Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

ARTTU RAITTINEN

Lightning Service Provider

SALAMAMAKSUVERKOSTON PYSTYTTÄMINEN

SÄHKÖ- JA AUTOMAATIOTEKNIIKKA
2023

Tekijä(t) Raittinen, Arttu	Opinnäytetyö, AMK	Päivämäärä Kuukausi Vuosi
	Sivumäärä 31	Kieli: Suomi

Julkaisun nimi
Lightning Service Provider SALAMA MAKSUVERKOSTON PYSTYTTÄMINEN

Tutkinto-ohjelma
Sähkö- ja automaatiotekniikka

Tiivistelmä

Tämä opinnäytetyö tutki digitaalista Bitcoinin maksuprotokollaa nimeltä Salamaverkko (Lightning-Network). Työn tavoitteena oli toteuttaa Salamamaksuverkko ja avata lukijalle mahdollisimman laajasti kryptovaluutat, lohkoketjut ja niiden taustalla toimivat tekniikat.
Lukijalle tuotiin myös esille Salamaverkon toiminta ja sen toimintaan liittyvät tekniikat.
Opinnäytetyön toimeksiantajana toimi Cervid Oy, joka toimii ohjelmistokehityksessä ja konsultoinnissa digitaalisten valuuttojen ympärillä.

Työ toteutettiin artikkeleiden ja toimeksiantajan tiedoilla. Aihe oli uusi, joten luotettavien lähteiden ja teorian kasaaminen oli suhteellisen haasteellista.

Opinnäytetyö toteutettiin onnistuneesti ja tekijä oppi työstä paljon. Työ sisältää kokonaisuuden salamamaksuverkon pystyttämiseen ja sen monitoroinnista. Tämä opinnäytetyö sopii hyvänä oppaana salamaverkoista kiinnostuneille harrastajille sekä harjoittajille.

Avainsanat
kryptovaluutat, salamaverkko, lohkoketju, bitcoin

Author(s) Raittinen, Arttu	Type of Publication Bachelor's thesis	Date Month Year
	Number of pages 31	Language of publication: Finnish

Title of publication
Lightning Service Provider

Degree programme
Electrical and Automation Engineering

Abstract

This thesis studied the digital Bitcoin transaction protocol named Lightning Network. The goal of this work was to implement a Lightning Network Payment-Channel and to explain the concepts of cryptocurrency, blockchain and the technologies that run them.
This thesis also brings up the concepts of Lightning Network implementations and their technologies. This thesis was commissioned by Cervid Oy, who focuses mainly on software development and consultation revolving around digital currencies.

This work was carried out using articles and with information acquired from Cervid Oy. The subject of this thesis was relatively new so finding reputable sources and compiling theory was relatively difficult.

This thesis was successfully implemented, and the author learned a lot from this project. This work includes an example of a successful implementation of the Lightning Network protocol and how to monitor it. This thesis servers as a good guide to Lightning Networks for those who are interested and for those who want to implement one for use.

Keywords
cryptocurrencies, lightning network, blockchain, bitcoin

SANASTO

Lightning Network	Salamaverkko
Peer-to-Peer	Vertaisverkko, jossa ei ole kiinteitä palvelimia tai asiakkaita. Jokainen taho toimii sekä palvelimena että asiakkaana verkon jäsenille.
Node	Solmu. Verkkoa pyörittävä palvelin
Global state	Maailman tila on joukko dataa. Yleisin toteutus tälle on tietokanta.
Proof of Work	Työntodiste. Konsensusalgoritmi malli.
Proof of Stake	Varantotodiste. Konsensusalgoritmi malli
Double Spending	Digitaalisen rahan käyttö kahteen kertaan
ASIC	Application Specific Integrated Circuit. Sovelluskohtainen integroitu piiri.
Hashing	Hajautusalgoritmi.
Payment Channel	Maksukanava.
Multi-signature (multisig)	Tarkoittaa moniallekirjoitusta, ja se on tietyntyyppinen digitaalinen allekirjoitus.
Circular rebalancing	Lohkoketjun ulkopuolinen tasapainottaminen, jossa palvelin suorittaa maksun itselleen ketjutettujen maksukanavien kautta.
Hot Wallet	Digitaalinen tallennustila kryptovaluuttojen tallentamiseen.
Linux	Avoimen lähdekoodin käyttöjärjestelmä.
CPU	Central Processing Unit. Tietokoneen prosessori.
RAM	Rapid Access Memory. Tietokoneen muisti, joka tallentaa ohjelman tarvitsemia tietoja sen ollessa käynnissä.
SSH	Secure Shell. Salattuun tietoliikenteeseen tarkoitettu protokolla.
Ansible Playbook	Käytettään säännöllisesti IT-infrastruktuurin automatisointiin.
YAML	käytetään usein konfiguraatiotiedostoissa, mutta sitä voi käyttää myös muunlaiseen tietojen talletukseen.

Daemon	Linuxin kaltaisissa käyttöjärjestelmissä taustalla suoritettava järjestelmäohjelma, jota käyttäjä ei suoraan hallitse.

SISÄLLYS

1 JOHDANTO 7
2 KRYPTOVALUUTTA 7
2.1 Kryptovaluutta Bitcoin 7
2.2 Arvo ja sen määräytyminen 8
2.3 Kryptovaluuttalompakko 8
2.4 Hyödyt ja haitat 9
3 LOHKOKETJUTEKNOLOGIA 10
3.1 Lohkoketjun toiminta 11
3.1.1 Lohkoketjun palvelut 12
3.2 Hajautusalgoritmit (Hashing) 12
3.3 Konsensusmekanismit 13
3.3.1 Konsensusmekanismi tyyppejä 13
3.4 Louhinta 14
4 SALAMAVERKKO 15
4.1 Salamaverkko teoriassa 15
4.2 Salamaverkon toiminta 15
4.2.1 Salamaverkko-kanava 16
4.3 Salamaverkon heikkoudet 18
5 TOTEUTUSVAIHE 19
5.1 Työn menetelmät 19
5.2 Laitteisto 19
5.3 Red Hat Ansible käyttö 20
5.4 Docker ja Docker-compose käyttö 23
5.5 Bitcoin-Core (bitcoind) käyttö 24
5.6 Core Lightning (c-lightning) 25
5.7 Prometheus ja Grafana 25
6 LOPPUAJATUKSET 28

1 JOHDANTO

Tämä opinnäytetyö tutkii kryptovaluuttoja, lohkoketjuja ja niihin liittyviä tekniikoita. Työn tavoitteena on toteuttaa Salamamaksuverkko. Aloitan kertomalla ensiksi teoriaa kryptovaluutta Bitcoinista, jonka jälkeen jatkan lohkoketjuteknologiaan ja Salamaverkkoon. Bitcoinista ja Salamaverkosta löytyy paljon englanninkielistä termejä, jonka vuoksi olen kirjottanut kyseiset termit myös englanniksi.

Salamaverkon tarkoituksena on helpottaa Bitcoin-kryptovaluutan transaktioiden kulkua. Salamaverkon avulla voidaan toistuvat pienet maksut hoitaa, jolloin ne ei kuormita Bitcoin-verkkoa turhaan. Salamaverkko mahdollistaa maksusuoritusten kulkemisen kahden tahon välillä ilman että siitä jää merkintää lohkoketjuun.

2 KRYPTOVALUUTTA

Kryptovaluutta on digitaalinen tai virtuaalinen valuutta, joka on suojattu kryptografialla, mikä tekee sen väärentämisen tai kaksinkertaisen kulutuksen melkein mahdottomaksi. Monet kryptovaluutat ovat hajautettuja verkkoja, jotka perustuvat lohkoketjutekniikkaan, jota monet tietokoneet verkossa pyörittävät. Kryptovaluuttojen määräävä piirre on, että ne eivät ole yleensä minkään keskusviranomaisen myöntämiä, mikä tekee niistä teoreettisesti immuuneja hallituksen puuttumisille tai manipuloinnille. (Frankenfield, J 2022a).

2.1 Kryptovaluutta Bitcoin

Bitcoin on virtuaalinen valuutta, joka on suunniteltu toimimaan rahana ja ne liikkuvat käyttäjien välillä toisille internetin kautta. Bitcoinilla ei ole fyysistä muotoa.

Bitcoinin alkuperä juontaa juurensa anonyymiin Satoshi Nakamotoon, joka julkaisi kryptografiasta kiinnostuneiden keskustelufoorumille tutkimuspaperin (Bitcoin: A Peer-to-Peer Electronic Cash System). Tutkimuspaperissa Nakamoto kuvaa maksujärjestelmää, joka toimii täysin vertaisverkossa ilman luotettua kolmatta osapuolta.

Bitcoinin ensimmäinen liikkeellelasku tapahtui lokakuussa vuonna 2009, kun eräs internet-pörssi myi 5 050 bitcoinia hintaan 5,02 Yhdysvaltain dollaria. Eli yksi dollari vastasi 1 006:ta bitcoinia. Hinta määriteltiin mittaamalla yhden bitcoinin tuottamiseen tarvittavan sähkön arvo.

2.2 Arvo ja sen määräytyminen

Bitcoinin arvo ei määräydy perinteisen valuutan perustein. Bitcoinia ei ole laskenut liikkeeseen keskuspankki tai se ei ole valtion takaama, siksi rahapolitiikka sekä inflaatiotasot, jotka tyypillisesti vaikuttavat valuuttaan, eivät päde Bitcoiniin. Näistä syistä Bitcoinin arvo määräytyy erilaisista tekijöistä.
Asiat, jotka vaikuttavat Bitcoinin arvoon voidaan luokitella lyhyesti näin:

- Bitcoinin tarjota ja markkinan kysyntä sille
- Sen tuotantokustannukset louhintaprosessin kautta
- Kilpailevien kryptovaluuttojen määrä ja niiden markkinavahvuus
- Bitcoinin myyntiä ja sen käyttöä koskevat määräykset
- Media ja uutiset

(Bloomenthal, A. 2022, Rosenberg, E. 2022 & Bitcoin.org www-sivut 2022.)

2.3 Kryptovaluuttalompakko

Kryptovaluutta-lompakolla käyttäjä voi säilyttää, lähettää ja ottaa vastaan kryptovaluuttoja, kuten myös Bitcoinia. Kryptovaluutta-lompakot ovat digitaalisia lompakoita, jotka tallentavat salausmateriaalia, joka mahdollistaa pääsyn Bitcoinin julkiseen osoitteeseen ja mahdollistaa transaktiot lompakoiden välillä.
(Rodeck, D. & Schimdt, J. 2022)

Kryptovaluuttoja ei ”talleteta” minnekään, vaan ne ovat tietokantaan tallennettuja tietoja. Nämä tiedot eli databitit ovat hajallaan kaikkialla tietokannassa; kryptovaluuttalompakko löytää kaikki bitit liittyen sinun julkiseen osoitteeseesi ja laskee summan sinulle sovelluksen käyttöliittymässä. (Frankenfield, J 2022b)
Maksutapahtumat ovat mahdollista suorittaa lompakkosovellusten kautta puhelimelta tai tietokoneelta, joissa käyttäjä tarvitsee vastaanottajan lompakon osoitteen ja maksu summan.

2.4 Hyödyt ja haitat

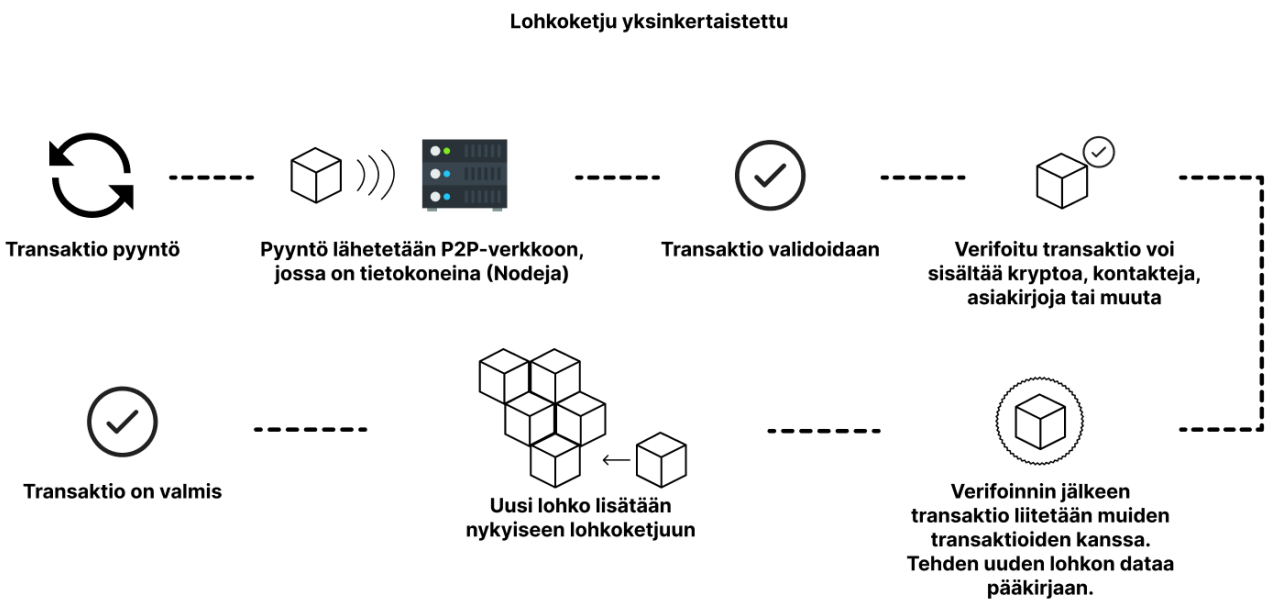
Koska Bitcoin on vielä uusi ja vasta leviämisvaiheensa alussa, sen hinta on heilahdellut villisti kysynnän mukaan. Yksinään auktoriteetti ei kuittenkaan pysty mielivaltaisesti kasvattamaan sen tarjontaa vastauksena hintapiikkeihin, mikä selittää valuutan ostovoiman raketinkaltaisen nousun. (Ammous, S. 2018)

Bitcoinilla on lyhyt sijoitushistoria täynnä erittäin vaihtelevia hintoja. Se, onko kyseessä hyvä sijoitus, riippuu taloudellisesta profiilistasi, sijoituskyvystäsi ja riskinsietokyvystä. (Frankenfield, J. 2022)
Bitcoinia voi lähettää ja vastaanottaa kaikkialla maailmassa milloin tahansa. Bitcoin antaa sen käyttäjille mahdollisuuden hallita rahaa täysin. Bitcoinien vastaanottamisesta ei peritä transaktiomaksua, ja monet kryptovaluuttalompakot antavat sinun hallita, kuinka suuren transaktiomaksun kulutat maksussa. Korkeammat transaktiomaksut yleisesti voivat nopeuttaa maksutapahtumien vahvistamista. Transaktiomaksut eivät liity siirrettyyn summaan, joten on mahdollista lähettää 1000 bitcoinia samalla transaktiomaksulla kuin yhden bitcoinin lähettäminen.
Bitcoin käyttäjät ovat täydessä hallinnassa heidän transaktioistaan. Käyttäjien identiteetti on myös vahvasti suojattu, koska Bitcoin-maksuja voidaan suorittaa ilman sidottuja henkilötietoja ja ne ovat turvallisia ja peruuttamattomia.
(Bitcoin.org www-sivut 2022)

Näistä huolimatta Bitcoin maksutapana ei ole kovin suosittu tai hyväksytty kivijalkamyymälöissä.
Bitcoinin kurssin jatkuva päivittäinen radikaalinen vaihto ja Bitcoinin turvallisuus ja niiden kavaltaminen saavat ihmiset vieroksumaan Bitcoinia maksutapana. (Reese, F. 2018.)
Tammikuussa vuonna 2011, Ross William Ulbricht, perusti sivuston ”Silk Road”, joka toimi pimeässä verkossa laittomien tavaroiden ja palveluiden kauppana.
Sivulla käytettiin Bitcoinia kaupankäynti välineenä ja se pahensi Bitcoinin mainetta vakavana otettavana valuuttana. Bitcoinin tarjoama anonyymisyys maksu asioissa antoi sivun asiakkaille mahdollisuuden tehdä kauppaa ilman jättämättä rahan siirrosta henkilöllisyyteen liittyviä jälkiä. (Adler, D. 2018.)

3 LOHKOKETJUTEKNOLOGIA

Lohkoketjuteknologiassa data on käytännössä tallennettuna jokaiselle verkkoa pyörittävälle palvelimelle, ja näitä palvelimia kutsutaan nimellä Node, eli solmu. Käytännössä lohkoketju on verkko, jossa lukuisat sitä tukevat palvelinkoneet ovat toisiinsa yhteydessä internetin kautta. Lohkoketjussa ei siis ole keskuspalvelimia tai muita kriittisiä pisteitä, jotka lamauttamalla sen toiminta voitaisiin estää.
(Kryptovaluutta.fi www-sivut 2022)
Kyseisiä verkkoja tyypillisesti kutsutan vertaisverkoiksi (Peer-to-Peer) ja lohkoketjuja hallinnoidaan vertaisverkossa julkisena hajautettuna kirjanpitona, jossa palvelimet noudattavat kollektiivisesti konsensusalgoritmiprotokollaa uusien transaktiolohkojen lisäämiseksi ja vahvistamiseksi.
Konsensusalgoritmi on tietojenkäsittelytieteen prosessi, jota käytetään pääsemään yhteisymmärrykseen tietystä data arvosta hajautettujen prosessien tai järjestelmien välillä. (Iansiti, M. & Lakhani. Karim R. 2017)



Kuvio 1 Lohkoketju yksinkertaistettu

3.1 Lohkoketjun toiminta

Perusideana lohkoketjuteknologiassa on tavoitteena luoda autonomista ja keskitetystä hallinnoijasta riippumattomia automatisoitavia arvonsiirtomekanismeja, palveluprosesseja ja liiketoimintaverkostoja, joissa hyödynnetään vertaisverkkopohjaista automatisoitua luottamusta ja virtuaalisia rahakkeita. (Rahkola, M. 2019)

Lohkoketjuteknologiat ovat sääntöjä ja standardeja siitä, miten hajautettua kirjanpitoa luodaan ja ylläpidetään.
Lohkoketjut koostuvat kolmesta toimintakerroksesta, jotka kukin lisäävät eri komponentteja sen kehittämiseen:

- **Protokollakerros** muodostaa perusrakenteen lohkoketjulle. Se määrittelee mahdolliset laskentasäännöt ja ohjelmointikielen, jota käytetään lohkoketjussa.
- **Verkkokerroksessa** säännöt, jotka määriteltiin protokollakerroksessa, oikeasti toteutetaan.
- **Sovelluskerros** yhdistää protokolla- ja verkkokerrokset toimiviksi palveluiksi. Käytännössä tässä luodaan käyttöliittymät loppukäyttäjien palveluille.

Nämä toimintakerrokset voivat vaihdella lohkoketjujen välillä, muuttaen niiden sääntöjä ja standardeja.
Esimerkkejä eri lohkoketjuista: Algorand, Avalanche, Bitcoin, Ethereum, EOS.
(OECD www-sivut & Lewis, A 2018)

3.1.1 Lohkoketjun palvelut

Lohkoketjut voidaan jakaa kahteen eri palveluihin, avoimiin ja suljettuihin.
Avoin lohkoketju on nimensä mukaisesti avoin kenelle tahansa. Voit liittyä lohkoketjun toimintaan, tarkastella ja myös lisätä siihen tietoa sekä toimia verkoston tasavertaisena jäsenenä. Avoimiin lohkoketjuihin liittyy aina rahake (virtuaalivaluutta tai älyraha), jolla verkoston jäsenille korvataan heidän verkostollensa luovuttamaa tietoteknistä resurssia. Teoriassa avoimessa lohkoketjussa kaikissa solmuissa pitäisi olla täysi kopio koko lohkoketjun sisällöstä. Bitcoin on tunnetuin esimerkki avoimesta lohkoketjusta.

Suljettuun lohkoketjuun liittyminen edellyttää lohkoketjun hallinnoijalta hyväksyntää. Suljetussa lohkoketjussa ei välttämättä tarvita tai käytetä rahakkeita verkoston vaatimien tietoteknisten resurssien korvaamiseen, mutta rahakkeita voidaan käyttää esimerkiksi verkoston sisällä tapahtuvien palveluiden tai niihin liittyvien käyttöoikeusarvojen siirtoon. Suljettuun lohkoketjuun tallennetun tiedon luku- ja kirjoitusoikeuksia hallitaan eri toimijoiden rooliin liittyen käyttöoikeuksien perusteella.
(Rahkola, M 2019)

3.2 Hajautusalgoritmit (Hashing)

Hajautusta (Hash) voi ajatella kuin digitaalisena sormenjälkenä, se on ainutlaatuinen jokaiselle lohkoketjun datalle. Käyttäjät ilmoittavat transaktioon kuuluvat tiedot (vastaanottajan ja lähettäjän nimi sekä summa, joka siirretään) kryptograafiseen hajautusalgoritmiin ja vastaanottaa sarjan kirjaimia ja numeroita, jotka eroavat kyseisestä tapahtumasta. Syötetty tieto, jos se ei muutu tuottaa aina täsmälleen saman sarjan kirjaimia ja numeroita. Jos jotain syötetyn tiedon osaa kuitenkin muutetaan (esim.

pahantahtoinen toimija muuttaa siirrettyä summaa) merkkisarja muuttuisi täysin erilaiseksi joukoksi ja tekee siitä yhteensopimattoman lohkoketjulle. Näin ollen, vaikka solmut ei ikinä näkisi transaktio tapahtuman yksityiskohtia, voivat solmut nopeasti kertoa, että lohkon tietoja on peukaloitu ja hylkää tämä versio. Juuri tämä kryptografinen tietoturva tekee lohkoketjun kirjanpidon luotettavammaksi ja melkein muuttumattomaksi. (OECD Blockchain Primer.)

Syöte	Hajausalgoritmi tulos (Käyttäen SHA 256 algoritmia)
SOTFS	726d47c2dcab08c5c01beeea7532862c8a9d74c7371097494ea7ae1e46466864
SoTFS	8ff2acee8f2de438f062333529da09b966234a555f7d7339472f82179ef681ef

Kuvio 2 SHA 256 hajautusalgoritmi

3.3 Konsensusmekanismit

Yksi lohkoketjun tärkeimmistä ominaisuuksista on konsensusmekanismialgoritmit, joita se käyttää transaktioiden suostumuksen keräämiseen. Solmujen välinen yhteisymmärrys pääkirjan ´tilasta´ on olennainen lohkoketjun toiminnan kannalta. (OECD Blockchain Primer)

Ilman toimivaa konsensusmekanismia järjestelmässä tulisi olla keskitettyä järjestelmää muistuttava luottamussuhde joidenkin toimijoiden väillä. Useat älysopimusalustat ratkaisevat tämän ongelman erottamalla ns. maailman tilan (global state) ja transaktiolohkoketjun toisittaan erillisiksi kokonaisuuksiksi.

(Kryptovaluutta.fi www-sivut 2022)

3.3.1 Konsensusmekanismi tyyppejä

Proof-of-Work (PoW)

PoW-protokolla suosii lohkoja, joiden louhinnassa on käytetty eniten laskentatehoja. Ongelmatapauksessa lohkonmuodostus tapahtuu tietyn raja-arvon alittavia tiivistefunktioita laskemalla. PoW:ssa vaikeustaso skaalautuu laskentatehon myötä, jolloin se on suhteellisen epäedullinen energiatehokkuudeltaan.

Proof-of-Stake (PoS)

PoS-protokolla suosii niitä lohkoja, joiden louhinnan takana on eniten panostettua krypto omaisuuseriä. PoS on energiatehokkuudeltaan huomattavasti edullisempi PoW:n verrattuna. Tunnetuista kryptovaluutoista Ethereum on siirtynyt PoS-protokollaan. (Ethereum.org www-sivut 2022 & kryptovaluutta.fi www-sivut 2022)

Proof-of-Work ja Proof-of-Stake ovat kaksi yleisimmin käytettyä konsensusmekanismia. Löytyy myös muita konsensusmekanismeja, jotka eivät ole niin yleisessä käytössä.
(Crypto.com www-sivut 2022)

3.4 Louhinta

Louhinta on tapa lisätä transaktio tietoja lohkojen kautta hajautettuun kirjanpitoon. Louhijat ovat verkon solmuja, jotka varmistavat, että lohkon transaktiot ovat kelvollisia. Erityisesti ne varmistavat, että varoja ei kopioida (double-spending) tai lohkoketjun sisältöä muuteta. Louhinnan ensisijainen tehtävä on taata siirtojen pysyvyys ja luoda pysyvä tallenne niiden keskinäisestä järjestyksestä. Tämä on toteutettu määrittelemällä kelvollisen lohkon tiivisteelle tietyt ehdot.
Bitcoin louhinnassa louhijat kilpailevat keskenään ratkoen matemaattisen ongelman liittyen kryptografiseen tiivistealgoritmiin. Se joka ratkaisee algoritmin nopeimmin, saa palkinnoksi bitcoineja sekä transaktiokorvauksen.
Yksittäisten lohkojen on sisällettävä todiste työstä (Proof-of-Work) jotta ne voidaan pitää validina. Muut solmut vahvistavat tämän todisteen joka kerta kun he saavat lohkon.

Bitcoinien louhimista voi harjoittaa kuka tahansa, mutta nykyään louhintaan käytetään ASIC (application specific integrated circuit) koneistoa, joiden louhintateho on moninkertainen verrattuna tavallisen tietokoneen louhintatehoon. ASIC-laitteet ovat kalliita hankintoja niin yleisesti suurimmat louhimiset tapahtuvat louhintayrityksissä (pool mining) jolloin kustannuksista huolimatta tuottoa saadaan aikaseksi.
(DeMartino, 2018, s. 150–155)

4 SALAMAVERKKO

Salamaverkko on ideana jo monia vuosia vanha. Sen ensimmäiset askeleet voidaan jäljittää Bitcoinin ensimmäisiin koodiversioihin eli noin vuoteen 2007. Satoshi kirjoitti jo tuolloin Payment Channels-ideasta eli maksukanavasta kahden tai useamman tahon välillä.

Salamaverkko alkoi muuttua teoriasta käytäntöön vuonna 2018 taitteessa, jolloin julkaistiin ensimmäiset versiot salamaverkon ohjelmakoodista, joka mahdollisti innokkaiden henkilöiden liittymisen verkkoon. Salamaverkko koostuu Bitcoinin tavoin solmuista, jotka ovat ohjelmakoodia pyörittäviä palvelinkoneita.

(Bitcoinkeskus.com www-sivut 2021)

4.1 Salamaverkko teoriassa

Salamaverkko mahdollistaa maksusuoritusten kulkemisen kahden tahon välillä ilman että siitä jää merkintää lohkoketjuun. Verkko on riippuvainen lohkoketjun taustalla toimivasta tekniikasta. Verkon tavoitteena on nopeuttaa maksutapahtumien siirtymisen kahden osapuolen kesken sekä alentaa transaktiokorvauksen määrää pitämällä sen poissa pääverkosta.

Salamaverkon ideana on tarjota vaihtoehtoinen verkko etenkin mikromaksuja varten. Salamaverkossa voi siirtää suuriakin maksuja, mutta tämä vaatii verkon kapasiteetilta kasvua. Sen edut tulevat esiin pienissä transaktioissa, jotka ovat saatava perille parissa sekunnissa esim. kaupankäyntitilanteessa.

(Bitcoinkeskus.com www-sivut 2021)

4.2 Salamaverkon toiminta

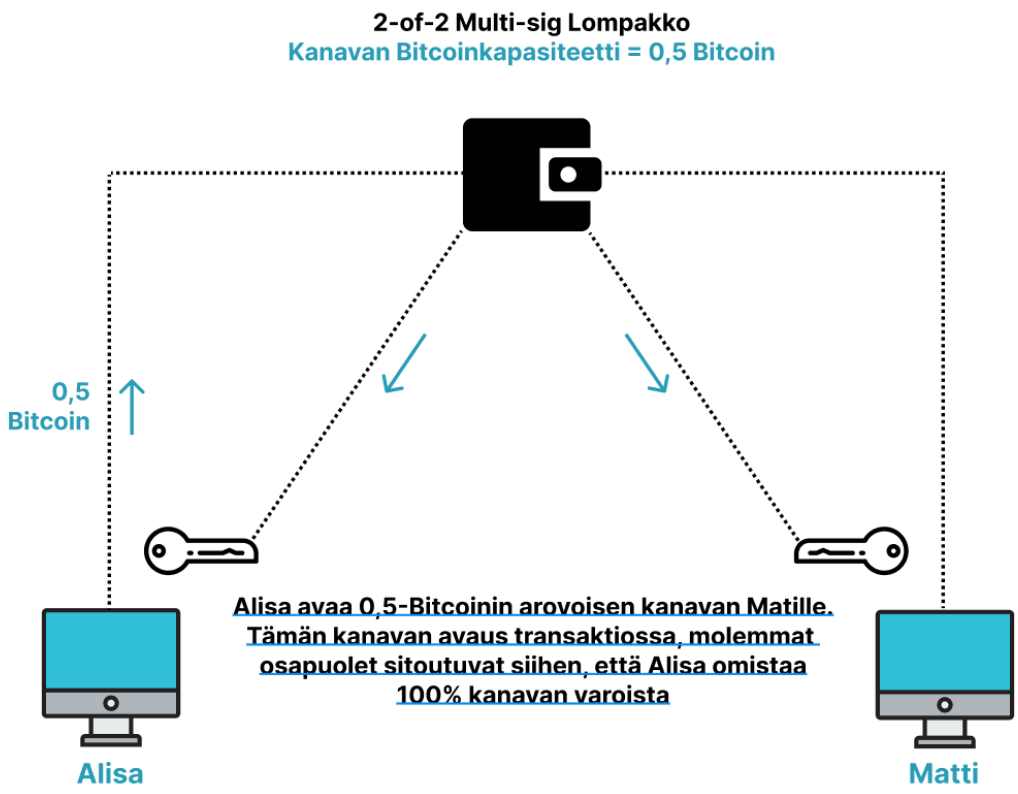
Kuten myös Bitcoin lohkoketju, Salamaverkko koostuu solmuista, jotka pyörivät Salamaverkko ohjelmistossa. Toisin kuin Bitcoinissa, Salamaverkon transaktiot eivät ole julkisesti lähetetty ja tallennettu jokaiselle jäsenelle verkossa. Sen sijaan, yksittäiset Salamaverkko solmut keskustelevat toistensa kanssa yksityisesti. Salamaverkko solmut käyttävät kanavia tällaisten maksujen suorittamiseksi.

(River.com www-sivut 2022

4.2.1 Salamaverkko-kanava

Salamaverkko-kanava on kaksisuuntainen maksukanava, tarkoittaen että, molemmat osapuolet voivat lähettää maksuja toisilleen kanavan kautta. Nämä kanavat muodostavat Salamaverkon ja niillä on määritelty bitcoinkapasiteetti. Tämä kapasiteetti on jaettu kanavan kahden osapuolen kesken, ja bitcoineja siirretään toiselta puolelta kanavaa toiselle Salamaverkko-transaktioiden avulla.

Kaksi osapuolta voi avaa Salamaverkko-kanavan tallentamalla bitcoineja 2-of-2 Multi-sig osoitteeseen. Tämä tapahtuma tallennetaan Bitcoin lohkoketjuun ja kun kyseinen tapahtuma on vahvistettu, Salamaverkko-kanava avataan.



Kuvio 3 Kanavan avaustransaktio

Kun Salamaverkko-kanava on avattu, molemmat osapuolet voivat suorittaa minkä määrän tahansa transaktioita nopeasti ja halvasti. Kun osapuolet ovat saaneet kaupan

valmiiksi, he voivat sulkea kanavan toisella Bitcoin lohkoketjun sisäisellä transaktiolla, joka heijastaa molempien osapuolien saldojen nettomuutosta. (River.com www-sivut 2022)

Maksukanava on kahden osapuolen kesken jaettu varojen konsernitili. Nämä varat ovat aina tallennettu Multi-sig osoitteeseen. Salamatransaktiot tapahtuvat tässä kanavassa jakamalla osoitteeseen tallennetut varat uudelleen. Aina kun Bitcoineja siirretään kanavan kautta – osapuolelta A osapuolelle B – kanavan saldo päivittyy. Näitä päivityksiä ei kuitenkaan tallenneta lohkoketjuun.

Kuvio 4 Suora Maksukanava

Varojen selvitys tapahtuu, kun molemmat osapuolet päättävät sulkea kanavan. Kun kanava sulkeutuu, Bitcoinin lohkoketjuun tallennetaan ketjun sisäinen tapahtuma, joka kuluttaa Bitcoinia multi-sig-osoitteesta. Kun tämä tapahtuu kanavan saldo, on silloin laskettu. Alisalla on nyt 0,4 Bitcoinia ja Matilla 0,1 Bitcoinia.

4.3 Salamaverkon heikkoudet

Salamaverkot tarjoavat hyvän skaalausratkaisun Bitcoinille, mutta sillä on tietysti jotain rajoituksia.

Kanavien hallinta

Jos osapuoli suorittaa paljon maksuja yhteen suuntaan, kanavat voivat muuttua epätasapainoisiksi, tarkoittaen, että kaikki kanavan varat jäävät toiselle puolelle kanavaa. Tämä vaatii siten käyttäjän toimimaan tasapainottamalla kanavat. Tämä voidaan hoitaa Circular rebalancing (maksamalla itsesi yhdestä kanavasta toiseen) tai vaihtopalvelun avulla, jonka avulla voit täyttää tai tyhjentää olemassa olevan kanavan pientä maksua vastaan. Yleisissä Salamaverkko palvelin hallintatyökaluissa on sisäänrakennettu jonkinlainen uudelleen tasapainottamismenetelmä.

Saapuva likviditeetti

Jos käyttäjä avaa kanavan jollekin toiselle, kaikki varat ovat aluksi hänen puolellaan kanavaa. Tämä tarkoittaa että, he voivan vain lähettää maksuja eikä vastaanottaa niitä. Suosituimmat Salamaverkko lompakot ovat julkaisseet päivityksiä, jotka vähentävät tätä ongelmaa avaamalla uusia kanavia tarpeen mukaan.

Hot Wallet

Salamaverkon luonteen takia, käyttäjänpalvelimen pitää olla online-tilassa 24/7 voidakseen kuitata ja allekirjoittaa transaktioita. Tämä tarkoittaa että, on suositeltavaa, että käyttäjät eivät lukitse suuria määriä Bitcoineja ryhtymättä asianmukaisiin turvatoimiin ja varmuuskopiointiin.

Varmuuskopiot

Salamaverkko-kanavat saavat skaalautuvuus- ja tietosuojaetunsa erittäin yksinkertaisella tekniikalla, jossa et kerro kenellekään muulle kanavan sisäisestä toiminnasta. Tämä on toisin kuin lohkoketjulla tapahtuvissa maksuissa, joissa sinun on kerrottava kaikille jokaisesta maksusta ja tallennettava ne lohkoketjuun.

Mutta Salamaverkossa, koska olet ainoa, joka tallentaa kaikki taloustietosi, et voi palauttaa näitä mistään muualta. Tämä tarkoittaa, että sinun on vastuullisesti varmuuskopioida käyttämällä erilaisia prosesseja ja automaatioita.

(Lightning.readthedocs.io www-sivut)

5 TOTEUTUSVAIHE

Opinnäytetyön tavoitteena on toteuttaa Lightning Service Provider (Lightning-palveluntarjoaja). Salamaverkko on maksukanavien yhdistämistä. Näissä maksukanavissa on useita ominaisuuksia, jotka sekä tekevät verkosta turvallisen ja mahdollisesti hankalia uusille käyttäjille. Tavoitteena on toteuttaa Salamaverkko-palvelun, johon asiakas voi liittyä, hallinnoida hänen kanaviansa ja tehdä sen kautta maksuja.

5.1 Työn menetelmät

Tässä työssä tulen käyttämään seuraavia välineitä Salamaverkko-palveluun:

- Linux-palvelin
- Red Hat Ansible (Palvelimen pystyttämisen automatisointiin)
- Docker ja Docker-compose
- Bitcoin Core (Bitcoind)
- Core-Lightning (c-lightning)
- Prometheus ja Grafana (Järjestelmän datan monitorointiin)

5.2 Laitteisto

Lightning pohjaiset järjestelmät ovat yleisesti suunniteltu pyörimään Linux-käyttöjärjestelmällä. Joten käytimme projektintekovaiheessa vuokra Linux-palvelimia.
Koneessa on prosessorina Intel Xeon Gold 4VCPU ja 16Gb RAM. Koneeseen otettiin lisäksi lisää massamuistia, jotta saadaan ladattua koko Bitcoin-lohkoketju koneelle.

5.3 Red Hat Ansible käyttö

Ansible on ohjelmistotyökalu, joka tarjoaa yksinkertaisen mutta tehokkaan automaatio järjestelmän eri tietokone alustoille. Se on tarkoitettu ensisijaisesti IT-ammattilaisille, jotka käyttävät sitä sovellusten käyttöönottoon, työasemien ja palvelimien päivitykseen, konfigurointien hallintaan ja lähes kaikkeen mitä järjestelmänvalvoja tekee madollisesti viikoittain ja päivittäin.
Ansiblessa on kaksi tietokoneluokkaa: Ohjaussolmu ja hallitut solmut. Ohjaussolmu on tietokone, jossa on Ansible asennettuna. Hallitut solmut ovat mikä tahansa Ohjaussolmun hallitsema laite.

Ansible toimii muodostamalla yhteyden verkon solmuihin (asiakkaisiin, palvelimiin tai mihin tahansa määritettävään) ja lähettämällä sitten Ansible-moduuliksi kutsutun pienen ohjelman kyseiselle solmulle. Ansible suorittaa nämä moduulit SSH:n yhteyden kautta ja poistaa ne, kun se on valmis.
(Ansible.com www-sivut 2022)

Käytämme paljon Ansible Playbooks ominaisuutta tässä työssä. Se tarjoaa toistettavan, uudelleen käytettävän ja yksinkertaisen konfiguraatio hallintajärjestelmän. Playbookit tallentavat ja suorittavat Ansiblen määritys-, käyttöönotto- ja organisointitoiminnot. Ne voivat esimerkiksi kuvata käytäntöä, jota haluat etäjärjestelmien valvovan, tai joukon vaiheita yleisessä IT-prosesseissa. Playbookit ilmaistaan YAML-muodossa.

```yaml
hosts: all
become: yes
vars:
  jsonVar: "{{ lookup('file', 'users.json') }}"

tasks:
  - name: Add user
    ansible.builtin.user:
      name: "{{ item.user }}"
      groups: sudo
      create_home: True
      state: present
      shell: /bin/bash
      password: "{{ item.password | password_hash('sha512') }}"
    loop: "{{jsonVar}}"
    no_log: true

  - name: Add pub key
    ansible.posix.authorized_key:
      user: "{{ item.user }}"
      state: present
      key: "{{ item.ssh_public }}"
    loop: "{{jsonVar}}"
    no_log: true
```

Kuvio 5 Perus Ansible-playbook, jota käytän tässä työssä (add-users.yaml) jossa lisätään palvelimelle käyttäjiä ja asennetaan ssh public-key. Työssä löytyy monia Ansible-playbook tiedostoja eri sovellusten asentamiseen ja konfigurointiin.

```yaml
- hosts: all
  tasks:

- name: adding users
  import_playbook: add-users.yaml
 - name: ssh_hardening
   import_playbook: hardening.yaml
- name: tailscale
  import_playbook: install-tailscale.yaml
- name: docker install
  import_playbook: install-docker.yaml
- name: portainer install
  import_playbook: install-portainer.yaml
- name: node exporter install
  import_playbook: install_node_exporter.yaml
- name: docker_compose service start
  import_playbook: install-compose.yaml
```

Kuvio 6 Master-playbook niminen YAML tiedosto, joka suoritetaan palvelimen konfiguroinnissa ensimmäiseksi. Tämä asentaa kaikki tarvittavat ohjelmistot käymällä läpi monta eri Playbook:ia joissa asennetaan ja konfiguroidaan kyseiset ohjelmistot.

Tämän Playbookin suorittaminen suorittaa seuraavat toiminnot hallittuun solmuun:

- Adding users. Lisätään käyttäjiä Ansiblen user moduulilla. Käyttäjille annetaan Linuxilla sudo oikeudet ja myös lisätään ssh-yhteyttä varten omat ssh-avaimet.
- ssh_hardening. Konfiguroidaan ssh-palvelimen turvallisuutta.
- install-tailscale. Tailscale on VPN-palvelu.
- Docker install. Asennetaan Docker ja siihen liittyvät ohjelmistot (docker-compose, yms.) Samalla lisätään 1-vaiheessa tehdyt käyttäjien oikeudet dockeriin.
- Portainer install. Asennetaan Portainer, jolla pystyy helpommin seuraamaan ja säätämään Dockeria.
- Node exporter. Tällä pystymme hakemaan palvelimelta dataa, jota voimme näyttää Prometheus ja Grafana avulla.
- Docker_compose service start. Tässä siirretään Ohjaussolmulta tiedostoja hallittuun solmuun ja suoritetaan Docker-compose konfigurointi ja käynnistys.

5.4 Docker ja Docker-compose käyttö

Docker on avoimenlähdekoodin alusta, jonka avulla kehittäjät voivat rakentaa, ottaa käyttöön, päivittää ja hallita Container-nimisiä ‘säilöjä’. Ne ovat standardoituja, suoritettavia komponentteja, jotka yhdistävät sovelluksen lähdekoodin käyttöjärjestelmien (OS) kirjastoihin ja riippuvuuksiin, joita tarvitaan kyseisen koodin suorittamiseen missä tahansa ympäristössä.
(IBM.com www-sivut)
Dockerin avulla voit nopeasti ottaa käyttöön ja skaalata sovelluksia mihin tahansa ympäristöön ja tietää, että koodisi toimii.

Docker Containerit toimittavat usein sekä sovelluksen asennukseen että konfigurointiin, joka tarkoittaa, että järjestelmänvalvojien ei tarvitse käyttää yhtä paljon aikaa ‘säilössä’ olevan sovelluksen suorittamiseen verrattuna, kun sovellus asennettaan perinteisestä lähteestä.
Suuri hyöty on ‘säilöjen’ kyky sammua siististi ja käynnistyä uudelleen, kun sitä vaaditaan. Johtuipa ‘säilön’ sammuminen kaatumisesta virheen takia tai siitä että sitä ei enää yksinkertaisesti tarvita, ne ovat helppoja uudelleen käynnistää ja ne on suunniteltu saumattomasti ilmaantumaan ja katoamaan.
(Opensource.com www-sivut)

Docker-compose on työkalu, joka on kehitetty auttamaan Multi-Container sovellusten määrittämiseen ja luomiseen. Composen avulla voimme luoda YAML-tiedoston palveluiden määrittämiseksi ja yhdellä komennolla ajaa kaiken ylös ja myös sammuttamaan ne.

```yaml
version: '3'
services:
  bitcoind: ···
  lightningd: ···
  btc_exporter: ···
  prometheus:
    image: prom/prometheus:v2.34.0
    container_name: prometheus
    restart: always
    expose:
      - 9090
    ports:
      - 9090:9090
    volumes:
      - ./config/:/config/
      - prometheus:/prometheus
    command:
      - --config.file=/config/prometheus.yml
      - --storage.tsdb.path=/prometheus
  alertmanager: ···
  grafana: ···
  nginx: ···
  dns: ···
networks: ···
volumes: ···
```

Kuvio 7 Työn Docker-compose.yml. Tässä näkyy prometheuksen asennus ja konfigurointi

5.5 Bitcoin-Core (bitcoind) käyttö

Bitcoin-Core on avoimen lähdekoodin projekti, joka ylläpitää ja julkaisee Bitcoin-asiakasohjelmistoa nimeltä “Bitcoin Core”. Se on suora jälkeläinen alkuperäisestä Bitcoin ohjelmasta, jonka Satoshi Nakamoto julkaisi.

Bitcoin-Core koostuu “full-node” ohjelmistosta lohkoketjun täydelliseen validointiin sekä myös Bitcoin lompakosta. (Bitcoincore.org www-sivut)

Bitcoin-Coresta on saatavilla kaksi variaatiota. Yksi, jossa on graafinen käyttöliittymä (jota yleisesti kutsutaan vain “Bitcoin”) ja toinen, jossa ei ole graafista käyttöliittymää ja sitä kutsutaan bitcoind. Ne ovat täysin yhteensopivia keskenään ja käyttävät samoja komentoriviargumentteja, lukevat samoja konfiguraatio tiedostoja ja lukevat ja kirjoittavat samoja data tiedostoja.

(Bitcoin.org wiki www-sivut)

Tarvitsemme bitcoind tässä työssä, jotta voimme ladata ja validoida lohkoketjun lohkoja ja transaktioita. Latasimme koko lohkoketjun erilliselle kovalevylle, jota linkitettiin uusiin palvelimiin, joita teimme. Tällä tavoin ei tarvinnut kuin kerran ladata lohkoketju kokonaisuudessaan ja pääsemme yhdistämään lohkoketjuun.

5.6 Core Lightning (c-lightning)

Core Lightning on Salamaverkko protokollan standardiyhteensopiva toteutus. Se vaatii pääsyn täysin synkronoituun bitcoind voidakseen synkronoida itsensä Bitcoin-verkkoon. Lightning-deamon kysyy bitcoind uusia lohkoja, joita se ei ole vielä käsitellyt, ja synkronoi itsensä bitcoind kanssa.

Core Lightning toteutus rakennettiin alusta alkaen hyödyntäen Lightning-tekniikan perusspesifikaatio dokumentteja täysin yhteensopivan sovelluksen rakentamiseksi. Se keskittyy tekemään perusasiat turvallisesti ja tehokkaasti. Käyttäjät voivat itse lisätä lisäosia heidän oman käyttötarpeensa mukaan. Tämän lähestymistavan haittapuoli on, että Core Lightning vaatii käyttäjältä työtä saadakseen sovelluksen pyörimään halutulla tavalla.

Tässä työssä otimme käyttöön perusasioiden lisäksi Prometheus ja helpme lisäosat. Prometheus lisäosa helpottaa datan haravoimista Salamaverkko-solmusta. Helpme lisäosa toimii apuvälineenä solmun ja kanavien avaamisessa, konfiguroinnissa ja huoltamisessa.

Core Lightning asennus ja konfiguraatio hoidettiin Docker-composen avulla. Sen kautta saimme helposti Salamaverkko solmun uudelleen konfiguroitu tai pystytetty eri palvelimelle.

5.7 Prometheus ja Grafana

Prometheus on avoimen lähdekoodin järjestelmien valvonta- ja hälytystyökalusarja. Prometheus kerää ja tallentaa metriikkansa aikasarjatietona, eli metriikkatiedot säilytetään tallennetun aikaleiman kanssa.

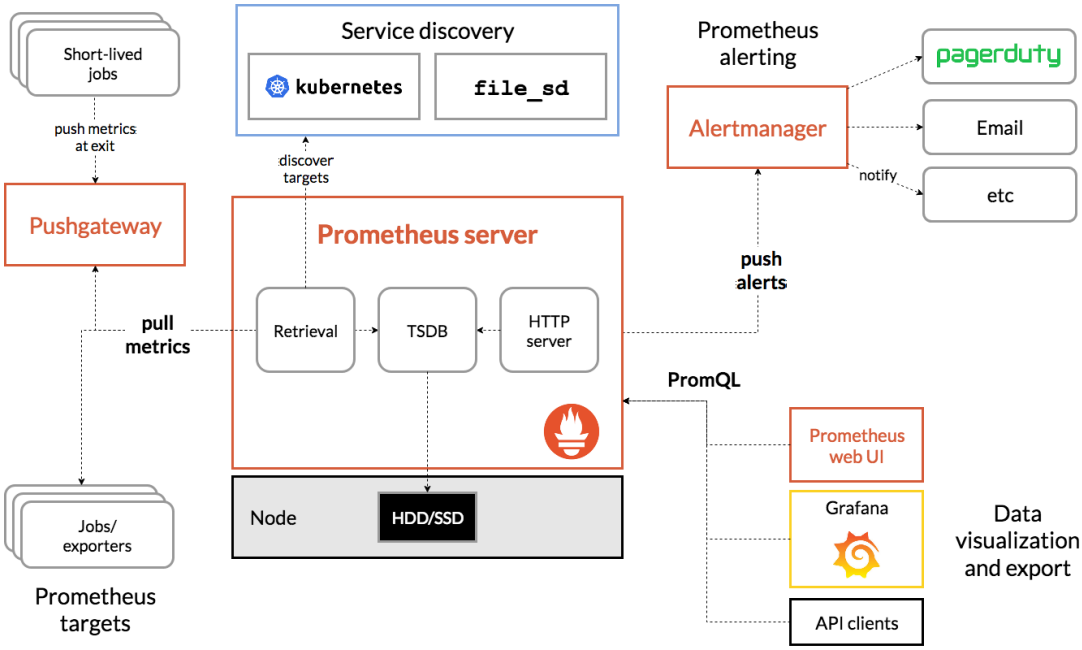
(Prometheus.io www-sivut 2022)

Datan saamiseksi Prometheus vaatii avoimen HTTP-päätepisteen. Kun päätepiste on saatavilla, Prometheus voi aloittaa haravoimaan numeerista data, kaapata sen aikasarjana ja tallentaa sen paikalliseen tietokantaan. Prometheus voidaan myös integroida etätallennustietokantaan.

Käyttäjät voivat hyödyntää kyselyitä luodakseen tilapäisiä aikasarjoja lähteestä. Nämä sarjat ovat määritelty metrien nimillä ja tunnisteilla. Kyselyt kirjoitetaan PromQL-kielellä, jonka avulla käyttäjät voivat valita ja koota aikasarjatietoja reaaliajassa. PromQL

voi myös määritellä hälytysolosuhteita, joita voit ilmoittaa ulkoisille järjestelmille kuten Gmail tai Slack.

Prometheus voi näyttää kerätyt tiedot taulukko- tai kaaviomuodossa web-pohjaisessa käyttöliittymässä. Voit myös käyttää sovelluksen rajapintoja integroidaksesi kolmannen osapuolen visualisointiratkaisuihin, kuten Grafanaan.



Kuvio 8 Tämä kaavio havainnollistaa Prometheuksen arkkitehtuuria ja sen ekosysteemi komponentteja. (Prometheus.io www-sivut)

Grafana on avoimen lähdekoodin ohjelma, jonka avulla voit tehdä kyselyitä, visualisoida, hälyttää ja tutkia mittareitasi ja tallentaa lokejasi. Grafana OSS tarjoaa työkalut, joilla voit muuttaa aikasarjatietokanta datasi selviksi kaavioiksi ja visualisoinneiksi. (Grafana.com www-sivut)

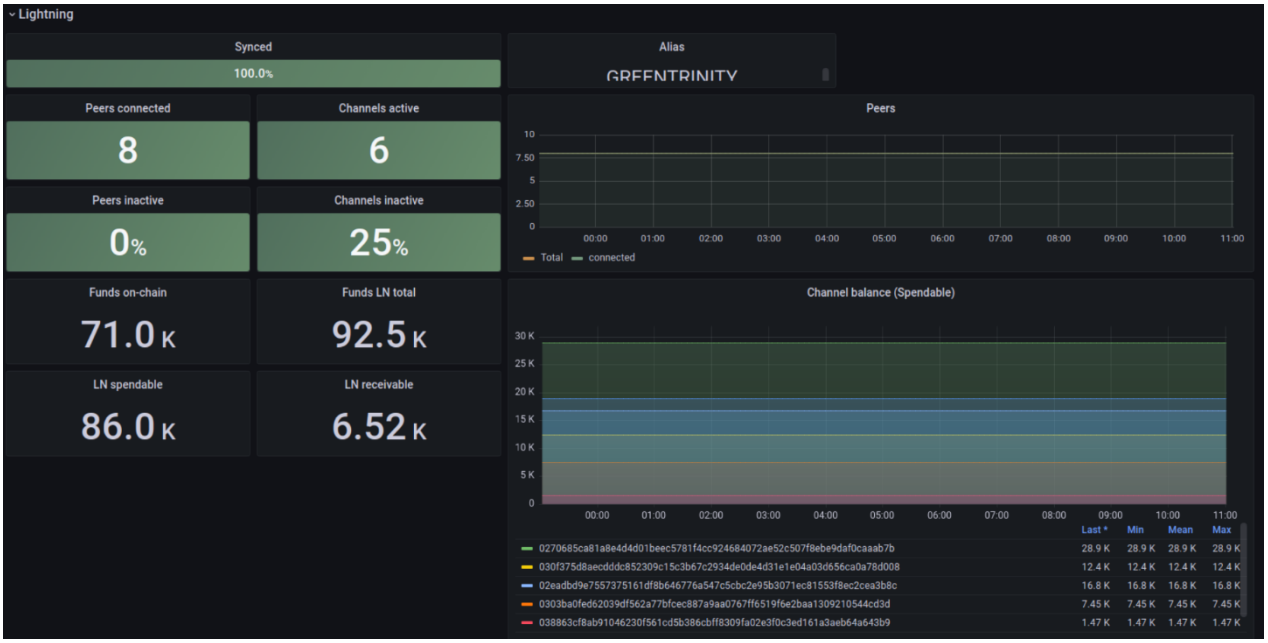
Grafana on ratkaisu data-analytiikan suorittamiseen, järkevän datan keräilyyn valtavasta datamäärästä ja sovellusten valvomiseen mukautettavien kojelaudoin avulla.

Grafana oli tässä työssä erittäin tärkeä työkalu, koska sillä pystyimme integroimaan kaikki tietolähteet yhdeksi järjestetyksi näkymäksi ja visualisoimaan niitä käyttäen Grafanan kojelautoja.

Kuvio 9 Kuva Grafana näkymästämme.

Tässä näkyy tietoja palvelimesta, jossa Salamaverkko on asennettuna ja myös että onko yhteyden lohkoketjuun kunnossa.

Grafanan avulla pystyimme helpommin seuraamaan Salamaverkko-kanavien tilannetta, balanssia ja yhteyksiä. Kaikki mitä Salamaverkko-solmuissa ja kanavissa tapahtuu, pystyy Grafanan avulla monitoroimaan ja visualisoimaan.



Kuvio 10 Tietoja meidän Salamaverkko-solmustamme ja sen yhteyksistä.

6 LOPPUAJATUKSET

Opinnäytetyön tavoitteena oli toteuttaa Salamamaksukanava ja samalla avata lukijalle käsitteet kryptovaluutta, lohkoketju ja siihen liittyvät tekniikat. Työn tärkein osa oli Salamamaksuverkon onnistuminen, jotta toimeksiantaja voi ottaa järjestelmän yrityksen käyttöön. Tämä työ sisältää kokonaisuuden Salamaverkkokanavasta, joka käy läpi tarvittavat työkalut ja menetelmät maksuverkon käynnistämiseen. Opinnäytetyö toimii hyvänä alkuna suuremmalle Salamaverkko järjestelmille.
Aiheesta ei löytynyt kokonaisvaltaista tiedon lähdettä, joten suuri osa lähteistä tässä työssä ovat artikkeleita ja kirjoitelmia.

Kokonaisuudessaan opinnäytetyö pääsi tavoitteeseensa ja tekijä oppi paljon uutta tietoa. Työn tekemistä helpotti Cervid Oy:n asiantieto, jonka avulla työn toteutuspuoli tehtiin onnistuneesti. Toimeksiantaja myös jakoi luotettavia tiedon lähteitä ja kirjoja, jonka avulla opinnäytetyö saatiin kerättyä hyvä kokonaisuus aiheesta.

LÄHTEET

Frankenfield, J. (22. Marraskuu 2022). What is Bitcoin? How to Mine, Buy and Use it. Noudettu 22.06.2022 osoitteesta https://www.investopedia.com/terms/b/bitcoin.asp

Antonopoulo, A., Osuntokun, O. & Pickhardt, R. (2022). Mastering the Lightning Network: A Second Layer Blockchain Protocol for Instant Bitcoin Payments. O'Reilly Media Inc.

Frankenfield, J. (26. Syyskuu 2022). Cryptocurrency Explained with Pros and Cons for Investment. Noudettu 30.06.2022 osoitteesta https://www.investopedia.com/terms/c/cryptocurrency.asp

Frankenfield, J (27. Toukokuu 2022). Cryptocurrency Wallet: What It Is, How It Works, Types, Security. Noudettu 04.07.2022 osoitteesta https://www.investopedia.com/terms/b/bitcoin-wallet.asp

Ammous, S. (2018). The Bitcoin Standard: The Decentralized Alternative to Central Banking. (4. Painos). John Wiley Sons Inc.

DeMartino, I. (2018) The Bitcoin guidebook – How to obtain, invest and spend the world's first decentralized cryptocurrency. (2. Painos) Skyhorse.

Bloomenthal, A. (11. Toukokuu 2022). What Determines Bitcoin's Price? Noudettu 15.07.2022 osoitteesta https://www.investopedia.com/tech/what-determines-value-1-Bitcoin/

Rosenberg, E. (22. Toukokuu 2022). How is Bitcoin Valued? Noudettu 15.07.2022 osoitteesta https://www.thebalance.com/who-sets-Bitcoin-s-price-391278

Bitcoin.org (2022). Frequently Asked Questions. bitcoin.org. Noudettu 15.07.2022 osoitteesta https://bitcoin.org/en/faq#what-determines-bitcoins-price

Rodeck, D. & Schmidt, J. (13. Toukokuu 2022). What Is A Bitcoin Wallet? Forbes.com. Noudettu 22.07.2022 osoitteesta https://www.forbes.com/uk/advisor/investing/cryptocurrency/what-is-a-bitcoin-wallet/

Reese, F. (15. Tammikuu 2018). Should I Buy Bitcoin? Bitcoinmarketjournal.com. The Pros and The Cons. Noudettu 23.07.2022 osoitteesta https://www.Bitcoinmarketjournal.com/should-i-buy-Bitcoin-now/

Adler, D. (21. Tammikuu 2018). Silk Road: The Dark Side of Cryptocurrency. Fordham Journal of Corporate & Financial Law. Noudettu 23.07.2022 osoiteesta https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/

Kryptovaluutta. (2022). Lohkoketju eli Blockchain. Haettu 24.07.2022 osoitteesta https://www.kryptovaluutta.fi/lohkoketju

Iansiti, M. & Lakhani, Karim R. (Tammikuu 2017). Hardward Business Review. The Truth About Blockchain. Haettu 29.07.2022 https://hbr.org/2017/01/the-truth-about-blockchain

Rahkola, M. (Tammikuu 2019). KATSAUS LOHKOKETJUTEKNOLOGIEN HYÖDYNTÄMISEEN SUOMESSA. EDUSKUNNAN TULEVAISUUSVALIO-KUNNAN JULKAISU. Haettu 30.07.2022 osoitteesta https://www.eduskunta.fi/FI/naineduskuntatoimii/julkaisut/Documents/NETTI_TUVJ_1_2019_Lohkoketjuteknologiat.pdf

Lewis, A. (2018.) The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and The Technology That Powers Them. https://www.2masterit.com

OECD. OECD Blockchain Primer. https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf

Etheurem.org. (3. Marraskuu 2022). PROOF-OF-STAKE (POS) Haettu 04.08.2022 osoitteesta https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

Crypto.com. (13. Toukokuu 2022). Consensus mechanisms in Blockchain: A Beginner's Guide. Haettu 10.08.2022 osoitteesta https://crypto.com/university/consensus-mechanisms-in-blockchain

Bitcoinkeskus. (21. Kesäkuu 2021). Bitcoinin salamaverkko (Lightning Network). Haettu 15.08.2022 osoitteesta https://bitcoinkeskus.com/lightning-network-salamaverkko/

River.com. (2022) River FINANCIAL. What Is the Lightning Network? Haettu 19.08.2022 osoitteesta https://river.com/learn/what-is-the-lightning-network/

Ansible.com. Ansible Documentation. Haettu 22.08.2022 osoitteesta https://docs.ansible.com/

IBM. What is Docker? Haettu 23.08.2022 osoitteesta https://www.ibm.com/cloud/learn/docker

opensource.com. What is Docker? Haettu 23.08.2022 osoitteesta https://opensource.com/resources/what-docker

BitcoinCore. Bitcoin Core RPC. Haettu 25.08.2022 osoitteesta https://bitcoincore.org/en/about/

Bitcoin Wiki. (10. Kesäkuu 2019). bitcoind. Haettu 01.09.2022 osoitteesta https://en.bitcoin.it/wiki/Bitcoind

Prometheus. What is Prometheus? Haettu 04.09.2022 osoiteesta https://prometheus.io/docs/introduction/overview/

Core-lightning. Core Lightning Documentation. Haettu 06.09.2022 osoitteesta https://lightning.readthedocs.io