden validointisolmujen tehtävä on tarkistaa ja hyväksyä ehdotettu lohko ennen kuin se lisätään lohkoketjuun. Tämän prosessin avulla lohkoketjussa voidaan saavuttaa konsensus ilman, että tarvitaan valtavia määriä laskentatehoa. (Hooda 2022.)

2.2.2 PoS hyvät ja huonot puolet

Hyvät puolet

- Energiatehokkuus: PoS-konsensusmekanismi kuluttaa huomattavasti vähemmän energiaa kuin PoW, koska se ei vaadi laskentatehoa lohkojen validointiin. Tämä tekee PoS:sta ympäristöystävällisemmän vaihtoehdon.
- Validointia vaikeampi keskittää: Keskittymisen aikaansaaminen vaatii suurten kryptovaluuttamäärien omistamista ja panostamista. Vaikka tämä on mahdollista, useimmat PoS-järjestelmät on suunniteltu estämään tai vähentämään keskittymistä ja näin varmistamaan järjestelmän turvallisuus ja oikeudenmukaisuus.
- Parempi palkitsemisjärjestelmä: PoS kannustaa osallistujia investoimaan ja järjestelmään panostamalla siihen kryptovaluuttaa. Tämä palkitsemisjärjestelmä on tasapuolisempi ja todella paljon helpommin lähestyttävä.

- Skaalautuvuus: Skaalautuvuutta pystytään hallitsemaan ja tehostamaan paremmin PoS:n avulla, mikä parantaa järjestelmän käyttöä suuremmassa mittakaavassa.

Huonot puolet

- Nothing at Stake -ongelma: Tässä ongelmatilanteessa validointisolmut voivat yrittää validoida useita kilpailevia lohkoketjuja samanaikaisesti ilman suuria taloudellisia riskejä, mikä voi johtaa turvallisuusongelmiin ja haitata konsensuksen saavuttamista.
- Long-range attacks: Hyökkääjä voi yrittää uudelleenkirjoittaa lohkoketjun historian käyttämällä vanhoja avaimia, jotka ovat aikaisemmin omistaneet suuren määrän kryptovaluuttaa. Tämä voi johtaa esimerkiksi kaksoiskulutukseen.
- Varallisuuden keskittyminen: Suurempien panosten omistajat voivat saada enemmän validointimahdollisuuksia, mikä voi johtaa varallisuuden keskittymiseen tietyille tahoille.

Yhteenvetona voidaan todeta, että Proof of Stake on konsensusmekanismi, joka eroaa Proof of Work -mekanismista perustuen osallistujien panokseen, eikä laskentatehoon. Siinä validointisolmut lukitsevat panoksen, joka antaa tarjoaa mahdollisuuden osallistua lohkojen validointiin. Järjestelmä valitsee validointisolmut satunnaisesti tai painotetusti panoksen mukaan, valitut solmut voivat ehdottaa, validoida ja hyväksyä lohkoja lohkoketjuun. Järjestelmä tarjoaa useita etuja PoW:hen verrattuna, kuten vähentyneen energiankulutuksen ja paremman palkitsemisjärjestelmän. Sitä myös kehitetään todella aktiivisesti mm. Ethereumin toimesta, joka on kirjoitus hetkellä suosituin PoS-järjestelmän omaava kryptovaluutta. (Hooda 2022.)

3 MIKÄ ON ETHEREUM?

Ethereum on noussut nopeasti yhdeksi maailman merkittävimmistä ja vaikutusvaltaisimmista lohkoketjuteknologioista. Sen luoma avoin ja hajautettu ekosysteemi on muuttanut käsitystämme digitaalisista valuutoista, älykkäistä sopimuksista ja hajautetuista sovelluksista. Ethereum ei ole vain digitaalinen valuutta vaan se on ennen kaikkea alusta, joka tarjoaa monipuoliset työkalut kehittäjille ja yhteisöille, jotka haluavat luoda ja toteuttaa hajautettuja sovelluksia ja älykkäitä sopimuksia. (Buterin 2023.)

3.1 Ethereumin historia

Vuonna 2013 19-vuotias venäläis-kanadalainen ohjelmoija nimeltä Vitalik Buterin julkaisi valkoisen kirjan, jossa hän kertoi näkemyksestään uudesta lohkoketju alustasta nimeltä Ethereum. Buterin, joka oli ollut mukana Bitcoin-yhteisössä vuodesta 2011, oli turhautunut ensimmäisen sukupolven lohkoketjun rajoituksiin. Bitcoinin ensisijainen tarkoitus oli mahdollistaa vertaisverkossa toteutuvat digitaaliset siirrot, mutta sen taustalla oleva teknologia ei sallinut paljon mukauttamista tai soveltamista muihin käyttötarkoituksiin. (Buterin 2023.)

Buterin (2023) visio Ethereumin kohdalla oli luoda alusta, joka voisi tukea paitsi kryptovaluuttoja, myös laajaa valikoimaa hajautettuja sovelluksia ja älykkäitä sopimuksia. Nämä innovaatiot tarjoaisivat kehittäjille mahdollisuuden luoda itseään toteuttavia sopimuksia ja sovelluksia, jotka toimivat Ethereum-lohkoketjussa.

3.1.1 Ethereumin alkuperäinen kolikkotarjous (ICO)

Ethereum-valkoisen kirjan julkaisemisen jälkeen joukko kehittäjiä, mukaan lukien Gavin Wood, Charles Hoskinson ja Joseph Lubin, liittyivät Buterinin tiimiin toteuttamaan hänen visiotaan. Yhdessä he perustivat Ethereum-säätiön, joka oli voittoa tavoittelemattoman organisaatio minkä pohjimmainen tarkoitus oli keskittyä Ethereum alustan kehittämiseen. (Cryptopedia 2022.)

Rahoittaakseen projektin Ethereum-säätiö järjesti alkuperäisen kolikkotarjouksen (ICO) heinäkuussa 2014. Tämän avulla sijoittajat saivat ostaa Bitcoinilla Etheriä, Ethereumin natiivia kryptovaluuttaa. ICO oli valtava menestys, ja se keräsi yli 18 miljoonaa dollaria, mikä teki siitä yhden historian menestyksekkäimmistä joukkorahoitustapahtumista tuolloin. Tämä taloudellinen tuki tarjosi resurssit, jotka olivat tarpeen Ethereumin alustan kehittämiseen ja käyttöönottoon. (Cryptopedia 2022.)

3.1.2 Ethereumin käynnistys

Vain vuoden kestäneen kehitys- ja testaustyön jälkeen Ethereum-alusta otettiin käyttöön 30. heinäkuuta 2015 Frontier-verkon julkaisun myötä. Tämä merkitsi Ethereumin lohkoketjun alkua, josta on sen jälkeen tullut vauras ekosysteemi hajautettujen sovellusten ja älykkäiden sopimusten tukemiseksi. (Ethereum 2023.)

3.2 Ethereumin päivitykset vuosien varrella

Ethereumin jatkuvasti kasvava suosio ja käyttöönotto ovat johtaneet useisiin merkittäviin päivityksiin sen julkaisun jälkeen vuonna 2015. Näiden päivityksien tarkoitus on ollut pyrkiä parantamaan alustan suorituskykyä, turvallisuutta ja energiatehokkuutta. (Ethereum 2023.)

3.2.1 Homestead (2016)

Homestead oli ensimmäinen merkittävä Ethereum-päivitys, joka julkaistiin maaliskuussa 2016. Tämä päivitys toi mukanaan parannuksia alustan turvallisuuteen ja vakauteen. Homestead sisälsi myös useita uusia ominaisuuksia, kuten uusia ohjelmointikieliä ja työkaluja kehittäjille, mikä puolestaan auttoi luomaan entistä monipuolisempia ja kehittyneempiä sovelluksia alustalle. (Ethereum 2023.)

3.2.2 Byzantium

Byzantium julkaistiin lokakuussa 2017 ja se oli osa Ethereumin laajempaa Metropolis-vaihetta. Tämä päivitys sisälsi useita merkittäviä parannuksia Ethereum-verkon turvallisuuteen, skaalautuvuuteen ja toimivuuteen. Erityisesti Byzantium esitteli zk-SNARKs-tekniikkaa, joka mahdollisti paremman yksityisyyden suojaamisen älykkäissä sopimuksissa. Lisäksi päivitys paransi lohkopalkkioiden ja transaktiokäsittelyiden tehokkuutta. (Ethereum 2023.)

3.2.3 Constantinople

Constantinople-päivitys julkaistiin helmikuussa 2019 ja se toi mukanaan joukon teknisiä parannuksia Ethereum-verkon tehokkuuden ja taloudellisuuden optimoimiseksi. Tämä päivitys sisälsi useita EIP (Ethereum Improvement Proposals) -ehdotuksia, jotka keskittyivät lohkoketjun energiatehokkuuteen, kaasun kustannuksiin ja kehittäjien työkalujen parantamiseen. Constantinople auttoi myös valmistelemaan Ethereumin siirtymistä kohti Proof of Stake (PoS) -järjestelmää, joka tunnetaan myös nimellä Ethereum 2.0 tai Ethereum merge. (Ethereum 2023.)

3.2.4 Istanbul

Istanbul-päivitys julkaistiin joulukuussa 2019 ja se toi mukanaan useita parannuksia Ethereum-verkon skaalautuvuuteen sekä yhteensopivuuteen muiden lohkoketjujen kanssa. Tämä päivitys sisälsi muun muassa parannuksia älykkäiden sopimusten käsittelyyn, kaasun kustannusten optimointiin ja yksityisyyden parantamiseen. Istanbul auttoi myös lisäämään Ethereumin kykyä integroitua muihin lohkoketjuihin, esimerkiksi Zcashin ja Ethereum Classicin kaltaisten kryptovaluuttojen kanssa. (Ethereum 2023.)

3.2.5 London

London-päivitys julkaistiin elokuussa 2021 ja se oli erityisen merkittävä EIP-1559-ehdotuksen ansiosta, joka muutti tapaa, jolla Ethereum-verkossa käsitellään kaasumaksuja. Päivitys otti käyttöön uuden mekanismin, joka polttaa osan kaasumaksuista jokaisessa lohkossa, mikä vähentää Ether kryptovaluutan kokonaismäärää. Tämän päivityksen tavoitteena oli parantaa Ethereumin käyttäjäkokemusta ja tehokkuutta. (Ethereum 2023.)

3.3 Ethereumin fuusio (Ethereum 2.0)

Syyskuussa 2022 Ethereum, toiseksi suurin lohkoketjuverkosto, koki yhden merkittävimmistä päivityksistään - Merge-päivityksen. Tämä hetki oli kriittinen ja pitkään odotettu Ethereumin monivaiheisessa päivityssuunnitelmassa. Se tarkoituksena oli parantaa verkon skaalautuvuutta, turvallisuutta ja kestävyyttä. Merge merkitsi myös Ethereumin siirtymistä PoS -mekanismiin, muuttaen tehokkaasti tapaa, jolla uudet lohkoketjun lohkot vahvistetaan ja lisätään lohkoketjuun. (Ethereum Merge 2023.)

3.3.1 Fuusion ymmärtäminen

Merge oli kauan odotettu päivitys, joka yhdisti lopulta Ethereum 1.0:n ja Ethereum 2.0:n. Ethereum 1.0, oli alkuperäinen Ethereum-lohkoketju, joka toimi PoW-konsensusmekanismilla, joka perustui energiaa vaativaan louhintaan transaktioiden vahvistamiseksi ja verkon turvaamiseksi. Ethereum 2.0 puolestaan esitteli PoS-mekanismin, jonka avulla validointiin osallistuvat voivat turvata verkon panostamalla Ether tokeninsa sen sijaan, että käyttäisivät laskentatehoa.

Yhdistämällä kaksi verkkoa Ethereumista tuli yksi, skaalautuvampi ja energiatehokkaampi lohkoketju. Merge mahdollisti verkon säilyttävän olemassa olevat älykkäät sopimukset, hajautetut sovellukset ja token-ekosysteemin samalla hyötyen Ethereum 2.0:n tuomista parannuksista. (Ethereum Merge 2023.)

3.3.2 Fuusion vaikutukset

Yksi merkittävimmistä Merge-päivityksen eduista on energiankulutuksen väheneminen. Ethereum 1.0:n käyttämä PoW-mekanismi vaati valtavasti laskentatehoa ja energiaa, mikä aiheutti ympäristöhuolia. Siirtymällä PoS-mekanismiin Ethereumin energiankulutus laski dramaattisesti, tehden verkosta ympäristöystävällisemmän ja kestävämmän.

Ethereumin käyttöön ottama PoS-mekanismi tarjosi vahvemman turvallisuuden verkossa. Validointiin osallistuvat valitaan ehdottamaan uusia lohkoja sen perusteella, kuinka paljon he ovat panostaneet tokeneitaan ja muiden tekijöiden perusteella, mikä vähentää haitallista käyttäytymistä. Useampien validointiin osallistuvien mukana ollessa Ethereum muuttuu hajautetummaksi ja turvallisemmaksi. (Ethereum Merge 2023.)

Merge loi pohjan skaalautuvuuden parantamiselle entisestään. PoS-mekanismin avulla Ethereum voi nyt ottaa käyttöön sirpaloinnin (sharding), joka jakaa verkon pienempiin osiin, niin sanottuihin sirpaleisiin. Jokainen sirpale voi käsitellä transaktioita ja älykkäitä sopimuksia itsenäisesti, mikä lisää verkon kokonaistehokkuutta. (Ethereum Merge 2023.)

Päivitys avasi myös mahdollisuuksia passiivisen tulon lähteisiin Ethereum-tokenien haltijoille panostuksen kautta. Validointiin osallistuvat, jotka panostavat ETH-tokeninsa ja osallistuvat verkon turvaamiseen, palkitaan uusilla ETH-tokeneilla. Tämä kannustinjärjestelmä rohkaisee käyttäjiä panostamaan tokeneitaan, mikä lisää entisestään verkon turvallisuutta. (Ethereum Merge 2023.)

3.3.3 Tulevat vaikutukset ja kehitykset

Onnistunut siirtyminen PoS-mekanismiin avaa tien lisäpäivityksille, kuten sirpaloinnille ja roll-upeille, jotka lisäävät entisestään Ethereumin skaalautuvuutta ja ratkaisevat nykyisiä rajoituksia.

Ethereumin kehittyessä jatkuvasti odotetaan, että verkosto houkuttelee lisää kehittäjiä, käyttäjiä ja sijoittajia, vahvistaen asemaansa johtavana lohkoketjualustana hajautettujen sovellusten ja älykkäiden sopimusten alalla. Lisäksi vähentyneen energiankulutuksen ja ympäristöystävällisyyden ansiosta Ethereumista tulee entistä houkuttelevampi ympäristötietoisille organisaatioille ja yksilöille.

Merge luo myös pohjan Ethereumin jatkuvalla matkalla kohti täysin hajautettua ja itseohjautuvaa verkostoa. Ethereum-parannusehdotus (EIP) -prosessi, joka mahdollistaa yhteisölähtöiset päivitykset, jatkaa kriittistä roolia alustan kehityksessä. Tämä avoimen lähdekoodin lähestymistapa varmistaa, että Ethereum-verkosto pysyy innovatiivisena ja sopeutuu käyttäjiensä tarpeisiin. (Ethereum Merge 2023.)

Yksi odotetuimmista Mergeä seuraavista kehityksistä on Ethereum WebAssemblyn (eWASM) esittely, uusi suoritusmoottori, joka on suunniteltu korvaamaan Ethereum-virtuaalikone (EVM). Sen odotetaan parantavan suorituskykyä ja yhteensopivuutta eri alustojen välillä, mikä helpottaa kehittäjiä luomaan ja käyttöönottamaan älykkäitä sopimuksia. (Ivanontech 2021.)

Toinen lupaava kehitys on nollatietojen todistuksiin ja yksityisyyden ratkaisuihin liittyvä jatkuva tutkimus. Nämä teknologiat saattavat merkittävästi parantaa Ethereumin verkoston transaktioiden yksityisyyttä ja turvallisuutta, houkutellen lisää käyttäjiä ja kehittäjiä, jotka etsivät turvallisia ja yksityisiä ratkaisuja hajautettuihin sovelluksiin. (Ethereum Merge 2023.)

3.4 Kryptovaluutta Ether

Ether (ETH) on Ethereumin lohkoketjun alkuperäinen kryptovaluutta. Se on digitaalinen valuutta, joka kiihdyttää toimintoja Ethereum-verkossa toimien sekä arvovarastona että vaihdon välineenä. Markkina-arvoltaan toiseksi suurimpana kryptovaluuttana Ether on saavuttanut merkittävää huomiota ja omaksumista vuosien varrella.

3.4.1 Ether kaasuna

Yksi Etherin kriittisimmistä rooleista on toimia "kaasuna" Ethereum-verkossa. Kaasu on mittaustapa, jota käytetään resurssien jakamiseen Ethereum-lohkoketjussa älykkäiden sopimusten ja transaktioiden suorittamiseen. Kun käyttäjä lähettää transaktion tai aloittaa älykkään sopimuksen, hänen on maksettava tietty määrä Etheriä kaasumaksuina. Nämä maksut vaaditaan korvaamaan kaivostyöläiset tai validointivastaavat, jotka käsittelevät ja turvaavat verkon. (Frankenfield 2022.)

Kaasumaksut määräytyvät tarjonnan ja kysynnän dynamiikan sekä suoritettavien toimintojen monimutkaisuuden perusteella. Tämä tarkoittaa, että monimutkaisemmat transaktiot tai älykkäät sopimukset vaativat enemmän kaasua ja siten myös enemmän Etheriä suorituksen saavuttamiseksi. (Frankenfield 2022.)

3.4.2 Ether sijoituskohteena

Etheristä on tullut houkutteleva sijoituskohde niin yksityishenkilöille kuin instituutioillekin, koska sen arvo on kasvanut huomattavasti sen perustamisesta lähtien. Sijoittajat saattavat pitää Etheriä potentiaalisena arvonsäilyttäjänä ja vaihtoehtona perinteisille omaisuusluokille, kuten osakkeille tai kullalle. On kuitenkin tärkeää huomata, että Etherin hinta voi olla erittäin volatiilinen, ja sijoittajien tulisi olla tietoisia riskeistä, jotka liittyvät kryptovaluuttoihin sijoittamiseen.

3.4.3 Miten hankkia ja säilyttää Etheriä

Etherin hankkimiseen on useita tapoja:

- Osta Etheriä kryptovaluuttapörssistä: Käyttäjät voivat ostaa Etheriä käyttämällä fiat-valuuttaa (esim. USD, EUR) tai muita kryptovaluuttoja, kuten Bitcoinia, erilaisilla verkkopörsseillä. Joitakin suosittuja pörssejä ovat Coinbase, Binance ja Kraken.

- Ansaitse Etheriä staking-menetelmällä: Ethereum-verkossa validointeja suorittavat tahot saavat Etheriä palkkiona tapahtumien validoinnista ja verkon turvaamisesta. Kaikki verkon käyttäjät voivat vapaasti osallistua tähän prosessiin. Se edellyttää vain jo olemassa olevan Etherin omistusta.
- Hyväksy Etheriä maksuna tavaroista tai palveluista: Yritykset ja yksityishenkilöt voivat valita hyväksyvänsä Etheriä maksuna tuotteistaan tai palveluistaan. Tämä voidaan tehdä perustamalla Ethereum-lompakko ja antamalla asiakkaille lompakon osoite maksujen lähettämistä varten.

Kun Ether on hankittu, se tulisi säilyttää turvallisesti Ethereum-lompakossa. Lompakot voivat olla ohjelmistopohjaisia, laitepohjaisia tai kolmannen osapuolen hallinnoimia. Ohjelmistopohjaiset lompakot ovat sovelluksia, jotka asennetaan tietokoneelle tai mobiililaitteelle, kun taas laitepohjaiset lompakot ovat fyysisiä laitteita, jotka säilyttävät yksityisavaimet offline-tilassa. Kolmannen osapuolen hallinnoimat lompakot säilyttävät yksityisavaimet käyttäjän puolesta. Kullakin lompakkotyypillä on omat hyvät ja huonot puolensa, joten käyttäjien tulisi tutkia ja valita lompakko, joka parhaiten sopii heidän tarpeisiinsa. (Buy Ethereum 2023.)

3.5 Erot Bitcoinin ja Ethereumin välillä

Ethereum ja Bitcoin edustavat kahta tunnetuinta näkemystä siitä, miten toteuttaa kryptovaluutta ja sen lohkoketjujärjestelmä. Bitcoinin pääasiallinen tarkoitus on toimia digitaalisena valuuttana, joka tarjoaa hajautetun ja turvallisen arvonsäilytystavan ja vaihtovälineen. Ethereum puolestaan keskittyy älysopimusten ja hajautettujen sovellusten ekosysteemin kehittämiseen, mikä luo monipuolisemman ja laajemman käyttöalueen. Konsensusmekanismeissa, inflaatiossa ja tarjonnan rajoituksissa näiden kahden kryptovaluutan välillä on merkittäviä eroja, jotka vaikuttavat niiden käyttökohteisiin, arvoon ja yleiseen kiinnostukseen markkinoilla. (Bitcoin&Ethereum 2023.)

Lopulta sekä Ethereum että Bitcoin ovat tärkeitä osia kryptovaluuttamaailmassa, ja niillä on omat vahvuutensa ja heikkoutensa. Sijoittajien ja käyttäjien on syytä

tutustua näiden kryptovaluuttojen eroihin ja ymmärtää niiden taustalla olevat teknologiat, jotta he voivat tehdä informoituja päätöksiä niiden käytöstä ja sijoitus mahdollisuuksista. (Bitcoin&Ethereum 2023.)

3.5.1 Tarkoitus ja tavoitteet

Ensimmäinen ja merkittävin ero Ethereumissa ja Bitcoinissa on niiden perustamisen tarkoitus ja tavoitteet. Bitcoin syntyi vuonna 2008, kun henkilö tai ryhmä, joka käytti nimimerkkiä "Satoshi Nakamoto", julkaisi Bitcoinia käsittelevän asiakirjan. Bitcoinin tärkein tavoite oli tarjota hajautettu digitaalinen valuutta, joka mahdollistaa nopeat ja turvalliset rahansiirrot ilman keskuspankkien tai hallitusten väliintuloa. (Bitcoin&Ethereum 2023.)

Ethereum lanseerattiin vuonna 2015 kehittäjänsä Vitalik Buterinin toimesta. Sen tavoitteena ei ollut vain tarjota digitaalista valuuttaa vaan myös mahdollistaa älykkäiden sopimusten luominen ja hajautettujen sovellusten kehittäminen. Älykkäät sopimukset ovat itseohjautuvia sopimuksia, jotka toteutetaan automaattisesti, kun niiden ehdot täyttyvät. (Bitcoin&Ethereum 2023.)

3.5.2 Tekninen rakenne

Vaikka molemmat kryptovaluutat perustuvat lohkoketjuteknologiaan, niiden tekninen rakenne on hyvin erilainen. Bitcoinin lohkoketju koostuu transaktioista, jotka vahvistetaan ja lisätään lohkoketjuun louhijoille suorittaman työn todisteeksi Proof-of-Work-algoritmin avulla. Bitcoinin lohkoketju on suunniteltu yksinomaan rahansiirtojen tallentamiseen. (Bitcoin&Ethereum 2023.)

Ethereum käyttää Proof of Stake –algoritmia ja sen lohkoketju koostuu älykkäistä sopimuksista ja niitä tukevista Ethereum Virtual Machine -koodinpätkistä. Tämä mahdollistaa monimutkaisten sovellusten ja sopimusten luomisen, toisin kuin Bitcoinin yksinkertaisempi rakenne. (Bitcoin&Ethereum 2023.)

3.5.3 Inflaatio ja tarjonta

Bitcoinilla on rajallinen tarjonta, joka on suunniteltu olemaan enintään 21 miljoonaa kolikkoa. Tämän rajallisen tarjonnan ansiosta monet pitävät Bitcoinia digitaalisena kullan kaltaisena arvonsäilyttäjänä. Bitcoinin inflaatio hidastuu ajan mittaan ja viimeinen kolikko arvioidaan louhittavaksi noin vuonna 2140.

Ethereumilla ei ole samanlaista rajallista tarjontaa ja siihen on päivityksen myötä tehty ominaisuus, joka vähentää uusien Ether-kolikoiden syntyä ja polttaa osan käyttömaksuista. Tämän ansiosta Ethereumin inflaatio on muuttunut niin, että sen tarjonta vähenee ajan myötä.

3.5.4 Käyttötarkoitukset

Bitcoinin pääasiallinen käyttötarkoitus on digitaalisen valuutan rooli, jossa sitä käytetään arvon säilyttämiseen, siirtämiseen ja vaihtoon. Monet yritykset ja yksityishenkilöt hyväksyvät sen maksuvälineenä, ja se on usein kryptovaluuttojen "portti" aloitteleville sijoittajille.

Ethereum on paljon monipuolisempi ja sen käyttötarkoituksiin kuuluu esimerkiksi älykkäiden sopimusten luominen, hajautettujen sovellusten kehittäminen, pankeista riippumattomat hajautetun finanssimaailman palvelut ja NFT-markkinat. Vaikka Etherillä on myös valuuttana keskeinen arvonsiirron rooli, se on enemmänkin digitaalisen ekosysteemin polttoaine kuin pelkkä valuutta. (Bitcoin&Ethereum 2023.)

4 ETHEREUM: ÄLYKKÄÄT SOPIMUKSET

Ethereumin erityispiirteenä digitaalisessa maailmassa on sen kyky luoda ja hallita älykkäitä sopimuksia. Vaikka useimmat ovat tulleet tuntemaan Ethereumin lohkoketjuna ja kryptovaluuttana, se on älykkäiden sopimusten alusta, joka on mullistanut tapamme ymmärtää ja käsitellä digitaalisia sopimuksia. Tämän innovaation myötä on mahdollista automatisoida monimutkaisia prosesseja, lisätä läpinäkyvyyttä ja luottamusta sekä vähentää kustannuksia ja virheitä. (Ethereum smart contracts 2023.)

4.1 Mikä on älykäs sopimus?

Älykäs sopimus on itseohjautuva, itsenäisesti toteutuva sopimus, jonka ehdot on kirjoitettu tietokonekoodina. Se perustuu lohkoketjuteknologiaan, joka mahdollistaa sopimuksen osapuolille automaattisen ja läpinäkyvän transaktioiden toteutuksen ilman välikäsiä. Älykkäät sopimukset voivat automatisoida monimutkaisia prosesseja, vähentää kustannuksia ja virheitä sekä estää petoksia. (Ethereum smart contracts 2023.)

4.1.1 Tekninen toteutus ja lohkoketjun hyödyntäminen

Teknisesti älykäs sopimus on itseään toteuttava koodi, joka on tallennettu lohkoketjuun. Tämän koodin avulla voidaan luoda ja hallita digitaalisia sopimuksia, joita ei voida muuttaa jälkikäteen ilman kaikkien osapuolten suostumusta. Lohkoketjun avulla älykkäät sopimukset saavuttavat pysyvyyden ja hajautetun konsensuksen, mikä tarkoittaa, että niiden toiminta on avointa ja läpinäkyvää.

Älykkäiden sopimusten käyttökohteita on monia, ja ne voivat mullistaa perinteisiä liiketoimintaprosesseja, kuten sopimusten allekirjoittamista, äänestystä tai omaisuuden hallintaa. Älykkäitä sopimuksia voidaan käyttää esimerkiksi automaattisesti lunastamaan vakuutuskorvauksia, jakamaan osinkoja osakkeenomistajille tai hallitsemaan toimitusketjuja. Koska älykkäät sopimukset toimivat automaatti-

sesti ja läpinäkyvästi, ne voivat vähentää väärinkäytöksiä, petoksia ja kustannuksia sekä parantaa tehokkuutta ja luottamusta eri osapuolten välillä. (Ethereum smart contracts 2023.)

4.1.2 Kryptografiset allekirjoitukset ja aikaleimat

Älykkäät sopimukset käyttävät lohkoketjun ominaisuuksia, kuten kryptografisia allekirjoituksia, transaktioiden aikaleimoja ja monimutkaisia loogisia toimintoja. Kryptografiset allekirjoitukset tarjoavat turvallisuutta ja luotettavuutta, sillä ne varmistavat, että vain oikeutetut osapuolet voivat tehdä muutoksia sopimukseen. Transaktioiden aikaleimat puolestaan tarjoavat yksiselitteisen aikajärjestyksen tapahtumille, mikä auttaa estämään petoksia ja kaksoiskulutusta. (Ethereum smart contracts 2023.)

4.1.3 Loogiset ehdot ja toiminnot

Älykkäät sopimukset sisältävät usein loogisia ehtoja ja toimintoja, jotka aktivoituvat, kun tiettyjä edellytyksiä täyttyy. Esimerkiksi, älykäs sopimus voi sisältää ehdot, jotka määräävät, milloin ja minkälaisissa olosuhteissa varat siirtyvät osapuolelta toiselle. Näitä ehtoja voidaan toteuttaa erilaisten loogisten rakenteiden avulla, kuten if-lausekkeiden, silmukoiden ja funktioiden avulla. Esimerkiksi, älykäs sopimus voi sisältää ehdot, jotka määräävät, että varat siirtyvät myyjältä ostajalle vain, jos ostaja on maksanut sovitun summan ja myyjä on toimittanut tuotteen. (Ethereum smart contracts 2023.)

4.1.4 Hajautettu rakenne

Älykkäät sopimukset ovat hajautettuja, mikä tarkoittaa, että ne eivät ole riippuvaisia keskitetystä tahosta, kuten pankista tai viranomaisesta. Sen sijaan ne toimivat hajautetulla verkostolla, jossa jokainen solmu säilyttää kopion sopimuksesta.

Tämä hajautettu rakenne tekee älykkäistä sopimuksista vastustuskykyisiä vikoihin, manipulointiin ja petoksiin.

4.1.5 Turvallisuus ja luotettavuus

On syytä huomata, että älykkäiden sopimusten turvallisuus ja luotettavuus riippuvat siitä, miten hyvin ne on suunniteltu ja toteutettu. Virheellisesti laadittu älykäs sopimus voi olla altis hyökkäyksille, ja siinä voi esiintyä ei-toivottuja toimintoja. Siksi älykkäiden sopimusten kehittämiseen ja auditointiin tulee kiinnittää erityistä huomiota. Sopimusten auditointiin löytyy tänä päivänä erikoistuneita yrityksiä, joiden avulla kehittäjä pystyy varmistamaan sopimuksen toimivuuden ja kartoittamaan mahdollisia haavoittuvuuksia. (Ethereum smart contracts 2023.)

4.2 Olemassa olevia älykkäitä sopimuksia ja niiden käyttökohteita

Ethereum on yksi suosituimmista alustoista älykkäiden sopimusten kehittämiseen ja toteuttamiseen. Sen keskeinen ominaisuus on hajautettu sovelluskehys (dApp), joka mahdollistaa kehittäjien luoda ja hallita turvallisia, hajautettuja sovelluksia. Alla on listattuna muutamia esimerkkejä olemassa olevista älykkäistä sopimuksista.

4.2.1 MakerDAO

MakerDAO on hajautetun rahoituksen (DeFi) protokolla, joka mahdollistaa luottamuksellisen ja vakuudellisen lainanannon. Sen avulla käyttäjät voivat luoda DAI-stabiilirahaa, joka on sidottu Yhdysvaltain dollariin. MakerDAO käyttää älykkäitä sopimuksia hallitsemaan vakuuksien lukitsemista ja lainanantoprosessia.

Tämän lisäksi MakerDAO:n ekosysteemi tarjoaa käyttäjille mahdollisuuden osallistua hallintoon ja päättää tulevista muutoksista, kuten vakuuksien tyyppien lisäämisestä tai korkojen muokkaamisesta. Näin ollen MakerDAO edistää ha-

jautettua ja avointa rahoitusmallia, joka pyrkii vähentämään perinteisten rahoituslaitosten aiheuttamaa keskitettyä riskiä ja tarjoaa käyttäjille enemmän valtaa ja joustavuutta. (MakerDAO n.d)

4.2.2 Uniswap

Uniswap on hajautettu kryptovaluuttapörssi (DEX), joka perustuu Ethereum-alustalle. Se käyttää automaattista markkinatakaajaa (AMM) ja likviditeettialtaita varmistaakseen jatkuvan kaupankäynnin. Uniswapin toiminta perustuu älykkäisiin sopimuksiin, jotka hallitsevat likviditeetin tarjoamista ja kaupankäyntiä. (Uniswap n.d)

Yksi Uniswapin merkittävistä eduista verrattuna perinteisiin keskitettyihin pörsseihin on sen avoimuus ja hajautettu luonne. Tämä tarkoittaa, että kuka tahansa voi osallistua likviditeetin tarjoamiseen ja hyötyä siitä ansaitsemalla transaktiokuluja käyttäjien tekemistä kaupoista. Lisäksi Uniswapin käyttäjät voivat käydä kauppaa ilman, että heidän täytyy luottaa kolmansiin osapuoliin tai rekisteröityä mihinkään palveluun. Tämä parantaa käyttäjien yksityisyyttä ja turvallisuutta kryptovaluuttamarkkinoilla. (Uniswap n.d)

5 ÄLYKKÄIDEN SOPIMUSTEN KEHITYS

5.1 Solidity

Solidity on korkean tason ohjelmointikieli, joka on suunniteltu erityisesti älykkäiden sopimusten kehittämiseen Ethereum-lohkoketjuun. Se tarjoaa kehittäjille työkaluja ja rakenteita, joiden avulla he voivat rakentaa turvallisia ja tehokkaita sopimuksia, jotka hyödyntävät lohkoketjun ominaisuuksia.

Syntaksiltaan Solidity muistuttaa JavaScriptiä ja muita C-tyylisiä ohjelmointikieliä, mikä tekee siitä helpon omaksua ja oppia niille, jotka ovat jo tuttuja muiden ohjelmointikielten kanssa. (Solidity 2023.)

5.1.1 Ominaisuudet

Älykäs sopimus on ohjelmakoodia, joka suoritetaan lohkoketjun päällä. Solidityn keskeinen rakenne on sopimus, joka on samanlainen kuin luokka perinteisissä ohjelmointikielissä. Sopimus sisältää muuttujia, funktioita ja tapahtumia, jotka määrittelevät sen toiminnallisuuden.

Sopimuksen sisällä olevat muuttujat voivat olla erilaisia tyyppejä, kuten kokonaislukuja, merkkijonoja, osoitteita ja jopa muita sopimuksia. Muuttujat voivat olla julkisia tai yksityisiä, mikä määrittelee niiden näkyvyyden sopimuksen ulkopuolelle.

Funktiot ovat sopimuksen tärkein osa, ja ne määrittelevät, mitä sopimus tekee. Funktiot voivat olla julkisia, yksityisiä, sisäisiä tai ulkoisia riippuen siitä, missä niitä kutsutaan ja kuka niitä voi kutsua.

Tapahtumat ovat lohkoketjuun kirjattavia tietueita, jotka ilmoittavat, että sopimuksessa on tapahtunut jotain merkittävää. Ne auttavat muita lohkoketjun osapuolia seuraamaan sopimuksen tilaa ja reagoimaan sen muutoksiin. (Solidity 2023.)

5.1.2 Turvallisuus ja virheenkorjaus

Solidityn avulla kehitettyjen älykkäiden sopimusten turvallisuus on kriittisen tärkeää, koska ne toimivat avoimessa, hajautetussa ympäristössä ja niiden tulee käsitellä arvokasta dataa, kuten kryptovaluuttaa. Solidity sisältää useita ominaisuuksia, jotka auttavat kehittäjiä luomaan turvallisia sopimuksia.

Yksi näistä ominaisuuksista on modifierit. Modifierit ovat funktioiden päälle lisättäviä toimintoja, jotka voivat muuttaa funktioiden toimintaa. Ne voivat esimerkiksi varmistaa, että funktiota voi kutsua vain sopimuksen omistaja tai että funktioon liittyvät ehdot täyttyvät ennen sen suorittamista.

Virheenkorjauksessa Solidity tarjoaa "require" ja "revert" -operaatiot, joiden avulla kehittäjät voivat tarkistaa ehtoja ja peruuttaa sopimusten toiminnan, jos ne eivät täyty. Nämä mekanismit auttavat varmistamaan, että sopimukset käyttäytyvät odotetulla tavalla ja estävät mahdolliset väärinkäytökset. (Solidity 2023.)

5.1.3 Perintä ja rajapinnat

Solidity tukee myös perintää, joka on yleinen ohjelmointikäsite, jossa yksi sopimus voi periä toisen sopimuksen ominaisuuksia ja käyttää niitä omassa toiminnassaan. Tämä mahdollistaa koodin uudelleenkäytön ja modularisoinnin, mikä tekee sopimusten kehittämisestä tehokkaampaa ja helpompaa.

Rajapinnat ovat toinen käsite, joka helpottaa sopimusten välistä vuorovaikutusta. Rajapinnat määrittelevät sopimuksen toiminnon allekirjoitukset ilman niiden toteutuksia, mikä mahdollistaa erilaisten sopimusten keskinäisen yhteensopivuuden. (Solidity 2023.)

5.1.4 Kirjastot ja metasopimukset

Solidity-ohjelmointikieli tarjoaa myös kirjastoja, jotka ovat kokoelmia hyödyllisiä funktioita ja työkaluja, jotka voidaan liittää sopimuksiin. Kirjastot auttavat vähentämään päällekkäistä koodia ja tehostavat sopimusten kehittämistä.

Metasopimukset ovat toinen kehittyneempi käsite Solidityssä, jotka mahdollistavat sopimusten hallinnan ja päivittämisen. Ne ovat sopimuksia, jotka voivat luoda, hallita ja päivittää muita sopimuksia. Metasopimusten avulla kehittäjät voivat suunnitella joustavampia ja modulaarisempia järjestelmiä, jotka voivat mukautua ajan myötä ja helpommin reagoida uusiin vaatimuksiin. (Solidity 2023.)

5.2 Vyper

Vyper ohjelmointikieli on kehitetty parantamaan Solidityn ohjelmointikielen puutteita, joka on ollut Ethereum-alustan ensisijainen ohjelmointikieli älykkäiden sopimusten luomiseen. Vyperin kehitystyön taustalla on ollut muun muassa tarve lisätä tietoturvaa ja tehdä älykkäiden sopimusten koodista helpommin ymmärrettävää ja läpinäkyvämpää (Vyper 2023).

5.2.1 Ominaisuudet

Vyperin ohjelmointikieli on suunniteltu nimenomaan älykkäiden sopimusten kehittämiseen, ja se sisältää useita ainutlaatuisia ominaisuuksia, jotka erottavat sen muista ohjelmointikielistä. Yksi merkittävimmistä eroista Vyperin ja muiden ohjelmointikielten, kuten Solidityn, välillä on se, että Vyper on Python-pohjainen kieli. Tämä tarkoittaa, että Vyperin syntaksi on selkeä ja helppolukuinen, mikä helpottaa koodin ymmärtämistä ja pienentää virheiden mahdollisuutta.

Vyperin suunnittelussa on keskitytty poistamaan joitakin ominaisuuksia, jotka voivat aiheuttaa turvallisuusriskejä tai tehdä koodista monimutkaisempaa. Esimerkiksi Vyper ei sisällä luokkia, periytymistä tai itsekorjauksia, jotka voivat vaikeuttaa koodin ymmärtämistä ja lisätä virheiden mahdollisuutta. (Vyper 2023.)

5.2.2 Turvallisuus

Vyper sisältää useita turvallisuuteen liittyviä ominaisuuksia, jotka auttavat kehittäjiä tunnistamaan ja estämään mahdollisia tietoturvariskejä. Vyperin kieli tarjoaa muun muassa seuraavia turvallisuusmekanismeja:

- Staattinen tyypitys: Vyper vaatii muuttujien tyypin määrittämistä ennalta, mikä vähentää tyypinmuuntovirheiden riskiä ja parantaa koodin läpinäkyvyyttä.
- Bounds- ja overflow-tarkistukset: Vyper sisältää automaattisia tarkistuksia, jotka varmistavat, etteivät muuttujat ylitä sallittuja arvoja ja että laskutoimituksissa ei tapahdu ylivuotoja.
- Erikoistuneet funktiot: Vyper tarjoaa kehittäjille valmiita funktioita, jotka on suunniteltu erityisesti älykkäiden sopimusten kehittämiseen, näistä esimerkkinä tokenien siirtoon ja hallintaan liittyvät funktiot.

5.3 Älykkäiden sovellusten julkaiseminen

Kehittäjien on hyvä muistaa, että älykkäät sopimukset ovat pääosin muuttumattomia, eli niitä ei voi päivittää suoraan jälkikäteen. Tämä ominaisuus takaa lohkoketjun tietojen luotettavuuden ja turvallisuuden. On kuitenkin olemassa menetelmiä, joiden avulla voidaan suunnitella älykkäitä sopimuksia niin, että niiden toiminnallisuutta voidaan päivittää tai korjata tarvittaessa.

Älykkäiden sopimusten kehittäminen ja julkaiseminen Ethereum-verkkoon voi olla monimutkainen prosessi, mutta perehtymällä kehitystyökaluihin ja prosesseihin, kehittäjät voivat luoda ja julkaista omia älykkäitä sopimuksia tehokkaasti ja turvallisesti. (Habou 2022.)

5.3.1 Valmistautuminen kehitykseen, testaukseen ja Ethereum-verkon valintaan

Ennen älykkään sopimuksen julkaisemista on ensisijaisen tärkeää kehittää ja testata se huolellisesti. Tähän tarkoitukseen on olemassa useita työkaluja, kuten Remix-kehitysympäristö ja Truffle-kehitystyökalu (Ekholm 2023, 31.). Nämä apuvälineet auttavat kehittäjiä kirjoittamaan ja testaamaan älykkäitä sopimuksia tehokkaasti.

Kun kehitystyö on valmis ja sopimus testattu, seuraava askel on valita Ethereum-verkko, johon älykäs sopimus julkaistaan. Testiverkkoja, kuten Sepolia ja Goerli, voidaan käyttää sopimusten testaamiseen ennen julkaisua pääverkkoon (mainnet). Tämä mahdollistaa toimivuuden varmistamisen ilman oikean Etherin käyttöä. (Habou 2022)

5.3.2 Älykkään sopimuksen julkaiseminen kehitystyökalujen avulla

Sopimuksen kehitykseen ja julkaisuun löytyy kaksi suosittua vaihtoehtoa. Näistä helpompi käyttöinen on selainpohjainen Remix, joka tarjoaa helpon ja nopean tavan julkaista älykkäitä sopimuksia. Se sisältää kattavan valikoiman työkaluja, kuten koodieditorin, kääntäjän, testiympäristön ja lompakon yhdessä käyttöliittymässä (Remix 2023).

Truffle on toinen kehitystyökalu, joka on suunniteltu älykkäiden sopimusten kehittämiseen ja julkaisemiseen. Se tarjoaa monipuoliset toiminnot, kuten koodin kääntämisen, testaamisen, verkon hallinnan ja sopimusten julkaisemisen. Truffle on erityisen hyödyllinen monimutkaisempien sovellusten kehittämisessä, sillä se mahdollistaa laajemman hallinnan ja konfiguroinnin (Truffle Suite 2023).

5.3.3 Transaktion luominen

Viimeinen vaihe älykkään sopimuksen julkaisemisessa on transaktion luominen ja lähettäminen, joka sisältää tavukoodi-muotoisen sopimuskoodin sekä mahdolliset parametrit, jotka määrittävät sopimuksen lähtöarvot. Remix-kehitysympäristössä tämä tehdään valitsemalla "Deploy" välilehti ja valitsemalla Ethereum-lompakon, josta halutaan lähettää transaktio. Remix pyytää vahvistamaan transaktion ja kattamaan kaasumaksut. Kun transaktio on vahvistettu, Remix lähettää sen Ethereum-verkkoon (Remix 2023).

Truffle-kehitystyökalussa älykkään sopimuksen julkaiseminen suoritetaan käyttämällä "truffle migrate" -komentoa. Tämä komento käsittelee tavukoodin-käännöksen ja julkaisuprosessin automaattisesti. Ennen julkaisua on tärkeää määrittää lompakon tiedot ja verkon asetukset (Truffle Suite 2023).

Kun transaktio on lähetetty Ethereum-verkkoon, on odotettava, että se vahvistetaan lohkoketjuun. Tämän jälkeen älykäs sopimus on julkaistu ja valmis käytettäväksi. Sopimuksen osoitetta ja toimintaa voi tarkastella ja seurata esimerkiksi Etherscan-palvelussa (Habou 2022).

6 POHDINTA

Tämän opinnäytetyön laaja katsaus Ethereumiin ja sen tarjoamiin mahdollisuuksiin osoittaa, kuinka digitaalisten teknologioiden ja lohkoketjuteknologian maailma on viimevuosien aikana muuttunut ja jatkaa muuttumistaan.

Lohkoketjuteknologian osalta on erityisen tärkeää huomata, kuinka konsensusalgoritmit, kuten Työntodistus (Proof of Work) ja todistuksen osuus (Proof of Stake), ovat kehittyneet ja miten ne vaikuttavat kryptovaluuttojen ja lohkoketjujen toimintaan. Työntodistuksen ja todistuksen osuuden vertailu antaa arvokasta näkemystä teknologian kehitykseen, pyrkimyksiin vähentää ympäristökuormitusta ja tehostaa verkon toimintaa.

Ethereumin historia kertoo tarinaa jatkuvasta innovaatiosta ja kyvystä sopeutua muuttuviin olosuhteisiin. Ethereum 2.0, joka tunnetaan myös nimellä Ethereum-fuusio, korostaa tätä sitoutumista. Sen mukanaan tuomat parannukset saattavat olla ratkaisevia Ethereum-alustan tulevaisuudelle ja sille, kuinka se kilpailee muiden lohkoketjujen kanssa.

Älykkäät sopimukset ovat epäilemättä yksi Ethereum-alustan merkittävimmistä saavutuksista. Niiden kyky automatisoida, vähentää virheitä ja tuoda läpinäkyvyyttä monimutkaisiin prosesseihin on mullistava. Kuitenkin niiden kehityksessä, kuten Solidityn ja Vyperin vertailu osoittaa, on vielä paljon tekemistä. Turvallisuus, skaalautuvuus ja käytettävyys ovat jatkuvia haasteita, joiden kehitystä pitää jatkaa, jotta tämä teknologia voi saavuttaa suuremman yleisön ja käyttäjäkunnan.

Lisäksi Ethereum ja Bitcoinin välinen vertailu osoittaa kahden kryptovaluutan filosofisten ja teknisten erojen syvyyden. Vaikka molemmat jakavat lohkoketjujen perusperiaatteet, niiden tarkoitus, käyttötarkoitukset ja tekniset yksityiskohdat eroavat merkittävästi toisistaan.

Ethereumin mahdollisuus tukea hajautettuja sovelluksia ja erilaisia älykkäitä sopimuskäytäntöjä kuten MakerDAO, Uniswap ja Aave kertoo sen monipuolisuudesta ja laajemmista mahdollisuuksistaan verrattuna muihin kryptovaluuttoihin.

Tulevaisuuden suhteen Ethereumilla on edessään monia mahdollisuuksia, mutta myös haasteita. Teknologian, turvallisuuden, skaalautuvuuden ja ympäristövaikutusten tasapainottaminen määrittää pitkälti, miten Ethereum kehittyy ja mitä roolia se näyttelee digitaalisen talouden tulevaisuudessa.

LÄHTEET

Bitcoin&Ethereum. 2023. Bitcoin vs. Ethereum: Whats the difference. Verkkosivu. Viitattu 20.11.2023. https://www.investopedia.com/articles/investing/031416/bitcoin-vs-ethereum-driven-different-purposes.asp

Buterin, V. 2023. Ethereum Whitepaper. Verkkosivu. Viitattu 15.3.2023. https://ethereum.org/en/whitepaper/

Buy Ethereum. 2023. Where to buy ETH. Verkkosivu. Viitattu 25.3.2023. https://ethereum.org/en/get-eth/

Cryptopedia. 2022. Ethereum and the ICO Boom. Verkkosivu. Viitattu 15.3.2023. https://www.gemini.com/cryptopedia/initial-coin-offering-explained-ethereum-ico#section-ethereums-role-in-the-ico-boom

Ekholm, V. 2023. Yleiskatsaus Ethereumiin ja älykkäisiin sopimuksiin. Tietojenkäsittely, ohjelmistotuotannon tutkinto-ohjelma. Tampereen Ammattikorkeakoulu. Opinnäytetyö. Viitattu 3.12.2023.

Ethereum. 2023. The history of Ethereum. Verkkosivu. Viitattu 2.4.2023. https://ethereum.org/en/history/

Ethereum Merge. 2023. The Merge. Verkkosivu. Viitattu 10.4.2023. https://ethereum.org/en/roadmap/merge/

Ethereum smart contracts. 2023. Introduction to smart contracts. Verkkosivu. Viitattu 20.11.2023. https://ethereum.org/en/developers/docs/smart-contracts/

Frankenfield, J. 2022. Gas (Ethereum): How Gas Fees Work on the Ethereum Blockchain. Verkkosivu. Viitattu 20.3.2023. https://www.investopedia.com/terms/g/gas-ethereum.asp

Habou, S.A. 2022. How To Create A Smart Contract: The Ultimate Guide (2022). Verkkosivu. Viitattu 21.4.2023. https://www.bluelabellabs.com/blog/how-to-create-smart-contract/

Hooda, P. 2022. Proof of Stake (PoS) in Blockchain. Verkkosivu. Viitattu 10.3.2023. https://www.geeksforgeeks.org/proof-of-stake-pos-in-blockchain/

Hooda, P. 2023. Blockchain – Proof of Work (PoW). Verkkosivu. Viitattu 10.3.2023. https://www.geeksforgeeks.org/blockchain-proof-of-work-pow/

IBM. N.d. What is blockchain technology. Verkkosivu. Viitattu 5.3.2023. https://www.ibm.com/topics/blockchain

Ivanontech. 2021. Breaking Down ETH 2.0 – eWASM and EVM Explained. Verkkosivu. Viitattu 10.4.2023. https://academy.moralis.io/blog/breaking-down-eth-2-0-ewasm-and-evm-explained

MakerDAO. N.d. The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System. Verkkosivu. Viitattu 20.4.2023. https://makerdao.com/en/whitepaper

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Verkkosivu. Viitattu 2.3.2023. https://bitcoin.org/bitcoin.pdf

Remix. 2023. Remix - The Native IDE for Web3 Development. Verkkosivu. Viitattu 21.4.2023. https://remix.ethereum.org/

Solidity. 2023. What is Solidity. Verkkosivu. Viitattu 20.11.2023. https://www.alchemy.com/overviews/solidity

Truffle Suite. 2023. The most comprehensive suite of tools for smart contract development. Verkkosivu. Viitattu 21.4.2023

UniSwap. N.d. Swap, earn, and build on the leading decentralized crypto trading protocol. Verkkosivu. Viitattu 20.4.2023. https://uniswap.org/

Vyper. 2023. Vyper. Verkkosivu. Viitattu 20.11.2023. https://docs.vyperlang.org/en/stable/index.html